Insight

Ransomware Bereit-schaft Best Practices

Reagieren, wiederherstellen und weitermachen.

Hacker werden immer raffinierter, und es ist wichtiger denn je, den sich entwickelnden Bedrohungen einen Schritt voraus zu sein.

In der heutigen IT-Landschaft sind Cyber-Angriffe eher eine Frage des "Wann" als des "Ob". Aber mit dem richtigen Plan können Sie Ihre sensiblen Daten besser schützen, einen Angriff bewältigen und weiteren Schaden verhindern.
Erfahren Sie in diesem Leitfaden mehr über die wichtigsten Komponenten einer effektiven Vorbereitung und Reaktion auf Ransomware.

43%

der IT-Führungskräfte geben an, in den letzten 12 Monaten von einem Verstoß gegen die Cybersicherheit betroffen gewesen zu sein.[1]

$4,88M

Durchschnittliche Gesamtkosten eines Sicherheitsverstoßes - Anstieg um 10 %, höchster Anstieg seit der Pandemie.[2]

11 Tage

Die durchschnittliche Zeit, die IT-Manager angeben, um die letzte Cybersicherheitsverletzung zu beheben.[1]

Ransomware im Wandel der Zeit

Seit den Anfängen der Trojaner-Angriffe im Jahr 1989 hat sich Ransomware von einem unbedeutenden Problem zu einer der größten Bedrohungen für die Cybersicherheit entwickelt. Mit der Einführung von Verschlüsselung in die Angriffsstrategie in den frühen 2000er Jahren nahm Ransomware Fahrt auf und entwickelte sich zwischen 2010 und 2020 noch schneller.

Dieser Wachstumsschub ist zum Teil auf das Aufkommen von Bitcoin als bequeme Methode der Lösegeldzahlung zurückzuführen, die die Anonymität der böswilligen Akteure schützt, und zum Teil auf den Erfolg von Exfiltrationsangriffen (auch bekannt als Leakware oder Doxware), bei denen böswillige Akteure damit drohen, sensible Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird.

Fünf Jahrzehnte Ransomware

1980

Der erste bekannte Ransomware-Angriff, ein Trojaner, wird gestartet.

1990

Öffentliches Bewusstsein für Cyber-Sicherheit durch den Boom von Heim-PCs und E-Mail-Viren.

2000

Bitcoin kommt auf den Markt und erleichtert böswilligen Akteuren die Erpressung.

2010

Ransomware-Strategie wird von Exfiltration und Erpressung dominiert.

2020

Berufe im Bereich Cybersicherheit gehören zu den am schnellsten wachsenden. Nach Angaben des U.S. Bureau of Labor Statistics wird die Beschäftigung von Informationssicherheitsanalytikern zwischen 2023 und 2033 um 33 % zunehmen – deutlich schneller als der Durchschnitt aller Berufe.[3]

Aktuelle Ransomware-Trends

Ransomware wird immer ausgefeilter und die Angreifer immer hartnäckiger. Ohne die richtige Reaktions- und Wiederherstellungsstrategie können die Folgen verheerend sein.

Die wichtigsten Ransomware-Ziele nach Branche:

Bildungs-wesen

Bauwesen & Immobilien

Zentral- und Föderal-regierung[5]

Ransomware ist eine wachsende Bedrohung, die eine proaktive Strategie und einen vielschichtigen Ansatz erfordert. Das Wissen um die Wahrscheinlichkeit und die finanziellen Auswirkungen eines Angriffs ist nur der Anfang..

Die richtige Planung kann den Unterschied zwischen einer kleinen Störung und einer Katastrophe ausmachen.

73%

der Unternehmen weltweit zahlten 2023 Lösegeld für die Wiederherstellung von Daten.[6]

$479.000

Im dritten Quartal 2024 lag die durchschnittliche Lösegeldforderung für Cyberangriffe in den USA bei über 479.000 US-Dollar.[4]

Kennen Sie Ihre Schwachstellen

1. Risiken lauern auf jeder Ebene Ihrer IT-Umgebung.

Der Schutz vor Ransomware beginnt mit einer ganzheitlichen Betrachtung Ihrer gesamten Infrastruktur. Eine einzige Schwachstelle reicht aus, um Angreifern Zugang zu verschaffen. Die Identifizierung und Behebung bestehender Sicherheitsprobleme auf jeder Ebene Ihres Unternehmens, von der Netzwerksicherheit bis hin zur Backup-Architektur und darüber hinaus, sollte oberste Priorität haben.

2. Die meisten erfolgreichen Ransomware-Angriffe sind auf menschliches Versagen zurückzuführen.

Menschliches Versagen ist so weit verbreitet, dass die meisten Ransomware-Angriffe darauf zurückzuführen sind. Auch wenn sich Ransomware weiterentwickelt hat, basieren die meisten Angriffe immer noch darauf, dass ein Endnutzer versehentlich Anmeldedaten eingibt oder auf ein schädliches Programm klickt, um es zu aktivieren.

Auch wenn menschliches Versagen nie ganz ausgeschlossen werden kann, ist es doch möglich, die Risiken zu minimieren und die Lücken zu schließen, indem die Architektur und die Sicherheitsprotokolle in Ihrem Unternehmen ordnungsgemäß implementiert werden.

Sicherheitsvorfälle mit Vertrauen und Effizienz entschärfen.

Angriffe auf die Cybersicherheit können zum Verlust oder zur Unterbrechung wichtiger Vermögenswerte oder Geschäftsfunktionen führen. Eine solide Sicherheitsstrategie ist wichtiger denn je, um böswilligen Akteuren einen Schritt voraus zu sein. Lesen Sie unseren **Expertenleitfaden zur Reaktion auf Vorfälle** und erfahren Sie mehr über 11 Best Practices für den Umgang mit modernen Bedrohungen.

Schützen Sie Ihre Daten.

Die Überlegungen zum Schutz Ihrer Daten beginnen mit der Frage, was Sie schützen wollen. Die Häufigkeit von Exfiltrationsangriffen kann mit dem steigenden Wert von Daten und der wachsenden Menge an sensiblen Daten in Verbindung gebracht werden, die von Unternehmen mit hohem Risiko erstellt, gespeichert und verwendet werden.

Ein weiterer zu berücksichtigender Aspekt ist die Unveränderbarkeit von Daten, d. h. die Erstellung von Daten, die anschließend nicht mehr verändert werden können. Dieser Begriff taucht häufig in Diskussionen über Ransomware auf. Theoretisch ist dies eine praktische Lösung. In der Praxis kann es jedoch schwierig sein, sie zu erreichen. Vor allem, wenn Ihre Angreifer den Zugang zu internen Kontrollen nutzen, um Ihre Backup-Umgebungen zu kompromittieren.

Da es schwierig ist, Daten wirklich unveränderbar zu machen, ist es wichtig, dass Ihre Datenschutzplattform sicher ist. Dies gilt zwar auch für Daten vor Ort, doch müssen Unternehmen beim Schutz von Daten, die in der Cloud gespeichert sind, besondere Vorsicht walten lassen.

Es besteht die allgemeine Annahme, dass Daten in der Cloud automatisch sicherer sind. Dies könnte nicht weiter von der Wahrheit entfernt sein. In den Verträgen für Cloud-Dienste wird oft ausdrücklich empfohlen, einen Drittanbieter mit dem Schutz der Daten zu beauftragen. Denken Sie daran: Sie sind für Ihre Daten verantwortlich.

Gehen Sie datenorientiert vor und fragen Sie sich:

"Mit welcher Art von Daten habe ich es zu tun?"

"Wo befinden sich diese Daten?"

"Wie schützen wir sie?"

Wenn Sie all diese Fragen beantworten können, haben Sie eine viel solidere Grundlage, um voranzukommen.

Sichern Sie Ihre Backups.

Bis vor kurzem war die Datensicherung die wichtigste Maßnahme zur Abwehr eines Angriffs. Und heute? Die Angreifer beginnen bei den Backups.

Und so funktioniert es: Ihre Backup-Software und -Architektur sind hervorragend; Sie glauben, Sie seien geschützt. Dann macht jemand in Ihrem Unternehmen einen Fehler. Dadurch gelangt ein Angreifer an Administrator-Zugangsdaten. Mit diesen Zugangsdaten kann er sich in Ihrer Umgebung umsehen, Ihren Backup-Prozess kennenlernen und die Backups angreifen, bevor er seine Ransomware freigibt. Jetzt ist Ihr Failsafe weg und es ist viel wahrscheinlicher, dass Sie das Lösegeld bezahlen, um Ihre restlichen Daten zu entschlüsseln.

Backups allein reichen nicht aus, und Backups in der Cloud bedeuten nicht, dass Ihre Daten sicher sind. Backups waren sicherer, als Netzwerke und physische Umgebungen noch einfacher zu sichern waren. Mit der Entwicklung von Heimarbeitsplätzen und dem Internet of Things (IoT) ist es jedoch schwieriger geworden, Grenzen zu definieren und zu sichern. Umso wichtiger ist es, die Backup-Umgebungen zu überprüfen und geeignete Strategien für die Datenisolierung/Luftsicherheit zu entwickeln.

Hinweise zum Datenschutz:

Bewahren Sie mehrere Kopien Ihrer Daten auf.

Decken Sie mehrere Arten von Medien ab.

Speichern Sie Daten an mehreren Standorten.

"Ich hatte einen Kunden, der alle richtigen Schritte in Bezug auf Backup-Appliances, Datenreplikation zwischen zwei Rechenzentren usw. unternommen hat. Das Problem war jedoch nicht die Backup-Software oder die Appliances selbst, sondern entweder ein Standardpasswort oder jemand konnte die Admin-Zugangsdaten kompromittieren. Sie drangen ein, löschten die Backup-Appliances und setzen dann die Ransomware frei."

– DATA PROTECTION SOLUTIONS ARCHITECT, INSIGHT

Lösungen für den Datenschutz

Daten sind das Rückgrat Ihres Unternehmens. Zuverlässige Technologien helfen dabei, sie zu schützen, Compliance zu gewährleisten und vor Beschädigung zu bewahren.

Cyber-Sicherheitslösungen, die Ihre Daten in den folgenden Schlüsselbereichen schützen:

Identität

Werkzeuge wie Multi-Faktor-Authentifizierung (MFA) und Single Sign-On (SSO) helfen, den Benutzerzugriff auf Ihre internen Systeme zu verwalten.

Endpunkte

Lösungen zur Datenspeicherung und zum Schutz Ihrer Geräte schützen Ihre Teams vor böswilligen Angreifern. Egal, wo und wann Ihre Mitarbeiterinnen und Mitarbeiter arbeiten.

Netzwerke

Netzwerklösungen wie Firewalls und virtuelle private Netzwerke bieten robusten Schutz. Sie umfassen Verschlüsselung, Netzwerkerkennung, Reaktionssteuerung und Fernzugriffsfunktionen.

Erstellen Sie einen Plan – testen, ändern und üben Sie ihn.

Es gibt viele Dinge, die Sie tun können, um das Risiko eines Ransomware-Angriffs zu verringern, aber es gibt keine Möglichkeit, ihn vollständig zu verhindern. Bereiten Sie sich am besten so vor, als seien Sie sich sicher, dass es zu einem Datenverlust kommen wird, denn statistisch gesehen ist dies sehr wahrscheinlich.

"Wir sollten davon ausgehen, dass es nicht um das "ob" geht, sondern um das "wann". Sind wir vorbereitet und was werden wir tun?"

– LEAD ARCHITECT, INSIGHT

Erstellung eines strategischen Wiederherstellungsplans für Notfälle

Planung

Die Entwicklung eines Notfallwiederherstellungsplans ist ein wichtiger und oft übersehener Teil des Ransomware-Puzzles. Bewerten Sie alle potenziellen Auswirkungen eines Ransomware-Vorfalls, von Überlegungen zur Netzwerksicherheit bis hin zu rechtlichen Konsequenzen, und erstellen Sie einen Aktionsplan. Sie können mit Sicherheitsdienstleistern zusammenarbeiten, um einen maßgeschneiderten, umsetzbaren und gut dokumentierten Vorfallreaktionsplan zu erstellen, der Ihr gesamtes Unternehmen abdeckt.

Testen

Genauso wichtig wie die Entwicklung eines Plans ist seine Erprobung. Testen Sie Ihren Plan in Ihrer aktuellen Umgebung auf Schwachstellen, passen Sie ihn an, üben Sie ihn regelmäßig und überarbeiten Sie ihn bei Bedarf. Auf diese Weise stellen Sie nicht nur sicher, dass Ihre internen Teams bereit sind, im Falle eines Ereignisses schnell und effektiv zu reagieren, sondern auch, dass Ihr Plan auf dem neuesten Stand und optimal positioniert ist, um die besten Ergebnisse zu erzielen.

Aufklärung

Da menschliches Versagen an der Spitze der Ransomware-Kettenreaktion steht, darf die Aufklärung nicht vernachlässigt werden. Alle Mitarbeiter eines Unternehmens sollten eine grundlegende Schulung über Ransomware erhalten, insbesondere darüber, wie Phishing-Versuche erkannt und gemeldet werden können.

Ransomware ist bereit. Sie auch?

Jedes Unternehmen hat seine eigene Strategie für den Umgang mit Ransomware. Eine wirksame Strategie muss mehrere Faktoren berücksichtigen, darunter die Menge und Art Ihrer Daten sowie die Komplexität Ihrer IT-Infrastruktur.

Insight hilft Ihnen dabei, Ihre aktuelle Sicherheitslage im Hinblick auf die sich entwickelnden Ransomware-Bedrohungen zu bewerten und gemeinsam mit Ihnen einen ganzheitlichen Cybersicherheitsansatz zu entwickeln, der jede Ebene Ihrer IT-Umgebung schützt und den spezifischen Anforderungen Ihres Unternehmens gerecht wird.

End-to-end Sicherheit beginnt mit Insight.

Seien Sie nicht unvorbereitet auf die sich ständig verändernden Bedrohungen von heute - unsere Experten haben bereits unzähligen Kunden geholfen, Sicherheitsherausforderungen zu meistern.
Finden Sie heraus, was wir für Ihr Unternehmen tun können.

Über Insight

Insight Enterprises, Inc. ist ein Fortune 500-Lösungsintegrator, der Unternehmen dabei unterstützt, ihre digitale Transformation zu beschleunigen, ihr Geschäft zu modernisieren und den Wert ihrer Technologie zu maximieren. Die technische Expertise von Insight umfasst Cloud- und Edge-basierte Transformationslösungen mit globaler Skalierbarkeit und Optimierung, die auf mehr als 35 Jahren enger Partnerschaften mit den weltweit führenden und aufstrebenden Technologieanbietern basieren.

at.insight.com | ch.insight.com | de.insight.com

[1] MarketPulse Research by Foundry Research Services. (June 2024). The Path to Digital Transformation: Where IT Leaders Stand in 2024. Commissioned by Insight.

[2] IBM and Ponemon Institute. (July 2024). Cost of a Data Breach Report 2024. IBM.

[3] U.S. Bureau of Labor Statistics. (2024, Aug. 29). Occupational Outlook Handbook: Informational Security Analysts. U.S. Department of Labor.

[4] Petrosyan, A. (2024, Nov. 19). U.S. average amount of ransom payments related to cyberattacks Q1 2022-Q3 2024. Statista.

[5] Irei, A. (2024, Jan. 31). Top 13 ransomware targets in 2024 and beyond. TechTarget.

[6] Petrosyan, A. (2023, Aug. 31). Annual share of companies worldwide that paid ransom and recovered data from 2018 to 2023. Statista.