BlackBerry | Cybersecurity

RANSOMWARE-PRÄVENTION IST MÖGLICH

Effektiver Schutz vor Ransomware beginnt mit einer Zero-Trust-Mentalität und einer präventiven Strategie. Ob doppelte, dreifache oder gar vierfache Erpressung – angesichts der aktuell teuersten und gefährlichsten Malware-Bedrohungen brauchen Unternehmen unbedingt eine angemessene Verteidigung, eine Minimierung der Angriffsfläche und die Fähigkeit, Bedrohungsakteure zu stoppen, bevor diese überhaupt aktiv werden.

Die Folgen von Ransomware

Ransomware ist eine ernsthafte Bedrohung für Unternehmen. Auch 2021 erwies sie sich wieder als eine wachsende Gefahr:

1,85 MILLIONEN $
kostete ein Ransomware-Angriff 2021 im Durchschnitt[1]

21 TAGE
beträgt die durchschnittliche Ausfallzeit für Unternehmen[2]

14 VON 16
kritischen Infrastruktursektoren wurden 2021 angegriffen[3]

32 % DER ENTSCHEIDER
mussten ihren Arbeitsplatz nach einem folgenschweren Ransomware-Angriff räumen[4]

80 % DER UNTERNEHMEN
wurden wiederholt Opfer eines Angriffs[5]

ZEITLEISTE RANSOMWARE

1989
Erster bekannter Ransomware-Angriff
Üblicher Ablauf: Daten werden verschlüsselt → Geld wird erpresst → Nach der Lösegeldzahlung wird ein Entschlüsselungsschlüssel bereitgestellt

2017
WannaCry und Not-Petya verursachten eine globale Sicherheitskrise
- *WannaCry wütete in 150 Ländern*[6]
- *NotPetya verursachte weltweit einen Schaden von über 10 Milliarden $*[7]

2019
Erste bekannte doppelte Erpressung
Die Zahl der Unternehmen, deren Daten im Beobachtungszeitraum auf einer Erpressungsseite veröffentlicht wurden, stieg um 935 %[8]

2020
Erste bekannte dreifache Erpressung
Der Anstieg bei Ransomware um 93 % geht hauptsächlich auf das Konto der dreifachen Erpressung[9]

2021
Erste bekannte vierfache Erpressung
- *Diese Angriffsart ist sehr selten.*
- *Die durchschnittlichen Lösegeldzahlungen stiegen um 171 % auf mehr als 312 Tsd. $*[10]

RANSOMWARE IST BELIEBTER DENN JE

Dem BlackBerry® Threat Research zufolge sind dies die Top-Ransomware Bedrohungen des vergangenen Jahres:

REVIL

Üblicherweise verbreitet durch:
- Phishing-Attacken
- Bekannte Software-Schwachstellen
- Brute-Force-Angriffe auf Remote Desktop Protokoll (RDP)

DARKSIDE
- Nutzt doppelte Erpressungstaktiken
- Zielt ab auf Windows®- und Linux®-Systeme

CONTI
- Im Visier waren weltweit die verarbeitende Industrie sowie Unternehmen im Gesundheitswesen und der Versicherungsbranche
- Sehr anpassungsfähig, gegen eine Vielzahl von Zielen einsetzbar

AVADDON
- Erstmals 2020 in Erscheinung getreten
- Nutzt doppelte und dreifache Erpressung

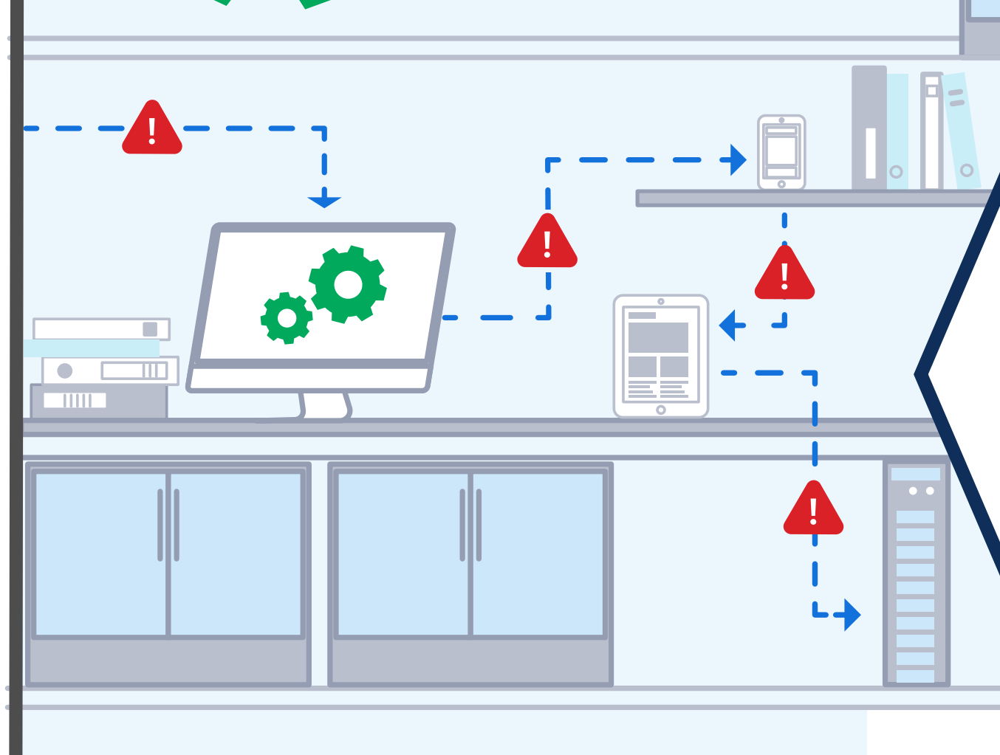
RAGNAR LOCKER
- Beliebt bei Bedrohungsakteuren, die ihre Angriffe als Service für ihre Opfer tarnten[11]
- Nutzt doppelte Erpressung und listet seine Opfer auf der „Wand der Schande“ auf

HIVE
- Charakteristisch ist die Nutzung der relativ neuen Programmiersprache Go
- Setzt doppelte Erpressung ein

TIPPS ZUM SCHUTZ VOR RANSOMWARE-ATTACKEN

1 Aktualisieren Sie Ihre Software

Viele Ransomware-Kampagnen nutzen bekannte Schwachstellen aus. Wenn Ihre Gerätesoftware immer auf dem neuesten Stand ist, nehmen Sie den Bedrohungsakteuren einen großen Vorteil.

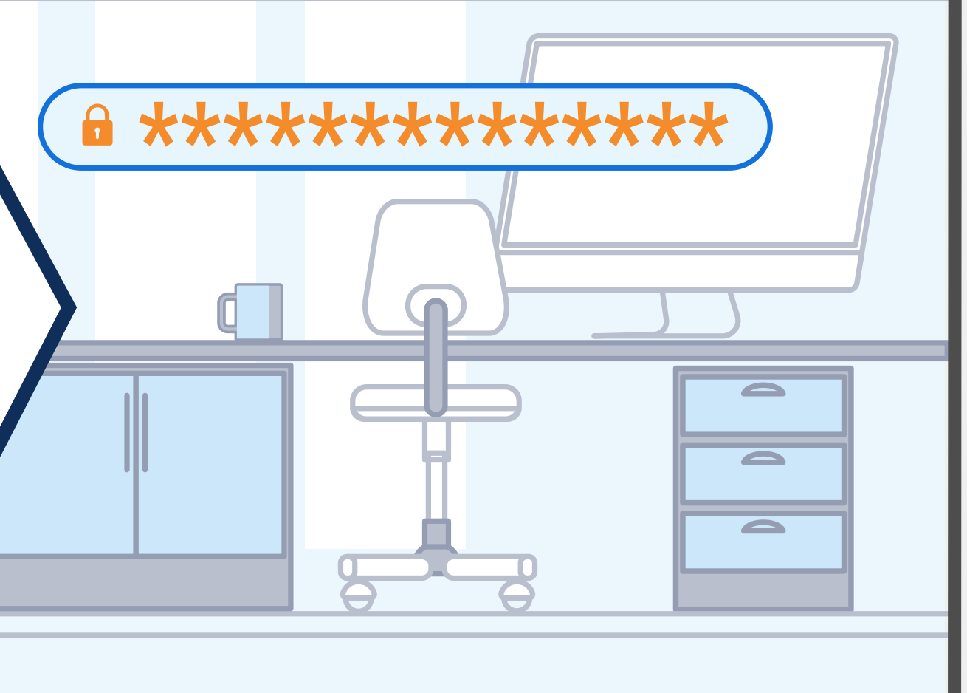


2 Tracken und verwalten Sie Schwachstellen

Implementieren Sie ein System zur Nachverfolgung von Schwachstellen bei Netzwerken, Geräten und Services, da sich Ihre Umgebung schnell ändern kann.

3 Arbeiten Sie mit starken Passwortrichtlinien und Multi-Faktor-Authentifizierung (MFA)

Kompromittierte und geteilte Zugangsdaten sind eine gefährliche Schwachstelle.

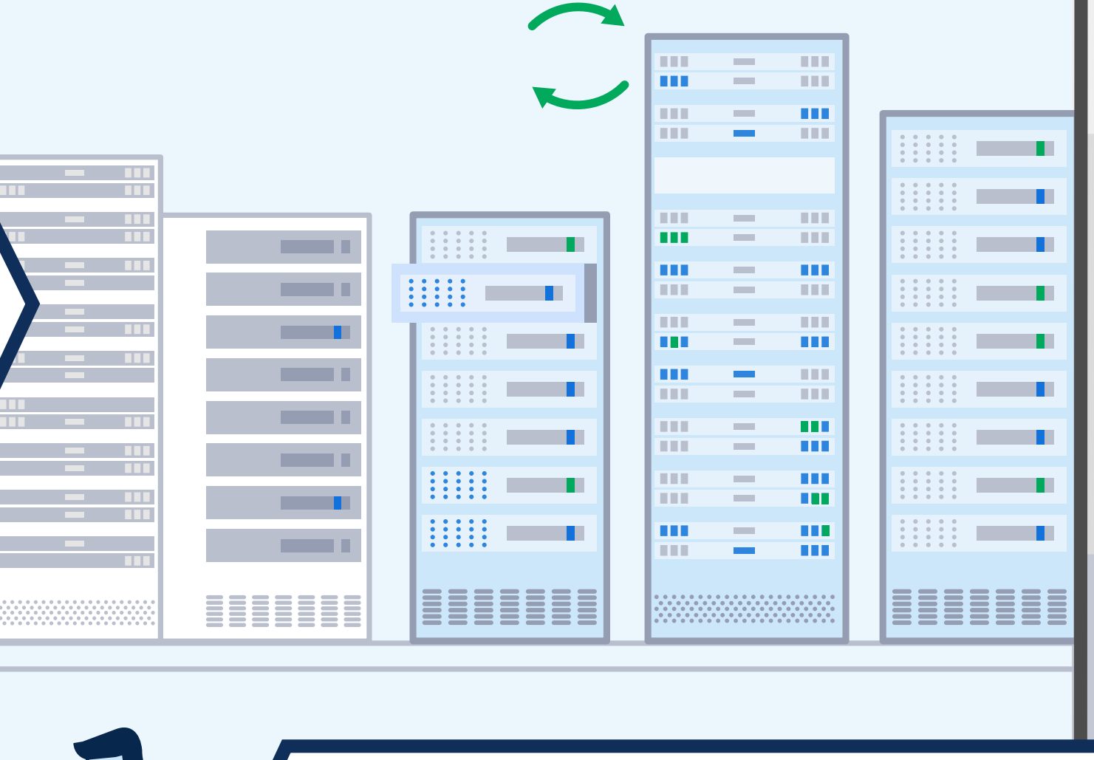


4 Reduzieren Sie Ihre Angriffsfläche

Befolgen Sie das Least-Privilege-Prinzip. Entfernen Sie unnötige Geräte und Software aus Ihrer Umgebung. Beschränken Sie Netzwerkverbindungen und -zugriff aufs Nötigste.[12]

5 Schützen Sie sensible Daten

Erstellen Sie starke Richtlinien für die Datenwiederherstellung (inklusive Tests und Back-ups).



6 Verfolgen Sie bewährte Sicherheitspraktiken

Schulen Sie Mitarbeiter, nutzen Sie MFA und implementieren Sie starke Passwörter.

SEIEN SIE VORBEREITET.

Schützen Sie Ihr Unternehmen jetzt vor Ransomware mit einer hochwertigen und bezahlbaren Lösung der nächsten Generation, die Ihnen Managed Extended Detection and Response (XDR) Plattformen und künstliche Intelligenz (KI) bietet. Mit der Cylance® Endpoint Security profitiert Ihr Unternehmen von KI-gesteuertem Schutz und einem Zero-Trust-Framework, das jedes Gerät überall und jederzeit vor Ransomware schützen kann.

Weitere Informationen zur
Prävention und Beseitigung von Ransomware
finden Sie auf unserer Website →

BlackBerry | Cybersecurity

Über BlackBerry: BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Das Unternehmen sichert mehr als 500 Millionen Endpunkte ab, darunter 215 Millionen Fahrzeuge. Das Unternehmen mit Sitz in Waterloo, Ontario, setzt KI und maschinelles Lernen ein, um innovative Lösungen in den Bereichen Cybersicherheit, Sicherheit und Datenschutz zu liefern, und ist in den Bereichen Endpoint Security, Endpoint Management, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist klar – das Sichern einer vernetzten Zukunft, der Sie vertrauen können.

*Besuchen Sie für weitere Informationen **BlackBerry.com** und folgen Sie **@BlackBerry**.*

---

[1] https://www.itpro.com/security/ransomware/359364/cost-of-ransomware-doubles-in-a-year

[2] https://www.forbes.com/sites/hillennevins/2021/07/26/how-to-survive-a-cybersecurity-attack/

[3] https://www.securityweek.com/ransomware-targeted-14-16-us-critical-infrastructure-sectors-2021

[4] https://www.techrepublic.com/article/the-many-ways-a-ransomware-attack-can-hurt-your-organization

[5] https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/

[6] https://dataprot.net/statistics/ransomware-statistics/

[7] https://dataprot.net/statistics/ransomware-statistics/

[8] https://www.rhisac.org/ransomware/ransomware-double-and-triple-extortion/

[9] https://cybernews.com/news/ransomware-surged-93-in-last-6-months-fueled-by-triple-extortion/

[10] https://threatpost.com/ransomware-payments-quadruple-extortion/168622/

[11] https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-ransomware-what-you-need-to-know/

[12] https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege