Lösungen für das Gesundheitswesen

Wie gut ist Ihre IT geschützt?

Decken Sie Ihre IT-Sicherheitslücken auf.

Sicherheitsverletzungen im Gesundheitswesen

Bei der Sicherheit im Gesundheitswesen geht es zunehmend ums Überleben. Selbst mit guten Sicherheitsmaßnahmen ist das Restrisiko nie gleich Null, wie das Lukaskrankenhaus in Neuss im Februar 2016 schmerzhaft erfahren musste—„Hacker hatten per E-Mail einen Trojaner in das Computersystem der Klinik geschleust. Die Schadsoftware drohte sämtliche Dateien zu verschlüsseln, sodass man alle Server und Rechner herunterfahren musste. Nur gegen Lösegeld bekäme man den Code zur Entschlüsselung, lautete die Botschaft der bislang unbekannten Angreifer. Wie bei einer Geiselnahme. Nur digital."[1]

Die rasante technologische Entwicklung und Veränderung im Gesundheitswesen birgt ein erhöhtes Risiko und erfordert somit ein dringendes Augenmerk auf Sicherheitslücken. Da keine Organisation gegen Sicherheitsverletzungen wie Cyberkriminalität, Hacker Attacken, Verlust oder Diebstahl von mobilen Geräten, bewußtes Umgehen, Betrug, bösartige Insider, Schnüffelprogramme, Erpresserprogramme und vieles mehr immun ist, gewinnt ein Vergleich mit dem Rest der Gesundheitsbranche immer mehr an Bedeutung. Keine Gesundheitsorganisation möchte in Bezug auf IT-Sicherheitsrisiken ein einfaches Ziel für Internetkriminalität sein. Sicherheit ist jedoch ein komplexes Thema mit einer sich schnell verändernden Bedrohungslandschaft. Hinzu kommt ein drastischer Mangel an Sicherheitsexperten im Gesundheitswesen. Immer mehr Gesundheitsorganisationen halten die grundlegende Erfüllung gesetzlicher Auflagen zwar für notwendig, aber für unzureichend, um das Risiko von Sicherheitslücken zu verringern.

Reifegrad der Sicherheitsmaßnahmen

Reifegradmodelle haben sich im Gesundheitswesen nachweislich bewährt. Weltweit verwenden beispielsweise über 5.300 Krankenhäuser das EMR Adoption Model (EMRAM) von HIMSS Analytics. Dieses basiert auf einem Modell, das Gesundheitsdienstleistern eine rasche Beurteilung ihres Reifegrads ermöglicht, Sicherheitslücken aufzeigt und Verbesserungsmöglichkeiten prüft. Darauf aufbauend haben wir ein Reifegradmodell für IT-Sicherheit erstellt, das die Grundlage für die Beurteilung Ihrer Sicherheitsmaßnahmen ist, eine rasche Beurteilung ihrer IT-Sicherheit ermöglicht, Sicherheitslücken aufzeigt und Verbesserungsmöglichkeiten prüft.

Highlights

- Schnelle Beurteilung und Ermittlung von Sicherheitslücken
- Vergleichen Sie Ihre IT-Sicherheitsrisiken mit der Gesundheitsbranche
- Erstellen Sie einen Aktionsplan zur Eliminierung von eventuell vorhandenen Sicherheitslücken

Leistungen

- Erstgutachten und Quartalsberichte
- Ermittlung von Vergleichswerten aus der Gesundheitsbranche
- Erkennen von Sicherheitslücken und Verbesserungen
- Erstellung eines angepassten Mehrjahresplans
- Fortschrittsüberprüfung

Durchführung

- Dauer: 1-2 Stunden
- Telefonisch oder persönlich

BASIS	ERWEITERT	FORTGESCHRITTEN
• Regelwerk • Risikobewertung • Audit und Compliance • Anwenderschulung • Mobilgeräte-Management • Geräteverschlüsselung am Endpoint • Prävention vor Datenverlust (Ermittlung) • Anti-Malware • Ein-Faktor-Zugriffskontrolle • Firewall • E-Mail-Gateway • Web-Gateway • Schwachstellenmanagement, Patching • Reaktionsplan für Sicherheitsvorfälle • Sichere Entsorgung • Datensicherung und Wiederherstellung	• Gerätekontrolle • Penetrationstests/Schwachstellen-Scan • Verschlüsselte Laufwerke für Clients • Prävention vor Datenverlust am Endpoint • Prävention vor Datenverlust im Netzwerk Überwachung, Erfassung • Anti-Diebstahl: Lokalisieren, Sperren und Löschen per Fernzugriff • Multi-Faktor-Authentifizierung mit Timeout • Sichere Fernadministration • Richtlinienbasierte Verschlüsselung für Dateien und Ordner • Verschlüsselung von Server/Datenbank/Backup • Netzwerksegmentierung • Eindringungsschutzsystem (Intrusion Prevention System, IPS) im Netzwerk • Vereinbarungen mit Geschäftspartnern • Virtualisierung	• Verschlüsselte Laufwerke für Server • Prävention vor Datenverlust im Netzwerk • Überwachung der Datenbankaktivitäten • Digitale Forensik • Sicherheitsinformationen und Event-Management • Informationsaustausch zu sicherheitsrelevanten Bedrohungen • Multi-Faktor-Authentifizierung mit Walk-Away-Lock • Whitelisting von Kunden-Anwendungen • Whitelisting von Server-Anwendungen • De-Identifikation/Anonymisierung • Tokenisierung • Disaster Recovery

REIFEGRADMODELL FÜR IT-SICHERHEIT

Beurteilung Ihrer Sicherheitsmaßnahmen

Bei der Beurteilung von eventuell auftretenden Sicherheitslücken wird im Zeitraum von 1-2 Stunden gemeinsam mit einem Sicherheitsberater der Ist-Zustand in Ihrer Organisation evaluiert und hinsichtlich des Reifegradmodells bewertet. Die interviewte Person sollte mit den vorhandenen Sicherheitsvorkehrungen sehr gut vertraut sein. Das Assessment ist telefonisch oder persönlich möglich. Nach der Beurteilung erhalten Sie einen zusammenfassenden Bericht, der Aufschluss über den Reifegrad und den Vergleich zur restlichen Gesundheitsindustrie gibt, Sicherheitslücken aufzeigt und ggf. einen mehrjährigen Plan zum schrittweisen Ausbau Ihrer IT-Sicherheit enthält. Sie erhalten nach dem Assessment zudem ein Jahr lang Quartalsberichte, die ihre Position im Vergleich zur Gesundheitsbranche aufzeigen. Es kann Sicherheitslücken aufdecken und zu einem weiterführenden Engagement einschließlich Richtlinienerstellung oder -aktualisierung, Risikobewertung, Penetrationstests, Schwachstellen-Scanning, Audit, Benutzerschulung oder Implementierung verschiedener Sicherheitsvorkehrungen führen. Die Ergebnisse werden vertraulich behandelt. Nur anonymisierte Daten werden für den Branchenvergleich herangezogen.

Branchenweite Zusammenarbeit

Intel und Partner führen die Beurteilung der Sicherheitsausstattung von Leistungserbringern im Gesundheitswesen, Krankenversicherungen, Pharma-und Life-Sciences Unternehmen weltweit bis Ende 2017 in einem Pilotprogramm durch.

Teilnahme

Wir freuen uns über Ihre Teilnahme an unserem Pilotprogramm. Um weitere Informationen zu erhalten, z.B. einen Probe-Report einzusehen oder teilzunehmen, besuchen Sie bitte intel.com/breachsecurity oder wenden sich an:

Intel Health & Life Sciences
Privacy & Security
BreachSecurity@Intel.com

oder

Microsoft Deutschland GmbH
Abteilung für das öffentliche Gesundheitswesen
BreachSecurity@microsoft.com

[1] http://www.welt.de/politik/deutschland/article152471885/Hacker-haben-in-deutschen-Kliniken-leichtes-Spiel.html

1116/DW/HBD/PDF ♻ Bitte entsorgen 333968-001DE

Microsoft intel