Deloitte.

LIFE SCIENCES & GESUNDHEITSWESEN
FEBRUAR 2023

Nicht ob, sondern wann: Umgang mit Ransomware-Angriffen im Gesundheitswesen

Inhaltsverzeichnis

Weltweit kam es in den letzten Jahren zu einem dramatischen Anstieg von Ransomware-Angriffen auf das Gesundheitswesen.

2022 kam es in US-amerikanischen Gesundheitseinrichtungen zu durchschnittlich 1'410 Cyberangriffen pro Woche – ein Anstieg um 86 Prozent im Vergleich zu 2021.[1] In Kanada waren die Hälfte aller Ransomeware-Opfer Unternehmen in kritischen Sektoren wie dem Gesundheitswesen.[2] Auch in Europa nahmen Cyberattacken auf Spitäler und Gesundheitsnetzwerke 2020 um 47%[3] zu.

Ein wichtiger Grund für diesen Anstieg ist die Cybercrime-Wirtschaft. Ein lukratives Geschäft: Jährlich werden hier über USD 1,5 Billionen generiert.

Das Gewinnpotenzial ist riesig, wenn man bedenkt, dass die ungefähren Durchschnittskosten für den Zugriff auf ein potenzielles Ziel nur rund USD 0,0004 bis USD 400 betragen.[4]

Bei etwa der Hälfte der Ransomware-Angriffe kommt es auch zu einer Datenschutzverletzung[5], und die folgenden beiden Anreize sind für Cyberkriminelle nahezu unwiderstehlich: der Verkauf personenbezogener Daten, der jährlich rund USD 160 Milliarden einbringt, und Lösegelderpressung mithilfe von Ransomware, womit sich gut USD 1 Milliarde jährlich erwirtschaften lässt.[6]

Gerade in diesen beiden Bereichen ist das Gesundheitswesen (Spitäler und Gesundheitsnetzwerke) besonders anfällig.

In diesen Einrichtungen gibt es nämlich jede Menge wertvoller Daten: von persönlich identifizierbaren Informationen (PII) und damit sensiblen Daten der Patientinnen und Patienten, Verschreibungsinformationen und Krankenversicherungsdaten bis hin zu internen Mitarbeiterdaten, Finanzdaten und geistigem Eigentum. Viele dieser Daten haben eine lange Lebensdauer. Damit lassen sie sich leicht verkaufen und für weitere Straftaten wie Identitätsdiebstahl, Erpressung oder Betrug nutzen.

Um die Sache noch komplizierter zu machen: Mit der jüngsten globalen Pandemie kamen auch neue Angriffsmöglichkeiten für Cyberkriminelle auf. Die schnelle Umstellung der Branche auf eine virtuelle Umgebung hat kritische Mängel bei der Kontrolle von Cybersicherheit aufgedeckt. Dies gilt insbesondere für wertvolle Informationen, die weiterhin in komplexen IT-Umgebungen gespeichert werden. Diese bestehen normalerweise aus veralteten, massgeschneiderten Systemen und Plattformen, die für den heutigen Grad der Vernetzung nicht geschaffen sind.

Hinzu kommen unterbesetzte Sicherheitsteams und knappe Cyberbudgets, was schliesslich erklärt, warum das Gesundheitswesen ins Visier von Cyberkriminellen geraten ist.

Unglücklicherweise macht diese Situation eine Systemverletzung praktisch unvermeidbar. Glücklicherweise jedoch gibt es Massnahmen, die Sie treffen können, um Ihr Unternehmen zu einem weniger attraktiven Ziel zu machen und den Schaden zu begrenzen, wenn ein Angriff erfolgt. Zentral dabei ist es, den gewieften Akteuren hinter den Cyberattacken mit einer wirksamen Cyberabwehr und der Fähigkeit zu begegnen, nach einem Angriff Ihre Systeme souverän wiederherstellen zu können.

In diesem Artikel erkunden wir Möglichkeiten, so vorzugehen, dass Unternehmen in einem sich rasch verändernden Cybersicherheitsumfeld Schritt halten können.

Entwicklung einer Abwehrstrategie

Die meisten Unternehmen haben erkannt, dass es sich bei den Cyber-gegnern nicht mehr um einzelne Hacker handelt, sondern um bestens organisierte Cyberbanden, staatlich geförderte Akteure und gewiefte Verbrecherorganisationen.

Auch wenn die Angriffe verschiedene Formen annehmen und aus unterschiedlichen Richtungen kommen können – das Hauptziel ist in der Regel das gleiche: beim Zielobjekt so viel Schaden wie möglich anzurichten, sodass die betroffenen Unternehmen das entsprechende Lösegeld bezahlen.

Mit Geld und Ressourcen im Rücken erreichen diese Gruppen ihr Ziel auf vielerlei Art. Ein typisches Angriffsmuster im Gesundheitswesen: Man bedient sich eines Insiders, um intern Zugriff auf die Unternehmensnetzwerke zu erlangen. Interne Mitarbeitende oder Auftragnehmende werden angeworben und erhalten Geld, damit sie intern im Auftrag der Angreifer agieren.

Andere Kriminelle dringen mithilfe von Angriffen Dritter, die speziell auf einfache Webanwendungen abzielen, in Unternehmenssysteme ein.[7]

Unabhängig davon, wie Cyberkriminelle in das System von Einrichtungen des Gesundheitswesens gelangen: In 93 Prozent der Fälle[8] wird der Zugang zu lokalen Netzwerkressourcen erheblich einfacher, sobald der Perimeter einmal durchdrungen ist.

Von dort aus können sie kritische Systeme stilllegen, den Zugriff auf wichtige Informationen und Daten blockieren oder sogar verknüpfte, möglicherweise lebensrettende oder lebensunterstützende medizinische Geräte hacken und Lösegeld für deren Entsperrung verlangen.

Neben einer Datenschutzverletzung können diese Angriffe weitere verheerende Konsequenzen haben: Sie haben möglicherweise längere Spitalaufenthalte, Verzögerungen bei Verfahren und Untersuchungen und sogar eine höhere Patientensterblichkeit zur Folge.[9]

Um ein Eindringen in den Perimeter zu verhindern, sollten Einrichtungen des Gesundheitswesens ihre Cyberabwehr verbessern, damit Angriffe für Kriminelle schwieriger und kostspieliger werden. Idealerweise konzentrieren sie sich dabei auf die folgenden fünf Schlüsselbereiche (siehe Seite 04).

Eindringen in den Perimeter verhindern

Stärkere Mitarbeitersensibilisierung
Die Mitarbeitenden sind in der Regel die erste Verteidigungslinie eines Unternehmens. Durch gezielte Cyberschulungen und Stärkung des Bewusstseins für Cyberrisiken sowie ständige Überwachung der Leistung von Nutzergruppen können Sie Hackern das Eindringen in Ihren Perimeter erheblich erschweren.

Verringerung der technischen Angriffsfläche Am liebsten greifen Hacker Unternehmen dort an, wo sie am leichtesten verwundbar sind. Daher ist es äusserst wichtig, Ihre Angriffsfläche durch aktives Schwachstellenmanagement, Patching und das «Abspecken» (Hardening) von Systemen sowie Anwendersicherheit (z. B. Browser-Isolierung) zu verringern.

Verbesserung der Erkennungsrate
Die Cyberlandschaft verändert sich ständig. Daher müssen Sie Ihr Umfeld ständig überwachen, um ungewöhnliches Verhalten oder Anzeichen eines Angriffs – wie etwa verdächtige Dateiaktivitäten auf Speichergeräten – erkennen zu können.

Begrenzung seitlicher Bewegung
Greift ein Hacker auf Ihre Systeme zu, sollten Sie verhindern, dass sich eine mögliche Gefährdung ausweitet. Durch die Anwendung von Zero-Trust-Prinzipien – wie Identitäts- und Privileged-Access-Management und Netzwerksegmentierung – können Sie die Möglichkeiten von Angreifern, sich seitlich im Netzwerk zu bewegen, begrenzen.

Isolierung und Eindämmung
Je schneller Sie betroffene Systeme isolieren können, desto schneller können Sie damit verbundene Schäden eindämmen. Eine Möglichkeit, dies zu erreichen, ist die proaktive Integration von Abschottungsfunktionen in das Infrastrukturdesign.

“Um ein Eindringen in den Perimeter zu verhindern, sollten Einrichtungen des Gesundheitswesens ihre Cyberabwehr verbessern, damit Angriffe für Kriminelle schwieriger und kostspieliger werden.”

Resilienz und Aufrechterhaltung der wichtigsten betrieblichen Funktionen

Eine starke Abwehrstrategie ist ein zentrales Element der Cybersicherheit. Ebenso wichtig ist aber die Fähigkeit Ihres Unternehmens, auf einen Angriff zu reagieren.

Kurze Reaktionszeiten und die Fähigkeit, unmittelbar auf einen Ransomware-Angriff zu reagieren, verbessern die Resilienz eines Unternehmens erheblich, verringern das Risiko, erpresst zu werden, und können in Extremfällen sogar Leben retten.

Das bedeutet, dass Sie Reaktions- und Recovery-Fähigkeiten aufbauen und Ihre Reaktionsteams so vorbereiten müssen, dass sie schon wissen, was zu tun ist, bevor es zu einer Systemverletzung kommt.

Aufbau von Reaktions- und Recovery-Fähigkeiten

Vorbereitung und Ausrichtung Ihres Unternehmens
Damit Ihr Unternehmen bei einer Systemverletzung wie eine gut geölte Maschine weiterläuft, ist es hilfreich, schon im Vorfeld funktionsübergreifende Krisen- und Reaktionsteams aufzubauen. Durch gezielte Übungen, Stresstests und Nachuntersuchungen früherer Vorfälle soll eine problemlose unternehmensweite Systemwiederherstellung ermöglicht werden.

Recovery-Planung
Technische und nicht technische Pläne sowie Strategiebücher ermöglichen es Ihrem Unternehmen, jede Phase der Wiederherstellung zu meistern und zu ermitteln, welche Vorgänge je nach Geschäftskritikalität priorisiert werden sollten. Ein durchgängiges Verständnis der gesamten Wertschöpfungskette ist für die Festlegung der Prioritäten und Abfolgen bei der Wiederherstellung unerlässlich.

Vorhaltung von Recovery-Tools
Bevor Sie eine beschädigte Infrastruktur wieder aufbauen können, müssen die richtigen Tools und Mittel vorhanden sein. Dazu können unveränderliche Kopien von Daten, isolierte Recovery-Umgebungen sowie die Orchestrierung und Automatisierung der Wiederherstellung zählen – all das kann eine Wiederherstellung beschleunigen.

Steuerung der Burst-Kapazität
Um wirksam auf einen laufenden Angriff zu reagieren, müssen Sie in der Lage sein, Ressourcen dort zuzuweisen, wo sie knapp sind, und übermässige Ressourcen zu steuern. Dazu zählen alle Arten von Ressourcen – von physischen Ressourcen bis hin zur Bereitstellung durch Dritte.

Wirksame Kommunikation
Bei einer Systemverletzung benötigt Ihr Unternehmen klare Kommunikationskanäle und -prozesse. Zudem muss es in der Lage sein, während der gesamten Reaktionsphase transparent zu agieren und den Mitarbeitenden ständig in Erinnerung zu rufen, beherrscht und kontrolliert vorzugehen. Ein robuster Kommunikationsplan, der interne und externe Kommunikationsbedürfnisse berücksichtigt, kann dazu beitragen, die Wiederherstellung ruhig und konzentriert zu koordinieren. Dies ist bei Einrichtungen des Gesundheitswesens besonders wichtig, denn möglicherweise müssen Sie angesichts der sensiblen Natur und des Umfangs der Datenschutzverletzung mit Patientinnen und Patienten und Behörden kommunizieren.

Souveräne Wiederherstellung

Die Cyberbedrohungslage entwickelt sich ständig weiter, und Einrichtungen des Gesundheitswesens müssen sich entsprechend anpassen.

Das bedeutet, dass es nicht nur darum geht, Cyberangriffe zu erkennen und unternehmenskritische Ressourcen zu schützen. Vielmehr muss auch die Resilienz gesteigert werden, um im Falle einer Systemverletzung die Wiederherstellung zu ermöglichen.

Dies umfasst unter Umständen die Instandsetzung beschädigter Systeme und Datenbestände. Es kann aber auch bedeuten, Pläne zu erstellen, um den Betrieb bei einem länger andauernden Systemausfall aufrechtzuerhalten.

In jedem Fall müssen Einrichtungen des Gesundheitswesens eine Grundlage zum Schutz ihrer Patientinnen und Patienten schaffen und dafür sorgen, dass kritische Systeme betriebsbereit bleiben.

Diese Aufgabe wird angesichts der sich fortlaufend ändernden Bedrohungslage immer herausfordernder. Eine optimale Vorbereitung ist daher umso wichtiger.

Indem Sie Ihre unternehmenskritischen Dienste ermitteln, das Zusammenspiel Ihrer einzelnen Systeme nachvollziehen, auf laufende Schulungen setzen und ständig Ihre Wiederherstellungsfähigkeit verbessern, können Sie Angriffe, die zunehmend auf Sie abzielen, erfolgreich abwehren.

Vernetzen Sie sich mit uns

Quellen

1 *https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022*

2 *https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/*

3 *https://www.balcanicaucaso.org/eng/Areas/Europe/Cyber-attacks-are-growing-in-the-European-Union-21652*

4 *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

5 *https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-constitute-data-breach*

6 *https://www.techrepublic.com/article/cybercriminals-raking-in-1-5-trillion-every-year/*

7 *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

8 *https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=70ea31106b61*

9 *https://www.ibm.com/thought-leadership/institute-business-value/report/medical-device-security*

Kishwar Chishty
Partner – Global LSHC Industry Cyber Leader – Deloitte Switzerland
Life Sciences Risk Advisory

kchishty@deloitte.ch

Florian Widmer
Partner – Deloitte Switzerland
Cyber and Strategic Risk

fwwidmer@deloitte.ch

John Lu
Principal – Deloitte & Touche LLP
Cyber and Strategic Risk

jolu@deloitte.com

Deloitte.