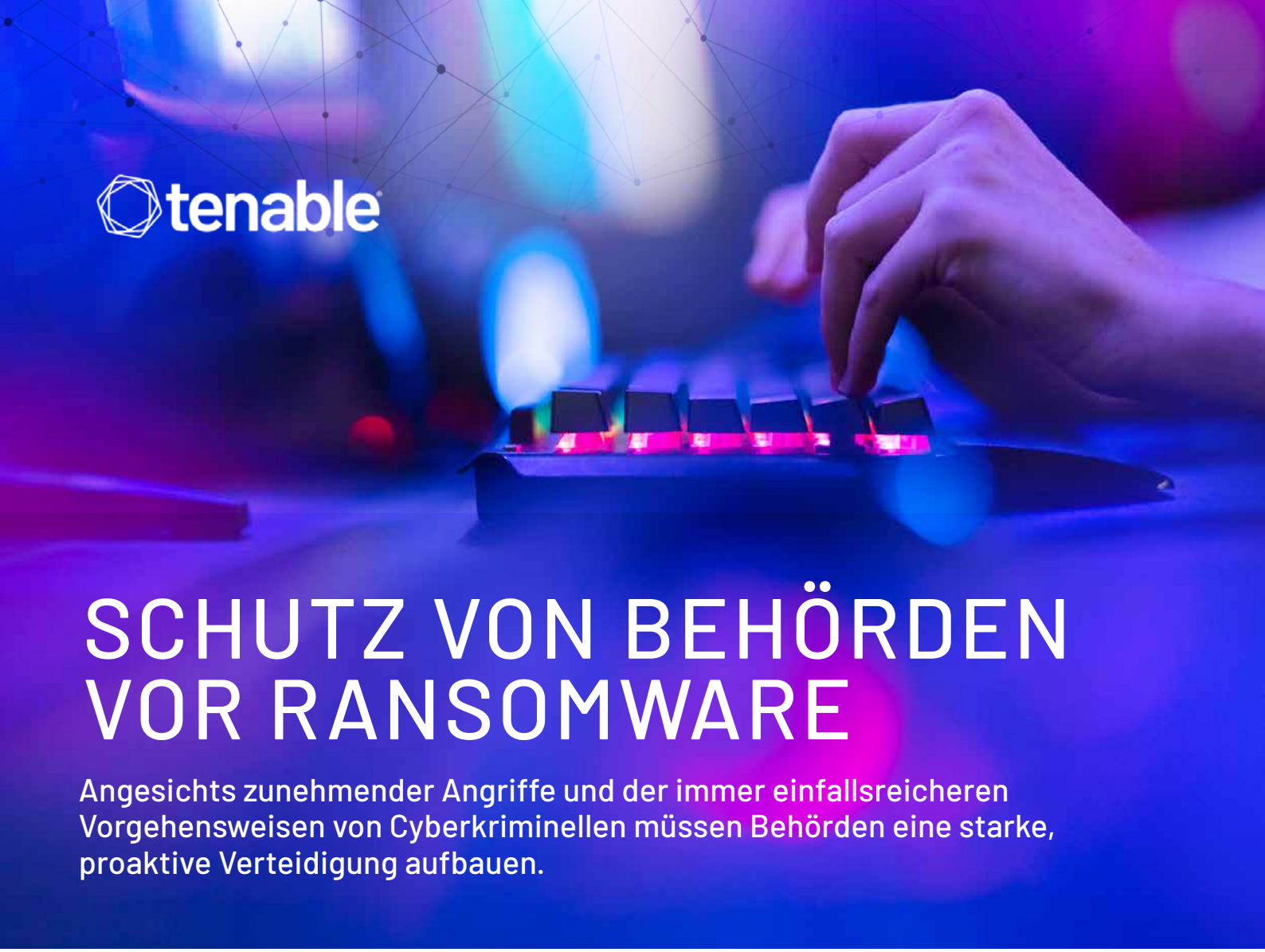


SCHUTZ VON BEHÖRDEN VOR RANSOMWARE

Angesichts zunehmender Angriffe und der immer einfallsreicheren Vorgehensweisen von Cyberkriminellen müssen Behörden eine starke, proaktive Verteidigung aufbauen.

Beispiele für Ransomware-Angriffe auf bundesstaatliche und kommunale Behörden gibt es zuhauf. In den letzten Jahren haben Angreifer städtische Computernetzwerke lahmgelegt, Studenten aus WLAN-Netzen und online zugänglichen Lehrbüchern ausgesperrt, für Voicemails und Gesetzesentwürfe eingesetzte Anwendungen der Legislative auf bundesstaatlicher Ebene abgeschaltet, kommunale Wasser- und Stromversorgungssysteme bedroht und vieles mehr. Vorkommnisse wie diese beeinträchtigen wichtige öffentliche Dienste, gefährden Menschenleben und kosten Steuerzahler Unsummen an Geld. Im Jahr 2020 machte Ransomware ein Drittel aller Cybersecurity-Angriffe auf Regierungsstellen aus[1] – und die Flut der Ransomware-Angriffe wird mit der Zeit nur weiter an Intensität gewinnen. Eigenen Angaben zufolge wurden dem Internet Crime Complaint Center des FBI in der ersten Jahreshälfte 2021 insgesamt 2.084 Ransomware-Fälle gemeldet, was einer 62-prozentigen Steigerung im Jahresvergleich entspricht.[2] Erschwerend kommt hinzu, dass sich Ransomware weiterentwickelt. Cyberkriminelle gehen von großflächig angelegten Phishing-Angriffen zu sehr gezielten Angriffen auf bestimmte Organisationen über. Zum Schutz Ihrer Behörde vor diesen Bedrohungen ist es daher notwendig, die Anatomie von Ransomware zu verstehen.

Wie Ransomware funktioniert

Hier eine einfache Beschreibung eines Ransomware-Angriffs:

- Durch großflächig angelegtes Phishing, gezieltes Spear-Phishing oder direkte Angriffe auf anfällige VPN-Systeme und Webanwendungen schleust der Angreifer Schadcode ein.
- Sobald Malware in ein Computernetzwerk von Behörden gelangt ist, sucht sie zunächst nach Schwachstellen und Fehlkonfigurationen und nutzt diese dann aus.
- Der Angreifer bewegt sich daraufhin seitwärts durch Ihre Organisation fort und sammelt dabei Zugangsdaten.
- Im letzten Schritt weitet der Angreifer Rechte aus und verschafft sich dadurch Zugriff auf Hunderte oder gar Tausende von Geräten, um darauf befindliche Daten in seinen Besitz zu bringen und zu verschlüsseln.

Angreifer nutzen heutzutage nicht einfach nur den Computer eines Endbenutzers aus, um sich einen ersten Zugang zu einem Netzwerk zu verschaffen. Sie haben ihre Angriffsmethoden ausgeweitet, um Malware schnell zwischen Netzwerken auf andere Geräte und Assets zu übertragen. Inzwischen könnten fast alle Geräte, Anwendungen, Betriebssysteme oder Netzwerke zu Einstiegspunkten werden. Und die wachsende Angriffsoberfläche und mit Schwachstellen übersäte Umgebungen machen es fast unmöglich zu verhindern, dass Angreifer zumindest einen Einstiegspunkt kompromittieren.
Angreifer bewegen sich auch nicht mehr linear zu ihrem Ziel fort, sondern verfolgen vielmehr einen dynamischen Ansatz, der auf der jeweiligen Umgebung des kompromittierten Geräts beruht. Zu ihren Taktiken gehört es häufig, Schutzmaßnahmen zu umgehen, Schadcode auszuführen, Zugangsdaten zu sammeln, das Netzwerk sowie Active Directory (AD) aufzulisten und Passwörter abzugreifen. Angreifer sammeln Informationen, analysieren die Umgebung und nutzen Schwachstellen und Fehlkonfigurationen aus, um dadurch noch mehr Zugriffsrechte zu

erlangen. Fast immer ist AD das erste Angriffsziel, da es in den meisten Organisationen als primäres Tool der Authentifizierung und Autorisierung dient.
Sobald sich Angreifer Berechtigungen in AD verschafft haben, ist ihre Arbeit fast schon getan. Zu den letzten Schritten gehört dann, die Zieldaten zu kopieren, Ransomware zu verteilen (in der Regel über Gruppenrichtlinien), Persistenz und Backdoors einzurichten, Backup-Dateien zu löschen und die Verschlüsselung der Netzwerkinfrastruktur auszulösen.

Wo anfangen?

Schlechte Cyberhygiene wird durch Ransomware zu Geld gemacht. Deshalb müssen Behörden wichtige Grundvorkehrungen treffen, um Risiken zu reduzieren. Experten der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) und des britischen National Cyber Security Centre (NCSC) empfehlen die folgenden grundlegenden Maßnahmen:

- Führen Sie Schulungen zur Schärfung des Cybersecurity-Bewusstseins durch, um Phishing-Angriffe zu verringern.
- Segmentieren Sie Ihre Netzwerke, um unterschiedliche Geschäftsbereiche und Ressourcen voneinander zu trennen. Dadurch können Sie Eindringversuche leichter eindämmen, wenn es dazu kommt.
- Aktivieren Sie die Multi-Faktor-Authentifizierung in allen Bereichen.
- Erstellen Sie regelmäßig verschlüsselte Backups von Daten und System-Images.
- Führen Sie kontinuierlich risikobasiertes Schwachstellen-Management und Active Directory-Bewertungen auf Ihrer gesamten Angriffsoberfläche durch.

Sechs Schritte zur Abwehr von Ransomware

Zusätzlich zu diesen grundlegenden Maßnahmen stellen wir an dieser Stelle sechs spezifische Schritte vor, mit denen Behörden ihre Infrastruktur vor Ransomware-Angriffen schützen können.

Schritt 1

Häufig und umfassend scannen

Immer mehr Ransomware-Varianten nutzen Software-Schwachstellen als primären Angriffsvektor. Bei diesen Sicherheitsmängeln kann es sich um ältere und hinlänglich bekannte oder um neue Schwachstellen wie etwa Log4j handeln. Deshalb ist es unerlässlich, Ihre gesamte Angriffsoberfläche kontinuierlich zu analysieren, da sich Ihre Umgebung verändert und neue Bedrohungen auftreten.
Hierzu gibt es keine universelle Lösung – ein adaptiver Ansatz ist notwendig.
Netzwerk-Scanner sind ein überaus effektives Mittel, um Gefährdungen in klassischer On-Premises-IT-Infrastruktur zu identifizieren.
Zudem ist es entscheidend, wo immer möglich Credentialed-Scans einzusetzen, um detaillierte Erkenntnisse zu Schwachstellen und Fehlkonfigurationen zu gewinnen.
Für Organisationen, die es vorziehen, Zugangsdaten nicht zu verwalten oder Remote-Endgeräte während geplanter Scans nicht regelmäßig vom Netzwerk zu trennen, eignet sich agentenbasiertes Scannen als weiterer Ansatz.
Moderne Webanwendungen erfordern einen speziell dafür entwickelten Scanner, um Einblick in dynamische sowie JavaScript- und HTML5-basierte Elemente und Single-Page-Anwendungen zu gewinnen, die für viele andere Scanner unsichtbar sind.
Ein weiteres Anliegen besteht für Behörden im Schutz von operativer Technologie (OT). Bei OT-Assets handelt es sich im Allgemeinen um zweckgebundene Systeme, die dem Betrieb von Wasserwerken, Stromnetzen und anderen industriellen Infrastrukturen dienen.
Sie funktionieren ganz anders als IT-Assets. OT-Systeme können eigenständig sein. Doch in anderen Fällen ist die IT- und OT-Umgebung konvergent, wodurch Angriffsvektoren entstehen, die beide Umgebungen umspannen. In diesen komplexen Umgebungen ist es nicht möglich, mit IT-basierten Netzwerk-Scannern aktiv auf Bedrohungen zu scannen, da diese Scanner erfolgskritische Services stören könnten. Stattdessen ist zur Bewertung von OT-Geräten ein Mix aus geräte- und netzwerkbasierten Erkennungsmethoden erforderlich, die sich native Befehlssprache, Protokolle und passives Monitoring von Datenverkehr zwischen Systemen zunutze machen.

Schwachstellen, die durch Ransomware ausgenutzt werden, häufen sich in der Regel bei bestimmten Arten von Sicherheitsmängeln oder Asset-Kategorien. Wenn versierte Verteidiger diese Muster im Vorfeld kennen, können sie vorhersagen, welche Schwachstellen Angreifer ausnutzen werden, und sie proaktiv beheben.

Schritt 2

Stärken der Active Directory-Abwehr

Ransomware-Gruppen greifen immer häufiger Active Directory an, weil AD die Schlüssel zu Ihrer gesamten Umgebung enthält und Zugangsdaten, Konfigurationseinstellungen und Zugriffsrichtlinien für sämtliche Benutzer, Endgeräte, Dienste und Server kontrolliert. Da es sich um eine Legacy-Umgebung handelt, schenken Behörden dem Schutz von AD häufig leider nicht genug Beachtung. Organisationen müssen sicherstellen, dass AD keine kritischen Fehlkonfigurationen aufweist, die es Angreifern ermöglichen können, sich lateral fortzubewegen und Rechte auszuweiten. Diese vorhandenen AD-Fehlkonfigurationen aufzuspüren und zu beheben, kann eine mühsame Aufgabe sein, die dennoch unerlässlich ist. Sobald AD abgesichert ist, müssen Behörden sämtliche Änderungen kontinuierlich analysieren, um sicherzustellen, dass dadurch keine neuen Fehlkonfigurationen und Angriffspfade entstehen. Ein Hardening der Sicherheit in diesem Ausmaß ist die einzige Möglichkeit, Angreifer daran zu hindern, AD zur Verteilung von bösartiger Software in Ihrer Computing-Umgebung einzusetzen.

Schritt 3

Verhindern von Rechteausweitung

AD auf ungewöhnliche und bösartige Aktivitäten zu überwachen, ist unerlässlich – genauso wie es wichtig ist, Anti-Malware-Programme einzusetzen, um Windows auf ungewöhnliche Dateien und Prozesse zu scannen. Angreifer richten häufig Angriffswege ein, die sie für AD-Angriffe nutzen können. Dies führt schließlich zu einer Ausweitung von Rechten, sodass sie Verschlüsselungssoftware verteilen, Daten zwecks Ausnutzung herunterladen, Backups löschen und Backdoors für künftige Zugriffe einrichten können. Mit den richtigen Erkenntnissen können Sie AD-Änderungen, Syslog-Änderungen und Windows-Ereignisprotokolle korrelieren, um so den Missbrauch von privilegierten Konten und die Ausnutzung von aktiven Fehlkonfigurationen aufzudecken. Mithilfe dieser Informationen können Incident Response-Teams proaktiv verhindern, dass sich Ransomware-Angriffe über AD ausbreiten. Integrieren Sie diese Daten in Ihr SIEM-System (Security Information and Event Management), um Informationen zu sammeln, die von den Windows Server-Ereignisprotokollen und anderen Systemen weitergeleitet werden.

Schritt 4

Nutzung eines risikobasierten Ansatzes und Priorisierung anhand von Prognosen

Es ist schlichtweg nicht möglich, alles zu patchen. Die gute Nachricht ist: Dies ist auch gar nicht nötig. Nur für 5 Prozent der 18.000 neuen Schwachstellen, die im Jahr 2020 veröffentlicht wurden, gab es einen öffentlich verfügbaren Exploit. Und auf diese 5 Prozent müssen Sie sich konzentrieren.

Nutzen Sie Echtzeit-Bedrohungsdaten, um die neuesten Angriffspfade von Ransomware-Gruppen zu verstehen und Ihre Behebungsstrategie entsprechend auszurichten. Doch damit ist es nicht getan. Schwachstellen, die durch Ransomware ausgenutzt werden, häufen sich in der Regel bei bestimmten Arten von Sicherheitsmängeln und Asset-Kategorien. Wenn versierte Verteidiger diese Trends im Vorfeld kennen, können sie vorhersagen, welche Schwachstellen Angreifer ausnutzen werden, und sie proaktiv beheben.

Risikobasiertes Schwachstellen-Management (RBVM) reduziert Risiken auf Ihrer Angriffsoberfläche, indem Schwachstellen anhand der jeweiligen Risiken für Ihre Organisation bei der Behebung priorisiert werden. RBVM nutzt maschinelles Lernen, um Asset-Kritikalität, Schwachstellen-Schweregrad und Aktivitäten von Bedrohungsakteuren zu korrelieren. Dies reduziert Schwachstellenüberlastung und unterstützt Sie dabei, sich auf die verhältnismäßig wenigen Schwachstellen zu konzentrieren, die das größte Risiko für Ihre Organisation darstellen – insbesondere jene, die wahrscheinlich in Ransomware-Angriffen zum Einsatz kommen.

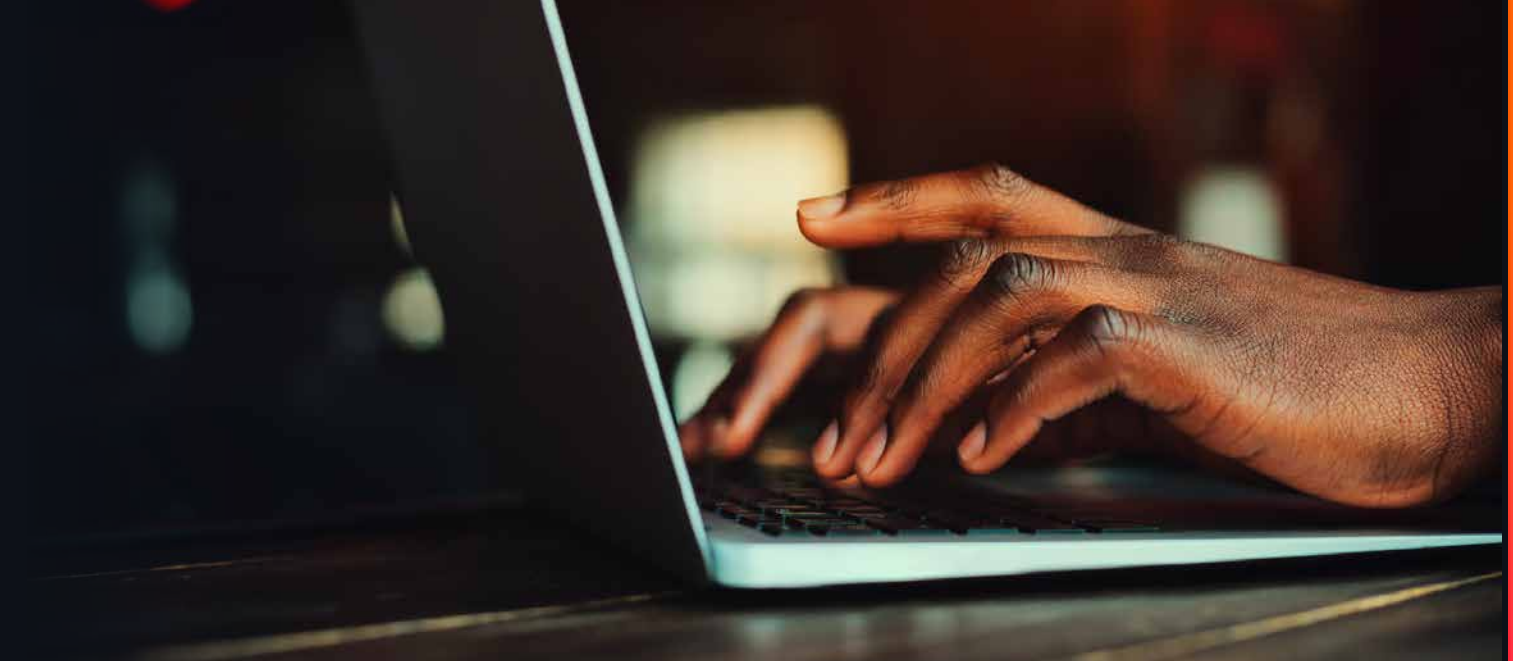
Schritt 5

Behebung von Schwachstellen als oberste Priorität

Allzu häufig werden Schwachstellen und Fehlkonfigurationen, die zur Behebung vorgesehen sind, nie vollständig behoben. Obwohl Sicherheitsteams für die Erkennung und Priorisierung von Schwachstellen zuständig sind, liegt das Patchen in der Verantwortung von IT-Betrieb und Entwicklern – und oftmals sprechen diese Gruppen eine andere Sprache und verfolgen andere Ziele.

Daher ist es wichtiger denn je, RBVM-Lösungen in Ihre ITSM- (IT-Service-Management) und Ticketing-Systeme einzubinden, um Workflows zu automatisieren, Schwachstellen mit Patches zu korrelieren und zu überprüfen, ob alle Instanzen einer Schwachstelle gepatcht oder durch eine kompensierende Kontrolle entschärft wurden. Sie können Daten zu Schwachstellen und Fehlkonfigurationen automatisch an Ihre SIEM-Systeme weiterleiten, um Informationen im Kontext von Ereignissen bereitzustellen und Bereiche zu identifizieren, die sich potenziell für automatisierte Reaktionen eignen.

Behebung ist Teamarbeit. Versenden Sie benutzerdefinierte Berichte, um DevOps-Teams und andere Gruppen in Ihrer Organisation über die Priorität von Schwachstellen zu informieren, sodass diese stets wissen, was zuerst behoben werden muss.



Dasselbe gilt für die Behebung von AD-Fehlkonfigurationen. Bei den meisten AD-Implementierungen ist eine manuelle Überwachung aufgrund der Größe und Komplexität dieser Systeme nicht durchführbar. Profitieren Sie von Technologien, die Ihnen schrittweise Anleitungen zur Behebung bieten, um Sicherheitsmängel in AD vollständig zu beseitigen und Angriffspfade zu blockieren.

Schritt 6

Erfolgsmessung zur Verbesserung der Sicherheitspraxis

Erfolgreiche Teams nehmen sich Zeit, um über ihre Leistung zu reflektieren. Das gilt auch für Sicherheitsteams. Entwickeln Sie Schlüsselmetriken, anhand derer Sie beurteilen und kommunizieren können, wie Ihre operativen Kontrollen funktionieren (bzw. nicht funktionieren). Sammeln Sie darüber hinaus Benchmarking-Daten, um die Leistung innerhalb interner Gruppen oder extern mit der ähnlicher Organisationen zu vergleichen.

Messungen sollten folgende Aspekte umfassen:

- Wie oft Sie den Großteil Ihrer Assets scannen
- Die Anzahl der von Ihnen erfassten offenen Schwachstellen
- Ihre Effektivität bei der Behebung Ihrer risikoreichsten Schwachstellen
- Ihre wichtigsten Funktionen und wie gut Sie damit verbundene Cyberrisiken reduzieren

Fazit

Zur Abwehr von Ransomware müssen Organisationen Sicherheitsmängel beseitigen, bevor Angreifer sie ausnutzen können. Daher ist es von entscheidender Bedeutung, sämtliche Schwachstellen und Fehlkonfigurationen auf der gesamten Angriffsoberfläche zu sehen, anhand von Bedrohungsdaten vorherzusagen, welche dieser Probleme am wichtigsten sind, und schnell zu handeln, um Cyberrisiken zu entschärfen.

Im gemeinsamen Ransomware Guide der CISA und des Multi-State Information Sharing and Analysis Center (MS-ISAC) sind zusätzliche Erkenntnisse zum Thema Ransomware-Bereitschaft enthalten.[3] Zu den Empfehlungen zählen u. a.:

- Führen Sie regelmäßiges Schwachstellen-Scanning durch, um Schwachstellen (insbesondere von Geräten mit Internetanbindung) zu identifizieren und zu beheben und dadurch die Angriffsoberfläche zu beschränken.
- Patchen Sie Software und Betriebssysteme regelmäßig und aktualisieren Sie sie auf die jeweils neueste verfügbare Version. Priorisieren Sie zeitnahes Patchen von bekannten Schwachstellen bei Servern mit Internetanbindung sowie bei Software, die Internetdaten verarbeitet (beispielsweise Webbrowser, Browser-Plugins und Dokument-Reader).
- Sichern Sie Domänencontroller (DC) ab. Bedrohungsakteure nehmen diese häufig ins Visier und nutzen sie als Ausgangspunkt zur Verteilung von Ransomware im gesamten Netzwerk.

Die in dieser Lösungsübersicht behandelten Maßnahmen sollten in Ihren alltäglichen Sicherheitsbetrieb eingebunden werden. Dieses zusätzliche Maß an Wachsamkeit trägt wesentlich dazu bei, dass von Ransomware ausgehende Bedrohungen eingedämmt werden und versuchte Angriffe mit hohem Störpotenzial erfolglos bleiben.

[1] https://www.afcea.org/content/sponsored-81-ransomware-statistics-data-trends-and-facts-2021
[2] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts
[3] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

tenable

Tenable® ist das Unternehmen für Exposure Management. Rund 40.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® erweitert Tenable sein Know-how im Bereich des Schwachstellen-Managements, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen rund 60 Prozent der Fortune 500-Unternehmen, rund 40.000 Prozent der Global 2000 sowie Regierungsbehörden auf Bundes-, bundesstaatlicher und kommunaler Ebene. Erfahren Sie mehr über uns auf **de.tenable.com**.