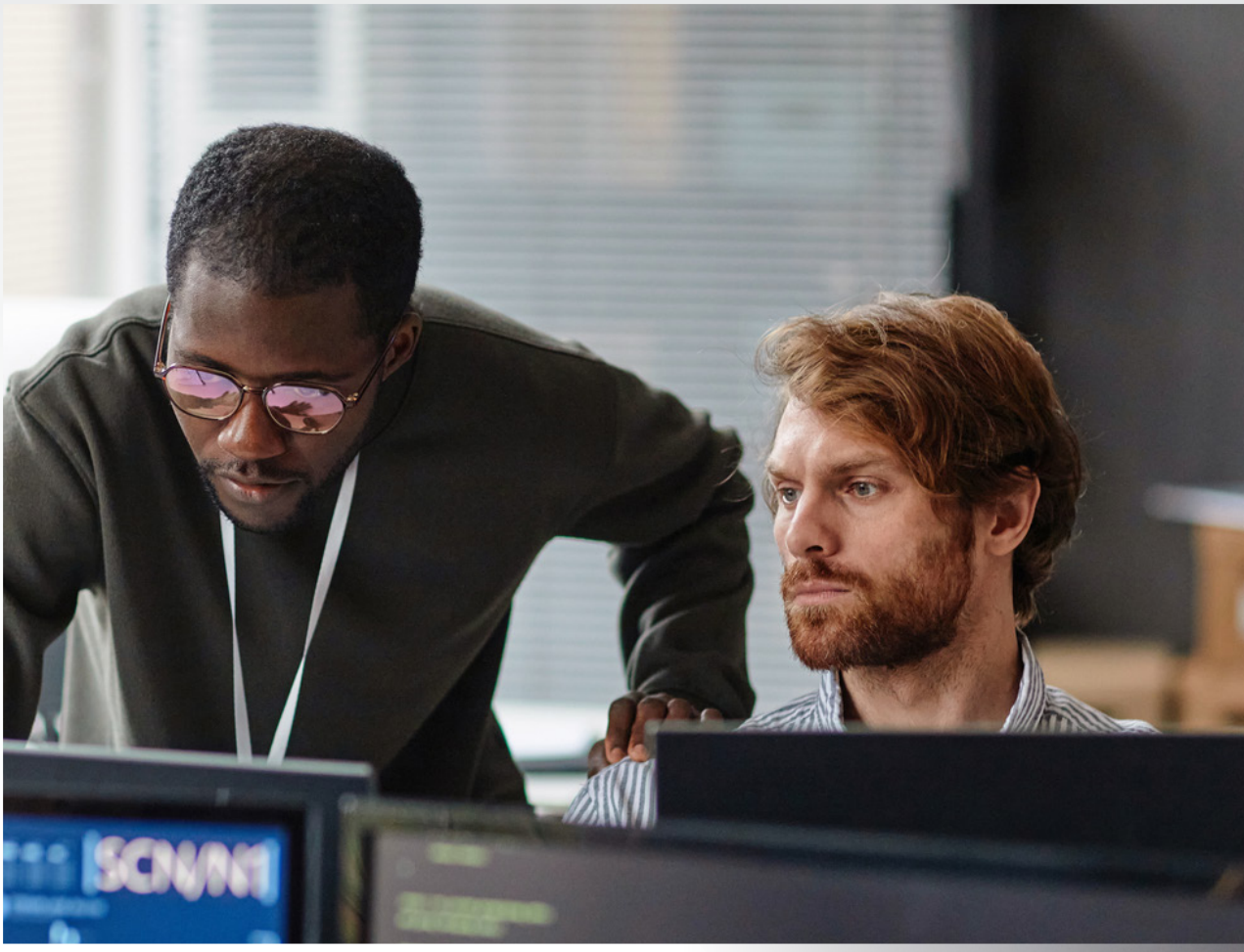
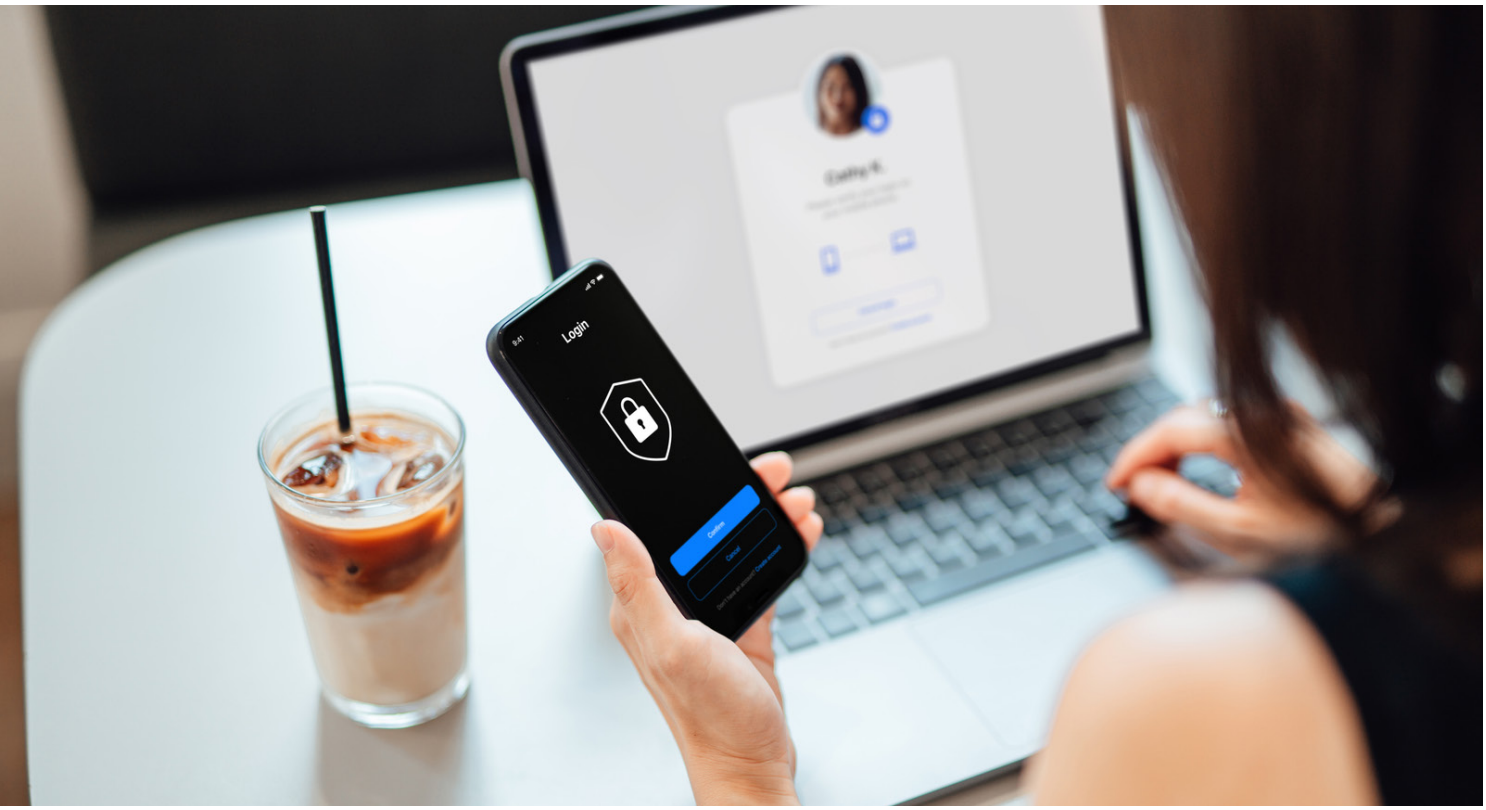


Ransomware ist auf dem Vormarsch, und Unternehmen brauchen neue Strategien für intelligente Schutzmaßnahmen und eine schnelle Wiederherstellung

Experten raten zunehmend zu einem Fokus auf Schadensbegrenzung statt einer narrensicheren Erkennung.



Ransomware ist wieder da!

Unternehmen und Privatpersonen konnten gleichermaßen aufatmen, als Ransomware-Angriffe im Jahr 2022 im Vergleich zu Ende 2021 deutlich zurückgingen. Doch leider hat sich der Trend seitdem umgekehrt: Die Zahl der Ransomware-Angriffe steigt wieder und hat im zweiten Quartal 2023 mit einer Zunahme von 72 % gegenüber dem Vorjahresstand sogar ein Allzeithoch erreicht.[1]

„Wir erleben dieses Jahr einen erheblichen Anstieg von Ransomware, und ich rechne damit, dass sich dies bis weit in das Jahr 2024 fortsetzen wird", sagt Chris Rogers, Senior Technology Evangelist bei HPE Zerto Software

Dieses Wiederaufleben ist zu einem nicht unerheblichen Teil auf den Aufstieg der künstlichen Intelligenz zurückzuführen. Die Zeiten offensichtlicher Phishing-Nachrichten voller Grammatikfehler und schlechter Bilder sind vorbei. Die KI-generierten Phishing-Angriffe von heute sind deutlich ausgeklügelter und sehen immer echter aus.

„Man kann eine Rohfassung einer E-Mail durch KI bearbeiten lassen und bekommt eine aufpolierte E-Mail ohne jegliche Grammatik- oder Rechtschreibfehler und mit dem richtigen Branding", sagt Rogers. „Am Ende sieht sie einer E-Mail eines seriösen Unternehmens zum Verwechseln ähnlich." Natürlich wird auch jede E-Mail für jeden Empfänger personalisiert, was sie noch schwieriger zu erkennen macht.

Rogers fügt an, dass KI auch eine völlig neue Art von Angriff möglich macht: Deepfakes menschlicher Stimmen. Beispielsweise könnte Ihr Vorgesetzter Sie anrufen und anweisen, Geld vom Firmenkonto abzuheben oder 100 Gutscheine zu kaufen, die Angestellten als Feiertagsbonus geschenkt werden sollen. Allerdings ist die Stimme nur eine Computersimulation, die darauf trainiert wurde, das genaue Sprechmuster Ihres Vorgesetzten auf Basis eines öffentlich zugänglichen YouTube™-Webinars, an dem er teilgenommen hat, nachzuahmen.

Rogers meint, man müsse auf jeden Fall besorgt sein, er fügt jedoch hinzu, dass er in den vergangenen Monaten eine deutliche Änderung der Einstellung bei Kunden, Partnern und Interessenten wahrgenommen habe. „Die meisten wurden entweder überhaupt nicht angegriffen oder gaben an, dass ein Angriff, den sie erlebt haben, nicht so schlimm war wie erwartet", sagt Rogers. Das bedeutet, dass viele möglicherweise vorzeitig unachtsam werden.

[1] „Q2 Ransomware Report: Global Attacks At All-Time High", Corvus, 31. Juli 2023

„Die Menschen glauben, dass sie in Sachen Cybersicherheit alles richtig machen, obwohl die Statistiken ganz klar darauf schließen lassen, dass die meisten Unternehmen einen Angriff erleiden werden – und dass dieser Angriff irgendwann auch Erfolg haben wird."

Die Aussage ist ganz klar: Sicherheitsvorkehrungen sind nach wie vor wichtig.

Neue Ratschläge zur Modernisierung Ihrer Sicherheitsvorkehrungen

Was können Sie angesichts der bedrohlichen Aussichten auf Ransomware und sonstige Angriffe tun, um sich auf künftige Angriffe vorzubereiten und sich dagegen zu schützen?

Laut Rogers finden die besten Ratschläge aus den vergangenen Jahren weiterhin Anwendung – allerdings müssen Unternehmen ihre Fähigkeit, sich gegen Angriffe zu verteidigen, realistisch betrachten. „Die Erkennung von Ransomware ist schwieriger denn je", sagt er. „Zudem wird die Dwell Time immer kürzer."

Als „Dwell Time" wird der Zeitraum bezeichnet, den ein Angreifer warten kann, bevor ein Angriff entdeckt oder die Malware freigesetzt wird und Schaden für das Opfer verursacht. Einem Bericht von Cyberint zufolge betrug die mittlere globale Dwell Time von Ransomware im Jahr 2022 neun Tage.[2] In der ersten Jahreshälfte 2023 fiel sie auf nur fünf Tage. Mit anderen Worten: Die Opfer haben weniger Zeit als je zuvor, Malware in ihrem Netzwerk zu erkennen, bevor Schaden entsteht. „Je weniger Zeit man hat, desto geringer ist die Chance, den Angriff zu erkennen", sagt Rogers.

Natürlich werden Unternehmen weiterhin auf Drittanbieter-Tools setzen, um eingehende Angriffe zu erkennen, doch laut Rogers versagt diese Strategie letztendlich bei Zero-Day-Angriffen, die sich brandneue Exploits zunutze machen. „Die meisten Unternehmen wissen letztendlich überhaupt nicht, dass etwas passiert ist, bis ein Benutzer anruft und mitteilt, dass er keinen Zugriff mehr auf viele Dateien hat", erklärt er.

Diverse Sicherheitstools nutzen jetzt KI, die sie beim Erkennen von Angriffen unterstützt, doch diese sind nach heutigem Stand alles andere als ein Allheilmittel. „Ich glaube nicht, dass es ein KI-Produkt gibt, das Menschen davon abhalten kann, auf schädliche Links zu klicken", so Rogers. „Und ich glaube auch nicht, dass Cybersicherheitsprodukte die Angreifer mittlerweile eingeholt haben, was den Einsatz von KI angeht." Der Grund dafür ist, dass ein fehlgeschlagener Angriff keine Sanktionen für den Angreifer nach sich zieht. In diesem Fall hat er sein Ziel einfach nicht erreicht und kann es noch einmal versuchen. Ein KI-basiertes Cybersicherheitstool müsste so gut wie perfekt sein, so Rogers – ein Versprechen, das diese entstehende Technologie noch lange nicht erfüllen kann.

Aktuell verfolgt HPE Zerto einen grundlegenderen Sicherheitsansatz, bei dem Daten in Echtzeit gescannt werden und eine sichere Kopie der Daten erstellt wird, während sie auf ein Speichergerät geschrieben werden. Rogers führt aus: „Im Vergleich zur Echtzeit fehlen uns etwa fünf Sekunden. So können wir schnell eine Warnung ausgeben und das Sicherheitsteam informieren, wenn in der Umgebung etwas nicht stimmt." Dieser Ansatz kann die Reichweite eines Angriffs verkleinern und Analysten dabei helfen, seinen Ursprung zu ermitteln, bevor der Angriff sich auf weiteren Systemen ausbreiten kann.

Backups werden ausgeklügelter als je zuvor

Das Gegenstück zur Erkennung ist die Vorbereitung. Das bedeutet heute mehr denn je, dass ein intelligenter Ansatz für Backups benötigt wird. Die Zeiten, in denen ein Bandlaufwerk in eine Ecke des Serverraums gestellt und darauf konfiguriert wurde, nachts zu laufen, sind lange vorbei. Selbst die altbewährte 3-2-1-Regel – drei Exemplare Ihrer Daten auf zwei verschiedenen Medientypen, wobei ein Exemplar an einem externen Ort gespeichert wird – reicht nicht mehr aus.

„Es braucht nur einen fehlenden Patch", damit ein Angriff es ins System schafft, sagt Paul Lloyd, Security Strategist bei HPE. „Man selbst muss die ganze Zeit wachsam bleiben, während die Angreifer nur einmal Erfolg haben müssen. Diese Weisheit hört man in dieser Branche ständig und ihre Korrektheit lässt sich nicht abstreiten."

Die aktuellsten Ratschläge für Backups empfehlen Unternehmen eine aggressivere 3-2-1-1-0-Backup-Routine. Dabei gilt weiterhin die 3-2-1-Regel. Die zusätzliche 1 bezieht sich auf ein Backup, das physisch vom primären Netzwerk abgekoppelt und somit immun gegen Ransomware-Angriffe ist, die sich über das primäre Netzwerk ausbreiten könnten.

Air Gapping ist heute von entscheidender Bedeutung. „Wenn Sie von zu Hause aus auf ein Backup zugreifen können, dann kann ein Hacker das auch", sagt Lloyd. Die neue 0 verdeutlicht, wie wichtig es ist, die Zuverlässigkeit, Genauigkeit und Vollständigkeit dieser Backups zu überprüfen, wobei bei Wiederherstellungstests keine Fehler auftreten dürfen.

[2] „Ransomware Trends Q3 2023 Report", Cyberint, 11. Oktober 2023

„Kriminelle wollen ins Netzwerk gelangen, ihr Geld bekommen und dann zu ihrem nächsten Ziel weiterziehen", führt Lloyd aus. Der Cybersicherheitsfirma Mandiant zufolge ist die durchschnittliche Zeit bis zur Ausnutzung neu entdeckter Schwachstellen von 63 Tagen in den Jahren 2018 und 2019 auf 44 Tage im Jahr 2020 und Anfang 2021 gefallen.[3] Im Jahr 2022 war dieser Durchschnitt auf 32 Tage gesunken.

Lloyd fährt fort: „Die Angreifer werden schneller, und die Unternehmen werden langsamer bei der Installation von Patches – und machen sich damit immer anfälliger für Angriffe. Wir bekommen die Grundlagen immer noch nicht richtig hin, und das schon seit Jahrzehnten. In manchen Fällen bedeutet das, dass man bestenfalls die Ausbreitung eines erfolgreichen Angriffs eingrenzen kann."

Fokus auf eine schnellere und bessere Wiederherstellung

Die gute Nachricht ist, dass die Lage hinsichtlich der Wiederherstellung nach einem Angriff heute besser ist als je zuvor. „Wir sind an einem Punkt angelangt, an dem man den Betrieb nach einem Angriff innerhalb von Minuten und mit einem Datenverlust von nur wenigen Sekunden wieder aufnehmen kann", sagt Rogers.

Der Trick besteht nicht in einer schnellen, sondern in einer sauberen Wiederherstellung von Daten. Dafür muss man nachvollziehen können, wann ein Angriff begonnen hat. Mit der Wiederherstellung eines Backups, das bereits infiziert wurde, verschlimmert man das Problem nur.

Die Implementierung von Cleanrooms und Data Vaults spielt dabei eine entscheidende Rolle. Diese Umgebungen, die früher nur zahlungskräftigen Firmen wie großen Finanz- oder Gesundheitsunternehmen zur Verfügung standen, werden dank sinkender Kosten und höherer Benutzerfreundlichkeit auch für die breite Masse immer zugänglicher.

Ein Cleanroom ist ein Infrastrukturbereich, der vom Produktionsnetzwerk abgekoppelt ist. Ein Data Vault ist eine Architektur, die Daten in einem unveränderlichen Format speichert. In Kombination erhalten Sie damit ein Netzwerk, das funktional von allen anderen Umgebungen isoliert ist, sodass ein Angriff von außen praktisch unmöglich ist. Da nur verifizierte Backups im Data Vault im Cleanroom gespeichert werden, hat der Benutzer eine deutlich größere Gewissheit, dass Dateien, die aus dieser Umgebung wiederhergestellt werden, sicher und nicht infiziert sind.

Eine effektive Überprüfung von Backups beinhaltet die Überprüfung von Daten während des Wiederherstellungsprozesses, um sicherzustellen, dass sie nicht verschlüsselt oder auf sonstige Weise durch ein Malware-Produkt kompromittiert wurden. Ebenso werden Daten und Anwendungen einzeln wiederhergestellt und im laufenden Betrieb geprüft und freigegeben. Werden während dieses Prozesses Unstimmigkeiten festgestellt, kann die Wiederherstellung angehalten und stattdessen ein älteres Exemplar der Daten bzw. der Anwendung wiederhergestellt werden. Moderne Sicherheitsplattformen wie die von HPE Zerto können all diese Aufgaben schneller durchführen als Wiederherstellungstools der vorherigen Generation. So sind die meisten Umgebungen innerhalb von Stunden statt Wochen wieder einsatzbereit.

Eine Sicherungs- und Wiederherstellungsarchitektur wie diese ist heute praktisch unabdingbar. „Wenn Sie nicht bereit sind, in diese Bereiche zu investieren, setzen Sie Ihr Unternehmen einem größeren Risiko aus", sagt Rogers.

Lassen Sie sich auch nicht von der Komplexität der modernen Sicherheitsumgebung verunsichern. Rogers rät: „Suchen Sie das nötige Know-how und wenden Sie sich an Sicherheitsdienstleister, die das Management für Sie übernehmen können."

[3] „Analysis of Time-to-Exploit Trends: 2021-2022", Mandiant, 28. September 2023

Visit HPE.com

Weitere Informationen unter

HPE.com/data

Jetzt chatten

a50010074DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com