vmware

20 Best Practices zum Durchsetzen von Ransomware-Schutz auf Zero-Trust-Basis

Ransomware-Angriffe verursachen Ausfallzeiten und finanzielle Verluste, schädigen den Ruf eines Unternehmens und beeinträchtigen dadurch die Business-Continuity massiv. Die durchschnittliche Ausfallzeit nach einem Ransomware-Angriff beträgt ungefähr 30 Tage und 96 % der Betroffenen können selbst nach Zahlung des Lösegelds nicht mehr auf all ihre Daten zugreifen.[1]

Wie wahrscheinlich ist es, dass Ihr Unternehmen Ziel eines Ransomware-Angriffs wird? Laut dem VMware-Report „Modern Bank Heists" aus dem Jahr 2022 wurden 63 % der Befragten in irgendeiner Form Opfer eines zerstörerischen Angriffs – 17 % mehr als 2021.[2] Tatsache ist, dass es sich Ihr Unternehmen nicht leisten kann, das Bedrohungspotenzial von Ransomware zu unterschätzen. Halbherzige Maßnahmen und Legacy-Strategien reichen nicht aus. Unternehmen benötigen ein ganzheitliches Konzept, das kontextbezogene Transparenz sowie vorbeugende und Recovery-Maßnahmen kombiniert.

277 Tage
durchschnittliche Verweildauer (Zeit bis zum Erkennen und Schließen eines Datenlecks)[3]

30 Tage
Ausfallzeit nach einem Ransomware-Angriff im Durchschnitt, aber auch deutlich längere Ausfälle sind möglich[1]

Prävention ist die beste Verteidigung

Wenn bösartiges Verhalten bereits im Vorfeld eines Angriffs erkannt wird, kann dieser automatisch blockiert werden.

20 Best Practices, empfohlen von unseren Sicherheitsexperten

1 Sensibilisierungs- und Schulungsprogramm implementieren
Anwender sind die häufigsten Ziele. Daher ist es wichtig, dass alle die Bedrohung durch Ransomware kennen und wissen, wie sie auftritt.

2 Alle ein- und ausgehenden E-Mails scannen und filtern
Durch Prüfen der Inhalte auf Vertrauenswürdigkeit und E-Mail-Filter erkennen Sie Bedrohungen, bevor sie Anwender erreichen.

3 Starke Spamfilter aktivieren
Spamfilter können verhindern, dass Phishing-E-Mails zu Anwendern gelangen.

4 Werbeblocker
Ransomware wird häufig über bösartige Werbung von bestimmten Websites verteilt. Dieses Risiko kann durch das Blockieren von Werbung verringert werden.

5 Firewalls konfigurieren
Interne und Perimeter-Firewalls erlauben berechtigten Anwendern und Workloads, auf Daten zuzugreifen, und blockieren den Zugriff für bekannte bösartige IP-Adressen.

6 Netzwerke logisch trennen
Durch das Trennen von Netzwerken verhindern Sie die Ausbreitung von Malware. Wenn sich alle Anwender und Server im selben Netzwerk befinden, können sich die neuesten Malware-Varianten ausbreiten.

7 East-West-Traffic (internen Traffic) überprüfen
Dadurch können Anomalien bei Zertifikaten erkannt werden, wenn der Datenverkehr verschlüsselt wird.

8 North-South-Traffic überprüfen
Mit Threat Intelligence werden bösartige IP-Adressen, Domänen usw. aufgespürt und Command-and-Control-Datenverkehr wird erkannt.

9 Netzwerkartefakte scannen
Das Verhalten von Dateien wird dynamisch auf Bedrohungen analysiert, indem mit KI nach Schadcode gesucht wird.

10 Daten nach ihrem Wert für das Unternehmen kategorisieren
Implementieren Sie eine physische und logische Trennung von Netzwerken und Daten für unterschiedliche Organisationseinheiten.

11 Prinzip der minimalen Zugriffsrechte für Konten anwenden
Sofern nicht unbedingt erforderlich, sollte Anwendern kein Administratorzugriff gewährt werden.

12 Anwendungskontrolle für kritische Systeme
Implementieren Sie eine Richtlinie, durch die nicht genehmigte Programme und Skripts standardmäßig abgelehnt werden. So stoppen Sie Ransomware, bevor diese Ihre kritischen Ressourcen erreicht.

13 Betriebssysteme, Software und Firmware auf Geräten patchen
Wir empfehlen ein zentrales System für das Patch-Management.

14 Prozesse zur Erkennung und Beseitigung von Schwachstellen etablieren

15 Daten regelmäßig sichern
Überprüfen Sie die Integrität der Backups und testen Sie den Wiederherstellungsprozess, um sicherzugehen, dass im Ernstfall alles funktioniert.

16 Offline-Backups schützen
Stellen Sie sicher, dass Backups nicht dauerhaft mit den Computern und Netzwerken verbunden sind, die sie sichern.

17 Jährliche Penetrationstests und Schwachstellen-Assessments

18 Reaktionsplan erstellen
Erstellen Sie einen Plan für die Wiederherstellung nach Ransomware und testen Sie ihn regelmäßig.

19 Verhaltensanalyse
Analysieren Sie das Verhalten aktiver Workloads mit Tools, um bei der Wiederherstellung dateilose Bedrohungen durch Ransomware einzudämmen und zu beseitigen.

20 Sicherheitstests
Stellen Sie eine isolierte Wiederherstellungsumgebung bereit, um Workloads sicher zu testen und zu iterieren und im Falle eines erfolgreichen Ransomware-Angriffs zu schützen.

Schützen Sie Ihr Multi-Cloud-Netzwerk umfassend vor Ransomware. Starten Sie jetzt: vmware.com/solutions/ransomware-protection.

1. Sophos, „The State of Ransomware 2022", April 2022
2. VMware, „Modern Bank Heists 5.0", April 2022
3. IBM Security, „Cost of a Data Breach Report 2022", Juli 2022

vmware

Artikelnr.: 1985358aq-info-best-prac-prot-ransmwr_DE 5/23