Microsoft

STRATEGIE-LEITFADEN FÜR MEHR SICHERHEIT, PRIVATSPHÄRE UND SCHUTZ

GEMEINSAM ZU MEHR SICHERHEIT UND VERTRAUEN IM INTERNET, AUSGABE 3

Fortschritte der Computer- und Kommunikationstechnologien verbinden immer mehr Anwender und erleichtern unser Leben wie nie zuvor. Onlinedienste unterstützen uns in vielen täglichen Dingen – im Beruf, beim Lernen, in der Kommunikation, in der öffentlichen Verwaltung und im sozialen Alltag. Obwohl viele dieser innovativen Dienste individuelle Vorteile bieten, stellen uns die dafür geschaffenen, miteinander verbundenen und sehr komplexen Systeme vor neuartige, große Herausforderungen. Denken Sie nur an die riesigen Datenbanken und technischen Infrastrukturen, die Milliarden öffentlicher und privater Datensätze verwalten.

Privatsphäre, Schutz und Sicherheit gehören daher weltweit unbestritten zu den Topthemen von Datenschützern, Anwendern, Unternehmen und Regierungen. Die technischen Hilfsmittel, die unser soziales Zusammenleben erleichtern, werden oft auch für kriminelle Machenschaften und bösartige Absichten genutzt. Kriminelle und verantwortungslose Unternehmen sind daher sehr ernst zu nehmende Bedrohungen.

Mit der Initiative Trustworthy Computing verfolgt Microsoft langfristig das Ziel, eine sichere, geschützte und zuverlässige Rechnerumgebung mit größtmöglicher Privatsphäre für alle Anwender zu schaffen. Bill Gates rief die Initiative im Jahr 2002 ins Leben, als er sie per E-Mail allen Microsoft-Mitarbeitern vorstellte.

Seitdem hat Microsoft immer wieder auf wichtige Veränderungen reagiert und die Initiative Trustworthy Computing entsprechend angepasst. Neue Bedrohungen stellten und stellen Computer-Sicherheitsexperten vor große Herausforderungen. Die Menschen sind mittlerweile mit sehr vielen internetfähigen Anwendungen miteinander vernetzt. Sie erzeugen dabei enorme weltumspannende Datenströme, die weit über das hinausgehen, was wir als traditionelles Modell für den Schutz der Privatsphäre, das Anwender informiert und Genehmigungen einholt, kennen. Untersuchungen der Onlinesicherheit haben seit 2002 ergeben, dass das Internet für Anwender weniger gefährlich ist, als wir alle ursprünglich angenommen haben. Mit dem Wachstum der digitalen Welt und immer mehr Anwendern, die sich in sozialen Netzen engagieren, entsteht ein neues Bewusstsein hinsichtlich Programmen, die dabei einen bestmöglichen Onlineschutz bieten.

Microsoft hat die Global-Compact-Initiative der Vereinten Nationen unterzeichnet und sich damit verpflichtet, seine Geschäftstätigkeiten und Strategien entsprechend zehn universell anerkannten Prinzipien auszurichten. Dazu gehören unter anderem die Menschenrechte, das internationale Abkommen über zivile und politische Rechte, das internationale Abkommen über Wirtschaftliches, Soziales und Kulturelles sowie die Erklärung der International Labour Organization (ILO) über die fundamentalen Arbeitsprinzipien und -rechte. Microsoft ist sich seiner Verantwortung als führender Technologieanbieter und weltweit tätiges Unternehmen bewusst und weiß, dass Firmen die Einhaltung der Menschenrechte sowohl fördern als auch behindern können. Jahr für Jahr wird die Messlatte für die Einhaltung der Menschenrechte höher gelegt, weil Informations- und Kommunikationstechnologien immer mehr an Bedeutung gewinnen bei der Zusammenarbeit, bei der Wissensnutzung und bei der zwischenmenschlichen Interaktion. Microsoft weiß, wie wichtig es ist, Verantwortung für die Einhaltung der Menschenrechte zu übernehmen. Das Unternehmen hat es sich daher zum Ziel gesetzt, mit leistungsfähigen Technologien eine Grundlage zu schaffen, mit der weltweit die Einhaltung der Menschenrechte forciert wird. Lesen Sie mehr über die Erklärung von Microsoft zum Schutz der Menschenrechte online unter **aka.ms/Human-Rights-Statement**.

Die Merkmale der Onlinesicherheit, des Datenschutzes und der Privatsphäre sind komplex und ändern sich ständig. Sie erfordern eine fortlaufende, mehrschichtige Entwicklung effizienter Lösungen. Das Ziel von Microsoft ist nicht nur, Informationen für die gemeinsame Nutzung bereitzustellen, sondern auch Technologien und Produkte für die Zusammenarbeit in allen Branchen und über Ländergrenzen hinweg zu ermöglichen. Darüber hinaus möchte das Unternehmen auch dazu beitragen, die Internetnutzung deutlich sicherer zu machen.

Die Informationen in diesem Leitfaden sind dafür ein guter Anknüpfungspunkt. Auf den folgenden Seiten finden Sie, neben den wichtigsten Eckpunkten, einen Überblick über das Microsoft-Engagement – mit Produkten, Dienstleistungen und weltweiten Kooperationen. Weiterhin stellen wir Ihnen Empfehlungen für Vorgehensweisen sowie eine Aufzählung hilfreicher Ressourcen und weiterführende Links zur Verfügung. Alle Informationen sind das Ergebnis langjähriger, umfangreicher Arbeiten und Erfahrungen internationaler Microsoft-Teams und externer Experten. Lesen Sie mehr über:

- die Onlineprivatsphäre und entsprechende Praxisbeispiele,
- den Onlineschutz von Jugendlichen,
- Cyber-Bedrohungen und deren Erkennung, Vermeidung und Behebung,
- Microsoft-Produkte, -Dienstleistungen und -Partnerschaften, und wie Microsoft den Schutz im Internet erhöht,
- die Microsoft-Zugangstechnologien.

Dieser Leitfaden eignet sich ganz besonders für Entscheider, die neue Ideen und Lösungen entwickeln und damit die Privatsphäre, die Sicherheit und den Schutz bei der Onlinenutzung erhöhen möchten.

Wir stellen diese Informationen weltweit und mit dem Wissen zur Verfügung, dass es regional unterschiedliche Prioritäten, Bedenken und Ideen hinsichtlich möglicher Lösungen gibt. Gerade deshalb ist es so wichtig, Ideen- und Informationsaustausch zu betreiben und damit effektive globale Richtlinien und Beispiele zu erarbeiten. Diese erfordern nicht nur eine hohe öffentliche Akzeptanz, sondern sie müssen auch weitgehend gesellschaftlich vertretbar sein, besonders wenn es um Sicherheit und Privatsphäre geht.

Die heutige digitale Abhängigkeit stellt uns weltweit vor Herausforderungen, die wir alleine nicht mehr lösen können. Um die Cyber-Bedrohungen zu reduzieren, müssen Unternehmen, Regierungen, Verbände und Anwender weltweit kooperieren. Microsoft unterstützt diese internationalen Kooperationen genauso wie neue Modelle der gemeinsamen Informationsnutzung und öffentlich-private Partnerschaften. Damit es uns gelingt, das Vertrauen bei der persönlichen Rechnernutzung zu erhöhen und für mehr Schutz und Sicherheit im Internet zu sorgen.

Der Inhalt

Microsoft Trustworthy Computing

Die wichtigsten Punkte im Überblick

- Microsoft verpflichtet sich, die Rechnernutzung vertrauenswürdiger und sicherer zu gestalten. Mit dem langfristigen Ansatz des Trustworthy Computing will das Unternehmen eine sichere, geschützte und zuverlässige Rechnerumgebung mit größtmöglicher Privatsphäre für alle Anwender schaffen.

- Microsoft ist überzeugt davon, dass Technologien und entsprechende Geschäftsprozesse Vertrauen erzeugen. Microsoft handelt nach dem Prinzip, dass Technologieunternehmen sich auf solide Entwicklungen und bewährte Methoden verlassen sollten – weil nur dann Produkte und Dienstleistungen entstehen, die zuverlässig, sicher und vertrauenswürdig sind.

- Microsoft arbeitet mit anderen Technologiefirmen, Regierungen, Anwendern und Unternehmen an Lösungen, die heutige und künftige Sicherheitsanforderungen erfüllen werden. Selbst Eltern sollten für ihre Familien mit entsprechenden Sicherheitseinstellungen die Onlinesicherheit erhöhen.

HINTERGRUND

Das Internet bereichert das Leben aller Anwender, es unterstützt Onlinehandel und die weltweite Kommunikation. Weil sich gleichzeitig immer mehr Menschen vernetzen, wird es umso wichtiger, allen den Stellenwert von Onlinesicherheit, -schutz und -privatsphäre deutlich zu machen.

Mit der langfristig ausgelegten Initiative Trustworthy Computing bekennen wir uns dazu, eine sichere und zuverlässige Rechnerumgebung mit größtmöglicher Privatsphäre für die Anwender zu schaffen. Weil das Internet im Computing-Ökosystem ein zunehmend kritischer Faktor wird, entwickeln wir auch die eigene Vision einer End-to-End-Vertrauenswürdigkeit ständig weiter.

Für uns sind der Schutz von wichtigen Daten und persönlichen Informationen unabdingbar, und Technologien und entsprechende Geschäftsprozesse müssen Vertrauen erzeugen. Wir handeln dabei nach dem Prinzip, dass Technologieunternehmen sich auf solide Entwicklungen und bewährte Methoden verlassen sollten – weil nur dann Produkte und Dienstleistungen entstehen, die zuverlässig, sicher und vertrauenswürdig sind. Gemeinsam mit Technologiefirmen, Regierungen, Anwendern und Unternehmen arbeiten wir an Lösungen, die heutige und künftige Sicherheitsanforderungen erfüllen werden.

SICHERHEIT

Wir konzentrieren uns auf innovative Entwicklungen von sicheren Anwendungen. Das Microsoft Security Engineering Center erhöht mit sicheren Produkten entsprechend dem Microsoft Security Development Lifecycle (SDL) den Schutz für unsere Kunden. Microsoft SDL ist ein Prozess, mit dem wir die Sicherheit bei der Anwendungsentwicklung berücksichtigen. Dabei werden in jeder Entwicklungsphase entsprechende Sicherheitsmerkmale integriert, wodurch tief im System verankerte Sicherheitsmechanismen mit einem hohen Schutz entstehen. Wir stellen SDL auch anderen Softwarefirmen zur Verfügung, damit gemeinsam sichere Rechnerumgebungen mit einem hohen Vertrauensfaktor für alle Anwender entstehen.

- Das Microsoft Security Science-Team untersucht und analysiert Onlineattacken und deren Techniken.

- Das Microsoft Malware Protection Center wertet sogenannte Malware aus und entwickelt Lösungen, die in unsere Sicherheitstechnologien einfließen.

- Wir erstellen den Security Intelligence Report. Der Bericht analysiert die Bedrohung durch Schadprogramme, Sicherheitslücken und Malware mit Daten von Internetdiensten und weltweit mehr als 600 Millionen Rechnern.
- Wird in einer unserer Anwendungen eine Sicherheitslücke entdeckt, die von Schadsoftware ausgenutzt werden könnte, überwacht unser Microsoft Security Response Center die Situation und reagiert auf den Vorfall. Es verwaltet zudem den unternehmensinternen Update-Veröffentlichungsprozess und koordiniert und kommuniziert als einzige zentrale Stelle alle Beiträge zu dem Thema.

PRIVATSPHÄRE

- Für uns ist das Vertrauen der Kunden entscheidend für den Unternehmenserfolg, und die Grundlage dafür ist der Schutz der Privatsphäre. Menschen und Firmen müssen jederzeit die Kontrolle über ihre Daten behalten; dazu gehört auch das Wissen, wie diese genutzt werden.
- Wir waren eines der ersten Unternehmen, das vor mehr als zehn Jahren einen Chief Privacy Officer einstellte. Heute arbeiten mehr als 40 Microsoft-Vollzeitmitarbeiter in diesem Unternehmensbereich. Sie werden von vielen Hundert weiteren Microsoft-Mitarbeitern unterstützt, die dafür sorgen, dass in allen Produkten und Diensten der Schutz der Privatsphäre mit geeigneten Technologien umgesetzt wird.
- Wir integrieren Technologien in Produkte und Dienste, mit denen Anwender ihre persönlichen Informationen besser schützen.
- Damit Unternehmen ihre Daten effizienter verwalten, bieten wir ihnen entsprechende Leitfäden, Rahmenbedingungen und Technologien an. Sie haben ein Ziel: persönliche Informationen besser zu schützen, Risiken zu minimieren, Richtlinien einzuhalten und Vertrauen sowie Verantwortungsbewusstsein zu schaffen.

ZUVERLÄSSIGKEIT

Cloud Computing bietet oft deutliche Vorteile bei den Kosten und der Effizienz. Sie erhalten damit die neuesten Werkzeuge und Technologien schnell und einfach. Allerdings kommt mit zunehmender Cloud-Nutzung der Zuverlässigkeit immer mehr Bedeutung zu. Wenn Cloud Computing alle seine Versprechen halten soll, müssen die online angebotenen Dienste mindestens genauso zuverlässig bereitgestellt werden wie ihre Pendants in einer lokalen Client-Server-Umgebung. Um diese Zuverlässigkeit zu verbessern, überarbeiten wir unsere Schlüsselprodukte wie Microsoft Exchange Server und Microsoft SharePoint Server, damit diese noch besser auch als Cloud-Dienste funktionieren. Zudem implementieren wir in den Onlinedatencentern wegweisende Datenschutzfunktionen mit redundant ausgelegten Diensten.

STRATEGISCHE ÜBERLEGUNGEN

Für uns sind öffentlich-private Partnerschaften ein wichtiger Faktor im Kampf gegen die immer komplexeren Cyber-Verbrechen. Daher arbeiten wir mit vielen Regierungsbehörden zusammen. Wir veranstalten technische Trainings für deren Mitarbeiter und unterstützen sie bei der Entwicklung neuer technischer Werkzeuge für den Kampf gegen Cyber-Kriminelle. Aber auch Anwender schützen wir, indem wir mit allen legalen Mitteln Cyber-Verbrechern das Handwerk legen. Ein Beispiel hierfür ist unsere maßgebliche Beteiligung an den legalen und technischen Aktionen, mit denen wir, gemeinsam mit weiteren Experten, die Botnetze Waledac und Rustock abgeschaltet haben. Es handelte sich um Abertausende Rechner, die ohne Wissen ihrer Eigentümer für die Verteilung von Malware, den Versand von Spam-Mails und viele weitere kriminelle Aktionen missbraucht wurden.

Hilfreiche Ressourcen

Microsoft Trustworthy Computing
www.microsoft.com/twc

Das Microsoft Safety and Security Center
www.microsoft.com/security

Das Microsoft Security Response Center
www.microsoft.com/msrc

Der Microsoft Security Intelligence Report
www.microsoft.com/sir

Ein Überblick über die Microsoft-Strategien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Trustworthy Computing Next

Die wichtigsten Punkte im Überblick

Im Jahr 2002 nannte Bill Gates die drei Grundlagen, die auch heute noch für Trustworthy Computing stehen: Sicherheit, Privatsphäre und Zuverlässigkeit. Allerdings hat sich seitdem die Rolle, die Rechner in unserem täglichen Leben spielen, geändert. Daher müssen die Grundlagen des Trustworthy Computing an die neuen Herausforderungen angepasst werden.

- Die Sicherheitsmodelle müssen einen ganzheitlichen Ansatz mit Prophylaxe, Entdeckung, Eindämmung und Wiederherstellung berücksichtigen. Das bisherige Hinweis- und Berechtigungsmodell muss durch Einstellungen für die Privatsphäre ersetzt werden, wobei die Rahmenbedingungen dem Nutzungsverhalten angepasst sein müssen. Das Zuverlässigkeitsmodell muss das Vertrauen in bisherige Datenreplikationen und -redundanzen steigern mit einer intelligenten Anwendung, die Ausfälle erkennt, isoliert und repariert.

- Regierungen spielen eine besondere Rolle bei der Umsetzung von Trustworthy Computing, weil sie die Macht haben, Märkte mit Anreizen und Gesetzen dafür vorzubereiten. Zudem sollten sie Regeln aufstellen, wie öffentliche und private Daten gemeinsam genutzt werden können und wie der internationale Datenzugriff durch Regierungen erfolgt.

HINTERGRUND

Am 15. Januar 2002 sendete Bill Gates eine E-Mail an alle Microsoft-Mitarbeiter. Darin kündigte er die Initiative Trustworthy Computing an und erklärte deren drei Grundlagen Sicherheit, Privatsphäre und Verfügbarkeit (wobei Letztere heute mit dem Begriff Zuverlässigkeit bezeichnet wird).

Seit 2002 hat es in diesen drei Bereichen jedoch gravierende Veränderungen gegeben. Neue Bedrohungen und Cyber-Kriminalität sind eine große Herausforderungen für die IT-Sicherheit und alle Computerexperten. Anwender sind durch viele Internetanwendungen miteinander verbunden. Sie erzeugen einen immensen weltweiten Datenverkehr, der weit über das hinausgeht, was wir bisher von dem herkömmlichen, unsere Privatsphäre schützenden Modell für Benachrichtigungen und Genehmigungen kannten. Die Zuverlässigkeit muss zudem so gesteigert werden, dass Cloud Computing mit diesem Wachstum Schritt halten kann – mit nahezu unbegrenzt skalierbaren Systemen, die jederzeit und an jedem Ort den Zugriff erlauben.

Die Grundlagen des Trustworthy Computing sind unverändert wichtig. Allerdings erfordern die neuen Herausforderungen innovative Lösungen, die wir als Trustworthy Computing Next bezeichnen.

- Um ausreichende Sicherheit vor zunehmenden, bekannten und ständigen Attacken zu erreichen, müssen Unternehmen eine ganzheitliche Sicherheitsstrategie verfolgen. Sie sollte sowohl die Prophylaxe als auch die Entdeckung, die Eindämmung und die Wiederherstellung umfassen.
- Um den Einfluss der immer mehr Daten verarbeitenden Welt auf die Privatsphäre besser zu kontrollieren, müssen Unternehmen Grundregeln erstellen und damit die Privatsphäre der Anwender schützen, ohne auf die Vorteile der Verarbeitung enormer Datenmengen (diese werden oft auch als Big Data bezeichnet) zu verzichten.
- Um die Zuverlässigkeit zu erreichen, auf der die Informations- und Kommunikationstechnologie (IuK) aufbaut, müssen Unternehmen zudem berücksichtigen, dass die Entwicklung von IuK-Systemen immer komplexer wird, und dafür Produkte und Dienste erstellen, die in Ausfallzeiten flexibel reagieren.

DER MICROSOFT-ANSATZ

Mit Trustworthy Computing Next reagieren wir auf die veränderte Onlinewelt und berücksichtigen dabei die drei Grundlagen von Trustworthy Computing: Sicherheit, Privatsphäre und Zuverlässigkeit.

- **Sicherheit**. Bedrohungen gefährden nahezu jeden Bereich eines IuK-Systems, wodurch eine absolute Sicherheit unmöglich wird. Diese sehr gefährliche Art der Bedrohung erfordert daher ein neues Sicherheitsmodell für Rechner, das die Prophylaxe, Entdeckung, Eindämmung und Wiederherstellung beinhaltet. Zwar sind diese einzelnen Bestandteile nicht neu, aber sie sind in vielen Unternehmen noch nicht in eine umfassende Sicherheitsstrategie integriert. Dies jedoch ist nötig, um ein eventuell betroffenes Netz – oder auch ein Teil davon – und den jeweiligen Schädling zu kontrollieren und zu isolieren. Zudem erfassen viele Sicherheitsstrategien einzelne Vorkommnisse in einem unternehmensweiten Netz nicht und vergleichen und analysieren diese nicht miteinander. Sie sind daher nicht in der Lage, auf diese Weise ungewöhnliche Vorgänge zu entdecken, die möglicherweise auf Angriffe auf das Netz hinweisen.
- **Privatsphäre**. Eines ist klar: Der Schutz der Privatsphäre in einer Cloud-Umgebung lässt sich nicht mit den traditionellen Mitteln des Benachrichtigungs- und Genehmigungsmodells – wie etwa bei der herkömmlichen Datenerfassung mit den dazugehörenden Informationen – erreichen. Die Verwendung der Daten bietet eine deutlich bessere Grundlage, um mit einer darauf aufbauenden Definition die persönlichen Informationen besser zu schützen. Ein solches Verwendungsmodell eignet sich sowohl für Unternehmen, die personenbezogene Daten erfassen, als auch für andere, die diese Daten verwenden. Unternehmen, die dieses Modell verwenden, müssen transparent sein, entsprechende Wahlmöglichkeiten anbieten und sicherstellen, dass sie die Risiken bei der Verwendung der personenbezogenen Daten berücksichtigen und vermeiden.
- **Zuverlässigkeit**. Weil die Technologie immer mehr unser tägliches Leben beeinflusst, muss die Zuverlässigkeit künftig sehr viel höher als derzeit sein. Dafür sind zwei grundlegende Veränderungen nötig: Erstens müssen Unternehmen für die Cloud-Umgebung und deren Big Data eine intelligente Auswertung schaffen, mit der sie die internen und unternehmensübergreifenden Abhängigkeiten verstehen. So könnte etwa die Beobachtung des Datenverkehrs zwischen Netzen wichtige Abhängigkeiten aufdecken, die so vorher nicht bekannt waren.

  Zweitens dürfen Unternehmen unter Zuverlässigkeit nicht mehr nur Datenredundanz und -replikation verstehen, denn alleine damit lassen sich keine hohen Zuverlässigkeitswerte für die Cloud erzielen. Die bisherige Praxis, Anwendungen vor Ausfällen zu schützen, muss ergänzt werden mit speziellen Anwendungen, die Ausfälle in miteinander verbundenen Rechnersystemen entdecken, vermeiden und, auch als kurzfristige Übergangslösung, reparieren.

STRATEGISCHE ÜBERLEGUNGEN

- **Die Aufgabe von Regierungen zum Schutz des Internets**. Regierungen sind in der Lage, Märkte mit Anreizen und Regularien vorzubereiten. Sie übernehmen zudem die sehr wichtige Aufgabe, mit Gesetzen die Onlinebedrohungen unter Strafe zu stellen und ihre Bürger damit vor Cyber-Kriminalität zu schützen.
- **Regeln für die Nutzung öffentlicher und privater Daten**. Viele Cyber-Attacken zielen auf öffentliche und private Infrastrukturen ab. Daher ist die Notwendigkeit einer öffentlich-privaten Partnerschaft unbestritten, auch wenn die Regeln der gemeinsamen Datennutzung dabei noch nicht festgelegt sind. Es ist die Aufgabe von Regierungen und Unternehmen, geeignete Mechanismen für eine sichere gemeinsame Datennutzung zu schaffen.
- **Regeln für den internationalen Datenzugriff von Regierungen.** Regierungen müssen neuen, international einheitlichen Rahmenbedingungen zustimmen, die den Datenzugriff regeln. Dies geht über die bisherigen Vereinbarungen, wie etwa Rechtshilfeabkommen, hinaus, mit denen die rechtliche Zuständigkeit in dem Staat bleibt, der die Daten speichert. Mit neuen Rahmenbedingungen sollten Staaten einem formellen Prozess für den Zugriff auf die Daten zustimmen.

Hilfreiche Ressourcen

Microsoft Trustworthy Computing Next
www.microsoft.com/twcnext

Gemeinsame Abwehr: Das Modell des Gesundheitswesens übertragen auf die Internetsicherheit

Die wichtigsten Punkte im Überblick

- Malware und Botnetze ermöglichen Cyber-Kriminalität, sie kosten Anwender und Unternehmen Milliarden US-Dollar pro Jahr. Eine gemeinsame und systematische Verteidigung im Internet ist nötig, um diese Bedrohungen abzuwehren. Von besser geschützten, mit dem Internet verbundenen Endgeräten profitieren nicht nur Anwender, sondern auch das gesamte Ökosystem der Informationstechnologie.

- Eine Möglichkeit, die Onlinesicherheit zu erhöhen, wäre ein Modell, das dem zur Bekämpfung von Krankheiten ähnelt. Dieses Modell im öffentlichen Gesundheitswesen, mit dem wir Infektionskrankheiten identifizieren und kontrollieren, enthält einige konzeptionelle Ansätze, die sich auch für die Internetsicherheit übernehmen lassen.

- Jede Verbesserung der Internetsicherheit muss den Kriterien einer sozialen, rechtlichen und persönlichen Privatsphäre entsprechen. Sie darf sich zudem nicht negativ auf die Wirtschaftlichkeit auswirken. Ein Internetsicherheitsmodell funktioniert aber nur dann wie ein gemeinsames Abwehrbollwerk, wenn es von allen Beteiligten akzeptiert wird und die Anwender überzeugt sind, dass ihre Privatsphäre damit bestens geschützt wird.

HINTERGRUND

Verbesserte Onlinetechnologien haben zu bemerkenswerten globalen Entwicklungen und sozialen Veränderungen geführt. Sie haben zudem die Art und Weise verändert, wie Unternehmen, zivile Gesellschaften und Regierungen ihre täglichen Aufgaben erledigen. Leider ist mit diesen Verbesserungen in gleichem Maße auch die Onlinekriminalität gestiegen, was zu einem Vertrauensverlust in der Öffentlichkeit führte. Führende Persönlichkeiten und Entscheider müssen sich dieser veränderten Realität mit neuen Ideen und Lösungen stellen, und sie müssen sich partnerschaftlich in die öffentliche Debatte um Internetsicherheit, Privatsphäre und Vertrauen einbringen.

Die Herausforderungen sind bedeutend und komplex.

- Cyber-Bedrohungen treten vermehrt auf, sind ausgefeilter und schwerer erkennbar geworden und haben immer weniger gemein mit ihrer ursprünglichen Version, Herkunft oder Wirkungsweise. Das ist der Grund dafür, warum es weltweit unzählige Abwehrversuche und Lösungen dafür gibt.

- Botnetze sind die heimtückischste Form von Malware. Sie bedrohen Infrastrukturen und damit auch Finanzmärkte, militärische Institutionen und die nationale Sicherheit jedes Staats.

- Personen und Unternehmen stehen viele Möglichkeiten für den Schutz ihrer Endgeräte vor Cyber-Attacken zur Verfügung. Dazu gehören Anti-Malware-Lösungen, Firewalls und SicherheitsUpdates. Obwohl diese Technologien bereitstehen, werden sie oft nicht komplett eingesetzt. Unternehmen verwenden sehr viel Zeit und Geld darauf, die Risiken mit gut ausgebildeten Experten und ausgefeilten Schutzsystemen zu verringern. Anwendern dagegen fehlt oft das nötige Fachwissen, um ihre Endgeräte selbst effektiv zu schützen.

Ein Weg, Cyber-Attacken zu vermeiden, ist es, dagegen mit einem Sicherheitsmodell ähnlich dem im Gesundheitswesen zu kämpfen. Dort werden Bürger über die Risiken infektiöser Krankheiten und über deren Vermeidung aufgeklärt. An Schulen etwa kann vor der Aufnahme eines Schülers eine Impfung vorgeschrieben werden. Oder die Schule warnt Schüler vor entdeckten ansteckenden Krankheiten, empfiehlt ihnen, falls sie sich angesteckt haben, zu Hause zu bleiben, und definiert bestimmte Kriterien für die erneute Zulassung zum Unterricht.

Um die Sicherheit im Internet zu verbessern, sollten sich Regierungen und Unternehmen systematisch engagieren und den Schutz der mit dem Internet verbundenen Endgeräte erhöhen. Sie könnten Mitarbeiter einstellen und Technologien entwickeln, um Präventivmaßnahmen

zu entwickeln, betroffene Endgeräte zu entdecken und deren Nutzer darüber zu informieren. Zudem sollten sie Anwender dabei unterstützen, ihren von Malware befallenen Rechner zu reparieren, und sie sollten mit weiteren Aktionen verhindern, dass noch mehr Rechner durch einen verseuchten Computer gefährdet werden.

Unternehmen und Regierungen haben bereits mit den oben beschriebenen Aktionen begonnen. So hat etwa die Internet Industry Association von Australien einen freiwilligen Verhaltenskodex für Internet Service Provider (ISP) veröffentlicht. Jeder ISP, der sich diesem Kodex unterwirft, verpflichtet sich, Anwender über deren betroffene Rechner zu informieren und ihnen für die Reparatur geeignete Werkzeuge bereitzustellen. In Deutschland arbeitet das Anti Botnet Advisory Centre auf ähnliche Weise mit lokalen ISPs zusammen: Diese informieren ihre Kunden, wenn ein Rechner von Malware befallen ist, und bieten ihnen Unterstützung bei der Reparatur an. Der finnische ISP TeliaSonera mit 164 Millionen Kunden setzt ein automatisches Überwachungssystem ein. Damit entdeckt er von Malware betroffene Endgeräte, warnt deren Nutzer und isoliert so lange jeden infizierten Rechner vom Netz, bis die Malware erfolgreich entfernt wurde.

DER MICROSOFT-ANSATZ

- Wir unterstützen ein gemeinsames Modell für die Abwehr von Cyber-Attacken, das ähnlich wie die Modelle moderner Gesundheitssysteme, mit denen die Ausbreitung gefährlicher Krankheiten verhindert wird, funktioniert. Unserer Meinung nach lassen sich mit einem solchen Abwehrmodell, das Regierungen und führende Unternehmen der IT-Industrie einsetzen, von Malware und Botnetzen befallene Rechner methodisch schützen, entdecken und reparieren.
- Dieses Modell ist aber nur der Anfang einer Vision, die wiederum nur mit der Unterstützung von Anwendern, Regierungen, ISPs und vielen anderen Unternehmen Realität werden kann.
- Wir arbeiten eng mit Mitgliedern der IT-Branche zusammen, um Informationen über Malware und Botnetze gemeinsam zu nutzen und betroffenen Anwendern zu helfen.

STRATEGISCHE ÜBERLEGUNGEN

- Weltweit sehen sich Anwender stetig steigenden Onlinegefahren gegenüber, während Unternehmen und Regierungen laufend mit Sicherheitsbedrohungen aus dem Cyberspace konfrontiert werden. Das ruft geradezu nach einem gemeinsamen Abwehrverhalten. Hohe und weitreichende Ziele lassen sich jedoch nur erreichen, wenn alle Beteiligten an einem Strang ziehen und einen offenen und ehrlichen Gedankenaustausch wünschen. Dazu gehört auch das Bekenntnis, miteinander Lösungen zu erarbeiten, die soziale, wirtschaftliche und politische Ansprüche berücksichtigen. Nur dann wird es uns gelingen, ein gemeinsames und effizientes Abwehrbollwerk gegen Cyber-Attacken zu errichten.
- Wie bei vielen anderen internationalen Kooperationen auch, haben Länder unterschiedliche Vorstellungen. Für gemeinsam zu schaffende Lösungen bedeutet dies: Sie müssen sozialverträglich sein und einer öffentlichen Prüfung standhalten. Das gilt insbesondere dann, wenn es um die ausgewogen Balance zwischen Sicherheit und Privatsphäre geht. Wenn wir weltweit mehr Sicherheit für die Onlinewelt erreichen möchten, müssen wir die Koordination zwischen Industrie, Regierungen, Forschungs- und Entwicklungseinrichtungen und Verbänden sowie den Gedanken- und Ideenaustausch untereinander verbessern – damit wir unsere Rechner im Internet besser vor Gefahren schützen.

Hilfreiche Ressourcen

Die Microsoft-Strategie und -Vorgehensweise für mehr globalen Schutz: die Health-Website
aka.ms/gssd-health

Microsoft-End-to-End-Vertrauen – Internet Health
aka.ms/internet-health

Das Internet-Health-Modell für mehr Cyber-Schutz. EastWest Institute, 2012
www.ewi.info/internet-health

Der Kampf gegen Botnetze

Die wichtigsten Punkte im Überblick

- Botnetze sind vernetzte infizierte Rechner, die von externen Kriminellen gesteuert werden. Sie führen, meistens ohne Wissen des Eigentümers, illegale Aktionen aus. Hierzu gehören der Versand von unerwünschten E-Mails genauso wie Betrugsversuche oder Attacken auf andere Rechner.

- Für Unternehmen und Regierungen stellen Botnetze eine enorme Bedrohung dar, weil sie sehr viele Rechner für gezielte gemeinsame Attacken auf IT-Infrastrukturen verwenden. Durch den gemeinsam mit IT-Unternehmen geführten Kampf gegen Botnetze und durch die Umsetzung ausgefeilter Regularien und Gesetze schützen Regierungen ihre Systeme und Bürger besser vor Botnetzen und damit verteilter Malware.

- Microsoft bekämpft Botnetze sehr aggressiv und in enger Zusammenarbeit mit Regierungen und Unternehmen. Wir stellen hierfür Sicherheitswerkzeuge zur Verfügung und unterstützen Unternehmen, Regierungen und Anwender.

HINTERGRUND

Ein Botnetz besteht aus vielen infizierten, mit dem Internet verbundenen Rechnern. Kriminelle Anwender steuern diese illegal und unbemerkt von den Eigentümern und nutzen sie für ungesetzliche Aktionen. Die Rechner in einem Botnetz werden auch Knoten, Bots, Robots oder Zombies genannt. Es handelt sich meistens um Rechner, die Anwender privat oder am Arbeitsplatz nutzen. Ein Rechner wird dann zu einem Knoten in einem Botnetz, wenn es einem Angreifer gelingt, Schadsoftware darauf zu installieren. Dies geschieht oft mit einem sogenannten Social-Engineering-Angriff, der die menschliche Schwäche eines Anwenders ausnutzt und ihn mit einem Trick zur Installation der Schadsoftware verleitet.

Die Eigentümer und Anwender bemerken es normalerweise nicht, wenn ein so infizierter Rechner für verbrecherische Zwecke genutzt wird. Ist ein Rechner von einer Botnetz-Malware infiziert, verbindet der Botnetz-Betreiber den Rechner unbemerkt mit dem Botnetz. Er versendet mit dem Rechner dann unerwünschte E-Mail-Werbung, hostet und verteilt damit Malware oder andere illegale Dateien oder attackiert damit andere Rechner.

Botnetze stellen für IT-Umgebungen von Unternehmen und Regierungen eine weitaus größere Gefahr dar als beispielsweise individuelle Hacker. Denn sie sind in der Lage, sehr viele Rechner für gezielte Angriffe zu koordinieren. Diese kombinierte Leistung blockiert mühelos nicht nur größte Websites und E-Mail-Server, sondern auch wichtige Kommunikations-, Datenverarbeitungs- und andere Elektroniksysteme.

Zudem bedrohen Botnetze auch IT-Wertschöpfungsketten.
Nach einer Microsoft-Untersuchung aus dem Jahr 2012 gelang es Cyber-Kriminellen, nicht ausreichend geschützte Wertschöpfungsketten mit dem Nitol-Botnetz zu infizieren. Dabei wurden auf Rechnern, noch vor deren Verkauf, unbemerkt mit Malware verseuchte Raubkopien installiert. Botnetze lassen sich zudem vollkommen anonym von Kriminellen – oft auch Botherders genannt – betreiben, weil sie den Ursprung einer Attacke hinter einem weit verzweigten Netz mit vielen Rechnern verbergen.

DER MICROSOFT-ANSATZ

- Wir bekämpfen Cyber-Verbrechen mit innovativen Technologien, gerichtlichen Schritten und Aufklärung der Anwender.
- Wir unterstützen Regierungen und gesetzgebende Organe mit technischen Trainings sowie bei kriminaltechnischen Ermittlungen und Untersuchungen. Zudem entwickeln wir kontinuierlich neue Werkzeuge für den Kampf gegen Cyber-Kriminalität.
- Mit der Initiative Microsoft Active Response for Security (MARS) vereinen wir rechtliches und technisches Fachwissen, um kriminelle Infrastrukturen aktiv zu vernichten. Dazu gehören zivilrechtlich eingeleitete Verfahren, aber auch technische Untersuchungen, mit denen wir Botnetze zerstören, sowie die Beschlagnahmung von Infrastrukturen und Domänen, mit denen Cyber-Kriminelle Botnetze kontrollieren. Mit den dabei gewonnenen Informationen erhöhen wir den Schutz aller Internet-Nutzer.

  MARS ist eine gemeinsame Initiative der Microsoft Digital Crimes Unit, des Microsoft Malware Protection Center, der Customer Support Services und von Trustworthy Computing. Einige Beispiele für den Erfolg der MARS-Initiative sind die kürzlich zerstörten Botnetze Waledac, Rustock, Kelihos, Zeus, Nitol und Bamital.

STRATEGISCHE ÜBERLEGUNGEN

- **Öffentlich-private Partnerschaften**. Wir freuen uns über die Unterstützung von Regierungen und gesetzgebenden Organen im Kampf gegen Botnetze. Die Kooperation mit Behörden ist unserer Meinung nach ein wesentliches Mittel, um Cyber-Bedrohungen effizient zu reduzieren, weil dabei auch entsprechende Gesetze und Regularien zum Einsatz kommen. Dazu gehören Initiativen wie der Anti-Bot-Verhaltenskodex für Internet Service Provider, den die U.S. Federal Communications Commission empfiehlt. Wir sind zudem überzeugt davon, dass eine Lockerung bestimmter Restriktionen in vielen Unternehmen zu mehr Innovationen und mehr Flexibilität im Kampf gegen Cyber-Kriminalität führen würde.
- **Internationale Kooperationen**. Wir fordern, wie viele andere Unternehmen auch, Staaten auf, das Übereinkommen über Computerkriminalität des Europarats zu übernehmen und zu ratifizieren. Die Unterzeichner verpflichten sich damit, die eigenen Gesetze und Prozeduren so anzupassen, dass sie dem Übereinkommen entsprechen und mit dessen Zielen übereinstimmen.
- **Kompromissloses Durchsetzen und ausgewogene Regularien**. Wir unterstützen eine kompromisslose Gesetzgebung, die rigorose Anwendung der Gesetze im Kampf gegen Botnetze und Cyber-Kriminelle unnachgiebig anklagt und verurteilt. Gleichzeitig ist es wichtig, dass diese Gesetze nicht nur Innovationen ermöglichen, sondern auch neue Technologien unverzüglich verwenden.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center hilft Ihnen mit Informationen über Sicherheitsthemen
www.microsoft.com/security

Die Microsoft Digital Crimes Unit
www.microsoft.com/dcu

Cyber-Sicherheit

Die wichtigsten Punkte im Überblick

- Cyber-Sicherheit besteht aus mehreren Aktivitäten und Ressourcen, mit denen Bürger, Unternehmen und Regierungen ihre Rechner sicher, geschützt und zuverlässig nutzen. Regierungen sind dabei gefordert, Sicherheitsmechanismen für vier Arten von Bedrohungen zu entwickeln: Cyber-Kriminalität, Militärspionage, Industriespionage und Cyber-Kriege.

- Microsoft sorgt für eine sichere und vertrauenswürdige Rechnernutzung, indem das Unternehmen fortlaufend Sicherheitsmerkmale von Produkten und Diensten verbessert und Methoden für mehr Cyber-Sicherheit entwickelt. Die enge Zusammenarbeit mit Regierungen und Partnern aus der IT-Branche reduziert die Bedrohungen der Cyber-Sicherheit zusätzlich.

- Eine effiziente Maßnahme für mehr Cyber-Sicherheit ist die Zusammenarbeit von öffentlichem Sektor und Privatwirtschaft, mit der sich Bedrohungen und Angriffe vermindern lassen. Dabei entstehen zudem nachhaltige und öffentlich anerkannte Rahmenbedingungen für mehr Cyber-Sicherheit, die weitere Innovationen in privaten Bereichen ermöglichen.

HINTERGRUND

Zur Cyber-Sicherheit gehört die Sicherheit von Informationen, Prozessen und Rechnersystemen. Im Zusammenspiel verschiedener Aktivitäten und Ressourcen entsteht eine sichere Umgebung, in der Bürger, Unternehmen und Regierungen Rechner sicher, geschützt und zuverlässig nutzen.

Die Erwartungen an die Cyber-Sicherheit sind unterschiedlich. Unternehmen erwarten davon sowohl im operativen als auch im informellen Bereich eine hohe Verfügbarkeit unternehmenswichtiger Anwendungen und einen bestmöglichen Schutz vertraulicher Daten.

Für Regierungen dagegen steht der Schutz von Bürgern, Unternehmen, Infrastrukturen und regierungseigenen Rechnersystemen an oberster Stelle. Sie stehen vor der großen Herausforderung, bewährte Methoden zu entwickeln, um die Öffentlichkeit wie auch die nationale Sicherheit vor vier Arten von Bedrohungen zu schützen.

Sie müssen die Öffentlichkeit vor vielen konventionellen Cyber-Verbrechen wie Betrug oder Vandalismus schützen, die von einzelnen Kriminellen, organisierten Banden und manchmal auch von lose zusammenhängenden Gruppen, den sogenannten „Hacktivists", verübt werden. Weiterhin müssen Staaten gegen Militärspionage kämpfen, die ebenfalls IT-Technologien verwendet. Ein gutes Beispiel hierfür sind die kürzlich wiederholt veröffentlichten, auf illegale Weise erlangten vertraulichen Daten aus militärischen Bereichen. Dies gilt auch für Industriespionage und andere, ähnlich gelagerte Fälle, über die Regierungen möglicherweise unterschiedliche Auffassungen bezüglich einer angemessenen Vorgehensweise haben. Zu guter Letzt müssen Regierungen sich den Herausforderungen des Cyber-Kriegs stellen und ihre Vorstellungen von traditioneller Kriegsführung an die veränderten Gegebenheiten anpassen.

Weil wir weltweit immer mehr von Informations- und Kommunikationstechnologien abhängig sind, wird auch die Cyber-Sicherheit mit der Zeit spürbar steigen. Damit das gelingt, sollten diejenigen, die dafür Richtlinien erstellen und Empfehlungen aussprechen, mit strategischen Überlegungen die Bedrohungen verringern.

DER MICROSOFT-ANSATZ

Als Unternehmen vermeiden wir Risiken, indem wir mit ständigen Weiterentwicklungen die Sicherheit verbessern. Dies betrifft sowohl unsere Produkte als auch Wertschöpfungsketten und operative Bereiche. Gleichzeitig erweitern wir ständig unser Wissen über Gefahren durch menschliches Fehlverhalten der Anwender, das sogenannte Social Engineering.

- **Verbesserte Sicherheit bei der Produktentwicklung.** Mit unserem Security Development Lifecycle sorgen wir für eine hohe Sicherheit, indem wir damit gezielt die Schwachstellen von Produkten aufspüren und ausmerzen. Mit diesem Prozess verwenden wir bereits während verschiedener Phasen der traditionellen Anwendungsentwicklung obligatorische Sicherheitsprüfungen.
- **Verbesserte Sicherheit von Wertschöpfungsketten.** Die Risiken für unsere Produkte und Dienste, die Bestandteile von Wertschöpfungsketten sind, reduzieren wir mit mehreren Hilfsmitteln. Dazu gehören Kontroll- und Steuerungselemente für die Identitäts- und Zugriffsverwaltung, der Security Development Lifecycle-Prozess, Richtlinien und Prozeduren, mit denen wir die Integrität der Microsoft-Anwendungen überwachen, sowie Maßnahmen gegen Fälschungen.

  Wir unterstützen zudem branchenübergreifende Entwicklungen von bewährten Methoden, um die Risiken für Wertschöpfungsketten zu verringern, oder Organisationen wie das Software Assurance Forum for Excellence in Code (SAFECode), um die Produktqualität zu erhöhen.
- **Verbesserte Sicherheit im operativen Bereich.** Damit Unternehmen Sicherheitsrisiken im operativen Bereich besser im Griff haben, stellen wir ihnen bewährte Methoden für mehr Sicherheit sowie regelmäßige Software-Updates zur Verfügung. Mit unserem Patch-Verwaltungssystem und den automatisch an jedem zweiten Dienstag eines Monats bereitgestellten Aktualisierungen schützen wir operative Bereiche mit standardisierten, planbaren und regelmäßig veröffentlichten Patches besser.
- **Verbesserte Sicherheit bei Social Engineering.** Wir bekämpfen Social-Engineering-Attacken, indem wir bewährte Methoden für deren Vermeidung und entsprechende Anleitungen für Anwender veröffentlichen. Zudem schützen wir Anwender mit Werkzeugen wie dem SmartScreen-Filter des Windows Internet Explorer.

Mit verschiedenen internen Programmen optimieren wir die Effektivität bei der Risikovermeidung ständig. Die Erkenntnisse, die wir dabei gewinnen, und die daraus resultierenden Methoden stellen wir, falls gewünscht, anderen Unternehmen und Regierungen zur Verfügung.

Unser Global Security Strategy and Diplomacy-Team arbeitet partnerschaftlich mit Regierungen, Industrieunternehmen und gemeinnützigen Organisationen an einer höheren Sicherheit im Internet. Dabei macht es Vorschläge, wie mehr Vertrauen mit welchen Richtlinien aufgebaut werden kann, und es hilft, Prozesse, die für die nationale, wirtschaftliche und öffentliche Sicherheit wichtig sind, besser zu schützen.

STRATEGISCHE ÜBERLEGUNGEN

- Regierungen und Privatwirtschaft sollten enger zusammenarbeiten, um Sicherheit, Privatsphäre und Zuverlässigkeit des IT-Ökosystems zu stärken und Cyber-Bedrohungen erfolgreich abzuwehren. Wir sind überzeugt davon, dass solche strategischen Partnerschaften und Initiativen entscheidend sind für mehr Sicherheit bei der Internetnutzung.
- Als Partner der Privatwirtschaft sollten Regierungen bewährte Methoden aus der Industrie als Grundlage für technologieneutrale Vorgaben zur Vermeidung von Cyber-Bedrohungen verwenden. Wenn sie diese getesteten Rahmenbedingungen übernehmen, bleibt jeder hart erkämpfte Sicherheitsvorteil bestehen und jede technische Innovation erfolgreich.
- Auch wenn Regierungen die nationale Sicherheit durch eine effiziente Cyber-Sicherheit verbessern, sollten sie darüber nicht die einzigartige IT-Infrastruktur für Informationen vergessen. Öffentlich-private Partnerschaften helfen oft dabei, Lücken zwischen dem Wunsch nach einer umfassenden nationalen Sicherheit und dem mit kommerziellen Produkten möglichen Grad an Sicherheit aufzudecken.

Hilfreiche Ressourcen

Die Microsoft-Strategie und -Vorgehensweise für mehr globalen Schutz
www.microsoft.com/gssd

Cyber-Bedrohungen begegnen: Rahmenbedingungen für die Zukunft
aka.ms/cyber-threat

Der Microsoft Security Intelligence Report
www.microsoft.com/sir

Software Assurance Forum for Excellence in Code (SAFECode)
www.safecode.org

Microsoft und der öffentliche Schutz und die nationale Sicherheit: Verbrechen mit bösartigen Anwendungen
aka.ms/DCU-economic-crime

Cyber-Sicherheitsnormen

Die wichtigsten Punkte im Überblick

- Die Privatwirtschaft mit ihren weltweiten Wertschöpfungsketten und Kunden kann einen wichtigen Beitrag leisten in der Diskussion über Normen für mehr Cyber-Sicherheit.
- Regierungen sollten auch weiterhin Lösungen und genormte Verhaltensregeln für mehr Cyber-Sicherheit entwickeln. Gleichzeitig verbessern zusätzliche internationale öffentlich-private Partnerschaften kritische Infrastrukturen und erlauben schnelle Reaktionen für mehr Sicherheit im Cyberspace.

HINTERGRUND

„In den vergangenen zwei Jahrzehnten haben wir erlebt, wie das Internet als soziales Medium rasend schnell und beispiellos wuchs. Kennzeichnend für die heutige Zeit ist das Vertrauen der sozialen Gemeinschaft in vernetzte Informationssysteme, mit denen sich für unser Leben wichtige kritische Infrastrukturen und Kommunikationssysteme kontrollieren lassen. Immer mehr Regierungen suchen Wege, die traditionelle nationale Leistungsfähigkeit in den Cyberspace zu verlagern."[1]

Die im Cyberspace verwendeten Technologien verändern sich sehr schnell. Leider halten die staatlich vereinbarten, standardisierten Verhaltensregeln mit diesem Tempo nicht Schritt, wodurch viele potenzielle Gefahrenherde entstehen. Nach einer Untersuchung der Vereinten Nationen haben mehr als 30 Staaten eine Militärdoktrin für die Nutzung des Cyberspace entwickelt, einige davon haben zudem Cyber-Abwehrzentren errichtet. Nur mit einem globalen Verständnis für Cyber-Sicherheitsnormen wird es uns gelingen, langfristig eine hohe Stabilität, Zuverlässigkeit und Sicherheit im Internet und Cyberspace zu erreichen.

Bis heute haben Regierungen internationale Diskussionen über Cyber-Sicherheit vor allem in Organisationen wie den Vereinten Nationen (in der Government Group of Experts) und in der europäischen Organisation für Sicherheit und Zusammenarbeit geführt.

Allerdings sind es Unternehmen aus der IT-Branche, die den größten Teil der Infrastruktur schaffen und betreiben, mit der wir auf das Internet zugreifen. Diese Firmen sind es, die innovative Technologien und bewährte Methoden erfinden und mit diesen technischen Normen die Cyber-Sicherheit erhöhen. Sie schließen Schwachstellen von Anwendungen, ermöglichen die sichere Entwicklung von Soft- und Hardware, reagieren schnell auf Sicherheitsbedrohungen und minimieren Sicherheitsrisiken. Während aktueller Cyber-Attacken übernimmt die Privatwirtschaft die kritische Aufgabe, schnell und effektiv die Bedrohung zu bekämpfen – oft verlässt sie sich dabei auf vertrauenswürdige Communities, in denen Ingenieure, Netzbetreiber und andere Experten versammelt sind, die keiner Regierung oder Behörde angehören.

Für eine weltweit geführte Diskussion über Cyber-Sicherheit ist eine privatwirtschaftliche Sichtweise wichtig, weil Regierungen dabei mehr über die technischen Herausforderungen und über die Prioritäten

[1] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Das Weiße Haus, Mai 2011.
aka.ms/WhiteHouse-cyberspace

mehrerer Millionen Internetnutzer erfahren. Viele in der Industrie bewährte Methoden könnten so von öffentlich-privaten Partnerschaften übernommen werden und als Grundlage für die Entwicklung von Normen für die Cyber-Sicherheit dienen. Weder Regierungen noch die Privatwirtschaft können diese Herausforderung alleine bewältigen.

DER MICROSOFT-ANSATZ

- Wir fühlen uns verpflichtet, Diskussionen bezüglich der Cyber-Sicherheit und der dafür geltenden Normen mit Partnerschaften zu unterstützen. Regierungen sollten auch weiterhin Lösungen und genormte Verhaltensregeln für mehr Cyber-Sicherheit entwickeln. Gleichzeitig verbessern zusätzliche internationale öffentlich-private Partnerschaften kritische Infrastrukturen und erlauben schnelle Reaktionen für mehr Sicherheit im Cyberspace.
- Unser Global Security Strategy and Diplomacy-Team arbeitet partnerschaftlich mit Regierungen, Industrieunternehmen und gemeinnützigen Organisationen zusammen und leistet dabei einen Beitrag zur internationalen Diskussion für mehr Cyber-Sicherheit.

STRATEGISCHE ÜBERLEGUNGEN

- **Geeignete Foren**. Diskussionen über die Entwicklung von Normen für eine hohe Cyber-Sicherheit sind dann erfolgreich, wenn Regierungen ein geeignetes Forum dafür schaffen. Mitglieder eines solchen Forums müssen die jeweiligen Fachbereichsexperten der Regierungen sein, zudem müssen Informationen aus der Privatwirtschaft in die Diskussion einfließen, und es sollten regelmäßige Fortschritte erzielt werden.
- **Öffentlich-private Partnerschaften**. Regierungen müssen Normen für mehr Cyber-Sicherheit gemeinsam mit der Privatwirtschaft entwickeln, weil diese den größten Teil der weltweiten Netze betreibt. Obwohl Regierungen primär für internationale Verhandlungen zuständig sind, leisten die Beiträge aus der Privatwirtschaft aufgrund der umfangreichen Erfahrungen beim Netzbetrieb einen wichtigen Beitrag zu der Diskussion.
- **Schwerpunkt ist der Konsens**. Regierungen sollten sich vor allem auf diejenigen Bereiche konzentrieren, in denen kurzfristige Übereinstimmungen erzielt werden können. Ein gutes Beispiel hierfür wäre eine Vereinbarung in bestimmten Bereichen mit allgemeinem Interesse – wie etwa, um die Bedrohung kritischer Infrastrukturen zu verhindern. Dies verspricht mehr Erfolg als die Diskussion komplexer Sachverhalte, für die durch unterschiedliche nationale und kulturelle Vorgaben eine Einigung komplizierter wird.

Hilfreiche Ressourcen

Die Microsoft-Strategie und -Vorgehensweise für mehr globalen Schutz
www.microsoft.com/security/gssd

Cyber-Schutz-Normen für eine sichere Cyber-Zukunft
aka.ms/Secure-cyber-future

Normen für Cyber-Schutz und öffentlich-private Partnerschaften: Mehr Vertrauen und Schutz im Cyberspace
aka.ms/norms-public-private

Entwicklungen im Bereich Information und Telekommunikation im Zusammenhang mit internationaler Sicherheit (UN First Committee)
aka.ms/UN-cyber-security

Schutz von kritischen Infrastrukturen

Die wichtigsten Punkte im Überblick

- Nationale Sicherheit und internationale Richtlinien für kritische Infrastrukturen haben sich zu den Kernsystemen des öffentlichen Lebens, des Gesundheitswesens und der allgemeinen Sicherheit entwickelt. Sie sind zunehmend vernetzt und abhängig von der IT-Infrastruktur.
- Die Sicherheit komplexer kritischer Infrastrukturen stellt uns vor eine einzigartige Herausforderung, auf die wir in nie gekannter Weise antworten müssen. Das erfordert die Zusammenarbeit von Technologieanbietern, Regierungen, Unternehmen und Anwendern, um innovative und effiziente Lösungen zu entwickeln und einzusetzen.
- Das Microsoft Global Security Strategy and Diplomacy-Team arbeitet mit Regierungen, Unternehmen und gemeinnützigen Organisationen an einer besseren Cyber-Sicherheit. Dabei macht es Vorschläge, wie mehr Vertrauen mit welchen Richtlinien aufgebaut werden kann, und es hilft, Prozesse, die für die nationale, wirtschaftliche und öffentliche Sicherheit wichtig sind, besser zu schützen.

HINTERGRUND

Regierungen konzentrieren ihre Anstrengungen auf die Verbesserung kritischer Infrastrukturen für die nationale Gesamtwirtschaft und Sicherheit. Als kritische Infrastrukturen gelten Kernsysteme und alle damit bereitgestellten Dienste und Funktionen, die, falls deren Bereitstellung unterbrochen wird, sowohl das öffentliche Gesundheitswesen als auch die allgemeine Sicherheit, den Handel und die nationale Sicherheit schwächen oder gar lahmlegen.

Mit verbesserten Anwendungen, Kommunikationstechnologien und IT-Diensten gelang es zwar, die Kernsysteme zu verbessern und miteinander zu vernetzen, aber gerade diese Vernetzung verstärkt auch die Bedenken. Kritische Infrastrukturen sind beliebte Ziele von Kriminellen, und die immer ausgefeilteren Attacken auf die vernetzten Systeme bergen die große Gefahr weit verbreiteter Schäden und Systemausfälle.

Diese einzigartigen Sicherheitsbedrohungen der komplexen kritischen Infrastrukturen erfordern schnelle Abwehrreaktionen. Technologieanbieter, Regierungen und Unternehmen müssen dabei eng kooperieren und innovative, effiziente Lösungen gemeinsam entwickeln und einsetzen. Wir unterstützen diese partnerschaftliche Zusammenarbeit und helfen dabei, die Quellen dieser Bedrohungen zu entdecken und aktiv zu bekämpfen. Dies ist der Grund, warum wir unser Global Security Strategy and Diplomacy-Team aufgebaut haben.

DER MICROSOFT-ANSATZ

Mit dem Global Security Strategy and Diplomacy-Team leisten wir einen Beitrag für mehr Sicherheit und weniger verwundbare kritische Infrastrukturen. Dies erreichen wir, indem wir vertrauenswürdige Anwendungen und IT-Dienste entwickeln, die Teil von innovativen Sicherheitslösungen sind. Zudem arbeitet unser Team eng mit Regierungen sowie den Betreibern und Verwaltern kritischer Infrastrukturen zusammen, um Risiken schnell zu beheben oder ganz zu vermeiden.

Der Schutz kritischer Infrastrukturen erfolgt in drei Bereichen:

- **Vorgaben und Richtlinien für mehr Vertrauen**. Verständliche und effiziente Richtlinien geben klar definierte Ziele und Prioritäten vor, mit denen IT-Verantwortliche Ressourcen besser schützen und Investitionen gezielt zur Vermeidung der größten Risiken einsetzen. Wir unterstützen die Entwicklung von effektiven, flexiblen und innovativen, national und international eingesetzten Lösungen zum Schutz kritischer Infrastrukturen.

- **Störungsresistenter Betrieb**. Wir helfen dabei, kritische Infrastrukturen besser vor Ausfällen zu schützen, die als Folge von Attacken entstehen. Zum einen stellen wir hierfür bewährte Methoden bereit, zum anderen schützen wir mit nahtlos ineinandergreifenden Abwehrmechanismen vor Attacken. Je geringer die Störungsanfälligkeit ist, umso zuversichtlicher verwalten IT-Experten ihre IT-Umgebungen.
- **Innovative Investitionen**. Kontinuierliche Weiterentwicklungen verbessern die Sicherheitsmerkmale deutlich. Mit innovativen Umgebungen profitieren IT-Experten und Unternehmen von neuen Ideen, erweiterten Produkten und Prozessen, umfassender Unterstützung und mehr Trainings. Wir unterstützen diese gemeinsamen Anstrengungen zum Schutz kritischer Infrastrukturen mit wegweisenden neuen Methoden, Programmen sowie Weiterbildungsmaßnahmen, und indem unsere Forschungsergebnisse in die Entwicklung neuer Sicherheitslösungen einfließen.

STRATEGISCHE ÜBERLEGUNGEN

Weltweit sind führende Persönlichkeiten über die Sicherheitsbedrohungen sehr besorgt. Insbesondere gilt dies für die Bedrohung der voneinander abhängigen globalen Systeme und der damit verbundenen wirtschaftlichen Stabilität, aber auch der Klimawandel und die nationale Sicherheit werden dadurch beeinflusst. Es existiert ein enormes Störpotenzial, das jederzeit kritische Infrastrukturen lahmlegen und damit unvorhersehbare, weltumspannende Schäden verursachen kann – ähnlich der aktuellen globalen Finanzkrise.

Die Vorhersage solcher Störungen und deren Folgen ist eine große Herausforderung für die Experten. Denn sie benötigen dafür unter anderem auch einheitliche Aussagen von Regierungen und Unternehmen über die Vorgehensweise zur Störungsbekämpfung.

Öffentlich-private Partnerschaften müssen zuverlässige Sicherheitskonzepte erstellen, mit denen sie kritische Infrastrukturen vor ständig wechselnden Bedrohungen und immer perfideren Attacken schützen.

Diese Sicherheitskonzepte sollten folgende Bestandteile berücksichtigen:

- **Eine bessere und sicherere Entwicklung** mit getesteten und effektiven Prozessen wie dem Microsoft Security Development Lifecycle.
- **Eine einheitliche Aussage** über die Vorgehensweise. Sie sollte Partnerschaften, Investitionen und die Mittel berücksichtigen, die für den Kampf gegen die Bedrohungen zur Verfügung stehen.
- **Gemeinsame Informationen und geprüfte Sicherheitsmechanismen** helfen Regierungen und den Betreibern von kritischen Infrastrukturen, situationsbedingte Sicherheitsrisiken zu erkennen. Sie reagieren damit schnell und verhindern oder eliminieren nationale oder internationale Bedrohungen im Nu.
- **Der Einsatz neuester Netztechnologien** ermöglicht moderne Sicherheitslösungen mit mehr und zuverlässigeren Kommunikationsmöglichkeiten.
- **Eine intensivere Forschung im Bereich IT-Sicherheit** löst aktuelle Probleme. Die Bündelung von akademischem und professionellem Fachwissen liefert Lösungsansätze für künftige Bedrohungen. Die daraus resultierenden Weiterbildungsmaßnahmen und die Weitergabe des Wissens durch Mentoren und Trainer halten künftige IT-Experten und verantwortliche Entscheider auf dem Stand der Technik.

Hilfreiche Ressourcen

Das Microsoft Security Response Center
www.microsoft.com/msrc

Die Microsoft-Strategie und -Vorgehensweise für mehr globalen Schutz
www.microsoft.com/security/gssd

Das Industriekonsortium für mehr Sicherheit im Internet
www.icasi.org

Software Assurance Forum for Excellence in Code (SAFECode)
www.safecode.org

Februar 2013

Datendiebstahl

Die wichtigsten Punkte im Überblick

- Der Diebstahl von Daten setzt Anwender einem erhöhten Betrugsrisiko und wahrscheinlicheren Identitätsmissbrauch aus. Zusätzlich wird das meist jahrelang gewachsene Vertrauensverhältnis zwischen Anwendern sowie Unternehmen und Regierungen empfindlich gestört.
- Microsoft will eine sichere und vertrauenswürdige Rechnernutzung aufbauen. Dazu gehört der Schutz vertraulicher Daten und persönlicher Informationen. Wir empfehlen für die Datenverwaltung einen Ansatz, der Richtlinien, Anwenderverhalten, Prozesse und Technologien berücksichtigt. Diese Empfehlung basiert auf unserer langjährigen Erfahrung bei Aufbau und Verwaltung sicherer Infrastrukturen und bei der Entwicklung ausgefeilter Systeme für die Identitäts- und Zugriffsverwaltung. Dazu gehört auch der Schutz von Informationen mit Überwachungs- und Berichtssystemen.
- Microsoft unterstützt Meldegesetze über Datendiebstahl, die mit einem risikoabhängigen Hinweissystem Nachrichten versenden, wenn eine nicht autorisierte Person auf geschützte Daten zugreift. Dies sollte nur geschehen, wenn ein erhöhtes Risiko für Betrug und Identitätsmissbrauch besteht, nicht bei einem minimalen Risiko. Dieses Gesetz sollte Anwender möglichst zeitnah informieren, es sei denn, eine Strafverfolgungsbehörde übernimmt dies im Zuge bereits eingeleiteter Ermittlungen.

HINTERGRUND

In den vergangenen Jahren berichteten Medien immer wieder von Datendiebstählen in öffentlichen Organisationen und Unternehmen der Privatwirtschaft. Weil dies auch Millionen vertraulicher persönlicher Daten und finanzieller Informationen betraf, war die öffentliche Aufmerksamkeit sehr hoch. Datendiebstahl bedroht nicht nur Anwender durch Betrug und Identitätsmissbrauch. Meistens wird auch das jahrelang gewachsene Vertrauensverhältnis zwischen ihnen und Unternehmen und Regierungen empfindlich gestört.

Viele Regierungen prüfen und überarbeiten derzeit die Meldegesetze über Datendiebstahl. Die vorhandenen Gesetze verpflichten normalerweise Unternehmen oder Behörden dazu, Anwender zu informieren, wenn ihre persönlichen Daten einem Risiko ausgesetzt sind oder missbraucht wurden. Dies geschieht entweder, wenn ein unbefugter Zugriff erkannt wird, oder mit einem risikoabhängigen Hinweissystem.

Im erstgenannten Fall müssen Unternehmen, die einen unbefugten Zugriff erkennen, die betroffenen Personen darüber informieren, dass ein nicht autorisierter Anwender auf ihre persönlichen Daten zugreifen wollte. Diese Informationspflicht ist unabhängig davon, ob der nicht autorisierte Anwender tatsächlich Daten entwendet hat oder der Versuch des Datendiebstahls erfolglos war. Im Gegensatz dazu müssen beim Einsatz eines risikoabhängigen Hinweissystems Unternehmen Anwender immer informieren, wenn ein potenzielles Risiko entdeckt wurde.

Obwohl Regierungen neue Richtlinien über die Hinweispflicht von Datendiebstählen entwickeln, ist ein Punkt besonders bemerkenswert: Es gibt in einigen Rechtsordnungen Unternehmen, die von einer Meldepflicht ausgenommen sind, wenn die Daten zum Zeitpunkt des Diebstahls verschlüsselt waren. Diese Ausnahmen sind für viele Unternehmen ein motivierender Faktor, Methoden zur Datenverschlüsselung einzusetzen und damit vertrauliche Daten besonders zu schützen. Unternehmen, die ausgefeilte Konzepte für die Datenverwaltung verwenden, reduzieren zusätzlich das Risiko eines Datendiebstahls. Denn sie machen dabei normalerweise effiziente Vorgaben für das Vorgehen im Falle entdeckter Sicherheitsrisiken.

DER MICROSOFT-ANSATZ

Wir empfehlen einen vielschichtigen Ansatz für die Datenverwaltung, der Richtlinien, Anwenderverhalten, Prozesse und Technologien berücksichtigt. Dieser Ansatz setzt auf:

- Eine mit Sicherheitsmechanismen verstärkte Infrastruktur, die Systeme vor Malware, Eindringlingen und nicht autorisierten Zugriffen auf vertrauliche Informationen schützt.
- Eine Identitäts- und Zugriffskontrolle, die vertrauliche Informationen vor unbefugten Zugriffen und Missbrauch schützt und eine ausgefeilte Verwaltung von Identitäten sowie deren Bereitstellung ermöglicht.
- Eine Speicherung vertraulicher, persönlicher Informationen in strukturierten Datenbanken, mit Schutzfunktionen wie einer Verschlüsselung von unstrukturierten Dokumenten, Nachrichten und Datensätzen.
- Ein Überwachungs- und Berichtssystem für die Systemintegrität, das zudem prüft, ob die Daten den unternehmensinternen Richtlinien entsprechen.

STRATEGISCHE ÜBERLEGUNGEN

- Sich widersprechende Gesetze können eine einheitliche regionale, nationale oder internationale Auslegung erschweren. Die große Vielfalt vorhandener Gesetze, Regeln, Verordnungen und Vorgaben verhindert oft den volkswirtschaftlichen Fortschritt und Innovationen. Ein gutes Beispiel hierfür sind die Vereinigten Staaten von Amerika mit ihren vielen verschiedenen Gesetzen in den einzelnen US-Bundesstaaten. Dort unterstützen wir eine breit angelegte, föderale Vorgehensweise für eine umfassende und einheitliche Gesetzgebung hinsichtlich der Privatsphäre. Gesetzgeber, Unternehmen und Organisationen müssen gemeinsam eine allseits anerkannte Lösung entwickeln, die sowohl die Privatsphäre als auch Innovationen schützt.
- Wir unterstützen Meldegesetze über Datendiebstahl, die Folgendes beinhalten:
  - » Ein risikoabhängiges Hinweissystem, das Anwender immer dann informiert, wenn eine nicht autorisierte Person auf vertrauliche Daten zugreift und wenn ein ernsthafter Verdacht auf einen Betrugsversuch oder Identitätsmissbrauch besteht.
  - » Wenn das potenzielle Risiko einer Schädigung oder eines Datendiebstahls sehr gering ist, soll keine Benachrichtigung des Anwenders erfolgen. Das ist beispielsweise dann der Fall, wenn die Informationen verschlüsselt oder auf andere Art und Weise für nicht autorisierte Personen unlesbar sind.
  - » Anwender sollen möglichst zeitnah informiert werden, es sei denn, eine Strafverfolgungsbehörde übernimmt dies im Zuge bereits eingeleiteter Ermittlungen.
- Obwohl wir eine obligatorische Information der Anwender über einen Datendiebstahl befürworten, sollte diese Hinweispflicht so ausgelegt werden, dass eine zeitnahe Benachrichtigung mit einer aussagekräftigen Beschreibung des Sachverhalts erfolgt. Werden Anwender zu schnell informiert, sind die gelieferten Informationen aufgrund der kurzen Zeit wahrscheinlich nicht genau genug oder nicht vollständig. Werden andererseits umfangreiche Hinweise auch bei einem vergleichsweise geringen Risiko auf einen Datendiebstahl versendet, werden Anwender höchstwahrscheinlich die vielen Meldungen recht schnell ignorieren.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiative hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Microsoft Computing Safety Index (MCSI)

Die wichtigsten Punkte im Überblick

- Der Microsoft Computing Safety Index (MCSI) basiert auf einer länderübergreifenden Umfrage. Damit ermittelten wir die besten Methoden für eine effiziente Verwaltung und Bekämpfung von Bedrohungen, die Onlineschutz und -sicherheit beeinträchtigen.

- Wir setzen das Werkzeug in unseren jährlichen Untersuchungen ein, mit denen wir weltweit das Onlineverhalten von Anwendern hinsichtlich Schutz und Sicherheit ermitteln und bewerten. Die Ergebnisse liefern einen wichtigen Beitrag für die Entwicklung von Sicherheitstechnologien, und sie sind die Basis für Initiativen, um Anwender besser über die Gefahren im Web aufzuklären.

- Das Microsoft Safety and Security Center bietet Trainings, Leitfäden und kostenlose Hilfsmittel an, mit denen sich Anwender online besser schützen können.

- Wir freuen uns, wenn Regierungen uns im Kampf gegen Online-Sicherheitsbedrohungen unterstützen. Die Kooperation mit staatlichen Institutionen ist einer der effektivsten Wege, um Cyber-Bedrohungen zu vermeiden. Für uns ist ein abgestimmter Ansatz mit gesetzlichen Vorgaben ein wichtiger Teil dabei.

HINTERGRUND

Je mehr Anwender sich online vernetzen, umso größer ist der Bedarf an Sicherheit, Schutz und Privatsphäre. Anwender sind immer öfter von ausgehebelten Sicherheitsvorkehrungen, Betrugsfällen und dem Diebstahl persönlicher, vertraulicher Daten betroffen. Wir glauben, dass ein umfassendes Verständnis des Anwenderverhaltens – wie reagieren sie auf Bedrohungen und wie schützen sie sich davor – wichtig ist. Weil es uns wertvolle Hinweise für die Entwicklung besserer Sicherheitstechnologien liefert und weil es eine hervorragende Basis für Initiativen ist, um Anwender über die Gefahren im Web aufzuklären.

Im Jahr 2010 haben wir eine Studie in Auftrag gegeben, mit der wir mehr darüber erfahren wollten, wie sich Anwender online schützen. Diese Studie ist die Basis, mit der wir den Microsoft Computing Safety Index (MCSI) entwickelt haben. Mit MCSI ist es möglich, das Onlineverhalten hinsichtlich der Sicherheit und der Verwendung von Sicherheitswerkzeugen einzuschätzen. Der Index bewertet mehr als 20 Schutzmaßnahmen, die Anwender nutzen können. Je mehr davon eingesetzt werden, umso höher ist der Wert der Onlinesicherheit. Maximal sind 100 Punkte möglich. Basis des Index ist eine dreistufige Sicherheitsbewertung:

- Grundlagen (30 Punkte). Dabei wird unter anderem der Einsatz und die Aktualität einer Antiviren-Anwendung berücksichtigt, und ob die automatische Aktualisierung von Anwendungen aktiviert ist.
- Technik (40 Punkte). Dabei wird geprüft, wie Onlineinformationen verwaltet werden, ob IP-Adressen sichtbar sind und ob die Einstellungen für die Privatsphäre überwacht werden.
- Verhalten (30 Punkte). Berücksichtigt wird dabei die Sicherheit von Kennwörtern, wie vertrauenswürdig die besuchten Sites sind und ob sich ein Anwender über neueste Sicherheits- und Schutztechnologien informiert.

Wir geben jedes Jahr eine Studie in Auftrag, die mithilfe des MCSI herausfindet, wie sich Anwender und ihre Familien online schützen. Im Jahr 2012 wurden mehr als 10 000 erwachsene Anwender aus 20 Ländern befragt. Mehr als die Hälfte der Befragten (55 Prozent) sahen sich mehrmals Onlinerisiken ausgesetzt, allerdings haben lediglich 16 Prozent mit geeigneten Maßnahmen sich selbst und ihre Daten aktiv geschützt.

Die Studie 2012 untersuchte zudem das Anwenderverhalten mit mobilen Endgeräten. Obwohl 42 Prozent der Befragten die Anwendungen ihrer Arbeitsplatzrechner aktualisieren, führen lediglich 28 Prozent regelmäßige Aktualisierungen der Anwendungen ihres mobilen Endgeräts durch.

Hier sind noch einige weitere bemerkenswerte Ergebnisse der MCSI-Umfrage 2012:

- Die beiden meistgenannten Bedrohungen waren betrügerische E-Mails, die nach vertraulichen Informationen fragten oder auf einen auf dem Rechner entdeckten Virus hinwiesen, sowie aktuelle Viren, Bots, Adware oder Spyware, die auf den Rechner gelangten.
- 31 Prozent der Befragten hatten auf ihrem mobilen Endgerät eine kontinuierlich aktualisierte Antiviren-Anwendung installiert. 23 Prozent prüften bei der Verwendung von sozialen Medien die Standortangaben und Privatsphäreneinstellungen.
- Die höchsten MCSI-Durchschnittswerte für die Rechnersicherheit erreichten die Einwohner von Singapur (42), Malaysia (40), Kanada (39) und Australien (39).

DER MICROSOFT-ANSATZ

Aufklärung und Führung. Das Microsoft Safety and Security Center bietet Anwendern online Unterstützung zum Thema Sicherheit an. Dazu gehören Tipps für einen sicheren Umgang mit sozialen Netzen und mobilen Endgeräten sowie eine verantwortungsvolle Nutzung von Onlinespielen. Weitere Hinweise klären darüber auf, wie Anwender ein unangemessenes Verhalten vermeiden, blockieren und melden.

Technologiewerkzeuge. Wir bieten viele kostenlose Werkzeuge an, mit denen Anwender Onlinerisiken reduzieren. Dazu gehört etwa die Anti-Malware-Anwendung Microsoft Security Essentials. Zusätzlich haben wir viele Sicherheitsfunktionen für Familien in unsere Produkte integriert, wie etwa Microsoft Family Safety als Bestandteil von Windows 8, womit Anwender Kinder überwachen und schützen, die online sind. Ein weiteres Werkzeug sind die Sicherheitseinstellungen für die Xbox- und Xbox 360-Konsole.

Sicherheitsupdates. In unserem Microsoft Security Response Center arbeiten einige der weltweit besten Sicherheitsexperten. Sie helfen unseren Kunden, auf Cyber-Bedrohungen priorisiert zu reagieren. Sobald eine neue Bedrohung auftaucht, wird sie von unserem Center analysiert und mit geeigneten Sicherheitsupdates eliminiert.

Richtlinien und Zusammenarbeit. Wir sind überzeugt davon, dass ein ganzheitlicher Ansatz für mehr Sicherheit nur gemeinsam mit Anwendern, Technologieanbietern, Unternehmen, Regierungen und anderen Organisationen realisiert werden kann.

STRATEGISCHE ÜBERLEGUNGEN

- Unserer Meinung nach ist die Kooperation zwischen Regierungen und führenden Technologieunternehmen der erfolgversprechendste und effektivste Weg im Kampf gegen Cyber-Bedrohungen. Daher unterstützen wir aufeinander abgestimmte Maßnahmen und gesetzliche Regelungen als Teil dieser Kooperation. Wir sind zudem der Meinung, dass weniger restriktive Vorgaben für die Industrie zu mehr Innovationen und flexibleren Reaktionen auf Cyber-Verbrechen führen.
- Die Zusammenarbeit mit Strafverfolgungsbehörden und Polizei ist unserer Meinung nach unbedingt notwendig. Wir bieten dafür technische Trainings an und stellen neue Technologien zur Verfügung, um die Auswirkungen von Cyber-Kriminalität einzudämmen.
- Um die Sicherheit von Onlinesystemen generell zu erhöhen, unterstützen wir Forschungsarbeiten von Regierungen im Bereich Sicherheit auch finanziell. Die Unterstützung von Regierungen im Kampf gegen Cyber-Bedrohungen ist für uns sehr wichtig.
- Wir schützen Anwender auch, indem wir Gerichtsverfahren initiieren oder Anwender unterstützen, die Cyber-Verbrechern das Handwerk legen wollen.

Hilfreiche Ressourcen

Eine Zusammenfassung der MCSI-Umfrage
aka.ms/MCSISurvey

Microsoft Security Essentials,
ein kostenloses Sicherheitswerkzeug
www.microsoft.com/security_essentials

Das Microsoft Safety and Security Center
www.microsoft.com/security

End-to-End-Vertrauen

Die wichtigsten Punkte im Überblick

- End-to-End-Vertrauen steht als Vision für mehr Sicherheit und Vertrauen bei der Rechnernutzung, ermöglicht durch die Zusammenarbeit von Technologieunternehmen und Regierungen.
- Das dem End-to-End-Vertrauen zugrunde liegende Konzept berücksichtigt grundlegende Funktionen für mehr Sicherheit und Privatsphäre. Damit soll eine vertrauenswürdige Architektur entstehen, die Hard- und Software, Daten sowie Anwender umfasst und die technische, soziale, politische und wirtschaftliche Kräfte bündelt. Ergebnis ist ein Identity-Metasystem, das den Abruf von Informationen überprüft.
- Wir arbeiten gemeinsam mit Regierungen sowie Partnern aus der Industrie und anderen Unterstützern an mehreren wichtigen Initiativen. Diese haben unter anderem auch das Ziel, die Sicherheit von personenbezogenen Daten durch eine persönliche Prüfung zu erhöhen. Ein weiteres Ziel ist es, die Risiken für Endgeräte durch Richtlinien für den Zugriff zu minimieren und so auch die im Internet übertragenen Daten besser zu schützen. Zudem sollen Anwender mit geeigneten Hilfsmitteln ihre Privatsphäre, und hierbei insbesondere die Veröffentlichung der persönlichen Daten, besser kontrollieren können.

HINTERGRUND

Das Internet stellt Anwendern viele Hilfsmittel zur Verfügung, mit denen sie sich das Leben erleichtern und weltweit mit anderen Menschen in Kontakt bleiben. Aber je mehr Menschen sich vernetzen, umso wichtiger ist es, die Folgen der Internetnutzung für die Sicherheit, den Schutz und die Privatsphäre zu kennen. Mit unserer Initiative Trustworthy Computing und der Vision des End-to-End-Vertrauens erhalten Regierungen auf der ganzen Welt wichtige Informationen, mit denen sie Richtlinien für mehr Cyber-Sicherheit verabschieden und Initiativen ins Leben rufen können, um so die individuelle Privatsphäre besser zu schützen.

Wir teilen unsere Informationen und Empfehlungen mit Entscheidern und Führungspersönlichkeiten aus Politik, Wirtschaft und Gesellschaft. Wir möchten so eine bessere Priorisierung sowie wirksame Aktionen für eine größere Onlinesicherheit erreichen.

Die konzeptionellen Grundlagen für das End-to-End-Vertrauen sind:

- **Sicherheit und Privatsphäre**. Eine vertrauenswürdige Onlineumgebung verwendet Technologien, die während ihrer Entwicklung von Anfang an sowohl Sicherheit als auch Privatsphäre berücksichtigen.
- **Innovative Technik**. End-to-End-Vertrauen entsteht nur, wenn in einer Umgebung nachvollziehbare und effiziente Vertrauensentscheidungen möglich sind. Solche Umgebungen hängen von einer Architektur ab, die vertrauenswürdige Hard- und Software, Daten sowie Anwender umfasst.
- **Soziale, wirtschaftliche, politische und informationstechnologische Ausrichtung**. Mit technischen Lösungen lässt sich End-to-End-Vertrauen nur implementieren, wenn diese gleichzeitig von einem wirtschaftlichen Modell unterstützt werden. Berücksichtigt eine Lösung keine sozialen Normen wie etwa die Privatsphäre, kann auch dies dem Aufbau von Vertrauen entgegenwirken. Nur wenn die technischen, wirtschaftlichen, politischen und sozialen Kräfte gebündelt werden, lässt sich eine hohe Vertrauensstellung erreichen.

Wir engagieren uns mit Regierungen und Industriepartnern in den folgenden drei Projekten, mit denen wir unsere Vision umsetzen möchten:

- **Geprüfte Identität**. Besonders hochwertige Transaktionen wie etwa beim Onlinebanking erfordern eine hohe Sicherheit. Um diese hinsichtlich der Identität zu erhöhen, ist eine

Möglichkeit die persönliche Prüfung. Weil viele andere Onlinetransaktionen eine derart hohe Sicherheit nicht benötigen, ist die Einführung eines Onlinesystems, das verschiedene Sicherheitsprüfungen anbietet, sehr wichtig – genauso wichtig übrigens wie ein integrierter Schutz der Privatsphäre, wenn etwa der Name eines Anwenders nicht unbedingt bekannt sein muss. Ein derartiges System sollte auch neue Identitätsdienste unterstützen, die jede Anforderung von Anwender- und Endgeräteinformationen überprüfen. Wir helfen anderen Unternehmen bei der Entwicklung solcher Identity-Metasysteme, die alle Abrufe von Informationen prüfen.

- **Endgeräte-Status**. Der Wunsch nach einer einfachen, einheitlichen, sicheren und unabhängigen Prüfung, ob Endgeräte, die sich mit dem Internet verbinden, vertrauenswürdig sind, ist groß. Mit diesem Projekt wollen wir eine standardisierte Lösung erstellen, die Rechner, die hochwertige Transaktionen durchführen, verifiziert.
- **Richtliniengesteuerter Datenschutz**. Eine der größten Herausforderungen im Internet und in der Cloud ist es, den Zugriff auf vertrauliche Daten nur Anwendern zu gestatten, die dazu berechtigt sind. Viele vertrauliche Daten werden oft von Unternehmen an externe Anwender und verschiedene Endgeräte weitergegeben. Ziel dieses Projekts ist eine Lösung, die Daten und den Zugriff darauf mit Richtlinien und Vorgaben verknüpft. Unabhängig davon, wo die Daten genutzt werden, sollen die gleichen Richtlinien für deren Verwendung gelten.

DER MICROSOFT-ANSATZ

Wir haben die folgenden Empfehlungen und Leitfäden veröffentlicht, mit denen wir die Sicherheit erhöhen und die Privatsphäre besser schützen möchten:

- Der Security Development Lifecycle-Prozess reduziert die Anzahl und Schwere von Attacken auf Software.
- Richtlinien für die Privatsphäre bei der Entwicklung von Anwendungen und Diensten enthalten bewährte Methoden für Entwickler.

Folgende Microsoft-Technologien verbessern die Sicherheit:

- Microsoft Security Essentials ist eine kostenlose Anti-Malware-Anwendung für Windows XP SP2, Windows Vista, Windows 7, Windows 8 und Windows RT.
- Microsoft Forefront besteht aus integrierten Anwendungen, mit denen Unternehmen vor Ort und in der Cloud für mehr Schutz, bessere Identitätsnutzung und sicheren Zugriff sorgen.
- Mit der Microsoft Identity and Access-Lösung erstellen und verwalten Unternehmen Identitäten in Rechenzentren und der Cloud mit einer einzigen und einheitlichen Darstellung. Die Information Protection-Lösung entdeckt, schützt und verwaltet vertrauliche Informationen automatisch und unternehmensweit, indem sie sich in vorhandene Plattformen und Apps integriert.

STRATEGISCHE ÜBERLEGUNGEN

- Wir werden auch weiterhin Regierungen vertrauensvoll beraten, um im Cyber-Ökosystem die Sicherheit und die Privatsphäre zu schützen, die Zuverlässigkeit zu erhöhen, und die Gefährdung durch Cyber-Attacken zu reduzieren. Wir sind davon überzeugt, dass strategische Partnerschaften, zielorientierte Initiativen und die Zusammenarbeit mit anderen Unternehmen und Regierungen entscheidende Faktoren dabei sind.
- Wir haben gemeinsam mit Partnern aus der Industrie Staaten ermutigt, das Übereinkommen über Computerkriminalität des Europarats zu übernehmen und zu ratifizieren. Die Unterzeichner müssen die Gesetze und Prozeduren im Kampf gegen Cyber-Kriminalität übernehmen und anpassen.
- Wir unterstützen Regierungen finanziell, die mit eigenen Mitteln Wege suchen, um die Sicherheit von Onlinesystemen zu verbessern.

Hilfreiche Ressourcen

Die Microsoft-Vision End-to-End-Vertrauen
www.endtoendtrust.org

Der Security Development Lifecycle
www.microsoft.com/SDL

Richtlinien für die Privatsphäre bei der Entwicklung von Anwendungen und Diensten
aka.ms/privacy-guidelines

Microsoft Security Development Lifecycle

Die wichtigsten Punkte im Überblick

- Mit dem Security Development Lifecycle (SDL) haben wir einen Prozess entwickelt, der die Sicherheit bereits in jeder Phase der Anwendungsentwicklung berücksichtigt. Damit entsteht ein Schutz mit tief im System verankerten Verteidigungsmechanismen.
- Der SDL enthält Prozeduren für Tester, Entwickler, Programmmanager und -architekten, die mit den unternehmensweit für die Produktsicherheit zuständigen Teams zusammenarbeiten. Die innovativen Sicherheitsfunktionen sind in Office, Windows-Betriebssysteme, SQL Server und viele weitere Microsoft-Produkte und -Dienste integriert.
- Wir entwickeln den SDL ständig weiter. Aktualisierungen nutzen die Vorteile neuer Sicherheitstechnologien und berücksichtigen neue Bedrohungen.
- Wir stellen den SDL der IT-Branche zur Verfügung. Er wird von vielen Soft- und Hardwareanbietern, Regierungen, Partnern und Anwendungsentwicklern unverändert oder modifiziert übernommen.

HINTERGRUND

Sicherheitsbedrohungen im Cyberspace sind komplex, ausgeklügelt und verändern sich ständig. Um sie erfolgreich zu bekämpfen, sind fortlaufende, mehrschichtige Aktionen aller Unternehmen der IT-Branche nötig. Sie müssen Lösungen für eine optimale Anwendungssicherheit entwickeln, die allen Anwendern weltweit mehr Schutz bei der Rechnernutzung bieten.

Der Security Development Lifecycle (SDL) ist ein Prozess, mit dem wir Aspekte der Sicherheit und Privatsphäre von Anfang an und bei jedem Schritt der Anwendungsentwicklung berücksichtigen. Mit einem ganzheitlichen, praxisorientierten Ansatz bekämpfen wir sich ständig weiterentwickelnde Bedrohungen und zunehmend ausgefeiltere Cyber-Kriminalität.

Wir haben den SDL-Prozess 2004 als Teil eines Ansatzes entwickelt, mit dem die Sicherheit bereits grundlegend auf allen Ebenen berücksichtigt wird. Wir wollten damit die Microsoft-Anwendungen weniger verwundbar machen und allen Anwender eine hochwertige, sehr exakt umgesetzte und intensiv geprüfte Anwendung zur Verfügung stellen, die gefährliche Attacken noch besser abwehrt. Die Microsoft-Entwickler und Sicherheitsexperten haben dann aber festgestellt, dass mit einem wiederholten Prozess ausgeführte Aktionen nicht nur zu mehr Sicherheit und einem schnelleren Return on Investment führen, sondern hierdurch auch eine deutlich besser geschützte Internetumgebung entsteht. Mit dem SDL erstellen Entwickler Anwendungen, die weniger anfällig sind und vor allem vor schweren Schäden besser geschützt sind.

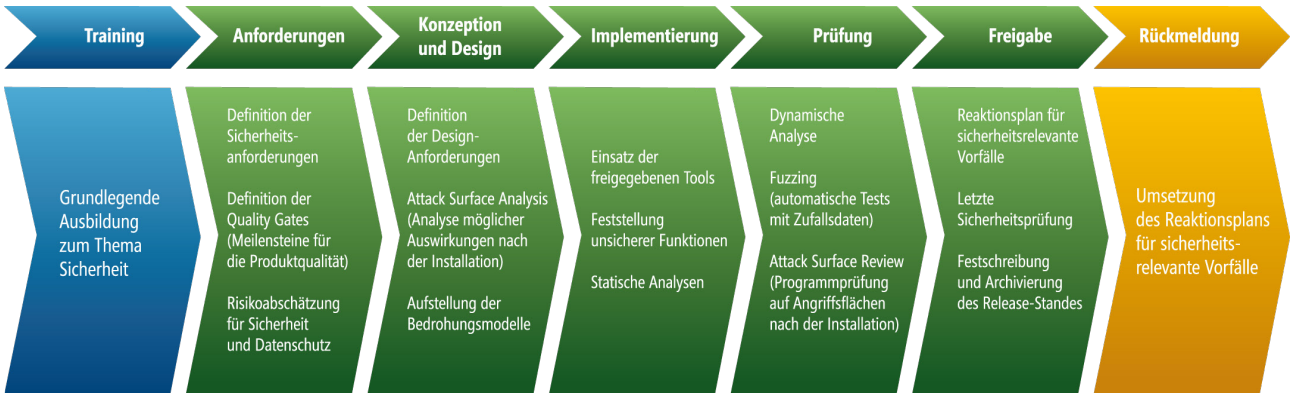
DER MICROSOFT-ANSATZ

- Die Verwendung des SDL ist für die Produktentwicklung bei Microsoft obligatorisch. Wie nachfolgend gezeigt, besteht er aus einer Reihe systematischer Aktivitäten für mehr Sicherheit und Privatsphäre, die während der Anwendungsentwicklung angewendet werden. Es handelt sich dabei unter anderem um technische Trainings für Entwickler oder um Prozesse, mit denen nach dem produktiven Einsatz auf Notfälle reagiert werden kann.
- Die Anwendungsentwicklung ist ein dynamischer Prozess, genau wie der SDL. Es ist unmöglich, während der Anwendungsentwicklung alle möglichen Verwundbarkeiten auszuschließen. Dennoch untersuchen die Microsoft-Entwickler jedes auftretende Problem bis ins kleinste Detail, definieren korrigierende Aktionen und übernehmen dieses Wissen in die nächste SDL-Version.
- Der Einsatz des SDL hat zu messbaren Verbesserungen von Sicherheit und Privatsphäre in Verbindung mit Microsoft-Produkten geführt.

STRATEGISCHE ÜBERLEGUNGEN

- Wir glauben, dass nur die gesamte IT-Community gemeinsam eine hohe Sicherheit erreichen kann. Dafür stellen wir weltweit allen Entwicklern und IT-Spezialisten unsere Erfahrungen und unser Wissen sowie Prozesse und Technologien zur Verfügung. Bis 2012 haben IT-Experten den SDL-Prozess, Whitepapers, Werkzeuge und andere Ressourcen mehr als eine Million Mal heruntergeladen.

  Die SDL Chronicles dokumentieren, wie der Security Development Lifecycle in öffentlichen Organisationen und privaten Unternehmen die Entwicklungsarbeit beeinflusst hat und so Anwendungen mit höherer Sicherheit entstanden sind. Führende Unternehmen wie Cisco und Adobe nutzen Microsoft SDL als Grundlage für die Entwicklung sicherer Anwendungen.
- Jede Regierung, die das Problem der Informationssicherheit lösen möchte, sollte zudem auch Innovationen schützen und immer die neuesten Technologien verwenden. Regierungen und Unternehmen sollten gemeinsam eine geeignete Grundlage entwickeln, die mit einer ausgewogenen Gewichtung von gesetzlichen Vorgaben und innovativen Lösungen eine effiziente Vorgehensweise erlaubt.



Hilfreiche Ressourcen

Der Security Development Lifecycle
www.microsoft.com/sdl

Die SDL Chronicles
aka.ms/SDL-Chronicles

Microsoft Trustworthy Computing
www.microsoft.com/twc/

Microsoft Security Intelligence Report

Die wichtigsten Punkte im Überblick

- Der Microsoft Security Intelligence Report bietet eine umfassende, aktuelle und geografisch aufbereitete Analyse der Cyber-Bedrohungen. Er berücksichtigt Informationen über Schadsoftware, Schwachstellen und Malware, die Internetdienste und weltweit mehr als 600 Millionen Rechner bereitstellen.

- Unser Trustworthy Computing-Team ist verantwortlich für die Umsetzung einer langfristigen Zusammenarbeit für mehr Sicherheit, Privatsphäre und Zuverlässigkeit bei der Rechnernutzung. Grundlage dafür sind die Security Science-Initiative, der Schutz kritischer Infrastruktur, die Bereitstellung sicherer Produkte und der Schutz vor Malware.

- Wir glauben, dass die Kooperation zwischen Industrie und Behörden der effizienteste Weg ist, um Cyber-Bedrohungen zu verringern. Daher unterstützen wir auch eine ausgewogene, angepasste Regulierung als Teil dieser Kooperation.

HINTERGRUND

Das Internet ist fester Bestandteil unseres Lebens geworden. Je mehr Menschen aber online sind, umso größer sind die Bedenken wegen ihrer Sicherheit. Aus gutem Grund, denn mit der zunehmenden Zahl an Internetanwendern geht auch ein dramatischer Zuwachs bei den Onlineverbrechen einher. Dies wiederum führt dazu, dass immer mehr Regierungen weltweit über dieses Sicherheitsproblem besorgt sind.

Onlinebedrohungen haben sich von kleineren Vergehen, mit denen Hacker Aufmerksamkeit auf sich ziehen, hin zu ausgefeilten kriminellen Attacken organisierter Banden ausgewachsen. Cyber-Kriminelle greifen Anwender per E-Mail, Browser, Sozialen Medien, Onlinespielen und gefälschten Sicherheitsanwendungen an. Betroffene Rechner werden für den Einbruch in Sicherheitssysteme und für den Datendiebstahl aus Finanzinstituten missbraucht, attackieren politische Parteien und stehlen Geld oder gar die Identität von Menschen – und letztendlich damit auch ihren Glauben an Sicherheit.

Als einer der Partner, die sich dem Kampf gegen Onlineverbrechen verschrieben haben, stellen wir Ressourcen und Fachwissen zur Verfügung. Hierzu gehört auch der zweimal pro Jahr veröffentlichte Security Intelligence Report (SIR), der über die jüngsten Bedrohungen informiert. Der Bericht enthält umfassende aktuelle und geografisch aufbereitete Analysen der Cyber-Bedrohungen. Er berücksichtigt Informationen über Schadsoftware, Schwachstellen und Malware, die einige der aktivsten Onlinedienste im Internet und weltweit mehr als 600 Millionen Rechner bereitstellen. Die SIR-Ausgabe 13, Januar bis Juni 2012[1], umfasst mehr als 900 Seiten und analysiert die Cyber-Bedrohungen aus 105 Ländern und Regionen der Erde.

Die jüngsten SIR-Ausgaben ergaben, dass Cyber-Kriminelle immer mehr dazu übergehen, mit gefälschten Schlüsseln für die Aktivierung von Anwendungen Malware auf einen Rechner zu schleusen. Diese immer öfter verwendete, sogenannte soziale Attacke ist mittlerweile zur weltweit größten Bedrohung für Anwender geworden. SIR zeigt aber auch, dass sich soziale und ähnlich gelagerte Attacken durch bewährte Sicherheitsmethoden, wie etwa den Einsatz eines effizienten technischen Schutzes, durchaus vermeiden lassen.

[1] **aka.ms/SIR-V13**

Wir kennen den Umfang und die sich laufend verändernde Komplexität der Onlinesicherheit. Wir wissen auch, welch enormer Aufwand von uns allen betrieben werden muss, wenn nach einer Attacke Support, Hilfe und aktuelle Informationen bereitgestellt werden müssen. Wir werden deshalb auch weiterhin den globalen Ansatz unterstützen, mit dem wir unser Wissen mit führenden Unternehmen, Regierungen und Sicherheitsorganisationen teilen.

DER MICROSOFT-ANSATZ

Unser Trustworthy Computing-Team ist verantwortlich für die Umsetzung einer langfristigen Zusammenarbeit für mehr Sicherheit, Privatsphäre und Zuverlässigkeit bei der Rechnernutzung. Das Team arbeitet unter anderem in den folgenden Bereichen:

- **Security Science**. Grundlage dieser Initiative sind Untersuchungen über die Art und Weise, wie Systeme attackiert werden und wie sich diese Attacken verhindern lassen. Im Rahmen unserer Security Science-Initiative entwickeln wir Werkzeuge und Techniken, die Attacken auf Systeme erschweren. Zudem überwachen wir mit der Initiative Bedrohungstrends und erkennen Schwachstellen von Anwendungen. Mit den dabei gewonnenen Informationen erstellen wir Werkzeuge und Techniken, mit denen Entwickler die Gesamtsicherheit verbessern können.
- **Der Schutz kritischer Infrastrukturen**. Technologien sind ein immer wichtigerer Bestandteil unseres Lebens. Das Trustworthy Computing-Team setzt sich gemeinsam mit Regierungen weltweit für einen besseren Schutz kritischer Infrastrukturen und mehr Sicherheit für Onlineanwender ein. Unser Team teilt seine Informationen und Innovationen mit anderen, damit gemeinsame Richtlinien die globale Cyber-Sicherheit verbessern.
- **Die Bereitstellung sicherer Produkte**. Das Microsoft Security Engineering Center schützt unsere Kunden durch Produkte, die wir mit dem Security Development Lifecycle (SDL) erstellen und die daher einen hohen Sicherheitsstandard aufweisen. Der SDL ist ein in der IT-Branche anerkannter Prozess für die Entwicklung sicherer Anwendungen. Er berücksichtigt in jeder Entwicklungsphase einer Anwendung sowohl Sicherheitsaspekte als auch die Privatsphäre.
- **Der Schutz vor Malware**. Das Microsoft Malware Protection Center analysiert Malware und entwickelt Lösungen, die wir mit unseren Sicherheitstechnologien verwenden. Entdecken wir eine Schwachstelle in einer Anwendung, überwacht das Malware Protection Center diese und entwickelt eine Gegenmaßnahme. Das Center verwaltet zudem den Prozess, mit dem wir Sicherheitsupdates veröffentlichen, und ist dabei die zentrale Koordinationsstelle.

STRATEGISCHE ÜBERLEGUNGEN

- Wir freuen uns, dass viele Regierungen uns im Kampf gegen Cyber-Verbrechen unterstützen. Wir sind überzeugt davon, dass nur die Kooperation von Unternehmen und Regierungen die Cyber-Bedrohungen effektiv reduzieren kann und dass ausgewogene gesetzliche Vorgaben Teil dieser Vorgehensweise sein müssen. Zudem sind wir überzeugt davon, dass weniger Restriktionen für Unternehmen zu mehr Innovationen und einer flexibleren Entwicklung und Implementierung von Lösungen für den Kampf gegen Cyber-Kriminalität führen.
- Wir ermutigen gemeinsam mit Partnern aus der Industrie Staaten, das Übereinkommen über Computerkriminalität des Europarats zu übernehmen und zu ratifizieren. Die Unterzeichner müssen die Gesetze und Prozeduren im Kampf gegen Cyber-Kriminalität übernehmen und anpassen.
- Wir unterstützen Regierungen finanziell, die mit eigenen Mitteln Wege suchen, um die Sicherheit von Onlinesystemen zu verbessern.

Hilfreiche Ressourcen

Das Microsoft Security Response Center
www.microsoft.com/msrc

Der Microsoft Security Intelligence Report
www.microsoft.com/sir

Das Microsoft Malware Protection Center
www.microsoft.com/mmpc

Das Übereinkommen über Computerkriminalität des Europarats
aka.ms/Convention-on-Cybercrime

Microsoft Security Response Center

Die wichtigsten Punkte im Überblick

- Das Microsoft Security Response Center (MSRC) ist die zentrale Anlaufstelle für die Koordination und Kommunikation aller Themen im Bereich der Sicherheit. Es wird von einigen der weltweit erfahrensten Experten geleitet. Das MSRC identifiziert, überwacht, löst und beantwortet Sicherheitsvorfälle, darunter auch Schwachstellen in Microsoft-Anwendungen. Zudem verwaltet es die monatlichen Sicherheitsupdates und veröffentlicht den Sicherheitsupdate-Leitfaden, Sicherheitsratschläge und den halbjährlich erscheinenden Security Intelligence Report.

- Wir befürworten eine nachvollziehbare, koordinierte Veröffentlichung der Schwachstellen unserer Anwendungen. Zudem nutzen wir MSVR, MAPP und den Microsoft Exploitability Index, um die Ausnutzung dieser Schwachstellen zu verhindern.

- Wir arbeiten mit der Sicherheits-Community und anderen weltweiten Partnern an einer sicheren Rechnerumgebung und einer besser geschützten, vertrauenswürdigen Internetnutzung. Unter anderem auch mit BlueHat-Sicherheits-Briefings und ICASI.

HINTERGRUND

Die Rechnersicherheit ist eine sich immer weiterentwickelnde, fortwährende Herausforderung. Immer mehr und immer komplexere Bedrohungen verbreiten sich genauso rasant, wie Cyber-Kriminelle immer perfidere Methoden für ihre Attacken entwickeln. Leidtragende sind sowohl große, miteinander vernetzte Systeme als auch einzelne Unternehmen.

Das Microsoft Security Response Center (MSRC) ist Teil unseres Trustworthy Computing-Teams. Wir haben es gegründet, um besser mit den sich weiterentwickelnden Bedrohungen Schritt zu halten und um Kunden mit zeitnahen Aktualisierungen und zuverlässigen Anleitungen umfassend vor Attacken bösartiger Anwendungen zu schützen. Die Leitung des MSRC obliegt einigen der weltweit erfahrensten Sicherheitsexperten, zudem ist es unsere zentrale Anlaufstelle für die Koordination und Kommunikation aller Themen rund um die Sicherheit und deren Bedrohung. Jedes Jahr bearbeitet das MSRC mehr als 100 000 Berichte über Schwachstellen in Microsoft-Anwendungen. Es wird dabei von einem weltweiten Netz von Sicherheitsforschern und Partnern unterstützt, die sehr genau die Inhalte von Newsgruppen und öffentlichen Foren zum Thema Sicherheit analysieren und auswerten. Das MSRC identifiziert, überwacht, löst und beantwortet Sicherheitsvorfälle mit vier Bearbeitungsschritten, sobald es einen Hinweis über eine potenzielle Bedrohung erhält:

- **Bewertung**. Das Team bewertet den zu erwartenden Schaden für Kunden.
- **Untersuchung**. Die MSRC-Experten sammeln so lange Informationen, bis sie die Schädigung nachvollziehen können, und stellen dann fest, welche Produkte oder Dienste davon betroffen sind.
- **Beurteilung der Schwere**. Das MSRC beurteilt jede Verwundbarkeit hinsichtlich ihrer Schwere und der Wahrscheinlichkeit ihres Auftretens.
- **Lösung**. Das Team entscheidet, ob das Problem mit einer sofortigen Aktualisierung des Microsoft-Produkts behoben wird oder ob die Lösung mit der Veröffentlichung eines künftigen Service Packs oder einer neuen Produktversion erfolgt.

Ziel des MSRC ist eine zeitnahe Lösung mit einer aufklärenden Beschreibung des Problems. Die Kommunikation mit Kunden erfolgt über mehrere Kanäle wie unter anderem Blogs, Bulletins, Leitfäden und Webcasts.

- Seit 2003 ist das MSRC unternehmensweit für die Veröffentlichung von Sicherheitsupdates verantwortlich, mit denen wir Schwachstellen

unserer Anwendungen beheben. Die MSRC-Experten schreiben zudem unsere Sicherheitsbulletins, die wir in mehrere Sprachen übersetzen und an jedem zweiten Dienstag eines Monats veröffentlichen.

- Im Jahr 2005 haben wir eine Ergänzung dieser Bulletins eingeführt, die Microsoft Security Advisories. Sie beschreiben Sicherheitsänderungen, für die kein Extra-Bulletin nötig ist, die aber möglicherweise doch die Gesamtsicherheit der Kunden beeinflussen.
- Das MSRC entwickelt den Microsoft Security Update-Leitfaden. IT-Spezialisten setzen unsere Sicherheitsupdates damit optimal um, weil sie so mehr über die zugrunde liegenden Informationen, Prozesse und Werkzeuge erfahren.
- Zweimal pro Jahr veröffentlicht das MSRC unseren Security Intelligence Report. Der Bericht enthält eine umfassende, aktuelle und geografisch aufbereitete Analyse der Cyber-Bedrohungen. Er berücksichtigt Informationen über Schadsoftware, Schwachstellen und Malware, die einige der aktivsten Internetdienste und weltweit mehr als 600 Millionen Rechner bereitstellen.

DER MICROSOFT-ANSATZ

Wir befürworten eine nachvollziehbare, koordinierte Veröffentlichung der Schwachstellen unserer Anwendungen und arbeiten kontinuierlich daran, diese zu beseitigen.

- **Microsoft Vulnerability Research (MSVR)** ist ein Programm, mit dem wir unsere Erfahrungen sowie bewährte Methoden bei der Beseitigung von Schwachstellen der Sicherheits-Community bereitstellen. Wir möchten mit diesem positiven Ansatz für eine weitere Verbesserung des Sicherheits-Ökosystems beitragen.
- Mit dem **Microsoft Active Protections Program (MAPP)** informieren wir Anbieter von Sicherheitsanwendungen über Schwachstellen, die wir im MSRC entdeckt haben. Weil dies vor der Veröffentlichung unserer monatlichen Sicherheitsaktualisierungen geschieht, haben die MAPP-Partner mehr Zeit, einen geeigneten Schutz zu entwickeln, und können ihren Kunden schneller eine Aktualisierung anbieten.
- Den **Microsoft Exploitability Index** haben wir 2008 eingeführt. Kunden bewerten damit Risiken anhand der Wahrscheinlichkeit, mit der eine Schwachstelle innerhalb von 30 Tagen, nachdem wir mit einem Sicherheitsupdate eine Aktualisierung veröffentlicht haben, ausgenutzt wird.

Wir arbeiten mit der Sicherheits-Community und weiteren Partnern an einer höheren Sicherheit für Anwender und einer besser geschützten, vertrauenswürdigen Internetnutzung.

- Die **BlueHat-Sicherheits-Briefings** sind eine exklusive Konferenz für eingeladene Teilnehmer. Ihr Ziel ist es, die Microsoft-Produkte sicherer zu machen. Unsere Sicherheitsexperten treffen sich dort mit externen Spezialisten und tauschen Ideen sowie Erfahrungen darüber aus, wie sich die Sicherheit global effizienter vor Bedrohungen schützen lässt.
- Das von uns mitgegründete **Industry Consortium for Advancement of Security on the Internet (ICASI)** ist ein nicht profitorientierter Zusammenschluss führender Unternehmen der IT-Branche. Wir wollen gemeinsam, international und produktübergreifend die Sicherheit und den Schutz der IT-Infrastrukturen von Unternehmen, Regierungen und Bürgern verbessern.

Hilfreiche Ressourcen

Das Microsoft Security Response Center
www.microsoft.com/msrc

Der MSRC-Blog
blogs.technet.com/msrc

Der Microsoft Security Intelligence Report
www.microsoft.com/sir

Der Microsoft Security Update-Leitfaden
aka.ms/msrc-guide

Microsoft Vulnerability Research (MSVR)
aka.ms/ms-msvr

Das Microsoft Active Protections Program (MAPP)
aka.ms/ms-mapp

Das Industry Consortium for Advancement of Security on the Internet (ICASI)
www.icasi.org

Der Microsoft Exploitability Index
aka.ms/Exploitability-Index

Microsoft Trustworthy Computing
www.microsoft.com/twc

Sicherheit für Wertschöpfungsketten

Die wichtigsten Punkte im Überblick

- Viele Regierungen sorgen sich um die Sicherheit der Wertschöpfungsketten. Insbesondere fürchten sie bösartige Angreifer, die Schadsoftware in IT-Produkte integrieren und damit die Wertschöpfungskette infiltrieren. Derart eingeschleuste gefährliche Produkte können beträchtliche Schäden an Informations- und Kommunikationssystemen verursachen.

- Mit einer vierstufigen Strategie begegnen wir den Risiken, denen unsere Produkte und Dienste als Teil einer Wertschöpfungskette ausgesetzt sind. Die Grundlagen dieser Strategie sind eine Identitäts- und Zugriffssteuerung, der Security Development Lifecycle, sowie Richtlinien und Prozeduren, mit denen wir die Integrität unserer Anwendungen überwachen. Selbstverständlich gehören dazu auch Maßnahmen gegen raubkopierte Anwendungen.

- Regierungen und Unternehmen müssen erkennen, dass die Sicherheit von Wertschöpfungsketten ein gemeinsames Problem ist. Sie müssen mit risikoorientierten Lösungen, bewährten Methoden und internationalen Kooperationen die Sicherheit erhöhen.

HINTERGRUND

Informations- und Kommunkationssysteme spielen für den Handel und in unserem Leben eine immer wichtigere Rolle. Einige der besonders wichtigen Systeme sind mittlerweile zu attraktiven Angriffszielen für Cyber-Kriminelle geworden. Diese starten oft ausgefeilte Attacken, die enorme Schäden bis hin zu langen Unterbrechungen verursachen oder mit denen sie einen nicht autorisierten Zugriff auf Daten erlangen.

Ein beliebtes Ziel der kriminellen Attacken ist die Wertschöpfungskette von Technologieprodukten. Das amerikanische National Institute for Standards and Technology definiert diese als „eine Zusammenfassung von Unternehmen, Menschen, Aktivitäten, Informationen und Ressourcen, mit denen ein Produkt oder ein Dienst (oder Teile davon) von einem Hersteller erstellt und an Unternehmenskunden verteilt wird".

Die Wertschöpfungskette für die Auslieferung von Informations- und Kommunikationstechnologien ist weltweit verteilt. Die Produkte selbst sind oft komplex und bestehen aus vielen Einzelteilen, die verschiedene, weltweit verteilte Unternehmen herstellen. Die Bedenken sind sehr groß, dass auf diesem Weg schädliche oder unerwünschte Funktionen oder gefälschte Elemente in die Wertschöpfungskette gelangen. Sind Produkte erst einmal so geschädigt, können Cyber-Verbrecher damit Systeme überwachen, abschalten oder das Vertrauen der Anwender in die Informations- und Kommunikationssysteme spürbar schädigen.

Der Schutz einer derart vielfältigen globalen Wertschöpfungskette stellt eine große Herausforderung für Regierungen und Unternehmen dar. Für beide sollte klar sein: Eine hohe Sicherheit einer Wertschöpfungskette lässt sich nur gemeinsam schaffen. Wobei die Lösungen dafür nicht nur bewährte Methoden berücksichtigen, sondern auch durch internationale Kooperationen die Risiken minimieren müssen.

DER MICROSOFT-ANSATZ

Unsere Strategie, mit der wir die Risiken für Wertschöpfungsketten und unsere damit eingesetzten Produkte und Dienste verringern möchten, beinhaltet:

- Eine **Identitäts- und Zugriffssteuerung** mit Richtlinien, Prozeduren und Technologien verwaltet persönliche Zugriffe auf geistiges Eigentum von Microsoft.

- Der **Security Development Lifecycle** trägt wesentlich dazu bei, bereits während der Entwicklung unserer Anwendungen die Risiken zu reduzieren. Zudem schützt er Produkte besser vor bösartigen und unbeabsichtigten Attacken und verringert ihre Verwundbarkeit.
- **Überwachung der Anwendungsintegrität.** Wir schützen mit Richtlinien, Prozeduren und Technologien die Integrität unserer Anwendungen. Dazu gehören auch Maßnahmen wie Code Signing und die Überprüfung wegen Malware.
- **Maßnahmen gegen Fälschungen.** Gefälschte Anwendungen enthalten oft Schwachstellen. Wir schützen Kunden davor, indem wir die Echtheit unserer eingesetzten Produkte gewissenhaft prüfen. Als weitere Maßnahme verbessern wir fortlaufend die Integrität der Softwareverteilung und arbeiten weltweit sehr eng mit Strafverfolgungsbehörden im Kampf gegen Raubkopierer zusammen.

Zudem verfolgen wir kriminelle, gegen die Wertschöpfungskette gerichtete Attacken sowohl gerichtlich als auch mit technischen Aktionen. Die Microsoft Digital Crimes Unit beispielsweise kämpft gemeinsam mit vielen unserer Teams gegen Botnetze. Eine solche Initiative ist Microsoft Active Response for Security (MARS), mit der wir kriminell genutzte Infrastrukturen bekämpfen. Dabei strengen wir Gerichtsverfahren an und führen technische Aktionen durch, mit denen wir Botnetze verfolgen und die von ihnen verursachten Schäden beheben. Im Jahr 2012 gelang es uns mit MARS, das Nitol-Botnetz auszuschalten, das Rechner durch Schwachstellen in der Wertschöpfungskette infizierte.

STRATEGISCHE ÜBERLEGUNGEN

Rahmenbedingungen, die Risiken für Wertschöpfungsketten verringern, sollten den folgenden Prinzipien folgen:

- Mit einem **risikoorientierten Ansatz** vermeiden es Regierungen, mit banalen Faktoren wie etwa dem Herkunftsland eines Originalprodukts das Risiko einzuschätzen. Denn aufgrund der weltweiten Verfügbarkeit von Produkten würde dies zu einem weit verbreiteten Bann der Produkte führen. Die Folge wäre eine Schwächung des öffentlichen Handels und ein Verzicht auf die Vorteile globaler Innovationen. Regierungen sollten daher besser auf bewährte Grundsätze der Risikobeurteilung vertrauen.
- **Transparenz**. Regierungen erwarten zu Recht eine angemessene Transparenz von IT-Unternehmen und deren Geschäftsprozessen. Dies gilt insbesondere auch für die Sicherheit bei der Entwicklung und dem Einsatz von Produkten.

  Ein gutes Beispiel hierfür liefert das Microsoft Government Security Program, mit dem wir einigen Regierungen Zugriff auf den Quelltext einiger unserer Anwendungen erlauben. Trotz aller Transparenz müssen Regierungen aber auch verstehen, dass Unternehmen ihr geistiges Eigentum und ihre Firmengeheimnisse nicht offenlegen möchten.
- **Flexibilität.** Auch wenn Regierungen Sicherheitsstandards für Wertschöpfungsketten übernehmen, muss die Verwaltung und Verwendung dieser Standards flexibel bleiben.
- **Gegenseitigkeit**. Die Entwicklung international gültiger, gemeinsam genutzter Standards für die Sicherheit einer Wertschöpfungskette ist ein wesentlicher Punkt für eine sichere Internetnutzung. Denn die Vorteile dabei setzen nicht nur die Sicherheit, sondern auch die Integrität von IT-Systemen voraus.

Hilfreiche Ressourcen

Die Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/gssd

Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust
aka.ms/supply-chain-risk

Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity
aka.ms/Trusted-Supply-Chain

Der Microsoft Security Development Lifecycle
www.microsoft.com/sdl

Das Software Assurance Forum for Excellence in Code (SAFECode)
www.safecode.org

Februar 2013

Die Privatsphäre im Überblick

Die wichtigsten Punkte im Überblick

- Anwender erwarten von den eingesetzten Produkten und Diensten einen hohen Schutz ihrer Privatsphäre, und sie haben sehr genaue Vorstellungen darüber, wie Unternehmen ihre Daten sammeln, verwenden und speichern sollten. Öffentliches Vertrauen entsteht dann, wenn Anwender wissen, dass ihre Privatsphäre geschützt wird und ihre persönlichen Daten angemessen verwendet werden.

- Wir unterstützen seit Langem eine geschützte Privatsphäre, indem wir mit geeigneten Maßnahmen Informationen über Kunden verantwortungsvoll und sehr transparent nutzen und dafür verschiedene optionale Einstellungen anbieten. Mehr als 40 Microsoft-Mitarbeiter arbeiten ausschließlich an der Verbesserung der Privatsphäre, und für weltweit mehrere Hundert Mitarbeiter ist dies ein wesentlicher Bestandteil ihres Berufs.

- Wir befürworten jede Gesetzgebung hinsichtlich des Schutzes der Privatsphäre, die den freien Informationsfluss ermöglicht und gleichzeitig Vertrauen schafft sowie Innovationen berücksichtigt. Daten werden immer mehr grenzüberschreitend ausgetauscht. Daher sind wir für eine höhere Standardisierung und eine weltweit bessere, einheitliche Anpassung von Gesetzen, Vorgaben, Richtlinien und Standards zum Schutz der Privatsphäre.

HINTERGRUND

Die digitale Wirtschaft hat die Welt auf grundlegende und erstaunliche Art und Weise verändert. Gleichzeitig sind die öffentlichen Bedenken wegen der Privatsphäre und der Sammlung und Verwendung persönlicher Daten gestiegen. Der Grund dafür sind viele bekannt gewordene Datendiebstähle und Attacken, die das Vertrauen der Anwender in den digitalen Handel und das Internet erschüttert haben.

Anwender erwarten einen hohen Schutz ihrer Privatsphäre, der bereits in Produkte und Dienste integriert ist. Sie haben zudem sehr genaue Vorstellungen darüber, wie Unternehmen ihre Daten sammeln, verwenden und speichern dürfen. Nur wenn Anwender wissen, dass ihre Privatsphäre geschützt wird und ihre persönlichen Daten angemessen verwendet werden, entsteht öffentliches Vertrauen. Mit jeder Firma, die diese Erwartungen nicht erfüllt, sinkt die Bereitschaft der Menschen, Onlinetechnologien einzusetzen. Leidtragende davon sind beide: Unternehmen und Anwender.

DER MICROSOFT-ANSATZ

Wir sehen uns seit Langem in der Pflicht, wenn es um den Schutz der Privatsphäre geht, und verwalten die Informationen unserer Kunden transparent und mit verschiedenen optionalen Sicherheitseinstellungen.

- **Grundlagen der Privatsphäre.** Respekt vor der Privatsphäre ist unserer Meinung nach mit das wichtigste Merkmal einer vertrauenswürdigen Rechnerumgebung. Mehr als 40 Microsoft-Mitarbeiter arbeiten daher ausschließlich an der Verbesserung der Privatsphäre. Sie werden von weltweit mehreren Hundert weiteren Mitarbeitern unterstützt, die dafür sorgen, dass Richtlinien, Prozeduren und Technologien unternehmensweit einheitlich umgesetzt und angewendet werden.

- **Schutz der Anwenderdaten.** Für uns ist klar, dass Anwender jederzeit die Kontrolle über ihre persönlichen Informationen behalten müssen. Unternehmen müssen verantwortlich dafür sein, wie sie diese Daten sammeln, verwenden und schützen. Unsere Prinzipien und Aussagen hinsichtlich des Schutzes der Privatsphäre beschreiben unmissverständlich, welche Informationen wir warum erfassen und wie wir diese verwenden. Zudem helfen wir Anwendern dabei, die uns zur Verfügung gestellten Informationen besser zu verwalten.

- **Richtlinien und Zusammenarbeit**. Wir arbeiten mit Regierungen, Unternehmen und führenden Technologieanbietern zusammen, um einerseits die Entwicklung von Gesetzesvorschlägen zu unterstützen und andererseits dafür zu sorgen, dass Gesetze von Gerichten angemessen angewendet werden. Wir entwickeln zudem Methoden für mehr Verantwortung gegenüber der Privatsphäre und forcieren den Einsatz von selbstregulierenden Mechanismen, die Anwender und deren persönliche Daten besser schützen.

  Wir unterstützen öffentliche Richtlinien, die mit neuen und aktualisierten Regularien mehr Sicherheit in einer offeneren Cloud-Umgebung schaffen, sowie grundlegende bundesweite gesetzliche Vorgaben. Weiterhin arbeiten wir weltweit mit Strafverfolgungsbehörden, Verbraucherschutzverbänden und Anwaltsvereinigungen zusammen, um Betrug, Spam, Spyware und andere Bedrohungen der Privatsphäre zu bekämpfen.

STRATEGISCHE ÜBERLEGUNGEN

- Wir befürworten jede Gesetzgebung hinsichtlich des Schutzes der Privatsphäre, die den freien Informationsfluss ermöglicht und gleichzeitig Vertrauen schafft sowie Innovationen berücksichtigt. Weil der Datenaustausch immer öfter grenzüberschreitend erfolgt, sind wir für eine höhere Standardisierung zum Schutz der Privatsphäre. Mit einer hierfür nötigen, weltweit besseren und einheitlichen Anpassung von Gesetzen, Vorgaben, Richtlinien und Standards.

- Während Regierungen auf Vorfälle mit neuen und weiterentwickelten Technologien und Onlinediensten reagieren, sollten sie jedoch nicht auf Innovationen und die Integration neuer Technologien in die Prozesse verzichten. Durch die Zusammenarbeit von Regierungen und Unternehmen entstehen angemessene und aufeinander abgestimmte Grundsätze, die sich als Standards weltweit einsetzen lassen.

- Wir sind davon überzeugt, dass die Verwendung der Daten und nicht die Art, wie sie gesammelt werden, eine bessere Voraussetzung für einen höheren Datenschutz bietet und so auch die Privatsphäre besser schützt. Wir unterstützen daher ein Modell, das im Gegensatz zu Benachrichtigungen und Zustimmungen die Datenverwendung berücksichtigt.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Die Grundsätze von Microsoft hinsichtlich der Privatsphäre
www.microsoft.com/privacy/principles.aspx

Die Microsoft-Aussagen hinsichtlich der Privatsphäre
aka.ms/privacy-statement

Leitfäden für die Privatsphäre bei der Anwendungs- und Diensteentwicklung
aka.ms/privacy-guidelines

Privatsphäre und Microsoft Cloud Computing
www.microsoft.com/privacy/cloudcomputing.aspx

Privatsphäre und Microsoft-Werbung
choice.microsoft.com

Eine einheitliche Gesetzgebung für den Schutz der Privatsphäre

Die wichtigsten Punkte im Überblick

- In Ländern, in denen noch keine umfassenden Gesetze gelten, sollten Kommunen, Landes- und Bundesregierungen die vielen stetig zunehmenden regionalen und nationalen Gesetze zusammenfassen und durch eine einheitliche, klare und allgemeingültige Gesetzgebung ersetzen.

- Wir fordern seit 2005 in den USA eine umfassende Gesetzgebung hinsichtlich der Privatsphäre. Wir befürworten nationale Gesetze, die Anwendern mehr Rechte geben, wenn es um die Sammlung, Verwendung sowie Veröffentlichung ihrer Informationen und um mehr Schutz für ihre Transaktionen geht.

- Wir glauben, dass eine grundlegende Gesetzgebung über die Privatsphäre die On- und Offlinenutzung umfassen sollte. Zudem muss sie die Anforderungen hinsichtlich der Transparenz, der Kontrolle durch Anwender und der Sicherheit erfüllen. Eine solche Gesetzgebung führt zu mehr Rechtssicherheit, weil sie lokale mit nationaler Gesetzgebung in Einklang bringt. Weiterhin sollte sie sicherstellen, dass Unternehmen kommerziell genutzte Daten verantwortungsvoll verwenden, speichern und verteilen.

- Eine Gesetzgebung löst nicht alle Probleme hinsichtlich der Privatsphäre. Sie schützt Anwender aber besser, indem sie selbstgesteuerte Verhaltensregeln für Unternehmen, bewährte Methoden, technische Lösungen und Anwenderaufklärung kombiniert.

HINTERGRUND

Viele Länder verfügen über Gesetze zum Schutz der Privatsphäre, die das Sammeln und Nutzen sowie die Weitergabe von personenbezogenen Daten regeln. Diese Gesetze werden normalerweise von Datenschutzbehörden initiiert. In einigen Ländern, wie etwa den USA, gibt es keine solche Gesetzgebung. Dort gilt eine Mischung aus regionalen und nationalen Gesetzen, die zudem noch zwischen verschiedenen Branchen unterscheiden. In den USA gibt es sehr viele unterschiedliche Regional- und Bundesgesetze mit einer für Unternehmen sehr geringen Rechtssicherheit.

Eine einheitliche Gesetzgebung für den Schutz der Privatsphäre schafft mehr Rechtssicherheit, weil sie regionale und nationale Gesetze in Einklang mit staatlichen Richtlinien und Vorgaben bringt. Sie fördert und fordert verantwortliches Handeln und Innovationen von Unternehmen bei der Sammlung, Verwendung und Weitergabe von Daten. Gleichzeitig ermutigt sie Firmen, sich mit stabilen und ausgefeilten Methoden für mehr Schutz der Privatsphäre einen zusätzlichen Wettbewerbsvorteil zu verschaffen.

Es ist die gemeinsame Aufgabe von Regierungen und Unternehmen, effiziente und konsistente Rahmenbedingungen zu schaffen, die die stetig wachsenden, komplexen Gesetze zum Schutz von Privatsphäre und Daten zusammenfassen und vereinheitlichen. Denn klare, verbindliche und einheitliche Regeln verbessern nicht nur die Transparenz, Sicherheit und Konsistenz, sondern gestatten Anwendern zudem mehr Kontrolle über ihre persönlichen Informationen.

Wir fordern schon seit Langem die Entwicklung und Umsetzung einer einheitlichen und umfassenden nationalen Gesetzgebung für den Schutz der Privatsphäre. Dafür erarbeiten wir mit verschiedenen regionalen Institutionen, wie etwa der Asia-Pacific Economic Cooperation (APEC), an Rahmenbedingungen. Die bereits vorhandene EU-Direktive zum Schutz von Daten und Privatsphäre enthält viele Vorschläge und Empfehlungen, wie in Europa die Sammlung, Verarbeitung und Sicherheit persönlicher Daten erfolgen sollte.

DER MICROSOFT-ANSATZ

- Wir fordern seit 2005 in den USA eine umfassende Gesetzgebung hinsichtlich der Privatsphäre. Wir befürworten nationale Gesetze, die Anwendern mehr Rechte geben, wenn es um die Sammlung, Verwendung sowie Veröffentlichung ihrer Informationen und um mehr Schutz für ihre Online- und Offlinetransaktionen geht.
- Seit Langem schon sind für uns – zum Schutz der Privatsphäre – Grundsätze, Richtlinien und Prozeduren wichtig, die wir mit unseren Produkten und Diensten berücksichtigen. Das beginnt bei der Entwicklung und geht bis hin zum Einsatz und der Ausführung.
- Wir geben Informationen weiter und teilen Ideen vieler gesetzlicher Vorschläge und Empfehlungen, die weltweit hinsichtlich des Schutzes der Privatsphäre entstehen. So kommentieren und beurteilen wir etwa den internen Vorabbericht der U.S. Federal Trade Commission (FTC) zum Thema Privatsphäre, der auch ergänzende und überarbeitete Vorschläge eines Gesetzes zum Schutz von Kindern online, Children's Online Privacy Protection Act (COPPA), enthält. Zudem gehören wir zu den Unternehmen, die als Berater die EU-Direktive für mehr Datenschutz unterstützen, und wir helfen der Asia-Pacific Economic Cooperation (APEC) bei der Entwicklung von Rahmenbedingungen für mehr Schutz der Privatsphäre.

STRATEGISCHE ÜBERLEGUNGEN

- Wir glauben, dass eine grundlegende Gesetzgebung über die Privatsphäre sowohl die Online- als auch die Offlinenutzung umfassen sollte. Zudem muss sie die Anforderungen hinsichtlich der Transparenz, der Kontrolle durch Anwender und der Sicherheit erfüllen. Eine solche Gesetzgebung führt zu mehr Rechtssicherheit, weil sie lokale Gesetze mit der nationalen Gesetzgebung in Einklang bringt. Zudem bietet sie Unternehmen, die Daten auf verantwortliche Art und Weise verwenden, speichern und verteilen, einen zusätzlichen Wettbewerbsvorteil.
- Gesetze für den Schutz der Privatsphäre sind keine alles umfassende Komplettlösung. Sie schaffen zwar mit Standardvorgaben eine flexible Grundlage, allerdings halten öffentliche Richtlinien und Vorgaben oft nicht mit den weiterentwickelten Technologie- und Geschäftsmodellen Schritt. Einer der erfolgversprechendsten Ansätze für mehr Schutz der Privatsphäre ist es, selbstgesteuerte Verhaltensregeln für Unternehmen mit bewährten Methoden sowie technischen Lösungen und einer verstärkten Anwenderaufklärung zu kombinieren.
- Für Unternehmen, die mit selbstgesteuerten und von lokalen Regierungen geprüften Verhaltensregeln den Schutz der Privatsphäre verbessern, bieten Gesetze bezüglich der Privatsphäre mehr Rechtssicherheit. Ein freiwilliger, in einem offenen Verfahren von mehreren Beteiligten und auf den gesetzlichen Grundlagen entwickelter Verhaltenskodex hilft dabei, neue und weiterentwickelte Technologien und Geschäftsprozesse besser zu berücksichtigen.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Privatsphäre und Microsoft Cloud Computing
www.microsoft.com/privacy/cloudcomputing.aspx

Privacy by Design von Microsoft
www.microsoft.com/privacy/bydesign.aspx

Internationale Standards für den Datenschutz

Die wichtigsten Punkte im Überblick

- Internationale und teilweise widersprüchliche Gesetze und Regelungen für den Datenverkehr über Landesgrenzen hinweg behindern Cloud Computing und Onlinehandel.
- Wir unterstützen die Entwicklung von global gültigen, einheitlichen Rahmenbedingungen für den weltweiten Datenverkehr, die einen höheren Schutz der Privatsphäre ermöglichen. Regierungen müssen dabei mit klaren Gesetzen und Vorgaben helfen, unterschiedliche und sich widersprechende Regelungen zu vereinheitlichen.
- Internationale Standards für die Privatsphäre müssen flexibel und technologieneutral für verschiedene Branchen gelten. Für eine ausgewogene Regelung ist die Zusammenarbeit von Unternehmen, Regierungen und der Öffentlichkeit nötig.

HINTERGRUND

Internet und Cloud Computing erlauben den grenzüberschreitenden, geografisch unbegrenzten Datenverkehr. Im Internet stellen Unternehmen beispielsweise in einem Land ihre Website online, während sie die Daten in einem zweiten Land speichern und weltumspannend Transaktionen mit Kunden durchführen. Von diesem internationalen Informationsfluss profitiert die globale Wirtschaft, weil damit die Produktivität steigt, sich neue Märkte eröffnen und zusätzliche großartige Geschäftschancen entstehen.

Gerade wenn Daten in vielen Ländern genutzt werden, ist es oft nicht klar, welche Gesetze, Regelungen und Schutzvorgaben dabei gelten. Aktuelle Regelungen stammen noch aus den Zeiten vor der digitalen Globalisierung, als Unternehmen ihre Geschäfte anders abwickelten. In der Europäischen Union gibt es die Direktive zum Schutz von Daten und Privatsphäre, die den Austausch und die Verwendung personnenbezogener Daten mit anderen Staaten regelt. In den USA hingegen existieren von Bundesland zu Bundesland und von Branche zu Branche verschiedene Vorgaben und Regeln für den Datenaustausch – wie etwa in den Bereichen Gesundheitswesen und Finanzen. Wenn international tätige Unternehmen diese komplexen Bedingungen erfüllen, steigen ihre Betriebskosten.

Unternehmen und Regierungen sollten gemeinsam einheitliche Rahmenbedingungen schaffen, mit denen sie die Komplexität der vielen internationalen, nationalen und regionalen Gesetze zum Schutz der Privatsphäre und Daten reduzieren. Genau dafür haben die Teilnehmer der 32sten Internationalen Konferenz für Datenschutz und Privatsphäre im Jahr 2010 eine Resolution verabschiedet. Sie fordern damit eine regierungsübergreifende Konferenz für die Entwicklung von verbindlichen und international anzuwendenden Vorgaben hinsichtlich des Schutzes der Privatsphäre und Daten. Zudem entwickelt die International Standards Organization (ISO) einheitliche globale Standards für mehr Datenschutz und Privatsphäre.

DER MICROSOFT-ANSATZ

Seit Langem schon sind für uns – zum Schutz der Privatsphäre – Grundsätze, Richtlinien und Prozeduren wichtig, die wir mit unseren Produkten und Diensten berücksichtigen. Das beginnt bei der Entwicklung und geht bis hin zum Einsatz und der Ausführung.

- Unsere Vorgaben für die Privatsphäre berücksichtigen wir bei der Entwicklung und dem Einsatz unserer Produkte und Dienste. Diese von uns veröffentlichten Standards bieten detaillierte Informationen und Empfehlungen, wie Anwender am besten benachrichtigt werden und bestimmten Prozeduren zustimmen sollen. Ziel ist ein verbesserter Schutz und eine höhere Integrität ihrer Daten sowie eine umfassendere Zugriffskontrolle und -steuerung. Mit unserem Security Development Lifecycle (SDL) verbessern wir die Sicherheit unserer Produkte und erhöhen den Schutz der Anwender. Mit SDL integrieren wir schon während der gesamten Entwicklungsphase Funktionen für mehr Schutz der Privatsphäre in jedes unserer Produkte. Dies gilt auch für unsere Cloud-Dienste, die wir so ebenfalls für einen größtmöglichen Schutz von Daten und Privatsphäre auslegen.
- Wir möchten, dass Mitarbeiter, Lieferanten und Partner sich ihrer Verantwortung bei der Nutzung von personenbezogenen Daten ihrer Kunden bewusst sind. Daher ist jeder unserer Geschäftsbereiche verantwortlich für die Entwicklung von Prozeduren, die den verantwortungsvollen Umgang mit diesen Daten unterstützen. Dafür übernehmen ausgewählte Mitarbeiter die Aufgabe, täglich die Einhaltung der Privatsphäre zu überwachen und zu schützen.
- Wir befolgen und übernehmen internationale Standards für die Privatsphäre und den Datenschutz. Office 365 zum Beispiel ist vollständig kompatibel mit der ISO-Norm 27001.

STRATEGISCHE ÜBERLEGUNGEN

- Wir unterstützen viele derzeitige Aktionen, deren Ziel die einheitliche Anpassung der Gesetze zum Datenschutz ist. Zudem befürworten wir die erweiterte ISO-Norm 27001, die mit ihren Standards für einen besseren Datenschutz die Grundlage für die zuvor erwähnte Gesetzesvereinheitlichung ist. Je häufiger die ISO-Vorgaben übernommen und angewendet werden, umso besser lassen sich in der Cloud genutzte Daten schützen.
- International gültige Standardvorgaben für die Privatsphäre müssen flexibel, technologieneutral und branchenübergreifend einsetzbar sein.
- Für uns verspricht ein verantwortungsorientierter Ansatz am meisten Erfolg für den Schutz der Privatsphäre, bei dem der Datentransfer über Landesgrenzen hinweg erlaubt ist und der Datenexporteur unabhängig von seinem geografischen Standort für den Datenschutz verantwortlich ist. Mit diesem Ansatz bleibt der Datenschutz in der Verantwortung eines Unternehmens, das aber dennoch die Daten flexibel und je nach Bedarf auch an anderen Standorten verwenden kann.
- Viele Cloud-Anbieter müssen ihre Rechenzentren an mehreren, weltweit verteilten Standorten, zwischen denen sie auch die Daten austauschen, betreiben. Damit sie einerseits die Onlinedienste effizient bereitstellen und andererseits die von den Kunden geforderte Leistung und Verfügbarkeit liefern können.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Privatsphäre und Microsoft Cloud Computing
www.microsoft.com/privacy/cloudcomputing.aspx

Privacy by Design von Microsoft
www.microsoft.com/privacy/bydesign.aspx

Februar 2013

Standortbezogene Dienste und die Privatsphäre

Die wichtigsten Punkte im Überblick

- Viele Apps verwenden standortbezogene Dienste wie eine Kartenansicht in Echtzeit oder die Anzeige von Unternehmen in der Nähe des eigenen Standorts. Viele Anwender nutzen diesen Dienst jedoch nur dann, wenn dabei ein angemessener Schutz der Privatsphäre gewährleistet ist.
- Unsere Standardvorgaben zum Schutz der Privatsphäre berücksichtigen wir sowohl während der Entwicklung als auch beim Einsatz von Diensten und Apps, die Standortinformationen nutzen. Dazu gehören Prozeduren, mit denen wir Anwender informieren und deren Zustimmung einholen sowie Daten und die Privatsphäre schützen.
- Wir glauben, dass die Sicherheit personenbezogener Standortangaben nur durch die Zusammenarbeit von IT-Unternehmen, Öffentlichkeit und Regierungen umfassend gewährleistet werden kann.

HINTERGRUND

Durch standortbezogene Dienste erhalten Anwender Informationen abhängig von ihrem aktuellen Aufenthaltsort. So ermöglichen sie in Echtzeit die Navigation, das Einchecken in soziale Netze, die Anzeige von lokalen Wetterdaten und die geografisch aufbereitete Anzeige von Suchergebnissen und stellen viele weitere hilfreiche Funktionen bereit. Die Standortdaten werden auf verschiedene Art und Weise ermittelt. Entweder mit der in vielen mobilen Endgeräten integrierten Global Positioning System (GPS)-Technologie oder mit IP-Adressen oder WiFi-Netz-Kartenzuordnungen.

Eine für uns 2010 in Deutschland, Großbritannien, Japan, Kanada und den USA durchgeführte Umfrage[1] ergab, das 94 Prozent aller Anwender den standortbezogenen Dienst als sehr wertvoll einstuften. Die gleiche Umfrage ergab jedoch auch, dass 52 Prozent der Anwender Bedenken wegen der damit verbundenen Gefahr für ihre Privatsphäre hatten.

Nachfolgend beschreiben wir die häufig genannten Bedenken wegen der standortbezogenen Dienste:

- **Benachrichtigung**. Anwender möchten informiert werden, wenn eine App standortbezogene Daten sammelt und verwendet, und dass dies explizit von ihnen bestätigt werden muss.
- **Kontrolle**. Anwender wünschen Zugriff auf die gesammelten Daten und möchten die Sammlung und Verwendung einschränken können.
- **Aufbewahrung**. Anwender möchten die Richtlinien kennen, die für die Aufbewahrung ihrer Daten gelten.
- **Wiederverwendung**. Anwender möchten über die Verwendung ihrer Daten, auch in Kombination mit weiteren Informationen, selbst bestimmen.
- **Weitergabe an Dritte**. Anwender wünschen mehr Kontrolle bei der Weitergabe ihrer Daten an Apps von Drittanbietern.
- **Gerichtsbeschluss**. Anwender möchten wissen, ob ihre Standortdaten per gerichtlicher Anordnung einsehbar sind.

[1] *Standortbezogene Dienste: Nutzung und Wahrnehmung*
aka.ms/Location-Research

DER MICROSOFT-ANSATZ

Wir sind auf viele Arten an der Bereitstellung von standortbezogenen Daten beteiligt: als App-Anbieter und als Anbieter einer Betriebssystemplattform für Apps von Drittanbietern.

- Unsere Produkte und Dienste, die standortbezogene Daten verwenden, unterliegen einem speziellen Designprozess, der die Privatsphäre besonders berücksichtigt. Damit halten unsere Produktteams die Microsoft-Richtlinien und -Vorgaben für die Privatsphäre exakt ein.
- Windows Phone-Anwendungen, die den Standort erfassen, müssen Anwendern die Möglichkeit bieten, diesen Dienst abzuschalten.
- Anwender können mit den **Standardeinstellungen** oder den **benutzerdefinierten Einstellungen** den Schutz ihrer Privatsphäre feinstufig kontrollieren. Dazu gehört unter anderem auch die Weitergabe der Standortdaten an andere Apps, sodass mit einer einzigen Einstellung der Zugriff auf die Windows Location-Plattform möglich ist.

  Ist diese Plattform aktiviert, wenn ein Anwender eine App aus dem Windows Store zum ersten Mal ausführt, fragt Windows den Anwender, ob die App auf die aktuellen Standortdaten zugreifen darf. Umgekehrt ist es einer App bei nicht aktivierter Windows Location-Plattform unmöglich, auf die Standortdaten zuzugreifen. Jedes Mal, wenn ein Anwender eine App aus dem Windows Store ausführt, kann er die Verwendung der Standortdaten sehr einfach ein- oder ausschalten.

STRATEGISCHE ÜBERLEGUNGEN

- Wir empfehlen und beraten seit langer Zeit Initiativen, die sich für gesetzliche Regelungen der Privatsphäre einsetzen und die so einen ungehinderten Informationsfluss ermöglichen, Vertrauen aufbauen und Innovationen fördern möchten.
- Während Regierungen auf Vorfälle mit neuen und weiterentwickelten Technologien und Onlinediensten reagieren, sollten sie jedoch nicht auf Innovationen und die Integration neuer Technologien in die Prozesse verzichten.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Die Microsoft-Prinzipien bezüglich der Privatsphäre
www.microsoft.com/privacy/principles.aspx

Bing Maps-Fragen und Antworten wegen der Privatsphäre
www.microsoft.com/maps/streetside.aspx

Voraussetzungen für die Windows 8-App-Zertifizierung
aka.ms/app-cert

Windows Phone-Ressourcen wegen der Privatsphäre
aka.ms/WindowsPhone-Privacy

Microsoft und der Schutz der Privatsphäre

Die wichtigsten Punkte im Überblick

- Mit verbesserten Erklärungen und Merkmalen erhöhen wir den Schutz der Privatsphäre. Mit erweiterten Designvorgaben und Funktionen sorgen wir für eine effizientere mehrschichtige Beschreibung wichtiger Informationen, die so einfacher zu ermitteln und zu verwenden sind.

- Die Migration auf das neue Format erfolgt stufenweise und kontinuierlich. Bing und Microsoft.com übernahmen es als Erste, gefolgt von Xbox. Alle anderen Produkte und Dienste folgen nach und nach.

- Wir werden in unseren Bemühungen für besser geschützte Kundendaten nicht nachlassen und unsere Richtlinien und Methoden hinsichtlich der Privatsphäre konsequent umsetzen. Es wird, als Ergebnis des Redesigns, keine negativen Auswirkungen auf die Art und Weise geben, wie wir Daten sammeln und verwenden.

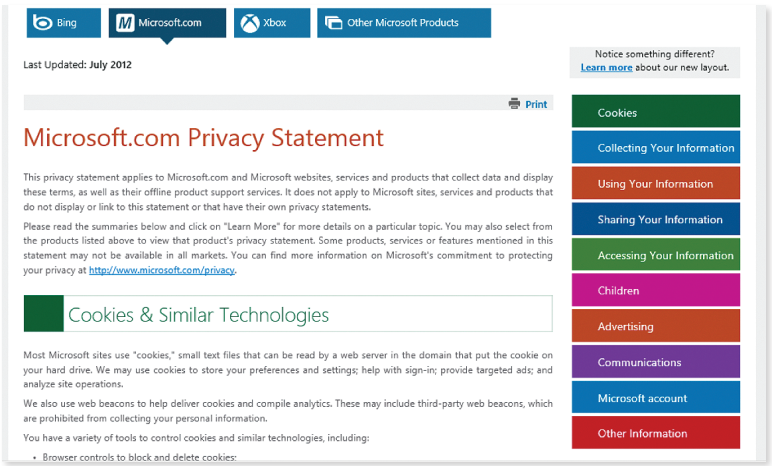
HINTERGRUND

Erklärungen über die Privatsphäre beschreiben die Informationen, die ein Unternehmen erfasst, und wie es sie verwendet und verteilt. Die immer komplexer werdenden globalen Datenübertragungen und neue Regeln haben jedoch dafür gesorgt, dass viele Erklärungen über die Privatsphäre immer mehr und schwer lesbaren Text enthalten. Weil viele Unternehmen zudem Dutzende oder gar Hunderte Onlineressourcen oder -dienste einsetzen, entstehen oft mehrere, sich überschneidende Erklärungen über die Privatsphäre.

Die Herausforderung für Unternehmen besteht darin, klare und verständliche Erklärungen über die Privatsphäre zu verfassen und Anwendern auf Wunsch einen einfachen Zugang zu weiteren, detaillierteren Informationen zu ermöglichen.

Eine Möglichkeit, dies zu erreichen, sind mehrschichtige Hinweise, die Anwender über die wichtigsten Merkmale zum Schutz der Privatsphäre informieren. Dies sind etwa Beschreibungen, welche Informationen ein Unternehmen sammelt und wie es sie verarbeitet. Dabei enthält jede Beschreibung eines Merkmals einen Link, mit dem Anwender weitere detaillierte Informationen aufrufen können. Bereits 2006 haben wir als eines der ersten Unternehmen eine solche mehrschichtige Erklärung über die Privatsphäre eingeführt.

Im Juli 2012 haben wir unsere Erklärung über die Onlineprivatsphäre mit zusätzlichen Funktionen aktualisiert, sodass sie einheitlich für unsere Produkte und Dienste gelten. Die Migration des neue Formats erfolgte zuerst für Bing und Microsoft.com, wie das Bild unten zeigt, und im Oktober 2012 für Xbox.



DER MICROSOFT-ANSATZ

Hier die Beschreibung unserer Erklärung über die Privatsphäre und deren neues Format und Design:

- Erweiterte Funktionen beschreiben wichtige Informationen mit mehreren Schichten besser, mit einer für die meisten unserer Produkte einheitlichen Zugriffsstruktur.
- Anwender erfahren schnell, einfach und direkt mehr über die Privatsphäre, wenn sie ein bestimmtes Produkt oder einen speziellen Dienst verwenden.
- Verständliche, eindeutige Formulierungen beschreiben für exakt definierte Bereiche spezielle Arten der Datensammlung und deren Verwendung. Beispiel hierfür sind Werbemaßnahmen und Cookies. Dazu gehören auch Hinweise darauf, wie und warum die Daten gesammelt, verwendet und verteilt werden, wie Anwender darauf zugreifen und wie die Privatsphäre, insbesondere von minderjährigen Anwendern, geschützt wird.

Wir werden in unseren Bemühungen für besser geschützte Kundendaten nicht nachlassen und unsere Richtlinien und Methoden hinsichtlich der Privatsphäre konsequent umsetzen. Es wird, als Ergebnis des Redesigns, keine negativen Auswirkungen auf die Art und Weise geben, wie wir Daten sammeln und verwenden.

STRATEGISCHE ÜBERLEGUNGEN

- Regierungen und Unternehmen haben ein berechtigtes Interesse daran, Anwender transparent und verständlich über die Privatsphäre zu informieren. Insofern sind wir davon überzeugt, dass flexible gesetzliche Rahmenbedingungen für Anwender einen zuverlässigen Schutz ihrer Privatsphäre ermöglichen und gleichzeitig für Unternehmen die Grundlage schaffen für die Entwicklung und Verwendung innovativer Produkte und Dienste. Wenn eine Gesetzgebung diese Kriterien berücksichtigt, ist sie nicht nur offen für technologische und geschäftliche Veränderungen, sondern schützt Anwenderdaten auch auf Jahre hinaus zuverlässig.
- Regierungen spielen eine wichtige Rolle dabei, Unternehmen zu klaren und verständlichen Erklärungen über die Privatsphäre von Anwendern zu motivieren. Sie müssen lediglich darauf achten, dass dabei Richtlinien nach dem Motto „Eine für alle" entstehen.
- Die Erwartung der Anwender an den Schutz der Privatsphäre hängen von der Art ihrer Beziehung zu einem Unternehmen ab. Jede Gesetzgebung muss es daher Unternehmen erlauben, die eigenen Richtlinien und Methoden einzusetzen, wenn es um die Verwendung und Weiterleitung personenbezogener Daten geht.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Die Microsoft-Prinzipien bezüglich der Privatsphäre
www.microsoft.com/privacystatement

Künftige Modelle für den Schutz der Privatsphäre

Die wichtigsten Punkte im Überblick

- Aktuelle Datenschutzmodelle verwenden Hinweise und Zustimmungen als primäres Kontrollmittel für Anwender. Diese Modelle müssen jedoch kritisch hinterfragt werden, weil die Verwendung der Anwenderdaten immer komplexer und schwerer überschaubar wird.
- Es gilt, andere Modelle zu entwickeln, die eine bessere Kontrolle bieten – wie etwa ein verwendungsorientiertes Modell. Es eignet sich besser für den Schutz der Privatsphäre sowohl für Unternehmen, die Anwenderdaten sammeln, als auch für andere Beteiligte, die diese Informationen ebenfalls nutzen.
- Ein verwendungsorientiertes Modell lässt sich problemlos mit vielen anderen Methoden und gültigen Gesetzen einsetzen. Es untergräbt nicht die Anforderung, dass Informationen fair und gesetzeskonform gesammelt werden.

HINTERGRUND

Im Januar 2002 sendete Bill Gates eine E-Mail an alle Microsoft-Mitarbeiter. Darin kündigte er die Initiative Trustworthy Computing an und erklärte deren drei Grundlagen Sicherheit, Privatsphäre und Zuverlässigkeit. Er erkannte schon damals, wie wichtig der Schutz der Privatsphäre für das Vertrauen der Anwender in IT-Technologien ist. Als Folge davon haben wir sehr viel Aufwand in ein Programm zum Schutz der Privatsphäre gesteckt. Auch heute investieren wir noch in dieses Programm, sodass unsere Mitarbeiter Technologien, Dienste und Merkmale entwickeln können, die den Anforderungen der Anwender entsprechen und ihnen vor Augen führen, wie wichtig der Schutz der Privatsphäre ist.

In vielen Ländern wurde die Vertraulichkeit von Daten bisher entsprechend den in den 1970er Jahren entwickelten, sogenannten Fair Information Practices realisiert. Dazu gehörte unter anderem die Information der Anwender, dass sie der Datennutzung zustimmen müssen. Mit einer Erklärung über die Privatsphäre mussten Unternehmen Anwender darüber informieren, welche Informationen sie sammeln und wie sie diese verwenden. Wobei das Unternehmen versprach, Daten nur so zu verwenden, wie es der Anwender erlaubte. Diese Erlaubnis erfolgte, indem Anwender der Erklärung eines Unternehmens über die Privatsphäre zustimmten. Für die Rechtsprechung spielt diese Zustimmung oft eine große Rolle, wenn es um den Schutz der Privatsphäre geht.

Die moderne digitale Welt verarbeitet enorme Datenmengen (oft auch Big Data genannt) und verursacht durch Cloud Computing sehr unübersichtliche Datenübertragungen. Hierfür eignet sich das Hinweis- und Zustimmungsmodell nur noch bedingt, weil es dabei in den folgenden drei Bereichen an seine Grenzen stößt:

- Die Entscheidungen bezüglich der Sammlung und Verwendung personenbezogener Daten sind sehr komplex und daher für viele Anwender schwer zu verstehen, geschweige denn zu verwalten.
- Das Modell setzt eine interaktive Beziehung zwischen einem Anwender und dem Unternehmen, das seine Daten sammelt und verwendet, voraus. In immer mehr Fällen ist eine solche Beziehung aber nicht mehr vorhanden.
- Der wahre Wert der Daten ist zum Zeitpunkt der Datensammlung möglicherweise nicht ersichtlich. Deren künftige Verwendung mit allen sich daraus ergebenden persönlichen und sozialen Vorteilen könnte mit einem Privatsphärenmodell, das lediglich die Sammlung von Daten berücksichtigt, unmöglich werden.

Es gibt keinen Grund, Anwendern in dieser Umgebung die Verantwortung für die korrekte Verwendung der Daten zu übertragen. Zumal es auch keine ausreichenden Prüfmethoden gibt für eine unangemessene und verantwortungslose Datennutzung. Das Ergebnis ist eine unverhältnismäßig hohe Verantwortung für Anwender.

Stattdessen eignet sich ein Modell, das sich an der Verwendung der Daten orientiert, besser für einen effizienteren Schutz. Dies gilt für das Unternehmen, das die personenbezogenen Daten der Anwender sammelt, genauso wie für andere Beteiligte, die diese Daten verwenden. Voraussetzung für ein verwendungsorientiertes Modell sind eine hohe Transparenz, das Angebot und die Berücksichtigung entsprechender Einstellungen sowie eine ausgefeilte Strategie, um eventuell durch die Datenverwendung entstehende Risiken für die Anwender zu erkennen und zu verwalten. Dieser Ansatz unterstreicht auch die Notwendigkeit, Unternehmen, die personenbezogene Daten verwalten und teilen, stärker in die Verantwortung zu nehmen.

Das Design eines verwendungsorientierten Modells sollte die folgenden fünf Ziele berücksichtigen:

1. Weitgehender Schutz der Privatsphäre.
2. Eine optimierte Datenverwendung mit Vorteilen für Anwender und Gesellschaft.
3. Verantwortlich für die Nutzung ist derjenige, der die Daten verwendet.
4. Eine effizientere Kontrolle und Übersicht durch verschiedene Regler.
5. Eine problemlose Integration in eine moderne, vernetzte Gesellschaft.

In einer datengetriebenen Welt sind für die Erreichung dieser Ziele eine ausgefeilte Anwendersteuerung und eine hohe Transparenz nötig.

DER MICROSOFT-ANSATZ

- Wir sind davon überzeugt, dass die Verwendung, nicht die Sammlung von Daten, die besten Voraussetzungen für einen effizienten Schutz der Daten und der Privatsphäre bietet. Daher unterstützen wir den Einsatz eines verwendungsorientierten Modells anstelle des bisher verwendeten Hinweis- und Zustimmungsmodells.
- Wir wissen, wie wichtig selbstregulierende Prinzipien sind. Sie geben Anwendern mehr Kontrolle über die Verwendung ihrer Daten, und sie sorgen für mehr Transparenz bei der Verwaltung und Verwendung der Daten durch Unternehmen. Unserer Methoden beinhalten die Information der Anwender über die Datennutzung, die sie jederzeit kontrollieren können, sowie einen hohen Datenschutz.
- Unsere Maßnahmen zum Schutz der Privatsphäre sind grundsätzlich immer an die Art der Informationen angepasst, die wir erfassen, und wie wir diese verwenden werden.

STRATEGISCHE ÜBERLEGUNGEN

- Wir unterstützen zum Schutz der Privatsphäre die Übernahme verwendungsorientierter Modelle, die selbstregulierende Prinzipien berücksichtigen. In den USA und Europa ist dies bereits Bestandteil von Gesetzesvorschlägen.
- Ein verwendungsorientiertes Modell lässt sich problemlos mit vielen anderen Methoden einsetzen und berücksichtigt gültige Gesetze. Es untergräbt nicht die Anforderung, dass Informationen fair und gesetzeskonform gesammelt werden.
- Während Regierungen auf Vorfälle mit neuen und weiterentwickelten Technologien und Onlinediensten reagieren, sollten sie jedoch nicht auf Innovationen und die Integration neuer Technologien in die Prozesse verzichten. Regierungen und Unternehmen sollten gemeinsam entsprechende Grundsätze erarbeiten.

Hilfreiche Ressourcen

Microsoft Trustworthy Computing Next
www.microsoft.com/twcnext

Ein Überblick über die Microsoft-Richtlinien und Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Ein Ansatz für mehr Schutz der Privatsphäre: Ein Diskussionsdokument. Das Business Forum for Consumer Privacy, Dezember 2009.
aka.ms/Use-Discussion

Verantwortung für die Privatsphäre

Die wichtigsten Punkte im Überblick

- Unternehmen müssen entsprechend den Grundsätzen handeln, mit denen die Verantwortlichkeit für den Datenschutz festgelegt ist. Dazu gehört, dass sie sich der Risiken bewusst sind, die durch ihre Verwendung der personenbezogenen und vertraulichen Anwenderdaten für die Anwender entstehen. Zu ihrer Verantwortung gehört auch, mit geeigneten Richtlinien, Hilfsmitteln und Prozessen diese Risiken zu minimieren sowie mit internen Kontrollen den Schutz von personenbezogenen Daten und Privatsphäre sicherzustellen.

- Verantwortung für die Privatsphäre zu übernehmen ist eines unserer Grundprinzipien. Wir legen dabei fest, wie wir, unsere Lieferanten und unsere Partner mit personenbezogenen Daten umgehen. Jeder unserer Unternehmensbereiche ist verantwortlich für die Entwicklung von Prozeduren, mit denen personenbezogene Daten entsprechend unseren Vorgaben geschützt werden.

- Mehr Verantwortung ist unser Ansatz für eine öffentliche Richtlinie, die einen länderübergreifenden Datenaustausch ohne Einschränkungen erlaubt, solange der Datenexporteur unabhängig von seinem geografischen Standort für den Datenschutz verantwortlich ist.

HINTERGRUND

Verantwortung zu übernehmen ist ein seit Langem etabliertes Prinzip für den Schutz von Privatsphäre und Daten, das die Organisation für wirtschaftliche Zusammenarbeit (OECD) erstmals Anfang der 1980er Jahre vorstellte. Die dabei verfolgten Ziele sind in EU-Gesetzen und Gesetzen der EU-Staaten festgelegt. Eine genauere Beschreibung enthalten das kanadische Gesetz über die Privatsphäre (PIPEDA) und die APEC-Rahmenbedingungen für die Privatsphäre.

Die Übernahme von Verantwortung lässt sich am besten als ein Ansatz beschreiben, der die Risiken bei der Verarbeitung und Speicherung personenbezogener Daten vermeidet beziehungsweise minimiert. Alle Unternehmen sollen so diese Risiken für die Privatsphäre besser analysieren und erkennen sowie mit geeigneten Maßnahmen schützen. Dafür ist es nötig, die Grundsätze des Datenschutzes mit der eigenen Verantwortung für eine sichere und angemessene Datenverarbeitung und -speicherung, unabhängig vom jeweiligen Standort, in Einklang zu bringen. Zudem sollten Unternehmen diese programmatischen Ansätze, mit denen sie personenbezogene Daten entsprechend den jeweiligen Vorgaben schützen, vorstellen und erklären.

Es war nie zuvor so wichtig wie heute, Verantwortung für den Schutz von Privatsphäre und Daten zu übernehmen. Technische Innovationen erleichtern es, Daten zu sammeln, zu analysieren und zu verarbeiten. Der weltweit zunehmende Datenverkehr, immer mehr Datenzugriffe und leistungsfähigere Analysewerkzeuge führten zu einer Situation, in der so viele Daten und Informationen über Anwender zur Verfügung wie nie zuvor. Für diese neue Welt, die vielfältige Zugriffe auf miteinander verbundene Daten ermöglicht, sind wirkungsvolle Schutzmechanismen für die Privatsphäre erforderlich.

Weltweit kam der Übernahme von Verantwortung für die Privatsphäre in letzter Zeit deutlich mehr Bedeutung zu. Viele Länder schaffen mittlerweile Rahmenbedingungen für den Schutz der Privatsphäre, die genau diese Verantwortung berücksichtigen.

Die dabei häufig übernommenen Grundsätze bieten viele Vorteile. Sie erleichtern den Datenverkehr über Landesgrenzen hinweg und ermöglichen Cloud Computing unabhängig vom Standort der Rechenzentren. Einzige Voraussetzung dafür ist, dass Unternehmen die Verantwortung für die Verwaltung und Verarbeitung der Informationen übernehmen – unabhängig vom Standort, an dem die Daten gespeichert und verwendet werden.

DER MICROSOFT-ANSATZ

- Ein Schlüsselmerkmal unserer Grundsätze für eine geschützte Privatsphäre ist die Übernahme von Verantwortung für personenbezogene Daten. Dies gilt sowohl innerhalb des Unternehmens als auch für unsere Lieferanten und Partner.
- Jeder Microsoft-Geschäftsbereich ist verantwortlich für die Entwicklung von Prozeduren für den Datenschutz. Dabei übernehmen bestimmte Mitarbeiter die Verantwortung für den Schutz der Privatsphäre und überwachen, ob dieser eingehalten wird.
- Wir arbeiten mit gesetzgebenden Behörden und anderen Beteiligten an der praktischen Umsetzung dieses verantwortungsbezogenen Modells. Dabei geht es auch darum, wie Unternehmen mehr Verantwortung übernehmen und welche Rolle Drittanbieter und Validierungsprogramme dabei spielen.

STRATEGISCHE ÜBERLEGUNGEN

- Mehr Verantwortung ist unser Ansatz für eine öffentliche Richtlinie, die einen länderübergreifenden Datenaustausch ohne Einschränkungen erlaubt, solange der Datenexporteur unabhängig von seinem geografischen Standort für den Datenschutz verantwortlich ist. Weil Unternehmen dabei für den Datenschutz verantwortlich sind, können sie Daten flexibel und je nach Bedarf austauschen.
- Gesetzgeber und andere Beteiligte müssen sorgfältig überlegen, wie ein verantwortungsbezogenes Modell am besten in gesetzliche Vorgaben eingebunden werden kann, um Anwender besser zu schützen. Dabei dürfen Unternehmen nicht mit zusätzlichen Auflagen und Aufgaben belastet werden, und es müssen klare Vorteile entstehen für diejenigen Unternehmen, die diese Verantwortung, etwa bei landesgrenzenüberschreitendem Datentransport, übernehmen.
- Gesetzgebende und regulierende Regierungen und Behörden sollten darauf achten, keine zusätzlichen, erschwerenden Prüfmechanismen einzuführen. Ein Beispiel hierfür wären Prüfungen oder Zertifizierungen durch Drittunternehmen, die zusätzliche Kosten verursachen, die Effizienz verringern und den Schutz der Privatsphäre nicht sonderlich erhöhen.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Über die Rolle und den Einfluss von unternehmerischer Verantwortung bei der Verwaltung und dem Schutz von Anwenderdaten
aka.ms/accountability-privacy

Verschiedene Abhandlungen des Information Policy Centre über die Verantwortung für den Datenschutz
aka.ms/accountability-papers

Standardvorgaben für den Schutz der Privatsphäre

Die wichtigsten Punkte im Überblick

- Wir sind überzeugt davon, dass standardisierte Einstellungen sehr wichtig für den Schutz der Privatsphäre sind. Vorgegebene Standardeinstellungen für eine sichere Privatsphäre könnten jedoch auch unvorhersehbare Folgen haben – wie etwa eingeschränkt nutzbare Innovationen und Funktionen und damit frustrierte Anwender.

- Am besten lassen sich standardisierte Voreinstellungen für die Privatsphäre verwenden, wenn sie für Technologien und Dienste maßgeschneidert angepasst werden. Standardisierte Einstellungen sollten fallweise mit einem ganzheitlichen Ansatz für das Design der Privatsphäre bestimmt werden.

- Wir untersuchen unsere Produkte und Dienste regelmäßig hinsichtlich des Schutzes der Privatsphäre. Die Ergebnisse helfen unseren Produktteams, unsere Richtlinien und Standardvorgaben für mehr Schutz der Privatsphäre einzuhalten.

HINTERGRUND

Die Einstellungen für die Privatsphäre sind ein wichtiges Hilfsmittel, mit dem Anwender ihre personenbezogenen Daten und Informationen besser schützen. Sie erwarten dafür von Unternehmen Einstellmöglichkeiten, die ihnen mehr Transparenz und Kontrolle bei der Sammlung, Speicherung und Verwendung ihrer persönlichen Daten einräumen. Unternehmen, die Arbeitsprozesse und Dienste online ausführen, müssen für den Schutz der Privatsphäre Mechanismen entwickeln, die diese Anforderungen erfüllen.

Standardisierte Privatsphäreneinstellungen sind ein konzeptioneller Bestandteil eines Anwendungsdesigns, das von vielen Datenschutzbehörden, darunter die Europäische Kommission, in Betracht gezogen wird. Einfach erklärt verbieten es standardisierte Privatsphäreneinstellungen, ohne explizite Zustimmung eines Anwenders dessen personenbezogene Daten zu sammeln, anzuzeigen oder weiterzugeben. Weitere Details betreffen Vorgaben, mit denen standardmäßig lediglich die eingeschränkte Weitergabe von personenbezogenen Daten möglich ist. Ein soziales Netz etwa könnte dementsprechend keine Informationen eines Mitglieds gegen dessen Willen anderen Netzteilnehmern anzeigen. Oder anders gesagt, wäre hierfür die ausdrückliche Genehmigung des Mitglieds zwingend notwendig.

Befürworter von standardisierten Privatsphäreneinstellungen führen oft an, dass viele Anwender nicht wissen, wie sie die Einstellungen ihrer Privatsphäre vornehmen, und dass die Konfiguration zu schwierig oder unverständlich sei. Zudem entstehe durch fehlende Konfigurationsmöglichkeiten häufig ein erhöhtes Risiko für den Schutz der Privatsphäre, was insbesondere die Daten von Kindern, die sehr oft soziale Netze nutzen, betreffe.

Es gilt also, viele Herausforderungen bei der Einführung standardisierter Privatsphäreneinstellungen zu beachten. So gibt es keine universellen Einstellungen, die gleichermaßen für alle Anwendungen und Onlineressourcen gelten. Genauso schwierig ist es, Einstellungen zu ermöglichen, die den Anforderungen aller Anwender entsprechen. Selbst das Anwendungsdesign wird von standardisierten Privatsphäreneinstellungen beeinflusst, wenn nämlich Anwender von wiederholten Hinweisen und Warnungen verwirrt und frustriert werden.

DER MICROSOFT-ANSATZ

- **Privatsphäre by Design**. Dieser Begriff bezeichnet nicht nur die Art und Weise, wie wir Produkte entwickeln, sondern auch, wie wir Dienste anbieten und dass wir uns als ein verantwortungsbewusstes, führendes Technologieunternehmen verstehen. Dies gilt für alle unsere Mitarbeiter, Prozesse und Technologien, die für mehr Schutz und die Verbesserung der Privatsphäre sorgen. Wir möchten mit dieser Vorgehensweise das Vertrauen der Anwender und Partner gewinnen, indem wir tagtäglich unsere Richtlinien und Prozeduren so transparent wie möglich darstellen.

- **Verantwortung**. Es ist einer unserer Grundsätze, Verantwortung für die Vertraulichkeit personenbezogener Daten zu übernehmen. Wir legen damit fest, wie unsere Mitarbeiter, Lieferanten und Partner die Informationen unserer Kunden verwalten. Jeder unserer Geschäftsbereiche ist verantwortlich für die Entwicklung von Prozeduren, mit denen wir unserer Verantwortung hinsichtlich der Privatsphäre jederzeit gerecht werden.

- **Fallweiser Ansatz**. Standardisierte Einstellungen für die Privatsphäre sollten auf Technologien oder Dienste abgestimmt und von Fall zu Fall ermittelt werden.

- **Aufklärung**. Wir wissen, dass Anwender einen hohen Schutz ihrer Privatsphäre durch unsere Produkte und Dienste erwarten. Wir stellen daher Hilfsmittel zur Verfügung, die sie bei der Konfiguration der Privatsphäreneinstellungen unterstützen. Die Verwaltung personenbezogener Daten online erleichtert unsere Webseite Privacy in Action, auf der wir die Einstellungen der Privatsphäre erklären. Dort stellen wir Videos bereit, die zeigen, wie Anwender ihre Onlineprivatsphäre schützen können, und veröffentlichen einen Bericht über unsere Forschungen zur Verbesserung der Privatsphäre.

STRATEGISCHE ÜBERLEGUNGEN

Regularien für einen besseren Schutz der Privatsphäre sollten unserer Meinung nach bestimmte Grundlagen erfüllen:

- **Technologieneutralität**. Technologien werden sich ständig und schnell weiterentwickeln. Daher sollten alle Rahmenbedingungen, die den Schutz der Privatsphäre regeln, konsequent auf eine Bevorzugung bestimmter Dienste, Lösungen oder Mechanismen verzichten, die Anwender informieren, ihnen Auswahlmöglichkeiten vorschlagen oder ihre Daten schützen. Der Vorzug einer bestimmten Privatsphäreneinstellung vor einer anderen könnte beispielsweise dazu führen, dass Innovationen verhindert werden, weil Anbieter verbesserte Alternativlösungen zum Schutz personenbezogener Daten dann gar nicht erst entwickeln.

- **Flexibilität**. Flexible Rahmenbedingungen für den Schutz der Privatsphäre sollten es Unternehmen erlauben, innovative Schutztechnologien und -werkzeuge zu entwickeln. Flexibel bedeutet, dass sie auch eigene Richtlinien und Methoden übernehmen können, die für die Verarbeitung und Veröffentlichung personenbezogener Daten gelten. Dies verbessert zudem fast immer das Verhältnis zwischen Unternehmen und Kunden.

- **Rechtssicherheit**. Ergänzend zu flexiblen Rahmenbedingungen für den Schutz der Privatsphäre müssen Unternehmen darauf achten, dass ihre Privatsphäreneinstellungen international gültige Standards erfüllen. Widersprüchliche oder international nicht einheitlich umgesetzte Standardvorgaben verzögern die Entwicklung neuer Produkte und Dienste aufgrund der fehlenden Rechtssicherheit. Daher sollten Gesetzgeber Unternehmen ermutigen, alle potenziellen Gefahren für die Privatsphäre abzuschätzen und mit innovativen Entscheidungen das Design der Privatsphäre und die Einstellmöglichkeiten der Anwender zu verbessern.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Standardvorgaben für die Privatsphäre: Microsoft-Sichtweise und -Ansatz
aka.ms/PrivacyDefault

Privacy by Design von Microsoft
www.microsoft.com/privacy/bydesign.aspx

DIe Privatsphäre in der Praxis
www.microsoft.com/yourprivacy

Privacy Impact Assessment (PIA)

Die wichtigsten Punkte im Überblick

- Die Gruppe Europäischer Regulierungsstellen für elektronische Kommunikationsnetze und -dienste definierte den Privacy Impact Assessment (PIA)-Standard als einen „systematischen Prozess, mit dem sich negative Einflüsse auf die Privatsphäre eines Projekts, einer Initiative oder eines Systems oder Schemas herausfinden lassen, und der Wege zeigt, um diese Einflüsse zu verringern oder ganz zu vermeiden".

- Wir nutzen einen Prozess, mit dem wir die Auswirkungen neuer Dienste und Produkte auf die Privatsphäre bewerten. Dieser Prozess entspricht im Allgemeinen dem, was viele Unternehmen und Organisationen als PIA kennen.

- PIA-Rahmenbedingungen sollten nur angewendet werden, wenn sie sich für den jeweiligen Zweck eignen. Sie sollten zudem so flexibel sein, dass Unternehmen eigene innovative Technologien und Werkzeuge entwickeln können.

HINTERGRUND

Privacy Impact Assessments (PIAs) sind in den vergangenen Jahren wichtige Mechanismen geworden, mit denen sich die Risiken beim Schutz der Privatsphäre zuverlässig einschätzen und minimieren lassen. Das EU-PIA-Projekt definiert PIA als einen „systematischen Prozess, mit dem sich negative Einflüsse auf die Privatsphäre eines Projekts, einer Initiative oder eines Systems oder Schemas herausfinden lassen, und der Wege zeigt, um diese Einflüsse zu verringern oder ganz zu vermeiden".

Viele Regierungsbehörden entwickelten PIAs Anfang der 1980er Jahre in Ländern wie den USA, Australien und Kanada. Seit einigen Jahren setzen immer mehr Länder in Europa und Asien sowie Unternehmen PIAs ein.

Es gibt viele Gründe für die PIA-Verwendung. Einige nennt das britische Information Commissioner's Office: Risiken für die Privatsphäre von Anwendern zu identifizieren, die Übereinstimmung von Privatsphäreneinstellungen und gesetzlichen Vorgaben zu erkennen, Unternehmen vor Imageverlusten zu schützen, das öffentliche Vertrauen in Produkte oder Dienste zu erhöhen und kostspielige Beschlüsse wegen zu spät entdeckter Probleme mit der Privatsphäre zu vermeiden.

Obwohl PIAs sich oft unterscheiden, identifizierte eine im Jahr 2007 von der britischen Loughborough University durchgeführte Studie vier Elemente, die für jedes PIA gleich waren. Jede PIA-Ausführung ergab immer eine vorausschauende Identifikation von Risiken für den Schutz der Privatsphären, noch bevor Systeme oder Anwendungen eingesetzt oder modifiziert wurden. Sie ermöglichte eine genauere Einschätzung der Wirkung auch im Hinblick auf die Gesetzeskonformität. Zudem ist eine PIA eher prozess- als ergebnisorientiert und verläuft systematisch.

DER MICROSOFT-ANSATZ

Wir bewerten mit einem Prozess die Auswirkungen neuer Dienste und Produkte auf die Privatsphäre. Dieser Prozess entspricht im Allgemeinen dem, was viele Unternehmen und Organisationen als PIA kennen. Mit diesem Prozess analysieren und bestimmen wir bereits in einem sehr frühen Stadium die Anforderungen und die Risiken unserer Produkte und Dienste hinsichtlich der Privatsphäre. Dazu gehören auch regelmäßige Ergebniskontrollen, mit denen wir sicherstellen, dass das endgültige Produkt unseren Richtlinien und Vorgaben entspricht.

Diesen Prüfprozess führen wir in fünf Phasen, wie auch in der Grafik auf der rechten Seite zu sehen ist, durch:

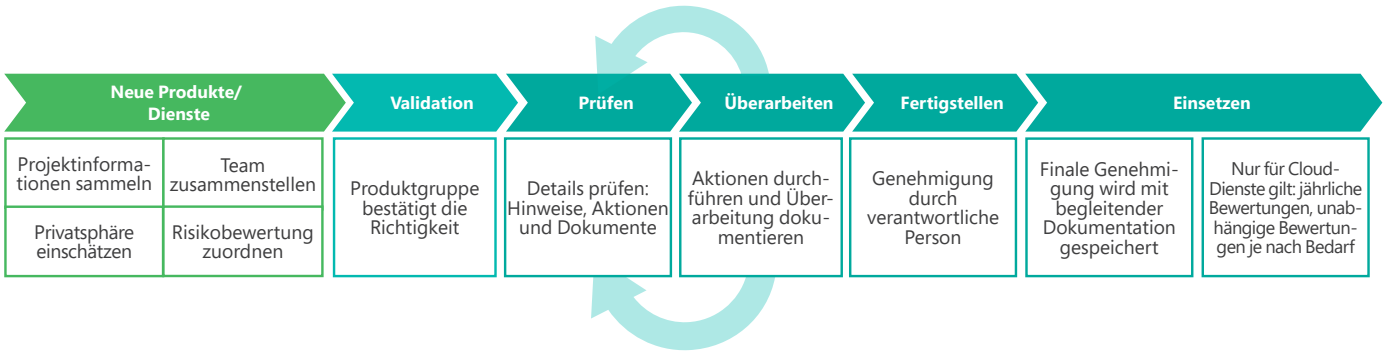
- **Risikobewertung**. Mit diesem ersten Schritt schätzen wir, wie hoch das Risiko für die Privatsphäre beim Einsatz unseres Produkts oder Diensts ist.

- **Bestätigung**. Unsere Teams, die für die Privatsphäre und die Produktentwicklung zuständig sind, bestätigen gemeinsam die Risikobewertung. Dabei werden schon während des Designs und der Entwicklung eines Produkts weitere Einschätzungen zum Schutz der Privatsphäre durchgeführt.
- **Nachprüfung und Korrektur**. Während dieser Phase identifiziert und implementiert das Entwicklungsteam weitere notwendige Schritte, um die Risiken für die Privatsphäre zu reduzieren. Dies erfolgt während der Produktentwicklung wiederholt und so lange, bis alle erkannten Risiken behoben sind.
- **Fertigstellung und Auslieferung**. Ist ein Produkt oder Dienst fertiggestellt, prüfen wir abschließend, ob alle Anforderungen hinsichtlich des Schutzes der Privatsphäre erfüllt werden. Wenn dem so ist, geben wir das Produkt oder den Dienst frei. Zusätzliche, unabhängige Prüfungen und Bestätigungen werden abhängig vom jeweiligen Dienst durchgeführt.

Die Prüfungen, die wir während der Entwicklung hinsichtlich des Schutzes der Privatsphäre durchführen, unterstützen wir mit selbst entwickelten Werkzeugen, die alle für den Abschluss des Prozesses erforderlichen Informationen ermitteln. Mit diesen intern eingesetzten Werkzeugen verfolgen wir auch die Fortschritte, die wir vom Konzept bis zur Fertigstellung des Produkts beim Schutz der Privatsphäre erreichen. Mit ihnen verwalten wir zudem die Bewertungen der vielen eigenen Produkte, inklusive Vollprodukten, Internetdiensten und webbasierten Marketingkampagnen, besser.

STRATEGISCHE ÜBERLEGUNGEN

- **Gezielte Verwendung**. Es gibt Fälle, in denen die Verwendung von PIAs durch gesetzgebende Regierungsbehörden nötig ist. Allerdings verursacht der freiwillige PIA-Einsatz in anderen Fällen oft einen Mehraufwand, der sich in der Produktentwicklung durch zusätzliche Kosten und eine höhere Komplexität niederschlägt.
- **Flexibilität**. PIA-Rahmenbedingungen müssen flexibel handhabbar sein und zu viele Vorschriften vermeiden. Schließlich sollen Unternehmen innovative Technologien und Werkzeuge ohne unnötige Zwänge entwickeln. Flexibilität bedeutet, dass Unternehmen ihre eigenen Richtlinien und Methoden, mit denen sie personenbezogene Daten speichern und weitergeben, und die Art und Weise ihrer Kundenbeziehung integrieren können. PIA-Rahmenbedingungen sollten zudem auf die Unterstützung Dritter verzichten, wenn es um die Ausführung eines PIA geht. Der Grund dafür ist einfach: Die Einbeziehung Dritter sorgt für eine geringere Transparenz und Offenheit zwischen gesetzgebenden Behörden und Unternehmen.
- **Anreize**. Im Gegensatz zu strengen Regeln und Vorschriften motivieren klar definierte Anreize Unternehmen eher, mit einer hohen Eigenverantwortung PIAs einzusetzen und einen zuverlässigen Schutz der Privatsphäre zu erreichen. Verantwortliche Kontrolleure könnten etwa von einer geringeren Zahl an vorgeschriebenen Anforderungen oder von einfacheren Mechanismen für die Datenübertragung profitieren.
- **Bewährte Methoden gemeinsam nutzen**. Unternehmen und Regierungen sollten bewährte Methoden bei PIAs und allen anderen Prozessen, mit denen sie den Schutz der Privatsphäre bewerten, austauschen und gemeinsam nutzen. Wir stellen dafür einen Leitfaden für den Schutz der Privatsphäre bei der Produkt- und Dienstentwicklung öffentlich zur Verfügung. Mit dem veröffentlichten Whitepaper Privatsphäre im Detail erklären wir, wie wir unsere vielfältigen Maßnahmen zum Schutz der Privatsphäre einmal pro Jahr untersuchen und bewerten.



Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Die Microsoft-Prinzipien bezüglich der Privatsphäre
www.microsoft.com/privacy/principles.aspx

Das EU-Projekt Rahmenbedingungen für Privacy Impact Assessment
www.piafproject.eu

Februar 2013

Privatsphäre in der Cloud: Office 365

Die wichtigsten Punkte im Überblick

- Cloud Computing bietet viele Vorteile und wird daher immer öfter genutzt. Dadurch erhöhen sich aber auch die Bedenken wegen der verteilten Datenspeicherung an geografisch verschiedenen Standorten, wegen der niedrigeren Transparenz sowie wegen des Datenzugriffs und der Sicherheit.

- Ein wirkungsvoller Schutz der Privatsphäre ist nötig, um Vertrauen in die Cloud aufzubauen und das volle Potenzial von Cloud Computing zu erschließen. Wir haben daher Office 365 als Onlinedienst für die Zusammenarbeit von Anfang an mit sehr wirkungsvollen Datenschutzfunktionen ausgestattet. Dafür haben wir sogar ein Team aus Sicherheitsexperten zusammengestellt, das sich ausschließlich um den Office 365-Datenschutz kümmert.

- Konflikte zwischen unterschiedlichen gesetzlichen Vorgaben und widersprüchliche Gesetze bezüglich der Datennutzung beeinträchtigen Cloud-Computing-Dienste nach wie vor sehr stark. Unterschiedliche Gesetze hinsichtlich der Privatsphäre, der Datenaufbewahrung und anderer Funktionen verwirren Anwender und Anbieter und erhöhen die Herausforderung an die Gesetzgeber.

HINTERGRUND

Cloud Computing basiert auf dem Internet, um Daten zu speichern und zu verarbeiten sowie Dienste auszuführen. Es handelt sich gleichermaßen um eine ernst zu nehmende Alternative und um eine ergänzende Methode für das traditionelle Modell der Datenverarbeitung, bei dem Anwendungen und Daten vor Ort oder auf persönlich genutzten Endgeräten der Anwender ausgeführt und gespeichert werden. Obwohl Cloud Computing einen bequemen und gemeinsamen Zugriff auf Apps und Onlinedienste, Server, Netze und Speicher erlaubt, entstehen durch dieses Datenmodell enorme Bedenken hinsichtlich des Schutzes der Privatsphäre und der Sicherheitsrichtlinien:

- **Gemeinsame Datenspeicherung**. Wenn die Daten vieler Kunden in einer physikalisch identischen Umgebung gespeichert werden, müssen Cloud-Anbieter mit geeigneten Maßnahmen die Daten so voneinander trennen, dass keine missbräuchliche Verwendung möglich ist oder Daten verloren gehen. Zusätzliche Schutzfunktionen wie eine sichere Verschlüsselung und ausgefeilte Kontrollen für Administratorzugriffe müssen die Sicherheit weiter erhöhen.

- **Transparente Zugriffe**. Kunden wollen wissen, wo ihre Daten gespeichert sind, wer darauf zugreift, wie sie verwendet und weitergegeben werden und welche Funktionen sie schützen. Wenn Cloud-Anbieter transparente Richtlinien verwenden und diese an Kunden und Regierungen kommunizieren, erfüllen sie die Anforderungen der Kunden und erhöhen das Vertrauen in ihr Angebot.

- **Der geografische Speicherort**. Die Weiterentwicklung von Cloud Computing lässt die geografischen Grenzen der Datenspeicherung und des Datentransports immer mehr verschwinden. So werden beispielsweise Daten mit einer Anwendung, die in Irland bereitgestellt wird, in Frankreich erfasst, in den Niederlanden gespeichert und in den USA verwendet. Als Konsequenz daraus wollen gesetzgebende Behörden und Cloud-Computing-Anwender mit klar definierten Richtlinien und Veröffentlichungen wissen, wo sich der physikalische Speicherort der Daten befindet.

- **Sicherheit**. Kunden vertrauen ihrem Cloud-Dienstanbieter nicht nur, was die sichere Datenspeicherung betrifft, sondern auch beim Schutz ihrer Daten vor Verlust, Diebstahl oder Missbrauch.

DER MICROSOFT-ANSATZ

Wir bieten viele Cloud-basierte Produkte wie Office 365 an. Mit diesem Dienst ist der Zugriff auf E-Mail, Webkonferenzen, Dateien und Office Web Apps möglich.

Wir wissen, dass der umfassende Schutz der Privatsphäre sehr wichtig für das Vertrauen in Cloud Computing ist. Daher haben wir in Office 365 folgende Schutzmaßnahmen integriert:

Datennutzung. Wir erklären klar, deutlich und explizit, wie wir Kundendaten verwenden – nämlich ausschließlich für die Verwaltung und Bereitstellung der Office 365-Dienste. Office 365 verwendet Kundendaten nicht, um etwa mit Inhalten von in der Cloud gespeicherten E-Mails oder Dokumenten gezielte Werbemaßnahmen durchzuführen.

Gemeinsame Datenspeicherung. Um Kosten zu senken und Synergien zu nutzen, speichern wir die Daten mehrerer Kunden in der gleichen physikalischen Umgebung, was oft auch als Multi-Tenant-Format bezeichnet wird. Allerdings unternehmen wir große Anstrengungen, um bei dem Multi-Tenant-Betrieb von Office 365 entsprechend den Kundenkonten eine logisch getrennte Speicherung und Verarbeitung der Daten zu erreichen. Dies betrifft natürlich auch den Schutz der Privatsphäre und die Datensicherheit.

Datenübertragung. Office 365-Kunden können ihre Daten jederzeit und ohne unsere Unterstützung komplett oder teilweise exportieren. Selbst wenn ein Office 365-Konto nicht mehr aktuell ist oder geschlossen wurde, haben Kunden noch bis zu 90 Tage danach die Möglichkeit, ihre Daten zu exportieren.

Transparenz. Das Office 365-Vertrauenscenter erklärt die Richtlinien und Methoden, mit denen der Office 365-Dienst die Daten der Kunden schützt.

Sicherheit. Wir schützen Office 365 mit vielfältigen Sicherheitsmaßnahmen, die eine tägliche Überwachung einschließen.

Zugriff. Wir kennen jedes Subunternehmen, das auf Kundendaten zugreifen kann und wissen, unter welchen Umständen dies möglich ist. Zudem erfassen und protokollieren wir jeden Zugriff auf kritische Daten. Weiterhin führen wir und externe Prüfunternehmen regelmäßig Stichproben durch, mit denen wir sicherstellen, dass Kundendaten auch wirklich nur für den entsprechenden Zweck eingesetzt werden.

Der geografische Speicherort. Für Kunden, die wissen möchten, wo ihre Daten gespeichert sind, haben wir die Standorte unserer Hauptrechenzentren veröffentlicht und erklären, wie wir den Speicherort von Daten bestimmen. Wir weisen dabei übrigens auch auf einen möglichen privaten Speicherplatz hin. Office 365-Administratoren informieren wir zudem auf Wunsch, wenn es am Standort eines Rechenzentrums zu Veränderungen kommt.

STRATEGISCHE ÜBERLEGUNGEN

- Konflikte zwischen verschiedenen gesetzlichen Vorgaben und widersprüchliche Gesetze bezüglich der Datennutzung beeinträchtigen Cloud-Computing-Dienste nach wie vor sehr stark. Unterschiedliche Gesetze hinsichtlich der Privatsphäre, der Datenaufbewahrung und anderer Funktionen verwirren Anwender und Anbieter und erhöhen die Herausforderung an die Gesetzgeber.
- Wir unterstützen eine Gesetzgebung zum Schutz der Privatsphäre, die den uneingeschränkten Datentransfer ermöglicht, Vertrauen aufbaut und Innovationen fördert. Aufgrund der globalen Datenübertragungen setzen wir uns für eine weltweit einheitliche Anpassung der Gesetze, Richtlinien, Vorgaben und Standards für den Schutz der Privatsphäre ein.
- Obwohl Regierungen für neuartige Technologien wie Cloud Computing Richtlinien für den Schutz der Privatsphäre und für mehr Datensicherheit schaffen, sollten sie auch künftige technologische Innovationen unterstützen. Gemeinsam können Regierungen und Unternehmen mit geeigneten Maßnahmen für mehr Schutz der Privatsphäre sorgen und Cloud-Daten besser schützen.

Hilfreiche Ressourcen

Ein Überblick über die Microsoft-Richtlinien und -Initiativen hinsichtlich der Privatsphäre
www.microsoft.com/privacy

Microsoft Office 365
office365.microsoft.com

Privatsphäre und Microsoft Cloud Computing
www.microsoft.com/privacy/cloudcomputing.aspx

Das Office 365-Vertrauenscenter
www.trust.office365.com

Onlinesicherheit

Die wichtigsten Punkte im Überblick

- Das Internet bereichert unser Leben auf vielerlei Art. Es erhöht aber auch das Risiko für die Privatsphäre, die Sicherheit, das private und unternehmerische Image und den Handel. Denn im Internet tummeln sich auch viele Cyber-Kriminelle, Onlinefallen und bösartige Anwendungen.

- Wir erhöhen die Onlinesicherheit mit technologischen Werkzeugen sowie Aufklärungsmaßnahmen und Führungsarbeit. Zudem gehen wir Partnerschaften ein mit Regierungen, Unternehmen, Strafverfolgungsbehörden und weiteren Entscheidern, die maßgeblich am Aufbau sicherer und vertrauenswürdiger Rechnerumgebungen beteiligt sind.

- Onlinesicherheit liegt in unserer aller Verantwortung. Regierungen und Unternehmen müssen gemeinsam dafür arbeiten. Technologieanbieter, Regierungen, Unternehmen und Anwender sollten partnerschaftlich und gemeinsam innovative und effiziente Lösungen dafür entwickeln und einsetzen.

HINTERGRUND

Das Internet hat vieles verändert: wie wir zusammenarbeiten, lernen, kommunizieren und spielen. Dabei entstanden aber auch neue Risiken und potenzielle Gefahren. Dazu gehört die Infektion durch bösartige Anwendungen wie Computerviren, Würmer und Spyware. Auch Onlinebetrüger verkaufen Anwendern oft gefälschte Waren, Raubkopien oder bieten ihnen in betrügerischer Absicht vielversprechende finanzielle Investitionen an. Dabei wird oftmals die Privatsphäre der Anwender verletzt, und es entsteht in vielen Fällen ein gestörtes Vertrauensverhältnis, wenn Kriminelle Identitäten übernehmen oder Anwender unerwünschte Spam-E-Mails und andere Nachrichten mit bösartigen Absichten empfangen.

Anwender sorgen sich immer mehr über diese Risiken und versuchen, sich besser davor zu schützen. Eine unserer Untersuchungen[1] aus dem Jahr 2011 ergab, dass 90 Prozent aller Anwender aus den USA und vier europäischen Ländern ihre Onlineprofile mit verschiedenen Maßnahmen schützen. Aber nur 44 Prozent der Befragten gaben an, sich schon mal Gedanken über die langfristigen Konsequenzen ihrer Onlineaktivitäten, und was diese für ihre Identität bedeuten könnten, gemacht zu haben.

Obwohl sich Anwender aktiv schützen, sind ihre Erwartungen an Unternehmen und Regierungen sehr hoch, wenn es um eine sichere Ausgestaltung der Onlinewelt geht. Wenn Unternehmen diese Erwartungen nicht erfüllen, sind Anwender weniger gewillt, Onlinetechnologien einzusetzen, was zu einem gegenseitigen Vertrauensverlust führt.

Die einzigartigen Herausforderungen, die durch die Schaffung der notwendigen Onlinesicherheit entstehen, erfordern ein koordiniertes Vorgehen. Technologieanbieter, Regierungen, Unternehmen und Anwender müssen gemeinsam innovative und effiziente Lösungen entwickeln und einsetzen. Technologieanbieter müssen sich verpflichten, für mehr Sicherheit und Vertrauen im Internet zu sorgen. Vertrauliche Daten und personenbezogene Informationen müssen geschützt werden, und Unternehmen sollten dafür mit technisch orientierten Methoden Vertrauen schaffen. Diese aktuellen und künftigen Herausforderungen können wir nur gemeinsam stemmen – Technologieanbieter, Regierungen, Anwender und Unternehmen.

[1] *Teen Online Reputation: 13-17 Jahre*
www.microsoft.com/security/resources/research.aspx#teen

DER MICROSOFT-ANSATZ

Wir helfen mit einem dreistufigen Ansatz, die Sicherheit und das Vertrauen in die Rechnerumgebung zu erhöhen.

- **Technologische Werkzeuge**. Wir bieten Anwendern viele Werkzeuge für mehr Onlinesicherheit an. Dazu gehört Microsoft Security Essentials, eine kostenloses Anti-Malware-Anwendung. Zudem ermöglichen wir allen Anwendern mit einem Microsoft-Benutzerkonto eine genaue Auswahl, wer ihr Profil anschauen und Kontakt mit ihnen aufnehmen darf oder wer ihnen Nachrichten senden und von ihnen veröffentlichte Inhalte ansehen darf. Mit Microsoft Family Safety überwachen und schützen Eltern ihre Kinder besser, wenn diese online sind. Auch die Xbox 360 ist standardmäßig mit entsprechenden Konsolen-Sicherheitseinstellungen ausgerüstet.

- **Aufklärung und Führung**. Unser Safety and Security Center unterstützt Anwender, die mehr Sicherheit im Internet wünschen. Es gibt ihnen Hinweise und Tipps, wie sie ihre Rechner und ihre Onlineidentitäten besser schützen, Onlinebetrügern aus dem Weg gehen, den Schutz ihrer mobilen Endgeräte erhöhen und unangemessene Verhaltensweisen vermeiden, erkennen und berichten.

- **Partnerschaften**. Eine sichere und vertrauenswürdige Rechnerumgebung entsteht nur mit einem ganzheitlichen Ansatz. Anwender, Regierungen, Technologieanbieter und Nichtregierungsorganisationen spielen dabei gleichermaßen eine wesentliche Rolle. Ein zentraler Bestandteil unserer Zusammenarbeit mit Regierungen und Nichtregierungsorganisationen wie der National Cyber Security Alliance ist dabei die einheitliche Umsetzung allgemeingültiger Richtlinien.

STRATEGISCHE ÜBERLEGUNGEN

- **Die Unterstützung öffentlich-privater Partnerschaften**. Öffentlich-private Partnerschaften sind wichtige Bausteine im Kampf gegen die immer komplexer werdende Cyber-Kriminalität. Wir arbeiten eng mit gesetzgebenden Behörden zusammen, für die wir technische Trainings durchführen und technologische Werkzeuge zur Abwehr von Cyber-Verbrechen entwickeln. Anwender unterstützen wir mit Gerichtsverfahren und anderen Aktionen gegen Cyber-Verbrecher, indem wir unter anderem bei der Vernichtung von Botnetzen helfen und Lieferanten von gefälschten Sicherheitsanwendungen anzeigen. Auch die Entwicklung und Bereitstellung von PhotoDNA gehört zu diesen Maßnahmen. Diese Technologie hilft Unternehmen und Behörden, im Internet Bilder mit kinderpornografischen Inhalten aufzuspüren und zu löschen.

- **Die Unterstützung selbstregulierender Maßnahmen und gesetzlicher Rahmenbedingungen**. Auch wenn Regierungen die Risiken durch weiterentwickelte Technologien und Onlinedienste berücksichtigen, ist es wichtig, dass sie eine Umgebung schaffen, die technologische Innovationen in den Prozess für mehr Onlinesicherheit einbindet. Regierungen und Unternehmen können gemeinsam Sicherheitsgrundsätze aufstellen und Service-Providern helfen, diese umzusetzen. Beispiele hierfür sind die Safer Social Networking Principles für die Europäische Union und der ISP Code of Practice in Australien.

- **Die Durchführung von Studien und die Finanzierung von Forschungsarbeiten**. Die Forschung trägt wesentlich dazu bei, Verursacher von Onlinerisiken zu entdecken. Sie widerlegt zudem Mythen, die ungeeignete Maßnahmen für mehr Internetsicherheit nach sich ziehen. Die finanzielle Unterstützung durch Regierungen ist essenziell für akademische und industrielle Forschungsprojekte zum Thema mehr Sicherheit im Internet.

- **Aufklärung in Schulen**. Unserer Meinung nach sollte Onlinesicherheit ein integraler Bestandteil eines jeden Lehrplans sein, damit es Schulen gelingt, ihre Schüler mit technischem Wissen für dieses Thema zu sensibilisieren. Einzelne Module sollten dabei besonders auf Onlinesicherheit, Onlineschutz und Onlineverhalten eingehen.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center hilft Ihnen mit Informationen über Sicherheitsthemen
www.microsoft.com/security

Onlinebetrug: Entdecken, schützen und Vertrauen zurückgewinnen
aka.ms/OnlineFraudBooklet

Sicherheitstipps und Hinweise der National Cyber Security Alliance
www.staysafeonline.org

Februar 2013

Onlinesicherheit für Kinder

Die wichtigsten Punkte im Überblick

- Obwohl das Internet für Kinder ein interessantes und bereicherndes Umfeld ist, birgt es einige Risiken für sie. Dazu gehören nicht kindgerechte Inhalte, Kontakte mit Kriminellen und Fremden und der Verlust der Privatsphäre.
- Mit technologischen Hilfsmitteln, Aufklärungsarbeit und Anleitungen erhöhen wir die Onlinesicherheit für Kinder. Wir entwickeln zuverlässige interne Richtlinien für den risikolosen Umgang mit Inhalten und zur Vermeidung von Onlinemissbrauch. Durch Partnerschaften mit Regierungen, Unternehmen, Strafverfolgungsbehörden und anderen Beteiligten entsteht eine vertrauenswürdige Rechnerumgebung, die allen Anwendern mehr Sicherheit und Schutz bietet.
- Onlinesicherheit geht uns alle an. Daher müssen Regierungen, Unternehmen und andere Beteiligte eng zusammenarbeiten und allgemeingültige Sicherheitsrichtlinien entwickeln und einsetzen. Auch wenn Regierungen die Risiken durch weiterentwickelte Technologien und Onlinedienste berücksichtigen, ist es wichtig, dass sie technologische Innovationen ermöglichen und fortlaufend in die Sicherheitsprozesse einbinden.

HINTERGRUND

Obwohl oder gerade weil das Internet Kindern so viele positive Erfahrungen ermöglicht, stehen Eltern vor einer großen Herausforderung. Sie müssen die Inhalte, die ihre Kinder online ansehen und mit anderen teilen, zuverlässig überwachen, und sie müssen prüfen, mit wem die Kinder sich online treffen. Kinder sind heute online folgenden Risiken ausgesetzt:

- **Nicht kindgerechte Inhalte**. Kinder sind neugierig. Daher passiert es immer wieder, dass sie nachfragen, wenn sie Inhalte nicht verstehen. Häufig klicken sie dabei auf einen im ersten Moment absolut unverdächtig aussehenden Link, den sie per Sofortnachricht erhalten, in einem Blog entdecken oder mit einer ausgetauschten Datei empfangen.
- **Unangemessenes Verhalten**. Kinder, und übrigens auch Erwachsene, belästigen im Internet oft andere Anwender. Dabei kommt es häufig vor, dass Kinder verletzenden oder bösartigen Kommentaren über ihre Person ausgesetzt sind oder mit kompromittierenden Bildern beleidigt werden.
- **Nicht erwünschte Kontakte**. Einige Erwachsene benutzen das Internet, um gezielt unerfahrene, schwache Jugendliche kennenzulernen. Häufig haben sie dabei das Ziel, eine für die Jugendlichen vermeintlich innige, tiefe Freundschaft aufzubauen – ein Vorgehen, das oft auch Grooming oder Komfortverhalten genannt wird.

DER MICROSOFT-ANSATZ

Mit einem vierstufigen Ansatz erhöhen wir die Onlinesicherheit von Kindern.

- **Technologische Hilfsmittel**. Eltern können die Onlinerisiken für ihre Kinder verringern, indem sie die in viele unserer Produkte und Dienste integrierten Sicherheitsfunktionen nutzen. Microsoft Family Safety hilft Eltern, die Onlineaktivitäten ihrer Kinder zu überwachen und den Onlineschutz zu erhöhen. Anwender, die ein Microsoft-Benutzerkonto verwenden, können entscheiden, wer ihr Profil anschauen und ihnen Nachrichten senden darf. Zudem haben wir in die Xbox 360-Konsole standardmäßig Sicherheitseinstellungen integriert.
- **Interne Richtlinien und Methoden**. Für die Entwicklung unserer Produkte und Dienste gelten unternehmensweite Richtlinien, Standardvorgaben und Prozeduren, die eine Verbindung mit dem Web nur mit entsprechender Onlinesicherheit erlauben. Dies erfordert von den Nutzern unserer Onlinedienste bestimmte Verhaltensweisen, aber auch Inhalte und Interaktionen müssen Missbrauch

und illegalen Aktionen vorbeugen, und es gilt, unangemessenes Material zu vermeiden.

- **Partnerschaften**. Eine sichere Onlineumgebung erfordert einen ganzheitlichen Ansatz, der Anwender, Regierungen, Technologieanbieter und Nichtregierungsorganisationen umfasst. Sie spielen alle eine gleichermaßen wichtige Rolle dabei.
- **Aufklärung und Anleitung**. Das Microsoft Safety and Security Center enthält altersbezogene Anleitungen für die Internetnutzung. Dazu gehören Tipps, mit denen Eltern ihren Kindern erklären, welche Inhalte sie anschauen und mit anderen teilen dürfen. Diese Webseite gibt Tipps, wie sich Onlinebeschimpfungen verhindern lassen, wie sich die Sicherheit in sozialen Netzen erhöhen lässt, wie mobile Endgeräte besser geschützt werden, auf was bei Onlinespielen besonders zu achten ist und wie unangemessenes Verhalten vermieden, verhindert und gemeldet werden kann.

STRATEGISCHE ÜBERLEGUNGEN

- **Es sind strengere Gesetze gegen die Ausbeutung und Ausnutzung von Kindern nötig**. Wir unterstützen das International Center for Missing and Exploited Children (ICMEC), Interpol und viele weitere Organisationen und ermutigen Regierungen, schärfere Gesetze gegen den Besitz und die Verbreitung von kinderpornografischen Bildern zu erlassen.
- **Mehr Selbstkontrolle und gesetzlich definierte Rahmenbedingungen**. Wenn Regierungen auf Vorfälle mit neuen und weiterentwickelten Technologien und Onlinediensten reagieren, sollten sie jedoch nicht auf Innovationen und die Integration neuer Technologien in die Schutzprozesse verzichten. Regierungen und Unternehmen müssen gemeinsam Sicherheitsgrundsätze erarbeiten und umsetzen, die eine Onlineumgebung mit mehr Sicherheit für Jugendliche schaffen. Beispiele für solche Zusammenarbeiten sind die EU-Richtlinien Safer Social Networking Principles, der ISP Code of Practice in Australien und die im Rahmen der Europäischen Union erfolgende Zusammenarbeit der Geschäftsführer mehrerer Unternehmen zum Thema Child Online Safety.
- **Wir befürworten die Aufnahme eines Lehrfachs Internetsicherheit in die Lehrpläne von Schulen und diesbezüglich besondere Trainings für Lehrer**. Schüler und Lehrer werden davon profitieren, weil sie frühzeitig lernen, Gefahren und Risiken bei der Internetnutzung zu erkennen und zu vermeiden, ihre dabei genutzten Rechner zu schützen und sich online angemessen und moralisch korrekt zu verhalten. Regierungen müssen Anreize für Internettechnologie-Anbieter, Organisationen für mehr Onlinesicherheit und Schulbehörden schaffen, um vorhandene Lehrpläne für mehr Onlinesicherheit einzusetzen und damit dieses Ziel zu erreichen.
- **Die Durchführung von Studien und die Finanzierung von Forschungsarbeiten**. Die Forschung trägt wesentlich dazu bei, Verursacher von Onlinerisiken zu entdecken. Sie widerlegt zudem Mythen, die ungeeignete Maßnahmen für mehr Internetsicherheit nach sich ziehen. Die finanzielle Unterstützung durch Regierungen ist essenziell für akademische und industrielle Forschungsprojekte zum Thema mehr Sicherheit im Internet.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center hilft Ihnen mit Informationen über Sicherheitsthemen
www.microsoft.com/security

Das International Centre of Missing and Exploited Children (ICMEC)
www.icmec.org

Das Family Online Safety Institute
www.fosi.org

Eine Übersicht über Kontrollwerkzeuge für Eltern und Aufklärungsmaterial für mehr Sicherheit
www.getnetwise.org

Der Kampf gegen Menschenhandel

Die wichtigsten Punkte im Überblick

- Obwohl die Technologie den verabscheuungswürdigen Menschenhandel erleichtert, ist sie doch auch eine starke Waffe dagegen.
- Wir nutzen all unsere im Kampf gegen technologieunterstützte Verbrechen gewonnene Erfahrung und investieren in Forschung und Entwicklung, Programme und Partnerschaften. Wir möchten die Menschenrechte schützen und den Kampf gegen Menschenhandel vorantreiben.
- Der Kampf gegen Menschenhandel ist komplex und erfordert eine mehrteilige Lösung mit starken öffentlich-privaten Partnerschaften und Interventionen, denen zuverlässige Recherchen zugrunde liegen.

HINTERGRUND

Menschenhandel umfasst Zwangsprostitution, Zwangsarbeit und viele weitere Formen des modernen Sklaventums. Technologie spielt bei der Durchführung und der Bekämpfung dieser Verbrechen eine Rolle. Derzeit gibt es noch zu wenige Recherchen über das Ausmaß, inwieweit Technologie den Menschenhandel unterstützt. Dies gilt auch für den Anteil der Technologie im Kampf gegen den Menschenhandel: Es ist nicht bekannt, inwieweit Strafverfolgungsbehörden und Nichtregierungsorganisationen damit Kriminelle und Opfer identifizieren können. Jüngste Untersuchungen zeigen, dass die Technologie ein durchaus großes Potenzial für den Kampf gegen den Menschenhandel besitzt.

Rechtsanwälte, Strafverfolgungsbehörden und Regierungen bekämpfen seit Langem weltweit den Menschenhandel. Wenn es um die Vermeidung und Bekämpfung von technologisch gestützten Verbrechen geht, kommt Technologieunternehmen eine wichtige Rolle zu. Mit detaillierten Recherchen und innovativen Lösungen müssen sie den Weg bereiten für eine effiziente Bekämpfung des Menschenhandels.

DER MICROSOFT-ANSATZ

Als eines der führenden globalen Technologieunternehmen respektieren wir die Menschenrechte und unterstützen den Kampf gegen Menschenhandel jeglicher Art. Wir haben dies im Juli 2012 mit unserem Bekenntnis zu den Menschenrechten deutlich gemacht, das den Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte entspricht.

Auf dieser Basis entstanden gemeinsame Aktionen unserer Geschäftsbereiche Microsoft Research, Microsoft Digital Crimes Unit und des Microsoft Technology and Human Rights Center. Hier eine auszugsweise Übersicht:

Forschung und Innovation. Wir erforschen sehr genau, welche Rolle Technologie insbesondere bei der Kinderzwangsprostitution spielt.

- Im Dezember 2011 bat Microsoft Research und die Digital Crimes Unit um Vorschläge für akademische Untersuchungen, welche Rolle Technologie im Bereich des sexuellen Missbrauchs von Kindern spielt. Die sechs besten Einreichungen honorierten wir mit 185 000 US-Dollar. Die Ergebnisse werden wir 2013 veröffentlichen.
- Gemeinsam mit der Harvard Kennedy School of Government und der Annenberg School, Universität von Südkalifornien führen wir eine weitere, ähnliche Untersuchung durch.

- Mit führenden Technologie- und Nichtregierungsorganisationen veranstalten wir beispielsweise International Girls Only Hackathon. Davon versprechen wir uns weitere technologische Hinweise, die uns im Kampf gegen Menschenhandel weiterbringen.

Partnerschaften. Wir unterstützen Organisationen wie das International Centre for Missing and Exploited Children sowie Strafverfolgungsbehörden auf der ganzen Welt im Kampf gegen den sexuellen Missbrauch von Kindern, der auch durch den Technologieeinsatz möglich wird. PhotoDNA, eine teilweise von uns entwickelte Anwendung für den Vergleich von Bildern, wird von vielen Nichtregierungsorganisationen, Strafverfolgungsbehörden und anderen Technologieanbietern wie Facebook und NetClean eingesetzt, um Bilder zu entdecken, die Kindesmissbrauch zeigen.

Wir nehmen an vielen öffentlich-privaten Initiativen gegen den Menschenhandel teil. Dabei handelt es sich unter anderem um die Global Business Coalition Against Trafficking, die White House Office of Science and Technology Policy, den Council on Women and Girls, UN.GIFT, die amerikanische Generalbundesstaatsanwaltschaft und regionale Polizeibehörden.

Im September 2010 wurden wir gemeinsam mit Facebook, Twitter, Google und anderen Unternehmen Gründungsmitglied der Thorn Foundation Technology Task Force. Deren Ziel ist es, mit neuen technologischen Möglichkeiten den sexuellen Missbrauch von Kindern zu verhindern. Wir unterstützen Nichtregierungsorganisationen, die den Menschenhandel bekämpfen und die sich um die Opfer kümmern – wie etwa das Polaris Project und die International Justice Mission.

Unterbrechung. Alle Aktionen, die den Menschenhandel empfindlich stören oder gar unterbinden, sind eine wichtige Hilfe. Gemeinsam mit anderen arbeiten wir daran, die Kosten, Risiken und Schwierigkeiten für Menschenhändler so zu erhöhen, dass Menschenhandel weniger lukrativ und damit weniger attraktiv wird.

Richtlinien und bewährte Methoden. Wir verbessern fortlaufend den Schutz unserer Technologien und Prozesse, damit sie intern sowie im Betrieb bei Lieferanten weniger verwundbar sind und nicht für verbrecherische Zwecke genutzt werden können.

Unternehmen, die für uns arbeiten, müssen unseren Code of Conduct unterzeichnen, der die Regeln für die geschäftliche Zusammenarbeit festlegt. Er enthält explizit das Verbot, Zwangsarbeiter zu beschäftigen. Für Hardwarehersteller und Verpackungsunternehmen haben wir ein Programm für mehr soziale und umweltbezogene Verantwortung entwickelt, das unabhängige Prüfungen durch Drittunternehmen vorsieht. So stellen wir sicher, dass der Code of Conduct und regionale sowie nationale Vorgaben eingehalten werden. Sollten Unternehmen die Standards nicht erfüllen, fordern wir sie zu Nachbesserungen auf, und im schlimmsten Fall müssen sie mit der Kündigung des Vertrags rechnen.

Wir verwenden Technologien wie PhotoDNA auch mit Bing und SkyDrive, weil wir nicht wollen, dass Verbrecher unsere Onlinedienste für Kindesmissbrauch und die Verteilung von kinderpornografischen Bildern nutzen.

STRATEGISCHE ÜBERLEGUNGEN

- Wir befürworten und unterstützen Gesetze, die Menschenhandel verbieten und unter Strafe stellen. Opfer müssen besser geschützt und Täter sehr viel härter bestraft werden.
- Forschungseinrichtungen und Technologieunternehmen müssen mit Regierungen, Strafverfolgungsbehörden und anderen am Kampf gegen den Menschenhandel Beteiligten über den dabei erfolgenden Missbrauch der Technologie aufklären. Sie müssen auf Basis ihrer Forschungen und Recherchen effiziente Techniken und Initiativen entwickeln, die den Menschenhandel empfindlich stören.
- Technologieunternehmen sollten bewährte Methoden entwickeln, die Investitionen in wissenschaftliche Forschung genauso vorsehen wie einen verpflichtenden Verhaltenskodex. Dazu gehören auch Mechanismen, mit denen Anwender potenzielle Probleme melden, Hotlines, die illegale Aktivitäten aufnehmen, und die Informationsbereitstellung für Opfer.

Hilfreiche Ressourcen

Die Microsoft-Erklärung über die Menschenrechte
aka.ms/Human-Rights-Statement

Die Microsoft-Initiative für die Erforschung des Technologie-Einflusses beim Kindesmissbrauch
aka.ms/human-trafficking-rfp

Die Digital Crimes Unit von Microsoft
www.microsoft.com/dcu

Microsoft Research
research.microsoft.com

Microsoft PhotoDNA
www.microsoftphotodna.com

Die Global Business Coalition gegen den Menschenhandel
gbcat.org

Februar 2013

Der Kampf gegen Online-Kindesmissbrauch

Die wichtigsten Punkte im Überblick

- Das Internet bietet viele Vorteile und konstruktive Anwendungsmöglichkeiten. Gleichzeitig eröffnet es Kriminellen neue Wege, um Kinder und Jugendliche zu missbrauchen – Stichwort: Kinderpornografie.
- Wir investieren viel in umfassende Untersuchungen, mit denen wir Technologien, Techniken und Prozesse für den Kampf gegen Kindesmissbrauch im Internet weiterentwickeln. Mit ausgefeilten Filtermethoden und einer fortschrittlichen Technologie wie PhotoDNA verfeinern und automatisieren wir die Suche nach kinderpornografischen Darstellungen in den Milliarden im Internet gespeicherten Fotos.
- Wir arbeiten mit Experten auf der ganzen Welt an innovativen Lösungen, mit denen wir den sexuellen Missbrauch von Kindern, etwa durch Kinderpornografie oder Zwangsprostitution, im Internet unterbinden können.

HINTERGRUND

Jeden Tag nutzen Millionen Anwender das Internet und stellen dort auf vielerlei Art hilfreiche Inhalte für alle bereit. Allerdings profitieren auch Verbrecher von dieser Art der Informationsverteilung, indem sie so die Möglichkeit erhalten, Jugendliche und Kinder zu missbrauchen. Sie stellen kinderpornografische Darstellungen online, bieten Kinder als Zwangsprostituierte an oder erschleichen sich zum Zweck des Missbrauchs das Vertrauen von Jugendlichen.

Die Erstellung und Veröffentlichung von Kinderpornografie ist ein großes Problem für Strafverfolgungsbehörden. Seit dem Jahr 2002 hat das National Center for Missing and Exploited Children (NCMEC) mehr als 65 Millionen Bilder und Videos mit kinderpornografischen Inhalten untersucht. Entdeckt wurde dieses Material in den meisten Fällen, weil es Anwender in pädophilen Kreisen untereinander und mit anderen Anwendern, die ebenfalls sexuelles Interesse an Kinderpornografie zeigten, tauschten.

Die meisten Opfer pornografischer Darstellungen im Jahr 2011 waren laut NCMEC Kinder, wobei Babys und Kleinkinder die am schnellsten wachsende Gruppe waren. Internetunternehmen kommt eine bedeutende Rolle im Kampf gegen diese abscheulichen und verabscheuungswürdigen Verbrechen zu. Sie müssen diese illegalen Bilder schnell finden, an Strafverfolgungsbehörden melden und löschen.

Eine weitere große Gefahr für Kinder sind Verbrecher, die wehrlose Opfer im Internet suchen. Diese Kriminellen suchen Schutz in der Anonymität, um aus sexuellen Gründen online enge Freundschaften und vertrauliche Beziehungen mit Kindern aufzubauen oder um Kontakt mit Menschenhändlern aufzunehmen, die Kinder als Zwangsprostituierte anbieten. Wie im Kampf gegen Kinderpornografie kommt auch hier Internetunternehmen eine besondere Rolle zu – sie müssen auch diesen Kriminellen mit geeigneten Maßnahmen das Handwerk legen. Dies kann mit einem Verhaltenskodex erfolgen, oder indem sie Kunden Mechanismen bereitstellen, mit denen diese kriminelle Subjekte melden können. Nicht zu vergessen der Einsatz innovativer Lösungen für eine bessere Entdeckung der Verbrecher.

Weltweit erfüllen die Strafverfolgungsbehörden ihre Aufgabe im Kampf gegen Kindesmissbrauch durchaus bewundernswert. Allerdings erfordert diese Art des Verbrechens eine stärkere und bessere Zusammenarbeit zwischen Strafverfolgungsbehörden, Regierungen, Industrieunternehmen, Nichtregierungsorganisationen und akademischen Bereichen.

DER MICROSOFT-ANSATZ

- Unsere Digital Crimes Unit (DCU) ist ein globales Team, bestehend aus Rechtsanwälten, Untersuchungsbeamten, technischen Analysten und anderen Experten. Ihr Ziel ist es, digitale Verbrechen durch Partnerschaften sowie mit legalen und technischen Maßnahmen zu verhindern, indem die operative Basis der Cyber-Kriminellen zerstört wird. Die DCU ist einzigartig in der IT-Branche, weil sie gegen eine der gefährlichsten Cyber-Bedrohungen kämpft, denen wir uns heute gegenübersehen. Inklusive des sexuellen Kindesmissbrauchs mithilfe des Internets.

- Wir setzen viele Ressourcen ein für die Entwicklung von Technologien, die den Kindesmissbrauch online vermeiden und Regierungen sowie Nichtregierungsorganisationen im Kampf dagegen unterstützen. Dazu gehören Filtermethoden, aber auch mehr als 100 extra ausgebildete Spezialisten, die Bilder mit Darstellungen von Kindesmissbrauch auf Bing, SkyDrive und weiteren Onlinediensten entdecken und klassifizieren. Wir geben Bilder mit kinderpornografischen Inhalten an die NCMEC weiter und entfernen die Bilder von dem jeweiligen Onlinespeicherort. Zusätzlich verwehren wir den für die Veröffentlichung der Bilder verantwortlichen Anwendern die weitere Nutzung unserer Onlinedienste.

- Ein Hilfsmittel im Kampf gegen die Veröffentlichung illegaler Bilder ist PhotoDNA, eine von unserem Research-Geschäftsbereich zusammen mit dem Dartmouth College entwickelte Technologie. Sie verfeinert und automatisiert die Suche nach Bildern mit kinderpornografischen Inhalten in den Milliarden im Internet gespeicherten Fotografien. Im Jahr 2009 hat die DCU die PhotoDNA-Lizenz an die NCMEC übertragen, damit auch andere Onlinedienste wie Facebook nach entsprechenden pornografischen Darstellungen von Kindern durchsucht werden können.

- Wir unterstützen Strafverfolgungsbehörden auf der ganzen Welt bei der Entwicklung von Hilfsmitteln, die ihnen den Kampf gegen Kindesmissbrauch erleichtern. Im Jahr 2012 begann unsere Zusammenarbeit mit NetClean, um die Bilderkennungsanwendung PhotoDNA kostenlos Strafverfolgungsbehörden für die Untersuchung von kinderpornografischen Inhalten bereitzustellen.

- Gemeinsam mit anderen erarbeiten wir Innovationen für den Kampf gegen Kindesmissbrauch. Zusammen mit Facebook, Twitter, Google und anderen Unternehmen sind wir Mitglied der Thorn Foundation. Dort forschen wir nach neuen Wegen und Technologien zur Lösung dieses Problems. Im Jahr 2012 haben unsere Geschäftsbereiche DCU und Research sechs Forscherteams mit Untersuchungen beauftragt, die uns ein besseres Verständnis darüber geben sollen, wie Kinder online von Verbrechern angeboten und verkauft und welche Technologien dabei eingesetzt werden. Die Ergebnisse dieser Untersuchungen werden wir im Lauf des Jahres 2013 veröffentlichen.

STRATEGISCHE ÜBERLEGUNGEN

- Wir befürworten und unterstützen Gesetze, die weltweit Besitz, Erstellung, Verteilung und Handel mit kinderpornografischen Darstellungen verbieten und unter Strafe stellen. 2010 berichtete das International Centre for Missing and Exploited Children (ICMEC), dass lediglich 45 Staaten über eine ausreichende Gesetzgebung für den Kampf gegen Kinderpornografie verfügen – und dass in 89 Staaten gar keine Gesetze gegen diese Verbrechen in Kraft sind.

- Internetunternehmen müssen weiterhin mit Regierungen und Strafverfolgungsbehörden zusammenarbeiten, um das Problem des Kindesmissbrauchs besser in den Griff zu bekommen. Dazu sind bewährte Methoden und Leitfäden nötig, und Unternehmen müssen motiviert werden, freiwillig nach kinderpornografischen Darstellungen im Internet zu suchen und diese zu melden und zu eliminieren. Durch ihre gezielte Einflussnahme können politische Entscheider und Regierungsbeamte dafür sorgen, dass Gesetze die Opfer stärker berücksichtigen und nicht nur Verbrechen verhindern, sondern auch besser davor schützen.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center mit altersbezogenen Tipps für die Internetnutzung
www.microsoft.com/security

Microsoft PhotoDNA
www.microsoftphotodna.com

Die Microsoft-Erklärung hinsichtlich der Menschenrechte
aka.ms/Human-Rights-Statement

Die Microsoft Digital Crimes Unit
www.microsoft.com/DCU

Das National Center for Missing and Exploited Children (NCMEC)
www.ncmec.org

Die Microsoft-Initiative zur Untersuchung, welche Rolle Technologie beim Kindesmissbrauch spielt
aka.ms/human-trafficking-rfp

Schutz vor unerwünschten Internetkontakten

Die wichtigsten Punkte im Überblick

- Beim Grooming, der unerwünschten Kontaktaufnahme mit Kindern zum Zweck des sexuellen Missbrauchs, suchen Sexualstraftäter im Internet gezielt nach Kindern und bauen mit ihnen eine vertrauensvolle Freundschaft auf.
- Mit innovativen Werkzeugen, Aufklärungsarbeit und Anleitungen, internen Richtlinien sowie Methoden für die Verarbeitung von Inhalten und zur Vermeidung von Onlinemissbrauch bekämpfen wir den Kindesmissbrauch. Weitere Maßnahmen hierbei sind die partnerschaftliche Zusammenarbeit mit Regierungen, Unternehmen und Strafverfolgungsbehörden.
- Wir befürworten strenge Gesetze und deren rigorose Anwendung im Fall von sexuellem Kindesmissbrauch. Wir unterstützen Strafverfolgungsbehörden, um im Internet Pädophile zu enttarnen und ihrer gerechten Strafe zuzuführen.

HINTERGRUND

Bei einer unerwünschten Kontaktaufnahme werden Kinder von pädophilen Erwachsenen mit dem Ziel des sexuellen Missbrauchs emotional manipuliert. Bei diesem auch Grooming genannten Prozess befreundet sich normalerweise ein Erwachsener mit einem Kind oder Jugendlichen. Er umschmeichelt dabei den jungen Menschen, gibt ihm Geschenke oder Geld oder verspricht ihm einen Job als Model. Damit und mit weiteren persönlichen Aufmerksamkeiten baut der Pädophile Vertrauen und Sympathie auf. Letztendlich wird er aber immer das so aufgebaute Vertrauensverhältnis für den sexuellen Missbrauch nutzen. Er übernimmt dabei die Kontrolle über das Kind, um es fortgesetzt zu missbrauchen, wobei er in vielen Fällen kinderpornografisches Material erstellt oder die Kinder weiteren pädophilen Straftätern zur Verfügung stellt.

Pädophile finden sich immer dort, wo sich Kinder aufhalten. Also auch im Internet, wo Pädophile folglich auch ihr Unwesen treiben und unerwünschte Kontakte mit Kindern suchen. Am Anfang steht dabei oft die Teilnahme an Foren, die vor allem von Jugendlichen und Kindern besucht werden. Hierzu gehören Onlinespiele, die auch Gespräche und Videoübertragungen unterstützen, oder Chat-Bereiche. Oft nehmen Pädophile auch mit Sofort- und Textnachrichten Kontakt auf. Sie nutzen dabei Informationen, die Kinder online über sich selbst veröffentlichen, und beeinflussen vor allem Jugendliche mit einem geringen Selbstwertgefühl, familiären Problemen oder Geldmangel.

Der sexuelle Kindesmissbrauch ist ein globales Problem. Besonders wichtig ist es, dabei den Anteil der Verbrechen, der online verübt wird, nicht außer Acht zu lassen. Nach Angaben des amerikanischen Crimes Against Children Research Center wurden im Jahr 2006 mehr als 600 Onlinepädophile inhaftiert – das sind ein Prozent aller sexuellen Kindesmissbrauchsfälle.

Internetunternehmen spielen eine wichtige Rolle im Kampf gegen pädophile Verbrecher. Sie können mit einem Verhaltenskodex, der Überwachung von Foren, die hauptsächlich von Kindern genutzt werden, und mit Mechanismen, mit denen Kunden verdächtige Personen melden, für mehr Schutz und Vorbeugung sorgen.

DER MICROSOFT-ANSATZ

Technologische Hilfsmittel. Mit den vielen Sicherheitsfunktionen, die wir in unsere Produkte und Dienste integriert haben, sollen Eltern die Onlineaktivitäten ihrer Kinder kontrollieren.

Windows 8 bietet etwa mit Family Safety Werkzeuge für eine solche Überwachung an. Alle Anwender, Erwachsene und Kinder, die ein Microsoft-Benutzerkonto nutzen, können dafür festlegen, wer ihr Profil sehen und mit ihnen Kontakt aufnehmen darf. Auch in Xbox Live haben wir Einstellmöglichkeiten für die Onlinesicherheit integriert. Damit legen Eltern fest, mit welchen anderen Anwendern Kinder kommunizieren dürfen und wer ihre Profile oder Freundeslisten sehen darf.

Interne Richtlinien und Methoden. Um die Anwender unserer Onlinedienste zu schützen, verwenden wir Richtlinien wie unseren Verhaltenskodex, und wir prüfen Inhalte und Interaktionen auf mögliche illegale Aktivitäten, unangemessenes Material und andere Arten von Missbrauch.

Partnerschaften. Der Kampf gegen unerwünschte Kontakte und Kindesmissbrauch erfordert einen ganzheitlichen Ansatz, der die wichtigsten Mitstreiter – Technologieanbieter, Regierungen, Strafverfolgungsbehörden und Nichtregierungsorganisationen – vereint.

- Die Microsoft Digital Crimes Unit (DCU) ist unsere zentrale Waffe zur Vermeidung von Kindesmissbrauch. Im Fokus des weltweit operierenden Teams aus Anwälten, Untersuchungsbeamten, technischen Analysten und anderen Experten steht der Kampf gegen sexuellen Kindesmissbrauch im Internet. Dafür geht das DCU-Team Partnerschaften mit führenden Personen und Unternehmen aus verschiedenen Bereichen ein und verwendet neue technische Hilfsmittel und Werkzeuge.
- Gemeinsam mit dem International Centre for Missing and Exploited Children, Interpol und vielen weiteren Organisationen unterstützen wir Regierungen im Kampf gegen den Kindesmissbrauch.

Aufklärung und Anleitung. Das Microsoft Safety and Security Center stellt altersbezogene Leitfäden für die Internetnutzung zur Verfügung. Sie enthalten Tipps für das Onlineverhalten. Dazu gehört, welche Inhalte für Kinder angemessen sind und welche sie mit anderen teilen können, wie sie sich bei Onlinespielen und bei der Verwendung mobiler Endgeräte schützen können und wie sie unangemessenes, verdächtiges Verhalten erkennen, blockieren und melden.

STRATEGISCHE ÜBERLEGUNGEN

- Wir befürworten und unterstützen Gesetze gegen Kindesmissbrauch, die Besitz, Erstellung, Verteilung und Handel mit kinderpornografischen Darstellungen verbieten und unter Strafe stellen.
- Internetunternehmen müssen weiterhin mit Regierungen und Strafverfolgungsbehörden zusammenarbeiten, um das Problem des Kindesmissbrauchs besser in den Griff zu bekommen. Sie müssen ihren Kunden Mechanismen zur Verfügung stellen, um potenzielle Pädophile zu melden. Zudem sollten sie einen Verhaltenskodex verwenden, Strafverfolgungsbehörden unterstützen sowie innovative Hilfsmittel und Werkzeuge entwickeln und einsetzen.
- Wichtig ist es, dass Regierungen Studien in Auftrag geben sowie akademische und industrielle Forschungsarbeiten unterstützen, die zu mehr Sicherheit im Internet führen. Diese Forschung ist wichtig, weil sie Faktoren identifiziert, die das Onlinerisiko erhöhen, und weil sie mit Mythen aufräumt, die oft ungeeignete Maßnahmen für mehr Internetsicherheit nach sich ziehen.

Hilfreiche Ressourcen

Das Microsoft Security and Safety Center für mehr Onlinesicherheit von Jugendlichen
aka.ms/young-safety

Ein Vergleich der Family Safety-Hilfsmittel von Microsoft
aka.ms/compare-tools

Die Microsoft-Initiative zur Untersuchung, welche Rolle Technologie beim Kindesmissbrauch spielt
aka.ms/human-trafficking-rfp

Das Crimes Against Children Research Center
www.unh.edu/ccrc

Das International Centre for Missing and Exploited Children
www.icmec.org

Februar 2013

Schutz vor Onlinebetrug

Die wichtigsten Punkte im Überblick

- Onlinebetrug ist ein großes, globales Problem, dem Millionen ahnungslose Anwender zum Opfer fallen. In den USA berichtete das Internet Crime Complaint Center des FBI im Jahr 2011 von 300 000 Betrugsdelikten, die einen Schaden von fast einer halben Milliarde US-Dollar verursachten.
- Mit einem vierstufigen Ansatz bekämpfen wir Onlinebetrug: mit speziellen Teams, mit besonderen Technologien, mit Aufklärung und Anleitungen sowie mit Partnerschaften mit Regierungen, Industrieunternehmen, Strafverfolgungsbehörden und anderen Organisationen.
- Wir unterstützen Regierungen, die mit internationalen Kooperationen, öffentlich-privaten Partnerschaften sowie strengen Gesetzen gegen Onlinebetrug kämpfen.

HINTERGRUND

Das Internet hat den weltumspannenden Handel von Grund auf geändert. Es erleichtert und verschönert unser Leben, ermöglicht den Aufbau neuer Unternehmen und Dienstleistungen und unterstützt viele wirtschaftliche Aktivitäten. Der weltweite E-Commerce wird im Jahr 2013 voraussichtlich mehr als 1,2 Billionen US-Dollar Umsatz erzielen.

Mit diesem stetigen Wachstum des Onlinehandelsvolumens steigen aber leider auch die Fälle von Onlinebetrug. Sie untergraben zudem das Vertrauen der Anwender in die Vorteile des E-Commerce.

Onlinebetrug ist ein großes, globales Problem, dem Millionen ahnungslose Anwender zum Opfer fallen. In den USA berichtete das Internet Crime Complaint Center des FBI im Jahr 2011 von 300 000 Betrugsdelikten, die einen Schaden von fast einer halben Milliarde US-Dollar verursachten. Organisierte Verbrecherbanden verüben immer mehr Cyber-Verbrechen und stehlen Identitäten, Geld und Waren.

Onlinebetrüger ködern ihre Opfer meistens mit hinterlistigen, schwer durchschaubaren Taktiken und verwenden soziale Netze, bösartige Anwendungen und andere Hilfsmittel für ihre Attacken. So werden jedes Jahr Millionen Internetanwender zum Opfer.

Mit sogenannten Social-Engineering-Attacken erschleichen Betrüger das Vertrauen eines Anwenders. Sie verleiten ihn dann zur Installation bösartiger Anwendungen, die als offizielle App getarnt sind, oder veranlassen ihn, vertrauliche persönliche Daten auf einer gefälschten Website einzugeben. In jedem Fall gefährden Anwender damit ihren Rechner und die damit verarbeiteten persönlichen Informationen.

Eine andere Betrugsmasche verwendet E-Mails, Sofortnachrichten oder Nachrichten in sozialen Netzen, die vorgeblich von einer angesehenen Firma versendet wurden. Mit diesen Phishing-Attacken fordern sie Anwender auf, geheime Informationen wie Kontonummern oder Kennwörter einzusenden. Im Jahr 2011 berichtete die Anti-Phishing Working Group über fast 200 000 verschiedene Phishing-Attacken weltweit. Die jüngst veröffentlichten Daten zeigen, dass die Zahl der durch Phishing-Attacken betroffenen Unternehmen auf einem Allzeithoch ist.

Um den Onlinebetrug wirkungsvoll zu bekämpfen, müssen Unternehmen, Regierungen, Nichtregierungsorganisationen und Anwender weltweit zusammenarbeiten.

DER MICROSOFT-ANSATZ

Mit einem vierstufigen Ansatz bekämpfen wir Onlinebetrug: mit speziellen Teams, mit besonderen Technologien, mit Aufklärung und Anleitungen sowie mit Partnerschaften mit Regierungen, Industrieunternehmen, Strafverfolgungsbehörden und anderen Organisationen.

- **Spezielle Teams**. Die Microsoft Digital Crimes Unit (DCU) ist ein globales Team, bestehend aus Rechtsanwälten, Untersuchungsbeamten, technischen Analysten und anderen Experten. Ihr Ziel ist es, digitale Verbrechen durch Partnerschaften sowie mit legalen und technischen Maßnahmen zu verhindern, indem die operative Basis der Cyber-Kriminellen zerstört wird. Die DCU ist einzigartig in der IT-Branche, weil sie gegen eine der gefährlichsten Cyber-Bedrohungen kämpft, denen wir uns heute gegenübersehen. Inklusive des sexuellen Kindesmissbrauchs mithilfe des Internets.
- **Technologische Werkzeuge**. Wir stellen viele Werkzeuge für mehr Onlinesicherheit bereit, mit denen sich Anwender vor Onlinebetrug schützen können. Hierzu gehören die kostenlose Anti-Malware-Anwendung Microsoft Security Essentials sowie SmartScreen-Technologien und -Dienste.
  - » Der SmartScreen-Dienst schützt Anwender davor, Malware als Teil von Social-Engineering-Attacken herunterzuladen, wie etwa per Phishing-Attacken auf Internet Explorer 9 und 10.
  - » Mithilfe des SmartScreen Application Reputation-Diensts treffen Anwender von Internet Explorer 9 und 10 bessere Entscheidungen, ob eine Anwendung, die sie herunterladen möchten, vertrauenswürdig ist. Lädt ein Anwender eine App aus dem Internet herunter, verwendet SmartScreen vorhandene Informationen, um unnötige Warnhinweise bei einer bekannten und vertrauenswürdigen Datei zu verhindern. Besteht ein erhöhtes Risiko, weil die herunterzuladende Datei möglicherweise bösartig ist, werden entsprechende Warnungen angezeigt.
  - » Mit den SmartScreen Antispam-Technologien und -Diensten schützen wir Anwender vor E-Mail-Nachrichten, die möglicherweise betrügerische Absichten fördern.
- **Aufklärung und Anleitung**. Das Microsoft Safety and Security Center bietet Anleitungen für eine sichere Internetnutzung. Darunter befinden sich Tipps, wie Anwender ihre Rechner effizient schützen und Onlinebetrugsversuche vermeiden.
- **Partnerschaften**. Wir arbeiten mit vielen Organisationen wie der Anti-Phishing Working Group und der National Cyber Security Alliance im Kampf gegen Onlinebetrug zusammen.

STRATEGISCHE ÜBERLEGUNGEN

- **Internationale Kooperationen**. Wir ermutigen gemeinsam mit Partnern aus der Industrie Staaten, das Übereinkommen über Computerkriminalität des Europarats zu übernehmen und zu ratifizieren. Die Unterzeichner müssen die Gesetze und Prozeduren im Kampf gegen Cyber-Kriminalität übernehmen und anpassen.
- **Öffentlich-private Partnerschaften**. Sie sind unserer Meinung nach sehr wichtig im Kampf gegen die immer komplexer werdenden Cyber-Verbrechen. Wir unterstützen Strafverfolgungsbehörden weltweit mit technischen Trainings und entwickeln fortlaufend neue Technologien, die Onlinebetrug bekämpfen. Zudem schützen wir Anwender, indem wir gesetzlich gegen Onlinebetrüger vorgehen.
- **Kompromissloses Durchsetzen und ausgewogene Regularien**. Wir unterstützen eine kompromisslose Gesetzgebung, die Gesetze im Kampf gegen Onlinebetrüger rigoros anwendet. Gleichzeitig ist es wichtig, dass diese Gesetze so ausgestaltet werden, dass die Übernahme von Innovationen und neuen Technologien nicht behindert wird.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center mit Anleitungen für Anwender
www.microsoft.com/security

Onlinebetrug: Vorbeugen, entdecken und beheben – ein Leitfaden
aka.ms/OnlineFraudBooklet

Die Microsoft Digital Crimes Unit
www.microsoft.com/dcu

Digitales Bürgertum

Die wichtigsten Punkte im Überblick

- Junge Menschen leben im Informationszeitalter mit oftmals unklaren Regeln und sozialen Normen. Sie müssen erst noch lernen, diesen Raum als digitale Bürger zu nutzen. Damit sie in der Onlinewelt verantwortungsbewusste und moralisch einwandfreie Entscheidungen treffen können, müssen sie erst ein Gespür für den Wert persönlichen Eigentums und persönlicher Verantwortung entwickeln.

- Das Internet bietet jungen Menschen großartige Möglichkeiten, allerdings mit einem hohen Risiko. Einige dieser Risiken lassen sich vermeiden, wenn sie lernen, als digitale Bürger verantwortungsbewusst zu handeln.

- Schützende Maßnahmen sind nicht alles, weil sie lediglich auf akute Bedrohungen reagieren. Viel besser ist es, die Onlinesicherheit mit vorbeugenden Maßnahmen zu vermeiden. Dazu gehört es, junge Menschen auf die digitale Welt vorzubereiten und ihnen zu zeigen, wie sie als digitale Bürger die eigene Sicherheit im Internet erhöhen. Die Aufklärung über digitale Kompetenz, ethische Grundsätze und angemessene Verhaltensweisen dürfen keine Option sein – sie sind ein Muss.

HINTERGRUND

- Neue Informationstechnologien haben die Welt, in der junge Menschen aufwachsen und lernen, grundlegend verändert. Die unendlichen Internetressourcen und die große Zahl der internetfähigen Endgeräte eröffnen ihnen ungeahnte Möglichkeiten der Kommunikation, des Lernens und der Informationsverteilung. Viele Erwachsene haben allerdings Bedenken wegen der Onlinesicherheit von Jugendlichen und Kindern, die im Internet auch mit unangemessenen Inhalten konfrontiert werden, sexuellem Missbrauch ausgesetzt sind, persönlich verunglimpft werden oder andere verletzende Onlineerfahrungen machen.

- Viele Staaten schützen junge Internetnutzer mit einem dreistufigen Ansatz, der technische Hilfsmittel, Aufklärungsmaßnahmen und den Schutz durch entsprechende Gesetze vorsieht. Dies sind zwar sehr wichtige strategische Hilfsmittel, sie reagieren aber leider nur auf bereits bekannte Bedrohungen. Mehr Onlinesicherheit verspricht dagegen ein Ansatz, der eine Aufklärung der Jugendlichen über die Regeln und Verhaltensmuster im Internet vorsieht, damit diese das Internet verantwortungsbewusst nutzen. Genau dies ist der Ansatz, mit dem aus jungen Menschen digitale Bürger werden.

- Digitale Bürger oder digitales Bürgertum wird oft beschrieben als „Verhaltensregeln unter Berücksichtigung der verwendeten Technologie“. Digitales Bürgertum bedeutet aber viel mehr als soziale Verhaltensnormen. Es muss junge Menschen auf ihr Leben und ihre Erfahrungen in einer technologisch orientierten Gesellschaft vorbereiten. Jugendliche und Kinder müssen ein Gespür für den Wert persönlichen Eigentums und persönlicher Verantwortung entwickeln, damit sie in der Onlinewelt angemessen und moralisch einwandfrei entscheiden. Zwei Elemente sind dabei wichtig:

- **Digitale Kompetenz**. Je besser junge Internetnutzer die Onlinewelt kennen, umso eher erkennen und vermeiden sie riskante Situationen, treffen mit mehr Informationen bessere Entscheidungen und wissen, wie sie ihre Privatsphäre schützen. Digitale Kompetenz bedeutet mehr als nur technisches Wissen; dazu gehört auch, die verschiedenen Quellen digitaler Informationen kritisch zu begutachten.

- **Digitale Ethik und Etikette**. Technisches Wissen ist eine solide Basis für das digitale Bürgertum. Aber nur wenn junge Menschen die digitale Ethik und Etikette kennen, können sie in der Onlinewelt vernünftige Entscheidungen treffen. Durch Aufklärung über die digitale Ethik entscheiden Jugendliche und Kinder moralisch einwandfrei, und mit dem Wissen über die digitale Etikette verhalten sie sich entsprechend den allgemeingültigen sozialen Normen.

DER MICROSOFT-ANSATZ

- Wir erhöhen die Onlinesicherheit von Kindern durch technologische Hilfsmittel, Aufklärungsarbeit und Anleitungen sowie durch Partnerschaften mit Regierungen, Unternehmen, Strafverfolgungsbehörden und anderen Organisationen. Unser Ziel ist es, für alle Anwender Rechnerumgebungen mit mehr Sicherheit und Vertrauen zu schaffen.
- Wir integrieren Informationen über das digitale Bürgertum in technische Anleitungen für Schüler und Studenten. Weil immer mehr Schulen und Universitäten neueste Technologien einsetzen, sollte unserer Meinung nach die Aufklärung über digitales Bürgertum ein wichtiger Bestandteil der Lehrpläne sein.
- Mit dem Microsoft Safety and Security Center stellen wir altersbezogene Leitfäden für die Internetnutzung zur Verfügung. Wir geben dort Tipps, wie Kinder über angemessene Inhalte aufgeklärt werden können, und erklären, wie sich Onlinemobbing vermeiden lässt. Weitere Themen sind die Sicherheit sozialer Netze, der Schutz mobiler Endgeräte, die verantwortungsbewusste Nutzung von Onlinespielen und der Umgang mit unangemessenem Verhalten.

STRATEGISCHE ÜBERLEGUNGEN

- Wir unterstützen breit gefächerte Maßnahmen für mehr Onlinesicherheit. Dazu gehört auch, durch digitale Medienkompetenz und Aufklärungsprogramme das Bewusstsein für das digitale Bürgertum zu schärfen. Wir helfen damit Eltern und Lehrern, Kinder für die Onlinewelt vorzubereiten und digitale Medien verantwortungsvoll zu nutzen.
- Wir empfehlen Bildungspolitikern, in ihrem Land Ziele für mehr Onlinesicherheit zu setzen. Dabei sollten zumindest Lehrpläne mit Standardvorgaben über die digitale Kompetenz eingesetzt werden, mit denen Kinder und Familien die täglichen multimedialen Anforderungen besser meistern.
- Zwar haben Regierungen noch viele Aufgaben zu erledigen. Wichtig ist aber auch, sie darauf hinzuweisen, was sie nicht tun sollten. Es ist ein verführerischer Gedanke, junge Menschen durch Gesetze zu schützen, die den Einsatz bestimmter Technologien vorschreiben. Doch diese haben sich in den meisten Fällen als ineffizient erwiesen, insbesondere aufgrund der weltumspannenden Reichweite und der enormen Größe des Internets. Zudem sind vorgeschriebenen Technologien sehr schnell veraltet, weil sie mit der hohen Geschwindigkeit, mit der sich die digitale Welt fortlaufend ändert, nicht mehr Schritt halten können.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center mit altersbezogenen Tipps für die Internetnutzung
www.microsoft.com/security

Onlinesicherheit 3.0:
Jugendliche besser schützen
aka.ms/Online-Safety30

Das Family Online Safety Institute
www.fosi.org

Forschungs- und Lehrmaterial für die Förderung des digitalen Bürgertums
www.digitalcitizenship.net

Kontrollmöglichkeiten für Eltern

Die wichtigsten Punkte im Überblick

- Eine gewissenhafte Kontrolle durch Eltern ist sehr wichtig für die Onlinesicherheit von Familien. Auch wenn sie keinen Ersatz für die elterliche Fürsorge darstellen, sind Technologien zum Überwachen und Filtern von Inhalten dennoch sehr hilfreich. Denn sie minimieren zusätzlich das Risiko, unangemessene Inhalte zu erhalten, von unerwünschten Personen kontaktiert und persönlich beleidigt zu werden.

- Wir unterstützen Eltern und Erziehungsberechtigte mit Funktionen für mehr Onlinesicherheit und zum Schutz der Privatsphäre, die wir in viele unserer Produkte, darunter Windows 8, Xbox 360 und Windows Phone 8, integriert haben.

- Die Entscheidung, welche Inhalte Kinder online anschauen und was sie im Internet tun dürfen, ist von Eltern und Erziehungsberechtigten zu treffen. Wir fördern die Zusammenarbeit von Regierungen mit Unternehmen und Nichtregierungsorganisationen, damit mehr Technologien für Onlinesicherheit bereitgestellt werden.

HINTERGRUND

Das Internet bietet Jugendlichen großartige Möglichkeiten, birgt aber auch Risiken hinsichtlich unangemessener Inhalte, unerwünschter Kontakte und persönlicher Verunglimpfungen. Viele gesellschaftliche Gruppen kämpfen für einen besseren Onlineschutz jugendlicher Anwender, der gleichzeitig aber nicht das uneingeschränkte Recht zur Informationsnutzung der volljährigen Anwender einschränkt. Das Internet soll schließlich frei und offen bleiben.

Jugendliche lassen sich mit Technologien schützen, mit denen Eltern die Onlineaktivitäten ihrer Kinder überwachen und kontrollieren. Dazu gehören die Filterung von Inhalten, Einschränkungen beim Herunterladen von Musikstücken, Apps und anderen Dateien sowie die Verwaltung von Kontakten. Diese Technologien werden mit Rechnern bereits seit Anfang der 1990er Jahre eingesetzt. Weil heute fast alle Endgeräte wie Mobiltelefone, Medienspieler, E-Reader und Spielekonsolen internetfähig sind, haben die meisten Hersteller darin ebenfalls Funktionen für eine bessere Kontrolle durch Eltern integriert.

Kontrollfunktionen für Eltern sind in vielen Ländern im Einsatz. Einer im Jahr 2011 durchgeführten Untersuchung des Family Online Safety Institute[1] zufolge werden diese in den USA von 54 Prozent der Eltern eingesetzt. Eine Studie der Europäischen Kommission[2] ergab, dass in Großbritannien 53 Prozent der Eltern diese Kontrollmöglichkeiten nutzen.

Obwohl die Kontrollfunktionen für Eltern beliebt und hilfreich sind, existieren darüber kontroverse Meinungen. Befürworter wünschen sich einen von Regierungen vorgeschriebenen Einsatz für Minderjährige, oft sogar für alle Onlineanwender. Dem stehen die Verfechter der Menschenrechte gegenüber, die eine solche Vorschrift strikt ablehnen. Andere Kritiker äußern Bedenken, dass mit dieser Technologie übereifrige Eltern ihre Kinder zu sehr kontrollieren und einschränken, dass damit Unternehmen Mitarbeiter ausspionieren, eifersüchtige Menschen ihre Partner überwachen oder totalitäre Staaten und Diktaturen die Internetnutzung durch ihre Bürger zensieren.

Unternehmen, die Kontrollfunktionen für Eltern entwickeln, müssen immer einen gesunden Kompromiss finden zwischen einem zuverlässigen Hilfsmittel, mit dem Eltern und Erziehungsberechtigte die Internetnutzung der Familienmitglieder verwalten, und einer so wenig wie möglich eingeschränkten Meinungsfreiheit und Privatsphäre.

[1] *Wer benötigt Kontrollfunktionen für Eltern? Eine Studie über Online-Kontrollfunktionen für Eltern und deren Nutzung*
www.fosi.org/research/900-who-needs-parental-controls.html

[2] *EU – Kinder online*
aka.ms/EUKidsOnlineReport

DER MICROSOFT-ANSATZ

Seit Jahren schützen wir Familien mit Funktionen für mehr Sicherheit und den Schutz der Privatsphäre, die wir in Windows-Betriebssysteme, Xbox, Xbox 360, Windows Phone und Bing integrieren. Wir wollen damit aber nicht kontrollieren, was Anwender sehen und tun dürfen und was nicht, sondern vielmehr Familien Hilfsmittel an die Hand geben, mit denen sie dies selbst entscheiden.

- **Windows 8: Microsoft Family Safety.** Damit erweitern wir die Windows-Kontrollfunktionen – wie Webfilterung, Blockieren unangemessener Inhalte sowie zeitliche und anwendungsbezogene Nutzungsvorgaben – für Eltern mit einer zentralen Onlineanlaufstelle, der Family Safety-Website. Dort verwalten sie die Rechner aller Familienmitglieder und erhalten Berichte über deren Onlineaktivitäten.
- **Windows Phone 8: Kinderecke.** Dies ist eine neue Windows Phone 8-Funktion, mit der Eltern und Erziehungsberechtigte spezielle Benutzerkonten für Kinder anlegen und damit den Zugriff auf Apps, Spiele, Videos und Musik einschränken. Kinder nutzen die Kinderecke des elterlichen Mobiltelefons, haben dabei aber keinen Zugriff auf wichtige Apps und Dokumente oder auf Funktionen, die ihrem Alter nicht angemessen sind – wie etwa im Web surfen oder Textnachrichten versenden.
- **Xbox 360 and Xbox LIVE.** Wir haben als erstes Unternehmen in unsere Spielekonsole mit den Family Settings eine auf Bewertungen basierende Kontrollfunktion für Eltern integriert. Dies gilt sowohl für das Video- und Unterhaltungssystem Xbox 360 als auch für unseren Onlinedienst Xbox LIVE.
  - » Mit den Sicherheitseinstellungen der Konsole entscheiden Eltern, welche Spiele Kinder online und offline spielen dürfen. Grundlage dafür sind Bewertungen von Spielen, Filmen und Fernsehshows. Eltern bestimmen mit dem Family Timer die Zeit, während der Kinder die Konsole nutzen dürfen.
  - » Mit den Einstellungen der Onlinesicherheit erstellen Eltern für jedes Kind ein Profil, das nur dem Alter und der Reife des Kindes angemessene Inhalte anzeigt. Damit ist es möglich, einem Kind bestimmte Aktivitäten zu erlauben, etwa Spiele mit mehreren Spielern gleichzeitig zu spielen, Videochats durchzuführen oder Sprach- und Textnachrichten zu nutzen. Zudem definieren Eltern damit, mit welchen Anwendern Kinder kommunizieren dürfen und wer das Profil oder die Freundesliste des Kindes ansehen darf.

STRATEGISCHE ÜBERLEGUNGEN

- Eltern und Erziehungsberechtigte wissen am besten, welche Inhalte Kinder online anschauen dürfen, und sollten daher diese Entscheidung selbst treffen. Kontrollfunktionen für Eltern oder Filteranwendungen müssen aber immer freiwillig verwendet werden. Wir fördern die Zusammenarbeit von Regierungen mit Unternehmen und Nichtregierungsorganisationen, damit mehr Technologien für Onlinesicherheit bereitgestellt werden. GetNetWise ist eine gemeinnützige Organisation, die Anleitungen und Hilfsmittel zur Verfügung stellt, die Kinder online mit neuesten Sicherheitstechnologien schützt.
- Wir befürworten eine Selbstregulierung von Unternehmen und ausgefeilte gesetzliche Rahmenbedingungen für technologieorientierte Bereiche. Auch wenn Regierungen die Risiken, die durch erweiterte Technologien und Onlinedienste entstehen, bekämpfen, dürfen sie eines nicht außer Acht lassen: Sie müssen dafür sorgen, dass innovative Entwicklungen jederzeit in diesen Prozess integriert werden.
- Wenn Regierungen und Unternehmen zusammenarbeiten, entstehen grundlegende Sicherheitsvorgaben und damit besser geschützte Onlineumgebungen. Gute Beispiel dafür sind die Safer Social Networking Principles der Europäischen Union und die Entwicklung des ISP Code of Conduct in Australien.
- Wir unterstützen eine Gesetzgebung mit ausreichender Rechtssicherheit für Unternehmen, die sich um angemessenes Verhalten der Anwender und angemessene Inhalte im Internet bemühen und deswegen nicht zusätzlich in die Verantwortung genommen werden. Beispiele hierfür sind Section 230 des U.S. Communications Decency Act und die Direktive 2000/31/EC der Europäischen Union.

Hilfreiche Ressourcen

Das Microsoft Security and Safety Center mit Anleitungen für alle Familienmitglieder
www.microsoft.com/security/family-safety

Die Microsoft Family Safety-Anwendung
aka.ms/Microsoft-family-safety

Sicherheitsressourcen für Videospiele und Onlinemedien
www.GetGameSmart.com

Ein umfassendes Verzeichnis mit Kontrollwerkzeugen für Eltern und Sicherheitsinformationen
www.getnetwise.org

Mobile Endgeräte und der Schutz von Jugendlichen

Die wichtigsten Punkte im Überblick

- Immer mehr junge Menschen verwenden Mobiltelefone, die mittlerweile zu einem sehr wichtigen Kommunikationsmittel für Familien geworden sind. Aber auch mit Mobiltelefonen entstehen Sicherheitsrisiken. Denn auch sie zeigen unangemessene Inhalte an, erlauben unerwünschte Kontaktaufnahmen, lassen persönliche Verleumdungen zu und unterstützen den Onlinehandel.

- Wir haben Windows Phone mit vielen Funktionen für mehr Sicherheit und den Schutz der Privatsphäre ausgestattet. Mit der Kinderecke erstellen Eltern spezielle Benutzerkonten für ihre Kinder, mit denen sie den Zugriff auf Apps, Spiele, Videos und Musikstücke einschränken.

- Gemeinsam mit Mobilfunkanbietern arbeiten wir an Richtlinien und bewährten Methoden, mit denen auf freiwilliger Basis klassifizierte Inhalte und standortbezogene Angaben sicherer verwendet werden und Daten für den mobilen Handel besser geschützt sind. Sie unterstützen Anwender dabei, die für ihre Familien besten Entscheidungen zu treffen.

HINTERGRUND

Im Jahr 2011, so eine Schätzung von MobileYouthReport.com, besaßen 1,6 Milliarden Menschen unter 30 Jahren ein Mobiltelefon. Die Vorteile liegen auf der Hand: Eltern und Kinder bleiben, genau wie Kinder mit ihren Freunden, besser in Kontakt. Mit Smartphones greifen sie zudem uneingeschränkt auf das Internet mit all seinen Inhalten zu.

Weil die meisten Mobiltelefone den Internetzugang ermöglichen, sind Kinder und Jugendliche dabei den gleichen Gefahren ausgesetzt wie mit jedem anderen internetfähigen Rechner:

- **Unangemessene Inhalte**. Kinder haben im Internet Zugriff auf Hassparolen oder andere unangemessene, sexuelle Inhalte. Zum Aufruf reicht es oft, einen Link in einer E-Mail, in einem sozialen Netz oder im Web anzuklicken.
- **Unangemessenes Verhalten**. Es gibt Jugendliche, die mit ihrem Mobiltelefon andere beleidigen oder verunglimpfen oder damit verletzende, schikanierende oder blamierende Bilder versenden. Ein besonderes Problem bei der Verwendung von Mobiltelefonen ist das sogenannte Sexting – der Versand sexuell anzüglicher, selbst mit der Kamera des Mobiltelefons erstellter Fotografien und Videos.
- **Unerwünschte Kontakte**. Einige Erwachsene benutzen das Internet, um gezielt unerfahrene, schwache Jugendliche kennenzulernen. Häufig haben sie dabei das Ziel, eine für die Jugendlichen vermeintlich innige, tiefe Freundschaft aufzubauen – ein Vorgehen, das oft auch Grooming oder Komfortverhalten genannt wird.
- **Betrügerischer Handel**. Kinder werden sehr leicht Opfer von Phishing-Attacken und anderen Betrugsversuchen. Sie werden zu einem schnellen Klick auf ein Flash-Werbebanner verleitet oder zu einem verlockenden, kostenlosen Spiel aufgefordert, das dann einen Virus überträgt. Oder sie sollen eine Klingelton herunterladen, der ebenfalls einen Virus oder Spyware oder andere bösartige Anwendungen enthält. In vielen Fällen entstehen dadurch sehr hohe Nutzungskosten, sodass die Eltern mit dem Erhalt der Mobilfunkrechnung eine böse Überraschung erleben.

DER MICROSOFT-ANSATZ

- Wir erhöhen die Onlinesicherheit von Kindern mit Technologien und Hilfsmitteln, mit Aufklärung und Anleitungen, mit internen Richtlinien und mit Methoden für die Verarbeitung von Onlineinhalten und die Vermeidung von Onlinemissbrauch. Durch die Zusammenarbeit mit Regierungen, Unternehmen, Strafverfolgungsbehörden und anderen Organisationen entsteht eine vertrauenswürdige Rechnerumgebung mit mehr Sicherheit.

- Wir arbeiten mit Unternehmen und Nichtregierungsorganisationen wie der GSM Association, der CTIA – The Wireless Association und dem Family Online Safety Institute ständig an einem verbesserten Schutz für Kinder und Jugendliche, die ihre mobilen Endgeräte online einsetzen.

- Windows Phone-Anwendern stehen viele Kontrollfunktionen zur Verfügung, mit denen sie ihre Privatsphäre mit Standardvorgaben oder benutzerdefinierten Einstellungen schützen können. Dazu gehört unter anderem auch die Weitergabe der Standortdaten an andere Apps, wodurch mit einer einzigen Einstellung der Zugang auf die Windows Location-Plattform möglich ist.

  Ist diese Plattform aktiviert, wenn ein Anwender eine App aus dem Windows Store zum ersten Mal ausführt, fragt Windows den Anwender, ob die App auf die aktuellen Standortdaten zugreifen darf. Umgekehrt ist es einer App bei nicht aktivierter Windows Location-Plattform unmöglich, auf die Standortdaten zuzugreifen. Jedes Mal, wenn ein Anwender eine App aus dem Windows Store ausführt, kann er die Verwendung der Standortdaten sehr einfach ein- oder ausschalten.

- Mit der Kinderecke von Windows Phone bestimmen Eltern, auf welche Apps, Spiele, Videos und Musikstücke Kinder zugreifen dürfen, und schützen ihr eigenes Benutzerkonto vor Missbrauch.

- Gemeinsam mit Mobilfunkanbietern und unabhängigen Softwareunternehmen arbeiten wir an verbesserten Sicherheitswerkzeugen für Mobiltelefone, die Familien besser schützen. Dazu gehören Methoden für die Inhaltsfilterung, definierbare Zugriffszeiten und eine bessere Kontakteverwaltung.

STRATEGISCHE ÜBERLEGUNGEN

- Wenn Regierungen auf Vorfälle mit neuen und weiterentwickelten Technologien und Onlinediensten reagieren, sollten sie jedoch nicht auf Innovationen und die Integration neuer Technologien in die Prozesse verzichten. Regierungen und Unternehmen müssen gemeinsam Sicherheitsgrundsätze erarbeiten und umsetzen, die eine Onlineumgebung mit mehr Sicherheit für Jugendliche schaffen.

- Für uns besteht die beste Art, Kinder vor unangemessenen Inhalten zu schützen, in einer freiwilligen Inhaltskontrolle und nicht in einer vorgeschriebenen Filterung oder Bewertung von Inhalten.

- Wir unterstützen Mobilfunkanbieter, die freiwillig umzusetzende Richtlinien und Methoden entwickeln, mit denen klassifizierte Inhalte und standortbezogene Angaben sicherer verwendet werden und Daten für den mobilen Handel besser geschützt sind. Sie unterstützen Anwender dabei, die für den Schutz ihrer Familien besten Entscheidungen zu treffen.

- Weil mobile Endgeräte effizientes Lernen ermöglichen, befürworten wir die Zusammenarbeit von Regierungen und Anbietern von Informations- und Kommunikationstechnologien, Datenschutzorganisationen und Schulen für mehr Aufklärung über Sicherheit und mobile Schutzmaßnahmen.

Hilfreiche Ressourcen

Das Microsoft Security and Safety Center mit Anleitungen für alle Familienmitglieder
www.microsoft.com/security/family-safety

Die Kinderecke von Windows Phone
aka.ms/Kids-Corner

Das Family Online Safety Institute
www.fosi.org

Die Koalition britischer Mobilfunkanbieter fordert soziale Verantwortung in der Mobilfunkbranche
www.mobilebroadbandgroup.co.uk

National Cyber Security Alliance

Die wichtigsten Punkte im Überblick

- Regierungen, Strafverfolgungsbehörden, Unternehmen und gemeinnützige Organisationen sind gemeinsam verantwortlich für mehr Sicherheit und Schutz im Internet.
- Seit zehn Jahren ist der Oktober in den USA der Monat der nationalen Cyber-Sicherheit (National Cyber Security Awareness Month, NCSAM). Er soll die Bevölkerung daran erinnern, das Internet sicher und verantwortlich zu nutzen.
- Wir sind Gründungsmitglied der National Cyber Security Alliance (NCSA) und der größte Sponsor des NCSAM, der mittlerweile auch in Kanada und einigen europäischen Ländern zum Monat der nationalen Cyber-Sicherheit geworden ist. Wir wünschen uns viele weitere Länder, die den Oktober zum Cyber-Sicherheits-Monat erklären und damit das Bewusstsein der Anwender für das Thema Internetsicherheit schärfen.

HINTERGRUND

Mit vielen anderen IT-Unternehmen sind wir der Meinung, dass die Onlinesicherheit von Anwendern und Familien am besten durch die Zusammenarbeit von Regierungen, Unternehmen, Strafverfolgungsbehörden und gemeinnützigen Organisationen gewährleistet werden kann.

Die National Cyber Security Alliance (NCSA) ist ein gutes Beispiel für eine solche erfolgreiche Partnerschaft. Ihr gehören das amerikanische Heimatschutzministerium, Unternehmen und gemeinnützige Organisationen an. Als Gründungsmitglied haben wir seit dem Jahr 2001 eine führende Rolle in der NCSA inne.

Der Monat der nationalen Cyber-Sicherheit in den USA ist ein Projekt der NCSA. 31 Tage lang wird die Öffentlichkeit auf Onlinerisiken hingewiesen, und Anwender werden individuell aufgeklärt, wie sie solche Risiken vermeiden. Unser Beitrag dabei sind Untersuchungen, Ratschläge für Anwender, Anleitungen für mehr Onlinesicherheit und -schutz sowie die Teilnahme an speziellen Foren und Veranstaltungen.

Im Oktober 2013 feiert der NCSAM den zehnten Jahrestag. Wir werden dann mit Kanada und acht Mitgliedsstaaten der Europäischen Union neue Teilnehmer begrüßen. Bereits 2012 haben die EU-Staaten Großbritannien, Luxemburg, Norwegen, Portugal, Rumänien, Slowenien, Spanien und die Tschechische Republik einen europäischen Monat der Cyber-Sicherheit erfolgreich als Pilotaktion ausgerufen.

Ein wichtiger Beitrag der NCSA und ein gutes Beispiel für die öffentlich-private Zusammenarbeit ist die Unterzeichnung der Kampagne STOP. THINK. CONNECT. im Oktober 2012, die Anwender für das Thema sensibilisiert und sie darüber aufklärt. Die klare Botschaft – erst denken, dann online gehen – ermahnt Anwender zu besonderer Vorsicht. Die Kampagne ist das Ergebnis einer beispiellosen Koalition aus 30 Unternehmen, gemeinnützigen Organisationen und Regierungsbehörden und 16 Monaten Forschungsarbeit und Tests.

DER MICROSOFT-ANSATZ

Wir verbessern die Onlinesicherheit mit einem dreistufigen Ansatz:

- **Technologische Hilfsmittel**. Wir stellen viele Werkzeuge für mehr Onlinesicherheit bereit. Hierzu gehört die kostenlose Anti-Malware-Anwendung Microsoft Security Essentials. Anwender können für ihr Microsoft-Benutzerkonto einstellen, wer ihr Profil anschauen, mit ihnen Kontakt aufnehmen und ihren veröffentlichten Inhalt kommentieren darf. Mit Microsoft Family Safety überwachen und schützen Eltern ihre Kinder im Web, und auch Xbox ermöglicht von Haus aus individuelle Sicherheitseinstellungen.
- **Aufklärung und Anleitungen**. Das Microsoft Safety and Security Center verhilft zu einer sicheren Internetnutzung. Es gibt Tipps, wie Anwender Rechner, mobile Endgeräte und Onlineidentitäten schützen, Betrugsversuchen aus dem Weg gehen und unangemessenes Verhalten erkennen, vermeiden und melden.
- **Partnerschaften**. Ein zentrales Thema für uns ist, öffentlichkeitswirksam mit Regierungen und Nichtregierungsorganisationen wie der NCSA Partnerschaften einzugehen.

STRATEGISCHE ÜBERLEGUNGEN

- Wir fordern weltweit Regierungen und Unternehmen auf, die Sicherheit im Internet durch die Unterstützung entsprechender Programme zu erhöhen. Ziel dabei ist es, die Öffentlichkeit über die Risiken aufzuklären. Ein Mittel dazu könnte die Deklaration des Oktobers als Monat der nationalen Cyber-Sicherheit oder die Teilnahme an der Kampagne STOP. THINK. CONNECT. sein.
- Die Kooperation aller Beteiligten ist aus unserer Sicht der erfolgversprechendste Weg, um die Internetrisiken zu minimieren. Dabei müssen ausgewogene Regelungen genug Raum lassen für die Weiterentwicklung und Einbindung innovativer Schutztechnologien und Lösungen.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center
www.microsoft.com/security

National Cyber Security Alliance
www.staysafeonline.org

Allianz für Cyber-Sicherheit
www.allianz-fuer-cybersicherheit.de

Microsoft-Onlinesicherheit - Aktualisierung für Facebook
www.facebook.com/SaferOnline

STOP. THINK. CONNECT. Tipps und Anleitungen für mehr Onlinesicherheit
www.stopthinkconnect.org

Onlinemobbing

Die wichtigsten Punkte im Überblick

- Onlinemobbing ist ein weitverbreitetes Problem, das bei den jugendlichen Opfern oft psychische und physische Schäden verursacht, die Selbstachtung zerstört und massive schulische Probleme nach sich zieht.
- Unternehmen, Regierungen, Lehrkräfte und andere Gruppen müssen gemeinsam gegen Onlinemobbing ankämpfen. Hierfür sind kombinierte Maßnahmen aus Aufklärung, Strafverfolgung, Vorgabe von Richtlinien und Nutzung technologischer Hilfsmittel nötig.
- Regierungen kommt dabei eine elementare Bedeutung zu. Sie müssen Onlineverunglimpfungen und -bedrohungen gesetzlich unterbinden und unter Strafe stellen. Die Gesetze müssen im Internet die notwendige Sicherheit bei gleichzeitig weitgehender Meinungsfreiheit gewährleisten.

HINTERGRUND

Das Mobbing unter Jugendlichen ist seit Jahren ein sehr ernstes Problem. Mit der Internettechnologie hat es aber eine ganz neue Form angenommen: Onlinemobbing oder auch Cyber-Mobbing genannt. Das amerikanische Cyberbullying Research Center definiert Onlinemobbing als „vorsätzlichen und wiederholt mit Rechnern, Mobiltelefonen und anderen elektronischen Geräten ausgeführten Psychoterror". Onlinemobbing kann vom Hänseln über bösartige Sticheleien und Schikanen bis hin zu Grausamkeiten alles bedeuten, mit dem ein Mensch einen anderen Menschen absichtlich verletzten will.

Jugendliche, die Opfer von Onlinemobbing werden, leiden oft unter massiven psychischen Störungen. Eine Untersuchung des Cyberbullying Research Center[1] ergab, dass „zwischen Cyber-Mobbing und geringer Selbstachtung, familiären und schulischen Problemen, Gewalttätigkeiten gegen Mitschüler und strafbaren Handlungen ein direkter Zusammenhang besteht".

Schätzungen über das Ausmaß von Cyber-Mobbing sind sehr ungenau – sie gehen davon aus, dass 10 bis 40 Prozent aller Jugendlichen in den EU-Mitgliedsstaaten, in den USA und in Australien schon mindestens einmal Opfer von Cyber-Mobbing waren. Nach einer Umfrage, die wir 2012 in 25 Ländern durchführten, haben 54 Prozent der Kinder zwischen 8 und 17 Jahren Angst vor Cyber-Mobbing.

Um diese große Gefahr zu bannen, müssen Technologieanbieter und IT-Unternehmen mit Regierungen, Branchenverbänden und anderen Organisationen eng zusammenarbeiten. Gute Beispiele für den gemeinsamen Kampf gegen Onlinemobbing sind GetNetWise in den USA und Insafe in der EU.

[1] *Cyber-Mobbing erkennen, vermeiden und bekämpfen* **www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf**

DER MICROSOFT-ANSATZ

- Wir setzen klare Richtlinien gegen Missbrauch und Verunglimpfungen mit unseren Onlinediensten wie Xbox LIVE um. Wir schließen rigoros die Benutzerkonten der Anwender, die unsere Dienste missbrauchen. Schwerwiegende Fälle übermitteln wir an die Strafverfolgungsbehörden.
- Wir stellen Sicherheitswerkzeuge wie Family Safety zur Verfügung, mit denen Eltern die Internetnutzung ihrer Kinder besser überwachen und kontrollieren können. Dazu gehört auch die Möglichkeit, unerwünschte Kontakte zu blockieren.
- Wir arbeiten weltweit mit Regierungen, Strafverfolgungsbehörden, Lehrkräften, Kinderschutzorganisationen und anderen zusammen, um Kindern eine Onlineumgebung mit mehr Sicherheit zu bieten. Wir überprüfen dabei Onlinedienste auf Missbrauchshinweise, stellen Sicherheitswerkzeuge zur Verfügung und leisten Aufklärungsarbeit.
- Wir entwickeln Aufklärungsprogramme und Lehrmaterialien, mit denen Schulen, Eltern und Erziehungsberechtigte jungen Menschen beibringen, wie sie sich gegen Onlinemobbing wehren.

STRATEGISCHE ÜBERLEGUNGEN

- Regierungen kommt eine elementare Bedeutung im Kampf gegen Onlineverunglimpfungen und -bedrohungen zu. Sie müssen diese gesetzlich unterbinden und unter Strafe stellen. Die Gesetze müssen im Internet die notwendige Sicherheit bei gleichzeitig weitgehender Meinungsfreiheit gewährleisten.
- Wir unterstützen eine Gesetzgebung mit ausreichender Rechtssicherheit für Unternehmen, die sich um angemessenes Verhalten der Anwender und angemessene Inhalte im Internet bemühen und deswegen nicht zusätzlich in die Verantwortung genommen werden. Beispiele hierfür sind Section 230 des U.S. Communications Decency Act und die Direktive 2000/31/EC der Europäischen Union.
- Wir fördern an Grund- und Hauptschulen die Aufklärung über Cyber-Mobbing als Teil eines umfassenden Lehrplans über Onlinesicherheit.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center schützt mit Materialien Jugendliche vor Onlinerisiken
www.microsoft.com/security/resources/young-people.aspx

Ein umfassendes Verzeichnis mit Kontrollwerkzeugen für Eltern und Sicherheitsinformationen
www.getnetwise.org

Das Cyberbullying Research Center
www.cyberbullying.us

Aufklärung über Onlinesicherheit – die Site entstand aus einer Kooperation mit der EU
www.saferinternet.org

Eine Übersicht über Onlineressourcen gegen Internetmobbing in Großbritannien
www.bullying.co.uk

Die kostenlose Microsoft-Anwendung Family Safety
aka.ms/Family-Safety

Onlinereputation

Die wichtigsten Punkte im Überblick

- Den eigenen Ruf online zu wahren ist sehr wichtig, weil er das Leben eines Menschen auf vielerlei Art sehr stark beeinflusst. Berufliche Aussichten, Freundschaften sowie Universitäts- und Schulzulassungen stehen dabei auf dem Spiel.
- Der Schutz von Kunden und das Bewahren ihres Rufs ist vor allem die Aufgabe von Unternehmen. Sie müssen durch entsprechende Aufklärungsmaßnahmen und Anleitungen sowie mit klaren Vorgaben dafür sorgen, dass Kunden ihre Informationen besser verwalten.
- Regierungen sollten mit ausgewogenen Gesetzen und Richtlinien den Onlineruf ihrer Bürger schützen, ohne dabei das Recht auf freie Meinungsäußerung einzuschränken.

HINTERGRUND

Rund um die Welt verbringen wir immer mehr Zeit unseres Lebens online. Viele Menschen präsentieren sich dort, verbringen Zeit mit Freunden, lernen oder suchen Arbeit oder einen Lebenspartner. Eine Umfrage[1] aus dem Jahr 2010 ergab, dass in Großbritannien 19 Prozent und in den USA 17 Prozent aller Ehen online angebahnt wurden. Seit 2010 nutzen fast drei Viertel aller Arbeitssuchenden das Internet, um eine geeignete Arbeit zu finden.

Weitere Untersuchungen zeigen, wie sich personenbezogene Onlineveröffentlichungen für Anwender auswirken, wenn sie Arbeit oder nach einer Lehranstalt suchen. Mit einer eigenen Studie[2], die wir 2009 durchführten, fanden wir heraus, dass in den USA 70 Prozent und in Großbritannien 41 Prozent aller Bewerbungen um eine Managementstelle aufgrund online entdeckter Informationen abgelehnt wurden. Eine Umfrage[3] aus dem Jahr 2012 ergab, dass bei 35 Prozent aller Zulassungsprüfungen in den USA die dafür in den Lehranstalten Verantwortlichen „Informationen entdeckten, die die Chance des Antragstellers auf seine Zulassung erheblich negativ beeinflussten".

Mit einer schnell und einfach durchgeführten Onlinesuche finden sich sehr viele persönliche Informationen über einen Anwender. Daher nimmt die Besorgnis über einen einwandfreien Onlineruf zu, insbesondere auch über den individuellen digitalen Fußabdruck. Dabei hinterlassen Anwender bei allen Onlineaktivitäten Spuren, also wenn sie Blogeinträge und Kommentare veröffentlichen, Bilder hochladen, online spielen und soziale Netze nutzen. Ein positiver digitaler Fußabdruck erhöht die Chancen eines Anwenders etwa auf eine Einstellung. Im Gegensatz dazu steht ein negativer digitaler Fußabdruck, der mit unangemessenen Bildern oder verletzenden Kommentaren oft jede Chance zunichtemacht.

Eine weitere Umfrage[4], die wir 2011 mit 5000 erwachsenen und jugendlichen Teilnehmern in Deutschland, Irland, Kanada, Spanien und den USA durchführten, ergab, dass zwar 90 Prozent der Befragten ihr Onlineprofil auf irgendeine Art und Weise verwalten, aber nur 44 Prozent an die langfristigen Folgen der Onlineaktivitäten für ihren Onlineruf denken.

[1] *Jüngste Trends: Online-Dating*
cp.match.com/cppp/media/CMB_Study.pdf

[2] *Der Onlineruf in der vernetzten Welt, 2009*
www.microsoft.com/security/resources/research.aspx#reputation

[3] *Kaplan-Testvorbereitung 2010, eine Umfrage unter College-Zulassungsstellen, 2012*
press.kaptest.com/research-and-surveys/kaplan-test-preps-2012-survey-of-college-admissions-officers

[4] *Die Verwaltung des Onlinerufs: Eltern und 8- bis 17-jährige Kinder, 2011*
www.microsoft.com/security/resources/research.aspx#onlinerep

DER MICROSOFT-ANSATZ

Aufklärung und Anleitung. Das Microsoft Safety and Security Center verhilft zu einer sicheren Internetnutzung. Es gibt Tipps, wie Anwender ihren Onlineruf schützen und unangemessenes Verhalten erkennen, vermeiden und melden.

Richtlinien. Die Microsoft-Vorgaben für korrektes Verhalten erlauben es Anwendern nicht, „Inhalte hochzuladen, zu veröffentlichen, zu übertragen, auszutauschen, zu verteilen oder die Verteilung zu ermöglichen, wenn dadurch Anwender oder Anwendergruppen diffamiert, betrogen, erniedrigt, verletzt oder bedroht werden". Unser Services Agreement besagt, dass „wir jeden Inhalt ohne Rücksprache mit der dafür verantwortlichen Person entfernen, wenn er eine oder mehrere Vorgaben des Services Agreements verletzt".

Technologische Hilfsmittel. Wir helfen Anwendern mit vielen in unsere Produkte und Dienste integrierten Funktionen, ihren digitalen Fußabdruck zu verwalten. Das Personal Data Dashboard ist die zentrale Anlaufstelle mit allen persönlichen Informationen, die bei der Nutzung ausgewählter Microsoft-Produkte und -Dienste anfallen. Anwender bestimmen damit, wie ihre Daten angezeigt werden. Mit Xbox LIVE verwalten Anwender ihre Informationen komplett selbst.

STRATEGISCHE ÜBERLEGUNGEN

- Regierungen müssen mit ausgewogenen Gesetzen und Richtlinien den Onlineruf ihrer Bürger schützen, ohne dabei das Recht auf freie Meinungsäußerung einzuschränken.
- Unternehmen müssen aufklären und anleiten sowie mit klaren Vorgaben dafür sorgen, dass Kunden ihre Informationen besser schützen, pflegen und verwalten.
- Wir unterstützen eine Gesetzgebung mit ausreichender Rechtssicherheit für Unternehmen, die sich um angemessenes Verhalten der Anwender und angemessene Inhalte im Internet bemühen und deswegen nicht zusätzlich in die Verantwortung genommen werden. Beispiele hierfür sind Section 230 des U.S. Communications Decency Act und die Direktive 2000/31/EC der Europäischen Union.

Hilfreiche Ressourcen

Der Microsoft-Verhaltenskodex
aka.ms/code-of-conduct

Das Microsoft Services Agreement
aka.ms/services-agreement

Das Microsoft Personal Data Dashboard
aka.ms/dashboard

Das Microsoft Safety and Security Center: Übernehmen Sie Verantwortung für Ihren Onlineruf
aka.ms/reputation

Aufklärung über Onlinesicherheit

Die wichtigsten Punkte im Überblick

- Das Internet eignet sich außergewöhnlich gut für die Wissensvermittlung und das Lernen. Es setzt Jugendliche dabei aber auch einem hohen Risiko aus, weil es unangemessene Inhalte enthält, Onlinemobbing erlaubt, die Privatsphäre ungenügend schützt und den Diebstahl personenbezogener Daten ermöglicht. Umso wichtiger ist eine umfassende Aufklärung über die Onlinesicherheit, mit der sich diese Risiken verringern beziehungsweise vermeiden lassen.

- Das Thema Onlinesicherheit sollte ein integraler Bestandteil der Lehrpläne aller Schulen werden, der Schülern und Studenten das hierfür nötige digitale Fachwissen vermittelt. Dabei sollte auch der Onlineschutz berücksichtigt und das moralisch einwandfreie Onlineverhalten gelehrt werden.

- Wir fördern eine umfassende schulische Aufklärung und die Übernahme des Themas Onlinesicherheit in Lehrpläne. Regierungen sollten Schulen zur Aufklärung ihrer Schüler über die Onlinesicherheit verpflichten. Dabei müssen selbstverständlich regionale Besonderheiten hinsichtlich der Lehrpläne berücksichtigt werden.

HINTERGRUND

Das Internet ist ein außergewöhnliches Hilfsmittel, mit dem Kinder besser lernen und die Welt entdecken können. Viele Eltern und Lehrkräfte wissen, dass eine Voraussetzung für diese Art der Internetnutzung ist, dass ihre Kinder beziehungsweise Schüler und Studenten gute digitale Bürger sind. Der Zugang zum Internet bietet Kindern viele Vorteile, setzt sie aber andererseits auch einem hohen Risiko aus. Indem sie etwa unangemessene Inhalte sehen, mit Pädophilen, Fremden und Kriminellen in Kontakt kommen oder ihre Privatsphäre preisgeben.

Zur Erziehung Jugendlicher zu guten digitalen Bürgern gehört es, ihnen diese Risiken zu verdeutlichen und ihnen zu zeigen, wie sie diese vermeiden. Weiterhin müssen Jugendliche wissen, warum ein positives Onlineverhalten mit Respekt vor geistigem Eigentum und der Einhaltung bestimmter moralischer und ethischer Verhaltensregeln so wichtig ist.

Digitales Bürgertum wird normalerweise definiert als „Verhaltensregeln unter Berücksichtigung der verwendeten Technologie". Aber digitales Bürgertum bedeutet mehr als nur die Einhaltung sozialer Normen. Es geht darum, Jugendliche auf das Leben in und mit einer technologiegetriebenen Welt vorzubereiten. Als digitale Bürger müssen sie ein Gespür für Eigentum und persönliche Verantwortung entwickeln, damit sie in der Onlinewelt selbstverantwortlich moralisch einwandfreie Entscheidungen treffen können.

Viele Schulen klären ihre Schüler nicht über Onlinesicherheit auf, oft weil dies kein Thema des Lehrplans ist. Obwohl viele Sicherheitsexperten und -organisationen genau dies schon lange fordern. Denn für sie ist die Aufklärung an Schulen eines der besten Mittel, um Kinder auf die Onlinegefahren aufmerksam zu machen und davor zu schützen. Eine solche schulische Aufklärung muss dabei auf die folgenden Themen eingehen:

- **Onlinesicherheit**. Dabei lernen Kinder mehr über das Verhalten, das bereits eine grundsätzliche Onlinesicherheit schafft und mit dem sie potenzielle Gefahren vermeiden. Sie lernen mehr über die Bedrohungen, und wie sie Probleme und Verdachtsmomente an welche zuständige Behörde weiterleiten.
- **Onlineschutz**. Kinder erfahren, wie sie ihre Benutzerkonten, ihre persönlichen Daten und ihre Onlineprivatsphäre schützen. Sie lernen, wie wichtig die Sicherheit und die Geheimhaltung von Kennwörtern sind und warum nur regelmäßig aktualisierte Rechner und Endgeräte zuverlässig Viren, Spam-E-Mails und Phishing-Attacken verhindern.
- **Onlinemoral**. Kinder werden darüber aufgeklärt, dass es auch in der Onlinewelt gute und schlechte Bürger gibt und dass es dort Risiken gibt wie Onlinemobbing und den Diebstahl geistigen

Eigentums, von Geld sowie persönlichen Daten. Mit geeignete Ressourcen müssen Kinder lernen, mit Onlinemobbing oder Belästigungen jeder Art umzugehen, und sie müssen erfahren, wie ihre Onlineveröffentlichungen und -kommentare auf andere wirken und welche persönlichen Konsequenzen bestimmte Aktionen nach sich ziehen.

DER MICROSOFT-ANSATZ

- Mit technologischen Hilfsmitteln, Aufklärungsarbeit und Anleitungen erhöhen wir die Onlinesicherheit für Kinder. Wir entwickeln zuverlässige interne Richtlinien für den risikolosen Umgang mit Inhalten und zur Vermeidung von Onlinemissbrauch. Durch Partnerschaften mit Regierungen, Unternehmen, Strafverfolgungsbehörden und anderen Beteiligten entsteht eine vertrauenswürdige Rechnerumgebung, die allen Anwendern mehr Sicherheit und Schutz bietet.
- Das Microsoft Safety and Security Center enthält altersbezogene Anleitungen für die Internetnutzung. Dazu gehören Hinweise, mit denen Eltern ihren Kindern erklären, welche Inhalte sie anschauen und mit anderen teilen dürfen. Die Webseite gibt zudem Tipps, wie sich Onlinebeschimpfungen verhindern lassen, wie sich die Sicherheit in sozialen Netzen erhöhen lässt, wie mobile Endgeräte besser geschützt werden, auf was bei Onlinespielen besonders zu achten ist und wie unangemessenes Verhalten vermieden, verhindert und gemeldet werden kann.

STRATEGISCHE ÜBERLEGUNGEN

- **Onlinesicherheit als Bestandteil schulischer Lehrpläne**. Viele Behörden und Organisationen fordern schon seit Langem, dass Onlinesicherheit als integraler Bestandteil von Lehrplänen an Schulen unterrichtet wird, weil nur so das erforderliche technische Wissen den Schülern vermittelt werden kann. Gerade weil an vielen Schulen in den Klassenzimmern die Technologie vorhanden ist, ist es aus unserer Sicht sehr wichtig, dort im Rahmen der Lehrpläne das Fach Onlinesicherheit einzuführen.
- **Onlinesicherheit als Bestandteil der Lehreraus- und fortbildung**. Genauso wie Schüler und Studenten müssen auch Lehrer über Onlinesicherheit Bescheid wissen. Sie benötigen ebenfalls Anleitungen und Fachwissen, um mit den technischen Weiterentwicklungen Schritt zu halten. Im gleichen Maße, wie Lehrer Trainings über den effizienten Einsatz der Technologie in den Klassenzimmern erhalten, müssen sie die im Internet lauernden Gefahren kennenlernen. Sie müssen zudem lernen, Situationen zu erkennen, in denen Schüler besonderen Onlinerisiken ausgesetzt sind, und sie müssen Schüler anleiten, sich im Web nach allgemein anerkannten moralischen Regeln zu verhalten.
- **Ein Onlinezugangsverbot ersetzt nicht die Aufklärung**. Die Kontrolle des Internetzugangs von Kindern mag in einigen Fällen berechtigt sein, etwa in Bereichen, in denen auch in der realen Welt Altersbeschränkungen gelten – wie Spielhallen und pornografische Angebote. Viele Sicherheitsexperten sind aber überzeugt davon, dass Zugangsverbote alleine das Problem nicht lösen. Für sie ist eine umfassende Aufklärung der Schlüssel für mehr Onlinesicherheit.
- **Aufklärung über Onlinesicherheit ist auch Sache von Unternehmen**. Viele Angestellte von IT-Unternehmen haben sich bereit erklärt, freiwillig die Programme für mehr Onlinesicherheit vorzustellen und bei deren Umsetzung zu helfen. In Australien und Großbritannien nehmen unsere Mitarbeiter gemeinsam mit Vertretern von Strafverfolgungsbehörden an einem Programm namens ThinkUKnow teil. Sie klären dabei über Onlinesicherheit auf und stellen Eltern, Lehrern und Kindern dafür geeignete Ressourcen zur Verfügung. Insgesamt beteiligen wir uns mit 26 europäischen Niederlassungen an derartigen Aufklärungsmaßnahmen und erreichen damit mehr als 90 000 Lehrer, Eltern und Schüler.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center mit altersbezogenen Tipps für die Internetnutzung
www.microsoft.com/security

Das Microsoft-Toolkit:
Digital Citizenship in Action
aka.ms/DC-Toolkit

Das Programm der Europäischen Kommission für mehr Internet-Sicherheit
aka.ms/EC-SaferInternet

Sicherheitswerkzeuge und -material der National Cyber Security Alliance
www.staysafeonline.org/teach-online-safety

Sicheres Spielen online

Die wichtigsten Punkte im Überblick

- Die Spielwelt ist besonders für Jugendliche sehr reizvoll. Dennoch enthalten einige Videospiele Inhalte, die sich nur für Erwachsene eignen. Das wirft viele Fragen auf. Unter anderem danach, wie Eltern ihre Kinder am besten davor schützen.

- Mit technologischen Hilfsmitteln, Aufklärungsarbeit und Anleitungen erhöhen wir die Onlinesicherheit für Kinder. Wir entwickeln Richtlinien und Methoden für den risikolosen Umgang mit Inhalten und zur Vermeidung von Onlinemissbrauch. Durch Partnerschaften mit Regierungen, Unternehmen, Strafverfolgungsbehörden und anderen Beteiligten entsteht eine vertrauenswürdige Rechnerumgebung, die allen Anwendern mehr Sicherheit und Schutz bietet.

- Um Risiken durch Onlinespiele zu vermeiden, müssen Familien umfassend darüber aufgeklärt werden und helfen, diese Gefährdungen zu verhindern. Zusätzlich hilfreich sind freiwillige Bewertungssysteme von Unternehmen und Organisationen wie ESRB, PEGI und CERO.

HINTERGRUND

Video- und Onlinespiele sprechen viele verschiedene Zielgruppen an. Ein generelles Problem dabei ist, wie bei allen Unterhaltungsangeboten, dass sich Inhalte nicht für alle Konsumenten gleichermaßen eignen oder von ihnen gewünscht sind. Viele Menschen haben große Bedenken wegen potenziell jugendgefährdender Inhalte von Spielen. Einige Regierungen haben darauf bereits reagiert. Sie haben den Zugriff auf bestimmte Videospiele mit pornografischen oder gewaltverherrlichenden Inhalten unterdrückt und deren Verkauf verboten.

Die Spieleindustrie hat eigene Maßnahmen umgesetzt und auf freiwilliger Basis Bewertungssysteme von Organisationen verschiedener Länder übernommen. Dazu gehören unter anderem in den USA das Entertainment Software Ratings Board (ESRB), in der Europäischen Union die Pan European Game Information (PEGI) und in Japan die Computer Entertainment Rating Organization (CERO).

Viele Händler veröffentlichen die Spielebeschreibungen dieser anerkannten Bewertungssysteme und bieten Eltern damit eine gute Entscheidungsgrundlage für den Erwerb eines Videospiels. Mehr als 30 EU-Staaten verwenden PEGI, und laut einer Umfrage aus dem Jahr 2008 kennen und berücksichtigen 93 Prozent der europäischen Konsumenten die PEGI-Klassifizierung. Nach einer Umfrage aus dem Jahr 2011 prüfen in den USA 65 Prozent der Eltern „vor dem Erwerb grundsätzlich die Bewertung eines Spiels“. Die amerikanische Federal Trade Commission (FTC) fand mit anonymen Einkäufen 2011 heraus, dass 87 Prozent der amerikanischen Händler den Verkauf eines nur für Erwachsene freigegebenen Spiels an Minderjährige verweigerten.

Unabhängig davon, von welchem Hersteller Familien Unterhaltungsprodukte erwerben oder ob Kinder Spiele nutzen, Videos anschauen, Video-Chats verwenden oder anderweitige Onlineinteraktionen durchführen, ist eines wichtig: Eltern müssen die sich ständig ändernde digitale Welt verstehen und erkennen, warum sie Kinder fasziniert und ihre Aufmerksamkeit auf sich zieht. Das gilt gleichermaßen auch für die Bewertungssysteme für Videospiele, Filme und Fernsehsendungen. Zudem müssen Eltern entscheiden, ob sie hilfreiche Anwendungen wie Family Safety Settings für einen besseren Schutz ihrer Kinder einsetzen möchten. Damit schränken sie den Internetzugang ein, verhindern den Zugriff auf bestimmte Inhalte und legen fest, wie lange Kinder ein Spiel nutzen dürfen.

DER MICROSOFT-ANSATZ

- **Technische Hilfsmittel**. Wir waren eines der ersten Unternehmen, das mit den Family Settings der Xbox eine auf Bewertungen basierende Kontrollmöglichkeit für Eltern eingeführt hat.
  - » Die Sicherheitseinstellungen der Konsole für die Xbox 360 verwenden Bewertungen für Spiele, Filme und Fernsehsendungen. Einstellungsänderungen sind nur mit einem Kennwort möglich. Der Family Timer legt den Zeitraum fest, in dem das Spielen mit der Konsole möglich ist.
  - » Mit den Einstellungen der Onlinesicherheit für Xbox LIVE erstellen Eltern für jedes Kind ein individuelles Profil, das dem Alter und der Reife des Kindes entspricht. Sie legen damit fest, an welchen Aktionen ein Kind teilnehmen darf – wie etwa an Spielen mit mehreren Spielern gleichzeitig oder an Video-Chats und dem Austausch von Text- oder Sprachnachrichten. Sie regeln damit die Kommunikationsmöglichkeiten des Kindes, und wer sein Profil oder seine Freundesliste sehen darf.
- **Partnerschaften mit Sicherheitsorganisationen, Unternehmen und Regierungen**. Mit vielen weiteren Organisationen wie unter anderem den Boys and Girls Clubs of America und dem National Center for Missing and Exploited Children haben wir im Jahr 2009 eine nationale Kampagne mit dem Namen Get Game Smart gestartet. Damit fordern wir Eltern auf, mit ihren Kindern über Videospiele und digitale Medien zu diskutieren.
- **Aufklärung und Hilfe für Konsumenten**. Wir hätten unsere Arbeit nicht vollständig getan, wenn Kunden nicht wüssten, wie sie die ihnen zur Verfügung gestellten Technologien, Werkzeuge und Ressourcen einsetzen sollten. Es ist sehr wichtig, Eltern und Familien fortlaufend über die bereitgestellten Ressourcen zu informieren. Wir tun dies mit dem Microsoft Safety and Security Center und auf der Get Game Smart-Website.
- **Interne Richtlinien und Methoden**. Wir erhöhen die Sicherheit mit unternehmensweiten Richtlinien, Standardvorgaben und Prozeduren, die für alle Produkte gelten, die eine Verbindung ins Internet nutzen. Wir haben einen Verhaltenskodex für Anwender unserer Spieledienste entwickelt, und wir prüfen Inhalte und Interaktionen darauf, ob sie Missbrauch und illegale Aktionen fördern oder unangemessenes Material enthalten. Viele unserer Dienste enthalten einen Link, um Missbrauch direkt an unsere Website www.microsoft.com/reportabuse weiterzugeben.

STRATEGISCHE ÜBERLEGUNGEN

- Wir unterstützen ein leistungsfähiges Ökosystem, in dem Spieleentwickler und -anbieter Produkte und Inhalte für Anwender jeden Alters anbieten. Gleichzeitig möchten wir Eltern das nötige Wissen vermitteln und Werkzeuge bereitstellen, mit denen sie fundierte Entscheidungen über die Qualität und Eignung interaktiver Spiele und Anwendungen für ihre Kinder treffen.
- Die Kombination von freiwilligen Bewertungssystemen von Unternehmen und Organisationen mit familiärer Aufklärung und der Einbindung von Eltern verspricht am meisten Erfolg, um die Risiken von Spielen und anderen Onlineunterhaltungsangeboten zu verringern.
- Unser Ziel sind bessere Gesetze zum Schutz von Kindesmissbrauch. Dafür arbeiten wir mit dem International Centre for Missing and Exploited Children, Interpol und vielen weiteren Organisationen zusammen und ermutigen Regierungen, schärfere Gesetze gegen den Besitz und die Verbreitung von kinderpornografischen Bildern zu erlassen.

Hilfreiche Ressourcen

Sicherheitsressourcen für Videospiele und Onlinemedien
www.GetGameSmart.com

Das Microsoft Safety and Security Center mit altersbezogenen Tipps für die Internetnutzung
www.microsoft.com/security

Das International Centre for Missing and Exploited Children
www.icmec.org

Das Entertainment Software Ratings Board
www.esrb.org

PEGI – Pan European Game Information
www.pegi.info

CERO – Die Computer Entertainment Rating Organization
www.cero.gr.jp

Mehr Sicherheit in sozialen Netzen

Die wichtigsten Punkte im Überblick

- Soziale Netze erfreuen sich immer größerer Beliebtheit. Sie bieten zwar großartige Möglichkeiten, bergen aber auch Risiken. So ist die Gefahr hoch, dort bösartigen Anwendungen ausgeliefert zu sein, den Schutz der Privatsphäre zu verlieren oder Belästigungen, Onlinemobbing oder einer Schädigung des Onlinerufs ausgesetzt zu sein.

- Mit technologischen Hilfsmitteln, Aufklärungsarbeit und Anleitungen erhöhen wir die Sicherheit in sozialen Netzen. Wir entwickeln Richtlinien und Methoden für den risikolosen Umgang mit Inhalten und zur Vermeidung von Onlinemissbrauch, und wir gehen dafür Partnerschaften mit Regierungen, Unternehmen, Strafverfolgungsbehörden und anderen Beteiligten ein.

- Regierungen müssen auch weiterhin mit Unternehmen zusammenarbeiten, um die Vorteile sozialer Netze zu bewahren und die Risiken bei deren Nutzung durch den Einsatz bewährter Methoden und Anleitungen aus der IT-Branche zu minimieren.

HINTERGRUND

In den zurückliegenden Jahren hat sich das Internet gravierend verändert. Anstatt statischer Webseiten sind jetzt fast nur noch dynamische Webseiten vorhanden, und eine Vielzahl interaktiver Communitys sind fester Bestandteil der Webkultur geworden. Dort vernetzen sich immer mehr Menschen per Facebook oder Pinterest mit Freunden oder per LinkedIn mit Kollegen. Sie entdecken virtuelle Welten wie Second Life, veröffentlichen Kommentare mit Twitter oder spielen online mit Xbox LIVE: Für Kinder gibt es sogar eigene Netz wie Webkinz oder Club Penguin.

Die beliebtesten sozialen Netze haben eine halbe Milliarde oder mehr Teilnehmer. Leider wirkt diese Attraktivität aber auch auf viele Kriminelle anziehend. Hacker, Spammer, Identitätsdiebe und andere Verbrecher benutzen die von den Teilnehmern veröffentlichten eigenen Informationen für Attacken, Mobbing und Betrügereien. Zudem geben viele Anwender in sozialen Netzen Details über ihr Leben preis, die nahezu unbegrenzt lange und für ein größeres Publikum, als ihnen lieb sein kann, verfügbar sind. Und mit Konsequenzen für ihren Ruf, die sie sich oft nicht vorstellen können. Daher ist es sehr wichtig, dass Anwender die Risiken kennen und verstehen, und mit welchen Maßnahmen sie sich, ihre Informationen, ihre Privatsphäre und ihren Ruf davor schützen.

Gerade wenn es um junge Anwender geht, erzeugen soziale Netze zusätzliche Bedenken. Das gilt insbesondere dann, wenn Kinder vor dem 13ten Lebensjahr soziale Netze nutzen, die für Erwachsene gedacht sind. Diese Jugendlichen, aber auch ihre Eltern und Erziehungsberechtigten, müssen wissen, dass diese Netze möglicherweise für Kinder unangemessene Inhalte enthalten und dass viele der dort genutzten Anwenderprofile von nahezu jedem Internetnutzer eingesehen werden können. Oft verstößt es gegen die Vertragsbedingungen der sozialen Netze, wenn sich Kinder dafür registrieren, die nicht das darin vorgeschriebene Mindestalter haben. Zudem für Jugendliche, die zwar älter als 13 Jahre, aber noch nicht volljährig sind, und die ihr Alter falsch angeben, Schutzmechanismen für unter 18-Jährige eventuell nicht mehr greifen.

DER MICROSOFT-ANSATZ

Um eine digitale Welt mit mehr Sicherheit und Vertrauen zu schaffen, nutzen wir mehrere Ansätze:

- **Technologische Hilfsmittel**. Wir bieten viele Sicherheitswerkzeuge wie die kostenlose Anti-Malware-Anwendung Microsoft Security Essentials und das Personal Data Dashboard an. Das Dashboard ist eine zentrale Anlaufstelle mit allen personenbezogenen Informationen eines Anwenders, die in Verbindung mit ausgewählten Microsoft-Produkten und -Diensten anfallen. Damit kontrollieren Anwender schnell und unkompliziert, wie ihre Informationen angezeigt werden.

  Zudem haben wir Funktionen zum Schutz von Familienmitgliedern in viele unserer Produkte integriert. Dazu zählen Family Safety von Windows 8, mit dem sich die Onlineaktivitäten von Kindern überwachen und schützen lassen, die Kinderecke von Windows Phone und die Sicherheitseinstellungen der Xbox- und Xbox 360-Konsole.

- **Aufklärung und Anleitung**. Das Microsoft Safety and Security Center enthält Hinweise für die sichere Nutzung sozialer Netze. Dazu gehören spezielle Tipps für Kinder und Teenager über die Verwendung standortbezogener Angaben. Anwender finden dort zudem Ratschläge, wie sie ihren Onlineruf verwalten und wiederherstellen, wie sie Onlinebetrügereien verhindern und wie sie unangemessene Verhaltensweisen vermeiden, blockieren und melden.

- **Interne Richtlinien und Methoden**. Wir verpflichten alle Nutzer unserer Onlinedienste zur Einhaltung eines Verhaltenskodex für Anwender. Wir prüfen Inhalte und Interaktionen darauf, ob es sich um illegale Aktionen, unangemessene Materialien oder andere Missbrauchsaktionen handelt.

- **Partnerschaften**. Um eine sichere Onlineumgebung zu schaffen, bedarf es eines ganzheitlichen Ansatzes, der von Regierungen, Strafverfolgungsbehörden, Technologieanbietern und Nichtregierungsorganisationen getragen werden muss. Für uns ist es besonders wichtig, dabei gemeinsam mit Regierungen und Nichtregierungsorganisationen wie der National Cyber Security Alliance und dem Family Online Safety Institute die Öffentlichkeit einzubeziehen.

STRATEGISCHE ÜBERLEGUNGEN

- **Öffentlich-private Partnerschaften**. Die Anbieter sozialer Netze sollten gemeinsam mit Regierungen Anwender besser schützen. Sie sollten hierfür in der Industrie bewährte Methoden und Leitfäden wie etwa die Safer Social Networking Principles für die EU umsetzen. Dieses Dokument „beschreibt die Grundsätze, mit denen Anbieter von sozialen Netzen die potenziellen Gefahren für Kinder und Jugendliche minimieren, und empfiehlt viele bewährte Methoden, mit denen sich diese Grundsätze umsetzen lassen". Diese Grundsätze wurden gemeinsam von uns, Facebook, Google und 15 weiteren sozialen Netzen erarbeitet.

- **Studien durchführen und Forschungen unterstützen**. Recherchen sind sehr wichtig für die Identifikation der Risikofaktoren, die Anwender online bedrohen. Sie entlarven zudem oft Mythen, die ansonsten zu unnötigen und kostspieligen Maßnahmen führen, die keinerlei Wirkung im Kampf gegen diese Risiken zeigen. Die finanzielle Unterstützung von akademischer und privatwirtschaftlicher Forschung in diesem Bereich ist unerlässlich.

- **Aufklärung über Onlinesicherheit an Schulen**. Unserer Meinung nach muss das Thema Onlinesicherheit ein fester Bestandteil des schulischen Lehrplans werden, weil sich nur so das technologische Verständnis der Schüler und Studenten erhöhen lässt. Der modulare Aufbau sollte Cyber-Sicherheit, Cyber-Schutz und Cyber-Ethik umfassen.

Hilfreiche Ressourcen

Das Microsoft Safety and Security Center mit Anleitungen für mehr Sicherheit
www.microsoft.com/security

Die National Cyber Security Alliance
www.staysafeonline.org

Das Family Online Safety Institute
www.fosi.org

STOP. THINK. CONNECT. Tipps und Anleitungen für mehr Onlinesicherheit
www.stopthinkconnect.org

STOP. THINK. CONNECT.

Die wichtigsten Punkte im Überblick

- Das Internet stellt eine enorme Antriebskraft für Innovationen, Erziehung und weltweites wirtschaftliches Wachstum dar. Gleichzeitig wird es wie nie zuvor von ausgefeilten bösartigen Verhaltensmustern und Kriminalität bedroht.

- Wir alle, Anwender, Eltern, Schüler und Studenten, Lehrer, Regierungen, Strafverfolgungsbehörden und Unternehmen, müssen an einem Strang ziehen, und jeder muss seinen Teil dazu beitragen, dass das Internet zu einer sicheren, besser geschützten und vertrauenswürdigen Umgebung wird.

- Wir haben gemeinsam mit vielen weiteren Beteiligten STOP. THINK. CONNECT. ins Leben gerufen. Dabei handelt es sich um eine Kampagne für mehr Schutz der Rechnerumgebung und mehr Onlinesicherheit. Sie soll das Bewusstsein von Anwendern für Internetrisiken schärfen und mit strategischen Hilfen einzelnen Anwendern und Unternehmen mehr Onlinesicherheit bieten.

HINTERGRUND

Das Internet ist wohl die bemerkenswerteste Erfindung unserer Zeit. Es ermöglicht neue Arten der Zusammenarbeit, der Kommunikation, der Wissensvermittlung, des Spielens, und es sorgt für mehr Wachstum. Aber das Internet birgt auch Risiken. Zu unserem Leidwesen hat das digitale Zeitalter zu raffinierten Methoden für Lug und Betrug geführt, die weder vor Menschen und ihrem Besitz noch vor Unternehmen oder Staaten haltmachen. Die vielen Vorteile des Internets überwiegen zwar die Risiken bei Weitem. Aber es ist dennoch wichtig, Anwender und deren Eigentum zu schützen. Am besten gelingt dies, wenn Anwender über die potenziellen Gefahren Bescheid wissen, die online lauern, und wenn ihnen bei der Entwicklung geeigneter Schutzstrategien und -maßnahmen geholfen wird.

Seit Jahrzehnten ist, wie für viele andere Unternehmen auch, die Aufklärung der Anwender über die sichere Nutzung unserer Produkte und des Internets ein zentraler Bestandteil unserer Arbeit. Mit der Zeit haben sich das Bewusstsein und das Verhalten der Anwender zum Besseren geändert. So hatten etwa Anfang der 2000er Jahre die meisten privaten Rechnernutzer noch nie von Phishing-Attacken gehört, obwohl deren Konzept schon damals seit nahezu 15 Jahren bekannt war. Phishing bezeichnet eine kriminelle Methode, mit der Verbrecher mit gefälschten, täuschend echten E-Mails oder Webseiten Anwender zur Preisgabe wertvoller persönlicher Informationen verleiten.

Heute sind zum Glück die meisten Anwender aufgrund der großen öffentlichen Aufmerksamkeit für dieses Phänomen sehr vorsichtig, wenn sie dazu aufgefordert werden, einen Link in einer E-Mail anzuklicken. Sie erkennen zudem dubiose E-Mails besser, die ihnen einen Gewinn anpreisen oder sie mit einem Geschenk von jemandem locken, den sie nicht kennen. Dennoch bleibt einiges zu tun, denn Phishing ist nur eine Art von Onlinebetrug. Wir, aber auch viele andere Unternehmen und Organisationen, können immer nur individuell darauf reagieren.

Im Juni 2009 gründeten die National Cyber Security Alliance (NCSA) und die Anti-Phishing Working Group (APWG) eine Gruppe, bestehend aus 30 Vertretern von Branchenverbänden, Unternehmen und gemeinnützigen Organisationen. Deren Ziel war und ist eine Kampagne, die mit einer einfach zu verstehenden Botschaft die Aufmerksamkeit der Öffentlichkeit auf das Thema Onlinesicherheit und -schutz lenkt.

Die Forderung des amerikanischen Präsidenten nach einer nationalen Kampagne, mit der die Öffentlichkeit über die Sicherheit und den Schutz von Rechnerumgebungen aufgeklärt werden sollte, führte dazu,

dass auch das amerikanische Heimatschutzministerium und andere Regierungsbehörden an der Aktion der NCSA und APWG teilnahmen.

Gestartet wurde die Kampagne STOP. THINK. CONNECT. (STC) mit dem Start des National Cyber Security Awareness-Monats Oktober 2010. STC ist eine beispielhafte öffentlich-private Zusammenarbeit und ein wichtiger Schritt hin zu einer neuen Kultur der Onlinesicherheit. Das ist durchaus vergleichbar mit der Art und Weise, wie die Öffentlichkeit vor Jahrzehnten über den Gebrauch und die Vorteile der damals neuartigen Sicherheitsgurte in Automobilen oder über die Vermeidung von Waldbränden aufgeklärt wurde. Im Jahr 2012 erfolgte die internationale Adaption der Kampagne: STOP. THINK. CONNECT. wurde von Kanada, der Organisation Amerikanischer Staaten und einigen Mitgliedern der Europäischen Union übernommen. Europa wird ab 2014 den Oktober als Monat der Cyber-Sicherheit einführen.

DER MICROSOFT-ANSATZ

Mit einem dreistufigen Ansatz helfen wir dabei, eine sichere und vertrauenswürdigere Rechnerumgebung aufzubauen:

- **Technologische Hilfsmittel**. Wir stellen viele Sicherheitswerkzeuge wie die kostenlose Anti-Malware-Anwendung Microsoft Security Essentials zur Verfügung. Anwender mit Microsoft-Benutzerkonten können zudem festlegen, wer ihr Profil ansehen und Kontakt mit ihnen aufnehmen darf und wer ihre Veröffentlichungen kommentieren und die Kommentare darüber ansehen darf. Mit Family Safety lassen sich die Onlineaktivitäten von Kindern überwachen und schützen, und Xbox 360 erhöht den Schutz mit den Sicherheitseinstellungen für die Konsole.
- **Aufklärung und Anleitung**. Das Microsoft Safety and Security Center enthält Tipps für die sichere Internetnutzung. Anwender erhalten dort Hinweise, wie sie ihre Rechner, mobilen Endgeräte und ihren Onlineruf besser schützen, Betrugsversuchen begegnen sowie unangemessenes Verhalten vermeiden, blockieren und melden.
- **Partnerschaften**. Um eine sichere Onlineumgebung zu schaffen, bedarf es eines ganzheitlichen Ansatzes von Regierungen, Strafverfolgungsbehörden, Technologieanbietern und Nichtregierungsorganisationen. Für uns ist es besonders wichtig, gemeinsam mit Regierungen und Nichtregierungsorganisationen wie der National Cyber Security Alliance die Öffentlichkeit einzubeziehen.

STRATEGISCHE ÜBERLEGUNGEN

- Wir fordern weltweit Regierungen auf, an STOP. THINK. CONNECT. teilzunehmen und die Arbeit der Gruppe zu fördern und zu unterstützen.
- Die Zusammenarbeit aller Beteiligten verspricht unserer Meinung nach am meisten Erfolg im Kampf gegen Internetbedrohungen. Gemeinsam mit bestens aufeinander abgestimmten, ausgewogenen Gesetzen und Regelungen muss dabei allerdings genug Raum für Innovationen bleiben, mit denen flexibel auf Onlinerisiken reagiert werden kann.

Hilfreiche Ressourcen

STOP. THINK. CONNECT. Tipps und Anleitungen für mehr Onlinesicherheit
www.stopthinkconnect.org

Das Microsoft Safety and Security Center
www.microsoft.com/security

Microsoft-Onlinesicherheit – Aktualisierung für Facebook
www.facebook.com/SaferOnline

Microsoft und das Thema Onlinesicherheit bei Twitter
twitter.com/Safer_Online

Februar 2013

Barrierefreiheit

Die wichtigsten Punkte im Überblick

- Barrierefreie Rechnertechnologien erleichtern Anwendern die Rechnernutzung durch besseres Hören und Sehen sowie mit einer individuellen Anpassung des Rechners an die persönlichen Anforderungen und Wünsche. Für viele Anwender wird durch die Barrierefreiheit ein Rechner erst nutzbar.

- Wir entwickeln schon seit Langem innovative Lösungen für mehr Barrierefreiheit. Wir konzentrieren uns dabei auf die vier Bereiche Barrierefreiheit von Produkten, Führerschaft und Bewusstsein, Innovation und Zusammenarbeit.

- Wir unterstützen die Arbeit von Regierungen an der Vereinheitlichung internationaler Standards und deren Umsetzung, wir fördern die Einhaltung von Standards der Barrierefreiheit, garantieren die Technikneutralität und sorgen für eine hohe Kompatibilität.

HINTERGRUND

Die Informationstechnologie bereichert unser aller Leben, forciert den Handel und ermöglicht die weltweite Kommunikation. Weil die Technik eine immer größere Rolle in unserem Leben spielt, müssen alle Menschen davon profitieren können. Unabhängig davon, wie alt oder fit sie sind, muss es Anwendern möglich sein, die Vorteile der digitalen Welt zu nutzen.

Technologien für mehr Barrierefreiheit vereinfachen Anwendern die Nutzung ihres Rechners, weil sie damit besser sehen und hören, kurzum: ihren Rechner besser nutzen. Zudem können sie den Rechner damit individuell an ihre Anforderungen und Wünsche anpassen. Für viele Anwender wird durch die Barrierefreiheit ein Rechner erst nutzbar. So kann etwa der an einem Bildschirm dargestellte Text für sehbehinderte Menschen zu klein zum Lesen sein, oder sie sehen ihn überhaupt nicht. Anwender mit eingeschränkter Bewegung können möglicherweise mit ihren Händen einen handelsüblichen Rechner nicht bedienen. Die Barrierefreiheit unterstützt insbesondere sehbehinderte, bewegungseingeschränkte, hörgeschädigte oder kognitiv eingeschränkte Anwender.

Merkmale der Barrierefreiheit von Rechnern sind:

- Funktionen für die Bildschirmanzeige, Maus- und Tastaturbedienung, Klänge und Spracherkennung,
- assistierende Technologien und Produkte für das Vorlesen von Bildschirminhalten und spezielle Tastaturen, die Anwender mit eingeschränkter Sehfähigkeit, Hörproblemen, motorischen Einschränkungen oder besonderen Anforderungen an die Interaktion mit einem Rechner unterstützen,
- die Kompatibilität aller assistierenden Technologien und Produkten mit dem Betriebssystem und anderen Anwendungen.

Barrierefreiheit sollte während des Designs, der Entwicklung, des Tests und der Veröffentlichung eines Produkts berücksichtigt werden.

DER MICROSOFT-ANSATZ

- **Barrierefreiheit**. Viele unserer Produkte enthalten Funktionen für Barrierefreiheit und die individuelle Anpassung eines Rechners an die Bedürfnisse des Anwenders.

  » Windows 8 unterstützt Rechner, die sich ausschließlich per Touch-Bildschirm bedienen lassen. Dafür haben wir viele Funktionen für die Barrierefreiheit aktualisiert, wie etwa die Sprachausgabe und die Lupe. Mit dem Windows 8 Ease of Access Center verwalten Anwender viele Einstellungen für die Barrierefreiheit.

» Office 2013 unterstützt nahtlos Windows 8-Barrierefreiheitsfunktionen wie die Sprachausgabe und die Lupe sowie das Werkzeug für die Prüfung der Barrierefreiheit von Dokumenten.

» Office 365 unterstützt Anzeigemodi, mit denen Bildschirmleseanwendungen auf Word Web App und PowerPoint Web App zugreifen können. Zudem bietet es Barrierefreiheitseinstellungen für die Tastatur sowie einen Modus für eine kontrastreiche Darstellung.

- **Führerschaft und Bewusstsein**. Wir engagieren uns besonders im Bereich Forschung und Entwicklung von Funktionen für die Barrierefreiheit. Dazu gehören große, landesweit durchgeführte Studien, zielgerichtete Machbarkeitsstudien und Einzelinterviews. Wir erhöhen die öffentliche Aufmerksamkeit, indem wir Trainern, Entwicklern und anderen Spezialisten detaillierte Informationen über Technologien für die Barrierefreiheit zukommen lassen. Auf unserer Accessibility-Website und mit dem Accessibility Update-Newsletter informieren wir tiefgehend über die Barrierefreiheit unserer Produkte. Dort stellen wir auch Demos, Tutorials und Anleitungen zur Verfügung. Informationen über die Barrierefreiheit und Personalisierungen sind in 58 Ländern und 41 Sprachen verfügbar.

- **Innovation**. Mit unserem Accessibility Developer Center fördern wir die Entwicklung innovativer Technologien für mehr Barrierefreiheit. Das Portal unterstützt die Entwicklung von Barrierefreiheits-Apps mit Anleitungen und Technologien. Mit vielen unserer aktuellen Forschungs- und Entwicklungsprojekte möchten wir die Bedienung eines Rechners vereinfachen. Dafür arbeiten wir mit führenden Unternehmen und Organisationen wie der Accessibility Interoperability Alliance und der Assistive Technology Industry Association zusammen.

- **Zusammenarbeit**. Wir arbeiten gemeinsam mit vielen Organisationen daran, das Bewusstsein für Technologien für Barrierefreiheit zu erhöhen. Um die Herausforderungen genauer kennenzulernen, mit denen behinderte Anwender bei der Verwendung eines Rechners konfrontiert werden, diskutieren wir mit Anwenderverbänden und erarbeiten gemeinsam mit ihnen technische Trainings, die die Fähigkeiten behinderter Menschen im Umgang mit einem Rechner verbessern. Einige dieser Verbände sind unter anderem Partnership in Opportunities for Employment through Technology in the Americas und Unlimited Potential. Wir implementieren diese technischen Trainings für behinderte Anwender.

STRATEGISCHE ÜBERLEGUNGEN

- **Entwicklung einheitlicher globaler Standards**. Eine wichtige Grundlage für ein zuverlässiges Ökosystem mit vollständig miteinander kompatiblen Technologien sind marktgetriebene Standards für die Barrierefreiheit. Sie müssen weltweit einheitlich sein und mit öffentlichen Beschaffungsprogrammen gefördert werden.

- **Die digitale Einbindung fördern**. Regierungen müssen mit Richtlinien und Programmen dafür sorgen, dass sowohl behinderte als auch ältere Menschen an der digitalen Welt teilnehmen können.

- **Technologieneutralität sicherstellen**. Wenn Regierungen Standards für die Barrierefreiheit umsetzen, sollten sie dabei besonders auf die Technologieneutralität achten. Denn Richtlinien, die diese berücksichtigen, fördern Innovationen und ermöglichen einen freien Handel sowie Zugang zu Märkten für alle Anwender. Zudem steigern sie den Wettbewerb, indem sie Verzerrungen bei der öffentlichen Beschaffung verhindern.

- **Kompatibilität unterstützen**. Die vollständige Kompatibilität unserer Technologien für die Barrierefreiheit ist für uns ein Schlüsselmerkmal. Wir plädieren daher für öffentliche Richtlinien, damit diese Kompatibilität auf vielerlei Art und Weise erreicht wird. Regierungen sollten Technologieanbietern und Käufern auch alternative Lösungen anbieten können, die sich besser für deren Anforderungen eignen.

Hilfreiche Ressourcen

Die Microsoft-Website für Berrierefreiheit, mit Informationen über Produktfunktionen, Anleitungen, Demonstrationen und Leitfäden
www.microsoft.com/enable

Die Assistive Technology Industry Association
www.atia.org

Februar 2013