THREATQUOTIENT™

ThreatQ™ für Gesundheitsunternehmen

Gesundheitsunternehmen sind heute attraktive Ziele für Hacker, da sie im Auftrag ihrer Kunden Unmengen personen- und gesundheitsbezogener Informationen verarbeiten und speichern. Die elektronischen Patientenakten umfassen wertvolle Daten wie den vollständigen Namen des Patienten, Geburtsdatum, Sozialversicherungsnummer und Abrechnungsinformationen, die Kriminellen als digitales Gold auf dem Schwarzmarkt zu großen Gewinnen verhelfen.

Ransomware-Angriffe sind für 72 % der Malware-Zwischenfälle im Gesundheitswesen verantwortlich. Bei diesen Kampagnen werden häufig Anmeldedaten gestohlen und bis zur Entdeckung mehrere Maschinen infiziert sowie Abläufe erheblich gestört. Angriffe wie die WannaCry-Attacke im Mai 2017, die mehr als 100 Länder betraf, dienen Gesundheitsanbietern als Warnung und unterstreichen den weltweit dringenden Bedarf nach Cybersicherheitsmaßnahmen für Gesundheitssysteme.

WICHTIGE HERAUSFORDERUNGEN

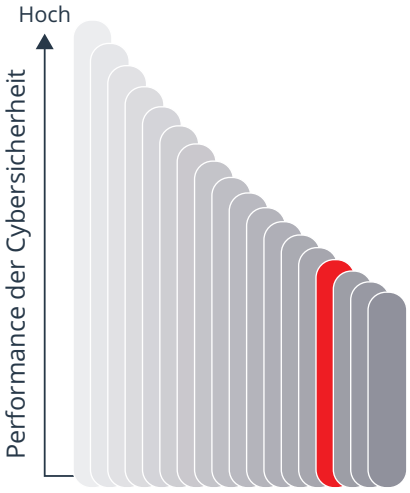
DATENVERFÜGBARKEIT

Sofortiger und zuverlässiger Zugriff auf exakte Patientendaten kann Leben retten. Daher müssen Mediziner bei Bedarf jederzeit Patientenakten abrufen können. Der ständige Blick auf das Wohlergehen und die Gesundheit der Patienten steht fasst immer über dem Schutz der Daten. Das führt dazu, dass sich Gesundheitsunternehmen immer noch auf einige unsichere Prozesse für den Informationsaustausch sowie auf veraltete Kommunikationstechnologien verlassen. Wachsamkeit ist jedoch ein Muss. Vertrauliche medizinische Daten sind besonders häufig das Ziel von Malware- sowie Ransomware-Angriffen und bedürfen daher besonders strenger Sicherheitskontrollen. Bedrohungsdaten bieten wertvolle Details zu den Motiven sowie zu den Taktiken, Techniken und Prozeduren (TTPs) der Angreifer und liefern damit nützliche Informationen dazu, wie effektive Schutzmaßnahmen gestaltet werden sollten.

VERALTETE SYSTEME

Medizinische Einrichtungen und Mediziner verfügen typischerweise lediglich über veraltete Systeme und Geräte, die häufig ältere Software und Sicherheitstools ausführen und daher besonders leicht kompromittiert werden können. Da Mitarbeiter im Gesundheitswesen jederzeit und überall auf Patienteninformationen zugreifen können müssen, schieben Administratoren das Upgrade der Geräte in Anbetracht potenzieller Unterbrechungen der Pflegeleistungen häufig auf. Gleichzeitig kann jedoch ein einziges veraltetes oder kompromittiertes System zu schwerwiegenden Sicherheitsverletzungen führen.

Um die Problembehebungsmaßnahmen zum Schutz der alten und neuen Ressourcen effektiv priorisieren zu können, müssen Gesundheitssysteme Bedrohungsdaten mit potenziellen Sicherheitsschwachstellen in der eigenen Umgebung korrelieren.



Das Gesundheitswesen liegt beim Vergleich der wichtigen US-Branchen in Bezug auf die Performance der Cybersicherheit auf Rang 15 von 18.[1]

8–10fach

Der Schwarzmarktpreis für Patientenakten liegt 8 bis 10 Mal über dem von Kreditkarten.[2]

Kosten pro gestohlener Patientenakte[3]

Durchschnittskosten durch Datenschutzverletzungen bei Gesundheitsunternehmen in den vergangenen zwei Jahren[4]

Dadurch können sich Anbieter mit begrenzten Sicherheitsressourcen auf die wichtigen Infrastrukturschwachstellen konzentrieren, die für das Unternehmen die größten Risiken darstellen.

MODERNE RESSOURCEN

Moderne Technologien – wie das Internet der Dinge (IoT) für medizinische Geräte und Anwendungen für elektronische Patientenakten – ermöglichen bisher unerreichte Verfügbarkeit, Konnektivität und Skalierbarkeit für effizientere und verbesserte Patientenbetreuung. Gleichzeitig vergrößern sie jedoch die Angriffsfläche und das Diebstahl- oder Missbrauchsrisiko für vertrauliche Daten. Die Suche nach der optimalen Balance zwischen fortschrittlicher Digitalisierung und erzwungenen Sicherheitsrichtlinien zum Schutz der Ressourcen gestaltet sich in Anbetracht der wachsenden Angriffsfläche auch weiterhin als schwierig. Die automatische Neuberechnung sowie Neu-Evaluierung der Prioritäten und Bedrohungsbewertungen anhand neuester Bedrohungsdaten sowie der Veränderungen in der internen Umgebung führt dazu, dass Sie sich kontinuierlich auf die relevantesten Strategien zur Risikominimierung konzentrieren können.

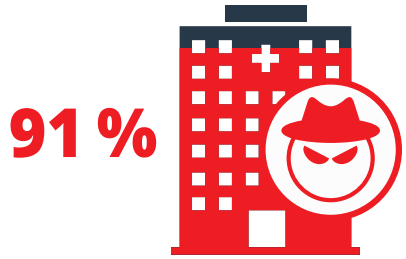
GEORDNETERE SICHERHEITSABLÄUFE IM GESUNDHEITSWESEN

Eine zuverlässige Bedrohungsdatenplattform bietet Gesundheitsanbietern den Kontext sowie die Möglichkeiten zur Anpassung und Priorisierung, die für fundiertere Entscheidungen, schnellere Erkennung und Reaktion sowie für die erweiterte Zusammenarbeit der Teams erforderlich sind. Sie müssen keine bestehenden Sicherheitsinfrastrukturen oder Abläufe ändern, da alle Tools und Technologien nahtlos mit der offenen Architektur von ThreatQ zusammenarbeiten.

MIT THREATQ MEHR ERREICHEN:

- **KONSOLIDIERUNG** aller Quellen für externe (z. B. NH-ISAC) und interne (z. B. SIEM) Bedrohungs- und Schwachstellendaten in einem zentralen Repository
- **AUSSORTIERUNG** nicht relevanter Informationen und einfache Navigation in enormen Mengen von Bedrohungsdaten zur Konzentration auf wichtige Ressourcen und Schwachstellen
- **PRIORISIERUNG** der Aspekte, die in Gesundheitssystemumgebungen am wichtigsten sind
- Integration nur solcher Indikatoren, die in Ihren HIPAA-bezogenen Sicherheitsrichtlinien (KRITIS in Deutschland) relevant sind
- **PROAKTIVE SUCHE** nach böswilligen Aktivitäten, die Patientenakten und Gesundheitsunternehmen erheblich schaden können
- **KONZENTRATION** auf bekannte Sicherheitsschwachstellen, die derzeit aktiv ausgenutzt werden und die Vorschriften-Compliance beeinträchtigen können
- **SCHNELLERE ANALYSE** und Reaktion auf Angriffe gegen mehrere Ziele (z. B. vernetzte medizinische Geräte)
- **AUTOMATISCHE** Einbindung von Bedrohungsdaten in Erkennungs- und Reaktionstools

Fordern Sie eine Live-Demo für ThreatQ Platform und ThreatQ Investigations an: threatq.com/demo



Anteil der Gesundheitsunternehmen mit mindestens einer Datenschutzverletzung in den letzten zwei Jahren[2]

Die Zahl kompromittierter Gesundheitskonten stieg von 26,4 Mio. auf 33,7 Mio. im Jahr 2017[5]

Die Zahl bekannt gewordener Hacking-Zwischenfälle im Gesundheitswesen stieg in den letzten zwei Jahren um das 2,6fache[6]

[1] SecurityScorecard: 2018 Healthcare Cybersecurity Report (Bericht zur Cybersicherheit im Gesundheitswesen für 2018)

[2] Cisco: Cybersecurity Strategies for Healthcare (Cybersicherheitsstrategien im Gesundheitswesen)

[3] Ponemon Institute, LLC: Ponemon Institute Research Report. 2017 Cost of Data Breach Study (Forschungsbericht des Ponemon Institute: Umfrage zu den Kosten für Datenschutzverletzungen 2017)

[4] Ponemon Institute, LLC Ponemon: Institute Research Report. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, 2016 (Forschungsbericht des Ponemon Institute: 6. Jährliche Benchmark-Umfrage zu Datenschutz und Sicherheit für Daten im Gesundheitswesen)

[5] Gemalto: 2017 Breach Level Index (Index der Datenschutzverletzungen 2017)

[6] HIPAA Journal: Largest Healthcare Data Breaches of 2017 (Größte Datenschutzverletzungen im Gesundheitswesen 2017)

ÜBER THREATQUOTIENT™

ThreatQuotient™ ist sich bewusst, dass Menschen die Grundlage für Intelligence-basierte Sicherheit darstellen. Die offene und erweiterbare Bedrohungsdatenplattform des Unternehmens, ThreatQ™ Platform, sowie die speziell für Cybersicherheits-Krisenteams ausgelegte Lösung ThreatQ Investigations unterstützen Sicherheitsteams mit dem Kontext sowie den Möglichkeiten zur Anpassung und Priorisierung, die für fundiertere Entscheidungen, schnellere Erkennung und Reaktion sowie für die erweiterte Zusammenarbeit der Teams erforderlich sind. Führende weltweite Unternehmen verwenden ThreatQuotient-Lösungen als Grundpfeiler für ihre Sicherheitsabläufe und ihr Bedrohungsmanagementsystem.

Weitere Informationen finden Sie unter threatq.com.

TQ_ThreatQ-for-Healthcare_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Allgemeine Fragen sowie Fragen zum Vertrieb: +1 703 574-9885