S.ICZ a.s.

Na hřebenech II 1718/10

140 00 Praha 4

Protecting Data in Microsoft Online Services

Studie zpracovaná na základě poptávky Microsoft s.r.o.

Dokument:	MICR00635-STUDIE-202.docx		
Zakázka:	MICR.00635	**Verze:**	2.2
Zpracoval:	Petr Hron a kolektiv	**Stav:**	finální
Datum:	24. 5. 2016	**Počet stran:**	168

1 PREAMBULE

1.1 IDENTIFIKACE DOKUMENTU

Název dokumentu je „Protecting Data in Microsoft Online Services (Ochrana dat s využitím cloudových služeb Microsoft Online Services)“ a je zpracován na základě smlouvy o dílo MICR.00635 (ICZ) a 97285845 (Microsoft) mezi objednatelem Microsoft s.r.o. a zhotovitelem S.ICZ a.s.

1.2 ROZSAH DOKUMENTU

Tato studie se zabývá ochranou dat v prostředí online služeb společnosti Microsoft (ochranou dat v cloudových službách) z pohledu požadavků Zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále také Zákon) a navazující vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti (dále také Vyhláška).

Dokument obsahuje dvě hlavní části:

- Identifikace a analýza požadavků Zákona
- Návrh ochrany dat

1.3 UŽIVATELÉ DOKUMENTU

Dokument je určen k výhradnímu užití následující skupinou osob:

- Microsoft s.r.o.
- Osoby určené společností Microsoft s.r.o.

1.4 HISTORIE DOKUMENTU

Tab. 1 Historie dokumentu

Verze	Datum	Autor	Poznámka
1.0	4.3.2016	Petr Hron a kolektiv	Draft k připomínkování
1.1	15.3.2016	Petr Hron a kolektiv a kolektiv	Draft se zapracovanými připomínkami
2.0	24.3.2016	Petr Hron a kolektiv	Dokument k akceptaci
2.1	4.4.2016	Petr Hron a kolektiv	Finální verze dokumentu
2.2	24.5.2016	Petr Hron a kolektiv	Zapracování připomínek NBÚ

2 OBSAH

1 PREAMBULE 3
1.1 Identifikace dokumentu 3
1.2 Rozsah dokumentu 3
1.3 Uživatelé dokumentu 3
1.4 Historie dokumentu 3
2 OBSAH 4
3 SEZNAM TABULEK A OBRÁZKŮ 10
3.1 Seznam tabulek 10
3.2 Seznam obrázků 10
4 ÚVOD 11
5 OCHRANA DAT V Microsoft Online Services 12
5.1 Principy důvěryhodného cloudu 12
5.2 Vyhodnocení 13
6 OBECNÝ MODEL INFORMAČNÍHO SYSTÉMU 14
7 IDENTIFIKACE A ANALÝZA POŽADAVKŮ ZÁKONA 16
7.1 Vymezení základních pojmů 16
7.2 Působnost Zákona 17
7.3 Přístup k analýze 17
8 ORGANIZAČNÍ OPATŘENÍ 19
8.1 Systém řízení bezpečnosti informací 19
8.1.1 Identifikace požadavků 19
8.1.2 Analýza požadavků 20
8.1.3 Vzor implementace 20
8.1.4 Prostředí Microsoft Online Services 21
8.2 Řízení rizik 21
8.2.1 Identifikace požadavků 21
8.2.2 Analýza požadavků 22
8.2.3 Vzor implementace 23
8.2.4 Prostředí Microsoft Online Services 23
8.3 Bezpečnostní politika 23
8.3.1 Identifikace požadavků 23
8.3.2 Analýza požadavků 24
8.3.3 Vzor implementace 24
8.3.4 Prostředí Microsoft Online Services 25

8.4 Organizační bezpečnost 25
8.4.1 Identifikace požadavků 25
8.4.2 Analýza požadavků 26
8.4.3 Vzor implementace 26
8.4.4 Prostředí Microsoft Online Services 26

8.5 Stanovení bezpečnostních požadavků pro dodavatele 26
8.5.1 Identifikace požadavků 26
8.5.2 Analýza požadavků 27
8.5.3 Vzor implementace 27
8.5.4 Prostředí Microsoft Online Services 28

8.6 Řízení aktiv 28
8.6.1 Identifikace požadavků 28
8.6.2 Analýza požadavků 29
8.6.3 Vzor implementace 29
8.6.4 Prostředí Microsoft Online Services 29

8.7 Bezpečnost lidských zdrojů 30
8.7.1 Identifikace požadavků 30
8.7.2 Analýza požadavků 30
8.7.3 Vzor implementace 31
8.7.4 Prostředí Microsoft Online Services 31

8.8 Řízení provozu a komunikací 32
8.8.1 Identifikace požadavků 32
8.8.2 Analýza požadavků 32
8.8.3 Vzor implementace 33
8.8.4 Prostředí Microsoft Online Services 33

8.9 Řízení přístupu a bezpečné chování uživatelů 34
8.9.1 Identifikace požadavků 34
8.9.2 Analýza požadavků 34
8.9.3 Vzor implementace 35
8.9.4 Prostředí Microsoft Online Services 35

8.10 Akvizice, vývoj a údržba 36
8.10.1 Identifikace požadavků 36
8.10.2 Analýza požadavků 36
8.10.3 Vzor implementace 36
8.10.4 Prostředí Microsoft Online Services 37

8.11 Zvládání kybernetických bezpečnostních událostí a incidentů 37
8.11.1 Identifikace požadavků 37
8.11.2 Analýza požadavků 37
8.11.3 Vzor implementace 38
8.11.4 Prostředí Microsoft Online Services 38

8.12 Řízení kontinuity činností 39
8.12.1 Identifikace požadavků 39
8.12.2 Analýza požadavků 39
8.12.3 Vzor implementace 40
8.12.4 Prostředí Microsoft Online Services 40

8.13 Kontrola a audit kritické informační infrastruktury a významných informačních systémů 41
8.13.1 Identifikace požadavků 41
8.13.2 Analýza požadavků 41
8.13.3 Vzor implementace 41

8.13.4 Prostředí Microsoft Online Services....42

9 BEZPEČNOSTNÍ DOKUMENTACE....43

9.1 Bezpečnostní dokumentace správce....43
9.1.1 Identifikace požadavků....43
9.1.2 Analýza požadavků....44
9.1.3 Vzor implementace....44

9.2 Bezpečnostní dokumentace Microsoft Online Services....44
9.2.1 Microsoft Cloud Infrastructure and Operations....45
9.2.1.1 Information Security Management System for MCIO....45
9.2.1.2 MCIO Statement of Applicability....46
9.2.1.3 Certifikační zpráva z auditu ISMS....46
9.2.1.4 Další dokumenty....46
9.2.2 Microsoft Online Services....46
9.2.2.1 Podmínky služeb online pro multilicenční programy společnosti Microsoft....46
9.2.2.2 Smlouva o poskytování služeb pro služby online pro multilicenční programy společnosti Microsoft....47
9.2.2.3 Microsoft Security Policy....47
9.2.2.4 Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014....48
9.2.2.5 Microsoft Public Cloud Compliance Certification and Attestation....48
9.2.3 Microsoft Office 365....48
9.2.3.1 Office 365 Architecture and Audit Reports....48
9.2.3.2 Office 365 ISMS Manual....48
9.2.3.3 Office 365 Statement of Applicability....48
9.2.3.4 Certifikační zpráva z auditu ISMS....49
9.2.3.5 Další dokumenty....49
9.2.4 Microsoft Azure....49
9.2.4.1 Azure Statement of Applicability....49
9.2.4.2 Certifikační zpráva z auditu ISMS....49
9.2.4.3 Další dokumenty....50
9.2.5 Prostředí České republiky....50
9.2.5.1 Stanovisko NBÚ ve věci výkladu vyhlášky č. 316/2014 Sb.....50
9.2.5.2 PwC ISAE 3000 Risk Assurance Report řízení rizik v cloudu....51

10 TECHNICKÁ OPATŘENÍ....52

10.1 Fyzická bezpečnost....52
10.1.1 Identifikace požadavků na fyzickou bezpečnost....52
10.1.2 Analýza požadavků na fyzickou bezpečnost....53
10.1.3 Vzory technických opatření fyzické bezpečnosti....53
10.1.4 Prostředí Microsoft Online Services....54

10.2 Nástroj pro ochranu integrity komunikačních sítí....55
10.2.1 Identifikace požadavků na ochranu integrity komunikačních sítí....55
10.2.2 Analýza požadavků na ochranu integrity komunikačních sítí....55
10.2.3 Vzory technických opatření pro nástroj pro ochranu integrity komunikačních sítí....56
10.2.4 Prostředí Microsoft Online Services....56

10.3 Nástroj pro ověřování identity uživatelů....59
10.3.1 Identifikace požadavků na nástroj pro ověřování identity uživatelů....59
10.3.2 Analýza požadavků na Nástroj pro ověřování identity uživatelů....59
10.3.3 Vzory technických opatření pro nástroj pro ověřování identity uživatelů....60

10.3.4 Prostředí Microsoft Online Services....61

10.4 Nástroj pro řízení přístupových oprávnění....62
10.4.1 Identifikace požadavků na nástroj pro řízení přístupových oprávnění....62
10.4.2 Analýza požadavků na nástroj pro řízení přístupových oprávnění....63
10.4.3 Vzory technických opatření pro nástroj pro řízení přístupových oprávnění....63
10.4.4 Prostředí Microsoft Online Services....63

10.5 Nástroj pro ochranu před škodlivým kódem....65
10.5.1 Identifikace požadavků na nástroj pro ochranu před škodlivým kódem....65
10.5.2 Analýza požadavků na nástroj pro ochranu před škodlivým kódem....65
10.5.3 Vzory technických opatření pro nástroj pro ochranu před škodlivým kódem..66
10.5.4 Prostředí Microsoft Online Services....66

10.6 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů....68
10.6.1 Identifikace požadavků na nástroj pro zaznamenávání činností....68
10.6.2 Analýza požadavků na nástroj pro zaznamenávání činností....68
10.6.3 Vzory technických opatření pro nástroj pro zaznamenávání činností....69
10.6.4 Prostředí Microsoft Online Services....70

10.7 Nástroj pro detekci kybernetických bezpečnostních událostí....76
10.7.1 Identifikace požadavků na nástroj pro detekci kybernetických bezpečnostních událostí....76
10.7.2 Analýza požadavků na nástroj pro detekci kybernetických bezpečnostních událostí....77
10.7.3 Vzory technických opatření pro detekci kybernetických bezpečnostních událostí....77
10.7.4 Prostředí Microsoft Online Services....78

10.8 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí....80
10.8.1 Identifikace požadavků na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí....80
10.8.2 Analýza požadavků na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí....80
10.8.3 Vzory technických opatření pro sběr a vyhodnocení kybernetických bezpečnostních událostí....81
10.8.4 Prostředí Microsoft Online Services....81

10.9 Aplikační bezpečnost....83
10.9.1 Identifikace požadavků na aplikační bezpečnost....83
10.9.2 Analýza požadavků na aplikační bezpečnost....83
10.9.3 Vzory technických opatření pro aplikační bezpečnost....84
10.9.4 Prostředí Microsoft Online Services....84

10.10 Kryptografické prostředky....86
10.10.1 Identifikace požadavků na Kryptografické prostředky....86
10.10.2 Analýza požadavků na Kryptografické prostředky....87
10.10.3 Vzory technických opatření pro Kryptografické prostředky....87
10.10.4 Prostředí Microsoft Online Services....87

10.11 Nástroj pro zajišťování úrovně dostupnosti....96
10.11.1 Identifikace požadavků na Nástroj pro zajišťování úrovně dostupnosti....96
10.11.2 Analýza požadavků na Nástroj pro zajišťování úrovně dostupnosti....96
10.11.3 Vzory technických opatření pro Nástroj pro zajišťování úrovně dostupnosti ..97
10.11.4 Prostředí Microsoft Online Services....98

10.12 Bezpečnost průmyslových a řídicích systémů....101
10.12.1 Průmyslové a řídicí systémy dle §27 Vyhlášky....101

10.12.2 Ostatní průmyslové a řídící systémy 101

11 VYPOŘÁDÁNÍ POŽADAVKŮ PŘÍLOHY Č. 1 VYHLÁŠKY ... 102

11.1 Popis technologií 102
11.1.1 Azure AD 102
11.1.2 Azure Backup 103
11.1.3 Azure App Service 104
11.1.4 Azure Disk Encryption 105
11.1.5 Azure Key Vault 105
11.1.6 Azure Resource Manager 106
11.1.7 Azure RMS 107
11.1.8 Azure Security and Audit Log Management 108
11.1.9 Azure Site Recovery 109
11.1.10 Azure Storage 109
11.1.11 Azure Traffic Manager 109
11.1.12 Azure VPN Gateway 110
11.1.13 BitLocker Drive Encryption 110
11.1.14 Customer LockBox 111
11.1.15 Express Route + VPN 111
11.1.16 Integrace Identit 111
11.1.17 Microsoft Intune 113
11.1.18 Šifrování komunikace po lokální síti 114
11.1.19 Více faktorová autentizace 115
11.1.20 Centrálně spravovaná a řízená konfigurace 116
11.1.21 Office 365 Advanced Encryption 116
11.1.22 Office 365 Per-File Encryption 117
11.1.23 Office 365 Message Encryption 117
11.1.24 SQL Server Always Encrypted 118
11.1.25 SQL Server Transparent data encryption (TDE) 119

11.2 Pokrytí požadavků na opatření technologiemi 120
11.2.1 Technická opatření pro zajištění důvěrnosti 122
11.2.2 Technická opatření pro zajištění integrity 125
11.2.3 Technická opatření pro zajištění dostupnosti 128

12 NÁVRH OCHRANY DAT 130

13 DATABÁZOVÉ SYSTÉMY 131

13.1 Scénář 131

13.2 Technická opatření pro zajištění důvěrnosti 132

13.3 Technická opatření pro zajištění integrity 136

13.4 Technická opatření pro zajištění dostupnosti 140

13.5 Technická opatření nezávislá na klasifikaci dat 142

14 OFFICE 365 143

14.1 Scénář 143

14.2 Technická opatření pro zajištění důvěrnosti 144

14.3 Technická opatření pro zajištění integrity 148

14.4 Technická opatření pro zajištění dostupnosti 152

14.5 Technická opatření nezávislá na klasifikaci dat 154
15 ZÁLOŽNÍ DATOVÉ CENTRUM 155
15.1 Scénář 155
15.2 Technická opatření pro zajištění důvěrnosti 156
15.3 Technická opatření pro zajištění integrity 158
15.4 Technická opatření pro zajištění dostupnosti 160
15.5 Technická opatření nezávislá na klasifikaci dat 161
16 SEZNAM POUŽITÝCH ZKRATEK 162
17 LITERATURA 164

3 SEZNAM TABULEK A OBRÁZKŮ

3.1 SEZNAM TABULEK

Tab. 1 Historie dokumentu 3
Tab. 2 Bezpečnostní dokumentace správce 43
Tab. 3 Přehled dostupnosti vybraných služeb Microsoft Azure 99
Tab. 4 Technická opatření pro zajištění důvěrnosti 122
Tab. 5 Technická opatření pro zajištění integrity 125
Tab. 6 Technická opatření pro zajištění dostupnosti 128
Tab. 7 Technická opatření pro zajištění důvěrnosti 132
Tab. 8 Technická opatření pro zajištění integrity 136
Tab. 9 Technická opatření pro zajištění dostupnosti 140
Tab. 10 Technická opatření pro zajištění důvěrnosti 144
Tab. 11 Technická opatření pro zajištění integrity 148
Tab. 12 Technická opatření pro zajištění dostupnosti 152
Tab. 13 Technická opatření pro zajištění důvěrnosti 156
Tab. 14 Technická opatření pro zajištění integrity 158
Tab. 15 Technická opatření pro zajištění dostupnosti 160
Tab. 16 Seznam použitých zkratek 162

3.2 SEZNAM OBRÁZKŮ

Obr. 1 Ochrana dat ve vrstvách, viz [3] 12
Obr. 2 Obecný model informačního systému 14
Obr. 3 Administrátorské role Office 365 64
Obr. 4 Přístupová oprávnění webu Sharepoint 64
Obr. 5 Microsoft Antimalware for Azure Cloud Services and Virtual Machines, viz [23] 67
Obr. 6 Schéma datové sítě MCIO 78
Obr. 7 Úrovně ochrany Azure infrastruktury, viz [25] 79
Obr. 8 Životní cyklus reakce na bezpečnostní incident, viz [27] 81
Obr. 9 ExpressRoute, viz [30] 85
Obr. 10 Scénář využití Azure Key Vault 89
Obr. 11 Typy klíčů v Microsoft Azure [57] 90
Obr. 12 Scénář BYOK s Azure Key Vault 91
Obr. 13 Šifrování disků CloudLink VM, viz [66] 91
Obr. 14 Využití Azure Key Vault v Microsoft SQL Server TDE [62] 92
Obr. 15 Office 365 Advanced Encryption, viz [5] 94
Obr. 16 Komponenty Azure Backup, viz [35] 104
Obr. 17 Schema Azure Key Vault, viz [39] 106
Obr. 18 Schema Azure RMS pro Office 365, viz [31] 107
Obr. 19 Schéna federace identit, viz [9] 112
Obr. 20 Schéma izolace sítě s využitím Active Directory, viz [52] 114
Obr. 21 Schéma Azure Mutli-Factor autentizace, viz [55] 115
Obr. 22 Office 365 Message Encryption 117
Obr. 23 Schéma klíčů Always Encrypted [61] 118
Obr. 24 Schéma architektury TDE 119

4 ÚVOD

Cílem studie je poskytnout ucelený pohled na oblast působnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „Zákon“), a návazných právních předpisů zastoupených vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti (dále jen „Vyhláška“). Zejména se jedná o implementaci požadavků na organizační úrovni a o technická bezpečnostní opatření[1] v prostředích informačních a komunikačních technologií, která zahrnují služby poskytované prostřednictvím cloudových služeb Microsoft Online Services.

Studie poskytuje informace o požadavcích Zákona a návazných právních předpisů na bezpečnostní opatření informačních systémů a o způsobech jejich naplnění ve formě organizačních opatření, návodů, doporučení a architektonických vzorů pro implementaci technických opatření.

[1] Požadavky na bezpečnostní opatření ve smyslu §4, odstavec (1) ZoKB jsou uvedeny v §5, odstavec a) a b) ZoKB a rozvedeny v §3-29 VoKB.

5 OCHRANA DAT V Microsoft Online Services

5.1 PRINCIPY DŮVĚRYHODNÉHO CLOUDU

Společnost Microsoft věří, že organizace potřebují silného partnera, který jim nejenom pomůže chránit jejich data, ale také jim pomůže se splněním regulatorních požadavků vyplývající z legislativy a norem. Takový partner by měl nejenom poskytovat technologická řešení a jejich neustálé zlepšování, ale i průběžně sledovat a implementovat regulatorní požadavky, a to vše dostatečně transparentním způsobem umožňujícím organizaci se ujistit o potřebné úrovni bezpečnostních opatření. Microsoft buduje technologie, datová centra a procesy tak, aby mohl být tímto partnerem v oblasti Cloud Computing, viz [3].

Společnost Microsoft se zaměřila na čtyři oblasti, ve kterých kterých naplňuje principy důvěryhodného cloudu:

- Bezpečnost
- Ochrana soukromí
- Shoda s požadavky
- Transparentnost

Ochrana dat v cloudových službách Microsoft Online Services je poskytována ve třech vrstvách (fyzická, logická, datová) pomocí různých opatření a technologií, viz například dokument [56].

Obr. 1
Ochrana dat ve vrstvách, viz [3]

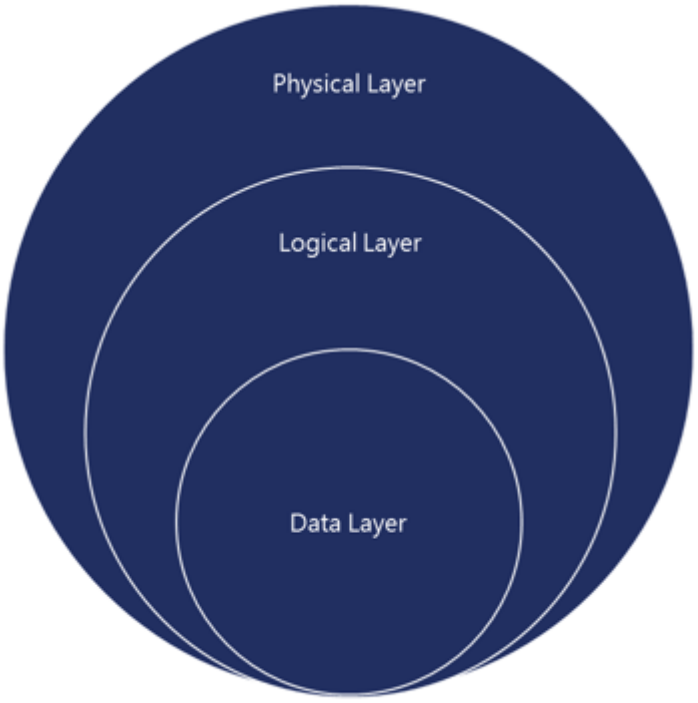


Figure 1 - Multiple layers of defense in depth

Mezi opatření patří:

- Fyzická vrstva:
  - Ochrana datových center.
  - Ochrana sítí.

- Logická vrstva:
  - Zavedení a řízení bezpečnosti, viz kapitola 8.1.4.
  - Organizační bezpečnost.
  - Bezpečný vývoj software.
  - Proces přístupu administrátorů cloudových služeb k datům zákazníků (Lockbox).
  - Správa konfigurací, bezpečnostní aktualizace, ochrana před škodlivým kódem.
  - Ochrana síťové infrastruktury.
  - Oddělení jednotlivých zákazníků.
  - Ochrana před bezpečnostními hrozbami.
  - Zákazníky řízená:
    - Bezpečnost.
    - Soukromí.
    - Soulad s požadavky.
- Datová vrstva:
  - Ochrana na úrovni sítě, při přenosu dat po síti.
  - Ochrana na úrovni pevných disků serverů a diskových polí.
  - Na úrovni souborového systému.
  - Ochrana na úrovni informace (soubor, mail) při přenosu i při jejím uložení.
  - Ochrana na úrovni databáze SQL.
  - Ochrana na úrovni sloupce tabulky databáze SQL.

5.2 VYHODNOCENÍ

Úroveň a způsob realizace bezpečnostních opatření v cloudových službách Microsoft Online Services umožňuje za předpokladu implementace níže uvedených opatření z oblasti organizační a technické bezpečnosti pokrýt požadavky Zákona a Vyhlášky v oblasti sdílených služeb.

Uvedené pokrytí se týká explicitně uvedených požadavků Zákona a Vyhlášky, a proto je možné, že u konkrétní implementace budou na základě hodnocení rizik provedeného organizací v některých oblastech požadavky na bezpečnostní opatření zvýšeny. Avšak i v tomto případě je možné předpokládat pokrytí daného požadavku jedním z nástrojů nabízených buď přímo společností Microsoft, nebo jejími partnery.

Vlastní bezpečnostní opatření realizovaná společností Microsoft v cloudových službách Microsoft Online Services jsou vyspělá a jsou na vysoké úrovni. Vzhledem k úsilí, rozsahu investic a úrovni standardizace těchto opatření bude pro lokální organizace poskytující cloudové služby v České republice velmi obtížné realizovat stejná opatření ve srovnatelném rozsahu a kvalitě.

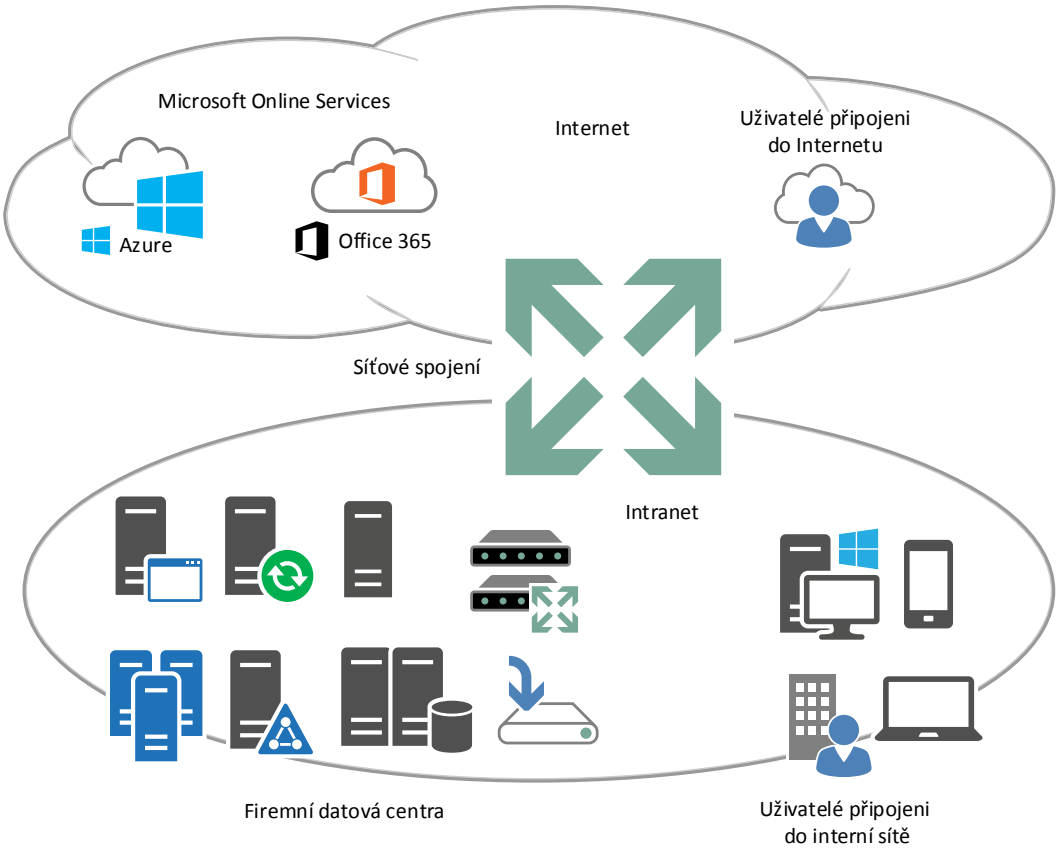
Poznámka: Při posuzování požadavků systému řízení bezpečnosti je třeba zohlednit skutečnost, že v cloudových službách obecně není možné garantovat výhradní přístup k šifrovacím klíčům umístěným v operační paměti počítačů, protože není možné zajistit výhradní fyzický přístup k počítačům pro vlastníky nebo autorizované uživatele klíčů. V cloudových službách Microsoft Online Services existují služby a technologie, viz kapitoly 10.10.4 a 11.1, které umožňují pro kryptografické operace použít on-premise generované klíče, které jsou nahrány do HSM provozovaných v rámci cloudových Microsoft Online Services (BYOK) ve kterých pak probíhají operace s klíči. Možnost využít tyto technologie závisí na architektuře konkrétního informačního systému. Jejich použití jako součástí technických opatření pak pro konkrétní situaci přispívá k naplnění bezpečnostních požadavků.

6 OBECNÝ MODEL INFORMAČNÍHO SYSTÉMU

Pro potřeby identifikace a analýzy požadavků Zákona je vytvořen obecný model informačního systému. Tento model zahrnuje cloudové služby Microsoft Online Services (Microsoft Azure a Office 365), on-premise datová centra, interní i veřejné počítačové sítě a koncová uživatelská zařízení (osobní počítače, notebooky, mobilní telefony a tablety a další zařízení umožňující uživateli zpracovávat data), viz Obr. 2. Pro potřeby obecného modelu informačního systému jsou operace s daty rozděleny na:

- Uložení dat – umístění dat na trvalém paměťovém úložišti – například na disku, paměťové kartě, optickém disku, diskovém poli nebo na zálohovací pásce – v koncovém uživatelském zařízení, on-premise datovém centru nebo v cloudové službě
- Zpracování dat – operace s daty, které zahrnují jejich přenos do operační paměti serverů nebo uživatelských zařízení, jejich zpracování procesorem a také jejich přenos po počítačové síti a jejich zobrazení na displeji

Obr. 2
Obecný model informačního systému



Zatímco ochrana jednotlivých centrálních komponent (které jsou zároveň i aktivy vyžadujícími ochranu) výše popsaného obecného modelu informačního systému je logická a obecně i očekávaná, v případě koncových uživatelských zařízení je situace méně jasná, a velmi záleží na konkrétní implementaci poskytované služby resp. služeb.

První otázkou, na kterou je vhodné odpovědět je, zda je dané zařízení (aktivum) zahrnuto do rozsahu systému řízení bezpečnosti informací[2] ve smyslu Vyhlášky, přičemž vzhledem k obtížné

[2] V některých případech je systém řízení bezpečnosti informací označován zkratkou ISMS (z anglického Information security management system). Pojem ISMS je však velmi často spojován

ochraně některých typů koncových uživatelských zařízení (např. chytrých mobilních telefonů) může existovat snaha tato zařízení do rozsahu nezařazovat. Obecně by mělo platit, že pokud zařízení obsahuje informace organizace (pravděpodobný případ) anebo poskytuje služby jiným zařízením nebo více uživatelům (méně pravděpodobný případ), potom by do rozsahu systému řízení bezpečnosti informací zařazeno býti mělo. Z tohoto vyplývá i nutnost toto zařízení, resp. na něm uložené informace, chránit pomocí bezpečnostních opatření, a to v plném rozsahu požadavků Vyhlášky.

Druhá otázka je, zdali je nutné zařízení chránit i v případě, kdy není v rozsahu systému řízení bezpečnosti informací, a tedy neobsahuje informace organizace nebo neposkytuje služby jiným zařízením nebo více uživatelům. V tomto případě platí, že pokud je ze zařízení přistupováno ke službám informačního systému, potom je nutné toto zařízení chránit pomocí bezpečnostních opatření minimálně tak, aby tak aby nebylo možné získat autentizační údaje ke službě, získat zobrazované informace anebo upravit zadávané informace.

---

se standardem ISO/IEC 27001 (resp. jeho předchůdcem BS 7799-2), který jej dostal do širšího povědomí odborné veřejnosti. Protože v tomto dokumentu primárně nepředpokládáme, že bude implementován systém řízení bezpečnosti informací podle standardu IEO/IEC 27001, ale spíše systém řízení bezpečnosti informací vycházející z požadavků vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, která s pojmem ISMS neoperuje, je v tomto dokumentu cíleně používáno obecnější označení „systém řízení bezpečnosti informací“ resp. pouze „systém řízení“.

7 IDENTIFIKACE A ANALÝZA POŽADAVKŮ ZÁKONA

V kapitolách 8, 9, 10 a 11 je provedena identifikace a analýza požadavků Zákona a Vyhlášky na obecný model informačního systému.

7.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

Před zahájením vlastí analýzy je vhodné zopakovat pár základních pojmů použitých v Zákoně a Vyhlášce.

Aktivum

Pojem aktivum je výčtem definován v § 2 Zákona, kde je určeno, že aktivem může být primární aktivum (informace nebo služba) nebo podpůrné aktivum (technické vybavení, komunikační prostředky, programové vybavení, zaměstnanci a dodavatelé). Stručně řečeno se jedná o cokoliv, co má pro organizaci nebo i jednotlivce hodnotu a je buď samo informací anebo s ní souvisí.

Bezpečnostní opatření

Pojem bezpečnostní opatření je definován v § 4 Zákona jako souhrn úkonů, jejichž cílem je zajištění bezpečnosti, dostupnosti a spolehlivosti, přičemž bezpečnostní opatření jsou dělena na organizační a technická.

Kybernetická bezpečnostní událost

Pojem kybernetická bezpečnostní událost je definován v § 7 Zákona, jako je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Stručně řečeno se jedná o potenciální (nepotvrzený) bezpečnostní incident.

Kybernetický bezpečnostní incident

Pojem kybernetický bezpečnostní incident je definován v § 7 Zákona jako narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Riziko

Pojem riziko je definován v § 2 Vyhlášky jako možnost, že určitá hrozba využije zranitelnosti informačního systému a způsobí poškození aktiva.

Hrozba

Pojem hrozba je definován v § 2 Vyhlášky jako potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.

Zranitelnost

Pojem zranitelnost je definován v § 2 Vyhlášky jako slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

7.2 PŮSOBNOST ZÁKONA

Zákon a tedy i na něj navazující Vyhláška neklade požadavky na bezpečnostní opatření všech informačních a komunikačních systémů (dále jen „IS“), ale klade požadavky na IS, které jsou důležité pro zachování funkce základních služeb společnosti, a to včetně služeb orgánů veřejné moci.

Konkrétně se jedná o IS[3] určené jako

- kritická informační infrastruktura (dále jen „KII“), což podle definice v § 2 Zákona je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy nebo
- významný informační systém (dále jen „VIS“), což podle definice v § 2 Zákona je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Obecně platí, že požadavky na bezpečnostní opatření KII jsou přísnější než požadavky na bezpečnostní opatření VIS.

Zákon klade požadavky na správce KII nebo VIS, tedy na organizace, které určují účel zpracování informací a podmínky provozování informačního systému. Tito správci mají následně povinnost zavést požadovaná bezpečnostní opatření podle § 5 Zákona.

IS se stane KII určením, které může nabývat formy uvedením v příloze nařízení vlády nebo opatřením obecné povahy.

IS se stane VIS po posouzení určujících kritérií správcem a následným nahlášením kontaktních údajů na NBÚ nebo uvedením v příloze vyhlášky o VIS.

Kromě výše uvedených IS a jejich provozovatelů Zákon klade požadavky i na poskytovatele služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a orgány nebo osoby zajišťující významnou síť. Vzhledem ke skutečnosti, že tyto požadavky nezahrnují preventivní implementaci bezpečnostních opatření, nejsou tyto subjekty v této analýze dále zohledněny.

7.3 PŘÍSTUP K ANALÝZE

Struktura analýzy kopíruje strukturu Vyhlášky. Je tedy rozdělena podle bezpečnostních opatření, a to nejprve organizačních (přičemž související dokumentace je uvedena samostatně) a následně technických.

V rámci každého bezpečnostního opatření je

- identifikován zdroj požadavků odkazem do Vyhlášky (a případně Zákona),
- shrnuty požadavky na bezpečnostní opatření pro významné informační systémy a prvky kritické informační a komunikační infrastruktury,
- analyzovány identifikované požadavky v rámci uvedeného modelu IS a
- stručně popsán způsob resp. způsoby implementace bezpečnostního opatření v rámci uvedeného modelu IS, které zajistí pokrytí výše identifikovaných požadavků a
- popsáno jak je uvedené opatření implementované v prostředí Microsoft Online Services.

[3] Správně se jedná jak o informační systémy, tak i komunikační systémy. Z důvodu zvýšení přehlednosti budeme dále v analýze mezi IS zahrnovat i komunikační systémy.

Při čtení analýzy je nutné si uvědomit, že požadavky Zákona a Vyhlášky na bezpečnostní opatření informačních systémů určených VIS nebo KII definují základní (převážně minimální) úroveň požadavků, které mohou být na základě provedené analýzy rizik

- zvýšeny (zpřísněny) – platí pro všechna opatření nebo
- sníženy (zlehčeny) – platí pouze pro opatření, kde je tato možnost Vyhláškou explicitně umožněna.

Z toho důvodu v případech, kdy

- je možné očekávat zvýšení požadavků na bezpečnostní opatření,
- je možné očekávat snížení požadavků na bezpečnostní opatření anebo
- kdy je požadavek Vyhlášky záměrně neurčitý (Vyhláška je cíleně implementačně nezávislá),

popis implementace, vzhledem k předpokládanému modelu IS, tuto skutečnost zohledňuje a popisuje nejpravděpodobnější způsob implementace. Na danou skutečnost (odchylku) je vždy explicitně upozorněno.

8 ORGANIZAČNÍ OPATŘENÍ

Seznam organizačních opatření je uveden v § 5, odstavec 2 Zákona, přičemž požadavky na tato opatření jsou rozvedeny v § 3 – § 15 Vyhlášky (část druhá, hlava I).

8.1 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Požadavky na systém řízení bezpečnosti informací (dále i jenom „systému řízení“) jsou specifikovány v §3 Vyhlášky.

8.1.1 IDENTIFIKACE POŽADAVKŮ

V plnění požadavků na systém řízení bezpečnosti informací je po správci IS určeného jako **VIS** požadováno

- řídit rizika,
- vytvořit a schválit bezpečnostní politiku v oblasti systému řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanovit bezpečnostní politiku v dalších oblastech,
- zavést příslušná bezpečnostní opatření,
- provádět aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.

V případě správce IS určeného jako **KII** je požadována vyšší úroveň zabezpečení, v rámci které správce musí

- stanovit rozsah a hranice systému řízení bezpečnosti informací, ve kterém určí, kterých prvků se systém řízení bezpečnosti informací týká,
- řídit rizika,
- vytvořit a schválit bezpečnostní politiku v oblasti systému řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanovit bezpečnostní politiku v dalších oblastech,
- zavést příslušná bezpečnostní opatření,
- monitorovat účinnost bezpečnostních opatření,
- vyhodnocovat vhodnost a účinnost bezpečnostní politiky,
- zajistit provedení auditu kybernetické bezpečnosti, a to nejméně jednou ročně,
- zajistit vyhodnocení účinnosti systému řízení bezpečnosti informací,
- aktualizovat systém řízení bezpečnosti informací a příslušnou dokumentaci a
- řídit provoz a zdroje systému řízení bezpečnosti informací a zaznamenávat činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

8.1.2 ANALÝZA POŽADAVKŮ

Vlastní model systému řízení bezpečnosti informací je v principu nezávislý na zvoleném nebo daném modelu informačního systému. Dílčí části a postupy řízení bezpečnosti informací, jako například rozsah a hranice systému řízení bezpečnosti informací, postupy řízení, obsah bezpečnostní politiky a provedení auditu je samozřejmě modelem informačního systému více či méně ovlivněno (což bude popsáno v následujících kapitolách). Vlastní postupy řízení by však měly být dostatečně implementačně nezávislé, aby je konkrétní model informačního systému neovlivnil.

V případě systému řízení bezpečnosti informací požadovaném Vyhláškou platí, že některé požadavky na KII, které nejsou pro VIS povinné, budou muset být implementovány i v prostředí VIS, neboť vyplývají z kontextu ostatních požadavků. Zejména se toto týká následujících požadavků:

- Stanovit rozsah a hranice systému řízení bezpečnosti informací, neboť jak bezpečnostní politika systému řízení, tak i návazné politiky musí být konkrétní a proto musí jasně definovat, čeho se týkají a čeho již ne.
- Řídit provoz a zdroje systému řízení bezpečnosti informací, neboť pokud má být systém řízení bezpečnosti informací funkční a ne pouze formální, existující jen ve formě politiky, bude vyžadovat zdroje, a bude nutné tyto zdroje řídit.

8.1.3 VZOR IMPLEMENTACE

Implementace systému řízení bezpečnosti informací se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně:

- stanovit rozsah a hranice systému řízení bezpečnosti informací,
- provést hodnocení rizik, navrhnout opatření pro snížení rizik a akceptovat přijatelná (zbytková) rizika (viz kapitola 8.2),
- vytvořit a schválit bezpečnostní politiku v oblasti systému řízení bezpečnosti informací (viz kapitola 8.3),
- vytvořit a schválit bezpečnostní politiku v dalších oblastech, a to i na základě opatření navržených v průběhu analýzy rizik (viz kapitola 8.3),
- zavést[4] příslušná bezpečnostní opatření (viz. kapitoly 8 až 11 této analýzy),
- provádět aktualizaci bezpečnostní dokumentace systému řízení (zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí), a to nejméně jednou za tři roky nebo v souvislosti se změnami a
- řídit provoz a zdroje systému řízení bezpečnosti informací.

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně:

- stanovit rozsah a hranice systému řízení bezpečnosti informací,
- provést hodnocení rizik, navrhnout opatření pro jejich snížení a akceptovat přijatelná (zbytková) rizika (viz kapitola 8.2),
- vytvořit a schválit bezpečnostní politiku v oblasti systému řízení bezpečnosti informací (viz kapitola 8.3),

[4] Zavedení opatření v sobě obsahuje jeho návrh, nasazení, používání, kontrolu a případné úpravy na základě výsledků kontroly nebo jiných podkladů.

- vytvořit a schválit bezpečnostní politiku v dalších oblastech, a to i na základě opatření navržených v průběhu analýzy rizik (viz kapitola 8.3),
- zavést příslušná bezpečnostní opatření (viz. kapitoly 8 až 11 této analýzy),
- zajistit zpětnou vazbu ve formě monitorování účinnosti bezpečnostních opatření, vyhodnocování vhodnosti a účinnost bezpečnostní politiky, prováděním auditu kybernetické bezpečnosti a vyhodnocení účinnosti systému řízení bezpečnosti informací,
- aktualizovat systém řízení bezpečnosti informací a příslušnou dokumentaci,
- řídit provoz a zdroje systému řízení bezpečnosti informací a zaznamenávat činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

8.1.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services je u klíčových služeb zaveden systém řízení bezpečnosti informací, certifikovaný v souladu s normou ISO/IEC 27001:2013, přičemž v rámci analyzovaného modelu informačního systému jsou relevantní následující procesy/služby:

- Microsoft's Cloud Infrastructure and Operations,
- Office 365 a
- Microsoft Azure.

Skutečnost, že výše uvedené procesy/služby jsou certifikované podle ISO/IEC 27001:2013 nemá přímý vliv na systém řízení bezpečnosti informací správce, jedná se však o formu ujištění, že služby a procesy související s outsourcingem, splňují normou stanovené bezpečnostní požadavky.

8.2 ŘÍZENÍ RIZIK

Požadavky na řízení rizik jsou specifikovány v § 4 a Příloze č. 2 Vyhlášky.

8.2.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků řízení rizik je po správci IS určeného jako **VIS** požadováno

- stanovit metodiku pro identifikaci a hodnocení aktiv a rizik včetně stanovení kritérií pro přijatelnost rizik,
- provést vlastní hodnocení (analýzu) rizik, tedy
  - identifikovat a hodnotit důležitost primárních aktiv (tedy informací a služeb), a to včetně hodnocení popsaného v § 8 Vyhlášky (řízení aktiv), která patří do rozsahu systému řízení. Výstupy zapracovat do zprávy o hodnocení aktiv a rizik,
  - identifikovat rizika, při kterých zohlední hrozby a zranitelnosti, posoudit možné dopady na aktiva, hodnotit tato rizika minimálně v rozsahu podle Přílohy č. 2 Vyhlášky. Výstupy zapracovat do zprávy o hodnocení aktiv a rizik,
- zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které bude obsahovat přehled vybraných a zavedených bezpečnostních opatření,
- zpracovat a zavést plán zvládání rizik, který bude obsahovat cíle a přínosy bezpečnostních opatření pro zvládání rizik, určovat odpovědné osoby, potřebné zdroje, termíny a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními,
- zohlednit bez zbytečného odkladu reaktivní a ochranná opatření vydaná NBÚ v hodnocení rizik a
- při hodnocení rizik zohlednit hrozby a zranitelnosti uvedené ve Vyhlášce.

Správce IS určeného jako **KII** má shodné povinnosti, má však povinnost identifikovat a hodnotit důležitost jak primárních, tak i podpůrných aktiv a musí zohlednit rozsáhlejší seznam hrozeb a zranitelností.

Vyhláška umožňuje používat i jiné způsoby řízení rizik za předpokladu, že zajistí stejnou nebo vyšší úroveň řízení rizik.

8.2.2 ANALÝZA POŽADAVKŮ

Pravidla a postupy hodnocení a řízení rizik (běžně reprezentované metodikou pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik) jsou v principu nezávislá na zvoleném nebo daném modelu informačního systému. Tato pravidla mohou vycházet z norem ISO/IEC 27005:2011 (Information technology - Security techniques - Information security risk management) a ISO 31000:2009 (Risk management - Principles and guidelines).

Průběh a výstupy vlastního hodnocení rizik jsou však modelem informačního systému ovlivněny výrazně – na každé aktivum informačního systému s určitou hodnotou se mohou uplatňovat různé hrozby o různých úrovních a zároveň mohou obsahovat různé typy a úrovně zranitelností. Z tohoto důvodu je vhodné pro každé aktivum informačního systému stanovit jeho hodnotu, existující zranitelnosti, související hrozby, zavedená bezpečnostní opatření a případně navrhnout nová bezpečnostní opatření.

Toto je nutné provést i v případě služeb zajišťovaných dodavatelem (například poskytovatelem cloudových služeb), kde je nutné počítat s jinými typy nebo projevy hrozeb a s potenciálně omezenými možnostmi správce ovlivnit množinu a úroveň zavedených bezpečnostních opatření.

Informace o opatřeních zavedených poskytovatelem outsourcovaných (cloudových) služeb je možné zejména získat (seřazeno podle míry záruky od nejnižší k nejvyšší) zejména následujícími způsoby:

(1) prohlášením poskytovatele služeb bez další kontroly,

(2) prohlášením poskytovatele služeb a ověřením nezávislým auditem a

(3) kontrolou u poskytovatele služeb[5].

Optimálním způsobem získání potřebných informací je druhá možnost, která může nabývat podoby dokumentace potřebné k certifikaci systému řízení bezpečnosti informací podle ISO/IEC 27001:

- prohlášení poskytovatele služeb o typech a rozsahu implementovaných bezpečnostních opatření (ve smyslu „CO“ bylo implementováno) – smlouva nebo všeobecné obchodní podmínky, bezpečnostní politika, prohlášení o aplikovatelnosti a případně další doplňující dokumenty a
- ověřením nezávislým auditem (ve smyslu „JAK DOBŘE“ bylo implementováno) – platný certifikát systému řízení bezpečnosti informací podle ISO/IEC 27001 a/nebo zpráva z auditu.

Poznámka: pro KII je v § 7 specificky požadováno hodnotit rizika spojená s dodávkami, tedy mimo jiné s outsourcovanými (cloudovými) službami.

[5] Tuto variantu je možné použít pouze u malých poskytovatelů a vyžaduje vysokou odbornost kontrolující osoby.

8.2.3 VZOR IMPLEMENTACE

Implementace řízení rizik se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** a **KII** minimálně

- stanovit metodiku pro identifikaci a hodnocení aktiv a rizik včetně stanovení kritérií pro přijatelnost rizik,
- provést hodnocení rizik, navrhnout opatření pro jejich snížení a akceptovat přijatelná (zbytková) rizika,
- zpracovat zprávu o hodnocení aktiv a rizik,
- zpracovat prohlášení o aplikovatelnosti,
- zpracovat a zavést plán zvládání rizik.

8.2.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Vzhledem k celosvětové působnosti společnosti Microsoft, a tedy i služeb Microsoft Online Services, je kontrola zavedených opatření prováděna vůči požadavkům různých norem a standardů, přičemž záznamy těchto kontrol jsou zákazníkům dostupné ve formě auditních zpráv (viz kapitola 9.2).

V rámci analyzovaného modelu informačního systému zahrnujícího služby Office 365 a Microsoft Azure je možné rozsah a stav zavedených bezpečnostních opatření zjistit z následujících dokumentů:

- Bezpečnostní politika „Microsoft Security Policy (External)“
- Prohlášení o aplikovatelnosti pro jednotlivé služby
- Zprávy z auditu podle normy ISO/IEC 27001

Konkrétní názvy dokumentů jsou uvedeny v kapitole 9.2.

Kromě toho platí, že společnost Microsoft provádí hodnocení a řízení rizik dle své metodiky, jejíž jádro je z velké části založeno na normách ISO/IEC 27001, ISO/IEC 27005 a je v souladu se standardem NIST 800-30. Soulad této metodiky s požadavky Vyhlášky byl hodnocen nezávislým auditorem, o jehož zprávě pojednává kapitola 9.2.5.2.

8.3 BEZPEČNOSTNÍ POLITIKA

Požadavky na bezpečnostní politiku jsou specifikovány v § 5 Vyhlášky.

8.3.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění těchto požadavků je po správci IS určeného jako **VIS** požadováno zavést bezpečnostní politiku v oblastech

- systém řízení bezpečnosti informací,
- organizační bezpečnost,
- řízení dodavatelů,
- klasifikace aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací,

- řízení přístupu,
- bezpečné chování uživatelů,
- zálohování a obnova,
- poskytování a nabývání licencí programového vybavení a informací,
- ochrana osobních údajů,
- používání kryptografické ochrany,
- ochrana před škodlivým kódem a
- nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.

Pro naplnění identifikovaných požadavků musí správce **KII** zavést bezpečnostní politiku ve stejných oblastech jako správce VIS, a navíc v oblastech

- bezpečné předávání a výměna informací,
- řízení technických zranitelností,
- bezpečné používání mobilních zařízení,
- dlouhodobé ukládání a archivace informací,
- fyzická bezpečnost,
- bezpečnost komunikační sítě a
- využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

Dále správci musí pravidelně hodnotit účinnost bezpečnostní politiky a aktualizovat ji.

8.3.2 ANALÝZA POŽADAVKŮ

Vytvoření a zavedení bezpečnostní politiky je v principu nezávislé na zvoleném nebo daném modelu informačního systému.

To se však již netýká vlastního obsahu bezpečnostní politiky, který naopak musí zohledňovat model informačního systému s tím, že vlastní úroveň zohlednění je daná úrovní podrobnosti (detailem) politiky.

V případě, kdy jsou některé služby zajišťované dodavatelem, by politika alespoň částečně měla zohledňovat specifikace implementace a kontroly bezpečnostních opatření u dodavatele, jako například poskytovatele outsourcovaných (cloudových) služeb.

8.3.3 VZOR IMPLEMENTACE

Implementace bezpečnostní politiky se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** a **KII** minimálně

- vytvořit návrh politiky ve formě jednoho nebo více dokumentů, přičemž politika musí pokrývat oblasti požadované Vyhláškou (viz kapitola 9.1),
- návrh politiky přijmout ve formě závazného předpisu,
- nastavit proces hodnocení účinnosti bezpečnostní politiky (viz kapitola 8.13) a její aktualizace.

8.3.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services je implementováno množství bezpečnostních politik (a návazných bezpečnostních standardů), přičemž většina z nich je z bezpečnostních důvodů dostupná pouze pracovníkům společnosti Microsoft.

Pro zákazníky využívající služby Office 365 a Microsoft Azure jsou k dispozici dokumenty popisující zavedená opatření a jejich úroveň s podrobností nabízející základní přehled o opatřeních, ale zároveň nezvyšující rizika služeb Microsoft Online Services. Zejména se jedná o následující dokumenty:

- Bezpečnostní politika „Microsoft Security Policy (External)“
- Dokument „Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014“
- Zprávy z auditu podle normy ISO/IEC 27001

Konkrétní názvy dokumentů jsou uvedeny v kapitole 9.2.

8.4 ORGANIZAČNÍ BEZPEČNOST

Požadavky na organizační bezpečnost jsou specifikovány v §6 Vyhlášky.

8.4.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků organizační bezpečnosti je po správci IS určeného jako **VIS** požadováno

- zavést organizaci řízení bezpečnosti informací,
- určit výbor pro řízení kybernetické bezpečnosti a
- určit bezpečnostní role (přiměřeně k rolím požadovaným po správci KII – viz dále) a jejich práva a povinnosti související s informačním systémem.

Pro naplnění identifikovaných požadavků musí správce **KII**

- zavést organizaci řízení bezpečnosti informací,
- určit výbor pro řízení kybernetické bezpečnosti a
- určit bezpečnostní role a jejich práva a povinnosti související s informačním systémem, konkrétně role
  - manažer kybernetické bezpečnosti,
  - architekt kybernetické bezpečnosti,
  - auditor kybernetické bezpečnosti a
  - garant aktiva.

Vyhláška dále definuje kvalifikační požadavky na osoby obsazující role pro **KII** uvedené výše a povinnost tyto osoby odborně proškolit. Odborně proškoleny musí být i osoby obsazené do bezpečnostních rolí v IS určeném jako **VIS**.

8.4.2 ANALÝZA POŽADAVKŮ

Oblast organizační bezpečnosti je v principu nezávislá na zvoleném nebo daném modelu informačního systému.

Zvolený model informačního systému se však částečně může odrážet v požadavcích na kvalifikaci jednotlivých osob a v odpovědnosti jednotlivých rolí (např. znalost bezpečnostních opatření typických pro cloudové poskytovatele služeb, odpovědnost za sledování a vyhodnocování zavedených bezpečnostních opatření u poskytovatele cloudových služeb, apod.)

8.4.3 VZOR IMPLEMENTACE

Implementace organizační bezpečnosti se (stejně jako převážná většina organizačních opatření) skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** a **KII** minimálně

- určit výbor pro řízení kybernetické bezpečnosti, jeho práva a povinnosti související s informačním systémem a
- definovat bezpečnostní role a jejich práva a povinnosti související s informačním systémem,
- tyto role obsadit a
- proškolit osoby v těchto rolích minimálně v oblasti jejich práv, povinností a odpovědnosti.

8.4.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) je definována odpovědnost jednotlivých rolí v oblasti bezpečnosti informací i odpovědnost za bezpečnost informací celkově a jsou stanoveny požadavky na oddělení jednotlivých rolí. Kromě toho jsou zavedené týmy odpovědné za řešení bezpečnosti v konkrétních oblastech. Bližší podrobnosti je možné nalézt v dokumentech uvedených v kapitole 9.2.

Uvedené role však nijak nesouvisí s rolemi zavedenými správcem.

8.5 STANOVENÍ BEZPEČNOSTNÍCH POŽADAVKŮ PRO DODAVATELE

Minimální rozsah bezpečnostních požadavků pro dodavatele je specifikován v §7 Vyhlášky.

8.5.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** požadováno

- zavést pravidla pro dodavatele, která vychází z provedeného hodnocení rizik, a to pro dodavatele nebo jiné osoby, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti informačního systému a
- uzavřít s dodavatelem smlouvu definující rozsah zapojení dodavatele a obsahující ustanovení o bezpečnosti informací.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc

- před uzavřením smlouvy provést hodnocení rizik spojených s dodávanými službami, a to v souladu s přílohou č. 2 Vyhlášky,
- uzavřít smlouvu o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,
- provádět pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a
- zjištěné nedostatky v zavedených bezpečnostních opatřeních odstranit (sám nebo po dohodě s dodavatelem služby).

8.5.2 ANALÝZA POŽADAVKŮ

Tato oblast (na rozdíl od ostatních oblastí) je s modelem informačního systému svázána velice úzce. Požadavky na dodavatele budou pravděpodobně stanoveny v politice každého správce, neboť v současné době není možné předpokládat, že by bylo možné vybudovat a provozovat důležitý informační systém bez alespoň částečného zapojení dodavatelů. Odlišnosti budou dané úrovní zapojení dodavatele – je rozdíl mezi poskytováním podpory druhé úrovně na jedné straně a kompletním outsourcingem služby do cloudu na straně druhé.

Zákon a Vyhláška využití dodavatelů (a to i ve formě outsourcingu služby) umožňuje, ale pouze za definovaných podmínek.

Společnost Microsoft v roli poskytovatele cloudových služeb požádala NBÚ o výklad §7 Vyhlášky, ze kterého opět vyplývá, že v případě splněných konkrétních podmínek je používání cloudových služeb možné. Podrobněji viz kapitola 9.2.5.1.

V případě, kdy dodavatel cloudových služeb bude zpracovávat osobní údaje podle zákona č.101/2000 Sb., o ochraně osobních údajů, v aktuálním znění, vystupuje tento v roli zpracovatele osobních údajů a správce s ním musí uzavřít smlouvu o zpracování osobních údajů. Zároveň musí dodavatel cloudových služeb plnit požadavky zákona č.101/2000 Sb. nebo směrnice 95/46/ES pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích.

8.5.3 VZOR IMPLEMENTACE

Zákon a Vyhláška využití dodavatelů (a to i ve formě outsourcingu služby) umožňuje, ale pouze za definovaných podmínek.

V případě **VIS** tyto podmínky zahrnují

(1) stanovení požadavků na bezpečnostní opatření resp. stanovení samotných bezpečnostních opatření na dodavatele a

(2) uzavření smlouvy definující rozsah zapojení dodavatele a obsahující ustanovení o bezpečnosti informací vycházející ze stanovených požadavků.

V případě správců **KII** tyto podmínky zahrnují

(1) stanovení požadavků na bezpečnostní opatření resp. samotných bezpečnostních opatření na dodavatele,

(2) provedení hodnocení rizik specifických pro konkrétní dodávku, a to včetně kontroly souladu metodik a postupů hodnocení rizik a zvládání rizik s požadavky Vyhlášky na straně dodavatele cloudových služeb,

(3) uzavření smlouvy

- definující rozsah zapojení dodavatele,
- obsahující ustanovení o bezpečnosti informací vycházející ze stanovených požadavků,
- stanovující způsoby a úrovně realizace bezpečnostních opatření a
- určující vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,

(4) opakované provádění pravidelného hodnocení rizik, a to včetně kontroly souladu metodik a postupů hodnocení rizik a zvládání rizik s požadavky Vyhlášky na straně dodavatele cloudových služeb,

(5) provádění pravidelné kontroly zavedených bezpečnostních opatření u poskytovaných služeb,

(6) odstraňování zjištěných nedostatků v zavedených bezpečnostních opatřeních.

Kontrolu souladu metodik a postupů hodnocení rizik a zvládání rizik s požadavky Vyhlášky na straně dodavatele cloudových služeb (body 2 a 4) je možné doložit vyjádřením nezávislého auditora a prováděním pravidelné kontroly zavedených bezpečnostních opatření u poskytovaných služeb a odstraňováním zjištěných nedostatků v zavedených bezpečnostních opatřeních (body 5 a 6) a doložit certifikací podle ISO/IEC 27001 spolu s bezpečnostní politikou dodavatele ve struktuře ISO/IEC 27001, prohlášením o aplikovatelnosti a auditní zprávou z certifikace služby podle ISO/IEC 27001.

8.5.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V případě služeb Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) je smlouva zastoupena všeobecnými podmínkami (viz. kapitola 9.2.2.1) a smlouvou o úrovni služeb (viz. kapitola 9.2.2.2), jejíž přílohou je standardní smluvní doložka ve smyslu čl. 26 odst. 2 směrnice 95/46/ES pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích.

Soulad metodik a postupů hodnocení rizik a zvládání rizik s požadavky Vyhlášky na straně Microsoft Online Services je možné doložit vyjádřením nezávislého auditora (viz kapitola 9.2.5.2).

Provádění kontrol bezpečnostních opatření zavedených na straně Microsoft Online Services je možné doložit certifikací podle ISO/IEC 27001 spolu s následujícími podklady:

- Bezpečnostní politika „Microsoft Security Policy (External)“
- Prohlášení o aplikovatelnosti pro jednotlivé služby
- Zprávy z auditu podle normy ISO/IEC 27001 pro jednotlivé služby

8.6 ŘÍZENÍ AKTIV

Požadavky na řízení aktiv jsou specifikovány v §8 a příloze č. 1 Vyhlášky.

8.6.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění těchto požadavků je po správci IS určeného jako **VIS** požadováno:

- identifikovat a evidovat aktiva, tedy
  - identifikovat a evidovat primární aktiva (informace nebo služby),
  - určit garanty aktiv, kteří jsou odpovědní za primární aktiva,
  - hodnotit důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a v rozsahu podle přílohy č. 1 k Vyhlášce,

- stanovit pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv, tedy
  - určit způsoby rozlišování jednotlivých úrovní aktiv,
  - stanovit pravidla pro manipulaci s aktivy a evidenci aktiv podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,
  - stanovit přípustné způsoby používání aktiv,
  - zavést pravidla ochrany odpovídající úrovni aktiv a
  - určit způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.

Správce IS určeného jako **KII** má shodné povinnosti, má však navíc povinnost identifikovat a evidovat jak primární, tak i podpůrná aktiva, a musí

- určit vazby mezi primárními a podpůrnými aktivy a
- hodnotit důsledky závislostí mezi primárními a podpůrnými aktivy.

8.6.2 ANALÝZA POŽADAVKŮ

Pravidla a postupy identifikace a evidence aktiv jsou v principu nezávislé na zvoleném nebo daném modelu informačního systému.

Oproti tomu nastavení pravidel ochrany aktiv musí zohledňovat model informačního systému s tím, že vlastní úroveň zohlednění je daná mírou podrobnosti (detailem) politiky. Metody ochrany dat v prostředí cloudových služeb se zcela jistě budou alespoň částečně lišit od metod ochrany typických pro vlastními silami provozované služby na vlastněném hardware.

Proto je nutné před uzavřením smlouvy s dodavatelem (viz kapitola 8.5) zkontrolovat, že opatření nasazená u dodavatele (poskytovatele cloudových služeb) nebo v rámci služeb samotných splňují (správcem) určená pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv.

8.6.3 VZOR IMPLEMENTACE

Implementace řízení aktiv se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** a **KII** minimálně:

- stanovit pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv (zavést klasifikaci aktiv při zohlednění přílohy č.1 Vyhlášky a definovat opatření pro zajištění ochrany dané kategorie aktiv),
- definovat pravidla pro identifikaci a evidenci aktiv (správce VIS pouze pro primární aktiva, správce KII i pro podpůrná aktiva),
- provést evidenci a identifikaci aktiv a seznam aktiv následně udržovat a
- zavést stanovená pravidla ochrany.

8.6.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Požadavky na ochranu dat specifikované v příloze č. 1 Vyhlášky je v prostředí služeb Microsoft Online Services možné pokrýt s využitím jednoho nebo více nabízených nástrojů. Kromě toho platí, že v prostředí Microsoft Online Services jsou technické nosiče vyřazovány řízeným způsobem v souladu se standardem NIST SP 800-88.

Bližší informace jsou uvedeny v samostatné kapitole 11.

8.7 BEZPEČNOST LIDSKÝCH ZDROJŮ

Požadavky na bezpečnost lidských zdrojů jsou specifikovány v §9 Vyhlášky.

8.7.1 IDENTIFIKACE POŽADAVKŮ

V rámci řízení bezpečnosti lidských zdrojů je po správci IS určeného jako **VIS** požadováno

- stanovit plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny,
- v souladu s plánem rozvoje bezpečnostního povědomí zajistit poučení definovaných osob formou vstupních a pravidelných školení,
- vést o školeních přehledy obsahují předmět školení a seznam osob, které školení absolvovaly,
- zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a
- zajistit vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc

- stanovit pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů,
- hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí,
- určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel a
- zajistit změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

8.7.2 ANALÝZA POŽADAVKŮ

Základní principy a postupy bezpečnosti lidských zdrojů jsou nezávislé na zvoleném nebo daném modelu informačního systému, s tím, že až konkrétní pravidla a výstupy (jako například plány rozvoje) by měly zohledňovat model informačního systému.

Zde je nutné počítat s tím, že správcem vypracovaný plán rozvoje bezpečnostního povědomí je možné použít pro jeho uživatele, administrátory, osoby zastávající bezpečnostní role a v omezené míře i pro dodavatele služeb (například služeb správy správcem provozovaných technologií). Naopak však tento plán rozvoje nebude možné použít pro pracovníky dodavatele - poskytovatele cloudových služeb, který danou oblast řeší vlastními opatřeními.

Proto bude potřebné zkontrolovat, že opatření nasazená u dodavatele (poskytovatele cloudových služeb) jsou dostatečná (například v rámci kontroly plnění požadavků ze strany dodavatelů popsaného v kapitole 8.5).

8.7.3 VZOR IMPLEMENTACE

Implementace procesů bezpečnosti lidských zdrojů se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně

- stanovit plán rozvoje bezpečnostního povědomí,
- v souladu s plánem provádět školení a o těchto vést záznamy,
- zavést kontroly dodržování bezpečnostní politiky a
- zavést pravidla resp. procesy pro zajištění vrácení svěřených aktiv a odebrání přístupových oprávnění a tyto dodržovat resp. provádět.

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně

- stanovit plán rozvoje bezpečnostního povědomí,
- v souladu s plánem provádět školení a o těchto vést záznamy,
- stanovit pravidla pro určení osob do konkrétních rolí,
- zavést kontroly dodržování bezpečnostní politiky,
- zavést hodnocení účinnost plánu rozvoje bezpečnostního povědomí,
- určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel,
- zavést pravidla resp. procesy pro zajištění vrácení svěřených aktiv a odebrání přístupových oprávnění a tyto dodržovat resp. provádět a
- zavést pravidla resp. procesy pro zajištění změn přístupových oprávnění při změně postavení uživatele nebo jiné osoby.

8.7.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření v oblasti bezpečnosti lidských zdrojů zavedena a kontrolována, a to minimálně v oblastech

- kontroly spolehlivosti pracovníků[6],
- zvyšování bezpečnostního povědomí,
- disciplinárního řízení,
- zachování mlčenlivosti,
- vracení aktiv pracovníkem v případě ukončení pracovního vztahu.

Bližší podrobnosti je možné nalézt v dokumentech uvedených v kapitole 9.2.

[6] Společnost Microsoft provádí kontrolu spolehlivosti zaměstnanců a dodavatelů pracujících u zákazníků nebo majících možnost přístupu k osobním údajům zákazníků, a to minimálně na základě informací o zaměstnancově nebo dodavatelově minulosti, přičemž u vybraných rolí je prováděna důkladnější kontrola spolehlivost zahrnující mj. i bezpečnostní prověrku. Při kontrole spolehlivosti je zejména prověřována kriminální historie nebo kontrola správnosti a úplnosti předložených dokladů nebo sdělených informací. Do ukončení kontroly spolehlivosti není zaměstnanci nebo dodavateli povolen přístup.
Více viz dokument uvedený v kapitole 9.2.2.4, opatření z cíle A.7.1.

8.8 ŘÍZENÍ PROVOZU A KOMUNIKACÍ

Požadavky na řízení provozu a komunikací jsou specifikovány v §10 Vyhlášky.

8.8.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** požadováno:

- pomocí nástrojů uvedených v §21 až 23 Vyhlášky detekovat kybernetické bezpečnostní události, pravidelně vyhodnocovat získané informace a na zjištěné nedostatky reagovat v souladu s §13,
- zajišťovat bezpečný provoz IS včetně stanovení provozních pravidel a postupů,
- provádět pravidelné zálohování a prověřování použitelnosti provedených záloh.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc:

- má jasně stanovený minimální obsah provozních pravidel a postupů,
- musí zajistit oddělení vývojového, testovacího a produkčního prostředí,
- musí řešit reaktivní opatření vydaná NBÚ tím, že
  - posoudí očekávané dopady reaktivního opatření na IS a na zavedená bezpečnostní opatření, vyhodnotí možné negativní účinky a bez zbytečného odkladu je oznámí NBÚ a
  - stanoví způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určí časový plán jeho provedení,
- musí zajistit bezpečnost a integritu komunikačních sítí a bezpečnost komunikačních služeb podle §17 Vyhlášky,
- musí určit pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi,
- musí provádět výměnu a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla dokumentovat a
- s ohledem na klasifikaci aktiv musí provádět výměnu a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.

8.8.2 ANALÝZA POŽADAVKŮ

Bezpečnost řízení provozu a komunikací musí zohledňovat model informačního systému s tím, že vlastní úroveň zohlednění je daná mírou podrobnosti (detailem) politiky.

V každém případě jsou jednotlivá provozní pravidla a postupy, zálohování, způsob zajištění řešení reaktivních opatření, způsob zajištění bezpečnosti a integrity komunikačních sítí a bezpečnosti komunikačních služeb úzce spojeny s prostředím, jehož specifika musí být zohledněna.

Pokrytí požadavků bude muset být v převážné míře zajištěno na straně správce (jeho postupy resp. pravidly určenými pro jeho pracovníky nebo vybrané dodavatele služeb), avšak v případě využití outsourcovaných (cloudových) služeb budou některé požadavky muset být pokryty i na straně poskytovatele těchto služeb (který danou oblast řeší vlastními opatřeními).

Proto bude potřebné zkontrolovat, že opatření nasazená u dodavatele (poskytovatele cloudových služeb) jsou dostatečná (například v rámci kontroly plnění požadavků ze strany dodavatelů popsaného v kapitole 8.5).

8.8.3 VZOR IMPLEMENTACE

Implementace řízení provozu a komunikací se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně

- zavést procesy pro detekci kybernetických bezpečnostních událostí (s využitím nástrojů popsaných v kapitolách 10.6 až 10.8), pravidelně vyhodnocovat získané informace a na zjištěné nedostatky reagovat v souladu s postupy zvládání kybernetických bezpečnostních událostí a incidentů (viz kapitola 8.11),
- stanovit provozní pravidla a postupy,
- zajišťovat bezpečný provoz IS podle těchto postupů,
- provádět pravidelné zálohování a prověřovat použitelnost provedených záloh.

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně

- zavést procesy pro detekci kybernetických bezpečnostních událostí (s využitím nástrojů popsaných v kapitolách 10.6 až 10.8), pravidelně vyhodnocovat získané informace a na zjištěné nedostatky reagovat v souladu s postupy zvládání kybernetických bezpečnostních událostí a incidentů (viz kapitola 8.11),
- stanovit provozní pravidla a postupy v definovaném rozsahu,
- zajišťovat bezpečný provoz IS podle těchto postupů,
- provádět pravidelné zálohování a prověřovat použitelnost provedených záloh,
- zajistit oddělení vývojového, testovacího a produkčního prostředí,
- zavést postupy pro řešení reaktivních opatření vydaných NBÚ obsahující posouzení očekávaných dopadů včetně vyhodnocení negativních účinků a stanovení způsobu rychlého provedení reaktivního opatření,
- zavést pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi,
- zavést pravidla pro provádění výměny a předávání informací.

8.8.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření v oblasti řízení provozu a komunikací zavedena a kontrolována, a to minimálně v oblastech

- provozní pravidla a postupy,
- zálohování a obnovy,
- škodlivého software,
- definované základní konfigurace bezpečnostní funkcionality,
- řízení změn,
- instalace software,
- záznamů událostí,
- řízení kapacity a výkonu,

- řízení zranitelností,
- přístupu k dokumentaci a
- ochrany koncových bodů.

Bližší podrobnosti je možné nalézt v dokumentech uvedených v kapitole 9.2.

8.9 ŘÍZENÍ PŘÍSTUPU A BEZPEČNÉ CHOVÁNÍ UŽIVATELŮ

Požadavky na řízení přístupu a bezpečné chování uživatelů jsou specifikovány v §11 Vyhlášky.

8.9.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** požadováno:

- řídit přístup k IS a přidělit každému uživateli jednoznačný identifikátor,
- přijmout opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů IS podle §18 a 19 Vyhlášky, a která brání ve zneužití těchto údajů neoprávněnou osobou.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc:

- přidělit přistupujícím aplikacím samostatný identifikátor,
- omezit přidělování administrátorských oprávnění,
- přidělovat a odebírat přístupová oprávnění v souladu s politikou řízení přístupu,
- provádět pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích,
- využívat nástroj pro ověřování identity uživatelů podle §18 a nástroj pro řízení přístupových oprávnění podle §19 Vyhlášky a
- zavést bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými správce nedisponuje.

8.9.2 ANALÝZA POŽADAVKŮ

Základní principy a postupy řízení přístupu a bezpečného chování uživatelů jsou nezávislé na zvoleném nebo daném modelu informačního systému, s tím, že až konkrétní pravidla a postupy by měly zohledňovat model informačního systému.

Pokrytí požadavků bude muset být v převážné míře zajištěno na straně správce (jeho postupy resp. pravidly určenými pro jeho pracovníky nebo vybrané dodavatele služeb), avšak v případě využití outsourcovaných (cloudových) služeb budou některé požadavky muset být pokryty i na straně poskytovatele outsourcovaných (cloudových) služeb (který danou oblast řeší vlastními opatřeními).

Proto bude potřebné zkontrolovat, že opatření nasazená u dodavatele (poskytovatele cloudových služeb) jsou dostatečná (například v rámci kontroly plnění požadavků ze strany dodavatelů popsaného v kapitole 8.5).

8.9.3 VZOR IMPLEMENTACE

Implementace řízení přístupu a bezpečného chování uživatelů se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně

- zavést procesy správy uživatelů, administrátorů a případně dalších osob, které zajistí přidělení jednoznačného identifikátoru každému subjektu,
- zavést opatření, která slouží k zajištění ochrany autentizačních údajů (například hesel nebo klíčů).

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně

- definovat pravidla (politiku) řízení přístupu,
- zavést procesy správy uživatelů, administrátorů, dalších osob a aplikací, které zajistí přidělení jednoznačného identifikátoru každému subjektu – procesy správy identifikátorů,
- přidělovat a odebírat přístupová oprávnění v souladu s politikou řízení přístupu – procesy správy oprávnění,
- zavést opatření, která slouží k zajištění ochrany autentizačních údajů (například hesel nebo klíčů),
- zavést pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích,
- zavést bezpečnostní opatření specifická pro přístup z mobilních zařízení nebo zařízení provozovaných nebo spravovaných jiným subjektem.

8.9.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření v oblasti řízení přístupu a bezpečného chování uživatelů zavedena a kontrolována, a to minimálně v oblastech

- politiky řízení přístupu,
- schválení a kontroly přístupu (interní proces LockBox),
- minimálního oprávnění,
- externích přístupů,
- autentizace,
- standardních uživatelských účtů,
- používaní privilegovaných programů,
- odebírání přístupu.

Bližší podrobnosti je možné nalézt v dokumentech uvedených v kapitole 9.2.

8.10 AKVIZICE, VÝVOJ A ÚDRŽBA

Požadavky na akvizici, vývoj a údržbu jsou specifikovány v §12 Vyhlášky.

8.10.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** požadováno:

- stanovit bezpečnostní požadavky na změnu IS spojené s jejich akvizicí, vývojem a údržbou a zahrnout tyto bezpečnostní požadavky do projektu akvizice, vývoje a údržby systému.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc:

- identifikovat, hodnotit a řídit rizika související s akvizicí, vývojem a údržbou IS. Pro postupy hodnocení a řízení rizik musí v maximální možné míře využít metodiky podle §4 odst. 1 písm. a) Vyhlášky,
- zajistit bezpečnost vývojového prostředí a zajistit ochranu používaných testovacích dat a
- provádět bezpečnostní testování změn IS před jejich zavedením do provozu.

8.10.2 ANALÝZA POŽADAVKŮ

Základní principy a postupy akvizice, vývoje a údržby jsou nezávislé na zvoleném nebo daném modelu informačního systému, s tím, že až jejich použití v konkrétním případě musí zohledňovat model informačního systému.

Pokrytí požadavků bude muset být v převážné míře zajištěno na straně správce (jeho postupy resp. pravidly určenými pro jeho pracovníky nebo vybrané dodavatele služeb), avšak v případě využití cloudových služeb budou některé požadavky muset být pokryty i na straně poskytovatele cloudových služeb (který danou oblast řeší vlastními opatřeními).

Proto bude potřebné zkontrolovat, že opatření nasazená u dodavatele (poskytovatele cloudových služeb) jsou dostatečná (například v rámci kontroly plnění požadavků ze strany dodavatelů popsaného v kapitole 8.5).

8.10.3 VZOR IMPLEMENTACE

Implementace opatření v oblasti akvizice, vývoje a údržby se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně:

- stanovit bezpečnostní požadavky na změnu IS spojené s jejich akvizicí, vývojem a údržbou a
- zahrnout tyto požadavky do projektu akvizice, vývoje a údržby systému.

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně:

- stanovit bezpečnostní požadavky na změnu IS spojené s jejich akvizicí, vývojem a údržbou,
- do projektu akvizice, vývoje a údržby systému zahrnout
  - zajištění splnění stanovených bezpečnostní požadavků a
  - provedení identifikace, hodnocení a řízení rizik souvisejících s akvizicí, vývojem a údržbou IS při maximálním využití metodiky popsané v kapitole 8.2,

- zajistit bezpečnost vývojového prostředí,
- zajistit ochranu používaných testovacích dat a
- provádět bezpečnostního testování změn IS před jejich zavedením do provozu.

8.10.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření v oblasti akvizice, vývoje a údržby zavedena a kontrolována, a to minimálně v oblastech

- definování a sledování plnění požadavků na bezpečnost,
- použití strategie ochrany do hloubky,
- bezpečného vývoje software,
- kontroly integrity dat a
- kontroly bezpečnostních funkcí.

Bližší podrobnosti je možné nalézt v dokumentech uvedených v kapitole 9.2.

8.11 ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

Požadavky na zvládání kybernetických bezpečnostních událostí a incidentů jsou specifikovány v §13, 30 – 32 Vyhlášky.

8.11.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** nebo **KII** požadováno:

- přijmout nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u IS ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. O oznámeních vést záznamy,
- připravit prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle §21 až 23 Vyhlášky, provádět jejich vyhodnocení a identifikovat kybernetické bezpečnostní incidenty,
- provádět klasifikaci kybernetických bezpečnostních incidentů, přijímat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, provádět hlášení kybernetického bezpečnostního incidentu podle §32 Vyhlášky a zajišťovat sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,
- prošetřovat a určovat příčiny kybernetického bezpečnostního incidentu, vyhodnocovat účinnosti řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanovovat nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu a
- dokumentovat zvládání kybernetických bezpečnostních incidentů.

8.11.2 ANALÝZA POŽADAVKŮ

Postupy a pravidla zvládání kybernetických bezpečnostních událostí a incidentů jsou v principu nezávislé na zvoleném nebo daném modelu informačního systému s tím, že pouze okrajově potřebují zohledňovat model informačního systému.

Pokrytí požadavků bude muset být zajištěno na straně správce (jeho postupy resp. pravidly určenými pro jeho pracovníky nebo vybrané dodavatele služeb) s tím, že dodavatel – poskytovatel cloudových služeb (který danou oblast řeší vlastními opatřeními) by měl správci předávat informace o událostech nebo incidentech v oblastech s vlivem na IS správce, ale zároveň i mimo dosah správce.

Proto bude potřebné zkontrolovat, že opatření nasazená u dodavatele (poskytovatele cloudových služeb) jsou dostatečná (například v rámci kontroly plnění požadavků ze strany dodavatelů popsaného v kapitole 8.5).

8.11.3 VZOR IMPLEMENTACE

Implementace bezpečnostních opatření v oblasti zvládání kybernetických bezpečnostních událostí a incidentů se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** a **KII** minimálně zavést pravidla a procesy zvládání bezpečnostních událostí a incidentů, které zajistí

- oznamování kybernetických bezpečnostních událostí u IS ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a vedení záznamů o oznámeních,
- detekci bezpečnostní události pomocí nástrojů popsaných v kapitolách 10.6 až 10.8,
- vyhodnocování události a identifikaci kybernetické bezpečnostní incidentů a provádění klasifikace kybernetických bezpečnostních incidentů podle §30 – 32 Vyhlášky.
- přijímání opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- provádění hlášení kybernetického bezpečnostního incidentu NBÚ,
- zajištění sběru věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,
- prošetření a určení příčiny kybernetického bezpečnostního incidentu,
- vyhodnocení účinnosti řešení kybernetického bezpečnostního incidentu,
- stanovení nutných bezpečnostních opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu a
- dokumentaci zvládání kybernetických bezpečnostních incidentů.

8.11.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření v oblasti zvládání kybernetických bezpečnostních událostí a incidentů zavedena a kontrolována s tím, že se společnost Microsoft zavazuje zákazníkovi ohlásit vznik bezpečnostního incidentu, spočívajícího v nezákonném přístupu k datům zákazníka, jehož výsledkem je ztráta, zveřejnění nebo změna zákaznických dat.

Bližší podrobnosti je možné nalézt v dokumentech uvedených v kapitolách 9.2 a 10.8.4.

8.12 ŘÍZENÍ KONTINUITY ČINNOSTÍ

Požadavky na řízení kontinuity činností jsou specifikovány v §14 Vyhlášky.

8.12.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** požadováno:

- stanovit práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role v rámci řízení kontinuity činností,
- stanovit cíle řízení kontinuity činností formou určení
  - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,
  - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb IS, a
  - dobu obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu, a
- stanovit strategii řízení kontinuity činností, která obsahuje naplnění výše stanovených cílů.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc:

- vyhodnotit a dokumentovat možné dopady kybernetických bezpečnostních incidentů a posoudit možná rizika související s ohrožením kontinuity činností,
- stanovit, aktualizovat a pravidelně testovat plány kontinuity činností IS,
- realizovat opatření pro zvýšení odolnosti IS vůči kybernetickému bezpečnostnímu incidentu a využívá nástroj pro zajišťování úrovně dostupnosti podle §26 a
- stanovit a aktualizovat postupy pro provedení opatření vydaných NBÚ podle §13 a 14 Zákona, ve kterých zohlední
  - výsledky hodnocení rizik provedení opatření,
  - stav dotčených bezpečnostních opatření a
  - vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.

8.12.2 ANALÝZA POŽADAVKŮ

Základní principy a postupy řízení kontinuity činností jsou nezávislé na zvoleném nebo daném modelu informačního systému, s tím, že až konkrétní pravidla a výstupy (jako například strategie řízení kontinuity činností nebo plány kontinuity činností) potřebují zohledňovat model informačního systému.

Pokrytí požadavků bude muset být zajištěno výhradně na straně správce (jeho postupy resp. pravidly určenými pro jeho pracovníky nebo vybrané dodavatele služeb) s tím, že u služeb zajišťovaných poskytovatelem cloudových služeb musí správce zohlednit poskytovanou a garantovanou úroveň služeb (stanovenou v SLA) u jím zvolených služeb.

8.12.3 VZOR IMPLEMENTACE

Implementace řízení kontinuity činností se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně:

- stanovit práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role v rámci řízení kontinuity činností,
- stanovit cíle řízení kontinuity činností formou určení minimální úrovně poskytovaných služeb, RTO a RPO,
- stanovit strategii řízení kontinuity činností, která obsahuje naplnění výše stanovených cílů a
- zajistit podmínky pro případnou realizaci strategie.

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně:

- stanovit práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role v rámci řízení kontinuity činností,
- stanovit cíle řízení kontinuity činností formou určení minimální úrovně poskytovaných služeb, RTO a RPO,
- provést analýzu dopadu (business impact analysis),
- stanovit strategii řízení kontinuity činností, která obsahuje naplnění výše stanovených cílů,
- rozpracovat strategii do plánů kontinuity činností IS (zahrnujících i havarijní plány),
- zajistit podmínky pro realizaci plánů kontinuity činností IS,
- realizovat opatření pro zvýšení odolnosti IS vůči kybernetickému bezpečnostnímu incidentu s využitím nástrojů popsaných v kapitole 10.11,
- stanovit a aktualizovat postupy pro provedení opatření (viz kapitola 8.8).

8.12.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření v oblasti řízení kontinuity činností zavedena a kontrolována tak, aby zajistila úroveň služeb definovanou v dokumentu „Smlouva o úrovni služeb pro Služby online společnosti Microsoft“ (viz kapitola 9.2.2.2) – typicky 99,9% nebo 99,95%.

Bližší podrobnosti o nasazených opatřeních je možné nalézt v dokumentech uvedených v kapitole 9.2.

8.13 KONTROLA A AUDIT KRITICKÉ INFORMAČNÍ INFRASTRUKTURY A VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMŮ

Požadavky na kontrolu a audit kritické informační infrastruktury a významných informačních systémů jsou specifikovány v §15 Vyhlášky.

8.13.1 IDENTIFIKACE POŽADAVKŮ

V rámci plnění požadavků je po správci IS určeného jako **VIS** požadováno:

- posuzovat soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k IS a určit opatření pro jeho prosazování a
- provádět a dokumentovat pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol zohledňovat v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

Pro naplnění identifikovaných požadavků musí správce **KII** splnit požadavky kladené na správce VIS a navíc:

- zajišťovat provedení posouzení souladu nebo provedení kontroly osobou s odbornou kvalifikací podle §6 odst. 6 Vyhlášky, která hodnotí správnost a účinnost zavedených bezpečnostních opatření a
- provádět kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reagovat na zjištěné zranitelnosti.

8.13.2 ANALÝZA POŽADAVKŮ

Postupy a pravidla kontroly a auditu IS jsou sice v principu nezávislé na zvoleném nebo daném modelu informačního systému, ale dílčí postupy posouzení souladu nebo kontroly (auditu) už musí model informačního systému zohlednit, a to zejména z pohledu schopnosti správce provést kontrolu dané komponenty nebo služby.

Pokrytí požadavků bude muset být v převážné míře zajištěno na straně správce (jeho postupy resp. pravidly určenými pro jeho pracovníky nebo vybrané dodavatele služeb), avšak v případě využití cloudových služeb nebude pravděpodobně správce schopen zajistit audit prostředí poskytovatele cloudových služeb a bude se muset spolehnout na výsledky auditů provedených u poskytovatele cloudových služeb nezávislou třetí stranou.

Proto bude v rámci provádění kontroly a auditu nutné zkontrolovat, že audit třetí strany proběhl v daném termínu a zkontrolovat jeho výsledky (nálezy).

8.13.3 VZOR IMPLEMENTACE

Implementace kontroly a audit se skládá zejména z návrhu pravidel a postupů, jejich ukotvení ve formě dokumentace a následně nasazení formou přidělení odpovědnosti, dodržováním pravidel a prováděním předepsaných postupů.

Pro naplnění identifikovaných požadavků musí správce **VIS** minimálně:

- zavést kontrolu souladu bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky (např. v rámci hodnocení rizik),
- zajistit provádění posouzení souladu bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky,

- vytvořit plány kontrol dodržování bezpečnostní politiky,
- provádět tyto kontroly a
- výsledky kontrol zohlednit v plánu rozvoje bezpečnostního povědomí a v plánu zvládání rizik.

Pro naplnění identifikovaných požadavků musí správce **KII** minimálně:

- zavést kontrolu souladu bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky (např. v rámci hodnocení rizik),
- zajistit provádění posouzení souladu bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky osobami s odbornou kvalifikací,
- vytvořit plány kontrol dodržování bezpečnostní politiky,
- provádět tyto kontroly osobami s odbornou kvalifikací,
- výsledky kontrol zohlednit v plánu rozvoje bezpečnostního povědomí a v plánu zvládání rizik a
- provádět testy zranitelností a na zjištěné zranitelnosti reagovat (např. odstraňovat).

8.13.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V prostředí Microsoft Online Services (konkrétně Office 365 a Microsoft Azure) jsou bezpečnostní opatření kontrolována a auditována.

Provádění jednotlivých kontrola auditů a auditů včetně jejich zaměření a případných nálezů společnost Microsoft dokládá zprávami z auditu, které jsou jejím zákazníkům k dispozici. Vybrané zprávy z auditu jsou uvedeny v kapitole 9.2.

9 BEZPEČNOSTNÍ DOKUMENTACE

V rámci analyzovaného modelu informačního systému je možné bezpečnostní dokumentaci rozdělit do dvou samostatných částí, a to na interní bezpečnostní dokumentaci správce tvořící základ a bezpečnostní dokumentaci poskytovatele externích služeb (Microsoft Online Services), na kterou se interní bezpečnostní dokumentace odkazuje (nebo z ní vychází).

9.1 BEZPEČNOSTNÍ DOKUMENTACE SPRÁVCE

9.1.1 IDENTIFIKACE POŽADAVKŮ

Vyhláška v §5 a příloze č. 4 po správci IS určeného jako VIS nebo KII požaduje vytvoření a zavedení bezpečnostní politiky v oblastech určených následující tabulkou:

Tab. 2 Bezpečnostní dokumentace správce

Oblast	VIS	KII
Systém řízení bezpečnosti informací	ANO	ANO
Organizační bezpečnost	ANO	ANO
Řízení vztahů s dodavateli (řízení dodavatelů)	ANO	ANO
Klasifikace aktiv	ANO	ANO
Bezpečnost lidských zdrojů	ANO	ANO
Řízení provozu a komunikací	ANO	ANO
Řízení přístupu	ANO	ANO
Bezpečné chování uživatel	ANO	ANO
Zálohování a obnova	ANO	ANO
Bezpečné předávání a výměna informací		ANO
Řízení technických zranitelností		ANO
Bezpečné používání mobilních zařízení		ANO
Poskytování a nabývání licencí programového vybavení a informací	ANO	ANO
Dlouhodobé ukládání a archivace informací		ANO
Ochrana osobních údajů	ANO	ANO
Fyzická bezpečnost		ANO
Bezpečnost komunikační sít		ANO
Ochrana před škodlivým kódem	ANO	ANO
Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí	ANO	ANO

Oblast	VIS	KII
Využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí		ANO
Používání kryptografické ochrany	ANO	ANO

9.1.2 ANALÝZA POŽADAVKŮ

Z výše uvedené tabulky sice vyplývá, že rozsah politiky správce VIS by mohl být menší než rozsah politiky pro správce KII, ve skutečnosti se však dá předpokládat, že množina pokrývaných oblastí bude pro oba dva typy správců shodná a lišit se bude zejména rozsah a úroveň jednotlivých opatření.

Vlastní sktruktura politiky není Vyhláškou striktně předepsána. Vyhláška předepisuje pouze oblasti, které musí politika minimálně upravovat (viz tabulka) a dále doporučený, ale ne závazný, obsah bezpečnostní dokumentace.

Proto je zcela na správci, zdali se rozhodne použít doporučenou strukturu politiky uvedenou v příloze č. 4 Vyhlášky, struktury vycházející z normy ISO/IEC 27002 nebo jinou strukturu. Podobně je zcela na volbě správce v kolika dokumentech bude politika obsažena – může se jednat o jeden rozsáhlejší dokument nebo množství kratších dokumentů. Z praktického pohledu je však možné předpokládat, že politika systému řízení bude samostatným dokumentem vzhledem předpokládanému obsahu, úrovni podrobnosti a času vzniku. Dále lze, vzhledem k využití cloudových služeb Microsoft Online Services, předpokládat podrobné rozpracování oblasti „Řízení vztahů s dodavateli“, možná též ve formě samostatného dokumentu.

9.1.3 VZOR IMPLEMENTACE

Správce VIS nebo KII vytvoří bezpečnostní politiku v jím zvolené struktuře, a tuto přijme ve formě závazného předpisu.

9.2 BEZPEČNOSTNÍ DOKUMENTACE MICROSOFT ONLINE SERVICES

V této kapitole je uveden přehled dokumentace vztahující se k bezpečnosti služeb Microsoft Online Services.

Vzhledem k poměrně značnému množství bezpečnostní dokumentace poskytované společností Microsoft je zde uvedena pouze dokumentace vztahující se k systému řízení a konkrétním opatřením nasazeným na straně provozovatele služeb, společnosti Microsoft. Nejsou zde (až na výjimky) uváděny dokumenty obecného charakteru, které nepopisují konkrétní opatření nebo alespoň neobsahují závazek mít toto opatření implementované a provozované, seznamy volitelných opatření, jejichž nasazení záleží na volbě zákazníka, a konkrétní technické postupy.

Vzhledem k celosvětové působnosti společnosti Microsoft, a tedy i služeb Microsoft Online Services, jsou seznamy implementovaných opatření a následných auditů ověřujících jejich zvedení a celkovou efektivitu vytvořeny z pohledu různých norem a standardů, jako například:

- ISO/IEC 27001 (a ISO/IEC 27002),
- CSA (Cloud Security Alliance) Cloud Control Matrix,
- SSAE 16/ ISAE 3402 resp. AT 101, na základě kterých jsou vytvářeny auditní zprávy SOC (Service Organization Controls) 1 Type II a SOC 2 Type II a,
- PCI DSS.

Protože v prostředí České republiky je z pohledu Zákona nejvíce zajímavý pohled ISO/IEC 27001, jsou v seznamu zejména uvedeny a podrobněji popsány dokumenty se vztahem k této normě. Dokumenty spojené s ostatními standardy nebo normami jsou dále pouze zmíněné, neboť mohou díky svému specifickému zaměření doplnit celkový obraz zajištění bezpečnosti v prostředí Microsoft Online Services.

Bezpečnostní dokumentace Microsoft Online Services je rozdělena do pěti částí, a to

- dokumentace služeb Microsoft Cloud Infrastructure and Operations,
- dokumentace společnosti Microsoft nebo služeb Microsoft Online Services,
- dokumentace služeb Microsoft Office 365,
- dokumentace služeb Microsoft Azure Core a
- dokumentace specifická pro Českou republiku a zákon č. 181/2014 Sb.

Pokud existuje česká verze dokumentu, je uvedena tato verze, jinak je uvedena verze anglická.

Celkovým zdrojem níže uvedených informací pro zákazníky (veřejně k dispozici) je Microsoft Trust Center obsahující rozcestník pro všechny služby (http://www.microsoft.com/en-us/trustcenter). Vlastní dokumenty jsou uloženy na Microsoft Trust portálu https://trustportal.office.com, který je přístupný administrátorům organizace po vytvoření Microsoft Office 365 nebo Microsoft Azure subskripce. Tito administrátoři mohou delegovat přístup do Microsoft Trust portálu pro další uživatele.

Správce bude z dokumentace poskytované společností Microsoft čerpat a odkazovat na ni při posuzování opatření v částech informačního systému, který je ve správě společnosti Microsoft.

9.2.1 MICROSOFT CLOUD INFRASTRUCTURE AND OPERATIONS

Microsoft's Cloud Infrastructure and Operations (MCIO), dříve nazývané Global Foundation Service (GFS), poskytují infrastrukturu a síť pro cloudové služby firmy Microsoft včetně služeb Microsoft Online Services. V oblasti infrastruktury se proto bezpečnostní dokumentace služeb Microsoft Office 365 a Microsoft Azure Core odkazuje na bezpečnostní dokumentaci MCIO.

9.2.1.1 INFORMATION SECURITY MANAGEMENT SYSTEM FOR MCIO

Jedná se o dokument označený jako „Information Security Management System for Microsoft's Cloud Infrastructure - Online Services Security and Compliance“, autorem je společnost Microsoft.

Tento informativní dokument popisuje systém řízení bezpečnosti informací (ISMS) pro služby Microsoft Cloud Infrastructure and Operations. Kromě jiného popisuje

- soulad s vybranými normami a standardy (ISO/IEC 27001:2013, SSAE 16/ ISAE 3402, AT 101, SOX, PCI-DSS, FedRAMP),
- činnost fóra pro řízení bezpečnosti informací,
- program pro řízení rizik a
- program pro správu politik bezpečnosti.

Dále dokument obsahuje odkaz na webové stránky, kde je možné nalézt informace o certifikátech ISMS vydaných společností BSI pro Microsoft Cloud Infrastructure and Operations.

9.2.1.2 MCIO STATEMENT OF APPLICABILITY

Jedná se o dokument označený jako „Microsoft Cloud Infrastructure and Operations – ISO/IEC 27001:2013 ISMS Statement of Applicability“, autorem je společnost Microsoft.

Dokument obsahuje prohlášení o aplikovatelnosti podle ISO/IEC 27001:2013, tedy uvádí která opatření podle ISO/IEC 27002:2013 byla vybrána k implementaci včetně důvodu.

9.2.1.3 CERTIFIKAČNÍ ZPRÁVA Z AUDITU ISMS

Jedná se o dokument označený jako „Assessment Report“, autorem je společnost BSI.

Dokument obsahuje zprávu z auditu systému řízení bezpečnosti informací pro službu MCIO a na základní úrovni popisuje, co bylo hodnoceno a nakolik společnost Microsoft pro službu MCIO plní požadavky normy ISO/IEC 27001:2013.

9.2.1.4 DALŠÍ DOKUMENTY

Informace o bezpečnostních opatření zavedených v prostředí MCIO je možné najít i v následujících dokumentech:

- MCIO SSAE16 SOC 1 Type II Report obsahující SOC 1 auditní zprávu (Service Organization Controls Report) typu II podle standardu SSAE 16/ISAE 3402, která se zaměřuje na bezpečnostní opatření se vztahem k finančnímu výkaznictví.
- MCIO AT 101 SOC 2 Type II Report obsahující SOC 2 auditní zprávu (Trust Services Principles) typu II podle standardu AT 101, která se zaměřuje na bezpečnostní opatření s cílem zajistit důvěrnost, integritu, dostupnost a soukromí.

9.2.2 MICROSOFT ONLINE SERVICES

9.2.2.1 PODMÍNKY SLUŽEB ONLINE PRO MULTILICENČNÍ PROGRAMY SPOLEČNOSTI MICROSOFT

Jedná se o dokument označený „Volume Licensing: Podmínky pro služby online“, autorem je společnost Microsoft.

Dokument obsahuje všeobecné obchodní podmínky pro služby Microsoft Dynamics CRM Online Services, Microsoft Office 365, Microsoft Azure Core a Microsoft Intune. Dokument mj. obsahuje

- podmínky ochrany osobních údajů (včetně standardních smluvních doložek definovaných Evropskou komisí v rozhodnutí 2010/87/EU[7])
  - závazek užití dat pouze pro poskytování služeb,
  - závazek neposkytnutí dat třetím stranám kromě vyjmenovaných situací a procesů,
  - závazek oznámení incidentu,
  - vymezení místa zpracování dat,
  - pravidla použití dodavatelů,
  - ochrana osobních údajů – vrácení / smazání dat, pracovníci, subdodavatelé;

[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf

- základní popis opatření, kterými společnost Microsoft zajišťuje ochranu dat zákazníků v oblastech
  - organizace zabezpečení informací,
  - správa prostředků,
  - zabezpečení lidských zdrojů,
  - fyzické zabezpečení a bezpečnost životního prostředí,
  - sdělení a správa operací,
  - řízení přístupu,
  - správa incidentů zabezpečení informací a
  - správa kontinuity podnikání;
- závazek společnosti provádět audity (např. podle ISO/IEC 27001, SSAE 16/ ISAE 3402, AT 101), a to pro každou službu minimálně jednou ročně, a výsledky zpráv poskytnout definovaným způsobem zákazníkovi (na základě dohody o mlčenlivosti).

9.2.2.2 SMLOUVA O POSKYTOVÁNÍ SLUŽEB PRO SLUŽBY ONLINE PRO MULTILICENČNÍ PROGRAMY SPOLEČNOSTI MICROSOFT

Jedná se o dokument označený „Volume Licensing: Smlouva o úrovni služeb pro Služby online společnosti Microsoft“, autorem je společnost Microsoft.

Dokument definuje úroveň služeb (SLA) z pohledu dostupnosti jednotlivých služeb pro služby Microsoft Dynamics, Microsoft Office 365, Microsoft Enterprise Mobility Services, Microsoft Azure Core a ostatní online služby.

9.2.2.3 MICROSOFT SECURITY POLICY

Jedná se o dokument označený jako „Microsoft Security Policy (External)“, autorem je společnost Microsoft.

Uvedená politika se uplatňuje na všechny informace a procesy společnosti Microsoft a je závazná pro zaměstnance, stážisty, dočasné pracovníky, výrobce, partnery a registrované návštěvy společnosti.

Politika definuje

- základní cíle, což je zajištění důvěrnosti, integrity a dostupnost při současném zajištění souladu s externími požadavky (legislativními, průmyslovými, regulačními a smluvními),
- základní principy použité pro zajištění bezpečnosti a
- dílčí cíle v oblastech
  - bezpečnostní politika,
  - organizace bezpečnosti informací,
  - bezpečnost lidských zdrojů,
  - správa aktiv,
  - řízení přístupu,
  - kryptografie,
  - fyzická bezpečnost a bezpečnost prostředí,
  - bezpečnost provozu,
  - bezpečnost komunikací,

- nákupu, vývoje a údržby,
- vztahů s dodavateli,
- řízení incidentů,
- řízení zachování činnosti a
- souladu.

9.2.2.4 MICROSOFT ONLINE SERVICES CONTROLS AS ALIGNED TO ISO/IEC 27001:2013 WITH ISO/IEC 27018:2014

Jedná se o dokument označený jako „Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014“, autorem je společnost Microsoft.

Dokument obsahuje tabulku bezpečnostních opatření podle ISO/IEC 27001:2013, kde ke každému ze 114 opatření rozdělených do 14 skupin je uveden způsob jeho implementace v prostředí Microsoft Online Services. Dokument popisuje i opatření realizovaná na úrovni MCIO.

9.2.2.5 MICROSOFT PUBLIC CLOUD COMPLIANCE CERTIFICATION AND ATTESTATION

Jedná se o dokument označený jako „Microsoft Public Cloud Compliance Certification and Attestation“, autorem je společnost Microsoft.

Tento informativní dokument obsahuje přehled získaných nebo probíhajících certifikací (mezinárodních, průmyslových nebo specifických pro konkrétní stát nebo oblast) pro služby Microsoft Online Services.

9.2.3 MICROSOFT OFFICE 365

9.2.3.1 OFFICE 365 ARCHITECTURE AND AUDIT REPORTS

Jedná se o dokument označený jako „Office 365 Architecture and Audit Reports“, autorem je společnost Microsoft.

Tento informativní dokument popisuje způsob zabezpečení prostředí Office 365 včetně splněných norem resp. standardů a auditů, které dokládají splnění požadavků příslušné normy resp. standardu.

9.2.3.2 OFFICE 365 ISMS MANUAL

Jedná se o dokument označený jako „Office 365 Information Security managment System (ISMS) Manual“, autorem je společnost Microsoft.

Dokument podrobně popisuje systém řízení bezpečnosti informací pro službu Office 365 v rozsahu požadovaném ISO/IEC 27001:2013.

9.2.3.3 OFFICE 365 STATEMENT OF APPLICABILITY

Jedná se o dokument označený jako „Microsoft Office ISO 27001:2013 Statement of Applicability“, autorem je společnost Microsoft.

Dokument obsahuje prohlášení o aplikovatelnosti podle ISO/IEC 27001:2013, tedy uvádí která opatření podle ISO/IEC 27002:2013 byla vybrána k implementaci včetně důvodu.

9.2.3.4 CERTIFIKAČNÍ ZPRÁVA Z AUDITU ISMS

Jedná se o dokument označený jako „Assessment Report. Microsoft Office 365“, autorem je společnost BSI.

Dokument obsahuje zprávu z auditu systému řízení bezpečnosti informací pro službu Office 365 a na základní úrovni popisuje, co bylo hodnoceno a nakolik společnost Microsoft pro službu Microsoft Office 365 plní požadavky normy ISO/IEC 27001:2013.

9.2.3.5 DALŠÍ DOKUMENTY

Informace o bezpečnostních opatření zavedených v prostředí Microsoft Office 365 je možné najít i v následujících dokumentech:

- Office 365 SOC 1 SSAE 16 Type II Report obsahující SOC 1 auditní zprávu (Service Organization Controls Report) typu II podle standardu SSAE 16/ISAE 3402, která se zaměřuje na bezpečnostní opatření se vztahem k finančnímu výkaznictví.
- Office 365 SOC 2 AT 101 Type II Report obsahující SOC 2 auditní zprávu (Trust Services Principles) typu II podle standardu AT 101, která se zaměřuje na bezpečnostní opatření s cílem zajistit důvěrnost, integritu, dostupnost a soukromí.
- Office 365 Mapping of CSA Cloud Control Matrix obsahující seznam bezpečnostních požadavků uvedených v CSA (Cloud Security Alliance) Cloud Control Matrix a způsob jejich pokrytí v prostředí Office 365.
- Office 365 Risk Management Lifecycle obsahující stručný popis způsobu řízení rizik v prostředí Office 365.
- Office 365 Security Incident Management obsahující stručný popis způsobu řízení incidentů v prostředí Office 365.

9.2.4 MICROSOFT AZURE

9.2.4.1 AZURE STATEMENT OF APPLICABILITY

Jedná se o dokument označený jako „Microsoft Azure 27001:2013 Statement of Applicability“, autorem je společnost Microsoft.

Dokument obsahuje prohlášení o aplikovatelnosti podle ISO/IEC 27001:2013, tedy uvádí která opatření podle ISO/IEC 27002:2013 byla vybrána k implementaci včetně důvodu.

9.2.4.2 CERTIFIKAČNÍ ZPRÁVA Z AUDITU ISMS

Jedná se o dokument označený jako „Assessment Report - Microsoft Azure“, autorem je společnost BSI.

Dokument obsahuje zprávu z auditu systému řízení bezpečnosti informací pro službu Microsoft Azure Core a na základní úrovni popisuje, co bylo hodnoceno a nakolik společnost Microsoft pro službu Microsoft Azure Core plní požadavky normy ISO/IEC 27001:2013.

9.2.4.3 DALŠÍ DOKUMENTY

Informace o bezpečnostních opatření zavedených v prostředí Office 365 je možné najít i v následujících dokumentech:

- Azure SOC 1 SSAE Type II Report obsahující SOC 1 auditní zprávu (Service Organization Controls Report) typu II podle standardu SSAE 16/ISAE 3402, která se zaměřuje na bezpečnostní opatření se vztahem k finančnímu výkaznictví.
- Azure SOC 2 AT 101 Type II Report obsahující SOC 2 auditní zprávu (Trust Services Principles) typu II podle standardu AT 101, která se zaměřuje na bezpečnostní opatření s cílem zajistit důvěrnost, integritu, dostupnost a soukromí.
- Standard Response to Request for Information - Microsoft Azure Security, Privacy, and Compliance obsahující seznam bezpečnostních požadavků uvedených v CSA (Cloud Security Alliance) Cloud Control Matrix a způsob jejich pokrytí v prostředí Microsoft Azure Core.
- Microsoft Azure for use with PCI DSS obsahující seznam bezpečnostních požadavků uvedených v PCI DSS v3.0 a způsob jejich pokrytí v prostředí Microsoft Azure Core.

9.2.5 PROSTŘEDÍ ČESKÉ REPUBLIKY

9.2.5.1 STANOVISKO NBÚ VE VĚCI VÝKLADU VYHLÁŠKY Č. 316/2014 SB.

Stanovisko NBÚ týkající se situace, kdy správce IS do svého systému řízení zahrne dodávku ICT formou sdílené služby (tzv. cloudové služby). NBÚ bude považovat za dostačující splnění požadavků podle §7 Vyhlášky, pokud správce doloží následující skutečnosti:

- Správce **významného informačního systému** zavede pravidla pro dodavatele cloudových služeb, která zohlední potřeby řízení bezpečnosti informací, přičemž ustanovení o bezpečnosti informací správce prokáže smlouvou, jejíž součástí je ustanovení o bezpečnosti informací, včetně výčtu zavedených bezpečnostních opatření na straně dodavatele.
- Správce **kritické informační infrastruktury** provádí podle §7 odst. 2 písm. a) a c) Vyhlášky hodnocení rizik podle přílohy č. 2 Vyhlášky vyžádáním následujících podkladů od dodavatele cloudových služeb:
  - Popis použité metodiky pro identifikaci a hodnocení rizik, včetně uvedení funkce hodnocení rizik, jejích proměnných a definice úrovní.
  - Výčet zohledněných hrozeb a zranitelností, který musí minimálně pokrývat seznam uvedený v §4 odst. 4 až 7 Vyhlášky.
- Dodavatel cloudových služeb by měl správci pro účely naplnění povinností plynoucích ze Zákona a Vyhlášky dále doložit:
  - Metody a přístupy pro zvládání rizik
  - Způsoby schvalování přijatelných rizik
  - Závazek řešení úrovní výsledných rizik „kritická“ a „vysoká“ podle přílohy č. 2 k Vyhlášce včetně časové lhůty stanovené ke snížení úrovně těchto rizik.
- Soulad doložených metod a nastavených interních procesů s výše uvedenými ustanoveními vyhlášky může dodavatel cloudových služeb doložit vyjádřením nezávislého auditora.
- Správce **kritické informační infrastruktury** uzavře s dodavatelem cloudových služeb smlouvu, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

- Požadavky lze ve smlouvě doložit certifikací ISO/IEC 27001 spolu s těmito podklady:
  - Bezpečnostní politika dodavatele ve struktuře ISO/IEC 27001.
  - Tzv. prohlášení o aplikovatelnosti, tedy výčet organizačních a technických bezpečnostních opatření ve struktuře ISO 27001 uplatněných dodavatelem cloudových služeb.
  - Auditní zprávou z certifikace cloudové služby podle ISO/IEC 27001.

9.2.5.2 PWC ISAE 3000 RISK ASSURANCE REPORT ŘÍZENÍ RIZIK V CLOUDU

Jedná se o dokument označený jako „Nezávislá zpráva o přiměřené jistotě - Pro management MICROSOFT s.r.o.“, autorem je společnost PWC ČR.

Dokument obsahuje zhodnocení metodiky pro posuzování rizik Microsoft Online Services z pohledu požadavků, vyplývajících ze Zákona a Vyhlášky, zejména v oblastech:

- Celkový přístup k řízení rizik v cloudu
- Metodika hodnocení rizik, funkce, definice proměnných a jejich úrovní
- Minimální seznam hrozeb a zranitelností (§4)
- Pravidelnost hodnocení rizik, způsoby schvalování přijatelných rizik
- Závazek včasného řešení vyšších úrovní výsledných rizik

Zpráva obsahuje výrok, že podle názoru auditora, hodnocená metodika MOSRAM vyhovuje ve všech významných ohledech požadavkům stanoveným v §5, odst.2, písm. b) Zákona, §4 Vyhlášky a §7 Vyhlášky.

10 TECHNICKÁ OPATŘENÍ

Seznam technických opatření je uveden v §5, odst. 2 zákona o kybernetické bezpečnosti, přičemž požadavky na tato opatření jsou rozvedeny v §16-27 Vyhlášky (část druhá, hlava II).

Požadavky na technická opatření vychází z požadavků Zákona, jejich konkrétní specifikace musí vyhovět výstupům provedené analýzy rizik, musí splňovat požadavky prováděcí bezpečnostní politiky (dle větší části §5 Vyhlášky) a zejména následnému návrhu bezpečnostních opatření pro konkrétní informační systém.

V následujících kapitolách jsou identifikována a analyzována jednotlivá technická opatření Zákona a Vyhlášky a způsoby jejich naplnění ve formě návodů, doporučení a architektonických vzorů.

10.1 FYZICKÁ BEZPEČNOST

Požadavky na technická opatření v oblasti fyzické bezpečnosti jsou uvedeny v §16 Vyhlášky. Jednotlivá požadovaná opatření se týkají objektů a vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému (KII, VIS).

10.1.1 IDENTIFIKACE POŽADAVKŮ NA FYZICKOU BEZPEČNOST

Vyhláška po správcích **VIS** požaduje přijmout opatření k

- zamezení neoprávněnému vstupu do vymezených prostor, kde jsou uloženy informace a technická aktiva IS,
- zamezení poškození a zásahům do vymezených prostor a
- předcházení krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního systému.

Po správci **KII** dále vyhláška požaduje stejné povinnosti jako v případě správce VIS, a navíc požaduje uplatnit prostředky fyzické bezpečnosti pro

- zajištění ochrany na úrovni objektů a
- zajištění ochrany v rámci objektů zajištěním bezpečnosti vymezených prostor,

přičemž mezi prostředky fyzické bezpečnosti jsou zejména počítány

- mechanické zábranné prostředky,
- zařízení elektrické zabezpečovací signalizace,
- prostředky omezující působení požárů,
- prostředky omezující působení projevů živelních událostí,
- systémy pro kontrolu vstupu,
- kamerové systémy,
- zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a
- zařízení pro zajištění optimálních provozních podmínek.

10.1.2 ANALÝZA POŽADAVKŮ NA FYZICKOU BEZPEČNOST

Pro naplnění požadavků Zákona a Vyhlášky v oblasti fyzické bezpečnosti je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření.

V případě IS určených jako VIS je na obecné úrovni požadováno řešit následují oblasti

- zajistit kontrolu osob při vstupu do prostor,
- zajistit ochranu prostor před poškozením nebo jiným zásahem (úmyslným nebo neúmyslným) a
- zajistit ochranu aktiv uložených v prostorách před poškozením, zneužitím nebo krádeží.

V případě IS určených jako KII jsou požadavky konkrétnější a je navíc požadováno zajistit ochranu jak na úrovni prostor, tak i na úrovni objektu, ve kterém jsou tyto prostory umístěny, a je specifikován seznam prostředků, které by na základě výsledků hodnocení rizik k tomuto účelu měly být použity.

10.1.3 VZORY TECHNICKÝCH OPATŘENÍ FYZICKÉ BEZPEČNOSTI

Následující vzory implementace technických opatření jsou rozděleny podle oblastí a typů prostředků fyzické bezpečnosti uvedených ve vyhlášce. V případě, kdy je možné vzor implementace uplatnit ve dvou anebo více oblastech za použití více prostředků, je zvolena ta oblast resp. ten prostředek, kde se vzor uplatní nejvíce.

Zajištění kontroly osob při vstupu (zamezení neoprávněného vstupu) je zajišťováno zejména:

- Mechanickými zábrannými prostředky
  - Ochranou přilehlého pozemku (úroveň objektu)
    - Oplocení pozemku
  - Ochranou pláště budovy (úroveň objektu)
    - Pevná konstrukce budovy z odolných materiálů
    - Bezpečnostní a protipožární dveře
  - Zabezpečením otvorů vymezeného prostoru (úroveň prostor, objektu)
    - Bezpečnostní dveře
    - Mříže ve dveřích a oknech
    - Uzavíratelná okna s bezpečnostní folií
- Systémy pro kontrolu vstupu (úroveň prostor, objektu)
  - Fyzickou ostrahou budovy
  - Zabezpečovacím systémem s autentizací do vyhrazené oblasti

Zajištění ochrany prostor před poškozením nebo jiným zásahem (zamezení poškození a zásahům do prostor) je zajišťováno zejména:

- Prostředky omezujícími působení požárů (úroveň prostor)
  - Protipožární dveře
  - Hasicí zařízení nebo přístroj

- Prostředky omezujícími působení projevů živelních událostí (úroveň objektu)
  - Umístěním budovy mimo záplavovou oblast
  - Umístěním budovy v dostatečné vzdálenosti od vedení vysokého napětí, letiště, významných průmyslových objektů, elektráren
  - Zvolením vhodné architektury budovy a stavebního materiálu pro odolnost proti povětrnostním vlivům (vichřice, orkány)
  - Zvolením vhodného umístění budovy z pohledu odolnosti proti geologickým vlivům (zemětřesení, sesuv půdy)

Zajištění ochrany aktiv uložených v prostorách (předcházení poškození, zneužití nebo krádeži) je zajišťováno zejména:

- Zařízeními elektrické zabezpečovací signalizace (úroveň prostor, objektu)
  - Zabezpečovací systém
- Kamerovými systémy (úroveň prostor, objektu)
  - Kamerovým systémem monitorujícím okolí a plášť budovy
  - Kamerovým systémem se záznamem, monitorujícím vstup do vyhrazené oblasti
- Zařízeními pro zajištění ochrany před selháním dodávky elektrického napájení (úroveň prostor)
  - Správně dimenzovaný systém UPS s přepěťovou ochranou, včetně zajištění pravidelné kontroly chodu a údržby
  - Agregát pro výrobu elektrické energie
  - Připojení z více směrů
- Zařízeními pro zajištění optimálních provozních podmínek (úroveň prostor)
  - Klimatizace s dostatečnou výkonnostní rezervou, včetně systému monitorujícího teplotu vyhrazené oblasti a provozní stav klimatizace, zajištění pravidelné kontroly a údržby klimatizace

10.1.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V oblasti fyzické bezpečnosti je prostředí Microsoft Online Services chráněno následovně:

Bezpečnostní politika společnosti Microsoft (Microsoft Security Policy) definuje požadavky na fyzickou bezpečnost a bezpečnost prostředí, které zahrnují:

- Definování pravidel pro zabránění neoprávněnému fyzickému přístupu nebo poškození a rušení informací
- Zabránění a kontrola neoprávněného fyzického přístupu k produkčním informačním systémům a zařízením
- Zabránění a kontrola neoprávněného fyzického přístupu k citlivým informačním systémům a zařízením
- Ochrana informačních systémů proti neplánovaným výpadkům, jako jsou výpadky proudu, selhání vybavení a ohrožení životního prostředí

Bližší podrobnosti o nasazených opatřeních je možné nalézt v dokumentech uvedených v kapitole 9.2.

10.2 NÁSTROJ PRO OCHRANU INTEGRITY KOMUNIKAČNÍCH SÍTÍ

Požadavky na technická opatření v oblasti ochrany integrity komunikačních sítí jsou uvedeny v §17 Vyhlášky.

10.2.1 IDENTIFIKACE POŽADAVKŮ NA OCHRANU INTEGRITY KOMUNIKAČNÍCH SÍTÍ

Vyhláška požaduje přijmout opatření k:

- Řízení bezpečného přístupu mezi vnější a vnitřní sítí
- Realizaci segmentace sítě, zejména použití demilitarizovaných zón s cílem zamezení přímé komunikace vnitřní sítě z vnější a ke zvýšení bezpečnosti aplikací dostupných z vnější sítě
- Pro KII k zajištění segmentace sítě se využívají nástroje pro ochranu integrity vnitřní komunikační sítě
- Zavedení kryptografických prostředků (podle §25 vyhlášky) pro:
  - Vzdálený přístup
  - Vzdálenou správu
  - Přístup pomocí bezdrátových technologií
- Odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity sítě

10.2.2 ANALÝZA POŽADAVKŮ NA OCHRANU INTEGRITY KOMUNIKAČNÍCH SÍTÍ

Pro naplnění požadavků Zákona a Vyhlášky v oblasti fyzické bezpečnosti je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Řídit komunikaci mezi vnitřní a vnější sítí. Bezpečnostní pravidla nastavit tak, aby byla umožněna pouze síťová komunikace, která je nezbytná k zajištění funkčnosti a provozu informačního systému
- Pomocí aktivních síťových prvků provést segmentaci sítě tak, aby nebyla možná přímá komunikace mezi vnitřní a vnější sítí
- Pro KII pomocí aktivních síťových prvků provést segmentaci sítě tak, aby nebyla možná přímá komunikace mezi oddělenými částmi vnitřní sítě
- Vzdálený přístup, vzdálená správa a přístup pomocí bezdrátových technologií musí pro zajištění důvěrnosti a integrity dat a pro identifikaci uživatelů využívat kryptografickou ochranu

Aby tato sada opatření měla správný a očekávaný efekt, je třeba je zasadit do kontextu informačního systému již od počátku jeho vlastního návrhu.

Architektura systému musí podporovat segmentaci sítě:

- Informační systém je navržen tak, aby měl oddělenou prezentační, aplikační a datovou vrstvu
- Komunikace mezi jednotlivými vrstvami je jednoznačně definovaná, což umožňuje správné nastavení bezpečnostních pravidel omezujících komunikaci na rozhraních sítí pouze na nezbytně nutnou

Síťová infrastruktura musí umožňovat požadovanou úroveň zabezpečení:

- Vzdálený přístup, vzdálená správa a přístup pomocí bezdrátových technologií (například Wi-Fi) je zabezpečen pomocí kryptografických prostředků
- Kryptografické algoritmy a kryptografické klíče musí splňovat minimální požadavky uvedené v příloze č. 3 Vyhlášky a v analýze rizik. Identifikace a analýza požadavků na kryptografické algoritmy a kryptografické klíče je uvedena v kapitole 10.10.

10.2.3 VZORY TECHNICKÝCH OPATŘENÍ PRO NÁSTROJ PRO OCHRANU INTEGRITY KOMUNIKAČNÍCH SÍTÍ

Řízení bezpečného přístupu mezi vnitřní a vnější sítí a odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity sítě, může být realizováno:

- Zavedením pravidel síťové komunikace a jejich prosazením do technologie. Vhodným nástrojem pro realizaci prosazení pravidel je:
  - Firewall
  - Paketový filtr

Segmentace sítě použitím demilitarizovaných zón může být realizována:

- Vytvořením fyzických nebo virtuálních sítí a jejich bezpečným propojením podle §17 odstavec (1) písmeno d), tedy například pomocí:
  - Firewallu
  - Paketového filtru

Kryptografická ochrana pro vzdálený přístup, vzdálená správa a přístup pomocí bezdrátových technologií může být realizována:

- Použitím autentizačních mechanismů, které vyhovuji kryptografickým požadavkům (protokol, šifrovací algoritmus, typ a délka klíče) analýzy rizik a přílohy č. 3 Vyhlášky, viz 10.3.3
- Zašifrováním síťové komunikace způsobem, který vyhovuje kryptografickým požadavkům (protokol, šifrovací algoritmus, typ a délka klíče) analýzy rizik a přílohy č. 3 Vyhlášky
  - Zašifrování síťové komunikace musí zajistit požadovanou úroveň integrity a důvěrnosti přenášených dat. Úroveň bezpečnosti závisí nejen na použitém šifrovacím algoritmu a délce klíče, ale také na způsobu výměny a uložení klíčů. Z protokolů mohou být využity například: TLS 1.2, IPSec, WPA2

10.2.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

V oblasti ochrany integrity komunikačních sítí je prostředí Microsoft Online Services chráněno následovně:

Microsoft Azure

Microsoft Azure poskytuje možnosti ochrany na úrovni datového centra Azure a to v několika úrovních, viz [3] a [4]:

- Zablokování neautorizované komunikace do a uvnitř datového centra s použitím:
  - Izolace prosazované na několika úrovních
    - Komunikace mezi virtuálními servery vždy prochází přes paketový filter (firewall)
    - Virtuální server není schopen komunikovat na úrovni 2 vrstvy ISO/OSI modelu a tudíž nemůže odposlouchávat síťovou komunikaci, která není určena přímo jemu

        - Virtuální server nemůže odeslat DHCP odpověď, pouze DHCP požadavek. Pouze Network Manager – komponenta Azure infrastruktury smí odesílat DHCP odpovědi
        - Virtuální servery nemohou komunikovat s klíčovými virtuálními servery Azure infrastruktury
        - Segmentace sítě je zajištěna pomocí Azure virtuálních sítí (Azure Virtual Netvork – VNET), virtuální síť může obsahovat jeden nebo více IP v4 subnetů. V rámci nasazení (deployment) je možné vytvořit množství VNET. Pomocí Network Security Group (firewallů) lze nastavit potřebnou komunikaci (definovat ACLs). Network Security Group může být přiřazena virtuální síti nebo jednotlivému síťovému adaptéru virtuálního serveru. Virtuální servery mohou být připojeny do jedné nebo více VNET. Na úrovni virtuálního síťového adaptéru lze řídit síťovou komunikaci pomocí interního firewallu virtuálního serveru nebo pomocí Network Security Group (firewallů)
    - Překladu IP adres – NAT, komponenta Endpoint
    - Fyzického oddělení back;end serverů od Internetu
    - Použití privátních IP adres
        - Po instalaci je virtuálnímu serveru v Microsoft Azure přidělena privátní IP adresa, která není z principu z Internetu dostupná
        - Pro zajištění přístupu z Internetu k virtuálnímu serveru je nutné vytvořit a konfigurovat Endpoint, který má přiřazenou veřejnou IP adresu a na kterém se nastavuje povolená komunikace (ACLs)
- Šifrování síťové komunikace je zajištěno v následujících případech:
    - Komunikace mezi datovými centry
    - Komunikace mezi lokalitou zákazníka a datovým centrem Azure. Tuto komunikaci lze zašifrovat pomocí:
        - End to End s použitím protokolu TLS (například HTTPS).
        - Point to Site VPN s použitím protokolu SSTP.
        - Site to Site (služba Virtual VPN Gateway) s použitím protokolu IPsec.
        - Pronajatý okruh mezi lokalitou zákazníka a datovým centrem Azure pomocí služby Express Route, které ale nešifruje data přenášená přes WAN – šifrování komunikace je nutné zajistit vlastními silami.
        - Řešení VPN koncentrátoru na straně Microsoft Azure pomocí produktů třetích stran, například Barracuda NextGen Firewall, Cicso ASAv nebo Fortinet FortiGate NGFW, které nabízí možnost provozovat v Microsoft Azure vlastní firewall s VPN koncentrátorem.
- Zabezpečení vzdáleného přístupu a vzdálené správy
    - Přístup k portálu správy je zašifrován pomocí protokolu TLS 1.2
    - Vzdálený přístup k virtuálním serverům s operačním systémem Windows (IaaS) používá pro připojení pomocí protokolu RDP náhodný port, komunikace je zašifrovaná pomocí protokolu SSL/TLS s konfigurací použitou pro operační systém virtuálního serveru.
    - Vzdálený přístup k virtuálním serverům s operačním systémem BSD/Linux/Unix (IaaS) používá pro připojení pomocí protokolu SSH náhodný port, komunikace je zašifrovaná s konfigurací použitou pro operační systém virtuálního serveru.
    - Další zabezpečení vzdáleného přístupu je možné pomocí:

- Využití připojení přes Point to Site VPN, Site to Site VPN nebo pronajatá okruh (služba Express Route) doplněný o šifrování komunikace.
- Omezení přístupu z Internetu pro vyjmenované IP adresy na úrovni Endpointů použitých pro vzdálenou správu virtuálních serverů
- Řešení VPN koncentrátoru na straně Microsoft Azure pomocí produktů třetích stran, například Barracuda NextGen Firewall, Cicso ASAv nebo Fortinet FortiGate NGFW, které nabízí možnost provozovat v Microsoft Azure vlastní firewall s VPN koncentrátorem.

Office 365

Microsoft Office 365 poskytuje možnosti ochrany komunikačních sítí, viz [5]:

- Protože Office 365 využívá technologie Microsoft Azure, automaticky využívá možností zabezpečení, která poskytují technologie Azure
- Office 365 je poskytován jako SaaS a proto není možné definovat architekturu služeb, serverů, síti ani jejich bezpečnostní parametry. Tato oblast bezpečnosti je zajišťována společností Microsoft
- Vzdálená správa služeb Office 365 je prováděna prostřednictvím webového rozhraní Office 365 portálu
  - Přístup k tomuto portálu je zabezpečen autentizací, kdy je možné:
    - Využít federované autentizace interní Active Directory nebo jinou kompatibilní adresářovou službou
    - Využít dvou faktorovou autentizaci
  - Integrita a důvěrnost přenášených dat je zajištěna použitím protokolu TLS
- Pro přístup ke službám Office 365 se používají různé síťové protokoly, jako například HTTPS, POP3, IMAP a další. Tyto protokoly jsou zabezpečeny pomocí protokolu TLS
- Pro některé případy je možné využít zabezpečení přenášených dat na aplikační úrovni:
  - Azure Rights Management (Azure RMS) pro zabezpečení obsahu jednotlivých dokumentů nebo mailů
  - Secure/Multipurpose Internet Mail Extensions (S/MIME) pro šifrování a digitální podepisování mailů
  - Office 365 Message Encryption, využívá Azure RMS, řeší zabezpečení mailů zasílaných externím uživatelům a partnerům
  - SMTP TLS pro partnery, umožňuje při použití certifikátů konfigurovat mezi definovanými poštovními servery šifrování na úrovni protokolu SMTP

10.3 NÁSTROJ PRO OVĚŘOVÁNÍ IDENTITY UŽIVATELŮ

Požadavky na technická opatření v oblasti ověřování identity uživatelů a administrátorů jsou uvedeny v §18 Vyhlášky.

10.3.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO OVĚŘOVÁNÍ IDENTITY UŽIVATELŮ

Vyhláška požaduje přijmout pro VIS i KII opatření k:

- Ověření identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému nástrojem pro ověřování identity
- Pokud nástroj pro ověřování identity používá autentizaci heslem, musí zajistit:
  - Minimální délku hesla 8 znaků
  - Složitost hesla, kdy heslo obsahuje minimálně tři z následujících čtyř požadavků:
    - Nejméně jedno velké písmeno
    - Nejméně jedno malé písmeno
    - Nejméně jednu číslici
    - Nejméně jeden speciální znak
  - Maximální doba platnosti hesla nepřesahuje 100 dnů
- Pro KII navíc nástroj:
  - Zamezení opětovnému používání dříve používaných hesel neumožněním opětovné změny hesla v období minimálně 24 hodin
  - Provádí opětovné ověření identity po určené době nečinnosti
  - V případě autentizace administrátorů heslem zajistí prosazení minimální délky hesla 15 znaků při dodržení dalších výše uvedených požadavků na hesla
- Nástroj pro ověřování identity může být zajištěn i jinými způsoby, pokud bude zabezpečeno, že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti hesla

10.3.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO OVĚŘOVÁNÍ IDENTITY UŽIVATELŮ

Pro naplnění požadavků Zákona a Vyhlášky v oblasti nástroje pro autentizaci uživatelů je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Informační systém sám anebo prostřednictvím infrastruktury IT musí spravovat identity uživatelů a administrátorů. Musí být tedy k dispozici nástroj pro správu identit, který:
  - Eviduje uživatele a administrátory
  - Ověřuje identitu uživatelů a administrátorů, provádí tedy jejich autentizaci a to před umožněním přístupu uživatelů a administrátorů k informačnímu systému
  - Prosazuje definovanou politiku hesel
    - Minimální délka hesla 8 znaků
    - Vynucená komplexnost hesla
    - Maximální doba platnosti hesla 100 dnů

- V případě KII je pro administrátory vyžadována odlišná, přísnější politika hesel, kdy k výše uvedeným požadavkům na hesla musí být použita
  - Minimální délka hesla 15 znaků
  - Minimální doba platnosti hesla 24 hodin
  - Opětovné ověření identity po určené době nečinnosti
- K ověření identity je možné používat i jiné metody, pokud zajistí minimálně stejnou nebo vyšší úroveň bezpečnosti, například více faktorová autentizace

10.3.3 VZORY TECHNICKÝCH OPATŘENÍ PRO NÁSTROJ PRO OVĚŘOVÁNÍ IDENTITY UŽIVATELŮ

Obecný model informačního systému, viz kapitola 6, nepředpokládá lokální přihlašování uživatele na servery, které provozují informační systém. Dnes je obvyklé, že je uživatel autentizován a k systému přistupuje prostřednictvím počítačové sítě. Z tohoto důvodu je nutné do architektury nástroje pro identifikaci uživatelů zahrnou i autentizační protokoly, které umožní autentizaci bez zasílání hesla po síti.

Z důvodu snížení komplexnosti informačního systému je vhodné využít adresářovou službu, která poskytne autentizační služby, zajistí bezpečnost uložených informací a implementuje autentizační protokoly.

Příkladem adresářové služby je:

- Microsoft Active Directory
- OpenLDAP
- Oracle Internet Directory

Vybrané řešení musí podporovat funkce a splňovat následující požadavky:

- Prosazení politiky hesel v souladu s požadavky zákona - hesla musí splňovat požadavky na maximální stáří a minimální délku a na složitost hesla. (například stáří max. 60 dní, délka min. 8 znaků, použití malých písmen, velkých písmen, číslic a speciálních znaků)
- Použití bezpečných autentizačních protokolů (například Kerberos, EAP-TLS s MS-CHAP2, SAML)
- Volitelně podporu více faktorových autentizačních metod doplňujících autentizaci uživatelským jménem a heslem
  - Biometrické autentizační metody
  - Autentizace s využitím asymetrické kryptografie
  - Jednorázová hesla (například HOTP, TOTP, jednorázová hesla zaslaná jiným komunikačním kanálem – například pomocí SMS)
- Další požadavky definované bezpečnostní politikou

10.3.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast nástroje pro autentizaci uživatelů je prostředí Microsoft Online Services realizována následovně:

Microsoft Azure i Office 365

Microsoft pro potřeby Microsoft Online Services provozuje multi-tenant cloudovou adresářovou službu a službu správy identit - Azure Active Directory, viz [10]. Azure AD podporuje autentizaci

- Jménem a heslem
- Multi-faktorovou autentizaci
  - Autentizace jménem a heslem je ještě doplněna o autentizaci pomocí zařízení
  - Telefonickým hovorem
  - Textovou zprávou
  - Mobilní aplikací – notifikací
  - Mobilní aplikací – ověřovacím kódem
  - OATH tokenem

Azure AD více faktorovou autentizaci lze použít v případech:

- Autentizace administrátora (Azure subscription) k Microsoft Azure
- Autentizace administrátora (Office 365 subscription) k Office 365
- Autentizace uživatelů ke službám Office 365 a dalším službám využívajícím Azure AD (včetně on-premise služeb)

Azure AD umožňuje definovat politiku hesel na úrovni předplatného nebo domény, viz [11]. Výchozí nastavení politiky hesel je následující:

- Délka hesla 8 – 16 znaků
- Maximální doba platnosti hesla 90 dní. Hodnotu lze měnit
- Oznámení o ukončení platnosti hesla 14 dní před ukončením. Hodnotu lze měnit
- Ukončení platnosti hesla je zakázané (heslo nevyprší). Hodnotu lze měnit
- Minimální doba platnosti hesla – poslední heslo nelze znovu použít
- Historie hesel bez omezení
- Zamykání účtu. Po deseti neplatných pokusech o přihlášení musí uživatel opsat zobrazený text (CAPTCHA), což zajišťuje ochranu před automatizovaným útokem.

Azure AD obsahuje funkci správy privilegovaných identit (Privileged Identity Management, viz [8]), která umožňuje spravovat řídit a monitorovat privilegované identity/organizační role:

- Global Administrator
- Billing Administrator
- Service Administrator
- User Administrator
- Password Administrator

Správa privilegovaných identit obsahuje funkce:

- Zjištění, kteří uživatelé AD jsou administrátory Azure
- Povolení on-demand „just in time“ administrátorského přístupu
- Reporty o historii přístupu administrátora a o změnách rolí
- Notifikace o přístupu k administrátorské roli

Azure AD podporuje integraci s interními adresářovými službami (On-Premise Directory), viz [9], pomocí:

- Synchronizace identit
  - Identity jsou synchronizované, hesla mohou být různá s různou politikou a musí být udržována separátně
- Synchronizace identit a hesel (synchronizuje se hash hesla)
  - Identity i hesla jsou synchronizovaná, uživatelé používají jedno heslo ke cloudovým i on-premise systémům. Změna hesla je propagována napříč synchronizovanými adresářovými službami
- Federace identit
  - Informace o identitě je synchronizována s Azure AD, vlastní autentizace ale zajišťuje on-premise adresářová služba (například Active Directory)

Z výše uvedeného vyplývá, že Azure AD je při použití autentizace jménem a heslem vhodná pro systémy VIS a pro systémy KII jen pro uživatele. Při použití multi-faktorové autentizace vyhoví všem požadavkům Zákona a Vyhlášky a to i pro administrátory KII.

Microsoft Azure umožňuje v prostředí IaaS provozovat širokou škálu adresářových služeb s i bez vazeb na adresářovou službu Azure AD.

10.4 NÁSTROJ PRO ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

Požadavky na technická opatření v oblasti řízení přístupových oprávnění jsou uvedeny v §19 Vyhlášky.

10.4.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

Vyhláška požaduje přijmout opatření k:

- Zajištění řízení oprávnění
  - Pro přístup k aplikacím a datům
  - Pro čtení dat, zápis dat a pro změnu oprávnění
- Zaznamenávání použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik

10.4.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

Pro naplnění požadavků Zákona a Vyhlášky v oblasti nástroje pro řízení přístupových oprávnění je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Řídit přístup k aplikacím a k datům
  - Granularita přístupu musí být minimálně
    - Čtení
    - Zápis
    - Změna přístupových oprávnění
- Zaznamenávat použití oprávnění
  - Provádět audit přístupu k aplikacím a datům
  - Provádět audit prováděných změn v přístupových oprávněních

10.4.3 VZORY TECHNICKÝCH OPATŘENÍ PRO NÁSTROJ PRO ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

Informační systém, jeho jednotlivé aplikace a infrastruktura IT, která je pro provoz informačního systému používána, musí při přístupu k aplikacím a datům informačního systému umožňovat autentizaci a autorizaci uživatelů a administrátorů. Také musí umožňovat provádění auditu těchto přístupů.

Při návrhu informačního systému je tedy třeba použít takovou architekturu a takové komponenty IS, které splňují výše uvedené požadavky. Například v případě operačních systémů Linux a Microsoft Windows jsou požadované funkce součástí jádra a systémových funkcí operačního systému.

10.4.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast nástroje pro řízení přístupových oprávnění je v prostředí Microsoft Online Services realizována následovně:

Microsoft Azure

Microsoft Azure obsahuje vestavěné funkce na řízení přístupu pomocí rolí (RBAC). Role může být přiřazena uživateli, skupině nebo službě z Azure AD, viz [12]. Přiřazení rolí může být realizováno na úrovni:

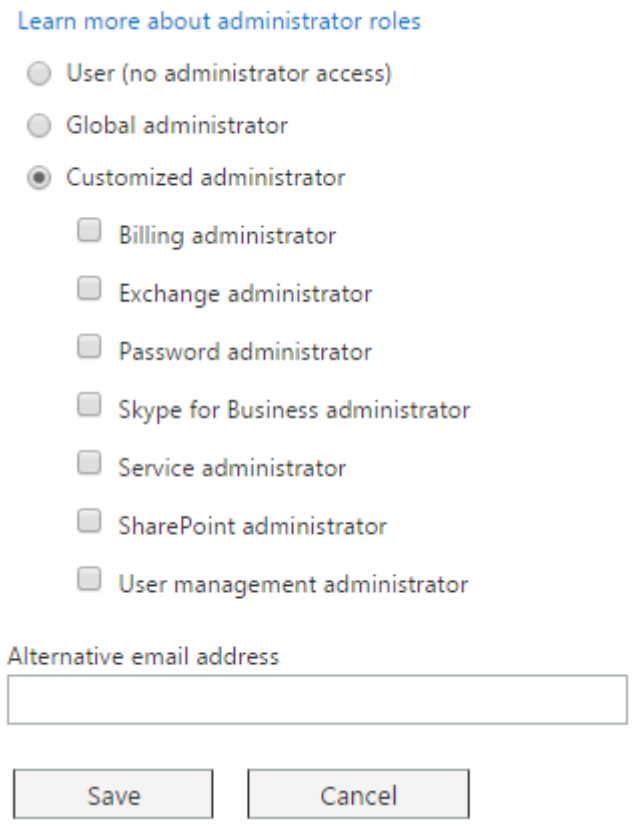
- Předplatného (Subscription)
- Skupiny zdrojů (Resource Group)
- Zdroje

Microsoft Azure umožňuje v prostředí IaaS provozovat informační systémy na virtualizovaných serverech. V takovém prostředí je řízení přístupových oprávnění realizováno na úrovni virtualizovaných serverů nebo na nich provozovaných komponent, služeb a aplikací.

Office 365

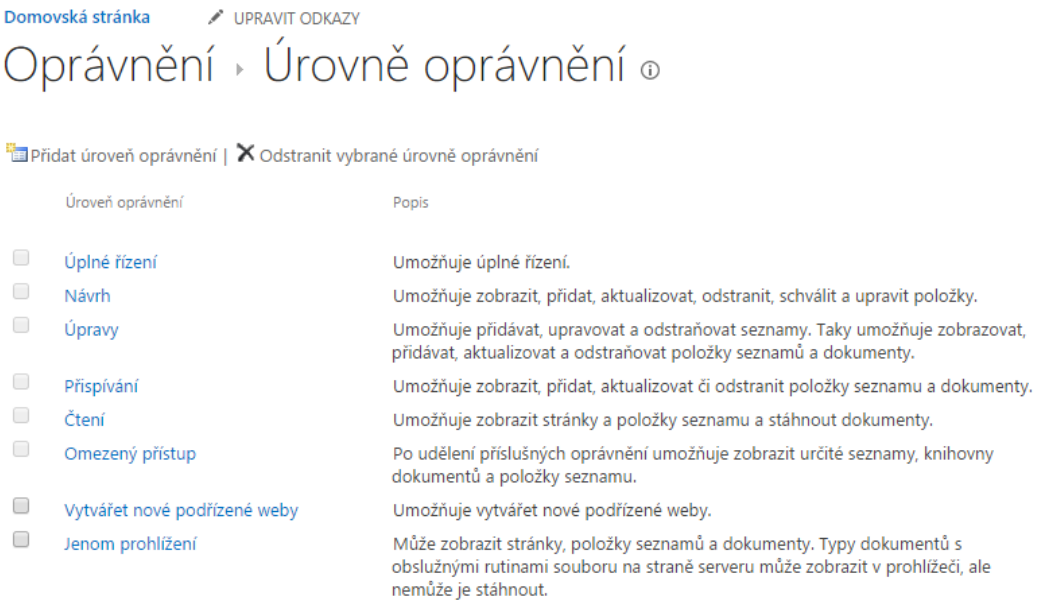
Office 365 obsahuje vlastní administrátorské role. Tyto role mohou být přiřazeny na úrovni portálu správy Office 365.

Obr. 3
Administrátorské role Office 365



Jednotlivé části Office 365, jako Exchange, Sharepoint a další mají vlastní portály správy (dostupné z portálu Office 365), kde je možné přiřazovat specifické administrátorské i uživatelské role a v rámci těchto částí.

Obr. 4
Přístupová oprávnění webu Sharepoint



Zaznamenávání používání přístupových oprávnění (auditing) je nutné řešit v prostředí Microsoft Online Services individuálně na jednotlivých službách a objektech. Informace o auditování v prostředí Microsoft Online Services jsou uvedeny v kapitole 10.6.4.

10.5 NÁSTROJ PRO OCHRANU PŘED ŠKODLIVÝM KÓDEM

Požadavky na technická opatření v oblasti ochrany před škodlivým kódem jsou uvedeny v §20 Vyhlášky.

10.5.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO OCHRANU PŘED ŠKODLIVÝM KÓDEM

Vyhláška požaduje přijmout opatření k:

Používání nástroje pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu:

- Komunikace mezi vnitřní sítí a vnější sítí
- Serverů a sdílených datových úložišť
- Pracovních stanic

Odpovědná osoba zajistí:

- Pravidelnou a účinnou aktualizaci nástroje
- Aktualizaci definic a signatur

10.5.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO OCHRANU PŘED ŠKODLIVÝM KÓDEM

Pro naplnění požadavků Zákona a Vyhlášky v oblasti nástroje pro ochranu před škodlivým kódem je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Vybrat antimalwareové řešení
- Implementovat antimalwareové řešení
- Zajistit provoz a provozní podporu pro antimalwareové řešení

Toto řešení musí zajistit ochranu KII a VIS na dále uvedených úrovních, a to v rozsahu daném hodnocením rizik:

- Na rozhraní sítí (perimetru), tj. umístěním nástroje v DMZ, na proxy serveru nebo firewallu tak, aby nástroj mohl provádět ochranu na úrovni síťové komunikace
- Serverů a datových úložišť tak, aby nástroj mohl provádět ochranu dat, která jsou uložena a ke kterým se přistupuje na datových úložištích a na serverech. Také má zajistit kontrolu kódu, který je na serverech spouštěn
- Pracovních stanic tak, aby nástroj mohl provádět ochranu dat, která jsou uložena a ke kterým se přistupuje na stanicích. Také má zajistit kontrolu kódu, který je na stanicích spouštěn. Z logického hlediska by měl být požadavek na pracovní stanice vztažen na veškerá koncová uživatelská zařízení, viz kapitola 6.

10.5.3 VZORY TECHNICKÝCH OPATŘENÍ PRO NÁSTROJ PRO OCHRANU PŘED ŠKODLIVÝM KÓDEM

Technického opatření nástroje pro ochranu před škodlivým kódem může být realizováno:

- Implementací antimalwareového řešení
  - Pro ochranu příchozí a odchozí komunikace informačního systému
    - Zajištění antimalwareové ochrany na úrovni protokolů aplikačních HTTP a SMTP, případně dalších, které jsou využívány informačním systémem
  - Pro ochranu serverů a datových úložišť využívaných pro provoz informačního systému
    - Zajištění ochrany na úrovni spouštěného kódu na serverech
    - Zajištění ochrany na úrovni uložených dat na serverech a diskových polích
  - Pro ochranu koncových uživatelských zařízení, která jsou používána k přístupu k informačnímu systému
    - Zajištění ochrany na úrovni spouštěného kódu na osobních počítačích, chytrých telefonech a tabletech
    - Zajištění ochrany na úrovni uložených dat na osobních počítačích, chytrých telefonech a tabletech
- Centrální správou antimalwareového řešení, která zajistí
  - Přehled o stavu antimalwareového řešení
  - Distribuci aktualizací definic a signatur
  - Provozní dohled

Vlastní technologie použitá pro realizaci těchto opatření je závislá na architektuře a použitých technologiích informačního systému.

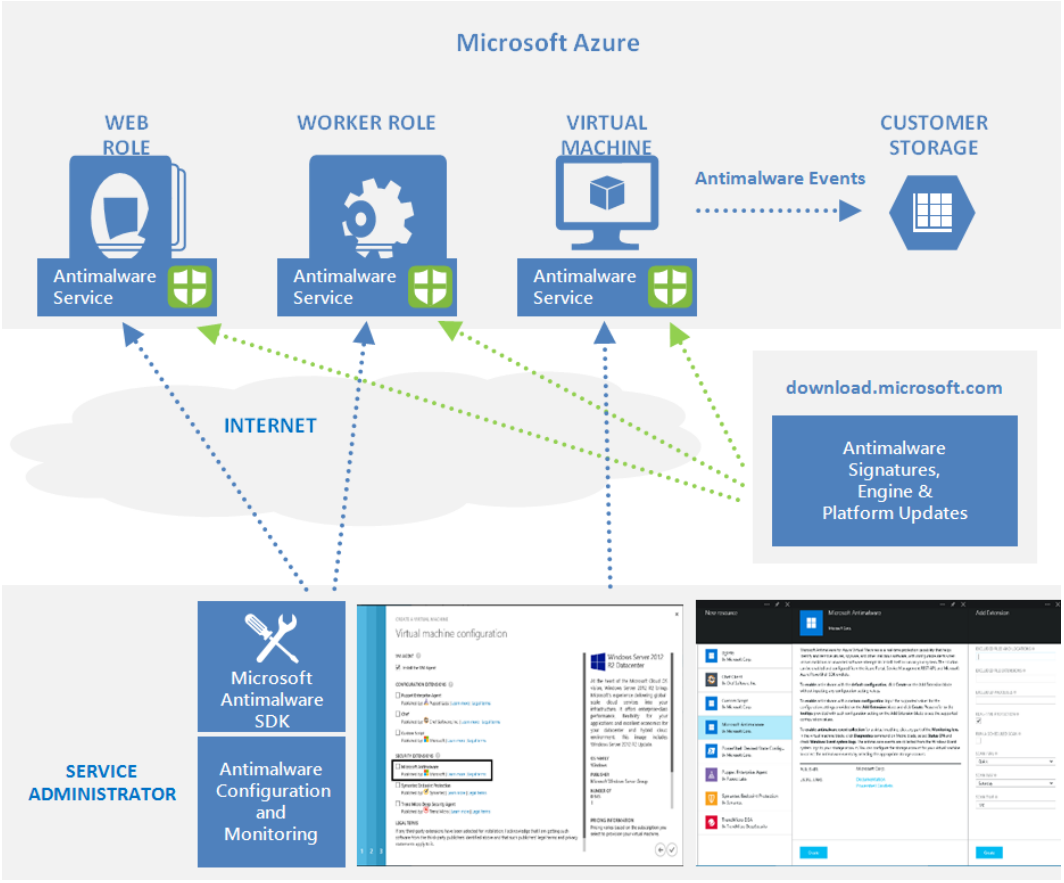
10.5.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast nástroje pro ochranu před škodlivým kódem je v prostředí Microsoft Online Services realizována následovně:

Microsoft Azure

V oblasti Microsoft Azure IaaS a PaaS je ochrana před škodlivým kódem prostřednictvím Microsoft Antimalware for Azure Cloud Services and Virtual Machines, viz [23], který umožňuje:

- Ochranu v reálném čase
- Plánované scanovaní
- Odstranění malwaru, karanténu
- Aktualizaci signatur
- Aktualizaci platformy a antimalwareového stroje
- Výjimky
- Aktivní ochranu – aktivní a rychlá odezva na detekované hrozby
- Reporting
- Auditní logování
- Vlastní přizpůsobení konfigurace (pomocí XML a JASON šablon)



Obr. 5 Microsoft Antimalware for Azure Cloud Services and Virtual Machines, viz [23]

Microsoft Azure poskytuje i integrované antimalwareové řešení třetích stran, například Deep Security od společnosti Trend Micro.

Office 365

V oblasti Microsoft Office 365 je ochrana před škodlivým kódem realizována prostřednictvím Microsoft Antimalware, který zajišťuje automatickou ochranu pro:

- Exchange Online Protection (EOP), viz [59]
  - Antispamová a antimalwareová ochrana příchozích a odchozích mailů
  - Multi-engine ochrana
  - Ochrana v reálném čase
  - Přednostní aktualizace signatur a definic
- Sharepoint Online
  - Antimalwareová ochrana pro soubory v knihovně dokumentů
- Exchange Online Advanced Threat Protection, viz [60]
  - Ochrana příloh proti neznámému škodlivému kódu
  - Ochrana proti zákeřným odkazům v reálném čase
  - Pokročilé reporty a sledování vektoru útoku

10.6 NÁSTROJ PRO ZAZNAMENÁVÁNÍ ČINNOSTÍ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY A VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMŮ, JEJICH UŽIVATELŮ A ADMINISTRÁTORŮ

Požadavky na technická opatření v oblasti nástroje pro zaznamenávání činností jsou uvedeny v §21 Vyhlášky.

10.6.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO ZAZNAMENÁVÁNÍ ČINNOSTÍ

Vyhláška požaduje přijmout opatření k:

- Používání nástroje pro zaznamenávání činností informačního systému, který zajistí:
  - Sběr informací o provozních a bezpečnostních činnostech
    - Přihlášení a odhlášení uživatelů a administrátorů
    - Činnosti provedené administrátory
    - Činnosti vedoucí ke změně přístupových oprávnění
    - Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
    - Zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury
    - Komunikačního systému kritické informační infrastruktury a významného informačního systému
    - Automatická varovná nebo chybová hlášení technických aktiv
    - Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností
    - Použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení
  - Ochranu získaných informací
    - Před neoprávněným čtením nebo změnou
    - Pro KII uchování informací nejméně po dobu 3 měsíců
- Zajištěni synchronizace systémového času technických aktiv KII a VIS nejméně jednou za 24 hodin

10.6.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO ZAZNAMENÁVÁNÍ ČINNOSTÍ

Pro naplnění požadavků Zákon a Vyhlášky v oblasti nástroje pro zaznamenávání činností je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Konfigurovat aktiva, na kterých je provozován informační systém tak, aby prováděly zaznamenávání činností podle požadavků Vyhlášky, viz kapitola 10.6.1. Vhodné je použití lokálního úložiště na daném systému s následnou centralizací událostí v centrálním nástroji pro zaznamenávání činností

- Tento záznam činností musí být proveden tak, aby obsahoval informace o:
  - Času výskytu události
  - Zdroji události
  - Objektu, na kterém se událost vyskytla
  - Typu události (chyba, varování, informace)
  - Popisu události
- Sběr a správa logů musí zajistit
  - Ochranu uložených informací (logů) pomocí přidělení přístupových oprávnění na úrovni čtení a zápisu
  - Pro KII uchování informací minimálně po dobu 3 měsíců
- Komponenty informačního systému i centrální nástroj pro zaznamenávání činností musí mít synchronizován systémový čas

10.6.3 VZORY TECHNICKÝCH OPATŘENÍ PRO NÁSTROJ PRO ZAZNAMENÁVÁNÍ ČINNOSTÍ

Technického opatření nástroje pro zaznamenávání činností může být realizováno:

- Nastavením zaznamenávání požadovaných činností a informací, tj. povolením a konfigurací auditování na jednotlivých komponentách, které slouží k provozu informačního systému, viz kapitola 6:
  - Servery a disková pole
  - Databázové systémy, webové a aplikační servery
  - Adresářové služby, nebo jiné komponenty, které slouží pro autentizaci uživatelů a správců
  - Aktivní síťové prvky
  - Koncová uživatelská zařízení
  - Nástroj pro zaznamenávání činností – log management
- Návrhem, implementací a provozem nástroje pro zaznamenávání činností – centrálním log managementem, který:
  - Má dostatečnou kapacitu pro uložení sebraných událostí (logů) po dobu minimálně 3 měsíce
  - Umožňuje nastavit přístupová oprávnění pro přístup k uchovávaným logům minimálně v úrovních pro čtení a zápis
- Nastavením synchronizace systémového času všech technických aktiv informačního systému s důvěryhodným zdrojem přesného času

10.6.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Zaznamenávání používání přístupových oprávnění (auditing) je nutné řešit v prostředí Microsoft Online Services individuálně na jednotlivých službách a objektech.

Microsoft Azure

Microsoft Azure umožňuje zákazníkům provádět generování a ukládání bezpečnostních událostí z Azure, infrastruktura jako služba (IaaS) a platforma jako služba (PaaS) do centrálního úložiště v předplatném, viz [13] a [14]. Zákazníci mohou poté tyto události agregovat a analyzovat pomocí HDInsight nebo tyto události exportovat a následně je zpracovávat v nástrojích typu SIEM nebo Log Management třetích stran.

Vytváření logů je ve výchozím stavu povoleno. Lze jej ovlivnit:

- IaaS
  - Skupinovou politikou, konfigurací systému
  - Desired State Managementem
- PaaS (Cloudová služba)
  - Startovacím kódem při nasazení služby

Pro sběr logů pro PaaS a IaaS slouží:

- Azure Diagnostics
  - Sběr logů z cloudové služby, webové role nebo z virtuálního stroje do Azure storage zákazníka
  - Pro Azure virtuální stroje i Cloudové služby i další Azure zdroje (například loadbalancer, síťová bezpečnostní skupina a podobně)
  - Podpora různých typů formátu logů (Windows event. Log, Windows event. Tracing, IIS logy
  - Data jsou při přenosu šifrována (HTTPS)
- Windows Event Forwarding
  - Sběr logů na centrálním serveru
  - Pro Azure virtuální stroje zařazené do domény
  - Podpora Windows event logů

Azure SQL Database

Azure SQL databaze auditing sleduje databázové události a zapisuje auditované události do auditního logu, který se nachází v Azure Storage. SQL database auditing umožňuje:

- Konfigurovat kategorie událostí, které mají být auditovány. K dispozici jsou následující kategorie:
  - Access to data
  - Schema changes (DDL)
  - Data changes (DML)
  - Accounts, roles, and permissions (DCL)
  - Stored Procedure, Login
  - Transaction Management
- Vytvářet reporty databázové aktivity

- Analyzovat reporty, podezřelé události, neobvyklé aktivity a trendy
  - K prohlížení logů lze použít nástroj Azure Storage Explorer
  - Předkonfigurované reporty jsou k dispozici ve formě Excelových sešitů
- Zasílat aletry o výskytu neobvyklé databázové aktivity

Azure Active Directory

Azure AD obsahuje auditní reporty, viz [16], které umožňují auditovat použití privilegovaných účtů a výskyt privilegovaných aktivit v Azure AD, viz [17]. Privilegované aktivity zahrnují vytváření rolí, mazání hesel, změnu politik nebo změnu konfigurace adresářové služby. Auditní události jsou uchovávány po 180 dní. Reporting API může být využito pro stažení auditních událostí z Azure AD do odděleného datového úložiště a poté mohou být zpracovávány dalšími bezpečnostními nástroji.

Každá auditovaná událost obsahuje:

- Datum a čas výskytu události
- Actor – identita, která událost způsobila
- Akce – provedená činnost
- Target – objekt, na kterém byla činnost provedena

Seznam auditovaných událostí je následující:

- Uživatelské události
  - Přidání uživatele
  - Odstranění uživatele
  - Nastavení vlastností licencí
  - Reset hesla
  - Změna hesla
  - Aktualizace uživatele (změna atributů objektu uživatele)
  - Vynucení změny hesla
- Události skupin
  - Přidání skupiny
  - Odstranění skupiny
  - Aktualizace skupiny
  - Přidání člena do skupiny
  - Odebrání člena ze skupiny
- Aplikační události
  - Přidání servisního účtu
  - Odstranění servisního účtu
  - Přidání oprávnění servisnímu účtu
  - Odebrání oprávnění servisnímu účtu
  - Přidání delegace
  - Nastavení delegace
  - Odebrání delegace

- Události rolí
  - Přidání člena do role
  - Odstranění člena z role
  - Nastavení preferencí kontaktu na firemní úrovni
- Události B2B
  - Nahrání pozvánky
  - Zprocesování pozvánky
  - Pozvání externího uživatele
  - Uplatnění externí pozvánky uživatelem
  - Přidání externího uživatele do skupiny
  - Přiřazení přístupu externího uživatele k aplikaci
  - Vytvoření tenantu na základě uplatnění pozvánky
  - Vytvoření uživatele na základě uplatnění pozvánky
- Události adresáře
  - Přidání partnera do adresáře
  - Odstranění partnera z adresáře
  - Přidání domény
  - Odstranění domény
  - Aktualizace domény
  - Nastavení autentizace na doméně
  - Nastavení federace na doméně
  - Ověření domény
  - Ověření domény mailem
  - Nastavení flagu DirSyncEnabled
  - Nastavení politiky hesel
  - Nastavení informací společnosti

Azure AD reporty, viz [16] umožňují auditovat spektrum událostí souvisejících s přihlašováním uživatelů a s jejich správou. Office 365 využívá Azure AD jako adresářovou databázi. Azure AD obsahuje následující reporty:

- Neobvyklá aktivita
  - sign ins from unknown sources
  - sign ins after multiple failures
  - sign ins from ip addresses with suspicious aktivity
  - sign ins from possibly infected devices
  - irregular sign in aktivity
  - users with anomalous sign in aktivity
  - users with leaked credentials
  - users with threatened credentials

- Záznam činností
  - Audit report
  - Password reset aktivity
  - Password reset registration aktivity
  - Self service groups aktivity
  - Office365 group name changes
- Integrované aplikace
  - Application usage
  - Account provisioning aktivity
  - Password rollover status
  - Account provisioning errors
- Externí přístup
  - Invitation summary

Office 365

Office 365 auditing umožňuje sledovat činnost a auditovat změny na úrovni Office 365 pomocí reportů (service usage reports, viz [13]) a compliance reportů (dostupné v compliance centru Office 365). Jsou k dispozici Compliance reporty, které využívají auditní logování. Toto logování musí být nejprve administrátorem Office 365 povoleno. Auditní informace jsou uchovávány v Office 365 po dobu 90 dnů. Informace o událostech lze získávat pomocí reportů, exportu reportů a pomocí powershellu.

Auditní reporty jsou rozděleny do kategorií:

- Office 365 audit log report
- Azure AD reports
- Exchange audit report
- Data loss prevention
  - Shody se zásadami a pravidly ochrany před únikem informací
  - Falešně pozitivní výsledky a přepsání zásad ochrany před únikem informací

Reporty (service usage reporty) jsou rozděleny do kategorií:

- Mail
  - Active and inactive mailboxes
  - New and deleted mailboxes
  - New and deleted groups
  - Mailbox usage
  - Types of mailbox connections
- Použití
  - Browser used
  - Operating systém used
  - Licensing vs Active Usage

- Skype pro Firmy
  - Active users
  - Peer-to-peer sessions
  - Conferences
  - Audio minutes and video minutes
  - Client devices
  - Client devices per user
  - User activities
  - PSTN usage
  - Users blocked
- SharePoint
  - Tenant storage metrics
  - Team sites deployed
  - Team site storage
- OneDrive pro Firmy
  - OneDrive for Business sites deployed
  - OneDrive for Business storage
- Auditing
  - Mailbox access by no-owners
  - Role group changes
  - Mailbox content search and hold
  - Mailbox litigation holds
  - Azure AD reports
- Ochrana
  - Top senders and recipients
  - Top malware for mail
  - Malware detection
  - Spam detection
  - Sent and received mail
- Pravidla
  - Top rule matches for mail
  - Rule matches for mail
- DLP
  - Top DLP policy maches for mail
  - Top DLP rules matches for mail
  - DLP policy matches by severity for mail
  - DLP policy matches, overrides and false positive for mail

Office 365 Management Activity API je RESTful API, které poskytuje bezprecedentní úroveň přístupu ke všem záznamům o uživatelských a administrátorských aktivitách uvnitř Office 365, viz [24] a [34]. Výhody management API zahrnují:

- Přístup k více než 150 typům transakcí
- Aktivity logy z SharePoint Online, Exchange Online and Azure Active Directory a dalších Office 365 služeb
- Konzistentní schema napříč všemi logy
- Jednoduché zapnutí a vypnutí a aktivity logů

Prohledávání logů je umožněno pomocí nástroje Audit Log Search který pomocí grafického rozhraní nebo powershellu umožňuje prohledávat unifikované auditní logy, které obsahují informace o:

- Uživatelské činnosti v SharePoint Online a OneDrive for Business
- Uživatelské činnosti v Exchange Online
- Činnosti administrátorů v Sharepoint Online
- Činnosti administrátorů v Exchange Online
- Činnosti administrátorů v Azure AD

Dále jsou k dispozici možnosti auditování na aplikační úrovni jednotlivých komponent Office 365, viz [18]. Rozsah i auditované události jsou dokumentovány v dokumentu, viz [19]:

- Exchange Online, viz [20]
  - Mailbox auditing
    - Sledování přístupu k mailboxu a dalších aktivit, viz [21]
  - Administrator auditing
  - Non-owner mailbox access
  - Administrator role group
  - In-place eDiscovery & Hold
  - Litigation hold per mailbox
  - Export mailbox audit
  - Admin audit log
  - External admin audit log
    - Aktivita jiných než vlastních administrátorů (například zaměstnanců společnosti Microsoft)
- Pro SharePoint Online a OneDrive for Business jsou jednotlivé typy zaznamenávaných událostí uvedeny v dokumentu, viz [22]. K dispozici jsou následující auditní reporty:
  - Content modification
  - Content type and list modifications
  - Content viewing
  - Deletion
  - Run a custom report
  - Expiration and Disposition

- Policy modifications
- Auditing settings
- Security settings

Synchronizace času

Synchronizace času v prostředí Microsoft Online Services je zajištěna službami cloudové platformy. Synchronizace času probíhá při startu virtuálního serveru nebo cloudové služby. Pomocí změny konfigurace lze nastavit synchronizaci i interval synchronizace s jiným zdrojem přesného času.

10.7 NÁSTROJ PRO DETEKCI KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Požadavky na technická opatření v oblasti nástroje pro detekci kybernetických bezpečnostních událostí jsou uvedeny v §22 Vyhlášky.

10.7.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO DETEKCI KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Vyhláška požaduje přijmout opatření k:

Používání nástroje pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí:

- Ověření komunikace
  - Mezi vnitřní komunikační sítí a vnější sítí
  - Pro KII i v rámci vnitřní komunikační sítě
  - Na úrovni serverů patřících do KII
- Kontrolu komunikace
  - Mezi vnitřní komunikační sítí a vnější sítí
  - Pro KII i v rámci vnitřní komunikační sítě
  - Na úrovni serverů patřících do KII
- V případě potřeby zablokování komunikace
  - Mezi vnitřní komunikační sítí a vnější sítí
  - Pro KII i v rámci vnitřní komunikační sítě
  - Na úrovni serverů patřících do KII

10.7.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO DETEKCI KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Pro naplnění požadavků Zákona a Vyhlášky v oblasti nástroje pro detekci kybernetických bezpečnostních událostí je tedy třeba v souladu s výsledky analýzy rizik přijmout sadu opatření:

- Využívat nástroj pro detekci kybernetických bezpečnostních událostí (výklad pojmu kybernetická bezpečnostní událost viz kapitola 7.1) pro sledování síťové komunikace na relevantních místech sítě za účelem detekce výskytu událostí a zablokování komunikace:
  - Na hranicích mezi vnitřní a vnější sítí
  - V rámci vnitřní sítě
  - Na úrovni serverů
- Zaznamenávat a vyhodnocovat jednotlivé kybernetické bezpečnostní události a předávat detekované události k následnému komplexnějšímu zpracování nástroji pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Nástroj pro detekci kybernetických událostí má vazbu na technické opatření na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

10.7.3 VZORY TECHNICKÝCH OPATŘENÍ PRO DETEKCI KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Technické opatření nástroje pro detekci kybernetických bezpečnostních událostí může být realizováno:

- Návrhem, implementací a provozem nástroje pro detekci kybernetických bezpečnostních událostí – Systémem prevence průniku (IPS), který provádí:
  - Detekci událostí
  - Vyhodnocení událostí
  - Zaznamenání informací o události
  - Poskytování informace o výskytu kybernetické bezpečnostní události – notifikace
  - Předání informací nástroji pro sběr a vyhodnocení kybernetických bezpečnostních událostí, viz kapitola 10.8
  - Spuštění definované aktivity v souvislosti s výskytem kybernetické bezpečnostní události, například
    - Zablokování komunikace mezi vnitřní a vnější sítí
    - Zablokování komunikace v rámci vnitřní sítě
    - Zablokování komunikace k serveru
- Nástroj/senzory jsou umístěny v závislosti na architektuře sítě na
  - Hranicích vnitřní a vnější sítě
  - Na uzlových bodech v rámci vnitřní sítě
  - Na úrovni serverů

Pro zajištění požadavků Zákona a Vyhlášky bude třeba implementovat komplexní IPS systém anebo skupinu specializovaných, spolupracujících IPS systémů po zajištění ochrany na požadovaných místech, jako například:

- Síťový IPS
- IPS pro bezdrátové sítě
- Behaviorální IPS
- Host-based IPS

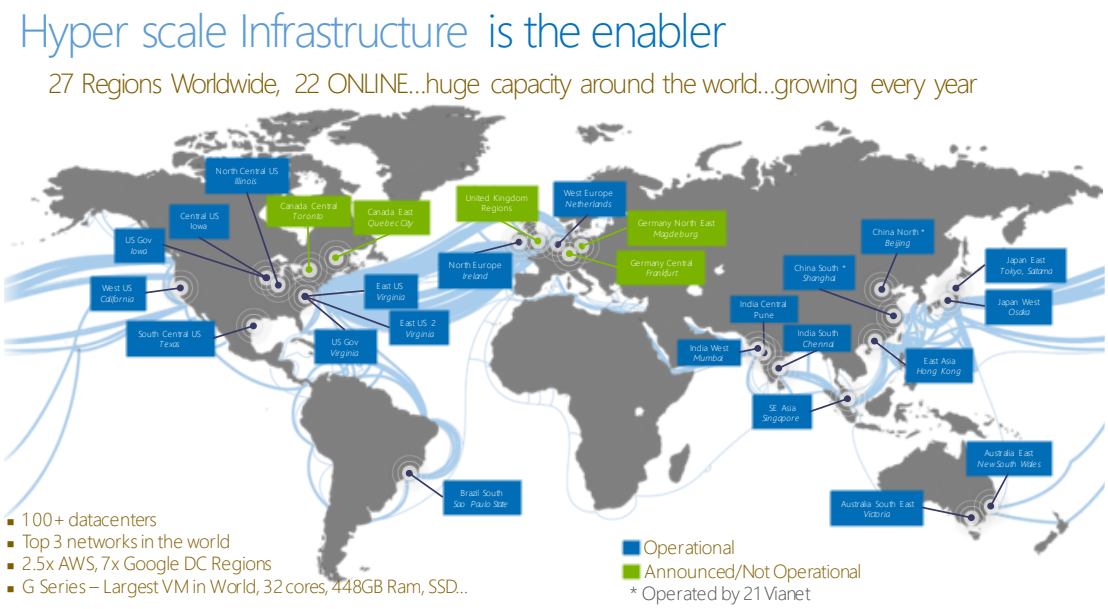
10.7.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast nástroje pro detekci kybernetických bezpečnostních událostí je prostředí Microsoft Online Services realizována následovně:

Microsoft's Cloud Infrastructure and Operations

Společnost Microsoft provozuje rozsáhlou, vysoce propustnou a výkonnou síť, na kterou je velmi obtížné efektivně útočit, viz Obr. 6. V případě lokálního útoku může být komunikace přesměrována jinou cestou bez vlivu na dostupnost a kvalitu poskytovaných služeb, viz [7] a [26].

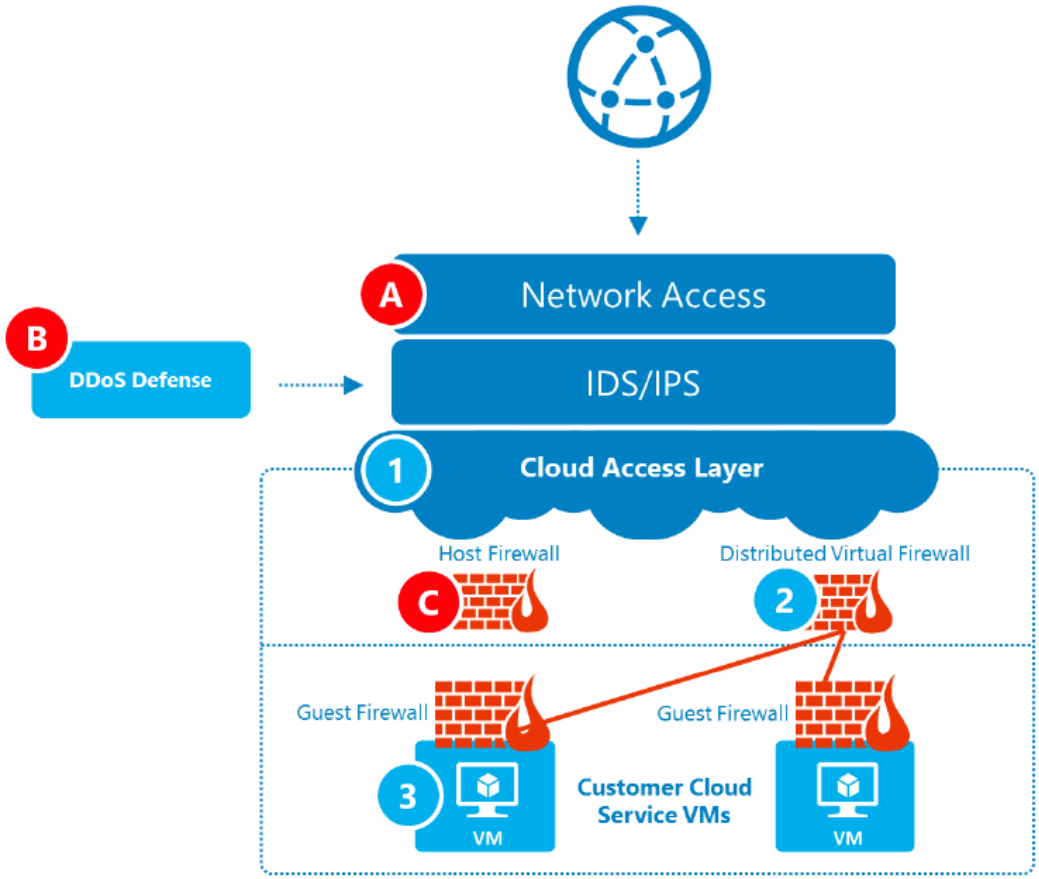
Obr. 6
Schéma datové sítě MCIO



Microsoft Azure

Microsoft Azure poskytuje ochranu na úrovni sítě MCIO a to v několika vrstvách, viz Obr. 7. Součástí ochrany je monitoring sítě a penetrační testování. Ochrana sítě je navržena jak pro ochranu proti vnějším útokům, tak i pro ochranu proti útokům od ostatních zákazníků Azure (ochrana mezi Azure tenanty). MCIO obsahuje distribuovaný DDoS obranný systém, který pomáhá platformu Microsoft Azure chránit. Tento systém používá standardní detekční a obranné mechanismy na úrovni síťového spojení.

Obr. 7
Úrovně ochrany Azure infrastruktury, viz [25]



Office 365

Office 365 využívá MCIO stejně jako Microsoft Azure a proto je pro Office 365 poskytována stejná ochrana na úrovni sítě jako pro Microsoft Azure.

10.8 NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Požadavky na technická opatření v oblasti nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí jsou uvedeny v §23 Vyhlášky.

10.8.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Vyhláška požaduje přijmout opatření k používání nástroje pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí pro KII, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajistí:

- Integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí
- Poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech
- Nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí

V rámci provozu nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí v KII musí být zajištěno:

- Pravidelná aktualizace nastavení pravidel pro vyhodnocování a včasné varování pro omezení nesprávných nebo falešných varování
- Využívání získaných informací pro optimalizaci nastavení bezpečnostních opatření

10.8.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Technické opatření na nástroj pro detekci kybernetických událostí má vazbu na technické opatření na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

Pro naplnění požadavků Zákona a Vyhlášky v oblasti nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
  - Ukládá události pro následnou analýzu
  - Průběžně události vyhodnocuje události a identifikuje bezpečnostní incidenty a kybernetické bezpečnostní události
  - Provádí notifikace o výskytu incidentu

Vlastní nasazení nástroje pro sběr a vyhodnocení kybernetických událostí je třeba pro jeho správnou funkci pravidelně aktualizovat a nastavení jeho konfiguraci upravovat pro správné a vyhodnocování událostí.

Získané informace je třeba využít nejen pro aktualizaci nastavení nástroje, ale také je promítnout jako opatření s cílem kontinuálního zlepšování zabezpečení informačního systému a jeho jednotlivých částí.

10.8.3 VZORY TECHNICKÝCH OPATŘENÍ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Technické opatření nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí může být realizováno:

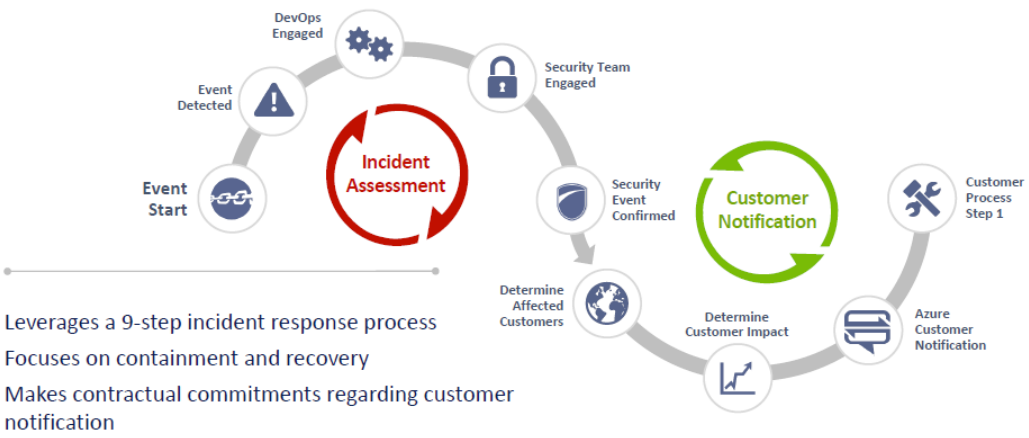
- Návrhem, implementací a provozem nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí – Security Information and Event Management Systému (SIEM), který provádí:
  - Agregaci událostí
  - Korelaci událostí
  - Poskytování informace o výskytu kybernetické bezpečnostní události ve formě:
    - Notifikací
    - Reportů
  - Ukládání událostí pro následnou analýzu
- Architektura a dimenzování nástroje SIEM musí odpovídat počtu událostí generovaných informačním systémem

10.8.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí je prostředí Microsoft Online Services realizována následovně:

Provozní události a logy Office 365, Microsoft Azure a platformy, na které jsou tyto služby provozovány jsou zpracovávány, analyzovány a vyhodnocovány bezpečnostně analytickým systémem COSMOS, viz [24], který využívá technologie Azure Machine Learning.

Výstupem zpracování jsou reporty a notifikace, které slouží k zjištění možné podezřelé aktivity v produkčním prostředí. Odhalené zranitelnosti jsou následně v souladu s interní politikou řešeny, viz Obr. 8.



Obr. 8
Životní cyklus reakce na bezpečnostní incident, viz [27]

Microsoft Azure

Microsoft Azure obsahuje bezpečnostní centrum (Azure Security Center, viz [28]), což je služba, která zákazníkům umožňuje efektivní prevenci, detekci a obranu proti hrozbám pomocí:

- Prevence
  - Monitorování bezpečnostního stavu
  - Definování politik na úrovni Azure předplatného
  - Bezpečnostní doporučení a návody
  - Nasazení bezpečnostních služeb
- Detekce
  - Sběr a analýza bezpečnostních logů
  - Využívání znalostí společnosti Microsoft a centra reakce na incidenty o hrozbách, službách a produktech
  - Využívání pokročilých analytických nástrojů včetně Machine Learning a analýzy chování
- Reakce
  - Poskytování alertů o bezpečnostních incidentech včetně priority
  - Informace o zdroji útoku a o dotčených komponentách
  - Návrh způsobů, jak zastavit současný útok a pomoc při předcházení budoucím útokům

Pro analýzu logů ze služby Azure Diagnostics, viz kapitola 10.6.4, která ukládá logy do Azure storage accountu zákazníka, mohou zákazníci Microsoft Azure využít svůj interní SIEM systém, do kterého si mohou logy importovat.

Office 365

Provozní stav a charakteristiky jednotlivých služeb Office 365 včetně platformy, na které jsou tyto služby provozovány, viz [24] je monitorován. Při provozu služeb jsou generovány logy událostí a auditní logy. Tyto logy jsou zašifrovaným kanálem přenášeny ke zpracování a následně zpracovávány (agregace a analýza) a vyhodnocovány interní službou na zpracování big dat – bezpečnostně analytický systém COSMOS. Před vlastním zpracováním dat dochází k jejich anonymizaci.

Office 365 Management Activity API, viz kapitola 10.6.4 je možné využít pro napojení systému SIEM, který může být provozován on-premise nebo v cloudu. Partneři společnosti Microsoft nabízejí hotová řešení pro sběr a vyhodnoceni kybernetických událostí, která využívají tohoto API.

10.9 APLIKAČNÍ BEZPEČNOST

Požadavky na technická opatření v oblasti aplikační bezpečnosti jsou uvedeny v §24 Vyhlášky.

10.9.1 IDENTIFIKACE POŽADAVKŮ NA APLIKAČNÍ BEZPEČNOST

Vyhláška požaduje přijmout následující opatření k aplikační bezpečnosti:

- Provádění bezpečnostních testů zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů
- V rámci aplikační bezpečnosti zajištění trvalé ochrany KII
  - Aplikací a informací dostupných z vnější sítě před:
    - Neoprávněnou činností
    - Popřením provedených činností
    - Kompromitací
    - Neautorizovanou změnou
  - Transakcí před:
    - Nedokončením
    - Nesprávným směrováním
    - Neautorizovanou změnou předávaného datového obsahu
    - Kompromitací
    - Neautorizovaným duplikováním nebo opakováním

10.9.2 ANALÝZA POŽADAVKŮ NA APLIKAČNÍ BEZPEČNOST

Pro naplnění požadavků Zákon a Vyhlášky v oblasti aplikační bezpečnosti je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Architektura informačního systému musí umožnit aplikovat bezpečnostní principy a nejlepší praktiky na jednotlivých úrovních systému. Informační systém musí být již od počátku navrhován s ohledem na dosažení požadované bezpečnostní úrovně.
- Vývoj informačního systému musí být prováděn s ohledem na definované bezpečnostní cíle. V rámci vývojových cyklů musí být prováděno ověření splnění těchto bezpečnostních cílů a to před jejich nasazením do produkčního prostředí.
- Informační systém musí obsahovat :
  - Prvky ochrany informací, viz kapitola 10.9.1. Ochrana integrity informací musí odpovídat stupni hodnocení aktiv, viz příloha č.1 Vyhlášky.

10.9.3 VZORY TECHNICKÝCH OPATŘENÍ PRO APLIKAČNÍ BEZPEČNOST

Technická opatření v oblasti aplikační bezpečnosti mohou být realizována:

- V rámci vývojového cyklu aplikace musí být prováděno penetrační testování s následným odstraněním detekovaných zranitelností a to minimálně před uvedením do provozu a po každé zásadní změně
- Aplikace dostupné z vnější sítě musí být chráněny:
  - Pomocí autentizace při přístupu a autorizace k provádění činností
  - Pomocí auditování aktivity uživatelů a správců aby bylo prokazatelné, kdo vykonal činnost
  - Pomocí zašifrování síťového spojení
- Požadavky na ochranu transakcí musí být vypořádány na úrovni kódu aplikace

10.9.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast aplikační bezpečnosti je v prostředí Microsoft Online Services realizována následovně:

Vývoj software

Společnost Microsoft řídí veškerý vývoj software prostřednictvím procesu Bezpečný vývojový životní cyklus (Security Development Lifecycle), který je navržen tak, aby pomáhal snižovat závažnost i počet zranitelností kódu při neustále se měnících požadavcích. Těmito pravidly se řídí nejen vývoj aplikací, ale také vývoj cloudového operačního systému, který pro svůj provoz využívá cloudová infrastruktura.

V rámci vývoje dochází k testování software v oblastech:

- Dynamická analýza
  - Ověření funkčnosti a monitorování chování aplikace
    - Porušení paměti
    - Použití privilegií
    - Kontrola kritických bezpečnostních aspektů
- Fuzzy testování
  - Vyvolání selhání záměrným použitím poškozených nebo náhodných dat
- Posouzení plochy útoky
  - Posouzení plochy útoku a modelu hrozeb po dokončení kódu
  - Přezkoumání nových vektorů útoků (v reakci na provedené změny) a jejich minimalizace

Office 365 a Microsoft Azure

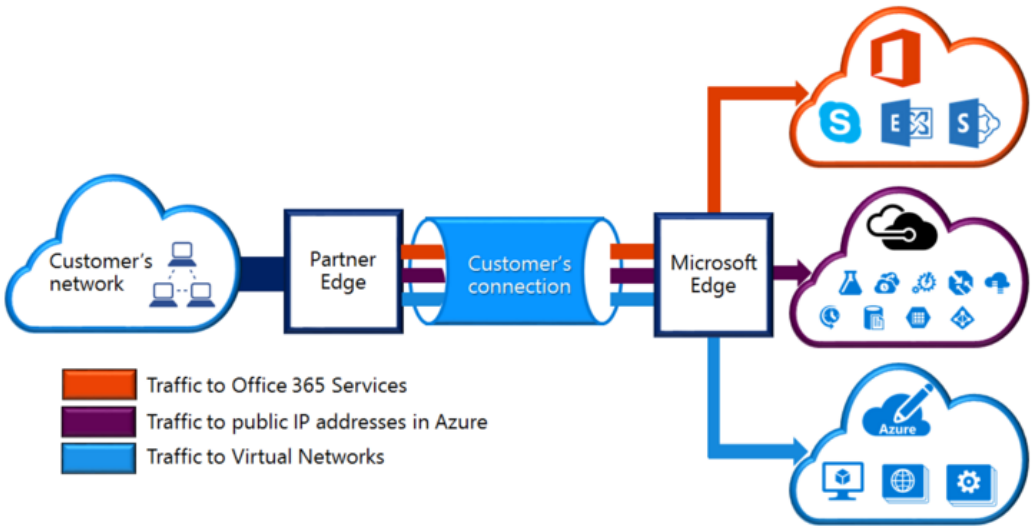
Průběžné zvyšování bezpečnostní konfigurace prostředí je zajišťováno konceptem Red Team & Blue Team (červený tým útočí a modrý tým útoku brání), viz [27], jedná se o pokročilou formu penetračního testování.

Ochrana aplikací a informací v prostředí Microsoft Online Services je zajištěna následovně:

- Autentizace administrátorů k Microsoft Azure a Office 365 je zajištěna pomocí Azure AD, viz kapitola 10.3.4
- Autentizace uživatelů k Office 365 je zajištěna pomocí Azure AD samostatně anebo federací s jinou autoritativní adresářovou službou, viz kapitola 10.3.4 a dokument [9].

- Autentizace k Office 365 a Microsoft Azure může být více faktorová. Toto nastavení lze vynutit na úrovni jednotlivých uživatelů, viz kapitola 10.3.4
- Řízení přístupu je zajištěno pomocí řízení přístupu pomocí rolí (RBAC), viz kapitola 10.4.4
- Audit přístupu k informacím včetně zaznamenávání typu provedené operace je realizováno pomocí auditních logů, diagnostického logování a sad reportů, viz kapitola 10.6.4 a pomocí Azure Security Centra, viz kapitola 10.8.4
- Ochrana informací při přenosu vnějšímu sítěmi je zajištěna
  - Pomocí protokolu HTTPS s využitím protokolu TLS 1.2.
  - Pomocí Site-to-Site VPN, která využívá protokol IPSec, konfigurační parametry, včetně algoritmů jsou uvedeny v dokumentu [29]
  - Pomocí pronajatého okruhu mezi interní sítí a datovým centrem Microsoft – Express Route, viz Obr. 9, který neprochází přes Internet a umožňuje dynamické směrování IP komunikace. Bezpečnost spojení mezi rozhraním Microsoft Edge a interní sítí zákazníka záleží na způsobu zabezpečení poskytovatele Express Route, viz [30]. Protože Express Route neposkytuje šifrované spojení, je třeba ho doplnit o Site-to-Site VPN, která zajistí zašifrování dat na síťové vrstvě.
- Ochrana integrity elektronickým podpisem je k dispozici pro
  - Veškeré dokumenty vytvořené v Microsoft Office. Tyto dokumenty lze podepisovat klientským certifikátem na klientské zařízení, privátní klíč klientské zařízení neopouští. Tato funkcionalita je vestavěná do Microsoft Office
  - Podepisování elektronické pošty. Elektronickou poštu lze podepisovat klientským certifikátem na klientském zařízení, privátní klíč klientské zařízení neopouští. Tato funkcionalita je vestavěná do Microsoft Outlook a dalšího klientského software spolupracujícího s poštovním serverem Exchange
  - Jakékoliv dokumenty a elektronickou poštu prostřednictvím Azure Rights Management, viz [31].

Obr. 9
ExpressRoute, viz [30]



10.10 KRYPTOGRAFICKÉ PROSTŘEDKY

Požadavky na technická opatření v oblasti kryptografických prostředků jsou uvedeny v §25 Vyhlášky.

10.10.1 IDENTIFIKACE POŽADAVKŮ NA KRYPTOGRAFICKÉ PROSTŘEDKY

Vyhláška požaduje přijmout opatření k používání kryptografických prostředků:

- Používání kryptografické ochrany
  - Stanovení úrovně ochrany
    - Typ algoritmu
    - Síla algoritmu
  - Pravidla ochrany pro
    - Přenos po komunikačních sítích
    - Při uložení na mobilním zařízení
    - Při uložení na vyměnitelné nosiče dat
- V souladu s bezpečnostními potřebami a výsledky hodnocení rizik stanovit použití kryptografických prostředků pro zajištění
  - Ochrany důvěrnosti předávaných nebo ukládaných dat
  - Ochrany integrity předávaných nebo ukládaných dat
  - Průkazné identifikace provedené činnosti
- Stanovení prostředků správy klíčů pro KII v oblastech
  - Generování klíčů
  - Distribuci klíčů
  - Ukládání klíčů
  - Archivaci klíčů
  - Změny klíčů
  - Ničení klíčů
  - Kontrolu klíčů
  - Audit klíčů
- Použití odolných kryptografických algoritmů a kryptografických klíčů pro KII
  - V případě nesouladu s přílohou č. 3 Vyhlášky řízení rizik spojených s tímto nesouladem

10.10.2 ANALÝZA POŽADAVKŮ NA KRYPTOGRAFICKÉ PROSTŘEDKY

Pro naplnění požadavků Zákona a Vyhlášky v oblasti kryptografických prostředků je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Definovat povolené algoritmy a protokoly pro případy, kdy je požadováno použití kryptografických prostředků. V případě KII tyto algoritmy a protokoly musí být v souladu s přílohou č. 3 Vyhlášky nebo v případě nesouladu musí být řízena rizika s tímto spojená
- Stanovit pravidla a procesy správy klíčů
  - Zajištění ochrany klíčů
  - Zajištění bezpečnosti pro operace s klíči, viz kapitola 10.10.1

Vlastí požadavky na způsob použití kryptografických prostředků je definován v jiných částech Zákona a Vyhlášky a tím i této studie, například se jedná o kapitoly 10.2, 10.3 a 11.

10.10.3 VZORY TECHNICKÝCH OPATŘENÍ PRO KRYPTOGRAFICKÉ PROSTŘEDKY

Technická opatření v oblasti kryptografických prostředků mohou být realizována pomocí:

- Definování povolených algoritmů
  - Použitý algoritmus odpovídá příloze č. 3 Vyhlášky
  - Požadovaná délka klíče odpovídá příloze č. 3 Vyhlášky
- Definování povolených protokolů
- Definování požadavků na HW kryptografické prostředky
  - HSM
  - Čipové karty
  - Kryptografické tokeny
- Definování postupů správy klíčů a certifikátů pro
  - Servery a další zařízení
  - Uživatele

Vlastní vzory technických opatření pro implementaci kryptografických prostředků jsou uvedeny kapitolách 10.2.3, 10.3.3 a 11.

10.10.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblasct kryptografických prostředků je prostředí Microsoft Online Services realizována následovně:

Aplikační protokoly

Aplikační protokoly používané pro přístup ke službám v rámci Microsoft Azure (například HTTP, POP3, IMAP, SMTP, SSTP) jsou zašifrovány pomocí TLS:

- Používány jsou pouze protokoly TLS 1.0, 1.1 a 1.2.
- Preferovány jsou kombinace kryptografických algoritmů využívající výměnu klíčů pomocí algoritmu Diffie-Hellman založený na eliptických křivkách (ECDHE) s délkou klíčů 384 (preferovaná) nebo 256 bitů. Z důvodů kompatibility se staršími klienty jsou povoleny kombinace algoritmů využívající pro výměnu klíčů asymetrický algoritmus RSA.
- Pro asymetrickou kryptografii je použit algoritmus RSA.

- Pro symetrickou kryptografii je použit algoritmus AES s délkou klíčů 256 (preferovaný) a 128 bitů v módu CBC. Z důvodu kompatibility se staršími klienty je použit i algoritmus 3DES s délkou klíče 168 bitů a RC4 s délkou klíče 128 bitů s nejnižší prioritou.
- Poporovány jsou hash funkce SHA-384 (preferovaný s AES-256), SHA-256 (preferovaný s AES-128) a SHA-1. Podpora pro SHA-1 by měla být ukončena k 1.1.2017 (viz [37]). Z důvodu kompatibility se staršími klienty je povolena i hash funkce MD5 společně s šifrovacím algoritmem RC4 s nejnižší prioritou.
- Certifikáty používané pro služby Microsoft Azure využívají asymetrický algoritmus RSA s délkou klíčů 2048 bitů a hash funkci SHA-256. Certifikáty obsahují odkazy na revokační informace CRL a OCSP. Použité certifikační autority mají stejné nebo vyšší parametry s výjimkou kořenové certifikační autority, která využívá hash funkci SHA-1 (což u kořenových certifikačních autorit nevadí – hash certifikátu není využíván pro jeho validaci).

Azure VPN Gateway

Služba Azure VPN Gateway zajišťuje VPN připojení externích uživatelů nebo sítí do prostředí Microsoft Azure a komunikaci mezi datovými centry Microsoft Azure (viz [85]):

- **Point-to-Point VPN:** používá protokol SSTP založený na TLS – paramatery viz předcházející odstavec o **šifrování komunikace Microsoft Azure**. Služba umožňuje využívat pro klienty certifikáty vydané v PKI zákazníka (max. 20 kořenových certifikačních autorit).
- **Site-to-Site VPN:** používá protokol IPsec s následujícími parametry: IKEv1 (Static Routing) nebo IKEv2 (Dynamic Routing), Diffie-Hellman 1024 bitů, Pre-Shared Key, AES 128 256 bitů 3DES, SHA1 MD5 a na straně zákazníka podporuje široké množství zařízení (viz [86]).
- **VNet-to-VNet VPN:** propojení dvou virtuálních sítí v rámci datových center Microsoft Azure využívá stejné algoritmy jako **Site-to-Site VPN**.

Azure Express Route

Pevný okruh mezi sítí zákazníka a datovým centrem Microsoft Azure dodávaný třetí stranou (v ČR se jedno o T-Mobile) s přenosovou rychlostí až 10 Gbps, který není šifrován. V případě, že je použita Azure Express Route a je nutné šifrovat komunikaci vlastními silami – na straně Microsoft Azure je možné použít VPN koncentrátory třetích stran – viz kapitola 10.2.4.

Azure Storage

Veškerá data (image virtuálních serverů, bloky dat, soubory, databáze a podobně) jsou uložena v Azure Storage, která využívá technologii BitLocker Drive Encryption (viz 11.1.13) pro šifrování celých disků:

- BitLocker Drive Encryption využívá kryptografický algoritmus AES se 128 nebo 256 bitovými klíči. Nové servery využívají pouze klíče s délkou 256 bitů, starší servery, které jsou postupně vyřazovány, mohou využívat klíče s délkou 128 bitů.
- BitLocker Drive Encryption využívá dvě kategorie klíčů:
  - BitLocker Managed klíče, které jsou přiřazeny instalaci operačního systému serveru nebo šifrovanému disku. Tyto klíče jsou smazány a resetovány během reinstalace serveru nebo formátování disku.
  - BitLocker Recovery klíče, které jsou spravovány mimo BitLocker, ale jsou určeny pro šifrování disků. Tyto klíče jsou využity v případě, že je přeinstalován operační systém serveru, který obsahuje zašifrované disky. Dále jsou využívány službou Exchange Online Managed Availability Diagnostic v případě, kdy je nutné odemknout diskový svazek.

- Kryptografické algoritmy použité v BitLocker Drive Encryption byly validovány podle FIPS 140-2 (viz [6]) v rozsahu:
  - Cryptographic Module Specification
  - Cryptographic Module Ports and Interfaces
  - Finite State Model
  - Operational Environment
  - Design Assurance
  - Mitigation of Other Attacks
  - Self-Tests

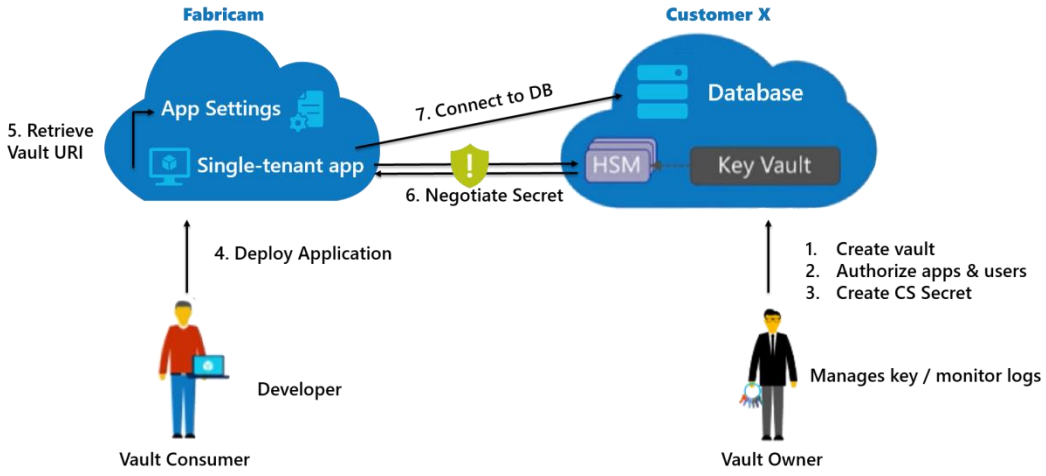
Azure Key Vault

Azure Key Vault je služba řešící problematiku bezpečného uložení symetrických i asymetrických klíčů pro cloudové služby provozované v rámci Microsoft Azure a Office 365:

- Azure Key Vault rozeznává dvě role:
  - **Azure Key Vault Owner:** vlastník klíčů, který vytváří úložiště klíčů, spravuje klíče a řídí přístupová oprávnění ke klíčům.
  - **Azure Key Vault Consumer:** uživatel klíčů který může provádět kryptografické operace s asymetrickými klíči a získat symetrické klíče v závislosti na přístupových oprávněních nastavených v Azure Key Vault.

Tyto dvě role umožňují oddělit správu/vlastnictví klíčů od jejich použití a umožňují zvýšit bezpečnost klíčů podle následujícího scénáře:

Obr. 10
Scénář využití Azure Key Vault

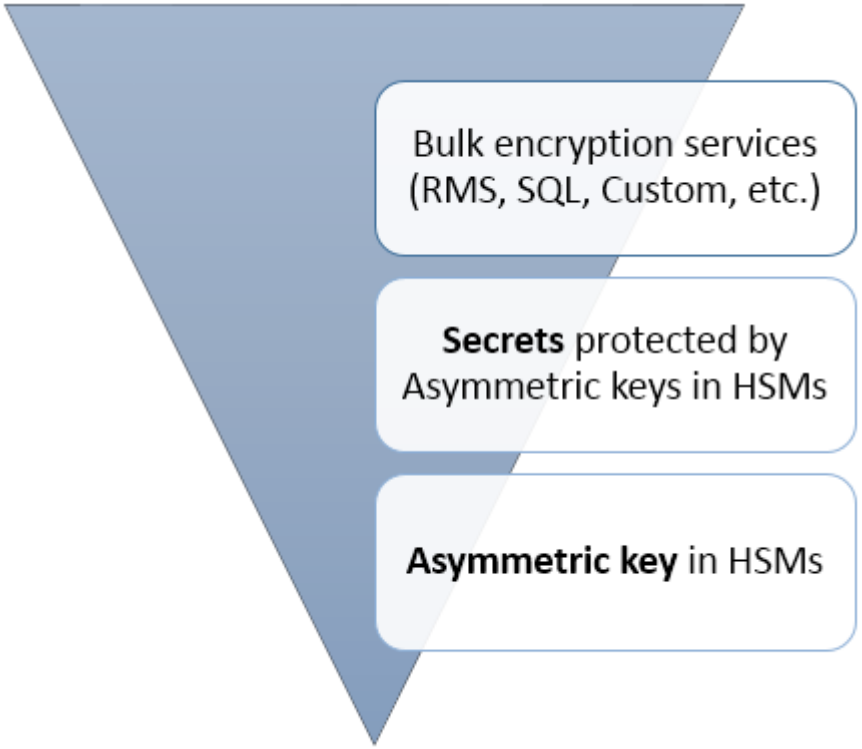


- V Azure Key Vault mohou být uloženy dva typy klíčů:
  - **Keys** asymetrické klíče pro algoritmus RSA s délkou 2048 bitů, které mohou být uloženy dvěma různými způsoby:
    - **HSM Protected Keys:** klíče jsou uloženy v hardwarovém Thales nShield HSM, který splňuje požadavky FIPS 140-2 Level 2 (viz [58]), a neumožňuje export soukromého klíče, pouze provést s ním operace.
    - **Software Protected Keys**: klíče jsou uloženy ve virtuálních serverech služby Azure Key Vault a jsou chráněny asymetrickými klíči uloženými v HSM. Tato varianta je levnější než HSM Protected Keys a je určena pro vývojové a testovací prostředí.

- **Secret**: bloky dat (BLOB) o velikosti maximálně 10 kB – obvykle symetrické šifrovací klíče, ale může jít i o jiné typy citlivých dat, například hesla nebo API tokeny – které, jsou uloženy ve virtuálních serverech služby Azure Key Vault a jsou chráněny asymetrickými klíči uloženými v HSM.

  Je třeba mít na zřeteli, že u tohoto typu klíčů získává role Azure Key Vault Consumer hodnotu klíče a musí být řešena jeho bezpečnost při využití v aplikaci (uložení v RAM, persistentní uložení v aplikaci a podobně).

Obr. 11
Typy klíčů v Microsoft Azure [57]

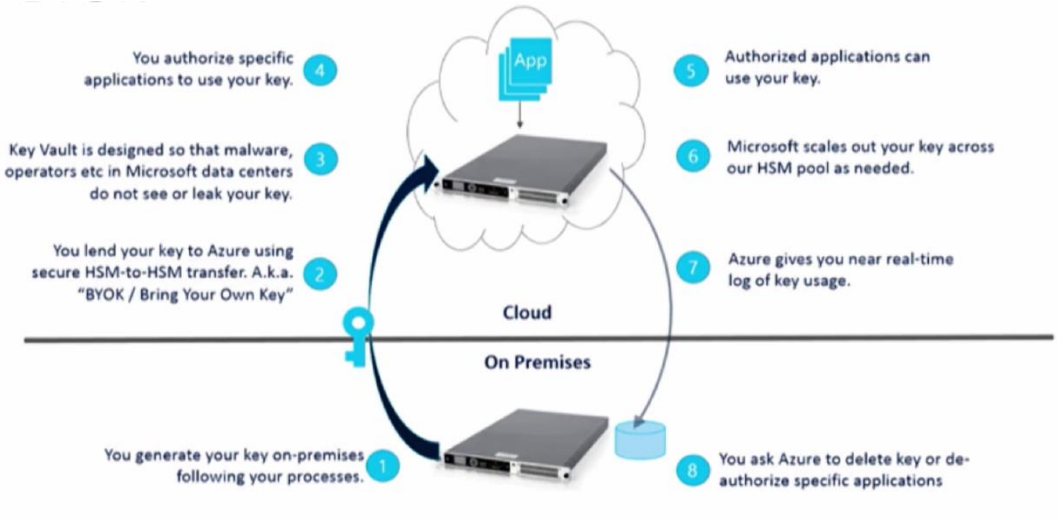


Azure Key Vault + BYOK

Využití Thales nShield HSM pro Azure Key Vault umožňuje realizovat scénář Bring your own Key (BYOK):

- Správce klíčů vygeneruje ve svém on-premise Thales nShield HSM pár klíčů pro RSA s délkou 2048 bitů.
- Správce klíčů pomocí Azure Key Vault BYOK Toolset exportuje soukromý klíč zašifrovaný pomocí veřejného klíče Microsoft Key Exchange Key do souboru. Soukromý klíč Microsoft Key Exchange Key je uložen v Azure Key Vault Thales nShield HSM.
- Správce klíčů nahraje soubor se zašifrovaným soukromým klíčem do Azure Key Vault. Zde je soubor nahrán do Thales nShield HSM a dešifrován soukromým klíčem Microsoft Key Exchange Key.

Obr. 12
Scénář BYOK s Azure Key Vault



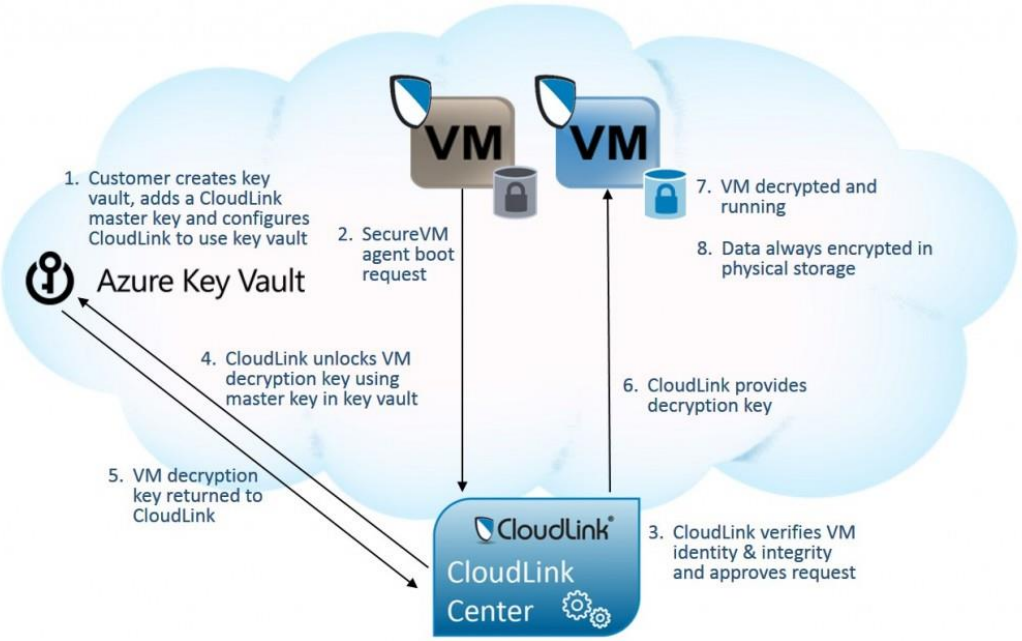
Azure Disk Encryption

Azure Disk Encryption umožňuje šifrování disků ve virtuálních serverech s operačními systémy Windows Server (BitLocker, viz [67]) a CentOS, RHEL, SUSE, SLES a Ubuntu Linux (DM-Crypt, viz [70]) běžících v Azure IaaS včetně bootovacího disku s využitím klíčů uložených v Azure Key Vault (viz [65]). Šifrovací klíče jsou vygenerovány při vytvoření virtuálního serveru a uloženy do Azure Key Vault.

CloudLink VM

Firma CloudLink dodává vlastní řešení šifrování disků virtuálních serverů v Azure IaaS a je schopna využít klíče uložené v Azure Key Vault (viz [66]). Pro šifrování disků virtuálních serverů je použit BitLocker, výhodou řešení firmy CloudLink je bezobslužný start virtuálních serverů bez nutnosti manuálně zadávat heslo pro Azure Key Vault.

Obr. 13
Šifrování disků CloudLink VM, viz [66]



Azure Blob Storage Client

Knihovna pro ukládání bloků dat (BLOB) do Azure Storage podporuje šifrování bloků dat na klientovi s asymetrickými klíči uloženými v Azure Key Vault. Tuto knihovnu je možné využít pro on-premise i pro cloudové aplikace (viz [45]).

Azure SQL Database

Veškerá komunikace s cloudovou službou Azure SQL Database je zašifrována s využitím TLS (viz 10.10.4 – Microsoft Azure – šifrování komunikace a [71]).

Data uložená v Azure SQL Database je možné šifrovat na úrovni databáze pomocí Transparent Data Encryption (TDE, viz [72]) algoritmem AES s 256 bitovými klíči. Symetrický šifrovací klíč použitý pro šifrování databází je chráněn certifikátem SQL serveru, který je unikátní pro každý SQL server a je obnovován jednou za 90 dní. Podrobnosti viz kapitola 11.1.25. Pokud je pro databázi zapnuto šifrování pomocí TDE, pak jsou automaticky šifrovány i transakční logy a zálohy vytvářené v rámci služby Azure SQL Database.

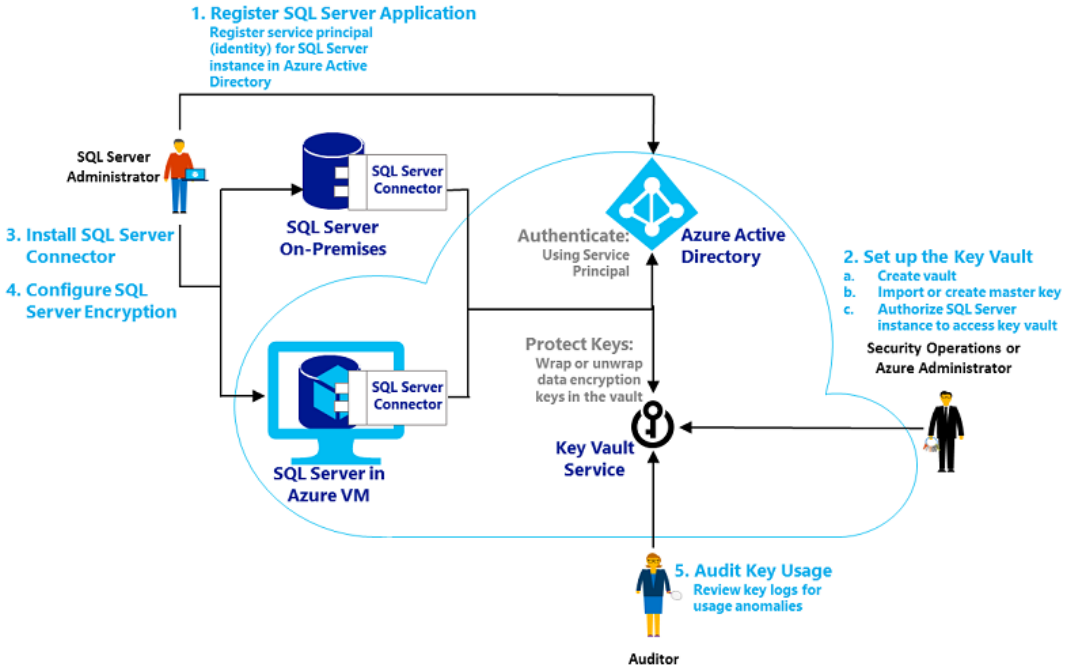
Azure SQL Database neumožňuje využít Azure Key Vault pro ochranu symetrického klíče pomocí certifikátu a privátního klíče uložených v Azure Key Vault.

Azure Key Vault je možné využít pro šifrování jednotlivých sloupců tabulek v Azure SQL Database (viz kapitola 11.1.24 a [61]) pomocí knihovny Enhanced ADO.NET. Šifrovací klíče jsou v tomto případě využívány na straně klientské aplikace a SQL server je nemá k dispozici.

Microsoft SQL Server

Microsoft SQL Server provozovaný on-premise nebo jako Azure VM umožňuje využít Azure Key Vault pro ochranu symetrického klíče pro šifrování databáze (Transparent Database Encryption, TDE, viz kapitola 11.1.25 a [62]) pomocí certifikátu a privátního klíče uloženého v Azure Key Vault. Symetrické šifrovací klíče určené pro šifrování transakčních logů a záloh SQL databáze šifrované pomocí TDE jsou chráněny stejným certifikátem a privátním klíčem uloženým v Azure Key Vault.

Obr. 14
Využití Azure Key Vault v Microsoft SQL Server TDE [62]



Azure Key Vault je možné využít i pro šifrování jednotlivých sloupců tabulek v Microsoft SQL Server provozovaném on-premise nebo jako Azure VM (Always Encrypted, viz kapitola 11.1.24 a [61]) pomocí knihovny Enhanced ADO.NET pro on-premise i cloudové aplikace. Šifrovací klíče jsou v tomto případě využívány na straně klientské aplikace a SQL Server je nemá k dispozici.

Azure RMS

Azure RMS je služba pro kryptografickou ochranu dokumentů a mailů (viz kapitola 11.1.7) může využívat asymetrické klíče v Azure Key Vault včetně BYOK.

Azure Backup

Azure Backup ukládá komprimované a šifrované zálohy jako bloková data (BLOB) do Azure Storage. Šifrování záloh pomocí algoritmu AES s 256 bitovými klíči probíhá na zálohovaném počítači. V případě že je Azure Backup použit pro zálohování on-premise prostředí je správa šifrovacího klíče plně ve správě zákazníka. Pokud je Azure Backup použit pro zálohování virtuálních serverů v rámci Azure IaaS je šifrovací klíč uložen ve virtuálním serveru.

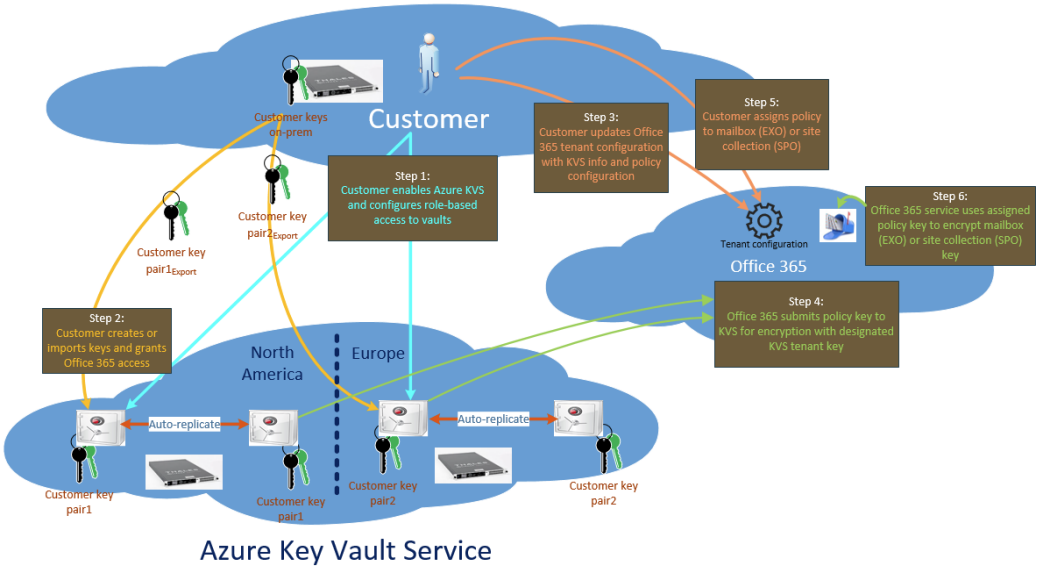
Office 365

Pro ochranu data uložených v Office 365 jsou využity následující kryptografické prostředky pro šifrování uživatelských dat (viz [5]):

- Šifrování uložených dat na úrovni diskových svazků (Volume-level Encryption) ve službách ve službách Exchange Online, SharePoint Online (včetně OneDrive for Business) a Skype for Business:
  - Office 365 využívá technologii Microsoft BitLocker pro šifrování všech zákaznických dat uložených na úrovni diskových svazků pro eliminaci hrozeb souvisejících se ztrátou, krádeží nebo nesprávně vyřazenými fyzickými disky nebo počítači.
  - Microsoft BitLocker využívá kryptografický algoritmus se 128 nebo 256 bitovými klíči. Nové servery využívají pouze klíče s délkou 256 bitů, starší servery mohou využívat i klíče s délkou 128 bitů.
  - Microsoft BitLocker využívá dvě kategorie klíčů:
    - BitLocker Managed klíče, které jsou přiřazeny instalaci operačního systému serveru nebo šifrovanému disku. Tyto klíče jsou smazány a resetovány během reinstalace serveru nebo formátování disku.
    - BitLocker Recovery klíče, které jsou spravovány mimo BitLocker, ale jsou určeny pro šifrování disků. Tyto klíče jsou využity v případě, že je přeinstalován operační systém serveru, který obsahuje zašifrované disky. Dále jsou využívány službou Exchange Online Managed Availability Diagnostic v případě, kdy je nutné odemknout diskový svazek.
  - Klíč použitý pro zašifrování diskového svazku (Full Volume Encryption Key) pomocí BitLockeru je zašifrován pomocí hlavního klíče diskového svazku (Volume Master Key), které jsou uloženy v zabezpečeném sdíleném adresáři a přístupné pouze prověřeným a pověřeným osobám. Hlavní klíče jsou chráněny pomocí Passphrase, které jsou uloženy v Secure Store. Ten při přístupu k uložené Passphrase vyžaduje vysokou úroveň oprávnění a schválení přístupu a přístupy jsou logovány. Schvalování přístupů zajišťuje jiná skupina než ta, která o přístup ke klíči žádá.
  - Kryptografické algoritmy použité v BitLockeru byly validovány podle FIPS 140-2 (viz [6]) v rozsahu:
    - Cryptographic Module Specification
    - Cryptographic Module Ports and Interfaces
    - Finite State Model
    - Operational Environment
    - Design Assurance
    - Mitigation of Other Attacks
    - Self-Tests

- Office 365 Advanced Encryption zahrnuje šifrování na úrovni souborů (File-level Encryption) a zpráv (Message-level Encryption):
  - Office 365 Advanced Encryption umožňuje využít Azure Key Vault pro uložení klíčů, pro:

Obr. 15
Office 365 Advanced Encryption, viz [5]



  - SharePoint Online včetně OneDrive for Business:
    - Všechny soubory v SharePoint Online jsou před uložením do Azure Storage zašifrovány pomocí AES s náhodně generovaným klíčem o délce 256 bitů. Před tím, než si uživatel soubor stáhne ze SharePoint Online je soubor získaný z Azure Storage dešifrován. Na úrovni infrastruktury Microsoft Azure nejsou k dispozici šifrovací klíče k uživatelským souborům služby SharePoint Online.
    - Uložené soubory jsou rozděleny do bloků, každý blok je zašifrován vlastním náhodným klíčem. Bloky jsou náhodně rozděleny mezi více Azure Storage Account.
    - Klíče jednotlivých bloků jsou zašifrovány hlavním klíčem souboru a jsou uloženy v SharePoint Content databázi společně s mapou uložení jednotlivých bloků souboru. Hlavní klíč souboru je uložen v odděleném SharePoint Secret Store a zašifrován pomocí Farm Key a zálohován do centrálního SharePoint Secret Store. Hlavní klíče jsou pravidelně jednou za 60 dní změněny a klíče bloků uložené v SharePoint Content databázi jsou při této příležitosti přešifrovány.
    - Hesla pro použitá pro Azure Storage Account jsou uložena v centrálním SharePoint Secret Store a delegovány do jednotlivých SharePoint farem podle potřeby. Jsou používána oddělená hesla Azure Storage Account pro zápis a pro čtení. Hesla pro Azure Strorage Account jsou pravidelně měněna po 60 dnech.
    - SharePoint Online tak odděluje vlastní soubory (Azure Storage), informace o místě uložení a šifrování souborů (SharePoint Content databáze) a informace potřebných pro získání a dešifrování souborů (Key Storage) do třech nezávislých komponent, které jsou fyzicky oddělené – bez přístupu ke všem třem komponentám není možné získat přístup k obsahu souborů.

- Skype for Business:
  - Uživatelská data ve formě souborů a prezentací, které byly nahrány účastníky konference, zašifruje server Web Conferencing pomocí AES s klíčem 128 bitů. Zašifrované soubory jsou uloženy do sdíleného adresáře. Náhodně generovaný klíč s délkou 128 bitů je uložen v XML souboru obsahující data o konferenci. Tento XML soubor je zašifrován náhodně generovaným hlavním klíčem konference (Conference Master Key).
  - Uživatel si v klientské aplikaci může stáhnout soubory přiložené ke konferenci – stáhne si zašifrovaný soubor pomocí HTTPS a klientská aplikace si od Web Cenferencing serveru vyžádá šifrovací klíč pro jeho dešifrování. Klientská aplikace při přihlášení ke konferenci protokolem SIP over TLS získá od Web Conferencing serveru autentizační Cookie, kterou využívá pro autentizaci při stažení souborů přiložených ke konferenci.
- Office 365 Message Encryption
  - Proprietární šifrování mailů s využitím Microsoft Rights Management Service (viz kapitola 11.1.23)
  - Při použití cloudové služby Azure RMS jsou pro šifrování mailů využity kryptografické algoritmy RSA s délkou klíčů 2048 bitů, AES s délkou klíčů 128 bitů a SHA-2.
  - Při použití on-premis Active Directory RMS mohou být použity dva režimy – Cryptographic Mode 1 – RSA s délkou klíčů 1024 bitů, AES s délkou klíčů 128 bitů a SHA-1 a Cryptographic Mode 2 – RSA s délkou klíčů 2048 bitů, AES s délkou klíčů 128 bitů a SHA-2.

- Šifrování mailů pomocí S/MIME:
  - Exchange Online podporuje End-to-End šifrování mailů ve formátu S/MIME a to včetně webového uživatelského rozhraní Outlook Web Access. Použité kryptografické algoritmy jsou závislé na konfiguraci mailového klienta a použitých certifikátech. Servery služby Exchange Online nemají k dispozici šifrovací klíče a nemohou získat obsah mailů.
- Pro šifrování uživatelských dat přenášených po Internetu se používá protokol TLS v rámci aplikačních protokolů HTTP, POP3, IMAP, SMTP, SIP a dalších:
  - Používány jsou pouze protokoly TLS 1.0, 1.1 a 1.2.
  - Preferovány jsou kombinace kryptografických algoritmů využívající výměnu klíčů pomocí algoritmu Diffie-Hellman založený na eliptických křivkách (ECDHE) s délkou klíčů 384 (preferovaná) nebo 256 bitů. Z důvodů kompatibility se staršími klienty jsou povoleny kombinace algoritmů využívající pro výměnu klíčů asymetrický algoritmus RSA.
  - Pro asymetrickou kryptografii je použit algoritmus RSA.
  - Pro symetrickou kryptografii je použit algoritmus AES s délkou klíčů 256 (preferovaný) a 128 bitů v módu CBC. Z důvodu kompatibility se staršími klienty je použit i algoritmus 3DES s délkou klíče 168 bitů. Služba Exchange online z důvodu kompatibility se staršími mobilními zařízeními podporuje navíc ještě algoritmus RC4 s délkou klíče 128 bitů s nejnižší prioritou.

- Poporovány jsou hash funkce SHA-384 (preferovaný s AES-256), SHA-256 (preferovaný s AES-128) a SHA-1. Podpora pro SHA-1 by měla být ukončena k 1.1.2017 (viz [37]). Služba Exchange online z důvodu kompatibility se staršími mobilními zařízeními podporuje navíc ještě algoritmus MD5 společně s šifrovacím algoritmem RC4 s nejnižší prioritou.
- Certifikáty používané u serverových služeb Office 365 využívají asymetrický algoritmus RSA s délkou klíčů 2048 bitů a hash funkci SHA-256. Certifikáty obsahují odkazy na revokační informace CRL a OCSP. Použité certifikační autority mají stejné nebo vyšší parametry s výjimkou kořenové certifikační autority, která využívá hash funkci SHA-1 (což u kořenových certifikačních autorit nevadí – hash certifikátu není využíván pro jeho validaci).

10.11 NÁSTROJ PRO ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI

Požadavky na technická opatření v oblasti nástroje pro zajišťování úrovně dostupnosti jsou uvedeny v §26 Vyhlášky.

10.11.1 IDENTIFIKACE POŽADAVKŮ NA NÁSTROJ PRO ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI

Vyhláška požaduje přijmout následující opatření k zajišťování úrovně dostupnosti:

- Pro KII a VIS používat, v souladu s bezpečnostními potřebami a výsledky hodnocení rizik, nástroj pro zajišťování úrovně dostupnosti informací
- Zajištění dostupnosti KII pro splnění cílů řízení kontinuity činností
- Zajištění odolnosti KII vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost
- Zajistit zálohování důležitých technických aktiv KII:
  - Využitím redundance v návrhu informačního systému
  - Zajištěním náhradních technických aktiv v určeném čase

10.11.2 ANALÝZA POŽADAVKŮ NA NÁSTROJ PRO ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI

Pro naplnění požadavků Zákon a Vyhlášky v oblasti nástroje pro zajišťování úrovně dostupnosti je tedy třeba, v souladu s výsledky analýzy rizik, přijmout sadu opatření:

- Nasadit nástroje pro zajišťování požadované úrovně dostupnosti
- Zavést organizační a technická opatření ke splnění cílů kontinuity činností. Technická opatření z této oblasti mohou zahrnovat:
  - Architektura informačního systému a jeho jednotlivých komponent musí vyhovovat požadavkům na úroveň dostupnosti informačního systému z pohledu
    - Celkové architektury včetně eliminace jednoho bodu výpadku (single point of failure)
    - Výkonosti a škálovatelnosti jednotlivých komponent
    - Redundance jednotlivých komponent
  - Provozní monitorování jednotlivých komponent informačního systému
  - Zálohování informačního systému a dat
  - Testování postupů obnovy informačního systému a dat

- Zavést opatření pro zajištění odolnosti vůči kybernetickým hrozbám. Tento požadavek může z technických opatření zahrnovat:
  - Implementaci firewallů, loadbalancerů, DMZ a segmentaci dítě
  - Implementaci aplikačních firewallů
  - Implementaci IPS systémů
  - Konfiguraci logování, auditování a implementaci systému SIEM

10.11.3 VZORY TECHNICKÝCH OPATŘENÍ PRO NÁSTROJ PRO ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI

Technická opatření v oblasti nástroje pro zajišťování úrovně dostupnosti mohou být, ve shodě s přílohou č. 1 Vyhlášky, realizována:

- Pro střední úroveň dostupnosti jsou využívány běžné metody zálohování a obnovy dat
  - Dostupnost systému je zejména zajišťována pravidelným zálohováním dat, aplikací, operačních systémů a virtualizační platformy
  - V závislosti na výsledcích analýzy rizik může být požadovaná úroveň dostupnosti zajišťována umístěním záloh off-site
  - V případě potřeby je provedena obnova podle předem připraveného, ověřeného a natrénovaného postupu
- Pro vysokou úroveň dostupnosti jsou využívány záložní systémy. Obnova poskytování služeb může zahrnovat zásahem obsluhy nebo výměnou zařízení
  - Dostupnost systému je zajišťována záložními systémy a pravidelným zálohováním dat, aplikací, operačních systémů a virtualizační platformy
  - V závislosti na výsledcích analýzy rizik může být požadovaná úroveň dostupnosti zajišťována umístěním záloh off-site a umístěním záložních systémů v geograficky odlehlém datovém centru
  - V případě potřeby je provoz převeden na záložní systémy. Zprovoznění těchto systémů vyžaduje zásah administrátora a může zahrnovat obnovu dat, případně aktuální konfigurace informačního systému ze zálohy
- Pro kritickou úroveň dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatická
  - Dostupnost systému je zajišťována záložními systémy s replikací dat a konfigurace a pravidelným zálohováním dat, aplikací, operačních systémů a virtualizační platformy
  - V závislosti na výsledcích analýzy rizik může být požadovaná úroveň dostupnosti zajišťována umístěním záložních systémů v geograficky odlehlém datovém centru
  - V případě potřeby je provoz převeden na záložní systémy automaticky

10.11.4 PROSTŘEDÍ MICROSOFT ONLINE SERVICES

Oblast nástroje pro zajišťování úrovně dostupnosti je prostředí Microsoft Online Services realizována následovně:

Architektura služeb

Architektura jednotlivých služeb poskytovaných zákazníkům je již od počátku navrhována jako vysoce dostupná. Takto navržená architektura zahrnuje:

- Redundance
  - Redundance disků a serverů v datovém centru
  - Redundance na úrovni budov datových center a napájení
  - Redundance na úrovni služeb jejich distribucí napříč datovými centry
  - Redundance dat jejich nepřetržitou replikací a udržováním násobného počtu replik
- Přizpůsobivost, elasticita
  - Rozkládání zátěže s dynamickou prioritou
  - Automatický i ruční přesun služeb na fungující zdroje v případě poruchy
  - Rutinní provádění obnov pro zajištění připravenosti na výskyt poruchy
- Distribuované služby
  - Komponenty SaaS a PaaP využívají distribuovanou funkcionalitu, kdy výpadek jednoho uzlu nebo lokality neohrozí dostupnost služby
  - Replikací adresářových služeb je zajištěna možnost autentizace uživatelů i v případě lokálního výpadku
  - Distribuované služby zjednodušují správu, údržbu, nasazování, diagnostiku a případné obnovy nebo opravy
- Monitorování
  - Probíhá neustálé monitorování všech poskytovaných služeb a jejich komponent
  - Probíhá analýza provozního stavu a veškeré odchylky jsou reportovány a tím je umožněn proaktivní zásah
  - Úroveň logování, auditování a trasování umožňuje izolovat a řešit problémy
- Snižování složitosti
  - Používání standardních komponent, kde je to možné
  - Používání standardizovaných procesů
  - Architektura software používá volné vazby mezi komponentami, takže monitorování a nasazování komponent je jednodušší
  - Propracovaný change-management zahrnuje ověření změn před jejich celosvětovým nasazením
- Support
  - 24/7 podpora pro zákazníky
- Průběžné zlepšování
  - Každý incident je zhodnocen a výsledky jsou využity k zamezení opakování podobného incidentu a pro zlepšení služeb

- Komunikace se zákazníkem
  - Konzistentní komunikace se zákazníkem je zajišťována několika způsoby

Dostupnost služeb

Dostupnost služeb **Microsoft Azure** je garantována poskytovatelem, společností Microsoft a je definována v dokumentu Service Level Agreement for Microsoft Online Services, viz [33]. Přehled dostupnosti pro vybrané služby je uveden v tabulce Tab. 3.

Tab. 3 Přehled dostupnosti vybraných služeb Microsoft Azure

Jméno služby	Dostupnost za měsíc v %
Azure Active Directory	99,9
Azure Rights Management	99,9
Microsoft Intune	99,9
Azure App Service	99,95
Application Gateway	99,9
Automation Service	99,9
Backup Service	99,9
BizTalk Services	99,9
Cache Services	99,9
CDN	99,9
Cloud Services	99,95
DocumentDB	99,95
ExpressRoute	99,9
Key Vault	99,9
Multi-Factor Authentication Service	99,9
Service-Bus Service	99,9
Site Recovery Service	99,9
SQL Database Service	99,99
Traffic Manager Service	99,99
Virtual Machines (Availability Set)	99,95
VPN Gateway	99,9

Dostupnost služeb Microsoft **Office 365** je garantována poskytovatelem, společností Microsoft a je definována v dokumentu Service Level Agreement for Microsoft Online Services, viz [33] jako 99,9%.

Zálohování

Služba Azure Backup umožňuje zálohování a obnovu, viz [35]

- Virtuálních severů provozovaných v Azure IaaS
- On-premise serverů
- On-premise virtuálních serverů Windows a Linux provozovaných na Hyper-V nebo VMware
- On-premise virtualizačních serverů Hyper-V
- Aplikačních serverů
  - SharePoint
  - Exchange
  - SQL
- Souborových serverů
  - Adresářů
  - Souborů

Zálohy jsou zašifrovány před přenosem do Azure úložiště. Toto úložiště (Backup Vault) je možné vytvořit na území EU a může být geograficky redundantní. Šifrovací klíče spravuje zákazník. Přenos záloh je realizován pomocí protokolu HTTPS a je tedy šifrován.

Služba Azure Site Recovery může být zahrnuta v business continuity i disaster recovery strategiích, viz [36]. Služba Azure Site Recovery replikuje servery běžící v datovém centru zákazníka (on-premise) do Azure Storage nebo do jiného datového centra zákazníka a provádí orchestraci failover. Při použití replikace do Azure Storage eliminuje požadavek na zřízení a provoz sekundárního datového centra zákazníka. Repliky jsou šifrovány před odesláním do sítě, a zůstávají zašifrovány v Azure Storage. Šifrovací klíče jsou uloženy odděleně od replikovaného obsahu v Azure Site Recovery vault a spravuje je zákazník. Přenos je realizován pomocí protokolu HTTPS a je tedy také šifrován Azure Site Recovery podporuje servery:

- Fyzický server
  - Windows
  - Linux
- Virtuální server
  - Běžící na Hyper-V
  - Běžící na VMware

Azure Site Recovery podporuje replikaci a orchestraci pro produkty:

- Active Directory
- DNS
- Web apps (IIS)
- SQL
- SCOM
- SharePoint
- SAP
- Exchange (ne DAG)
- Remote Desktop / VDI

- Linux
- Dynamic AX a CRM
- Oracle
- Souborový server Windows

Office 365

V Office 365 je ve službě Exchange Online k dispozici pro každého uživatele neomezený archiv (archivní mailbox).

10.12 BEZPEČNOST PRŮMYSLOVÝCH A ŘÍDICÍCH SYSTÉMŮ

Požadavky na technická opatření v oblasti bezpečnosti průmyslových a řídicích systémů jsou uvedeny v §27 Vyhlášky.

10.12.1 PRŮMYSLOVÉ A ŘÍDICÍ SYSTÉMY DLE §27 VYHLÁŠKY

Vzhledem k charakteru průmyslových a řídicích systémů KII dle §27 Vyhlášky nelze předpokládat využití cloudových služeb Microsoft Online Services pro realizaci vlastních průmyslových a řídicích systémů (například SCADA), pro které jsou určeny požadavky §27 Vyhlášky a proto pro ně nebyla provedena detailní analýza a návrh technických opatření.

Technická opatření ve zbývajících částech průmyslových a řídicích systémů KII dle §27 Vyhlášky (například manažerská nadstavba) realizovaných v rámci obecného modelu informačního systému (viz kapitola 6) lze pokrýt opatřeními popsanými v kapitole 10.

10.12.2 OSTATNÍ PRŮMYSLOVÉ A ŘÍDÍCÍ SYSTÉMY

Pro průmyslové a řídicí systémy nespadající do definice §27 Vyhlášky – například nově se rozvíjející oblasti Internetu věcí (IoT) – je možné využít cloudové služby Microsoft Online Services pro zpracování dat a jejich řízení. Technická opatření pro tyto průmyslové a řídicí systémy realizované v rámci obecného modelu informačního systému (viz kapitola 6) lze pokrýt opatřeními popsanými v kapitole 10.

11 VYPOŘÁDÁNÍ POŽADAVKŮ PŘÍLOHY Č. 1 VYHLÁŠKY

V příloze č. 1 Vyhlášky jsou uvedeny požadavky na zabezpečení informací dle jejich důležitosti, a to v oblastech důvěrnosti, integrity a dostupnosti. V každé z uvedených oblastí mají aktiva definovány čtyři úrovně důležitosti a z nich vyplývající požadavky na ochranu.

Tato kapitola popisuje způsoby pokrytí požadavků na zajištění bezpečnosti informací v navrženém modelu informačního systému, viz kapitola 6, pro úrovně střední, vysoká a kritická (úroveň nízká neklade na zabezpečení žádné požadavky (důvěrnost, integrita) anebo požaduje pouze běžné zálohování (důvěrnost)). Nejprve popisuje relevantní technologie a potom identifikuje jejich použití pro pokrytí požadavků přílohy Vyhlášky.

11.1 POPIS TECHNOLOGIÍ

V následujících kapitolách jsou uvedeny relevantní technologie, které lze použít pro vypořádání požadavků přílohy č. 1 Vyhlášky. Tyto technologie jsou následně uvedeny i v kapitole 11.2, která popisuje způsob pokrytí požadavků přílohy Vyhlášky.

11.1.1 AZURE AD

Azure Active Directory je komplexní cloudové řešení pro správa identit a přístupu, které umožňuje zabezpečit přístup k datům a aplikacím a zjednodušuje správu uživatelů a skupin. Spojuje v sobě základní adresářové služby, pokročilou správu identit, zabezpečení a řízení přístupu k aplikacím. Je klíčovým prvkem služeb Microsoft Cloud, včetně Microsoft Azure, Office 365, Microsoft Dynamics CRM Online, Intune, a SaaS aplikací třetích stran. Azure Active Directory také usnadňuje vývojářům vytvářet správu identit založenou na zásadách do svých aplikací.

Azure AD obsahuje následující bezpečnostní prvky:

- Jednotné přihlášení (Single sign-on)
  - Pro zařízení s různými systémy (Windows, Mac, Android a iOS)
  - Pomocí Aplikační proxy i přístup k publikovaným on-premise aplikacím
- Více faktorová autentizace pro cloudové i on-premise aplikace
- Bezpečnostní auditing, monitoring s notifikací a bezpečnostní reporty
- Možnost delegování operací (mazání hesel a správa skupin) a možnost povolit samoobslužné operace (mazání hesel a správa skupin)
- Integrace s Active Directory (synchronizace a federace identit)
- Dynamické členství v bezpečnostních skupinách
- Podpora řízení přístupu pomocí rolí - RBAC

- Podpora standardů
  - SAML 2.0
  - WS-Federation
  - OpenId Connect
  - OAuth 2.0
- Dostupnost služby 99,9%

Další informace o Azure AD jsou uvedeny v kapitolách 10.3.4 a 10.6.4.

V případě, že je Azure AD synchronizováno s on-premise Active Directory je nutné implementovat federaci Azure AD s on-premise Active Directory pomocí Active Directory Federation Service (ADFS), aby přihlašovací údaje (hashe hesel) nebyly uloženy ve službě Azure AD, protože databáze Azure AD je replikována i mimo území EU.

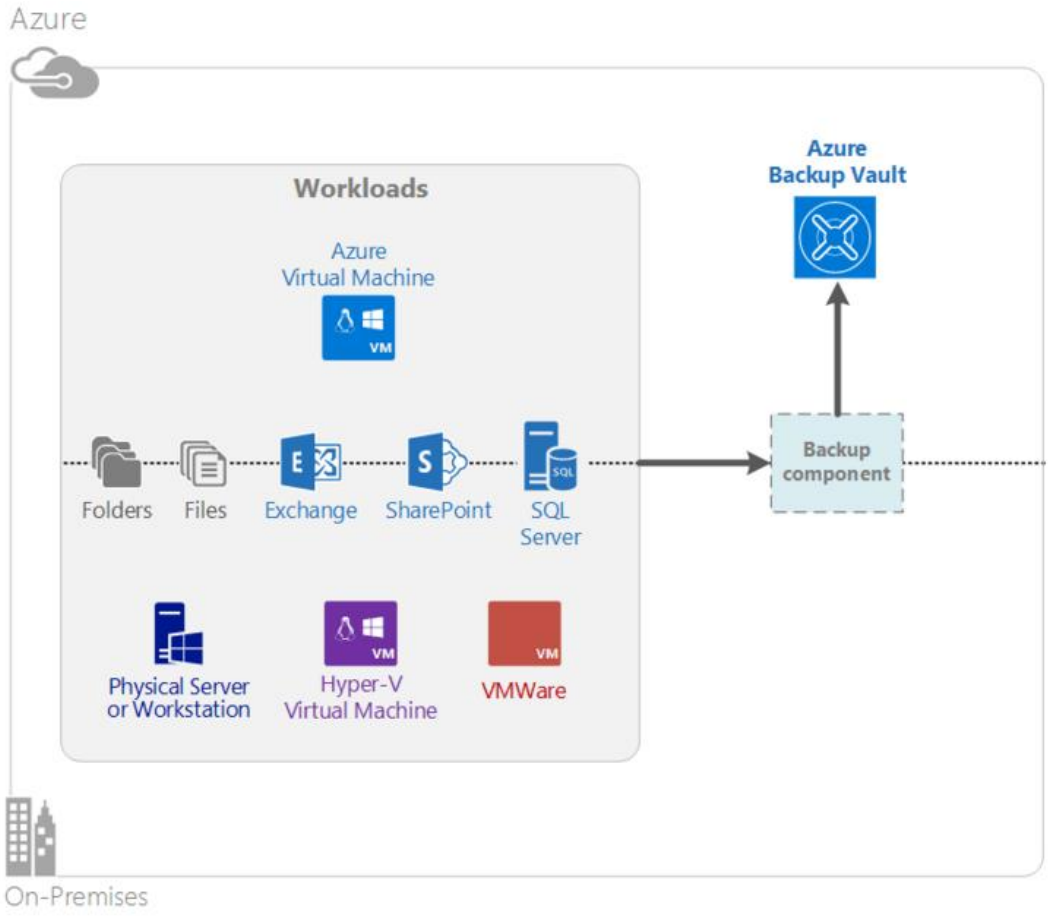
11.1.2 AZURE BACKUP

Azure Backup je služba pro zálohování a obnovení dat v cloudu společnosti Microsoft. Umožňuje nahradit existující zálohovací řešení existující on-premise nebo off-site. Azure Backup je spolehlivá, bezpečná a cenově konkurenceschopná služba. Také umožňuje zálohovat servery a služby, které běží v cloudu. Azure Backup poskytuje škálovatelnost, dostupnost a odolnost Microsoft Azure.

Azure Backup obsahuje následující bezpečnostní prvky:

- Centrální správa z jednoho místa
- Šifrování dat (AES 265)
  - Během přenosu z/do úložiště (cloudu)
  - V úložišti
  - Při zálohování on-premise serveru není šifrovací klíč nikdy přenášen nebo uložen v Microsoft Azure
- Automatická správa úložiště s neomezenou kapacitou
- Volba redundance úložiště dle požadavků
  - Lokální redundance (tři lokální kopie v datacentru)
  - Geo-redundance (další tři kopie v geograficky odlehlém datacentru)
- Dlouhodobé úložiště (až 99 let)
- Zálohovaný server musí být ve službě Azure Backup registrován a při přístupu k úložišti (Backup Vault) autentizován

Obr. 16
Komponenty Azure Backup, viz [35]



Další informace o Azure Backup jsou uvedeny v kapitole 10.11.4.

Informace o způsobu šifrování záloh Azure virtuálních serverů jsou uvedeny v dokumentu [82].

11.1.3 AZURE APP SERVICE

Azure App Service je cloudová služba, která zahrnuje veškeré potřebné služby pro jednoduché a rychlé vytváření a provozování webových a mobilních aplikací. Integruje schopnosti Azure Websites, Azure Mobile Services a Azure Biztalk Services. Azure App Services poskytují i bezpečnostní služby pro vývoj a provoz aplikací v cloudu, viz [68], které zahrnují:

- Bezpečnost na úrovni infrastruktury MCIO a Microsoft Azure platformy
  - Izolace aplikačních služeb od Internetu a ostatních zákazníků
  - Bezpečné uložení citlivých informací (přihlašovací údaje, připojovací řetězce), zabezpečení pomocí Azure Resource Manageru, viz 11.1.6
  - Šifrování veškeré komunikace, včetně PowerShell managementu, rozhraní příkazové řádky, REST API a dalších

- 24*7 ochrana proti hrozbám
  - Malware
  - DDoS
  - MitM
- Za bezpečnost na úrovni aplikace není poskytovatel cloudových služeb v tomto případě zodpovědný

Pro penetrační testování aplikací v App Service je možné použít Tinfoil Security. Použití jiných nástrojů musí být nejdříve schváleno a povoleno týmem Azure, viz [72].

11.1.4 AZURE DISK ENCRYPTION

Azure Disk Encryption pomáhá zajistit důvěrnost dat pomocí sady technologií pro šifrování, kontrolu a správu šifrovacích klíčů a auditováním přístupu k datům.

Azure Disk Encryption umožňuje šifrovat disky (jak systémové tak i datové) virtuálních serverů:

- Windows serverů pomocí BitLockeru
- Linux serverů pomocí DM-Cryptu

Azure Disk Encryption se integruje s Azure Key Vault, viz kapitola 11.1.5 čímž je zajištěna výhradní správa a přístup k šifrovacím klíčům.

Více informací o Azure Disk Encryption je uvedeno v kapitole 10.10.4 a v dokumentu [65].

11.1.5 AZURE KEY VAULT

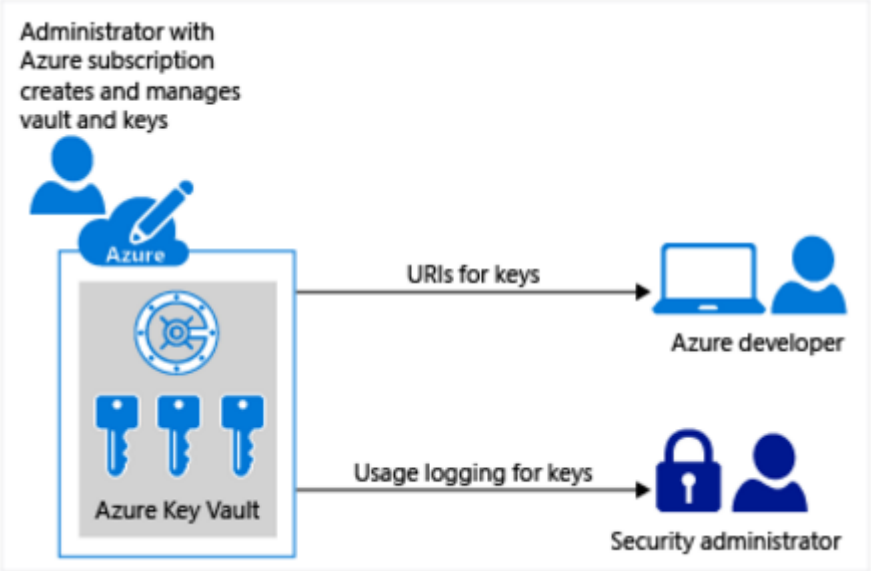
Azure Key Vault pomáhá chránit šifrovací klíče a tajemství používané v cloudových aplikacích a službách. Do Azure Key Vault, je možné uložit asymetrické klíče a tajemství (jako například autentizační API klíče, klíče Azure Storage účtu, šifrovací klíče, soubory PFX a hesla) pomocí klíčů, které jsou chráněny hardwarovými bezpečnostními moduly (HSM) splňujícími FIPS 140-2 Level 2 (hardware a firmware). Pro větší jistotu, je možné importovat nebo generovat klíče s využitím vlastního HSM (Bring Your Own Key, BYOK).

Key Vault zefektivňuje proces správy klíčů a umožňuje udržet si kontrolu nad klíči, které umožňují přístup a šifrování dat. Vývojáři mohou vytvářet klíče pro vývoj a testování během několika minut, a poté bez problémů migrovat na produkční klíče. Bezpečnostní administrátoři mohou přidělovat (a odebírat) oprávnění ke klíčům.

Azure Key Vault obsahuje následující bezpečnostní prvky:

- HSM jsou umístěny v datovém centru MCIO
- Možnost importovat vlastní klíče
- HSM odpovídají FIPS 140-2 Level 2
- Key Vault je navržen tak, aby Microsoft nemohl vidět nebo extrahovat zákaznické klíče
- Logování použití klíčů v reálném čase
- Centrální správa pro všechny úložiště klíčů
- Komunikace s Azure Key Vault probíhá přes protokol HTTPS
- Požadavky musí být autentizovány. Key Vault podporuje Azure AD access tokeny (OAuth 2.0)
- Podporované typy klíčů a algoritmů a operací jsou uvedeny v dokumentu [38]

Obr. 17
Schema Azure Key Vault, viz [39]



11.1.6 AZURE RESOURCE MANAGER

Jednotlivá řešení, aplikace či informační systémy se skládají z velkého množství komponent (virtuálních serverů, diskových úložišť, virtuálních sítí, databází, webových aplikací a dalších služeb). Azure Resource Manager umožňuje pracovat s komponentami jako se skupinou. Je možné nasadit, aktualizovat nebo mazat všechny komponenty (prostředky) řešení v jediné, koordinované operaci. Nasazení je možné provádět pomocí šablon. Jednu šablonu lze použít pro různá prostředí, například testovací, ověřovací a produkční. Pro správu prostředí poskytuje Resource Manager bezpečnostní, auditovací a označovací funkce.

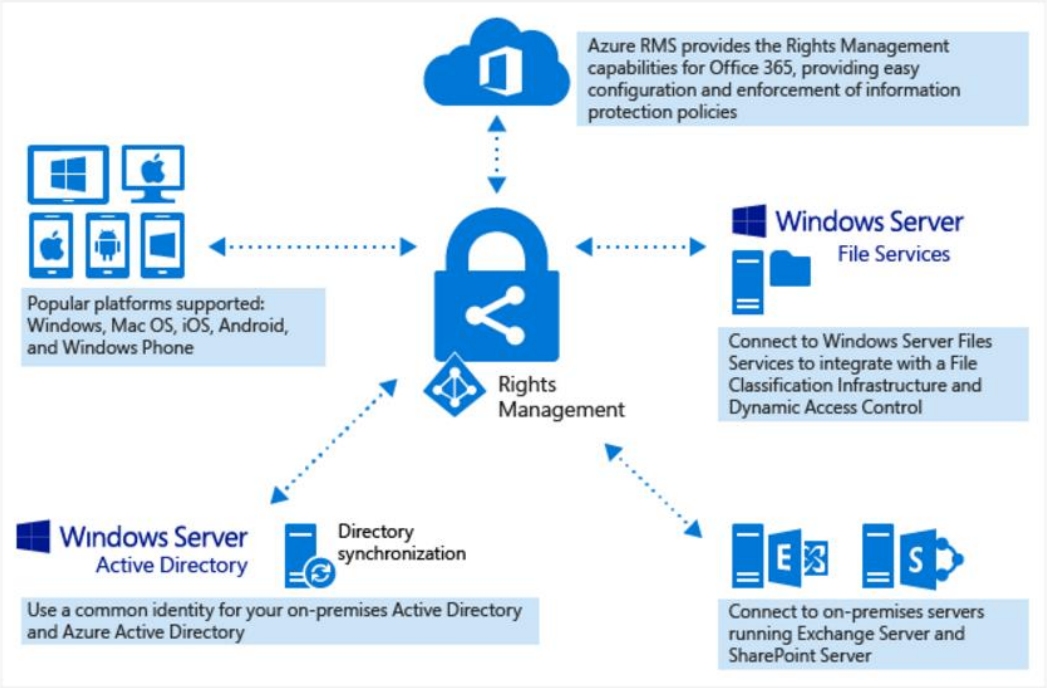
Azure Resource Manager, viz [40], poskytuje následující výhody:

- Skupinová správa, monitorování a nasazování komponent
- Deklarativní šablony pro opakovaná nasazení
- Definování závislostí mezi zdroji pro správné pořadí nasazení
- RBAC řízení přístupu ke všem komponentám ve skupině zdrojů
- Podpora označení zdrojů pro jejich logické řazení s vazbou na účtování

Azure Resource Manager nativně integruje OAuth a RBAC do správy platformy a aplikuje řízení přístupu ke všem službám ve skupině zdrojů. Předdefinované pro zdroje specifické RBAC role mohou být přiřazeny na úrovni Azure předplatného, skupiny zdrojů nebo na jednotlivém zdroji, seznam vestavěných rolí je uveden v dokumentu [42]. Více informací o Azure RBAC je uvedeno v kapitole 10.4.4 a v dokumentu [12].Prováděné operace (akce, čas a uživatel) jsou automaticky auditovány, viz [41].

11.1.7 AZURE RMS

Azure Rights Management je řešení pro ochranu informací zasílaných mailem, uložených na souborovém serveru nebo v cloudové službě a to i při přístupu k těmto informacím přes Internet z různých zařízení a při jejich sdílení s jinými uživateli či organizacemi. Trvalá ochrana informací, kterou Azure RMS poskytuje, nezabezpečuje jen data, ale pomáhá také splnit regulatorní požadavky.



Obr. 18
Schema Azure RMS pro Office 365, viz [31]

Azure RMS poskytuje následující funkcionality:

- Ochrana libovolného typu souboru
- Ochrana souboru bez ohledu na to, kde je uložen
- Ochrana příloh elektronické pošty (i pro mobilní zařízení). Pouze autorizovaný příjemce může vykonávat povolené aktivity s přiloženým, chráněným dokumentem. Zpráva jako taková šifrovaná není
- Auditování a monitorování chráněných souborů
- Podpora různých zařízení
  - Windows počítač, telefon a tablet
  - Mac počítač
  - iOS tablet a telefon
  - Android tablet a telefon
- Podpora spolupráci mezi organizacemi, pokud obě mají Office 365 nebo Azure předplatné
- Ochrana mailů v Exchange online integrací s DLP politikami
- Ochrana dokumentů v SharePoint Online integrací s chráněnými knihovnami

- Integrace s on-premise službami pomocí RMS konektoru
  - Exchange server
  - SharePoint server
  - Souborový server Windows se službou File Clasification Infrastructure
- Zjednodušení konfigurace požadované úrovně zabezpečení pomocí šablon
- API umožňující zabudovat podporu Azure RMS do aplikací třetích stran
- Kontrola vlastních dat
  - Použití vlastního tenant klíče v HSM modulu (BYOK) umožní ochránit data před poskytovatelem služby, viz [43]. Tato vlastnost není dostupná pro Exchange Online
  - Auditing a logování používání
    - Analýza používání RMS
    - Monitorování pokusů o zneužití
    - Forenzní analýza
  - Ochrana ztráty dat při ztrátě klíčů
  - Podpora federace identit mezi Azure AD a on-premise Active Directory a podpora jednotného přihlášení pomocí ADFS
  - Podpora exit scénáře bez ztráty chráněných dat, viz [44]

Azure RMS algoritmy a délky klíčů:

- Podpora kryptografických standardů a FIPS 140-2, viz [31]
- Ochrana dokumentů – AES s délkou klíče 128 bitů (AES s délkou klíče 256 bitů pro .p*file* a .ppdf soubory)
- Ochrana klíčů – RSA s délkou klíče 2048 bitů
- Podpis certifikátů – SHA-256

Jednotlivé generované klíče a způsoby jejich použití při ochraně informací v Azure RMS jsou popsány v dokumentu [31].

11.1.8 AZURE SECURITY AND AUDIT LOG MANAGEMENT

Azure umožňuje zákazníkům nastavit vytváření auditních záznamů bezpečnostních událostí a provádět jejich sběr a to jak ze služeb provozovaných v infrastruktuře jako služba (IaaS) tak i platformě jako služba (PaaS). Sběr záznamů se provádí do centrálního úložiště v předplatném (Azure Subscription). Zákazníci pak mohou využít HDInsight pro agregování a analýzu událostí. Kromě toho mohou být tyto shromážděné události exportovány do on-premise systémů SIEM k průběžnému monitorování.

Bezpečnostní logování, monitorování a analýza zahrnuje:

- Generování logu při výskytu události (Azure Diagnostics pro PaaS služby a IaaS virtuální stroje a služby)
- Sběr logů z různých zdrojů a jejich ukládání do centrálního úložiště (Azure Storage Account)
- Analýza logů (například pomocí HDInsight nebo SIEM systémem)
- Centralizované monitorování a reporty

Logy přenášené mezi systémem, který je generuje a úložištěm jsou při přenosu šifrovány na úrovni transportního protokolu HTTPS.

Více informací o Azure Security and Audit Log managementu je uvedeno v dokumentech [13] a [14]

11.1.9 AZURE SITE RECOVERY

Služba Azure Site Recovery může být zahrnuta v Business Continuity a Disaster Recovery strategiích, viz [36].

Služba je certifikovaná dle ISO 27001:2005, certifikace HIPAA, DPA a FedRAMP JAB probíhají.

Azure Site Recovery zajišťuje bezpečnost informací, viz [48]:

- Autentizací a šifrováním komunikace mezi agentem a Azure Site Recovery službou pomocí protokolu HTTPS
- Šifrováním replikovaných dat mezi agentem a Azure Site Recovery Vaultem. K zašifrování dat se používá klíč certifikátu X.509, který spravuje zákazník
- Data uložená v úložišti (Azure Site Recovery Vault) jsou šifrována AES s délkou klíče 256 bitů. K zašifrování dat se používá klíč certifikátu X.509, který spravuje zákazník
- Pouze pro obnovu při havárii je třeba poskytnout klíč k dešifrování serverů tak, aby mohly být spuštěny.

Další informace o Azure Site Recovery jsou uvedeny v kapitole 10.11.4.

11.1.10 AZURE STORAGE

Data ukládaná do Azure Storage Blobu mohou být pomocí rozšíření Azure Encryption Extensions zašifrována pomocí Microsoft Cryptographic Service Provideru. Pro šifrování a dešifrování, které probíhá na straně klienta (klíče tedy neopouští systém, který zapisuje, nebo čte data) je možné používat symetrickou i asymetrickou kryptografii. Toto řešení vyžaduje na straně klienta aplikační podporu.

Více informací o možnostech šifrování dat ukládaných do Azure Storage je v kapitole 10.10.4 a dokumentu [46].

Pro přístup k Azure Storage je nutné se autentizovat pomocí klíče. Každý Storage Account obsahuje vlastní administrátorský klíč, umožňující plný přístup. Pro delegování přístupu je možné vytvořit sdílené přístupové klíče a pro ně definovat omezený přístup k objektům ve Storage Accountu a dobu platnosti přístupového klíče. Více informací je uvedeno v dokumentu [47].

11.1.11 AZURE TRAFFIC MANAGER

Azure Traffic Manager umožňuje řídit síťovou komunikaci mezi externími uživateli nebo systémy a Azure službami. Řízení síťové komunikace spočívá v aplikování inteligentních politik do DNS odpovědí. Traffic Manager umožňuje inteligentní směrování komunikace při umístění služeb v různých celosvětově distribuovaných datových centrech Microsoft Azure pro:

- Zvýšení dostupnosti aplikací
- Zvýšení výkonosti a zkrácení doby odezvy
- Provádění údržby bez výpadku služby
- Distribuci komunikace pro velké a složité aplikace

Více informací o Traffic Manageru je uvedeno v dokumentu [77] .

11.1.12 AZURE VPN GATEWAY

Azure VPN Gateway umožňuje VPN přístup ke službám provozovaným v Microsoft Azure:

- Point-to-Site
  - Slouží pro připojení jednotlivých počítačů (s operačními systémy Microsoft Windows) k Azure virtuální síti
  - Využívá Azure VPN Gateway s dynamickým směrováním IP protokolu
  - Pro autentizaci klientů se využívají X.509 certifikáty
  - Pro zašifrování VPN komunikace se používá protokol SSTP
- Site-to-Site
  - Slouží pro propojení on-premise lokální sítě k Azure virtuální síti
  - Slouží pro propojení Azure virtuálních sítí (pokud se nachází v různých datových centrech, nebo v různých předplatných)
  - Využívá Azure VPN Gateway se statickým nebo dynamickým směrováním IP protokolu
  - Pro autentizaci a zašifrování komunikace se používá protokol IPSec

Více informací o Azure VPN je uvedeno v kapitolách 10.9.4, 10.10.4 a v dokumentu [29].

11.1.13 BITLOCKER DRIVE ENCRYPTION

BitLocker Drive Encryption chránit celé diskové jednotky a zabraňuje útočníkům v získání přístupu k systémovým souborům, které je možné využít k odhalení hesla, nebo v získání přístupu k disku jeho odebráním z počítače a následnou instalací do počítače jiného. BitLocker může zašifrovat jednotku, na které je nainstalovaný systém Windows (jednotka operačního systému), i pevné datové jednotky (jako jsou interní pevné disky). Pomocí nástroje BitLocker To Go je možné pomáhat při ochraně všech souborů uložených na vyměnitelných datových jednotkách (například externí pevné disky nebo jednotka USB Flash).

K funkcím a vlastnostem BitLockeru patří:

- Šifrování všech dat uložených na svazku operačního systému Windows a na nakonfigurovaných svazcích dat. Mezi šifrovaná data patří operační systém Windows, hibernační a stránkovací soubory, aplikace a data používaná aplikacemi
- Ve výchozím nastavení BitLocker používá čip TPM (Trusted Platform Module), který má pomoci zajistit integritu součástí, které se podílejí na prvotní fázi spouštění počítače (součástí použitých v raných fázích procesu spouštění), a zamkne všechny svazky chráněné nástrojem BitLocker tak, aby zůstaly chráněny i tehdy, když je s počítačem neoprávněně manipulováno v době, kdy není spuštěn operační systém
- Přispívá k ochraně dat před neoprávněným přístupem. Fyzické zabezpečení serverů sice zůstává důležité, avšak nástroj BitLocker navíc pomáhá chránit data při krádeži počítače, při přepravě počítače z jednoho místa na jiné místo nebo v jiných situacích, kdy je počítač mimo fyzickou kontrolu
- Šifrování disku pomáhá zabránit útokům offline, například pokusu obejít opatření pro zabezpečení systému Windows (jako jsou oprávnění vynucovaná seznamy řízení přístupu (ACL) systému NTFS) odebráním diskové jednotky z jednoho počítače a její instalací do jiného počítače
- Centrální správa BitLocker je možná pomocí nástroje MDOP a pomocí skupinových politik Active Directory, nebo pomocí nástrojů WBEM, které jsou kompatibilní s rozhraním WMI

- BitLocker Drive Encryption je možné nakonfigurovat pro zálohování informací potřebných pro obnovení BitLockerem chráněných disků a Trusted Platform Modulu (TPM) do Active Directory. Informace pro obnovení zahrnují 48-místné heslo a 256-bitový klíč pro obnovení pro každou jednotku chráněnou BitLockerem, TPM heslo a údaje požadované pro identifikaci počítače, kterého se obnova týká
- Šifrovací algoritmy používané BitLockerem se mezi verzemi operačního systému Windows liší. Využívá se kombinace AES-CBC s délkou klíčů 128 nebo 265 bitů, která je do verze Windows 7 včetně posílena o elephant diffuser. Použitou délku klíčů lze konfigurovat pomocí skupinové politiky

Informace o způsobu implementace BitLockeru v prostředí Microsoft Online Services jsou uvedeny v kapitole 10.10.4.

11.1.14 CUSTOMER LOCKBOX

Customer Lockbox pro Office 365 je navržen tak, aby zákazníkům poskytl bezprecedentní kontrolu nad jejich daty ve službě. Customer Lockbox dává zákazníkům explicitní kontrolu ve velmi vzácných případech, kdy může inženýr společnosti Microsoft potřebovat přístup k obsahu zákazníka za účelem vyřešení problému zákazníka.

Služby Microsoft Office 365 jsou vyvinuty tak, že pro svůj běh nevyžadují přístup zaměstnanců společnosti Microsoft k zákaznickým datům. Ten může být potřeba pouze při řešení požadavků nebo problémů zákazníka. V těchto případech je přístup umožněn a kontrolován pomocí Customer Lockboxu, který zajistí, že Microsoft inženýr nedostane přístup k obsahu zákazníka bez výslovného souhlasu zákazníka. Když zákazník dostane žádost o přístup, může žádost zkoumat a buď schválit, nebo odmítnout. Dokud není žádost schválena, nebude přístup Microsoft inženýrovi umožněn.

Veškeré aktivity jsou logovány v Office 365 Management Activity logu.

Více informací o Customer Lockboxu pro Office 365 je uvedeno v dokumentu [50].

11.1.15 EXPRESS ROUTE + VPN

Express Route umožňuje propojení interní sítě s cloudovými službami Microsoft Online Services pomocí vyhrazeného privátního spoje. Bezpečnost spojení je dána definováním privátních virtuálních okruhů přes vyhrazená fyzická spojení, viz [49]. Tato spojení neprochází přes veřejný Internet.

Express Route neposkytuje sama o sobě šifrování IP komunikace. To je třeba zajistit pomocí Site-to-Site VPN. Pro Site-to-Site VPN lze použít Azure VPN Gateway společnosti Microsoft, viz kapitola 11.1.11 nebo řešení třetích stran, jako například Barracuda Networks Firewally, Cisco ASA Firewally, Fortinet Fortigate firewally a další, které jsou k dispozici jak na straně on-premise, tak v Microsoft Azure, viz dokument [67].

Více informací o Express Route je uvedeno v kapitole 10.9.4 a v dokumentu [30].

11.1.16 INTEGRACE IDENTIT

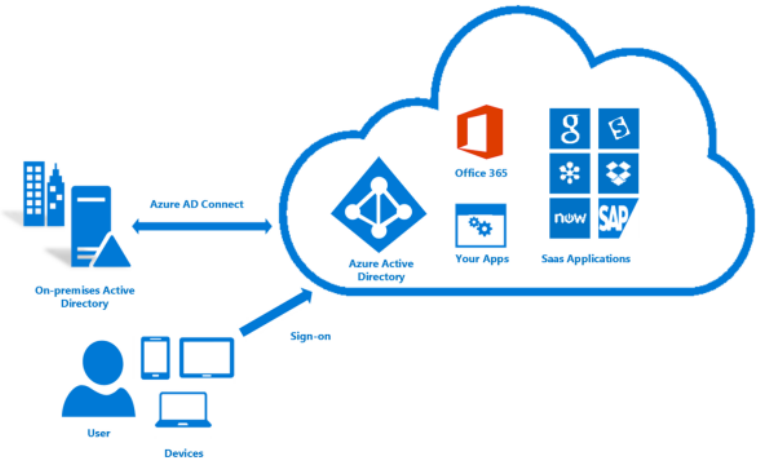
Integraci on-premise identit s adresářovými službami Azure AD je možné zajistit pomocí nástroje Azure AD Connect.

Azure AD podporuje integraci s interními adresářovými službami (On-Premise Directory), viz [9], pomocí:

- Synchronizace identit
  - Identity jsou synchronizované, hesla mohou být různá s různou politikou a musí být udržována separátně

- Synchronizace identit a hesel (synchronizuje se hash hesla)
  - Identity i hesla jsou synchronizovaná, uživatelé používají jedno heslo ke cloudovým i on-premise systémům. Změna hesla je propagována napříč synchronizovanými adresářovými službami
- Federace identit
  - Informace o identitě je synchronizována s Azure AD, vlastní autentizace ale zajišťuje on-premise adresářová služba (například Active Directory), která je zprostředkovaná promocí AD FS služby. AD FS služba je pomocí WAP publikovaná do Internetu
  - Při využití federační služby nejsou do Azure AD synchronizovány hashe hesel, autentizace probíhá v on-premise doméně AD
  - Umožňuje využívat Schopnosti Active Directory a skupinových politik pro definování politik hesel
  - Federaci identit lze používat s Více faktorovou autentizací, viz 11.1.19 a tím dále zvýšit bezpečnost autentizace

Obr. 19
Schéna federace identit, viz [9]



Federace identit umožní přístup ke cloudovým službám s autentizací v on-premise doméně Active Directory pro:

- Uživatele, kteří jsou přihlášeni k počítači zařazeném do domény se svým uživatelským jménem a heslem z on-premise domény, ale kteří nejsou připojení k podnikové síti.
- Uživatele, který nepoužije počítač zařazený do domény, ale musí se přihlásit doménovým jménem a heslem pro přístup ke cloudové službě
- Chytrý telefon, pro přístup ke cloudové službě, jako je Microsoft Exchange Online pomocí aplikace Microsoft Exchange ActiveSync, se musí uživatel přihlásit doménovým jménem a heslem pro přístup ke cloudové službě
- Uživatele, který se přihlásí doménovým jménem a heslem pro přístup k Office 365 e-mailu v případě, že používá aplikaci Outlook nebo e-mailového klienta, který není součástí sady Office; Například, IMAP nebo POP3 klienta

11.1.17 MICROSOFT INTUNE

Služba Microsoft Intune poskytuje správu mobilních zařízení, správu mobilních aplikací a správu počítačů prostřednictvím cloudu. Pomocí služby Intune je možné zajistit uživatelům přístup k podnikovým aplikacím, datům a zdrojům prakticky odkudkoli na téměř jakémkoli zařízení. Tato služba současně pomáhá se zabezpečením podnikových informací.

V oblasti ochrany podnikových dat Intune umožňuje zabezpečit data, včetně Exchange e-mailů, e-mailu aplikace Outlook a Onedrive for Business a to na základě enrollmentu zařízení a aplikování politiky pro zajištění schody s regulatorními požadavky.

Základní schopnosti Intune obsahují:

- Správu mobilních zařízení, která zahrnuje
  - Integrovanou ochranu dat a vynucení bezpečnostních politik
    - Vynucení aplikovaní politiky přístupového hesla
    - Vynucení zašifrování obsahu zařízení
    - Vynucení zamykání zařízení
    - Detekce, zda vestavěná bezpečnostní architektura zařízení nebyla porušena (root, jailbreak a podobně)
  - Podporu platforem Windows, Windows Phone, iOS a Android
  - Samoobslužný portál s instalací firemních aplikací
  - Vzdálenou správu zařízení
    - Správa certifikátů, WiFi a VPN profilů
    - Reset hesla
    - Uzamčení zařízení
    - Šifrování dat
    - Vymazání zařízení (pro případ ztráty nebo krádeže)
- Správu mobilních aplikací, která zahrnuje
  - Kontejnerizace firemních aplikací
    - Ochrana dat – selektivní vymazání dat a firemních aplikací
    - Definování povolených operací a zamezení výměny a sdílení dat s jinými aplikacemi na zařízení
  - Možnost zakázat přístup k definovaným URL a specifickým aplikacím
- Správu počítačů, která zahrnuje
  - Správu PC a notebooků, podporu platforem PC, Mac a UNIX/Linux
  - Integraci se System Center Configuration Managerem
  - Integraci s Azure RMS
  - Ochranu proti malware
  - Inventarizaci hardware a software
  - Instalaci a aktualizaci software
  - Správu konfigurace (například konfigurace firewallu)

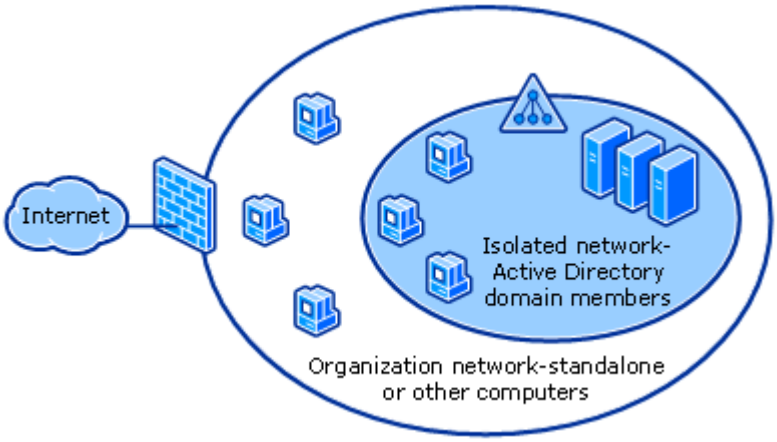
Další informace o způsobech ochrany podnikových informací pomocí Microsoft Intune jsou uvedeny v dokumentu [51].

11.1.18 ŠIFROVÁNÍ KOMUNIKACE PO LOKÁLNÍ SÍTI

Šifrování komunikace po lokální síti zajistí integritu a důvěrnost přenášených dat. Vlastní šifrování může být zajištěno na úrovni protokolů síťové nebo aplikační vrstvy.

Na úrovni síťové vrstvy se jedná o řešení využívající protokol IPSec. Pomocí konfigurace IPSec protokolu na jednotlivých počítačích nebo jejich skupinách je před započetím komunikace vynucena autentizace a autorizace a následně může být zajištěno i šifrování IP komunikace. Pro autentizaci může být využíván sdílený klíč nebo protokol Kerberos. Pro zajištění integrity a důvěrnosti jsou používány různé šifrovací algoritmy v závislosti na implementaci protokolu IPSec v konkrétním operačním systému.

Obr. 20
Schéma izolace sítě s využitím Active Directory, viz [52]



Na úrovni aplikační vrstvy se jedná:

- O využití TLS protokolu pro zabezpečení komunikace, která využívá protokoly HTTP, POP, IMAP, SMTP, LDAP
- O zabezpečení komunikace se souborovými servery, která využívá protokol SMB. Protokol SMB umožňuje šifrování (algoritmus AES-CCM s délkou klíče 128 bitů) a podepisování (algoritmus AES-CMAC ve verzi SMB3 nebo HMAC SHA-256 ve verzi SMB2) síťové komunikace
- O zabezpečení komunikace s doménovými řadiči (autentizace uživatelů a počítačů), která využívá protokol Kerberos. Protokol Kerberos pro zašifrování přenášených informací umožňuje používat šifrovací algoritmy (podpora jednotlivých algoritmů závisí na verzi operačního systému, viz [53]):
  - AES256-CTS-HMAC-SHA1-96
  - AES128-CTS-HMAC-SHA1-96
  - RC4_HMAC_MD5
  - ECC pro přihlašování pomocí čipových karet s použitím X.509 certifikátů

Více informací o konfiguraci šifrování protokolu Kerberos je uvedeno v dokumentu [54].

11.1.19 VÍCE FAKTOROVÁ AUTENTIZACE

Více faktorová autentizace je metoda ověřování, která vyžaduje použití více než jednoho způsobu ověření a přidává kritickou druhou úroveň zabezpečení pro uživatelské přihlašování. Funguje tak, že je vyžadováno použití dvou nebo více z následujících metod ověřování:

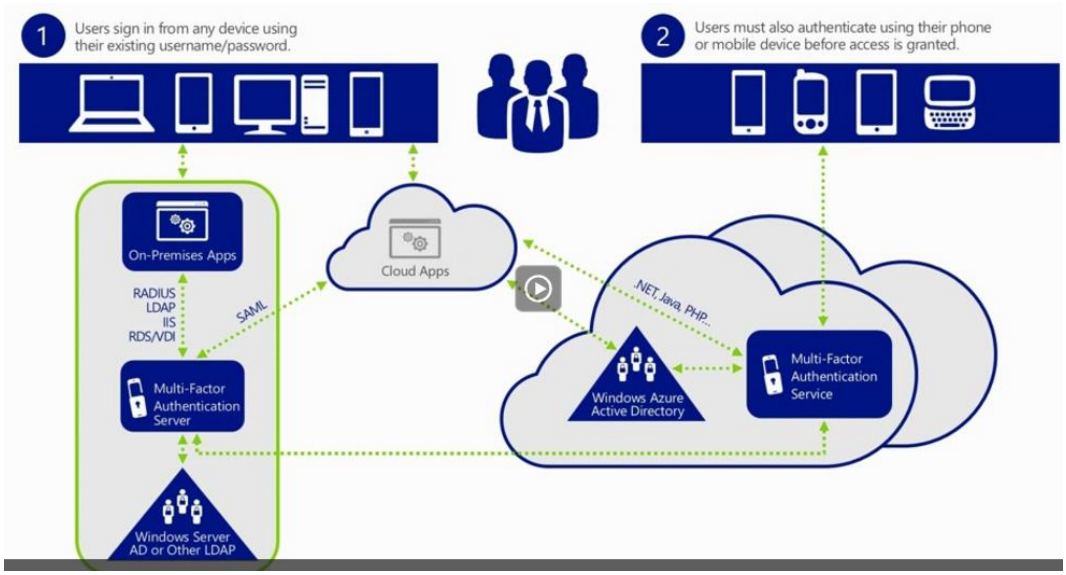
- Něco, co víte (typicky hesla)
- Něco, co máte (důvěryhodné zařízení, které není snadné duplikovat, jako telefon)
- Něco, co jste (biometrie)

Azure Multi-Factor Authentizace pomáhá zvýšit ochranu přístupu k datům a aplikacím při splnění požadavku na jednoduchý proces přihlášení. Poskytuje silnou autentizaci pomocí řady snadných ověřovacích metod:

- Telefonní hovor
- Textová zpráva
- Mobilní aplikace
  - Notifikace
  - Ověřovací kód
- OAth token třetí strany

Azure Multi-Factor Authentizaci lze používat pro ověření identity uživatelů při přístupu k:

- Office 365
- Microsoft Azure
- Cloudovým aplikacím
- On-premise aplikacím



Obr. 21
Schéma Azure Mutli-Factor autentizace, viz [55]

Více informací o Azure Multi-Factor Autentizace je uvedeno v dokumentu [55].

11.1.20 CENTRÁLNĚ SPRAVOVANÁ A ŘÍZENÁ KONFIGURACE

Centrálně spravovaná a řízená konfigurace je sada procesů a technologií, které mají za úkol řídit konfiguraci spravovaných počítačů (serverů a stanic) v oblastech:

- Instalace a konfigurace operačního systému
- Instalace a konfigurace aplikačního software
- Správa bezpečnostní konfigurace
  - Antimalwareové řešení
  - Firewall
- Správa aktualizací (včetně bezpečnostních)
- Inventarizace HW a SW

Tyto činnosti lze vykonávat za pomocí jednoho, nebo několika níže uvedených systémů a to v závislosti na konkrétní architektuře informačního systému:

- Skupinové politiky
- System Center Configuration Manager
- System Center Virtual Machine Manager
- Microsoft Intune

Cílem nasazení nástrojů centrální správy a řízení konfigurace je prosadit požadovaná bezpečnostní opatření, viz kapitola 10. do konkrétních technologií, zajistit monitorování správného nasazení realizovaných opatření a řešit případné nedostatky.

11.1.21 OFFICE 365 ADVANCED ENCRYPTION

Úroveň dosaženého stupně ochrany pro zajištění důvěrnosti dat nezáleží jen na způsobu šifrování dat. Neméně významným faktorem je správa šifrovacích klíčů. I když společnost Microsoft realizuje řadu opatření zamezujících neautorizovaný přístup k datům zákazníků, jako je například Customer LockBox (viz kapitola 11.1.14) je třeba zohlednit umístění šifrovacích klíčů, které jsou pro Office 365 Per-File Encryption uloženy v cloudu, viz kapitola 10.10.4 a dokument [5].

Toto omezení řeší Office 365 Advanced Encryption, které umožňuje zákazníkům kontrolovat přístup k šifrovacím klíčům a tyto klíče spravovat. Advanced Encryption zahrnuje:

- Oddělenou správu klíčů pro jednotlivé zákazníky
- Oddělení správy systému od dat zákazníků
- Správu přístupu ke klíčům ve výhradní moci zákazníka
- Použití vlastních on-premise generovaných klíčů (BYOK), viz dokument [58]
- Odebrání přístupu ke klíčům i pro vlastní služby Office 365 (i v případě ukončení služby)
- Customer LockBox

Více informací o Office 365 Advanced Encryption je uvedeno v dokumentu [5].

11.1.22 OFFICE 365 PER-FILE ENCRYPTION

Office 365 Per-File Encryption zajišťuje ochranu uložených dat v produktech Skype for Business, OneDrive for Business a SharePoint Online.

Princip šifrování dat při ukládání spočítá v šifrování souborů před jejich uložením do Azure Storage. Při přístupu k souboru jsou data po načtení z úložiště před odesláním uživateli dešifrovány. Azure Storage nemá schopnost dešifrovat, identifikovat nebo rozpoznat uložený obsah.

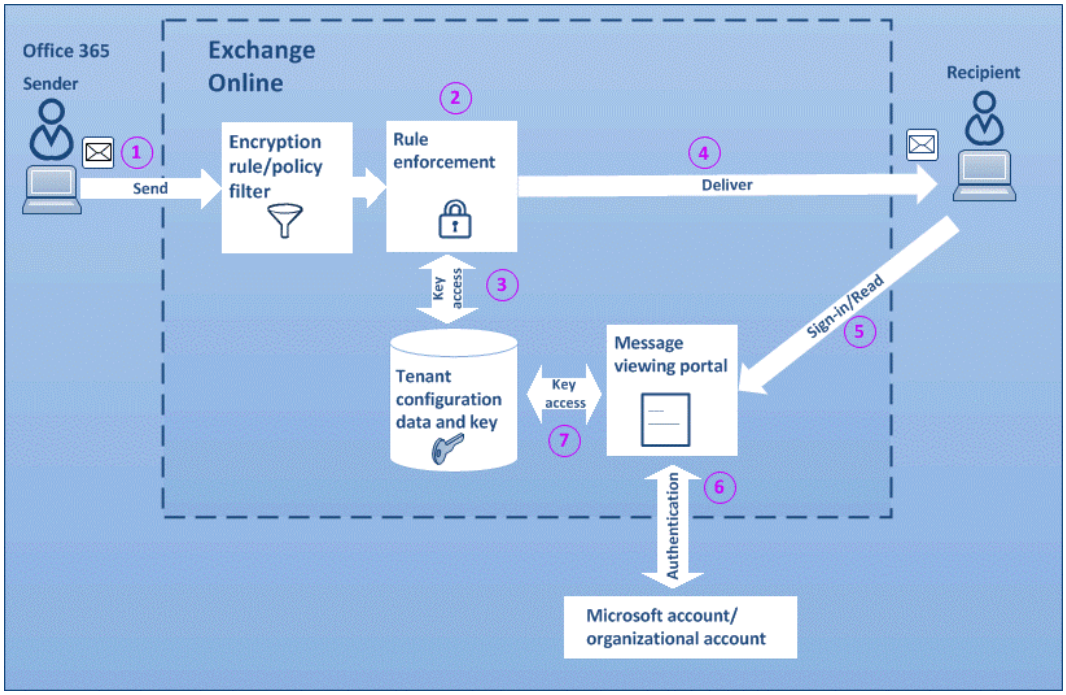
Detailní popis způsobu ochrany dat včetně použitých šifrovacích algoritmů a způsobu správy klíčů je uveden v dokumentu [5] a také v kapitole 10.10.4 tohoto dokumentu.

11.1.23 OFFICE 365 MESSAGE ENCRYPTION

Office 365 Message Encryption je nadstavba služby Exchange Online využívající pro šifrování mailů Azure RMS (viz [83]) :

- Šifrování mailů pomocí Azure RMS a transportních pravidel v Exchange Online umožňuje šifrovat celé maily libovolným příjemcům, i když nejsou schopni používat S/MIME nebo není znám jejich certifikát.
- Zašifrovaný mail má formát HTML formuláře, který musí příjemce zašifrovaného mailu nahrát na portál Office 365 kliknutím na odkaz, který je součástí HTML formuláře. Na portálu Office 365 je mail dešifrován a příjemci zobrazen. Příjemce je na portálu Office 365 autentizován svým účtem Microsoft, účtem organizace v Azure AD nebo pomocí jednorázového hesla zaslaného na mailovou adresu příjemce.
- Další možností pro čtení mailu je aplikace Office 365 Message Encryption Viewer (OME Viewer) určená pro mobilní aplikace, která zajistí nahrání HTML přílohy na portál Office 365 a následně zobrazení obsahu zašifrovaného mailu.
- Pokud uživatel na mail v rámci portálu Office 365 nebo OME Viewer odpoví, je odpověď také zašifrována, jako mailová adresa odesílatele je použita adresa Office365@messaging.microsoft.com, aby nedocházelo k problémům s klasifikací mailů jako spam v rámci protokolů SPF, DKIM a DMARC.

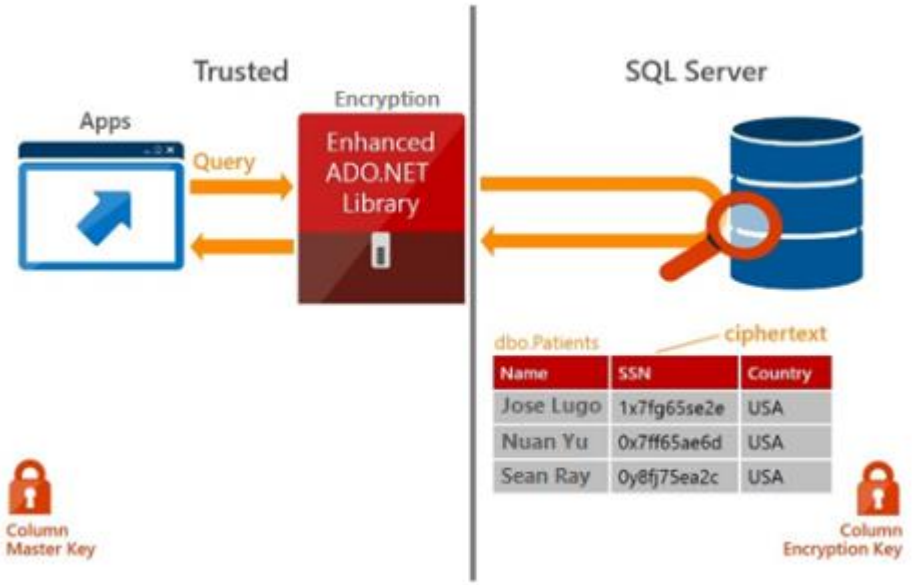
Obr. 22
Office 365 Message Encryption



11.1.24 SQL SERVER ALWAYS ENCRYPTED

Always Encrypted je vlastnost SQL databáze od verze SQL Serveru 2016, která umožňuje ochranu dat na úrovni sloupců SQL databáze. Data se šifrují v rámci klientské aplikace, šifrovací klíče se nikdy nedostávají do SQL serveru. Tím dochází pro takto chráněná data k oddělení vlastnictví dat od jejich správy.

Obr. 23
Schéma klíčů Always Encrypted [61]



Always Encrypted umožňuje použít algoritmus AEAD_AES_256_CBC_HMAC_SHA_256.

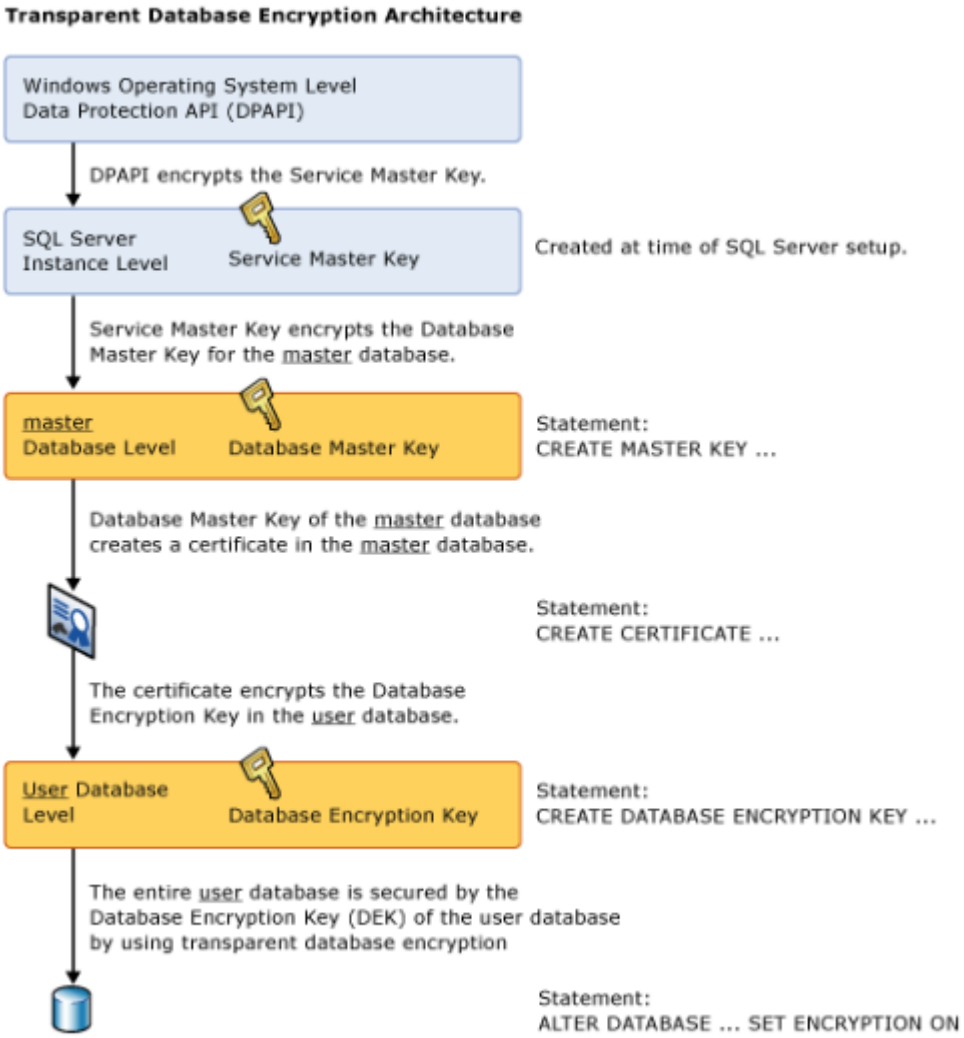
Více informací o technologii Always Encrypted je uvedeno v dokumentu [61].

11.1.25 SQL SERVER TRANSPARENT DATA ENCRYPTION (TDE)

Transparent Data Encryption šifruje databázové soubory v reálném čase. Tím je zajištěna ochrana dat uložených v databázi. Pro šifrování databáze se používá symetrický šifrovací klíč DEC. Tento klíč je zabezpečen pomocí certifikátu nebo asymetrických klíčů chráněných modulem Extensible Key Management (EKM), který umožňuje integraci s HSM moduly.

TDE umožňuje použít několik algoritmů: DES, 128-bit Triple DES, 192-bit Triple DES, RC2, RC4, 128-bit RC4, DESX, 128-bit AES, 192-bit AES, and 256-bit AES.

Obr. 24
Schéma architektury TDE



Transparent Data Encryption je podporováno i v Azure SQL Database, viz dokument [64] .TDE umožňuje integraci s Azure Key Vault, viz dokument [62].

Více informací o technologii Transparent Data Encryption je uvedeno v dokumentu [63].

11.2 POKRYTÍ POŽADAVKŮ NA OPATŘENÍ TECHNOLOGIEMI

V této kapitole jsou pro jednotlivé požadavky přílohy č. 1 Vyhlášky uvedena v tabulkách opatření (jednotlivé technologie včetně účelu jejich použití). Vyšší úrovně vždy předpokládají realizaci všech opatření nižších úrovní.

Technická opatření pro ochranu dat jsou zpracována pro tři úrovně definované ve Vyhlášce:

- **Střední úroveň:**
  - Vyžaduje řízení přístupu na všech úrovních – pro administraci, při komunikaci technologických komponent mezi sebou a pro přístup uživatelů ke službám.
  - Pro autentizaci administrátorů i uživatelů je využito Azure AD a federace s on-premise Active Directory pomocí ADFS, aby přihlašovací údaje (hashe hesel) nebyly uloženy ve službě Azure AD, protože databáze Azure AD je replikována i mimo území EU.
  - Není vyžadována vysoká dostupnost poskytovaných služeb – dostačují standardní mechanizmy zálohování a obnovy.
  - Vysoká dostupnost obsažená ve službe Office 365 převyšuje požadavky střední úrovně.
- **Vysoká úroveň:**
  - Musí být implementována všechna technická opatření pro střední úroveň a navíc:
  - Všechny přístupy musí být auditovány s centrálním zpracováním logů. Auditována musí být i historie změn.
  - Komunikace ve vnějších sítích musí být zašifrovány:
    - Přístupy ke službám z koncových zařízení přes veřejné sítě musí být zašifrovány pomocí TLS nebo VPN.
    - Z pohledu Vyhlášky jsou chápány virtuální sítě v datových centrech Microsoft Azure jako vnější síť, protože fyzická síťová infrastruktura není pod kontrolou provozovatele informačního systému a proto:
    - Soubory obsahující chráněné informace uložené ve virtuálních serverech nebo službách Microsoft Azure musí být zašifrovány, protože jsou přenášeny síťovou infrastrukturou datového centra Microsoft Azure do diskového úložiště bez kryptografické ochrany.
    - Komunikace na aplikační úrovni mezi virtuálními servery a cloudovými službami v rámci datového centra Microsoft Azure musí být zašifrovány pomocí TLS nebo VPN.
  - Je vyžadována vysoká dostupnost poskytovaných služeb, která vyžaduje manuální operace administrátorů pro obnovení provozu. Proto jsou využity služby Geo-Replikace dat do záložního datového centra Microsoft Azure, ve kterém může být provedena obnova provozu.
  - Vysoká dostupnost obsažená ve službe Office 365 převyšuje požadavky vysoké úrovně.

- **Kritická úroveň:**
  - Musí být implementována všechna technická opatření pro střední úroveň a navíc:
  - Striktní požadavek na identifikaci osob přistupující k aktivům informačního systému je podpořen více faktorovou autentizací uživatelů a administrátorů.
  - Požadavek na zabránění zneužití aktiv ze strany administrátorů musí být realizován na úrovni architektury informačního systému a organizačních opatření – klíčová je automatizovaná správa aplikačních klíčů pro Azure Storage a šifrování dat uložených v Azure Storage a SQL databázi již na straně klienta (aplikační server) s využitím Azure Key Vault oddělující správu systémů od vlastnictví dat a případně doplněný o BYOK. V prostředí Office 365 lze využít šifrování souborů a mailů s využitím Azure Key Vault a případně doplněný o BYOK.
  - Požadavek na zabránění zneužití aktiv ze strany administrátorů je realizován organizačními a technickými opatřeními v rámci služby Office 365 a jsou podpořeny využitím Azure Key Vault oddělující správu systémů od vlastnictví dat.
  - Speciální prostředky pro zajištění integrity dat a transakcí musí být realizovány na aplikační úrovni (například digitální podpis mailů pomocí S/MIME, digitální podpis souborů ukládaných do OneDrive for Bussiness a podobně).
  - Je vyžadována vysoká dostupnost poskytovaných služeb, s automatickým přepnutím provozu. Proto je informační systém redundantně rozmístěn do alespoň dvou datových center Microsoft Azure a využity služby replikace dat mezi datovými centry směrování síťového provozu z Internetu do funkčního datového centra.
  - Vysoká dostupnost obsažená ve službe Office 365 vyhovuje požadavkům kritické úrovně.

Technická opatření jsou rozdělena do třech oblastí podle Vyhlášky a každá z nich obsahuje tři výše zmíněné úrovně:

- Technická opatření pro zajištění důvěrnosti.
- Technická opatření pro zajištění integrity.
- Technická opatření pro zajištění důvěrnosti.

Na základě klasifikace informačního systému je pro každou oblast zvolena potřebná úroveň, například Důvěrnost – Vysoká, Integrita – Střední a Dostupnost – Kritická. V informačním systému pak musí být implementována technická opatření ze všech třech oblastí.

11.2.1 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DŮVĚRNOSTI

Pro tabulku Tab. 4 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 4 Technická opatření pro zajištění důvěrnosti

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
Microsoft Azure	Azure Resource Manager, viz 11.1.6. Azure AD, viz 11.1.1. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Konfigurace auditu a logování jednotlivých komponent. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4 nebo SQL Server Transparent Encryption, viz 11.1.25 a Azure Key Vault, viz 11.1.4. Šifrování komunikace mezi virtuálními servery a službami Azure s využitím protokolu TLS, viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Šifrování bloků dat (BLOB) ukládaných do Azure Storage na klientovi, viz 11.1.10 a Azure Key Vault, viz 11.1.4. SQL Server Always Encrypted pro SQL, viz 11.1.24. Více faktorová autentizace, viz 11.1.19.

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Office 365	Office 365 - přiřazení licencí, specifické uživatelské i administrátorské role a oprávnění. Azure AD, viz 11.1.1. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Office 365 Audit Log a audit na úrovni jednotlivých komponent Office 365. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4. Office 365 Message Encryption s Azure RMS a Azure Key Vault pro Exchange Online, viz 11.1.23 nebo End-to-End šifrování mailů pomocí S/MIME.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Office 365 Per-File Encryption pro SharePoint Online, Skype for Business a OneDrive for Business, viz 11.1.22. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. Více faktorová autentizace, viz 11.1.19.
Server on-premise	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Interní počítačová síť	Fyzická bezpečnost. Autentizace a autorizace koncového zařízení k portu sítě (802.1X). Řízení administrátorského přístupu k aktivním síťovým prvkům.	Audit přístupů na aktivních síťových prvcích. Šifrování bezdrátových sítí.	Audit provedených změn na aktivních síťových prvcích. Zabezpečení na úrovni aplikačních protokolů HTTP, SMTP a podobně pomocí TLS nebo šifrování pomocí IPSec nebo SMB, viz 11.1.18.
Veřejná počítačová síť	---	Zabezpečení na úrovni aplikačních protokolů HTTP, SMTP a podobně pomocí TLS nebo pomocí VPN.	Jako úroveň vysoká.

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Osobní počítač	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Notebook	Fyzická bezpečnost přístupu k zařízení. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací. BitLocker Drive Encryption, viz 11.1.13	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Mobilní telefon/tablet	Fyzická bezpečnost přístupu k zařízení. Přístup k zařízení zabezpečený pomocí hesla s resetem zařízení po neplatných pokusech o přihlášení.	Přístup k zařízení zabezpečený pomocí silného hesla nebo více faktorovou autentizací. Vzdálená správa mobilního zařízení, vynucení bezpečnostních politik – zamykání zařízení, délka hesla. Šifrování obsahu mobilního zařízení.	Kontejnerové oddělení aplikace od ostatních aplikací a dat (Microsoft Intune), oddělené šifrování a možnost vymazání dat.

11.2.2 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ INTEGRITY

Pro tabulku Tab. 5 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 5 Technická opatření pro zajištění integrity

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).
Microsoft Azure	Azure AD, viz 11.1.1. Azure Resource Manager, viz 11.1.6. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Konfigurace auditu a logování jednotlivých komponent. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4 nebo SQL Server Transparent Encryption, viz 11.1.25 a Azure Key Vault, viz 11.1.4. Šifrování komunikace mezi virtuálními servery a službami protokolem TLS, viz 10.10.4	Více faktorová autentizace, viz 11.1.19 Zajištění integrity dat je nutné řešit na aplikační úrovni.

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Office 365	Office 365 - přiřazení licencí, specifické uživatelské i administrátorské role a oprávnění. Azure AD, viz 11.1.1 Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Office 365 Audit Log a audit na úrovni jednotlivých komponent Office 365. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4. Office 365 Message Encryption s Azure RMS a Azure Key Vault pro Exchange Online, viz 11.1.23 nebo End-to-End šifrování mailů pomocí S/MIME.	Customer LockBox viz 11.1.14. Více faktorová autentizace, viz 11.1.19 End-to-End podepisování mailů pomocí S/MIME. Zajištění integrity dat je nutné řešit na aplikační úrovni – například podepisování dokumentů digitálním podpisem (Microsoft Office, Acrobat Reader).
Server on-premise	Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání změn – bezpečnostní logy a logy aplikací, řízení změn proces.	Více faktorová autentizace, viz 11.1.19 Zajištění integrity dat je nutné řešit na aplikační úrovni.
Interní počítačová síť	Fyzická bezpečnost. Autentizace a autorizace k portu sítě (802.1X). Řízení administrátorského přístupu k aktivním síťovým prvkům.	Audit přístupů na aktivních síťových prvcích. Audit provedených změn na aktivních síťových prvcích. Šifrování bezdrátových sítí.	Více faktorová autentizace pro aktivní síťové prvky, viz 11.1.19.
Veřejná počítačová síť	---	Zabezpečení na úrovni aplikačních protokolů HTTP, SMTP a podobně pomocí TLS nebo pomocí VPN.	Stejná opatření jako pro úroveň vysoká.

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Osobní počítač	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Bezpečnostní logy a logy aplikací.	Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni.
Notebook	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Bezpečnostní logy a logy aplikací. BitLocker Drive Encryption, viz 11.1.13.	Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni.
Mobilní telefon/tablet	Fyzická bezpečnost přístupu k zařízení. Přístup k zařízení zabezpečený pomocí hesla s resetem zařízení po neplatných pokusech o přihlášení.	Přístup k zařízení zabezpečený pomocí silného hesla Vzdálená správa mobilního zařízení, vynucení bezpečnostních politik – zamykání zařízení, délka hesla. Šifrování obsahu mobilního zařízení.	Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni.

11.2.3 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DOSTUPNOSTI

Pro tabulku Tab. 6 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 6 Technická opatření pro zajištění dostupnosti

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.
Microsoft Azure	Dostupnost dat a služby na této úrovni je vestavěná do jednotlivých služeb Microsoft Azure, viz kapitola 10.11.4. Azure Backup, viz 11.1.2	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci jednoho datového centra Microsoft Azure. Geo-replikace dat do záložního datového centra Microsoft Azure, ve kterém je možné provést obnovu informačního systému.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci alespoň dvou datových center Microsoft Azure s využitím Geo-Replikace. Azure Trafic Manager, viz 11.1.11.
Office 365	Dostupnost dat a služby na této úrovni je vestavěná do jednotlivých služeb Office 365, viz kapitola 10.11.4.	Dostupnost dat a služby na této úrovni je vestavěná do jednotlivých služeb Office 365, viz kapitola 10.11.4.	Dostupnost dat a služby na této úrovni je vestavěná do jednotlivých služeb Office 365, viz kapitola 10.11.4.
Server on-premise	Zálohování a obnova dat a konfigurací.	Centralizovaný zálohovací systém, záloha a obnova serverů, dat a konfigurací. Záložní datové centrum s manuálním nebo asistovaným převedením provozu – volitelně Azure Site Recovery, viz.11.1.9	Záložní datové centrum s redundancí na úrovni serverů, replikací dat mezi datovými centry a automatickým přepnutím provozu.

Komponenta modelu IS	Úroveň střední	Úroveň vysoká	Úroveň kritická
Interní počítačová síť	Záloha konfigurace aktivních síťových prvků.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění aktivního síťového prvku v požadovaném čase.	Redundantní aktivní síťové prvky, konfigurace s automatickým řešením výpadku nebo poruchy sítě.
Veřejná počítačová síť	---.	Záložní připojení k Internetu. Manuální převedení síťového provozu na záložní připojení k Internetu.	Zdvojené síťové připojení k Internetu, optimálně k různým ISP. Automatické směrování síťového provozu přes dostupné připojení k Internetu.
Osobní počítač	Záloha uživatelských dat a uživatelského profilu na externí zašifrované médium nebo umístění uživatelských dat a uživatelského profilu na serveru.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění počítače v požadovaném čase.	Sada počítačů ve skladu, připravená k výměně za porouchaný kus.
Notebook	Záloha uživatelských dat a uživatelského profilu na externí zašifrované médium nebo umístění uživatelských dat a uživatelského profilu na serveru.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění počítače v požadovaném čase.	Sada počítačů ve skladu, připravená k výměně za porouchaný kus.
Mobilní telefon/tablet	Zálohování dat na aplikační úrovni.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění mobilního zařízení v požadovaném čase.	Sada mobilních zařízení ve skladu, připravená k výměně za porouchaný kus.

12 NÁVRH OCHRANY DAT

V kapitolách 13 - 15 jsou pro vybrané scénáře předloženy návrhy implementace bezpečnostních opatření, které zajistí soulad s požadavky legislativy (Zákon a Vyhláška). Tato opatření jsou navrhována pro cloudové služby Microsoft Online Services (Microsoft Azure a Office 365), počítačové sítě (interní i veřejné), a koncová uživatelská zařízení (osobní počítače PC, chytré mobilní telefony a tablety). Návrh opatření je v dotčených případech škálován podle úrovně důležitosti aktiv, viz příloha č. 1 Vyhlášky. Vychází z tabulek uvedených v kapitole 11.2, vybírá z nich opatření relevantní pro daný scénář a komponentu a navíc přidává doplňková opatření pro zvýšení úrovně bezpečnosti ve specifických případech.

Technická opatření (např. nástroje jako firewall nebo IPS) navržená v následujících kapitolách budou, stejně jako téměř všechna technická opatření, muset být podporována organizačními opatřeními ve formě pravidel a procesů (např. správy uživatelů, údržby, aktualizace, správy incidentů). Uvedená organizační opatření budou ve většině případů společná pro více technických opatření a budou ukotvena v podobě bezpečnostních politik nebo návazných bezpečnostních standardů.

Konkrétní typ organizačního opatření bude dán typem souvisejících technických opatření, přičemž se až na výjimky bude jednat o jedno z organizačních opatření uvedených v kapitole 8. Z důvodu zvýšení přehlednosti dokumentu nebudou tato organizační opatření znovu uváděna – v této a následujících kapitolách proto implicitně platí, že uvedená technická opatření jsou podporována jedním nebo více organizačními opatřeními, bez kterých je přínos technických opatření omezený nebo přímo žádný.

13 DATABÁZOVÉ SYSTÉMY

V této kapitole je předložen návrh bezpečnostních opatření pro pokrytí požadavků Zákona a Vyhlášky pro databázové systémy.

13.1 SCÉNÁŘ

Scénář databázové systémy zahrnuje serverové služby umístěné v Microsoft Azure:

- Databázový systém
  - Varianta A: PaaS služba Azure SQL Database
    - SQL server poskytovaný jako služba v rámci Microsoft Azure
    - Online transakční databáze
    - Vysoká dostupnost
  - Varianta B: Microsoft SQL Server provozovaný jako virtuální server v rámci Azure IaaS
    - Online transakční databáze
    - Business inteligence
    - Vysoká dostupnost
- Aplikační systémy
  - Varianta A: PaaS služba Azure App Service
  - Varianta B: Aplikační a webové servery provozované jako virtuální servery v rámci Azure IaaS
- Azure Active Directory
  - Autorizace uživatelů a administrátorů
- Active Directory Domain Services + ADFS on-premise v interní síti
  - Autentizace uživatelů a administrátorů
- Active Directory Domain Services on-premise v Azure IaaS
  - Správa virtuálních serverů provozovaných v Azure IaaS
- Azure HDInsight
  - Sběr a vyhodnocení auditních logů v rámci Microsoft Azure.
- Virtuální sítě informačního systému umístěné v Microsoft Azure
  - Z pohledu Vyhlášky jsou chápány jako vnější síť, protože fyzická síťová infrastruktura není pod kontrolou provozovatele databázového systému.

V rámci tohoto scénáře jsou serverové služby v Microsoft Azure využívány z klientských zařízení (osobní počítače, notebooky, mobilní telefony a tablety a další) pomocí webového přístupu přes Internet; nepředpokládá se ukládání dat na klientských zařízeních.

13.2 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DŮVĚRNOSTI

Pro tabulku Tab. 7 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 7 Technická opatření pro zajištění důvěrnosti

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
PaaS služba Azure SQL Database	Řízení přístupu na úrovni správy Azure SQL Database - Azure Resource Manager a Azure Subscription. Řízení přístupu – autentizace SQL účty nebo pomocí Azure AD, autorizace pomocí SQL rolí [74]. Dynamic Data Masking [73].	Azure SQL Database Auditing [74]. Azure Security and Audit Log Management, viz 11.1.8. SQL Server Transparent Data Encryption, viz 11.1.25 a Azure Key Vault, viz 11.1.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Microsoft SQL Server v Azure IaaS	Řízení přístupu na úrovni správy virtuálního serveru – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu na úrovni SQL serveru – autentizace SQL účty nebo pomocí Azure AD, autorizace pomocí SQL rolí [74]. Dynamic Data Masking [73].	Auditování na úrovni operačního serveru VM a SQL Serveru. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4 nebo SQL Server Transparent Data Encryption, viz 11.1.25 a Azure Key Vault, viz 11.1.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).
Azure App Service	Řízení přístupu na úrovni správy Azure App Service - Azure Resource Manager a Azure Subscription. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1.	Auditování na úrovni aplikace. Azure Security and Audit Log Management, viz 11.1.8. Šifrování komunikace s SQL serverem a mezi aplikačními a webovými servery a poskytovaných služeb pomocí TLS, viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Šifrování bloků dat (BLOB) ukládaných do Azure Storage na klientovi, viz 11.1.10 a Azure Key Vault, viz 11.1.4. SQL Always Encrypted, viz 11.1.24 a Azure Key Vault, viz 11.1.4.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Aplikační a webové servery v Azure IaaS	Řízení přístupu na úrovni správy virtuálního serveru – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1.	Auditování na úrovni operačního systému VM a aplikace. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4. Šifrování komunikace s SQL serverem a mezi aplikačními a webovými servery a poskytovaných služeb pomocí TLS nebo IPsec, viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Šifrování bloků dat (BLOB) ukládaných do Azure Storage na klientovi, viz 11.1.10 a Azure Key Vault, viz 11.1.4. SQL Always Encrypted, viz 11.1.24 a Azure Key Vault, viz 11.1.4.
Azure AD	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure AD pomocí Azure AD. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Azure AD Audit Reports, viz [89]. Azure Security and Audit Log Management, viz 11.1.8.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Více faktorová autentizace, viz 11.1.19.
Active Directory v Azure IaaS	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS.	Auditování Active Directory. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Azure HDInsight	---	Řízení přístupu na úrovni správy Azure HDInsight – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure HDInsight pomocí Azure AD. Azure Security and Audit Log Management, viz 11.1.8.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).
Server on-premise	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Virtuální sítě informačního systému umístěné v Microsoft Azure	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu na úrovni IP komunikace pomocí Azure Network Security Groups, viz [83].	Site-to-Site VPN mezi datovými centry Microsoft Azure, viz 11.1.12.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).
Síťové spojení mezi Microsoft Online Services a klientskými zařízeními	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu ke službám na úrovni Azure Load Balancer, viz [88]	Šifrování poskytovaných služeb pomocí TLS, viz 10.10.4. nebo Point-to-Site VPN přístupy z klientských zařízení, viz 11.1.12 nebo Site-to-Site VPN mezi datovým centrem Microsoft Azure a interní sítí, viz 11.1.12 nebo Express Route + VPN, viz 11.1.15	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

13.3 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ INTEGRITY

Pro tabulku Tab. 8 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 8 Technická opatření pro zajištění integrity

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).
PaaS služba Azure SQL Database	Řízení přístupu na úrovni správy virtuálního serveru – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu na úrovni SQL serveru – autentizace SQL účty nebo pomocí Azure AD, autorizace pomocí SQL rolí [74]. Dynamic Data Masking [73].	SQL Server Data Changes (DML) pro logování historie změn v SQL databázi, viz [90]. Azure SQL Database Auditing [74]. Azure Security and Audit Log Management, viz 11.1.8. SQL Server Transparent Encryption, viz 11.1.25 a Azure Key Vault, viz 11.1.4.	Ochrana integrity transakcí musí být zajištěna na aplikační úrovni (například digitální podpis transakcí).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Microsoft SQL Server v Azure IaaS	Řízení přístupu na úrovni správy virtuálního serveru – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu na úrovni SQL serveru – autentizace SQL účty nebo pomocí Azure AD, autorizace pomocí SQL rolí [74]. Dynamic Data Masking [73].	Auditování na úrovni operačního serveru VM a SQL Serveru. SQL Server Data Changes (DML) pro logování historie změn v SQL databázi, viz [90]. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4 nebo SQL Server Transparent Encryption, viz 11.1.25 a Azure Key Vault, viz 11.1.4.	Ochrana integrity transakcí musí být zajištěna na aplikační úrovni (například digitální podpis transakcí).
Azure App Service	Řízení přístupu na úrovni správy Azure App Service - Azure Resource Manager a Azure Subscription. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1.	Auditování na úrovni aplikace včetně zaznamenání historie změn. Azure Security and Audit Log Management, viz 11.1.8. Šifrování komunikace s SQL serverem a mezi aplikačními a webovými servery pomocí TLS, viz 10.10.4.	Ochrana integrity transakcí musí být zajištěna na aplikační úrovni (například digitální podpis transakcí).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Aplikační a webové servery v Azure IaaS	Řízení přístupu na úrovni správy virtuálního serveru – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS. Řízení přístupu na úrovni uložení dat – aplikační klíče Azure Storage s nastavenými oprávněními, viz 11.1.10. Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1.	Auditování na úrovni operačního systému VM. Auditování na úrovni aplikace včetně zaznamenání historie změn. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4. Šifrování komunikace s SQL serverem a mezi aplikačními a webovými servery pomocí TLS nebo IPsec.	Ochrana integrity transakcí musí být zajištěna na aplikační úrovni (například digitální podpis transakcí).
Azure AD	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure AD pomocí Azure AD. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Azure AD Audit Reports, viz [89]. Azure Security and Audit Log Management, viz 11.1.8.	Více faktorová autentizace, viz 11.1.19.
Active Directory v Azure IaaS	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k VM pomocí AD v Azure IaaS.	Auditování Active Directory. Azure Security and Audit Log Management, viz 11.1.8. Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4.	Jako pro úroveň vysoká.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Azure HDInsight	---	Řízení přístupu na úrovni správy Azure HDInsight – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure HDInsight pomocí Azure AD. Azure Security and Audit Log Management, viz 11.1.8.	Jako pro úroveň vysoká.
Server on-premise	Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání změn – bezpečnostní logy a logy aplikací včetně změn.	Více faktorová autentizace, viz 11.1.19 Zajištění integrity dat je nutné řešit na aplikační úrovni.
Virtuální sítě informačního systému umístěné v Microsoft Azure	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu na úrovni IP komunikace pomocí Azure Network Security Groups, viz [83].	Site-to-Site VPN mezi datovými centry Microsoft Azure, viz 11.1.12	Jako pro úroveň vysoká.
Síťové spojení mezi Microsoft Online Services a klientskými zařízeními	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu ke službám na úrovni Azure Load Balancer, viz [88]	Šifrování poskytovaných služeb pomocí TLS, viz 10.10.4. nebo Point-to-Site VPN přístupy z klientských zařízení, viz 11.1.12 nebo Site-to-Site VPN mezi datovým centrem Microsoft Azure a interní sítí, viz 11.1.12 nebo Express Route + VPN, viz 11.1.15	Jako pro úroveň vysoká.

13.4 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DOSTUPNOSTI

Pro tabulku Tab. 9 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 9 Technická opatření pro zajištění dostupnosti

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.
PaaS služba Azure SQL Database	Pro zálohování a obnovu využít Point In Time Restore, viz [80].	Pro zálohování a obnovu využít Geo-Restore, viz [80].	Pro zálohování a obnovu využít Standard nebo Active Geo-Replication, viz [80].
Microsoft SQL Server v Azure IaaS	Azure Backup, viz 11.1.2.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci jednoho datového centra Microsoft Azure. SQL Mirroring, viz [81].	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci alespoň dvou datových center Microsoft Azure s využitím Geo-Replikace. SQL AlwaysOn Availability Groups, viz [81].
Azure App Service	Dostupnost dat a služby na této úrovni je vestavěná v Azure App Service.	Dostupnost dat a služby na této úrovni je vestavěná v Azure App Service.	Redundantní instance ve dvou datových centrech Microsoft Azure, viz [79].
Aplikační a webové servery v Azure IaaS	Azure Backup, viz 11.1.2.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci jednoho datového centra Microsoft Azure.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci alespoň dvou datových center Microsoft Azure s využitím Geo-Replikace.
Azure AD	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Active Directory v Azure IaaS	Azure Backup, viz 11.1.2.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci jednoho datového centra Microsoft Azure.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci alespoň dvou datových center Microsoft Azure s využitím Geo-Replikace.
Azure HDInsight	---	Dostupnost dat a služby na této úrovni je vestavěná.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci alespoň dvou datových center Microsoft Azure s využitím Geo-Replikace.
Server on-premise	Zálohování a obnova dat a konfigurací	Redundantní implementace on-premise Active Directory a ADFS s vysokou dostupností.	Geo-Redundantní implementace on-premise Active Directory a ADFS s vysokou dostupností.
Virtuální sítě informačního systému umístěné v Microsoft Azure	Dostupnost dat a služby na této úrovni je vestavěná v Microsoft Azure.	Dostupnost dat a služby na této úrovni je vestavěná v Microsoft Azure.	Dostupnost dat a služby na této úrovni je vestavěná v Microsoft Azure.
Síťové spojení mezi Microsoft Online Services a klientskými zařízeními	---	Přístupu ke službám pomocí Azure Load Balancer, viz [88]. Záložní připojení k Internetu pro klientská zařízení.	Redundantní služby v alespoň dvou datových centrech Microsoft Azure. Azure Traffic Manager, viz 11.1.11.

13.5 TECHNICKÁ OPATŘENÍ NEZÁVISLÁ NA KLASIFIKACI DAT

Pro ochranu aktiv informačního systému je kromě opatření uvedených v příloze č. 1 Vyhlášky nutné realizovat i technická opatření nezávislá na klasifikaci dat (§16 – §27 Vyhlášky). Konkrétní požadavky na tato technická opatření vyplynou z analýzy rizik, viz kapitola 8.

Níže uvedená opatření jsou konkretizací opatření uvedených v kapitole 10 do formy relevantní pro daný scénář a komponentu:

- Nástroj pro ochranu integrity komunikačních sítí, viz kapitola 10.2
  - Pro řízení bezpečného přístupu mezi vnější a vnitřní sítí v datovém centru Microsoft Azure je k dispozici služba Azure Load Balancer (viz [88]) a Azure Network Security Groups (viz [83]). Dále je možné využít firewally třetích stran provozované v Azure IaaS, například Barracuda NextGen Firewall, Cicso ASAv nebo Fortinet FortiGate NGFW.
  - Segmentace sítě v rámci datového centra Microsoft Azure s využitím Azure Network Security Groups (viz [83]) pro řízení přístupu do jednotlivých segmentů sítě a k jednotlivým virtuálním serverům.
  - Azure VPN Gateway (viz 11.1.12) pro vzdálený přístup a správu pomocí zašifrované VPN.
  - Systém COSMOS (viz 10.8.4), který je součástí MCIO, slouží i pro blokování neoprávněného síťového provozu.
- Nástroj pro ochranu před škodlivým kódem, viz kapitola 10.5
  - Microsoft Antimalware for Azure Cloud Services and Virtual Machines, viz [23] je určený pro virtuální servery s operačním systémem Windows provozovaným v Azure IaaS.
  - Dále je možné pro ochranu před škodlivým kódem využít řadu produktů třetích stran, které jsou k dipozici v Azure Marketplace.
- Nástroj pro detekci kybernetických událostí, viz kapitola 10.7
  - Pro Microsoft Azure poskytuje tento typ ochrany MCIO, viz kapitola 10.7.4
  - Dále je možné využít firewally třetích stran se zabudovanou funkcionalitou IDS/IPS, které jsou dostupné na Azure Marketplace.
- Nástroj pro sběr a vyhodnocení kybernetických událostí, viz kapitola 10.8
  - Systém COSMOS (viz 10.8.4), který je součástí MCIO, sbírá a vyhdonocuje kybernetické události vznikající v rámci MCIO.
  - Pro sběr a vyhodnocení událostí vznikajících ve virtuálních serverech v rámzi Azure Iaas a službách v rámci Azure PaaS v rozsahu požadovaném pro VIS lze využít službu Azure HDInsight. Pro vyhodnocení událostí v rozsahu požadovaném pro KII je nutné využít SIEM řešení třetí strany, do kteréhu budou exportovány události sebrané pomocí Azure HDInsight.
- Aplikační bezpečnost, viz kapitola 10.9
  - Vlastní aplikace není součástí scénáře, je však nutné pro její vývoj, nasazení a provoz aplikace splnit požadavky §24 Vyhlášky.

14 OFFICE 365

V této kapitole je předložen návrh bezpečnostních opatření pro pokrytí požadavků Zákona a Vyhlášky pro informační systém, který zahrnuje poštovní systém, systém pro skupinovou spolupráci, repositář dokumentů, hlasové a video konference v rámci SaaS služeb Office 365.

14.1 SCÉNÁŘ

Scénář poštovní systém, systém pro skupinovou spolupráci, repositář dokumentů, hlasové a video konference – při použití Microsoft Office 365 jako SaaS cloudu zahrnuje:

- Office 365
  - Exchange Online
    - Poštovní systém
  - Sharepoint Online
    - Systém pro skupinovou spolupráci
  - OneDrive for Business
    - Repositář dokumentů
  - Skype for Business Online
    - Hlasové a video konference
- Azure Active Directory
  - Autorizace uživatelů a administrátorů
- Azure HDInsight
  - Sběr a vyhodnocení auditních logů v rámci Microsoft Azure.
- Active Directory Domain Services (on-premise AD) + ADFS
  - Autentizace uživatelů a administrátorů
- Interní síť organizace
- Síťové spojení mezi Microsoft Online Services a interní sítí organizace
- Síťové spojení mezi Microsoft Online Services a klientskými zařízeními v Internetu
- Klientská zařízení (osobní počítače, notebooky, mobilní telefony a tablety a další)

14.2 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DŮVĚRNOSTI

Pro tabulku Tab. 10 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 10 Technická opatření pro zajištění důvěrnosti

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
Exchange Online	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. RBAC pro uživatele z Azure AD.	Office 365 Audit Log a audit na úrovni Exchange Online. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4 Office 365 Message Encryption s Azure RMS pro Exchange Online, viz 11.1.23 nebo End-to-End šifrování mailů pomocí S/MIME.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. Více faktorová autentizace, viz 11.1.19.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
OneDrive for Business	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. Řízení přístupu pro uživatele a skupiny z Azure AD nebo pro vestavěné role na úrovni knihoven a položek.	Office 365 Audit Log a audit na úrovni OneDrive for Business. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Více faktorová autentizace, viz 11.1.19. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. nebo Office 365 Per-File Encryption pro SharePoint Online, Skype for Business a OneDrive for Business, viz 11.1.22.
Sharepoint Online	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. Řízení přístupu pro uživatele a skupiny z Azure AD nebo pro vestavěné role na úrovni webů, seznamů, knihoven a položek.	Office 365 Audit Log a audit na úrovni Sharepoint Online. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Více faktorová autentizace, viz 11.1.19. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. nebo Office 365 Per-File Encryption pro SharePoint Online, Skype for Business a OneDrive for Business, viz 11.1.22.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Skype for Business Online	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. Řízení přístupu pro uživatele na úrovni konference.	Office 365 Audit Log a audit na úrovni Skype for Business Online. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Více faktorová autentizace, viz 11.1.19. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21.
Azure AD	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure AD pomocí Azure AD. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Azure AD Audit Reports, viz [89]. Azure Security and Audit Log Management, viz 11.1.8.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Více faktorová autentizace, viz 11.1.19.
Azure HDInsight	---	Řízení přístupu na úrovni správy Azure HDInsight – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure HDInsight pomocí Azure AD. Azure Security and Audit Log Management, viz 11.1.8.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).
Síťové spojení mezi Microsoft Online Services a klientskými zařízeními	---	Šifrování poskytovaných služeb pomocí TLS, viz 10.10.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Server on-premise	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Interní počítačová síť	Fyzická bezpečnost. Autentizace a autorizace koncového zařízení k portu sítě (802.1X). Řízení administrátorského přístupu k aktivním síťovým prvkům.	Audit přístupů na aktivních síťových prvcích. Šifrování bezdrátových sítí.	Audit provedených změn na aktivních síťových prvcích. Zabezpečení na úrovni aplikačních protokolů HTTP, SMTP a podobně pomocí TLS nebo šifrování pomocí IPSec nebo SMB, viz 11.1.18.
Osobní počítač	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Notebook	Fyzická bezpečnost přístupu k zařízení. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací. BitLocker Drive Encryption, viz 11.1.13	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Mobilní telefon/tablet	Fyzická bezpečnost přístupu k zařízení. Přístup k zařízení zabezpečený pomocí hesla s resetem zařízení po neplatných pokusech o přihlášení.	Přístup k zařízení zabezpečený pomocí silného hesla nebo více faktorovou autentizací. Vzdálená správa mobilního zařízení, vynucení bezpečnostních politik – zamykání zařízení, délka hesla. Šifrování obsahu mobilního zařízení.	Kontejnerové oddělení aplikace od ostatních aplikací a dat (Microsoft Intune), oddělené šifrování a možnost vymazání dat.

14.3 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ INTEGRITY

Pro tabulku Tab. 11 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 11 Technická opatření pro zajištění integrity

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).
Exchange Online	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. RBAC pro uživatele z Azure AD.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Office 365 Audit Log a audit na úrovni Exchange Online. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4. Office 365 Message Encryption s Azure RMS pro Exchange Online, viz 11.1.23 nebo End-to-End šifrování mailů pomocí S/MIME.	Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. Více faktorová autentizace, viz 11.1.19.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
OneDrive for Business	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. Řízení přístupu pro uživatele a skupiny z Azure AD nebo pro vestavěné role na úrovni knihoven a položek.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Office 365 Audit Log a audit na úrovni OneDrive for Business. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4.	Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni – například podepisování dokumentů digitálním podpisem (Microsoft Office, Acrobat Reader).
Sharepoint Online	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. Řízení přístupu pro uživatele a skupiny z Azure AD nebo pro vestavěné role na úrovni webů, seznamů, knihoven a položek.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Office 365 Audit Log a audit na úrovni Sharepoint Online. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4..	Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni – například podepisování dokumentů digitálním podpisem (Microsoft Office, Acrobat Reader).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Skype for Business Online	Evidence přiřazení účtů/licence konkrétním osobám v Azure AD (organizační opatření). Řízení přístupu k poskytovaným službám – Azure AD, viz 11.1.1. Řízení přístupu pro uživatele na úrovni konference.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Office 365 Audit Log a audit na úrovni Skype for Business Online. Azure Security and Audit Log Management, viz 11.1.8. TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.10.4.	Customer LockBox viz 11.1.14, COSMOS viz 10.8.4. Office 365 Advanced Encryption s Azure Key Vault, viz 11.1.21. Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni – například podepisování dokumentů digitálním podpisem (Microsoft Office, Acrobat Reader).
Azure AD	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure AD pomocí Azure AD. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Azure AD Audit Reports, viz [89]. Azure Security and Audit Log Management, viz 11.1.8.	Více faktorová autentizace, viz 11.1.19.
Azure HDInsight	---	Řízení přístupu na úrovni správy Azure HDInsight – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure HDInsight pomocí Azure AD. Azure Security and Audit Log Management, viz 11.1.8.	Jako pro úroveň vysoká.
Síťové spojení mezi Microsoft Online Services a klientskými zařízeními	---	Šifrování poskytovaných služeb pomocí TLS, viz 10.10.4.	Jako pro úroveň vysoká.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Server on-premise	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Více faktorová autentizace, viz 11.1.19 Zajištění integrity dat je nutné řešit na aplikační úrovni.
Interní počítačová síť	Fyzická bezpečnost. Autentizace a autorizace k portu sítě (802.1X). Řízení administrátorského přístupu k aktivním síťovým prvkům.	Audit přístupů na aktivních síťových prvcích. Audit provedených změn na aktivních síťových prvcích. Šifrování bezdrátových sítí.	Více faktorová autentizace pro aktivní síťové prvky, viz 11.1.19.
Osobní počítač	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni.
Notebook	Fyzická bezpečnost přístupu k zařízení. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací. BitLocker Drive Encryption, viz 11.1.13	Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni.
Mobilní telefon/tablet	Fyzická bezpečnost přístupu k zařízení. Přístup k zařízení zabezpečený pomocí hesla s resetem zařízení po neplatných pokusech o přihlášení.	Přístup k zařízení zabezpečený pomocí silného hesla nebo více faktorovou autentizací. Vzdálená správa mobilního zařízení, vynucení bezpečnostních politik – zamykání zařízení, délka hesla. Šifrování obsahu mobilního zařízení.	Více faktorová autentizace, viz 11.1.19. Zajištění integrity dat je nutné řešit na aplikační úrovni.

14.4 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DOSTUPNOSTI

Pro tabulku Tab. 12 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 12 Technická opatření pro zajištění dostupnosti

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.
Office 365 – společné pro všechny služby	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.
Exchange Online	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.
Sharepoint Online	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.
OneDrive for Business	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.
Skype for Business Online	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.	Dostupnost dat a služby na této úrovni je vestavěná v Office 365.
Azure AD	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.
Azure HDInsight	---	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Architektura s využitím principů Azure Business Continuity, viz [78] v rámci alespoň dvou datových center Microsoft Azure s využitím Geo-Replikace.

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Síťové spojení mezi Microsoft Online Services a klientskými zařízeními	---	Záložní připojení k Internetu pro klientská zařízení.	Jako pro úroveň vysoká.
Server on-premise	Zálohování a obnova dat a konfigurací	Redundantní implementace on-premise Active Directory a ADFS s vysokou dostupností.	Geo-Redundantní implementace on-premise Active Directory a ADFS s vysokou dostupností.
Interní počítačová síť	Záloha konfigurace aktivních síťových prvků.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění aktivního síťového prvku v požadovaném čase.	Redundantní aktivní síťové prvky, konfigurace s automatickým řešením výpadku nebo poruchy sítě.
Osobní počítač	Záloha uživatelských dat a uživatelského profilu na externí zašifrované médium nebo umístění uživatelských dat a uživatelského profilu na serveru.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění počítače v požadovaném čase.	Sada počítačů ve skladu, připravená k výměně za porouchaný kus.
Notebook	Záloha uživatelských dat a uživatelského profilu na externí zašifrované médium nebo umístění uživatelských dat a uživatelského profilu na serveru.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění počítače v požadovaném čase.	Sada počítačů ve skladu, připravená k výměně za porouchaný kus.
Mobilní telefon/tablet	Zálohování dat na aplikační úrovni.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění mobilního zařízení v požadovaném čase.	Sada mobilních zařízení ve skladu, připravená k výměně za porouchaný kus.

14.5 TECHNICKÁ OPATŘENÍ NEZÁVISLÁ NA KLASIFIKACI DAT

Pro ochranu aktiv informačního systému je kromě opatření uvedených v příloze č. 1 Vyhlášky nutné realizovat i technická opatření nezávislá na klasifikaci dat (§16 – §27 Vyhlášky). Konkrétní požadavky na tato technická opatření vyplynou z analýzy rizik, viz kapitola 8.

Níže uvedená opatření jsou konkretizací opatření uvedených v kapitole 10 do formy relevantní pro daný scénář a komponentu:

- Nástroj pro detekci kybernetických událostí, viz kapitola 10.7, který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní a vnější sítí
  - Pro Office 365 poskytuje tento typ ochrany MCIO, viz kapitola 10.7.4
- Nástroj pro sběr a vyhodnocení kybernetických událostí, viz kapitola 10.8
  - Systém COSMOS (viz 10.8.4), který je součástí MCIO, sbírá a vyhdonocuje kybernetické události vznikající v rámci MCIO.
  - Pro sběr a vyhodnocení událostí vznikajících ve virtuálních serverech v rámzi Office 365 v rozsahu požadovaném pro VIS lze využít službu Azure HDInsight. Pro vyhodnocení edálostí v rozsahu požadovaném pro KII je nutné využít SIEM řešení třetí strany, do kteréhu budou exportovány události sebrané pomocí Azure HDInsight.
- Aplikační bezpečnost, viz kapitola 10.9
  - Vývoj Office 365 je realizován prostřednictvím procesu Bezpečný vývojový životní cyklus (Security Development Lifecycle), viz kapitola 10.9.4
  - Office 365 může být rozšířen o další aplikace nebo komponenty, jako například SharePoint Web Part, při jejichž vývoji, nasazení a provozu je nutné splnit požadavky §24 Vyhlášky.
- Zabezpečení koncových stanic:
  - Koncové stanice musí být evidovány a spravovány a musí být řízena jejich bezpečnost.
  - Musí být řízen přístup ke koncovým zařízením a k aplikacím na nich provozovaných.
  - I v případě, že se na koncových zařízeních neukládají data informačních systémů, musí být vyřešena ochrana zbytkových informací (dočasné soubory, keše a podobně) v případě, že je vyžadována ochrana dat pomocí kryptografických prostředků.

15 ZÁLOŽNÍ DATOVÉ CENTRUM

V této kapitole je předložen návrh bezpečnostních opatření pro pokrytí požadavků Zákona a Vyhlášky pro záložní datové centrum.

V případě obnovy informačního systému do Microsoft Azure musí být v rámci Microsoft Azure implementována opatření podle klasifikace informačního systému.. Vzhledem k tomu, že součástí tohoto scénáře není popis vlastního informačního systému, který je zálohován do Microsoft Azure, není možné připravit pro něj odpovídající předhled opatření. Pro inspiraci lze využít opatření pro databázový systém popsaný v kapitole 13.

15.1 SCÉNÁŘ

Scénář záložní datové centrum zahrnuje:

- Azure Site Recovery
  - Replikace serverů běžících v datovém centru zákazníka (on-premise) do Azure Storage
  - Zotavení po havárii
    - V datovém centru zákazníka
    - V Microsoft Azure
- Azure Active Directory
  - Autorizace uživatelů a administrátorů
- Active Directory Domain Services + ADFS on-premise v interní síti
  - Autentizace uživatelů a administrátorů
- Interní síť organizace
- Síťové spojení mezi Microsoft Online Services a interní sítí organizace

15.2 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DŮVĚRNOSTI

Pro tabulku Tab. 13 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 13 Technická opatření pro zajištění důvěrnosti

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
Azure Site Recovery - replikace	Řízení přístupu na úrovni správy Azure SQL Database - Azure Resource Manager a Azure Subscription.	Azure Security and Audit Log Management, viz 11.1.8. Šifrování replikovaných serverů v Azure Storage, viz 11.1.10.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).
Azure Site Recovery - zotavení po havárii v Microsoft Azure	Řízení přístupu na úrovni správy Azure SQL Database - Azure Resource Manager a Azure Subscription. Azure Storage, viz 11.1.10	Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Azure AD	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure AD pomocí Azure AD. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Azure AD Audit Reports, viz [89]. Azure Security and Audit Log Management, viz 11.1.8.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Více faktorová autentizace, viz 11.1.19.
Server on-premise	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Interní počítačová síť	Fyzická bezpečnost. Autentizace a autorizace koncového zařízení k portu sítě (802.1X). Řízení administrátorského přístupu k aktivním síťovým prvkům.	Audit přístupů na aktivních síťových prvcích. Šifrování bezdrátových sítí.	Audit provedených změn na aktivních síťových prvcích. Zabezpečení na úrovni aplikačních protokolů HTTP, SMTP a podobně pomocí TLS nebo šifrování pomocí IPSec nebo SMB, viz 11.1.18.
Síťové spojení mezi Microsoft Online Services a interní sítí organizace	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu ke službám na úrovni Azure Load Balancer, viz [88]	Šifrování poskytovaných služeb pomocí TLS, viz 10.10.4. nebo Point-to-Site VPN přístupy z klientských zařízení, viz 11.1.12 nebo Site-to-Site VPN mezi datovým centrem Microsoft Azure a interní sítí, viz 11.1.12 nebo Express Route + VPN, viz 11.1.15	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

15.3 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ INTEGRITY

Pro tabulku Tab. 14 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 14 Technická opatření pro zajištění integrity

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).
Azure Site Recovery - replikace	Řízení přístupu na úrovni správy Azure SQL Database - Azure Resource Manager a Azure Subscription.	Azure Security and Audit Log Management, viz 11.1.8. Šifrování replikovaných serverů v Azure Storage, viz 11.1.10.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).
Azure Site Recovery - zotavení po havárii v Microsoft Azure	Řízení přístupu na úrovni správy Azure SQL Database - Azure Resource Manager a Azure Subscription. Azure Storage, viz 11.1.10	Azure Disk Encryption, viz 10.10.4 a Azure Key Vault, viz 11.1.4.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Azure AD	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu k Azure AD pomocí Azure AD. Federace Azure AD a on-premise Active Directory pomocí AD Federation Services.	Azure AD Audit Reports, viz [89]. Azure Security and Audit Log Management, viz 11.1.8.	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4). Více faktorová autentizace, viz 11.1.19.
Server on-premise	Fyzická bezpečnost přístupu k počítači. Řízení přístupu pomocí rolí a skupin adresářové služby.	Zaznamenávání přístupu – bezpečnostní logy a logy aplikací.	Detailní monitorování a audit oprávnění administrátorů. RMS nebo šifrování dat klíči administrátorům nepřístupnými.
Interní počítačová síť	Fyzická bezpečnost. Autentizace a autorizace k portu sítě (802.1X). Řízení administrátorského přístupu k aktivním síťovým prvkům.	Audit přístupů na aktivních síťových prvcích. Audit provedených změn na aktivních síťových prvcích. Šifrování bezdrátových sítí.	Více faktorová autentizace pro aktivní síťové prvky, viz 11.1.19.
Síťové spojení mezi Microsoft Online Services a interní sítí organizace	Řízení přístupu na úrovni správy Azure AD – Azure Resource Manager a Azure Subscription. Řízení přístupu ke službám na úrovni Azure Load Balancer, viz [88]	Šifrování poskytovaných služeb pomocí TLS, viz 10.10.4. nebo Point-to-Site VPN přístupy z klientských zařízení, viz 11.1.12 nebo Site-to-Site VPN mezi datovým centrem Microsoft Azure a interní sítí, viz 11.1.12 nebo Express Route + VPN, viz 11.1.15	Interní procesy Microsoft (LockBox viz 8.9.4, COSMOS viz 10.8.4).

15.4 TECHNICKÁ OPATŘENÍ PRO ZAJIŠTĚNÍ DOSTUPNOSTI

Pro tabulku Tab. 15 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 15 Technická opatření pro zajištění dostupnosti

Komponenta systému	Úroveň střední	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.
Azure Site Recovery	Dostupnost dat a služby na této úrovni je vestavěná v Azure Site Recovery.	Dostupnost dat a služby na této úrovni je vestavěná v Azure Site Recovery.	Dostupnost dat a služby na této úrovni je vestavěná v Azure Site Recovery.
Azure Site Recovery - zotavení po havárii v Microsoft Azure	Dostupnost dat je závislá na architektuře IS po obnově, standardně se pohybuje v rozmezí 99,9 – 99,95%	Dostupnost dat je závislá na architektuře IS po obnově, standardně se pohybuje v rozmezí 99,9 – 99,95%	Dostupnost dat je závislá na architektuře IS po obnově, standardně se pohybuje v rozmezí 99,9 – 99,95%
Azure AD	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.	Dostupnost dat a služby na této úrovni je vestavěná v Azure AD.
Server on-premise	Zálohování a obnova dat a konfigurací	Redundantní implementace on-premise Active Directory a ADFS s vysokou dostupností.	Geo-Redundantní implementace on-premise Active Directory a ADFS s vysokou dostupností.
Interní počítačová síť	Záloha konfigurace aktivních síťových prvků.	Smlouva o podpoře zajišťující výměnu nebo zprovoznění aktivního síťového prvku v požadovaném čase.	Redundantní aktivní síťové prvky, konfigurace s automatickým řešením výpadku nebo poruchy sítě.
Síťové spojení mezi Microsoft Online Services a interní sítí organizace	---	Přístupu ke službám pomocí Azure Load Balancer, viz [88]. Záložní připojení k Internetu pro klientská zařízení.	Redundantní služby v alespoň dvou datových centrech Microsoft Azure. Azure Traffic Manager, viz 11.1.11.

15.5 TECHNICKÁ OPATŘENÍ NEZÁVISLÁ NA KLASIFIKACI DAT

Pro ochranu aktiv informačního systému je kromě opatření uvedených v příloze č. 1 Vyhlášky nutné realizovat i technická opatření nezávislá na klasifikaci dat (§16 – §27 Vyhlášky). Konkrétní požadavky na tato technická opatření vyplynou z analýzy rizik, viz kapitola 8.

Níže uvedená opatření jsou konkretizací opatření uvedených v kapitole 10 do formy relevantní pro daný scénář a komponentu.

- Nástroj pro detekci kybernetických událostí, viz kapitola 10.7
  - Pro Azure Site Recovery poskytuje tento typ ochrany MCIO, viz kapitola 10.7.4
- Nástroj pro sběr a vyhodnocení kybernetických událostí, viz kapitola 10.8
  - Systém COSMOS (viz 10.8.4), který je součástí MCIO, sbírá a vyhdonocuje kybernetické události vznikající v rámci MCIO.
  - Pro sběr a vyhodnocení událostí vznikajících ve virtuálních serverech v rámzi Azure Iaas a službách v rámci Azure PaaS v rozsahu požadovaném pro VIS lze využít službu Azure HDInsight. Pro vyhodnocení událostí v rozsahu požadovaném pro KII je nutné využít SIEM řešení třetí strany, do kteréhu budou exportovány události sebrané pomocí Azure HDInsight.

16 SEZNAM POUŽITÝCH ZKRATEK

Tab. 16
Seznam použitých zkratek

Zkratka	Význam
AD	Active Directory
ADFS	Active Directory Federation Service
BLOB	Binary Large Object
BYOK	Bring Your Own Key
DDoS	Distribuovaný útok typu Denial of Service
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting & Conformance
DMZ	Demilitarizovaná zóna
HSM	Hardware Security Module
IaaS	Infrastructure as a Service Infrastruktura jako služba – model poskytování cloud služeb
ICZ	S.ICZ a.s.
IPS	Intrusion Prevention System
IS	Informační systém
KEK	Key Encryption Key
KII	Kritizká informační infrastruktura ve smyslu Zákona
MCIO	Microsoft's Cloud Infrastructure and Operations
MS	Microsoft s.r.o.
Multi-tenant prostředí	Prostředí, které je poskytováno množství subjektů a které zajišťuje, aby činnost jednoho subjektu neovlivňovala činnost ostatních subjektů
NAT	Network Address Translation
OME	Office 365 Message Encryption
OTP	One Time Password
PaaS	Platform as a Service
PKI	Public Key Infrastructure
RMS	Rights Management Service
SaaS	Service as a Service

Zkratka	Význam
SCADA	Průmyslové řídicí systémy
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SPF	Sender Policy Framework
SSTP	Secure Socket Tunneling Protocol
TDE	SQL Server Transparent Database Encryption
TLS	Transport Layer Security
TPM	Trusted Platform Module
VIS	Významný informační systeém ve smyslu Zákona
VM	Virtual Machine
Vyhláška	Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
WAF	Web Application Firewall
WBEM	Web-Based Enterprise Management
WMI	Windows Management Instrumentation
Zákon	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

17 LITERATURA

[1] Microsoft Corporation: Microsoft Security Policy, 6.1.2016

[2] Microsoft Corporation: Office 365 SoA 2014 Security and Privacy ISO 27001.2013 & 27018, 31.10.2014

[3] Microsoft Corporation: Trusting the Cloud, White Paper, 22.11.2015

[4] Microsoft Corporation: Windows Azure Network Security, 28.11.2013

[5] Microsoft Corporation: Data Encryption Technologies in Office 365, 22.1.2016

[6] NIST: Windows Server 2008 R2 BitLocker Drive Encryption Security Policy For FIPS 140-2 Validation, 31.8.2011

[7] Microsoft Corporation: Defending Office 365 against Denial-of-Service attack, 2/2015

[8] Microsoft Corporation: Azure AD Privileged Identity Management, 21.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-privileged-identity-management-configure/)

[9] Microsoft Corporation: Integrating your on-premises identities with Azure Active Directory, 25.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/)

[10] Microsoft Corporation: What is Azure Active Directory?, 14.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-whatis/)

[11] MSDN: Password policy in Azure AD, 8.6.2015 (https://msdn.microsoft.com/en-us/library/azure/jj943764.aspx)

[12] Microsoft Corporation: Azure Role-Based Access Control, 10.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/role-based-access-control-configure/)

[13] Microsoft Corporation: Microsoft Azure Security and Audit Log Management, 14.11.2014

[14] Microsoft Corporation: Microsoft Azure security and audit log management, 10.12.2015 (https://azure.microsoft.com/cs-cz/documentation/articles/azure-security-audit-log-management/)

[15] Microsoft Corporation: View and download reports about service usage in Office 365 (https://support.office.com/en-us/article/View-and-download-reports-about-service-usage-in-Office-365-30e5558f-d3c0-4a3b-a0d5-58fc7750c0ad?CorrelationId=4ba19226-3592-4db3-a4a2-3bbe8a1f1d9c&ui=en-US&rs=en-US&ad=US)

[16] Microsoft Corporation: View your access and usage reports, 7.12.2015 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-view-access-usage-reports/)

[17] Microsoft Corporation: Azure Active Directory Audit Report Events, 7.12.2015 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-reporting-audit-events/)

[18] Microsoft Technet: Auditing in Office 365, 13.1.2016 (https://technet.microsoft.com/en-us/library/dn790283.aspx)

[19] Microsoft Corporation: Search the audit log in the Office 365 Protection Center (https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Protection-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c?ui=en-US&rs=en-US&ad=US)

[20] Microsoft Technet: Exchange auditing reports, 21.9.2015 (https://technet.microsoft.com/library/jj150497(v=exchg.150).aspx)

[21] Microsoft Technet: Enable mailbox auditing in Office 365, 28.9.2015 (https://technet.microsoft.com/en-us/library/dn879651.aspx)

[22] Microsoft Corporation: View audit log reports (https://support.office.com/en-us/article/View-audit-log-reports-b37c5869-1b47-4a82-a30d-ea20070fe527?CorrelationId=b47f8144-3ef7-4fb6-99e7-1ad349bbe8f9&ui=en-US&rs=en-US&ad=US#__toc272842194)

[23] Microsoft Corporation: Microsoft Antimalware for Azure Cloud Services and Virtual Machines, 10.12.2015 (https://azure.microsoft.com/cs-cz/documentation/articles/azure-security-antimalware/)

[24] Microsoft Corporation: Auditing and Reporting in Office 365, 13.8.2015

[25] Microsoft Corporation: Microsoft Azure Network Security, 3.10.2014

[26] Microsoft Corporation, Cloud Infrastructure Operational Excellence & Reliability, 13.3.2015

[27] Mark Russinovich, An Inside Look at Cloud Service Provider Security, 20.4.2015

[28] Microsoft Corporation, Introduction to Azure Security Center, 9.2.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/security-center-intro/)

[29] Microsoft Corporation, About VPN devices for Site-to-Site VPN Gateway connections, 14.12.2015 (https://azure.microsoft.com/cs-cz/documentation/articles/vpn-gateway-about-vpn-devices/)

[30] Microsoft Corporation, ExpressRoute technical overview, 16.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/expressroute-introduction/)

[31] Microsoft Corporation, What is Azure Rights Management?, 1.2.2016 (https://technet.microsoft.com/en-us/library/jj585026.aspx#BKMK_RMScrytographics)

[32] Microsoft Corporation, Microsoft Trust Centrum (https://www.microsoft.com/en-us/TrustCenter/Security/DesignOpSecurity)

[33] Microsoft Corporation, Service Level Agreement for Microsoft Online Services, 1.2.2016

[34] Office 365 Team, Announcing the new Office 365 Management Activity API for security and compliance monitoring, 21.4.2015 (https://blogs.office.com/2015/04/21/announcing-the-new-office-365-management-activity-api-for-security-and-compliance-monitoring/)

[35] Microsoft Corporation: What is Azure Backup?, 5.2.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/backup-introduction-to-azure-backup/)

[36] Microsoft Corporation: What is Site Recovery?, 22.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/site-recovery-overview/)

[37] Microsoft Technet: Windows Enforcement of Authenticode Code Signing and Timestamping, 24.9.2015 (http://aka.ms/sha1)

[38] MSDN: About Keys and Secrets, 16.10.2015 (https://msdn.microsoft.com/library/azure/dn903623.aspx)

[39] Microsoft Corporation: What is Azure Key Vault?, 8.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/key-vault-whatis/)

[40] Microsoft Corporation: Azure Resource Manager overview, 2.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/resource-group-overview/)

[41] Microsoft Corporation: Audit operations with Resource Manager, 2.12.2015 (https://azure.microsoft.com/en-us/documentation/articles/resource-group-audit/)

[42] Microsoft Corporation: RBAC: Built-in roles, 21.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/role-based-access-built-in-roles/)

[43] Microsoft Technet: Planning and Implementing Your Azure Rights Management Tenant Key, 1.2.2016 (https://technet.microsoft.com/library/dn440580.aspx)

[44] Microsoft Technet: Decommissioning and Deactivating Azure Rights Management, 1.12.2015 (https://technet.microsoft.com/en-us/library/jj658940.aspx)

[45] Microsoft Azure: Encrypt and decrypt blobs in Microsoft Azure Storage using Azure Key Vault, 6.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/storage-encrypt-decrypt-blobs-key-vault/)

[46] Stefan Keir Gordon: Storing Data Securely in Azure Blob Storage with Azure Encryption Extensions, 17.6.2015 (http://blogs.msdn.com/b/partnercatalystteam/archive/2015/06/17/storing-data-securely-in-azure-blob-storage-with-azure-encryption-extensions.aspx)

[47] Microsoft Corporation: Shared Access Signatures, Part 1: Understanding the SAS model, 14.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/storage-dotnet-shared-access-signature-part-1/)

[48] Microsoft Corporation: Azure Site Recovery: Our Commitment to Keeping Your Data Secure, 2.9.2014 (https://azure.microsoft.com/en-us/blog/azure-site-recovery-privacy-security-part1/)

[49] Microsoft Corporation: ExpressRoute circuits and routing domains, 16.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/expressroute-circuit-peerings/)

[50] Office 365 Team: Announcing Customer Lockbox for Office 365, 21.4.2015 (https://blogs.office.com/2015/04/21/announcing-customer-lockbox-for-office-365/)

[51] Microsoft Technet: Architecture guidance for protecting company email and documents, 30.9.2015 (https://technet.microsoft.com/en-us/library/mt574220.aspx)

[52] Microsoft Technet: Introduction to Server and Domain Isolation, 20.1.2009 (https://technet.microsoft.com/en-us/library/cc725770(v=ws.10).aspx)

[53] Microsoft Technet: Changes in Kerberos Authentication, 10.5.2012 (https://technet.microsoft.com/en-us/library/dd560670(v=ws.10).aspx)

[54] Microsoft Technet: Network security: Configure encryption types allowed for Kerberos, 15.11.2012 (https://technet.microsoft.com/en-us/library/jj852180.aspx)

[55] Microsoft Corporation: What is Azure Multi-Factor Authentication?, 3.3.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/multi-factor-authentication/)

[56] Microsoft Corporation: Security in Office 365 White Paper, 22.1.2016

[57] Microsoft Technet: Azure Key Vault – Making the cloud safer, 8.1.2015, (https://blogs.technet.microsoft.com/kv/2015/01/08/azure-key-vault-making-the-cloud-safer/)

[58] Microsoft Corporation: How to generate and transfer HSM-protected keys for Azure Key Vault, 1.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/key-vault-hsm-protected-keys/#step-4-prepare-your-key-for-transfer)

[59] Microsoft Corporation: Exchange Online Protection, 2016 (https://products.office.com/en-us/exchange/microsoft-exchange-online-protection-email-filter-and-anti-spam-protection-email-security-email-spam)

[60] Microsoft Corporation: Exchange Online Advanced Threat Protection, 2016 (https://products.office.com/en-us/exchange/online-email-threat-protection)

[61] Microsoft Corporation: Always Encrypted (Database Engine), 4.3.2016 (https://msdn.microsoft.com/en-us/library/mt163865.aspx)

[62] MSDN: Extensible Key Management Using Azure Key Vault (SQL Server), 10.12.2015 (https://msdn.microsoft.com/en-us/library/dn198405.aspx)

[63] MSDN: Transparent Data Encryption (TDE), 23.11.1015 (https://msdn.microsoft.com/en-us/library/bb934049.aspx)

[64] MSDN: Transparent Data Encryption with Azure SQL Database, 28.1.2016 (https://msdn.microsoft.com/en-us/library/dn948096.aspx)

[65] Microsoft Azure: Azure Disk Encryption for Windows and Linux IaaS VMs, 29.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/azure-security-disk-encryption/)

[66] Cloudlink: CloudLink SecureVM leveraging the Azure Key Vault, 14.1.2015 (https://blogs.technet.microsoft.com/kv/2015/01/14/cloudlink-securevm-leveraging-the-azure-key-vault/)

[67] Microsoft Azure: About VPN devices for Site-to-Site VPN Gateway connections, 15.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpn-devices/)

[68] Microsoft Azure: Secure an app in Azure App Service, 12.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/web-sites-security/#secure-data-tier)

[69] Microsoft Technet: BitLocker Overview, 21.8.2013 (https://technet.microsoft.com/en-us/library/hh831713.aspx)

[70] dm-crypt: Linux kernel device-mapper crypto target, (https://gitlab.com/cryptsetup/cryptsetup/wikis/DMCrypt)

[71] Microsoft Azure: Azure SQL Database security guidelines and limitations, 16.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/sql-database-security-guidelines/)

[72] Microsoft Azure: Penetration Testing Overview (https://security-forms.azure.com/penetration-testing/terms)

[73] Microsoft Azure: Get started with SQL Database Dynamic Data Masking, 1.12.2015 (https://azure.microsoft.com/en-us/documentation/articles/sql-database-dynamic-data-masking-get-started/)

[74] Microsoft Azure: Securing your SQL Database, 22.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/sql-database-security/)

[75] Microsoft Azure: Get started with SQL database auditing, 2.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/sql-database-auditing-get-started/)

[76] Microsoft Azure: Active Geo-Replication for Azure SQL Database 7.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/sql-database-geo-replication-overview/)

[77] Microsoft Azure: What is Traffic Manager?, 17.3.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/traffic-manager-overview/)

[78] MSDN: Azure Business Continuity Technical Guidance, 26.3.2015, (https://msdn.microsoft.com/library/azure/hh873027.aspx)

[79] Microsoft Azure: Scale a web app in Azure App Service, 25.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/web-sites-scale/)

[80] Microsoft Azure: Overview: Cloud business continuity and database disaster recovery with SQL Database (https://azure.microsoft.com/en-us/documentation/articles/sql-database-business-continuity/)

[81] Microsoft Azure: High availability and disaster recovery for SQL Server in Azure Virtual Machines, 22.1.2016 (https://azure.microsoft.com/cs-cz/documentation/articles/virtual-machines-sql-server-high-availability-and-disaster-recovery-solutions/)

[82] Microsoft Azure: Dealing with encrypted disks during VM backup, 14.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/backup-azure-vms-encryption/https://azure.microsoft.com/cs-cz/documentation/articles/backup-azure-vms-encryption/)

[83] Office 365 Message Encryption FAQ, 14.1.2016 (https://technet.microsoft.com/en-us/library/dn569285.aspx)

[84] Microsoft Technet: Comparing Azure Rights Management and AD RMS, 1.2.2016 (https://technet.microsoft.com/en-us/library/jj739831.aspx)

[85] Microsoft Azure: VPN Gateway FAQ, 10.3.02016 (https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-vpn-faq/)

[86] Microsoft Azure: About VPN devices for Site-to-Site VPN Gateway connections, 15.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpn-devices/)

[87] Microsoft Azure: What is a Network Security Group (NSG)?, 11.2.2016 (https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)

[88] Microsoft Azure: Azure Load Balancer overview, 17.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/load-balancer-overview/)

[89] Microsoft Azure: Azure Active Directory Reporting Guide, 7.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-guide/)

[90] Microsoft Azure: Get started with SQL Database Dynamic Data Masking, 1.12.2015 (https://azure.microsoft.com/cs-cz/documentation/articles/sql-database-dynamic-data-masking-get-started/)

[91] Barracuda: Barracuda Web Application Firewall, (https://techlib.barracuda.com/WAF/Azure)