Quantum

EXPERTEN-GUIDE:

MIT VERHALTENSÄNDERUNGEN AUS DER RANSOMWARE-FALLE

Proaktive Maßnahmen zur Bekämpfung der Bedrohungen durch Ransomware-Attacken

INHALT

EXECUTIVE SUMMARY

Viele Organisationen sind in Sachen Cybersecurity in einen scheinbar ausweglosen Teufelskreis geraten. Schuld daran ist Ransomware. Je verzweifelter sie versuchen, eine Attacke in den Griff zu bekommen, desto tiefer wird das Loch, das sie sich selbst graben. Ransomware ist ein heimtückischer Gegner, der wie ein Löwe im hohen Gras geduldig auf sein nächstes Opfer lauert. Gemeinsam mit Malware und Phishing stellt Ransomware mittlerweile die mit Abstand größte Bedrohung für Unternehmen dar. Sie ist damit gefährlicher als Naturkatastrophen, Hardwareausfälle oder selbst eine Zero-Day-Attacke.

Die höchsten gemeldeten Ransomware-Zahlungen lagen 2019 bei über 10 Mio. US-Dollar. Für Attacken mit Ryuk-, REvil-, DoppelPaymer- und Maze-Malware wurden Lösegelder von insgesamt 75 Mio. US-Dollar gefordert.

USD	BTC	Malware
12,5 Mio. $	ca. 1.600	Ryuk
10,9 Mio. $	565	DoppelPaymer
10,0 Mio. $	1.326	REvil
9,9 Mio. $	1.250	Ryuk
6,1 Mio. $	850	Maze
6,0 Mio. $	763	REvil
5,3 Mio. $	680	Ryuk
2,9 Mio. $	375	DoppelPaymer
2,5 Mio. $	250	REvil
2,5 Mio. $	250	DoppelPaymer
2,3 Mio. $	300	Maze
1,9 Mio. $	250	DoppelPaymer
1,6 Mio. $	216	BitPaymer
1,0 Mio. $	128	Maze

Tabelle 1: Die größten gemeldeten Lösegeldforderungen im Jahr 2019. Die Lösegeldforderungen erreichten 2019 die Marke von 12,5 Mio. US-Dollar. Quelle: CrowdStrike, „2020 Global Threat Report", März 2020, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

2020 stiegen Ransomware-Zahlungen gegenüber 2019 um 311 % an.[1]

Bei einigen Ryuk-, BitPaymer- oder REvil-Attacken werden Managed Service Provider (MSPs) ins Visier genommen. Kriminelle nutzen dabei einen einzelnen Zugangspunkt, um mehrere Unternehmen mit Ransomware oder anderer Malware zu infizieren. Auf diese Weise wurden bereits kleine und große Unternehmen sowie Ämter, Schulbezirke, Bildungs- und Gesundheitseinrichtungen zu Fall gebracht. Eine Gesundheitsorganisation, bei der nach einer Ransomware-Attacke ein medizinisches Gerät ausgefallen war, musste sogar einen Todesfall vermelden.

Wie Raubtiere, die sich an das schwächste Mitglied der Herde heranpirschen, picken sich Kriminelle gezielt unterbesetzte oder überlastete Organisationen heraus. Viele davon wissen, dass sie wiederholten Angriffen ausgesetzt sein werden, weil ihnen die Möglichkeiten zu einem proaktiven Schutz fehlen. Einige Cyberkriminelle nehmen nach Art der „Großwildjäger" früher oder später große Konzerne ins Visier, suchen sich ihre Beute aber gleichzeitig auch immer wieder unter kleinen und mittelständischen Unternehmen.

[1] „Chainalysis 2021 Crypto Crime Report"

In der freien Wildbahn reagiert selbst das kleinste und wehrloseste Opfer auf Jäger, indem es wegläuft und sich versteckt. Kein Tier ergibt sich freiwillig seinem Schicksal, und auch Organisationen sollten sich nicht einfach mit der allgegenwärtigen Ransomware-Gefahr abfinden. Sie müssen lernen, ihren wichtigsten Besitz zu schützen: ihre Daten.

Zusätzlich erschwert wird die Situation für betroffene Unternehmen durch den immer heimtückischeren Charakter der Attacken. Leider sind Ransomware-Angriffe extrem lukrativ und äußerst gut finanziert.

Es ist an der Zeit, dass Organisationen diese Entwicklung umkehren. Dieser Leitfaden beleuchtet aktuelle Verfahren und Verhaltensweisen, mit denen Organisationen das Risiko eines Angriffs minimieren und sich aus diesem Dilemma befreien können.

ANGRIFFSPUNKTE FÜR KRIMINELLE UND RANSOMWARE

Welche Einfallstore sind in den Unternehmen am gefährdetsten? Cyberkriminelle arbeiten mit vielen Angriffsvektoren, und der Malware-Stamm, den die Kriminellen freisetzen, entscheidet über den verwendeten Vektor. Phishing-E-Mails waren oft die Hauptverbreitungsvektoren. Man braucht dafür kein Expertenwissen, und Menschen sind leichter zu täuschen als Maschinen oder Netzwerke.

Seit COVID-19 und dem damit verbundenen Anstieg der Remote-Arbeit gewinnen RDP (Remote Desktop Protocol) oder SMB (Server Message Block) als internetbasierte Angriffsvektoren an Bedeutung. Einige Angreifer geben sich auch als Windows Shared Service Host aus, um unerkannt zu bleiben.

Egal, zu welcher Methode sie greifen: Die Kriminellen gehen mit Geduld, Ausdauer und äußerster Fokussierung vor, um ihr Ziel – sei es finanzieller oder politischer Natur – zu erreichen. Sie arbeiten im gesamten Prozess mit Verschlüsselungs- und Maskierungstechniken, um nicht entdeckt zu werden, und stehlen mitunter auch Daten als zusätzliches Erpressungsmittel.

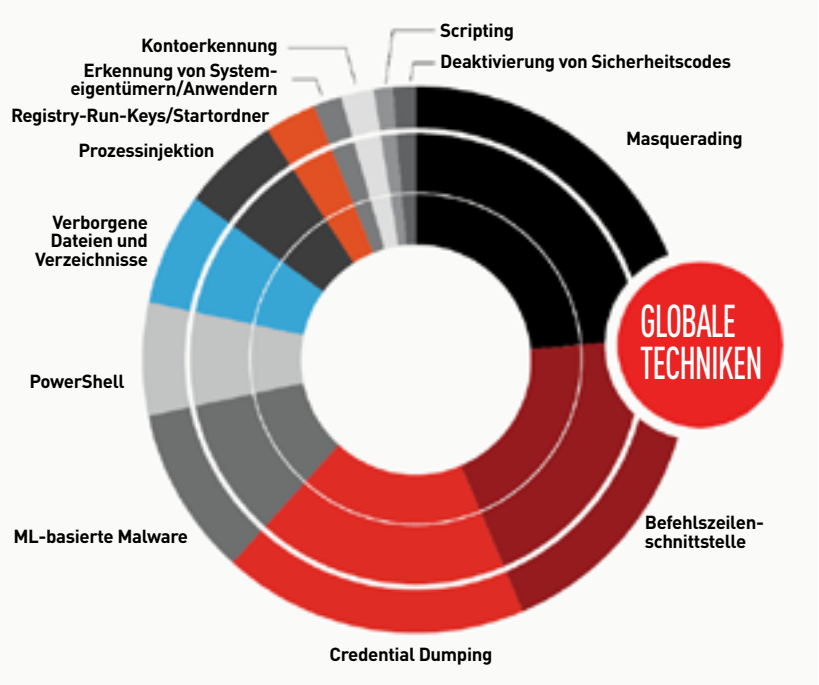

Abb. 1: Tools, Taktiken und Prozesse von Angreifern im Jahr 2019. Cyberkriminelle gehen nach unterschiedlichen Taktiken vor. Quelle: CrowdStrike, „2020 Global Threat Report", März 2020, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf.

AKTUELLE METHODEN UND VERHALTENSWEISEN VON CYBERKRIMINELLEN

Nicht selten spionieren Angreifer ein Netzwerk monatelang heimlich aus. Im Fall eines Hollywood-Studios blieben sie 2016 sogar über ein Jahr unentdeckt. Einmal eingedrungen, bewegen sie sich maskiert und unerkannt im Netzwerk und deaktivieren, verschlüsseln, extrahieren oder zerstören Daten und Systeme.

Zurzeit sind mehrere Ransomware-Typen und -Strategien in Umlauf, die besonderen Anlass zur Sorge geben. Das datenverschlüsselnde Virus REvil wurde z. B. erstmals im April 2019 von Sicherheitsforschern der Cisco Talos Intelligence Group entdeckt und ist auch unter dem Namen Sodinokibi/Sodin bekannt. Über Zero-Day-Lücken können Angreifer remote per HTTP auf Oracle WebLogic-Server zugreifen und Malware manuell einschleusen.[2] Soweit bekannt, gibt es für diesen raffinierten Schadcode derzeit keine Entschlüsselungstools. Zur Wiederherstellung der Daten werden also Alternativen benötigt.

Geschäftsmodell einiger Malware-Entwickler ist Ransomware-as-a-Service. Sie verkaufen die Schadsoftware als Dienst, sodass selbst Kleinkriminelle ohne den technischen Background im großen Stil Unternehmen und Privatpersonen angreifen können. Bei diesen Geschäften erhält der Entwickler einen Teil der erbeuteten Summe. Um RaaS-basierte Malware-Familien wie REvil zu installieren, nutzen Cyberkriminelle meist RDP. Zu den Angriffszielen gehören kleine und mittelständische Unternehmen ebenso wie Fortune 500-Konzerne aus allen Sektoren. Die Lösegeldforderungen bei einer REvil-Attacke liegen im Durchschnitt im zweistelligen Millionenbereich. 2020 wurden deutlich höhere Summen gefordert als noch 2019.

Ransomware-Betreiber sind kriminell, aber auch professionell aufgestellt, gut finanziert und hervorragend organisiert. Sie werben oft Personen mit Erfahrung in Unternehmensnetzwerken an, und richten teilweise sogar Helpdesks im Darknet ein, um die Erfolgsquote der Attacken zu erhöhen. Diese Angreifer gehen mit äußerster Entschlossenheit vor – und wenn sie Ihre Sicherheitssoftware erst einmal umgangen haben, bleibt als letzte Verteidigungslinie nur noch Ihr Backup.

Cybersecurity-Anbieter betonen, wie wichtig es ist, die Vorgehensweise von Cyberkriminellen zu verstehen. Bewaffnet mit diesem Wissen können Netzwerkbetreiber oder Sicherheitsbeauftragte geeignete Maßnahmen ergreifen, um Angreifer davon abzuhalten, bösartige Skripts auszuführen und sich Zugriffsberechtigungen auf die Sicherheitssoftware oder das Betriebssystem zu verschaffen.

Wenn die Kriminellen Ihre Daten erst einmal gestohlen oder verschlüsselt haben, drohen Lösegeldforderungen von mehreren Hunderttausend US-Dollar bis zu zweistelligen Millionenbeträgen. Eine gute Cybersecurity-Software kann die meisten Angriffe abwehren. Tatsächlich wird ein Großteil der Malware entdeckt. Das Beispiel REvil zeigt aber, dass ihre Erkennung und die Behebung der Folgen immer schwieriger wird. Das gilt insbesondere, wenn Edge-Daten betroffen sind. Der Grund dafür liegt in der Regel in menschlichem Versagen. Kriminellen bietet sich hier eine lukrative Einnahmequelle. Deshalb schließen viele Unternehmen eine Cyberversicherung ab, die für die Kosten aufkommt.

Eine renommierte Cybersecurity-Software kann dazu beitragen, kriminelle Angreifer abzuwehren. Damit ist aber erst die Hälfte gewonnen. Ebenso wichtig ist Ihre Backup-Umgebung.

[2] 2-Spyware, „Remove REvil ransomware (Removal Instructions) - Recovery Instructions Included", https://www.2-spyware.com/remove-revil-ransomware.html.

WARUM ORGANISATIONEN ZAHLEN

Auf jeden Ransomware-Angriff, über den berichtet wird, kommen Hunderte andere, die niemals an die Öffentlichkeit gelangen. Leider gilt es nach wie vor als Stigma, Opfer einer Ransomware-Attacke zu werden. Das ist nicht weiter verwunderlich, denn das betroffene Unternehmen gerät häufig mit all seinen Schwachstellen ins Licht der Öffentlichkeit. Viele Organisationen verschweigen Angriffe lieber, sodass diese ungemeldet bleiben. In der Regel hören wir von einer Handvoll Angriffe pro Woche. Hinzu kommen aber viele weitere Unternehmen, die im Stillen die geforderten Summen zahlen. Eine wachsende Zahl an Organisationen bezahlt Lösegelder, um wieder Zugang zu ihren Daten zu erhalten: 2020 waren es 58 % der Ransomware-Opfer, die zahlten, gegenüber 45 % im Jahr 2019 und 39 % im Jahr 2018.[3]

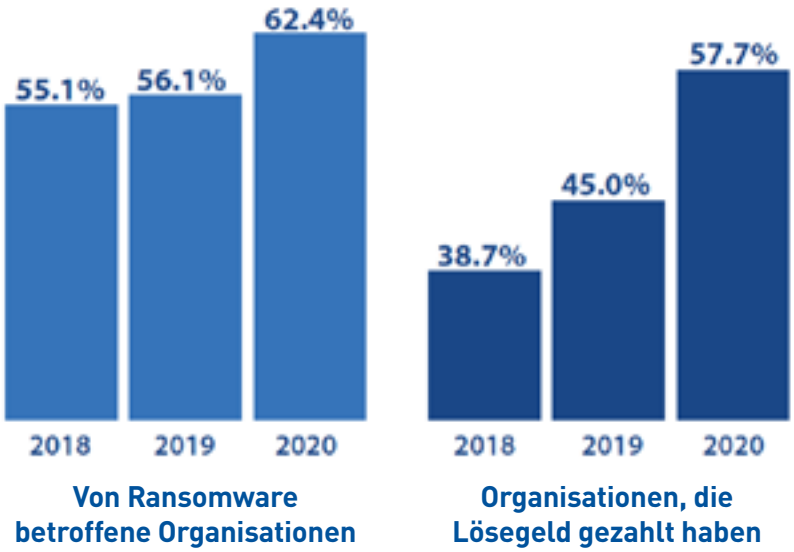

Abb. 2: Immer mehr Organisationen werden Opfer von Ransomware und zahlen das geforderte Lösegeld. Quelle: CyberEdge Group, „2020 Cyberthreat Defense Report", März 2020, https://media.bitpipe.com/io_15x/io_152789/item_2193329/ar-cyberedge-2020-cdr-report.pdf.

Je größer die Aussicht auf Zahlungen, desto häufiger und gefährlicher auch die Ransomware-Angriffe. Cyberkriminelle haben verschiedene RaaS-Varianten entwickelt und schrauben ihre Forderungen immer weiter in die Höhe.

Haben Unternehmen bewusst die Augen vor einer rasant wachsenden Bedrohung verschlossen? Vermutlich nicht – es scheint aber so, als wären sie nur als passive Zuschauer an dieser Ransomware-Schlacht beteiligt. Da ihnen die nötigen Einblicke zur Vorgehensweise der Cyberkriminellen fehlen, haben sie sich allein auf die Frage konzentriert, ob sie zahlen sollen oder nicht. Gleichzeitig wurden in den letzten fünf Jahren vielerorts die IT-Ausgaben zur Datensicherung zusammengestrichen.

Viele Organisationen vernachlässigen ihre Sicherheitsrichtlinien und Backup-Strategien. So haben Diebe leichtes Spiel, wenn es darum geht, Lösegeld für Daten zu erpressen. Den Organisationen bleibt keine andere Wahl als zu zahlen. Einziges Ziel dieser Unternehmen ist es, ihre Daten wiederherzustellen und zum normalen Betrieb zurückzukehren. Sie setzen daher oft auf den Abschluss einer Cyberversicherung, unter deren Schirm die Zahlungen ausgehandelt werden, sodass im Anschluss die regulären Abläufe wieder etabliert werden können.

Eine erfolgreiche Attacke bedeutet Ausfallzeiten, Umsatzeinbußen in Millionenhöhe und einen erheblichen Imageverlust. Es ist dringend nötig, der Stigmatisierung von Ransomware-Angriffen ein Ende zu bereiten. IT-Experten müssen das Thema Cybersecurity proaktiv angehen und die Verteidigungsmechanismen stufenweise betrachten und analysieren.

IT-Experten müssen das Thema Cybersecurity proaktiv angehen und die Verteidigungsmechanismen stufenweise betrachten und analysieren.

[3] CyberEdge Group, „2020 Cyberthreat Defense Report", März 2020, https://media.bitpipe.com/io_15x/io_152789/item_2193329/ar-cyberedge-2020-cdr-report.pdf.

WARUM ORGANISATIONEN NICHT ZAHLEN SOLLTEN

Stellen Sie sich das folgende Szenario vor: Mit knappen Budgets und IT-Prioritäten, die seit COVID-19 auf der Aufrechterhaltung der Betriebskontinuität liegen, geben IT-Experten und Sicherheitsteams weiterhin alles, um die Netzwerkintegrität Ihrer Organisation zu gewährleisten. Das Rechenzentrum soll vor jeder Art von Attacke geschützt sein, auch bei einem akuten Mangel an IT-Sicherheitsexperten.

Sie haben Cybersecurity-Software installiert (einschließlich Software, die Zero-Trust-Architekturen unterstützt), eine Cyberversicherung in Ihre Datenschutzstrategie eingebunden sowie solide Richtlinien und Verfahren für Daten-Backups implementiert. Sie unternehmen alles in Ihrer Macht Stehende, um Schwachstellen und Sicherheitslücken in Ihren Server- und Netzwerkverbindungen auszuschließen. Trotzdem hängt die Gefahr eines Datenverlusts oder -diebstahls wie ein Damoklesschwert über dem Netzwerk.

Auch größte Anstrengungen können nicht verhindern, dass Daten gefährdet sind – einfach deshalb, weil über das Netzwerk darauf zugegriffen werden kann. Das Netzwerk sperrt Sie aus und versetzt Sie in eine hilflose Lage. Ohne Ihr Wissen wird ein Befehl abgesetzt und mit dem heimlichen Exportieren und Löschen oder Verschlüsseln Ihrer Backup-Daten begonnen.

Was können Sie tun? Die Antwort hängt vom jeweiligen Unternehmen ab. Sobald Sie aber Lösegeld zahlen, signalisieren Sie den Kriminellen, dass sie freie Hand haben. Das Risiko, Opfer einer weiteren Attacke zu werden, steigt erheblich.

Organisationen dürfen Ransomware-Erpressern nicht länger nachgeben und die gestellten Forderungen aus ihrer Cyberversicherung bezahlen. Häufig führt die Zahlung des Lösegelds ohnehin nicht zum gewünschten Ergebnis. Nur 66,9 % der Unternehmen, die 2020 Lösegeld bezahlten, erhielten ihre Daten zurück. Von denen, die nicht zahlten, gelang es 84,5 %, die Daten wiederherzustellen.[4] Die Chancen stehen also besser, wenn kein Lösegeld bezahlt wird.

Die US-amerikanische Regierung versucht, Lösegeldzahlungen durch Unternehmen zu unterbinden. Das US-Finanzministerium hat Versicherer darüber informiert, dass sie Sanktionen riskieren, wenn sie Lösegeldzahlungen im Namen von Ransomware-Opfern leisten.[5] Anders gesagt: Wer durch Lösegeld eine auf der Blacklist geführte terroristische Organisation finanziert, wird bestraft. Einige Organisationen haben sogar dazu aufgerufen, Ransomware-Zahlungen für illegal zu erklären. Solche Entwicklungen könnten dazu beitragen, Unternehmen aus dem Teufelskreis zu befreien, in dem Lösegeldzahlungen weitere kriminelle Aktivitäten finanzieren.

Organisationen dürfen Ransomware-Erpressern nicht länger nachgeben und die gestellten Forderungen aus ihrer Cyberversicherung bezahlen.

ERARBEITUNG EINER STRATEGIE ZUR BEKÄMPFUNG VON RANSOMWARE

Was unternehmen Firmen, um gegen die Flut an Ransomware vorzugehen? IT-Sicherheitsexperten haben in dieser Hinsicht bereits einige Erfolge erzielt. Doch weitere Schritte sind nötig. Im Rahmen eines Cybersecurity-Berichts wurden interne Verfahren und Sicherheitsinvestitionen von Unternehmen aus mehreren Branchen verglichen. Als größte Hürden bei der Etablierung wirksamer Verteidigungsmaßnahmen konstatiert der Bericht (a) den Mangel an qualifizierten IT-Sicherheitsexperten und (b) das fehlende Sicherheitsbewusstsein unter Mitarbeitern.[6] Dass das größte Problem bei den Mitarbeitern liegt, ist nicht weiter überraschend. Was aber lässt sich dagegen tun? Wie können Organisationen einerseits die Gefahr von Sanktionen minimieren und andererseits die Verhaltensweisen abstellen, die erfolgreiche Cyberattacken begünstigen?

[4] Security, „End the vicious ransomware cycle", 4. Dezember 2020, https://www.securitymagazine.com/blogs/14-security-blog/post/94085-end-the-vicious-ransomware-cycle.

[5] US-Finanzministerium, „Ransomware Advisory", 1. Oktober 2020, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001.

[6] Security, „The Top Five Cybersecurity Defense Insights for 2020", 12. Juni 2020, https://www.securitymagazine.com/articles/92582-the-top-five-cybersecurity-defense-insights-for-2020.

Unternehmen müssen proaktiv gegen die Attacken vorgehen und einen robusten Datenschutzplan erstellen. Einfach weiter auf eine vorhandene Backup-Infrastruktur zu setzen, reicht nicht mehr aus. Ein Backup- und Recovery-Plan ist ein organisches Gebilde, das sich im Lauf der Zeit weiterentwickelt und regelmäßig an Ihre Technologie und die aktuellen Speicherplattformen angepasst werden muss.

10 Richtlinien zur Sicherung aller Einfallstore

Die folgenden zehn Richtlinien erleichtern Ihnen den Einstieg in einen besseren Schutz Ihres Unternehmens und seiner Daten. Ziel muss es sein, alle denkbaren offenen Flanken des Netzwerks und der Backup-Umgebung zu sichern:

1. Formulieren Sie eine gut überlegte Strategie zur Datensicherung.
2. Stellen Sie den Plan Ihren Vorgesetzten vor, um deren Zustimmung und Unterstützung zu erhalten.
3. Installieren Sie eine Antivirussoftware, um die Vordertür zum Netzwerk zu schließen.
4. Nutzen Sie Verschlüsselungstechnologie in jeder Phase des Datenlebenszyklus – bei der Speicherung, während der Übertragung und bei der aktiven Nutzung.
5. Bieten Sie Sicherheitsschulungen an, und fördern Sie das Sicherheitsbewusstsein der Mitarbeiter.
6. Implementieren Sie lokale Disk-Backups mit Objektsperre, um die schnelle lokale Wiederherstellbarkeit zu gewährleisten und Ihre RPO/RTO-Vorgaben zu erfüllen.
7. Stellen Sie kosteneffiziente Archivierungslösungen mit „Air Gap" bereit, die einen zeitlich unbegrenzten Schutz Ihrer Daten ermöglichen.
8. Replizieren Sie die Daten für DR-Zwecke mithilfe einer Cloud- oder Object Storage-basierten Lösung an einen externen Standort.
9. Implementieren Sie eine Tape-Lösung als lokalen „Air-Gap"-Schutz für Ihre Backups oder Archive.
10. Schließen Sie als letzten Ausweg eine Cyberversicherung ab.

AUSWAHL SICHERER PLATTFORMEN FÜR IHRE DATEN UND IMPLEMENTIERUNG EINER BACKUP-STRATEGIE

Die Sicherheit gehört zu den wichtigsten Aspekten bei der Auswahl einer Datenspeicherplattform. Wenn Sie die Public Cloud nutzen oder Ihre Workloads über mehrere Clouds und Rechenumgebungen verteilt sind, benötigen Sie über die Schutzeinstellungen in Ihrem eigenen Netzwerk hinaus zusätzliche Datenschutz- und Sicherheitsmaßnahmen. Sie brauchen einen umfassenden Ansatz, an dem mehrere Abteilungen, einschließlich Sicherheitsexperten, Netzwerkadministratoren und deren Vorgesetzte, mitwirken. Schulen Sie sich und Ihre Anwender, insbesondere, wenn die Belegschaft remote arbeitet.

1. Identifizieren Sie potenzielle Schwachstellen.
2. Implementieren Sie eine renommierte Antivirussoftware. Dieser Punkt sollte nicht verhandelbar sein.
3. Erstellen Sie Backups.
4. Bewahren Sie Offline-Kopien der Daten auf (wie vom FBI, der CISA und dem NCSC UK empfohlen).
5. Prüfen Sie, ob Disk, Tape (lokal oder als Cold Storage in der Cloud) oder Cloud/Object Storage die beste Recovery-Methode für Ihre Organisation darstellt.

Sicherung des Vordereingangs zu Ihrem Netzwerk

Der Schutz Ihrer Daten vor Cyberattacken beginnt mit dem Offensichtlichen. Sichern Sie die Haupteinstiegspunkte zum Netzwerk. Prüfen Sie, ob Backup-Software und -Ziele die nötigen Voraussetzungen erfüllen, um Ihre RPO- und RTO-Vorgaben zu erfüllen und die Sicherheit Ihrer Daten zu gewährleisten. Wenn Ihre Backup-Software keinen Schutz vor Ransomware bietet, ist sie vielleicht nicht die richtige Lösung für Sie.

Auswahl einer Datenspeicherlösung

Welche Datenspeicherplattform ist die richtige für Sie?

- Der Vorteil von NAS-Lösungen liegt (je nach SLAs) in der schnellen Wiederherstellung. Allerdings bleiben die Daten dabei immer online. Angetrieben durch die Aussicht auf profitable Beute dürfte es nur eine Frage der Zeit sein, bis Kriminelle eine Möglichkeit finden, den operativen „Air-Gap"-Schutz (also die Lücke zwischen Produktionsspeicher und unerreichbarem Speicher) zu überwinden. Viele Anbieter wenden unterschiedliche Methoden an, um die Objekte oder Dateien in den Systemen „einzusperren". Da die Daten aber immer online sind, lässt sich das Risiko nicht komplett ausschließen. Letztlich lassen sich die Daten nach einem Angriff aber mit dieser Verteidigungsmethode am schnellsten wiederherstellen.
- Tape bietet einen physischen „Air Gap"-Schutz. Die Daten sind vor Ransomware sicher, da Viren die physische Barriere zwischen den Daten und dem Netzwerk nicht überwinden können. Tape spielt eine zentrale Rolle, wenn es um die kostengünstige langfristige Archivierung von Daten zum Schutz vor Ransomware geht.
- Object Storage verteilt die Daten auf mehrere Nodes und sperrt sie, sodass keine Änderungen möglich sind. Je nach der gewählten Lösung und den definierten Richtlinien können Object Storage-Daten auch nach dem Ausfall einzelner oder mehrerer Nodes wiederhergestellt werden.

Abb. 3: Bei der Auswahl einer Datenspeicherplattform sollte die Wiederherstellung zu den wichtigsten Aspekten gehören.

Finanzielle Überlegungen

Jede Lösung hat ihre Vor- und Nachteile. Überlegen Sie, was Ihr Budget zulässt, und arbeiten Sie ein Szenario und einen Plan aus. Denken Sie daran, dass Ihr Netzwerk nur so stark ist wie das schwächste Glied. Beginnen wir mit der kostengünstigsten Option mit „Air Gap".

- **Tape:** Tape erfordert den geringsten Anschaffungsaufwand und stellt eine solide Lösung mit „Air Gap"-Schutz dar, da die Daten von Haus aus vom Netzwerk getrennt sind.
- **Disk:** Disk-Lösungen haben keinen echten „Air Gap"-Schutz – auch wenn sie das manchmal behaupten. Einige Lösungen verfügen über Sperrmechanismen, bei denen sozusagen die Tür zu den auf Disk geschriebenen Daten abgeschlossen wird. Allerdings wirken sich solche Funktionen drastisch auf den Preis aus.

Die Lösungsanbieter können Ihnen dabei helfen, die für den Schutz Ihres Netzwerks optimale Methode zu ermitteln. Letzten Endes müssen Sie aber selbst entscheiden, welche Lösung die beste und kosteneffizienteste für Ihre Organisation und das vorhandene Skillset ist.

Backups für Ihr Backup – Datensicherung nach dem „3-2-1-1"-Prinzip

Um künftig kein Lösegeld mehr zahlen zu müssen, sollten Sie auch ein Backup Ihres Backups erwägen. Kriminelle haben Zugang zu schier unbeschränkten finanziellen Mitteln. Es ist nur eine Frage der Zeit, bis sie ein Netzwerk in Ihrer Nähe ins Visier nehmen. Sie haben das Geld, um in die Überwindung der neuesten Patches zu investieren, und werden einen viralen Cocktail erstellen, mit dem sie sich Zugang zu jeder aktuellen Online-Lösung verschaffen.

Als robuste Strategie zur Datensicherung empfiehlt sich die Backup-Erstellung nach dem „3-2-1-1"-Prinzip. Diese sieht vor, 3 Kopien Ihrer Daten auf 2 unterschiedlichen Medienformaten aufzubewahren sowie 1 Kopie extern vorzuhalten und 1 Kopie offline. Dieser Ansatz ähnelt der „1-10-60"-Regel, nach der Sicherheitsteams Bedrohungen in der ersten Minute erkennen, die Bedrohung innerhalb von 10 Minuten verstehen und dann innerhalb von 60 Minuten darauf reagieren sollen. In beiden Fällen wird eine proaktive Strategie benötigt, um akuten Bedrohungen einen Schritt voraus zu sein.

Vorausplanung für die Remote-Arbeit

Sie müssen sich darüber klar sein, dass einige Attacken über die Hintertür erfolgen und Angreifer sich per Remote-Zugriff oder über Einstiegspunkte Zugang zum Netzwerk verschaffen. Bevor sie mehr Mitarbeitern die Arbeit im Homeoffice gestatten, sollten Organisationen Prozesse und Richtlinien implementieren, die potenzielle Sicherheitsschwachstellen adressieren. Das Risiko ist zu groß, um sich damit erst im Krisenmodus zu beschäftigen. Die folgenden Best Practices haben sich bewährt:

- **Daten verschlüsseln:** Beim Remote-Zugriff über Ihr WAN sollten Daten stets verschlüsselt sein. Das gilt für aktive Daten, gespeicherte Daten und vor allem für übertragene Daten.
- **Ausreichende Sicherheit beim Cloud-Zugriff gewährleisten:** Beim Zugriff auf Daten in der Public Cloud stellen sich eigene Sicherheitsprobleme, die adressiert werden müssen. Die zusätzliche Schutzebene zur weiteren Sicherung von Datenworkflows in der Public Cloud steckt aber noch in ihren Anfängen.
- **Die richtige Mentalität schaffen:** Die Verteidigung Ihres Netzwerks oder Rechenzentrums erfordert die richtige Einstellung. Verhandlungen mit Erpressern sind ebenso tabu wie Lösegeldzahlungen.

Natürlich können Sie in Sachen Lösegeld nur standhaft bleiben, wenn Sie Ihre Daten außerhalb des Netzwerks gesichert haben – sei es offline oder durch Segmentierung des Netzwerks. Wenn Sie über ausreichende Backups verfügen, können Sie Server und Daten aus den gesicherten BS-Images wiederherstellen. Allerdings sollten Sie dabei auf Vergeltungsmaßnahmen gefasst sein. Als sich in einem kürzlichen Fall ein Softwareunternehmen weigerte, ein hohes Lösegeld zu zahlen, veröffentlichten die Kriminellen private Informationen im Darknet.

Wenn Sie sich allein auf Ihre Antivirussoftware und die Übernahme des Lösegelds durch Ihre Cyberversicherung verlassen, nehmen Sie eine große Lücke in Ihrer Schutzstrategie in Kauf, die Sie unter Umständen teuer zu stehen kommt. Der Rückgriff auf die Versicherung sollte immer nur den allerletzten Ausweg darstellen.

GEMEINSAM GEGEN DEN DIEBSTAHL

Ähnlich wie der Klimaschutz erfordert auch der Kampf gegen Ransomware die Mitwirkung aller Beteiligten. In den nächsten fünf bis zehn Jahren müssen wir uns gemeinsam dafür engagieren, die Cyberwelt zu schützen, und Unternehmen jeder Größe die Möglichkeit geben, solide proaktive (und möglichst auch kosteneffiziente) Strategien und Richtlinien zu implementieren.

Bei der Navigation durch die trüben Gewässer der Cyberwelt können wir uns auf umfassende Daten von Cybersecurity-Unternehmen stützen. Wir wissen, wie die Kriminellen arbeiten und nach welchen Methoden sie vorgehen. Je raffinierter sie ihre Angriffe gestalten, desto dringender benötigen wir Technologien wie maschinelles Lernen (ML) oder künstliche Intelligenz (KI), um ihnen mithilfe fortschrittlicher Sicherheitsanalysen den entscheidenden Schritt voraus zu bleiben.

Risikominderung setzt mehrere Technologien voraus. Eine Absicherung gegen Ransomware muss aus mehreren Ebenen bestehen.

Natürlich erfordert eine solche Risikominderung den Einsatz mehrerer Technologien. Es gibt keine einzelne Lösung, die einen ausreichenden Schutz gegen die Wucht der Attacken bieten kann. Eine Absicherung gegen Ransomware muss aus mehreren Ebenen bestehen.

Parallel dazu benötigen wir zur Eindämmung dieser Machenschaften auch veränderte Prozesse und Einstellungen. Viele IT-Experten werden ihre Ansichten über bestimmte Technologien oder Backup-Methoden überdenken müssen. Auch Investitionen in Schulungen sind unumgänglich. Und weil es sich bei diesen Angriffen längst nicht mehr um isolierte Einzelfälle handelt, kann nicht länger jeder für sich allein dagegen ankämpfen. Wir müssen das Wissen über unsere unerfreulichen Ransomware-Erfahrungen dokumentieren und weitergeben, um gemeinsam den Ausweg aus dieser Cyberkrise zu finden.

Wie schon angesprochen, sollten IT-Profis auch jede Verhandlung mit Kriminellen verweigern. Die Weiterführung des Status quo bewirkt nur, dass sich die kriminellen Aktivitäten zu einer Milliardenindustrie auswachsen. Es gibt bessere Methoden als den Dieb für etwas zu bezahlen, das einem rechtmäßig gehört.

Lassen Sie sich auch nicht von Berichten täuschen, nach denen einige Ransomware-Familien den Betrieb einstellen. Diese Kriminellen schließen sich sehr wahrscheinlich mit anderen Familien zusammen und werden künftig unter neuem Namen noch mächtiger sein als bisher. In den letzten Jahren haben wir auf bittere Weise lernen müssen, dass Kriminelle über einen langen Atem verfügen. Solange es keine Verhaltensänderung in den Organisationen gibt, wird das Volumen der Lösegeldzahlungen weiter in hoher Geschwindigkeit steigen. Alle Untersuchungen weisen darauf hin, dass wir mit noch aggressiverer Cyberspionage und heimtückischeren Angriffen rechnen müssen, bei denen die verhaltensbasierten Algorithmen der Cybersoftware-Unternehmen umgangen werden.

Gemeinsam können wir unsere Unternehmen schützen. Auch wenn die Anzahl der Attacken gegenüber dem Vorjahr weiter angestiegen ist, können wir schon mit kleinen Schritten große Erfolge erzielen. Der erste Schritt ist dabei immer der schwerste. Auf lange Sicht kann es uns aber gelingen, die kriminellen Banden in die Knie zu zwingen und den Teufelskreis zu durchbrechen, der uns dazu zwingt, ihre Machenschaften mit Lösegeldzahlungen zu finanzieren.

Weitere Informationen zu Ransomware und Maßnahmen zur Minderung der Bedrohung bietet der Ransomware-Leitfaden der U.S. Cybersecurity and Infrastructure Security Agency (CISA):
https://www.cisa.gov/publication/ransomware-guide

NÄCHSTE SCHRITTE

Informieren Sie sich über die Ransomware-Lösungen von Quantum, mit denen Sie verlässliche, sichere Methoden zur Offline- oder „Air Gap"-Speicherung Ihrer Daten implementieren können:
https://www.quantum.com/de/solution/ransomware-recovery/

Quantum®

ÜBER QUANTUM

Quantum Technologien und Services helfen Kunden bei der Erfassung, Erstellung und gemeinsamen Nutzung von digitalen Inhalten – sowie deren Vorhaltung und Sicherung für Jahrzehnte bei minimalen Kosten. Die Plattformen von Quantum liefern die schnellste Performance für hochauflösende Videos, Bilder und industrielles IoT und umfassen Lösungen für jede Phase im Datenlebenszyklus – vom hochperformanten Ingest über Echtzeit-Zusammenarbeit und -Analyse bis zur kostengünstigen Archivierung. Führende Unterhaltungskonzerne, Wissenschaftler, Behörden, Unternehmen und Cloud-Anbieter aus aller Welt setzen täglich auf Quantum, um die Welt zu einem freundlicheren, sichereren und intelligenteren Ort zu machen. Weitere Informationen erhalten Sie unter **www.quantum.com/de**.

www.quantum.com/de • + 49 (0)89 94303-0

WP00263G-v01 Feb 2021