4 Best Practices für Ransomware Readiness

Insight

Eine kurze Geschichte über Ransomware

Seit den Anfängen der auf Lockern basierenden Trojanerangriffe im Jahr 1989 hat sich Ransomware von einem kleinen Problem zu einer großen Bedrohung für die Cybersicherheit entwickelt. Als die Verschlüsselung Anfang der 2000er Jahre in die Strategie der Angriffe aufgenommen wurde, nahm Ransomware Fahrt auf und entwickelte sich zwischen 2010 und 2020 noch schneller.

Dieser Wachstumsschub ist zum Teil auf das Phänomen zurückzuführen, dass Bitcoin als bequeme Methode der Lösegeldzahlung aufkam, die die Anonymität der Angreifer schützte, und zum Teil auf den Erfolg von Angriffen im Stil der Exfiltration (auch bekannt als Leakware oder Doxware), bei denen böswillige Akteure damit drohen, sensible Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird.

Ransomware über 40 Jahre

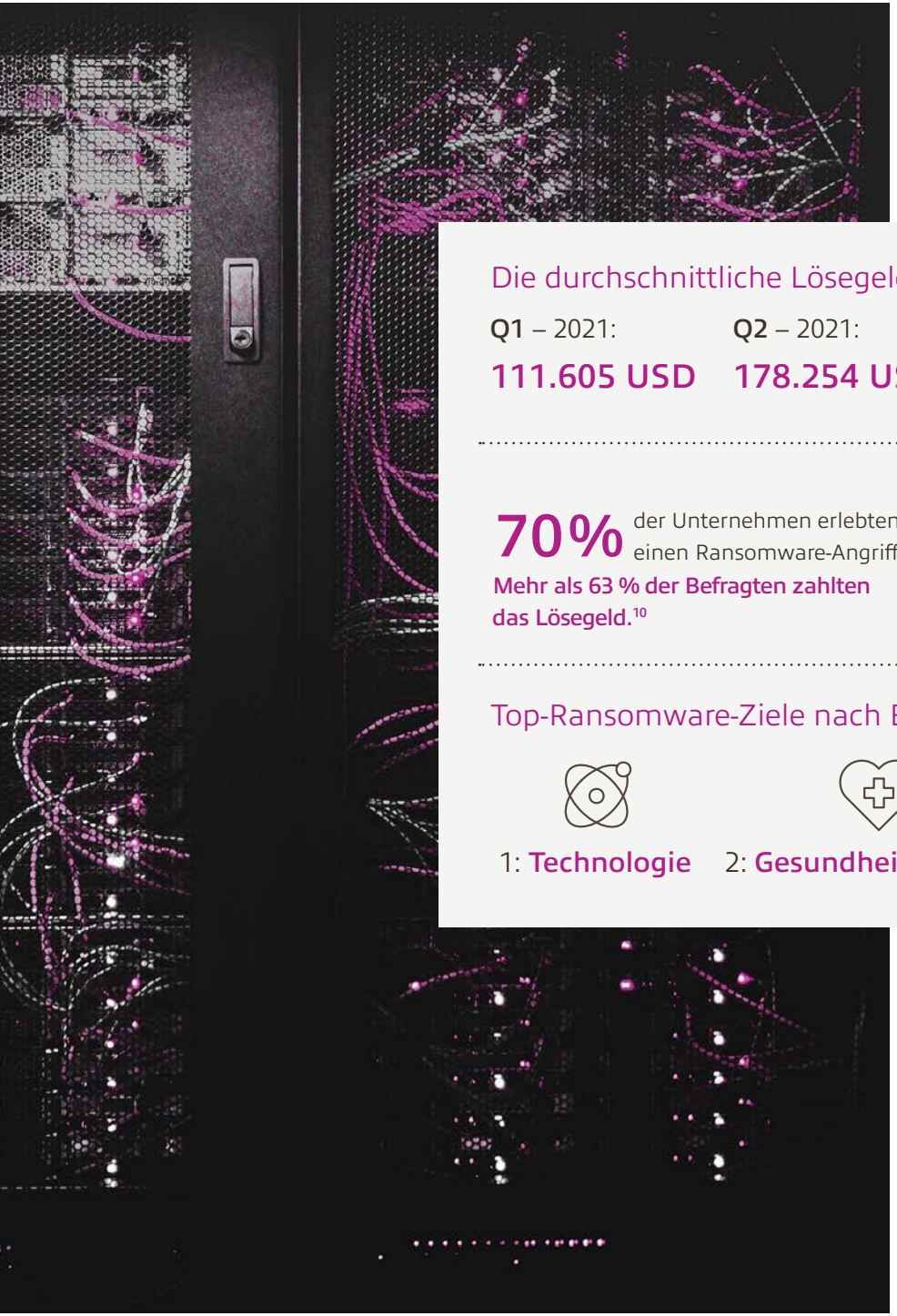
1989
Der erste bekannte Ransomware-Angriff; ein Trojaner, wird gestartet.[1]

1999
Upticks in Heim-PCs und E-Mail-Viren bringen Cybersicherheit ins öffentliche Bewusstsein.[2]

2009
Bitcoin kommt auf den Markt und macht Erpressung für böswillige Akteure einfacher.[3]

2019
Exfiltration und Erpressung beginnen, die Ransomware-Strategie zu dominieren.[4]

2029
Cybersicherheitsjobs gehören zu den am schnellsten wachsenden, mit einem Anstieg von 31 %.[5]



Ransomware-Trends heute

Ransomware-Angriffe haben an Stärke und Schwere zugenommen, und die damit verbundenen Kosten sind gestiegen, da die Anzahl der betroffenen Organisationen zunimmt und Backups als effektive Sicherheitsstrategie scheitern.[6,7]

Die durchschnittliche Lösegeldzahlung steigt:

Q1 – 2021:	**Q2** – 2021:	**Q3** – 2021:	**Q4** – 2021:
111.605 USD	**178.254 USD**	**139.739 USD**	**322.168 USD**[8]

265 MRD. USD Gesamte Ransomware-Kosten für alle Unternehmen im Jahr 2030[9]

70 % der Unternehmen erlebten 2021 einen Ransomware-Angriff.
Mehr als 63 % der Befragten zahlten das Lösegeld.[10]

Ransomware betrifft alle **2 Sekunden 1 Unternehmen.**[11]

Durchschnittliche Ausfallzeit pro Angriff **15 Tage**[12]

Top-Ransomware-Ziele nach Branche:

1: **Technologie** 2: **Gesundheitswesen** 3: **Bildungswesen**[13]

Das durchschnittliche IT-Sicherheitsbudget für 2022 beträgt **24,4 Millionen USD**, von denen **25 %** voraussichtlich für die Minderung von Ransomware ausgegeben werden[14].

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

Wie geht es nun weiter?

In diesem Leitfaden lernen Sie die vier wichtigsten Komponenten einer effektiven Ransomware Readiness und -Reaktion kennen.

1. Kennen Sie Ihre Schwachstellen

Ransomware macht sich die Schwachstellen eines Unternehmens zunutze, um die Umgebung zu infiltrieren. Es gibt zwei grundlegende Überlegungen, die bei der Bewertung der Schwachstellen Ihres Unternehmens zu beachten sind:

A. In jeder Ebene Ihrer IT-Umgebung besteht ein Risiko.

Ransomware-Schutz beginnt damit, einen vollständigen Überblick über Ihre gesamte Infrastruktur zu erhalten.
Es braucht nur eine Schwachstelle, um Angreifer hereinzulassen. Die Identifizierung und Behebung bestehender Sicherheitsbedenken auf allen Ebenen Ihres Unternehmens, von der Netzwerksicherheit bis hin zu Backup-Architekturen und darüber hinaus, sollte oberste Priorität haben.

B. Menschliche Fehler liegen hinter den meisten erfolgreichen Ransomware-Angriffen.

Menschliche Fehler sind so weit verbreitet, dass die meisten Ransomware-Angriffe darauf beruhen. Auch wenn sich Ransomware weiterentwickelt hat, beruhen die meisten Angriffe immer noch darauf, dass ein Endnutzer versehentlich Anmeldedaten angibt oder auf ein bösartiges Programm klickt, um es zu aktivieren.

Obwohl es niemals möglich ist, das Problem menschlicher Fehler vollständig zu lösen, ist es möglich, Ihre Risiken zu minimieren und die Lücken mit ordnungsgemäß aufgebauten Architekturen und ordnungsgemäß implementierten Sicherheitsprotokollen in Ihrem Unternehmen zu füllen.

85 % der Verstöße 2020 basierten auf menschlichem Versagen.[15]

Die Schaffung von Sicherheit auf Identitäts-, Endgerät-, Netzwerk- und Infrastrukturebene ist entscheidend für eine umfassende Risikominderung.

2. Ihre Daten sichern

Überlegungen zur Sicherung Ihrer Daten beginnen damit, zu verstehen, was Sie schützen möchten. Die Verbreitung von Exfiltrationsangriffen kann mit dem steigenden Wert von Daten und der wachsenden Menge an sensiblen Daten, die von risikoreichen Unternehmen erzeugt, gespeichert und genutzt werden, in Verbindung gebracht werden.

Die Unveränderlichkeit von Daten ist ein weiterer Punkt, den Sie berücksichtigen sollten – d. h. die Erstellung von Daten, die nach dem Schreiben nicht mehr geändert werden können. Der Begriff kommt oft in Gesprächen über Ransomware auf. Theoretisch ist es eine praktische Lösung. In der Praxis kann es schwierig sein, dies zu erreichen. Insbesondere, wenn Ihre Angreifer Zugriff auf interne Kontrollen nutzen, um Ihre Backup-Umgebungen zu gefährden – aber mehr dazu im nächsten Abschnitt.

Aufgrund der Schwierigkeit echter Datenunveränderlichkeit ist es wichtig, sicherzustellen, dass Ihre Datenschutzplattform sicher ist. Obwohl diese Überlegung für On-premises-Daten immer noch wichtig ist, müssen Unternehmen besonders vorsichtig sein, um in der Cloud gespeicherte Daten zu schützen.

Es gibt eine allgemeine Annahme, dass Daten in der Cloud automatisch sicherer sind. Das könnte kaum weiter von der Wahrheit entfernt sein. Cloud-Service-Vereinbarungen empfehlen oft ausdrücklich, eine Drittanbieterquelle für den Datenschutz einzusetzen. Denken Sie daran: Sie sind für Ihre Daten verantwortlich.

Denken Sie an einen datenorientierten Ansatz und fragen Sie sich:

„Mit welcher Art von Daten habe ich es zu tun?“

„Wo befinden sich dieseDaten?“

„Wie schützen wir sie?“

Wenn Sie all diese Fragen beantworten können, haben Sie eine viel stärkere Grundlage für die Zukunft.

3. Sichern Sie Ihre Backups

Lange Zeit galten Datensicherungen als wichtigster Plan für den Fall eines Angriffs. Und jetzt? Backups sind der Ort, an dem die Angreifer ansetzen. Das funktioniert in etwa so:

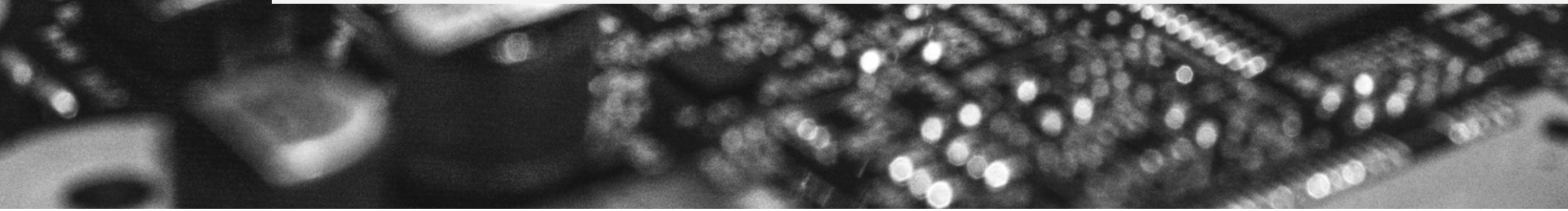
Ihre Backup-Software und -Architektur sind großartig; Sie glauben, dass Sie geschützt sind. Dann macht jemand in Ihrem Unternehmen einen Fehler.
Infolgedessen verfügt ein Angreifer über Admin-Anmeldedaten. Mit diesen Anmeldeinformationen können sie Zeit in Ihrer Umgebung verbringen, Ihren Backup-Prozess kennenlernen und dann die Backups angreifen, bevor sie ihre Ransomware freisetzen. Jetzt ist Ihr Sicherheitssystem nicht mehr verfügbar und es ist wahrscheinlicher, dass Sie das Lösegeld bezahlen, um Ihre restlichen Daten zu entschlüsseln.

> „Ich hatte Kunden, die alle richtigen Schritte unternommen haben, wie z. B. Backup-Anwendungen, Datenreplikation zwischen zwei Rechenzentren usw. Aber es waren nicht wirklich die Backup-Software oder die Geräte selbst, die ein Problem darstellten. Es handelte sich entweder um ein Standardpasswort, oder jemand konnte die Admin-Anmeldedaten kompromittieren. **Sie sind dort eingedrungen und haben im Grunde die Backup-Anwendungen gelöscht und dann die Ransomware freigesetzt.**“
>
> – **Data Protection Solutions Architect**, Insight

Backups allein reichen nicht aus, und Backups in der Cloud bedeuten nicht, dass Ihre Daten sicher sind. Backups waren sicherer, als Netzwerke und physische Grenzen noch einfacher zu sichern waren. Aber mit der Entwicklung zur Remote-Arbeit und dem Internet der Dinge (Internet of Things, IoT) sind Perimeter schwieriger zu definieren und zu sichern, was es noch wichtiger macht, Ihre Backup-Umgebungen zu überprüfen und über angemessene Datenisolierungsstrategien zu verfügen.

Der beste Weg, Ihre Daten vor Ransomware zu schützen, ist:

- Mehrere Kopien der Daten
- Mehrere Medientypen abdecken
- An mehreren Standorten gelagert, vorzugsweise auch außerhalb des Standorts



4. Einen Plan haben (und ihn testen, ändern und durchführen)

Es gibt viele Dinge, die Sie tun können, um Ihr Risiko für Ransomware-Angriffe zu reduzieren, aber es gibt keine Möglichkeit, sie vollständig zu verhindern. Die beste Vorgehensweise besteht darin, sich so vorzubereiten,als ob Sie sicher davon ausgehen, dass Sie eine Datenschutzverletzung erleiden werden, weil es – statistisch gesehen – wahrscheinlich ist.

„Die Annahme sollte sein, dass es nicht darum geht, ob, sondern wann. Sind wir also vorbereitet, und was werden wir tun?"

– **Lead Architect**, Insight

Planung

Die Entwicklung eines Notfallwiederherstellungsplans ist ein kritischer und oft übersehener Teil des Ransomware-Rätsels. Von Überlegungen zur Netzwerksicherheit bis hin zu rechtlichen Auswirkungen– bewerten Sie alle potenziellen Auswirkungen eines Ransomware-Ereignisses und legen Sie einen Aktionsplan fest. Sie können mit Sicherheitsdienstleistern zusammenarbeiten, um einen maßgeschneiderten, umsetzbaren Vorfallreaktionsplan zu erstellen. Zu viele Organisationen haben begrenzte Maßnahmenpläne, die nur im Kopf bestimmter Mitarbeiter existieren. Es ist auch wichtig, dass der Plan gut dokumentiert ist und sich auf Ihr gesamtes Unternehmen erstreckt.

Tests

Genauso wichtig wie die Entwicklung eines Plans ist es, ihn zu testen. Testen Sie Ihren Plan in Ihrer aktuellen Softwareumgebung auf etwaige Mängel, passen Sie ihn bei Bedarf an, und führen Sie ihn zeitnah durch, wobei Sie ihn bei Bedarf weiter überarbeiten. Dies stellt nicht nur sicher, dass interne Teams bereit sind, im Falle eines Ereignisses schnell und effektiv zu reagieren, sondern dass Ihr Plan auf dem neuesten Stand und optimal positioniert ist, um beste Ergebnisse zu erzielen.

Bildungswesen

Laut Daten von IBM sind nur 38 % der Staats- und Kommunalverwaltungen in der Ransomware-Prävention geschult, was insbesondere angesichts des Risikos für öffentliche Organisationen besorgniserregend ist.[16]

Da menschliche Fehler an der Spitze der Ransomware-Kettenreaktion stehen, sollte man über Schulungen nicht hinwegsehen.

Alle Personen innerhalb einer Organisation sollten eine grundlegende Schulung zu Ransomware erhalten, insbesondere dazu, wie man Phishing- und Spoofing-Angriffe erkennt und meldet.

Ransomware ist bereit. Bist du es auch?

Der Ansatz jeder Organisation im Umgang mit Ransomware ist einzigartig. Eine effektive Strategie berücksichtigt mehrere Faktoren, einschließlich der Menge und Art Ihrer Daten sowie der Komplexität Ihrer IT-Infrastrukturen.

Insight kann Ihnen dabei helfen, Ihre aktuelle Sicherheitslage im Hinblick auf die wachsende Bedrohung durch Ransomware zu bewerten und gemeinsam mit Ihnen einen ganzheitlichen Ansatz für die Cybersicherheit zu entwickeln, der alle Ebenen Ihrer IT-Umgebung schützt und den spezifischen Anforderungen Ihres Unternehmens entspricht.

Wenn Sie bereit sind, über Möglichkeiten zur Verbesserung der Ransomware Readiness Ihres Unternehmens zu sprechen, kontaktieren Sie uns.

Quellen:
[1] Kassner, M. (11. Jan. 2010). Ransomware: Extortion via the Internet. TechRepublic.
[2] FBI. (25. März 2019). The Melissa Virus: An $80 Million Cyber Crime in 1999 Foreshadowed Modern Threats. FBI.gov.
[3] Bernard, Z. (10. Nov. 2018). Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator. Business Insider.
[4] Siegel, B. (10. Jan 2020). The Marriage of Data Exfiltration and Ransomware. Security Boulevard.
[5] Columbus, L. (1. Nov. 2020). What Are The Fastest Growing Cybersecurity Skills in 2021? Forbes.
[6] FBI. (2. Okt. 2019). High-Impact Ransomware Attacks Threaten U.S. Businesses And Organisations. PSA: https://www.ic3.gov/Media/Y2019/PSA191002.
[7] Robinson, T. (7. Dez. 2020). Ransomware attacks target backup systems, compromising the company 'insurance policy.' SCmagazine.com.
[8] Coveware Quarterly Ransomware Report. (3. Feb. 2021). Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021.
[9] Mutig, D. (3. Jun. 2021). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. Cybersecurity Ventures.
[10] CyberEdge Group. 2022 Cyberthreat Defense Report.
[11] Mutig, D. (3. Jun. 2021). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. Cybersecurity Ventures.
[12] Kass, D.H. (13. Jan. 2022). Supply Chain Security and Ransomware Attacks: CrowdStrike Research Findings. MSSPAlert.
[13] Gruber, D. und Lundell, B. (Feb. 2020). Ransomware Still Rampant, Fueled by Insurance Companies. Enterprise Strategy Group.
[14] Gately, E. (24. Feb. 2022). Die hohen Kosten von Ransomware. ChannelFutures.
[15] Burbidge, T. (13. Mai 2021). Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report. Verizon.
[16] The Harris Poll. (2020). Public Sector Security Research: IBM-Harris Poll Survey 2020. On behalf of IBM Security.

MKT6203_AT

© 2021, Insight Direct USA, Inc. Alle Rechte vorbehalten. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.