Fünf Schritte der Ransomware-Abwehr

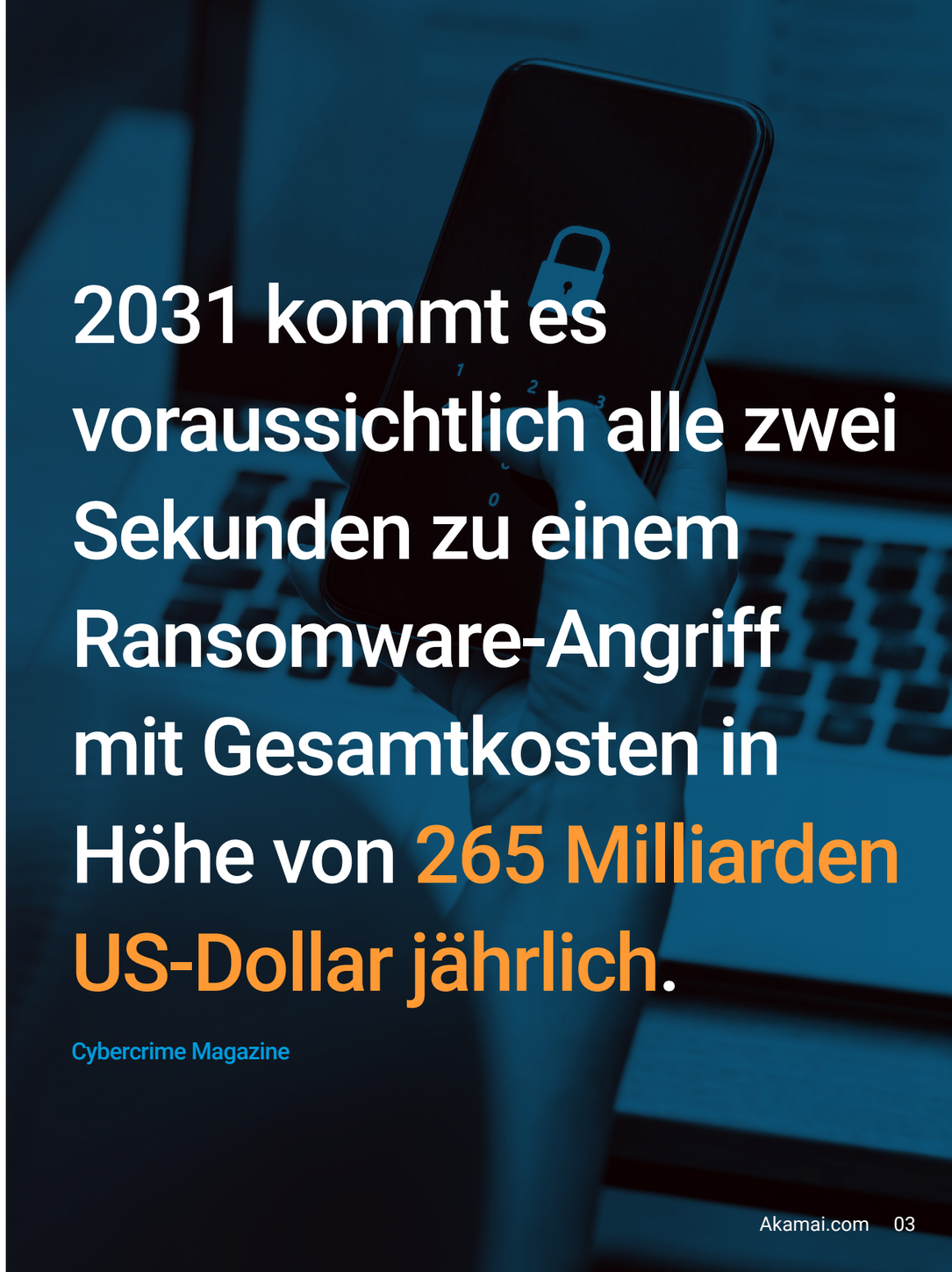
So erhöhen Sie die Sicherheit über Ihre Netzwerkgrenzen hinaus

INHALTSVERZEICHNIS

Einführung

Die rasante Ausbreitung von Ransomware

Ransomware, einst nichts weiter als lästige Malware, die von Bedrohungsakteuren verwendet wurde, um den Zugriff auf Dateien und Daten durch Verschlüsselung zu beschränken, hat sich zu einer Angriffsmethode mit gewaltigen Dimensionen entwickelt. Auch wenn ein dauerhafter Datenverlust bereits eine schreckliche Bedrohung darstellt, sind die Methoden von Cyberkriminellen und Hackern, mitunter mit staatlicher Rückendeckung, inzwischen so ausgeklügelt, dass sie Ransomware einsetzen, um große Unternehmen, staatliche und lokale Regierungsbehörden, globale Infrastrukturen und Organisationen im Gesundheitswesen zu durchdringen und lahmzulegen. Viele dieser Gruppen bieten ihre Dienste sogar als Ransomware-as-a-Service (RaaS) an.



2031 kommt es voraussichtlich alle zwei Sekunden zu einem Ransomware-Angriff mit Gesamtkosten in Höhe von 265 Milliarden US-Dollar jährlich.

Cybercrime Magazine

Ransomware kostet Sie Unsummen

Im Jahr 2022 zwang ein Ransomware-Angriff 7-Eleven, 175 Geschäfte zu schließen, da diese ihre Kassen nicht nutzen oder Zahlungen nicht annehmen konnten. Zu Beginn des Jahres waren 233 Tankstellen von einem BlackCat-Ransomware-Angriff auf ein deutsches Mineralölunternehmen betroffen, woraufhin Royal Dutch Shell seine Lieferungen an andere Versorgungslager umleiten musste. Der Angriff auf die Colonial Pipeline fand im Mai 2021 statt und hatte Unterbrechungen der Öl- und Gaslieferungen entlang der gesamten Ostküste der USA zur Folge. Und in 2020 brachte der Snake-Ransomware-Angriff die globalen Betriebsabläufe von Honda zum Erliegen.

Aufgrund einer Mischung aus veralteter Technologie, „ausreichenden" Verteidigungsstrategien, die sich ausschließlich auf Netzwerkgrenzen und Endpunkte konzentrieren, mangelnder Schulung (und schlechten Sicherheitsregeln) und dem Fehlen einer allgemeingültigen Lösung sind inzwischen Unternehmen jeder Größe gefährdet. Das Geschäftsmodell von Cyberkriminellen besteht häufig darin, so viel wie möglich von einem Unternehmensnetzwerk zu verschlüsseln, um dann ein Lösegeld von Tausenden bis Millionen Dollar zu erpressen.

Aber es steht weit mehr auf dem Spiel als nur das Unternehmensergebnis. Die Folgen eines Ransomware-Angriffs können verheerend sein: Ausfallzeiten können den Geschäftsbetrieb zum Erliegen bringen, die Produktivität beeinträchtigen und Ihre Daten gefährden.

Falls proprietäre Firmendaten verloren gehen oder kompromittiert werden, beschädigt dies wahrscheinlich Ihre Marke sowie das Ihnen entgegengebrachte Kundenvertrauen. Laut einer Umfrage aus dem Jahr 2020 waren 80 % der Datenschutzverletzungen mit persönlich identifizierbaren Informationen (PII) von Kunden verbunden. Geistiges Eigentum wurde bei 32 % der Angriffe kompromittiert und anonymisierte Kundendaten wurden bei 24 % der Verstöße kompromittiert. Ganz zu schweigen davon, dass Cyberkriminelle die sensiblen Daten gegen Ihr Unternehmen verwenden oder damit andere böswillige Handlungen vornehmen können, beispielsweise den Verkauf vertraulicher Daten.

Da sich Ransomware schnell über Netzwerke hinweg verbreitet, reicht es nicht aus, die Netzwerkgrenzen zu schützen.

Akamai

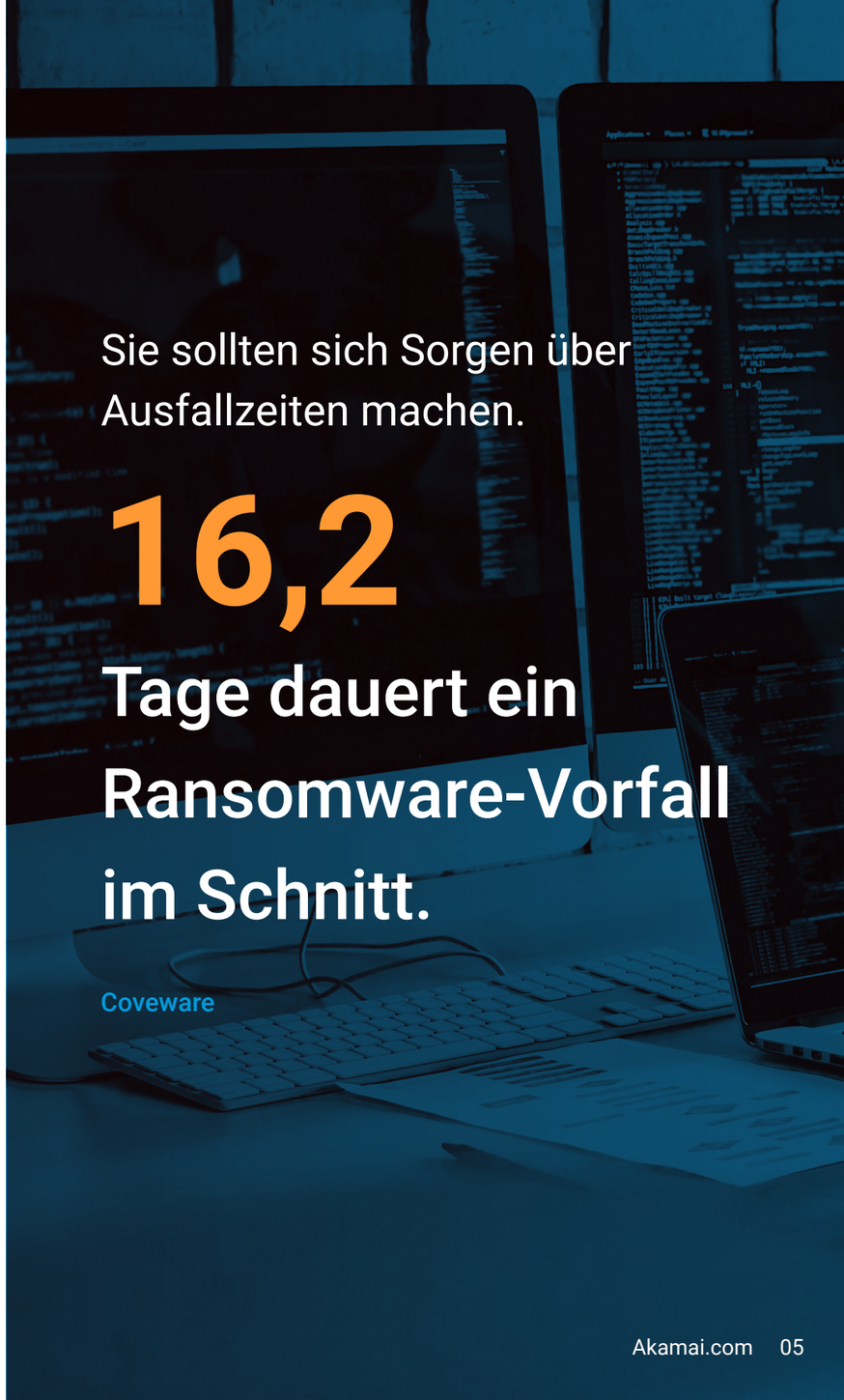
Stoppen Sie laterale Netzwerkbewegungen. Stoppen Sie die Verbreitung von Ransomware.

Ein Ransomware-Angriff beginnt mit einem ersten Eindringen, das häufig durch eine Phishing-E-Mail, eine Schwachstelle am Netzwerkrand oder Brute-Force-Angriffe ermöglicht wird. Derartige Angriffe verschaffen dem Angreifer Zugriff und lenken gleichzeitig die Verteidigung von seiner eigentlichen Absicht ab.

Sobald der Angriff in einem Gerät oder einer Anwendung erfolgreich war, wird er durch eine laterale Bewegung über das Netzwerk und mehrere Endpoints geführt, sodass sich die Infektions- und Verschlüsselungspunkte maximieren. Angreifer übernehmen in der Regel die Kontrolle über einen Domain-Controller, kompromittieren die Anmeldedaten und suchen und verschlüsseln anschließend das Backup, um zu verhindern, dass der Betreiber die lahmgelegten Dienste wiederherstellen kann.

Laterale Netzwerkbewegungen entscheiden über den Erfolg eines Angriffs. Wenn sich die Malware nicht über ihren ursprünglichen Ansatzpunkt hinaus ausbreiten kann, ist sie nutzlos. Daher ist es wichtig, laterale Bewegungen zu unterbinden.

Wie umfassend ist Ihre Strategie zur Abwehr von Ransomware?



Risikominderung

Aufbau einer erstklassigen Verteidigungsstrategie

Das Erkennen und Verhindern von lateralen Bewegungen innerhalb Ihres Netzwerks beruht auf zwei zentralen Maßnahmen: Reduzieren **Sie zunächst den ersten Angriffsvektor** und **begrenzen Sie dann die Ausbreitungspfade**.

Sie können beispielsweise die Anzahl der mit dem Internet verbundenen Server begrenzen, das Patch-Management stets auf dem aktuellen Stand halten, um Angriffsflächen weitgehend zu verringern, die Ausbreitungspfade zwischen Anwendungen reduzieren und Backups Ihrer Daten erstellen, damit Sie schnell wieder online sind und einen umfassenden Datenverlust im Falle eines Angriffs vermeiden.

Vier Möglichkeiten, die Sicherheitsplanung zur Priorität zu erheben

Die Sicherheit sollte Teil der umfassenderen Vorbereitungsstrategie, Planung und des Budgets Ihres Unternehmens sein. Dies bedeutet, dass Sie Ihre Führungskräfte und Vorstandsmitglieder sensibilisieren müssen, hinsichtlich potenzieller Risiken wachsam zu bleiben und die zur Minderung dieser Risiken notwendigen Maßnahmen zu kennen.

1. Stellen Sie sicher, dass Sie Cybersicherheit in die Geschäftseinheit einbeziehen, die für die allgemeine Risikominderung in Ihrem Unternehmen zuständig ist. Und sorgen Sie dafür, dass Ihr Führungsteam über Sicherheitsexpertise verfügt.
2. Vergessen Sie nicht, Budget und Ressourcen für das Generieren von Backups und die Netzwerksegmentierung zuzuweisen.
3. Erstellen Sie bereits im Vorfeld eines möglichen Notfalls oder unerwünschten Ereignisses (wie eines Ransomware-Angriffs) Reaktionspläne. Wenn Sie gut organisiert und vorbereitet sind, können Sie schneller und effizienter reagieren.
4. Analysieren Sie die Auswirkungen auf die Sicherheit jedes Mal, wenn Sie neue Produkte und Services integrieren, entwerfen oder entwickeln. Stellen Sie sich folgende Frage: Öffne ich damit eine neue Tür für Angreifer?

Checkliste zur Erkennung von Ransomware

Was geschieht in Ihrem Netzwerk?

In vielen Unternehmen kann das Erkennen von Ransomware durchaus eine Herausforderung darstellen. Leider bedeutet dieser Umstand auch, dass Ihr Netzwerk anfällig für Angriffe ist. Es ist zu spät, erst zu reagieren, wenn Sie eine Lösegeldforderung erhalten, weil Sie keine zuverlässige Erkennungsfunktionen implementiert haben: Denn der Großteil Ihres Netzwerks wird dann bereits verschlüsselt sein.

Sie müssen Ransomware stoppen, während sie sich ausbreitet. Dafür benötigen Sie Folgendes:

Umfassende Einblicke

Wenn Sie nicht wissen, was in Ihrem Netzwerk vor sich geht, können Sie Ransomware oder andere unerwünschte Cyberbedrohungen nicht erkennen.

IDS-System und Tools zur Malware-Erkennung

Diese erkennen die Verbreitungsversuche der Ransomware-Betreiber mithilfe vordefinierter Regeln und Signaturen für bekannte Schwachstellen oder Exploits oder durch eine allgemeinere oder automatisierte Erkennung von Anomalien.

Segmentierungsrichtlinie

Sobald alle Kommunikationsaspekte definiert und berücksichtigt wurden, löst alles außerhalb der Norm einen Alarm aus und Sie werden benachrichtigt.

Täuschungs-Tools

Köder, Honeypots oder eine Distributed Deception Platform, die nicht autorisierte laterale Bewegungen erkennen kann, können eine effektive Möglichkeit sein, einen aktiven Angriff bei High-Fidelity-Vorfällen aufzudecken.

Aufbau einer Verteidigungsstrategie gegen Ransomware

Auch mit der besten Netzwerkverteidigung lassen sich Sicherheitsverletzungen nicht gänzlich vermeiden. Aus diesem Grund benötigen Sie eine Verteidigungsstrategie, die die Effektivität von Angriffen minimiert und die Ausbreitung innerhalb Ihres Netzwerks verhindert. Sie benötigen einen Anbieter einer umfassenden Sicherheitslösung, die Bedrohungen im East-West-Traffic des Rechenzentrums erkennt und laterale Bewegungen blockiert.

Vorbeugen

Streben Sie eine Lösung an, mit der Sie alle Anwendungen und Assets identifizieren können, die in Ihrer IT-Umgebung ausgeführt werden. Mithilfe dieses umfassenden Einblicks können Sie kritische Assets, Daten und Backups schnell zuordnen und Schwachstellen und Risiken identifizieren. Wenn Sie ein vollständiges Bild Ihrer Netzwerkumgebung haben, können Sie bei einem Angriff schnell reagieren und Regeln aktivieren.

Verhindern

Sie sollten mit Ihrer Lösung Regeln festlegen können, um gängige Ransomware-Verbreitungstechniken zu blockieren. Mithilfe der softwaredefinierten Segmentierung können Sie Zero-Trust-Mikronetzwerke rund um kritische Anwendungen, Backups, Fileserver und Datenbanken erstellen. Sie können auch Segmentierungsrichtlinien anlegen, die den Traffic zwischen Nutzern, Anwendungen und Geräten einschränken und somit jegliche Versuche lateraler Netzwerkbewegungen unterbinden.

Erkennen

Implementieren Sie eine Lösung, die Sie auf jeden Zugriffsversuch auf segmentierte Anwendungen und Backups aufmerksam macht. Diese blockierten Zugriffsversuche sind Anzeichen für laterale Bewegungen. Außerdem sollten Sie einen reputationsbasierten Erkennungsansatz integrieren, der auf das Vorhandensein bekannter schädlicher Domains und Prozesse aufmerksam macht. Durch die schnelle Erkennung von Angriffen, die erfolgreich in das Netzwerk eingedrungen sind, können Sie die Verweilzeit minimieren und Angreifer abfangen, bevor sie den ursprünglichen Ansatzpunkt passieren können.

Beheben

Die automatische Einleitung von Maßnahmen zur Eindämmung und zur Quarantäne von Bedrohungen ist von entscheidender Bedeutung, sobald ein Angriff erkannt wird. Wenden Sie Isolationsregeln an, die eine schnelle Trennung von betroffenen Bereichen des Netzwerks ermöglichen. Darüber hinaus blockieren Segmentierungsrichtlinien den Zugriff auf kritische Anwendungen und System-Backups.

Wiederherstellen

Und nicht zuletzt benötigen Sie ebenfalls Visualisierungsfunktionen. Diese sollten schrittweise Wiederherstellungsstrategien unterstützen, bei denen die Konnektivität nach und nach wiederhergestellt wird, wenn in verschiedenen Bereichen des Netzwerks Entwarnung gegeben wird.

Akamai

Fazit

Zusammenfassung

Sind Sie von Ihrer Verteidigungsstrategie überzeugt?

Das Ransomware-Problem wird nicht einfach so verschwinden. Tatsächlich waren 2021 66 % der Unternehmen von Ransomware betroffen, ein Anstieg von 78 % gegenüber 2020, und diese Zahl scheint nicht zu sinken. Das bedeutet, dass die Welt weiterhin mit häufigeren Angriffen, größeren, wertvolleren Zielen und höheren Lösegeldforderungen zu kämpfen haben wird – und das alles mit erheblichen Konsequenzen für Ihr Unternehmen. Heute benötigen Sie mehr denn je Strategien zur Vorausplanung und Risikominderung, die über einen reinen Netzwerkansatz hinausgehen.

Verhindern Sie die lateralen Netzwerkbewegungen von Ransomware in Ihrem Netzwerk. Akamai zeigt Ihnen, wie Sie dabei am besten vorgehen.

Weitere Informationen finden Sie unter akamai.com/guardicore.