TANIUM

Ansichten aus der Führungsetage:

Warum Endpunktverwaltung wichtiger denn je ist

TANIUM

Ansichten aus der Führungsetage:

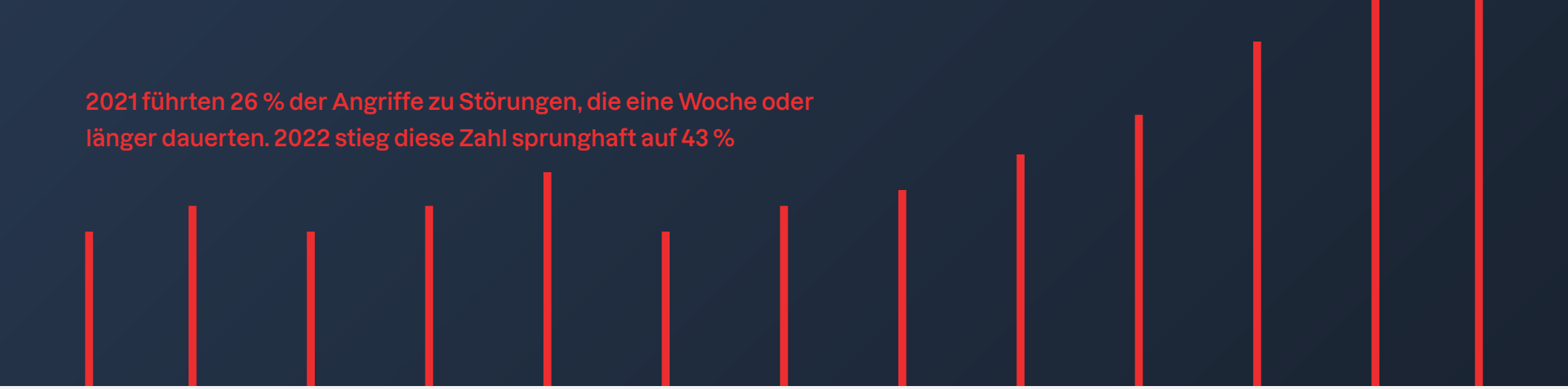
Warum Endpunktverwaltung wichtiger denn je ist

Endpunkte sind der neue Netzwerkrand. Ihre Verteidigung ist entscheidend.

Cloud-Architekturen und Remote-Mitarbeiter haben den Perimeter des Netzwerks, die traditionelle Verteidigungslinie für die IT-Sicherheit, effektiv aufgelöst. Ohne diese entscheidende Grenze hat sich die Arbeit der Sicherheitsteams verändert. Zur Prävention von Datenschutzvorfällen, Ransomware und anderen Arten von Cyberbedrohungen ist der Schutz von Netzwerkendpunkten wichtiger denn je.

Aber der Endpunktschutz birgt eine große Herausforderung, zum Teil aufgrund des großen Arbeitsumfangs. Endpunkte umfassen alles, von Laptops, Desktops und Tablets von Mitarbeitern bis hin zu lokalen Servern, Containern und Anwendungen, die in der Cloud ausgeführt werden. Die Endpunktsicherheit erfordert eine umfassendere und flexiblere Strategie von Sicherheitsteams als vor einem Jahrzehnt, wo sich die IT-Assets fast alle noch vor Ort befanden und durch eine Firewall geschützt waren.

In diesem E-Book sehen wir uns die größten IT-Sicherheitsbedrohungen an, berücksichtigen ihre Auswirkungen auf die Endgeräte und das Endpunktmanagement und bieten einige Richtlinien für Best Practices von IT-Sicherheitsverantwortlichen.



Die sich entwickelnde Bedrohungslandschaft

Ransomware und andere Bedrohungen entwickeln sich weiter und umgehen bisher erfolgreiche Verteidigungsstrategien.

Ransomware bleibt nach wie vor eine große Bedrohung für Organisationen jeder Größe. Nachdem sie einige Jahre abgenommen haben, nehmen Ransomware-Angriffe wieder zu. Sie stiegen von 2021 bis 2022 um 23 %.

Nicht nur ereignen sich die Angriffe häufiger, sie stören auch stärker. 2021 führten 26 % der Angriffe zu Störungen, die eine Woche oder länger dauerten. 2022 stieg diese Zahl sprunghaft auf 43 %.[1]

Im Durchschnitt kostete jeder dieser Angriffe seinem Opfer 4,54 Millionen USD, einschließlich der geleisteten Lösegeldzahlungen sowie der Kosten für die Behebung.[2]

So schlimm diese Zahlen auch sind, sie werden nicht besser werden. Das liegt daran, dass die Angreifer im vergangenen Jahr neue Modelle eingeführt haben, um von ihren Opfern Geld zu erpressen.

Als ursprüngliche Idee hinter Ransomware sollten die Daten der Opfer verschlüsselt und verhindert werden, dass sie diese entschlüsseln, es sei denn, sie bezahlten ein Lösegeld mit Kryptowährung. Aber da Unternehmen ihre Netzwerke besser segmentieren und sichere Backups erstellen konnten, sank die Effektivität dieser Angriffsmethode. Unternehmen konnten sich die Lösegeldzahlung sparen, ihre Daten mehr oder weniger in den vorherigen Zustand zurückversetzen und weiterhin wie gewohnt arbeiten.

Angesichts dieses Widerstands haben Angreifer ihre Strategie verändert.[3] Anstatt die Daten von Unternehmen auf unbestimmte Zeit verschlüsselt zu lassen, drohen sie jetzt damit, sie der Öffentlichkeit zugänglich zu machen, indem sie personenbezogene Daten, Finanzunterlagen, Support-Protokolle, Quellcode, Patentanmeldungen und andere wertvolle Daten preisgeben, auf die sie zugreifen konnten.

Diese zweite Erpressungsebene lässt sich für Angreifer noch einfacher bewältigen als die erste. Das liegt daran, dass große Datenmengen schwierig zu verschlüsseln sind. Angreifer verlassen sich oft auf Partner mit Erfahrung in der Verschlüsselung. Aber selbst mit diesem Know-how funktioniert die Verschlüsselung nicht immer wie geplant. Manchmal werden Daten nicht richtig verschlüsselt. Manchmal werden sie stattdessen beschädigt. Dann können Unternehmen ihre Daten nicht entschlüsseln, selbst wenn sie das Lösegeld bezahlen.

Falls andere Unternehmen erfahren, dass die Entschlüsselungssoftware einer bestimmten Ransomware-Bande nicht funktioniert, zahlen diese wahrscheinlich nicht das Lösegeld, wenn die eigenen Daten bei einem Angriff verschlüsselt werden.

Aber Kriminelle müssen sich nicht unbedingt auf die Verschlüsselung verlassen, wenn sie die Daten von Opfern einfach von einem entfernten Ort stehlen möchten. Kein Unternehmen möchte interne Daten an die Öffentlichkeit weitergeben. Diese Daten könnten Beziehungen zu Kunden und Partnern beeinträchtigen, was es schwierig macht, die Reputationsschäden für die Marke zu beheben. Dadurch könnten auch Geschäftsgeheimnisse offenbart werden, die einen Wettbewerbsvorteil für immer zunichtemachen.

Angreifer können auch über eine dritte Erpressungsebene agieren: Kunden, Partner und Mitarbeiter des Unternehmens direkt kontaktieren und sie darüber informieren, dass ihre Daten heimlich kopiert wurden. Die Angreifer ermutigen diese Stakeholder dann dazu, das Unternehmen zur Lösegeldzahlung zu drängen, damit die Daten nicht weitergegeben werden. Oder sie verlangen, dass diese Stakeholder zum Schutz ihrer personenbezogenen Daten eigene Lösegeldzahlungen leisten. Die kriminelle Bande „Clop“ hat diese Strategie 2021 übernommen und zwei Lösegelder verlangt: eines zur Entschlüsselung von Daten und ein weiteres dafür, dass diese Daten nicht an die Öffentlichkeit weitergegeben werden.[4]

Mit drei möglichen Erpressungsstufen sind die Einsätze bei Ransomware höher als je zuvor.

Zum Schutz vor diesen neuen Formen der Erpressung reicht das Erstellen von Backups Ihrer Daten nicht aus. Jetzt müssen Sie Ihre Daten schützen, wo immer sich diese auch befinden. Das bedeutet, dass Sie alle Ihre Endpunkte überall, unabhängig vom jeweiligen Standort sichern müssen, damit sie nicht zum Einfallstor für einen Angriff werden.

Wie Ransomware Endpunkte erreicht

Wie erreicht Ransomware die Endpunkte? In den jüngsten Forschungsberichten identifizierte die Analystenfirma IDC diese Wege:

- Öffnen eines bösartigen Anhangs oder Anklicken eines Links in einer Phishing-E-Mail
- Zum Opfer einer Drive-by-Kompromittierung fallen, bei der böswillige Angreifer im Rahmen des normalen Internet-Browsings Zugriff auf einen Endpunkt erhalten
- Aufrufen von Peripheriegeräten oder mit Malware infizierten Wechselmedien[5]

Schwachstellen sind heute eine der Hauptquellen für Datenschutzverletzungen. Das Patching ist deshalb wichtiger denn je. Patching erfordert jedoch Visibilität in alle Endpunkte – etwas, das den meisten Organisationen fehlt.

„Je schwieriger wir es Kriminellen machen, Authentifizierungssysteme zu hacken, desto stärker verlassen sie sich auf Softwareschwachstellen für ihre Angriffe. Es werden immer Schwachstellen auftreten. Deshalb müssen diese schnell entdeckt und gepatcht werden. Aus diesem Grund starten auch immer mehr Unternehmen Bug-Bounty-Programme. Interne Teams und Softwareanbieter selbst wissen, dass der Einsatz noch nie höher war."

Tim Morris
Chief Security Advisor, Americas
Tanium

BEC-Angriffe (Business Email Compromise)

Eine weitere verbreitete Form ist der BEC-Angriff (Business Email Compromise) auf geschäftliche E-Mails. Bei dieser Art von Angriff senden Kriminelle eine E-Mail, die sich als vertrauenswürdiger Geschäftskontakt ausgibt, z. B. als CEO eines Unternehmens, als Personal- oder Einkaufsleiter. Die E-Mail, die oft eine gewisse Dringlichkeit vermitteln soll, weist den Empfänger an, eine Rechnung zu bezahlen, Geld zu überweisen, W-2-Informationen, Seriennummern von Geschenkkarten zu senden oder andere Maßnahmen zu ergreifen, die legitim, wenn auch ungewöhnlich erscheinen. Wenn der Empfänger diesen Anweisungen folgt, werden die angeforderten Gelder oder Daten tatsächlich an die Kriminellen, anstatt an den angeblichen Empfänger gesendet. Die Mittel könnten unterwegs sogar heimlich in Kryptowährungen umgewandelt werden, was eine Zurückgewinnung fast unmöglich macht.

Zwischen Juni 2016 und Dezember 2021 verzeichnete das FBI über 240.000 nationale und internationale Beschwerden über BEC-Angriffe, was kumulativ zu Verlusten von 43 Milliarden US-Dollar führte. Ransomware mag für mehr Schlagzeilen sorgen, aber BEC-Angriffe sind 64-mal teurer.[6] Und sie werden immer häufiger und stiegen zwischen 2019 und 2021 um 65 %.[7]

BEC-Angriffe lassen sich nur sehr schwer erkennen, da Kriminelle ziemlich gut darin sind, sich als CEOs und andere Führungskräfte eines Unternehmens auszugeben. Sie können viele personenbezogene Daten über diese Führungskräfte und ihr Privatleben abrufen – einschließlich sozialer Aktivitäten, Familien, philanthropischer Arbeit und Reisepläne – aus Social-Media-Konten, Nachrichtenartikeln und anderen Quellen. Dadurch senden die Angreifer Nachrichten, die Informationen enthalten, von denen die Empfänger der E-Mail glauben könnten, dass nur die Führungskraft, als die sich die Angreifer ausgeben, davon wissen kann.

Kriminelle können auch legitime E-Mail-Threads abfangen und dann eine Nachricht senden, die eine Antwort von einer Partei des Threads zu sein scheint. Da die anderen Nachrichten im Thread legitim sind, gehen die Empfänger davon aus, dass die BEC-Nachricht ebenfalls legitim ist. Dann handeln sie nach den Anweisungen in der Nachricht.

Jetzt, da Mitarbeiter von zu Hause aus arbeiten, sind sie für diese Angriffsformen noch anfälliger.[8]

Bei BEC-Angriffen sind die Endpunkte selbst nicht unbedingt kompromittiert. Vielmehr dienen die Endpunkte dem Staging des Angriffs. Daher liefern sie Sicherheitsteams wertvolle Kontextinformationen, wenn diese verstehen möchten, wie der Angriff stattgefunden hat und welche anderen damit verbundenen Bedrohungen noch lauern könnten.

Strategien für das Endpunktmanagement

Wie sollten IT-Sicherheitsteams auf diese sich weiter entwickelnden Bedrohungen reagieren? Hier erhalten Sie 10 Vorschläge.

1

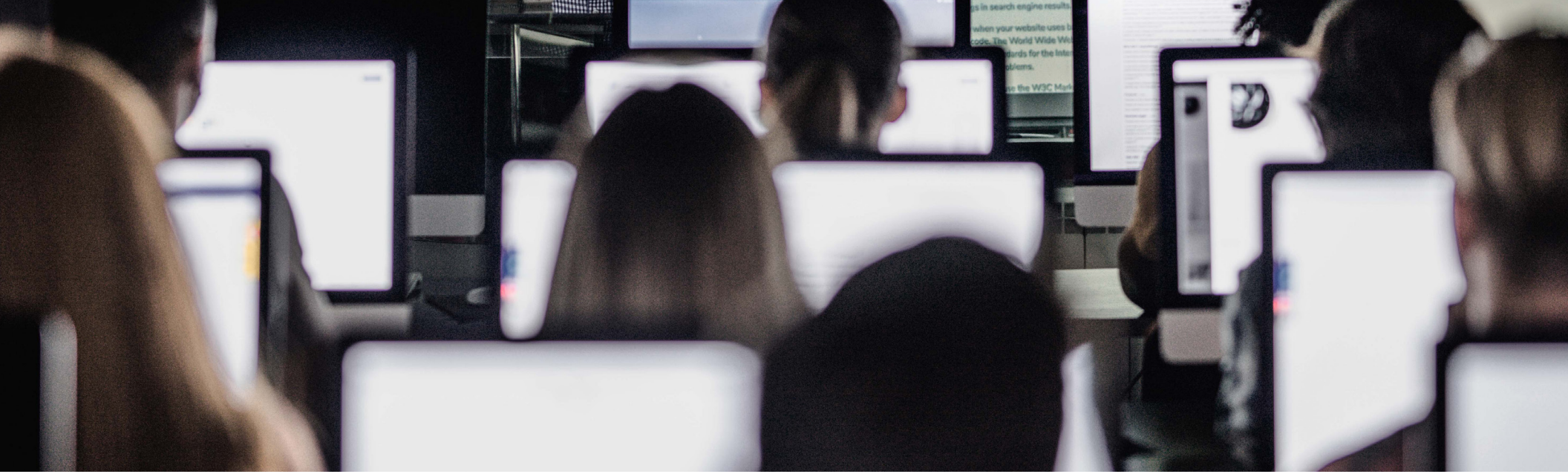
Behandeln Sie Endpunkte wie den neuen Netzwerkrand.

Da so viele Menschen remote arbeiten und 48 % der Anwendungen in der Cloud ausgeführt werden, muss jetzt erkannt werden, dass die neue Verteidigungslinie, um jeden Endpunkt zu ziehen ist, unabhängig von dessen Standort und der Art der Netzwerkverbindung – mit oder ohne VPN.

2

Sorgen Sie dafür, dass Sie alle Geräte identifizieren können, die mit dem Netzwerk verbunden sind, auch persönliche Geräte, die nicht offiziell zur Verwendung autorisiert sind.

„Man kann nicht sichern, was man nicht verwalten kann“, so Tim Morris, Chief Security Advisor, Americas bei Tanium. „Und man kann nicht verwalten, was man nicht kennt.“ Security Operations Center müssen über alle Endpunkte informiert sein, für die sie verantwortlich sind. Ausführliche Audits von Unternehmensnetzwerken stellen routinemäßig fest, dass Systeme für die Endpunktverwaltung etwa 20 % der Endpunkte übersehen. SOC-Teams sollten Tools und Prozesse einrichten, damit sie den vollständigen Bestand an Endpunkten im Blick haben und den Status dieser Endpunkte in Echtzeit überwachen können.



3

Denken Sie daran: Selbst, wenn Sie Mitarbeitern gestärkte Geräte ausgeben, werden die meisten von ihnen auch weiterhin persönliche Geräte verwenden.

Die BYOD-Ära ist noch nicht vorbei. Als IDC die Benutzer fragte, ob sie weiterhin persönliche Geräte für die Arbeit nutzen würden, auch wenn der Arbeitgeber ihnen Geräte zur Verfügung stellte, sagten die meisten, dass sie zumindest manchmal weiterhin persönliche Geräte einsetzen würden. Strategien für die Endpunktsicherheit müssen die Idee berücksichtigen, dass viele Endpunkte, die sich mit dem Netzwerk verbinden und sensible Daten handhaben, persönliche Geräte sind, über die das Sicherheitsteam nur teilweise die Kontrolle hat.

4

Ständiges Patchen.

Patching war schon immer wichtig, damit Endpunkte Zugriff auf die neuesten Funktionen und Fehlerbehebungen haben. Aber jetzt, da sich Softwareschwachstellen als wichtigster Angriffsweg erwiesen haben und mit gestohlenen Anmeldedaten als Vektor für Datenschutzverletzungen konkurrieren, ist die sofortige Anwendung von Patches wichtiger denn je. Unternehmen können nicht auf eine Reaktion bei Supply-Chain-Angriffen wie Log4j hoffen, ohne dass sie automatisierte Lösungen für Software-Materialien und Patches nutzen.

5

Erhalten Sie Visibilität in Softwarekomponenten auf Endpunkten, damit Sie auf den nächsten Supply-Chain-Angriff vorbereitet sind.

Supply-Chain-Angriffe nutzen Schwachstellen in Softwarekomponenten, die heute in Unternehmen sowohl in kommerziellen als auch intern entwickelten Anwendungen weit verbreitet sind. Als die Log4j-Schwachstelle angekündigt wurde, verschwendeten Kriminelle keine Zeit damit, neue Angriffe zu entwickeln, um die Log4j-Schwachstelle auszunutzen, da sie sich so lange im Vorteil sahen, wie Unternehmen Schwierigkeiten mit dem Identifizieren und Patchen anfälliger Anwendungen hatten. Zur Verteidigung gegen zukünftige Angriffe wie diese benötigen SOC-Teams Echtzeit-Visibilität in alle auf den Endpunkten installierten Softwarekomponenten, damit sich gefährliche Lücken schnell schließen lassen. Es ist an der Zeit, dass Sicherheitsteams Software-Stücklisten (SBOM) zur Standardanforderung für jedes SOC-Toolset machen.

6

Setzen Sie die Multifaktor-Authentifizierung durch, um Angreifern die Nutzung kompromittierter Endpunkte zu erschweren.

Phishing-Angriffe täuschen Mitarbeiter weiterhin dazu, ihre Anmeldedaten preiszugeben. Kriminelle können auch auf Anmeldedaten zugreifen, indem sie sich in Verzeichnisserver hacken, Datenschutzverletzungen ausnutzen oder von böswilligen Insidern geleakte Daten einsetzen. Um Kriminellen die Nutzung dieser Anmeldedaten zu erschweren, ist es sinnvoll, wo irgend möglich Multifaktor-Authentifizierung (MFA) durchzusetzen – insbesondere für Back-Office-Systeme und Konsolen, die für das Netzwerkmanagement und andere IT-Funktionen verwendet werden. Bei der Multifaktor-Authentifizierung muss ein Benutzer verschiedene, nicht verwandte Datentypen oder Aktionen zur Authentifizierung verwenden. Diese Faktoren werden normalerweise als etwas beschrieben, das Sie kennen (z. B. ein Passwort), als etwas, das Sie haben (z. B. ein Hardware-Token) und als etwas, das Sie sind (z. B. ein biometrisches Zeichen wie ein Fingerabdruck).

7

Kontext von Endpunkten abrufen.

Wenn Angriffe auftreten, muss so schnell wie möglich reagiert werden. Um effektiv reagieren zu können, müssen Sicherheitsteams verstehen, was auf den betroffenen Endpunkten passiert, unabhängig vom jeweiligen Standort davon. Welche Prozesse werden ausgeführt? Welcher Netzwerkverkehr findet statt? Welche Dateien wurden kürzlich heruntergeladen? Was war der Patch-Status? Diese Art von Untersuchungen gestalteten sich einfacher, als alle Endpunkte noch vor Ort waren. Jetzt benötigen Analysten möglicherweise in wenigen Minuten Antworten von Endpunkten, die sich Tausende Kilometer entfernt befinden. Und sie haben keine Zeit, neue Software zu installieren, oder zu hoffen, dass der Remote-Benutzer ihnen beim Aufbau einer Verbindung helfen kann. Sicherheitsteams müssen bereits über ein System zur Analyse von Endpunkten und zur Erfassung dieser Daten verfügen, damit sie bei jedem Angriff – auch bei BEC-Angriffen – die Kontextinformationen erfassen können, die für das genaue Verständnis der Geschehnisse und aktiv bleibenden Bedrohungen erforderlich sind. Sorgen Sie dafür, dass Ihre Organisation jederzeit und überall Kontextinformationen für jeden Endpunkt erhalten kann.

„Die Endpunktüberwachung stoppt einen BEC-Angriff nicht, aber sie könnte Ihnen etwas mehr über die Person erzählen, welche die E-Mail tatsächlich geöffnet hat, und dann, was sie damit gemacht hat, was sie aufgerufen hat oder was sonst noch vor sich ging. Der Kontext kann Ihnen die Hinweise geben, mit deren Hilfe Sie feststellen können, ob dieser Angriff Teil einer breiteren Kampagne ist, die andere Empfänger mit irreführenden Nachrichten erreichen will.“

Tim Morris
Chief Security Advisor, Americas
Tanium

8

Denken Sie wie ein Ersthelfer.

Können Sie schnell handeln, um Probleme zu diagnostizieren und einzudämmen? Verfügt Ihr Team über die nötigen Tools, Schulungen und Prozesse? Sorgen Sie dafür, dass Ihr Team aktiv werden kann, wenn Endpunkte angegriffen werden. Protokolle sind wichtig. Eine schnelle Reaktion kann Bedrohungen eindämmen, bevor sie sich auf andere Endpunkte und Standorte ausbreiten, was einer Organisation möglicherweise Millionen von Dollar spart.

„Bleiben Sie vorbereitet, damit Sie sich nicht vorbereiten müssen."

Tim Morris, Chief Security Advisor, Americas

9

Drills.

Sobald Sie einen Cybersicherheitsplan, ein Cybersicherheits-Toolset und geschultes Personal haben, müssen Sie die Jagd auf Bedrohungen und die Reaktion auf Angriffe aller Art üben. Das Verfolgen eines Ansatzes mit Red Team/Blue Team: Ein Team aus vertrauenswürdigen Sicherheitsanalysten ist beauftragt in ein Netzwerk einzudringen; dem dagegen steht ein Team aus anderen vertrauenswürdigen Sicherheitsanalysten für die Verteidigung.[9] Unabhängig von der Organisation decken diese Drills fast immer Lücken in der Sicherheitsabdeckung auf, was die Notwendigkeit neuer Tools oder Prozesse hervorhebt. Die Drills helfen den Teams auch dabei, das Vertrauen aufzubauen und effektiver zusammenzuarbeiten.

10

Denken Sie im großen Stil.

Die Anzahl der Endpunkte wird nur noch steigen. Die Sicherheitsteams sollten jetzt Tools und Prozesse einrichten, damit sie effektive Sicherheitsstrategien und -kontrollen einsetzen können, wenn sie viele weitere Endpunkte überwachen, verwalten und schützen müssen.

Fazit

Cyberbedrohungen wie Ransomware nehmen zu und Endpunkte sind vielfältiger, zahlreicher und stärker verteilt als je zuvor. Durch die Berücksichtigung der in diesem E-Book beschriebenen Strategien können Sicherheitsteams das Risiko von Cyberangriffen reduzieren und diese im Angriffsfall schnell und effizient eindämmen.

Um mehr über die Tanium-Lösung Converged Endpoint Management (XEM) zu erfahren, besuchen Sie www.tanium.com.

Fußnoten

1 IDC, Michael Suby, Tanium Converge-Präsentation, 2022.

2 *Cost of a Data Breach Report 2022,* IBM. https://www.ibm.com/reports/data-breach

3 https://www.darkreading.com/vulnerabilities-threats/fool-me-thrice-how-to-avoid-double-and-triple-ransomware-extortion-

4 https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/

5 *Future Enterprise Resiliency & Spending Survey,* März 2022, zitiert von IDC Vice President Michael Suby

6 https://www.lifars.com/bec-attacks-account-for-losses-64-times-worse-than-ransomware/

7 https://www.techrepublic.com/article/fbi-43-billion-losses-are-business-email-compromise-fraud-between-2016-2021/

8 Business Email Compromise: The $43 Billion Scam, FBI Public Service Announcement, Alert I-050422-PSA, 4. März 2022, https://www.ic3.gov/Media/Y2022/PSA220504

9 https://csrc.nist.gov/glossary/term/red_team_blue_team_approach