Checkliste: Schutz vor Ransomware im Zeitalter flexibler Arbeitsmodelle

kaspersky BRING ON THE FUTURE

Ransomware stellt nach wie vor für jedes Unternehmen eine zunehmende Bedrohung dar. Einer Schätzung zufolge sind 15,45 % aller Internetnutzer im Jahr 2021 mindestens einem Malware-basierten Angriff zum Opfer gefallen[1]. Vor diesem Hintergrund überrascht es nicht, dass Cybersicherheit zu einer der wichtigsten strategischen Prioritäten von Unternehmen geworden ist.

Infolge der zunehmenden Verlagerung der Arbeit ins Homeoffice im Zuge der Pandemie ist das Risiko einer Ransomware-Infektion in den letzten Jahren erheblich gestiegen. Untersuchungen zeigen, dass der schnelle Umstieg auf Remote-Arbeitsplätze dazu geführt hat, dass viele Unternehmen ihre Kontrollmechanismen abgeschwächt oder Sicherheitsprotokolle gelockert haben.

Bei Ransomware geht es vor allem darum, den Zugriff auf die verschlüsselten Daten so schnell wie möglich wiederherzustellen. Dabei darf man nicht vergessen, dass sich Cyberkriminelle die Dateien zusätzlich auch noch aneignen, um anschließend das Unternehmen noch einmal zu erpressen, dieses Mal mit der Veröffentlichung der sensiblen Daten.

Im Jahr 2021[2] haben weniger Unternehmen Tools für die Netzwerksicherheit (Abnahme um 5 %) oder die Überwachung von Endbenutzern (Abnahme um 6 %) eingesetzt. Ohne wirksame Endpoint-Überwachung und -Sicherheit nimmt das Risiko, einer Erpressung durch Ransomware zum Opfer zu fallen, rasant zu.

Endgeräte waren schon immer ein schwaches Glied in der Unternehmenssicherheit, mit dem Hacker oft leichtes Spiel haben. Aber mit der zunehmenden Fernarbeit befinden sich diese Endpoints jetzt auch noch **außerhalb** des Netzwerks, was die Verwaltung und Absicherung zusätzlich erschwert. Durch die räumliche Trennung haben Angreifer eine größere Auswahl an potentiellen Zielen, was ihre Erfolgschancen weiter erhöht.

Um einen größeren Ransomware-Übergriff zu verhindern, muss eine wirksame Ransomware-Strategie auf mehreren Ebenen greifen. Da das Arbeiten an entfernten Standorten immer mehr zum Normalfall wird, müssen Unternehmen ihren Endpoint-Schutz verstärken – vor allem im Hinblick auf die Erkennung und Abwehr von Ransomware-Infektionen.

Sie können diesen Leitfaden wie eine praktische Checkliste nutzen, um abzuhaken, in welchen Bereichen Sie gut vor Ransomware am Netzwerkrand geschützt sind und an welchen Stellen Sie nachbessern sollten.

- **1. Ransomware-Erkennung an Endpoints**
- **2. Endpoint-Konfiguration**
- **3. Vorkehrungen für Datensicherungen**
- **4. Auslagerung**
- **5. Schulungen für Endbenutzer**
- **6. Incident Response-Planung**

[1] Kaspersky Security Bulletin 2021. Statistik – Kaspersky–https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/

[2] Cyber Security Breaches Survey 2021 – Britisches Ministerium für Digitales, Kultur, Medien und Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

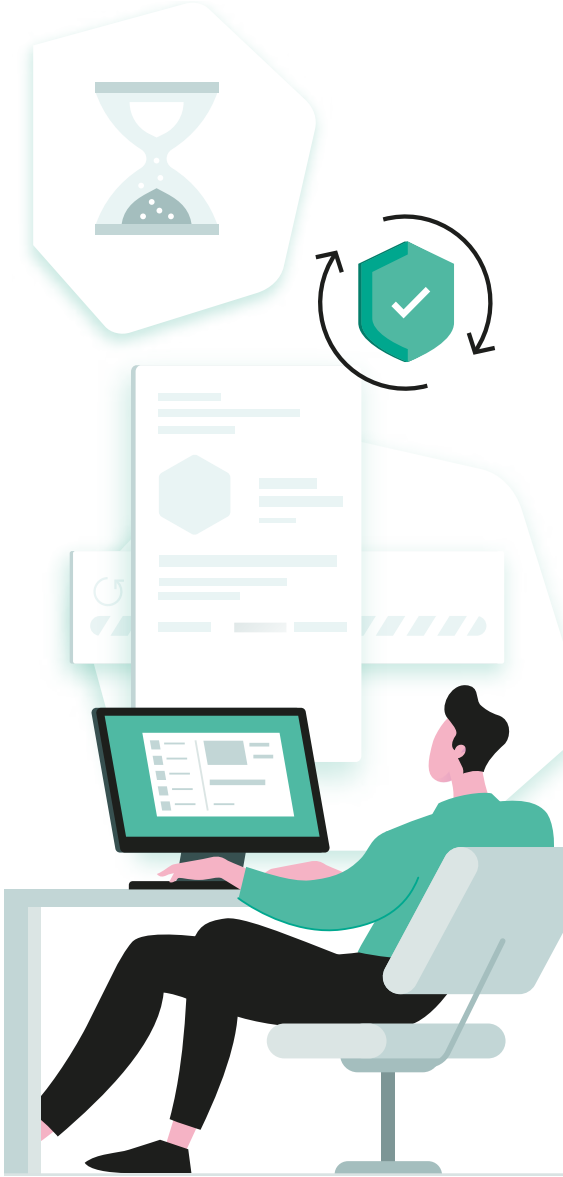
1. Ransomware-Erkennung an Endpoints

Der vielleicht wichtigste Schritt besteht darin, Ransomware zu stoppen, bevor sie sich ausbreiten kann. Je schneller die Infektion erkannt und abgewehrt wird, desto weniger Schaden kann sie anrichten.

In der Regel kann Ihr Unternehmen Malware gleich am Mail-Server abfangen, wenn diese direkt per Mail an die Mitarbeiter verschickt wurde. Aber damit verhindern Sie noch nicht, dass Mitarbeiter schädliche Programmdateien über eine gut gemachte Spear-Phishing-Mail öffnen.

Sie können Ihre Ransomware-Erkennung verbessern, indem Sie die Ausführung verdächtiger Programmdateien am Endpoint unterbinden:

- **Mithilfe eines robusten Malware-Schutzes lassen sich verdächtige Programmdateien identifizieren und entfernen, bevor es zu einer Verschlüsselung sensibler Dateien kommt.**
- **Nutzen Sie die lernfähigen Algorithmen von EDR-Tools (Endpoint Detection and Response), um verdächtige Systemaktivitäten automatisch zu erkennen und zu blockieren.**
- **Ziehen Sie den Einsatz einer Managed Detection and Response-Lösung (MDR) in Betracht, um Ransomware automatisiert und effektiver zu bekämpfen.**



Malware-Schutztools helfen eine Infektion einzudämmen und an der Ausbreitung auf andere Dateispeicher und Systeme zu hindern.

Durchaus erwähnenswert ist, dass Behörden und Regierungsstellen in ihren Ratschlägen an die Opfer von Ransomware mittlerweile eine schärfere Haltung einnehmen. So appellierte das FBI Internet Crime Complaint Center (IC3) 2019 an Unternehmen, Lösegeld unter keinen Umständen zu zahlen[3].

Dieser Empfehlung schließt sich auch Kaspersky an: „Gehen Sie nicht auf die Geldforderungen ein. Jede Lösegeldzahlung leistet einen finanziellen Beitrag zur Malware-Entwicklung und ist ein Signal an die Cyberkriminellen, dass sich die Methode lohnt. Es kann auch durchaus sein, dass Sie nichts bekommen, auch wenn Sie der Forderung nachkommen."[4]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät: „Der beste Schutz vor Lösegeldforderungen durch Cyberkriminelle sind konsequent umgesetzte IT-Sicherheitsmaßnahmen."[5]

Konsequent umgesetzte IT-Maßnahmen bedeutet, dass **außerhalb** des Netzwerkperimeters ein ähnlicher Schutz für die Endgeräte besteht wie innerhalb – in diesem Fall wirksamer, zuverlässiger Malware-Schutz und intelligente EDR-Tools, die Ransomware-ähnliche Aktivitäten automatisiert erkennen können.

2. Endpoint-Konfiguration

Schon mit der richtigen Konfiguration der Endpoints können Sie die potentiellen Auswirkungen einer Ransomware-Infektion verringern. Auf Firmengeräten:

- Arbeiten Sie mit Listen von zugelassenen Programmen, um sicherzustellen, dass Mitarbeiter nur autorisierte Software ausführen können. Mit der korrekten Einstellung können Mitarbeiter selbst keine Anwendungen installieren und damit auch keine infizierten Programme starten.
- Stellen Sie sicher, dass die Endpoint Security-Tools – wie auch jede andere installierte Software – automatisch aktualisiert werden, damit neue Bedrohungen abgewehrt und Sicherheitslücken zeitnah geschlossen werden[6].

Als Best Practice für die Sicherheit haben sich Software-Updates innerhalb von 14 Tagen nach Freigabe der Patches bewährt. Leider halten sich nur 43 % der Unternehmen daran[7]. Eine verschenkte Gelegenheit, sich vor Ransomware zu schützen – dabei ist die Umsetzung so einfach.

[3] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations – FBI Internet Crime Complaint Center – https://www.ic3.gov/Media/Y2019/PSA191002
[4] Fünf Tipps, wie Sie sich vor Ransomware schützen können – Kaspersky – https://www.kaspersky.de/blog/ransomware-five-tips/27248/
[5] Ebd.
[6] Ransomware world in 2021: who, how and why – Kaspersky – https://securelist.com/ransomware-world-in-2021/102169/
[7] Cyber Security Breaches Survey 2021 – Britisches Ministerium für Digitales, Kultur, Medien und Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Eine besondere Herausforderung stellen BYOD-Endpoints dar, da sie sich nur eingeschränkt kontrollieren lassen. Bei diesem Betriebsmodell haben Sie folgende Möglichkeiten:

- Sie können Ihren Mitarbeitern raten, auf jedem Gerät ein zugelassenes Malware-Schutztool zu installieren. Die kostenlose Bereitstellung dieser Software ist ein guter Anreiz, da sie sowohl die privaten Daten des Mitarbeiters als auch die Firmendaten schützt.
- Führen Sie Unternehmensprogramme und -daten in einer Sandbox aus. Wenn sich ein Mitarbeiter über seine privat genutzten Programme Malware einfängt, verhindert die Sandbox im Wesentlichen die weitere Ausbreitung.

Letztendlich wird es beim Schutz beruflich genutzter privater Geräte immer auf einen Kompromiss hinauslaufen, bei dem sich Unternehmen und Mitarbeiter auf beiderseitig akzeptable Maßnahmen einigen. Ist das nicht möglich, muss Ihr Unternehmen alternative Zugangsmöglichkeiten schaffen oder den Mitarbeiter mit Firmengeräten ausstatten.

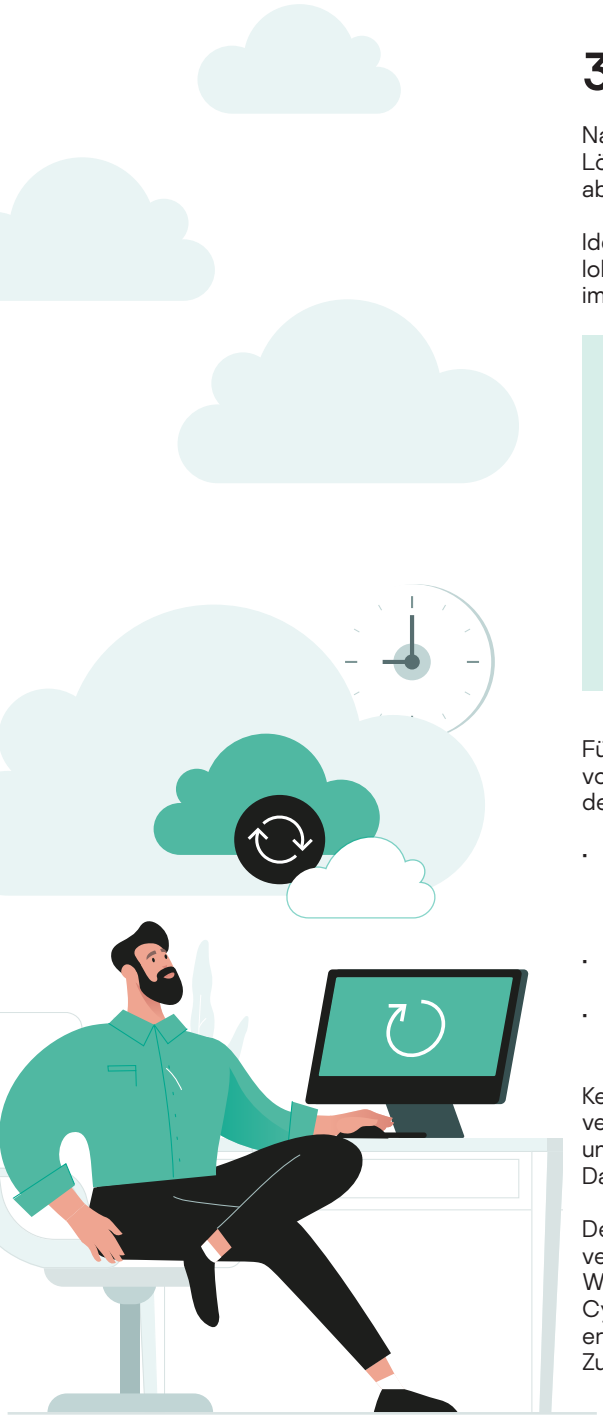
3. Vorkehrungen für Datensicherungen

Nachdem die Dateien verschlüsselt wurden, gibt es zwei Möglichkeiten: Sie bezahlen das Lösegeld oder ziehen „saubere" Kopien der Dateien aus einem Backup. Dafür braucht es aber eine solide, zuverlässige Backup-Routine für Ihre Endpoint-Geräte.

Idealerweise sollten Mitarbeiter keine Möglichkeit haben, Unternehmensdaten lokal abzuspeichern. In der Realität werden allerdings immer wieder Dokumente im Download-Ordner oder auf dem Desktop abgelegt.

Folgendes gilt es zu bedenken, wenn Sie sich daran machen, Fernarbeit sicherer zu gestalten:

- **Wie wahrscheinlich ist es, dass Unternehmensdaten lokal gespeichert werden?**
- **Welche Daten werden gespeichert?**
- **Welche Risiken bestehen, wenn diese Dateien verschlüsselt oder unzugänglich gemacht werden?**
- **Welche Möglichkeiten der Datensicherung gibt es?**



Für den Bereich außerhalb der Netzgrenzen ist das ein echtes Problem. Wie Sie dagegen vorgehen, hängt von Ihrer technischen Architektur und bis zu einem gewissen Grad von den IT-Kenntnissen des Endbenutzers ab. Mögliche Optionen:

- Synchronisierung von Daten in ausgewählten Ordnern mit einem Cloud-Speicher oder einem anderen Remote-Service, vorzugsweise mit unveränderlichen Backups, die nicht überschrieben oder geändert werden können
- Sicherung auf einem lokalen Wechseldatenträger
- Nutzung der Möglichkeiten des Betriebssystems zur Erstellung von automatischen Sicherungen und Wiederherstellungspunkten

Keine dieser Lösungen ist ideal, da die Gefahr besteht, dass Ransomware und verschlüsselte Dateien in das Backup kopiert werden. Schon allein um die Compliance- und Datenschutzvorgaben zu erfüllen, müssen Sie einen Weg finden, lokal gespeicherte Daten zu erfassen.

Denn: Die Datensicherung ist Ihre letzte Chance, wenn Ihre Dateien mit Ransomware verschlüsselt wurden. Sie dürfen auch nicht vergessen, dass Datensicherungen und Wiederherstellungspunkte keinen Schutz vor Datenlecks – oder Doxxing – bieten. Cyberkriminelle könnten Sie immer noch mit der Offenlegung sensibler Informationen erpressen. Der einzige Schutz für **vertrauliche Daten** besteht darin, Kriminelle am Zugriff auf Ihre Endpoints zu hindern.

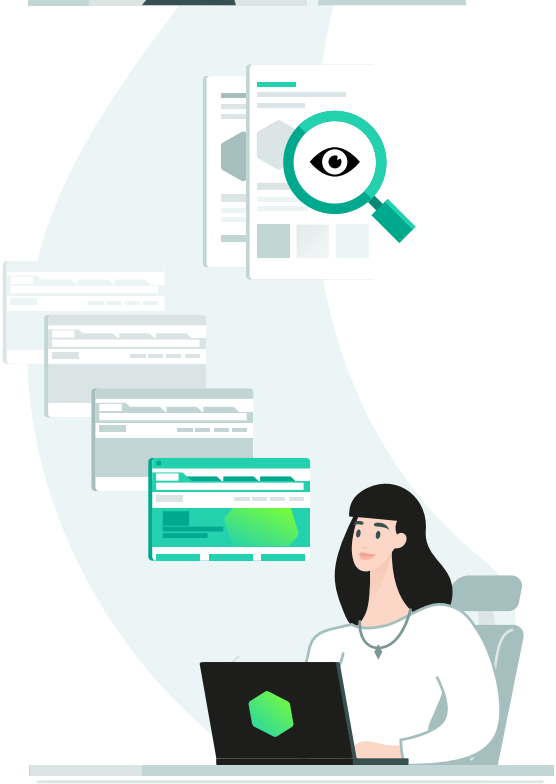
4. Auslagerung

Je mehr Daten und Anwendungen auf einem Endpoint gespeichert sind, desto mehr potentielle Schwachstellen lassen sich ausnutzen. Und desto attraktiver wird das Gerät für Hacker. Durch **Reduzierung** der Menge an lokal gespeicherten Programmen und Daten werden auch die Auswirkungen einer Ransomware-Infektion geringer.

Es gibt Cloud-Services, mit denen Sie Anwendungen auslagern und die Datenmenge auf lokalen Geräten minimieren können. Produktivitäts- und E-Mail-Programme können mittlerweile als Web-Applikationen in der Cloud ausgeführt werden. Dies gewährleistet, dass wenig bis nichts lokal übertragen wird. Vor allem E-Mail-Services bieten einen verbesserten Malware-Schutz, mit dem verdächtige Anhänge gescannt und im Falle eines Falles gesperrt werden, bevor Ihre Benutzer sie herunterladen können.

Eine weitere Möglichkeit bietet die Virtualisierung. Mit dem Streaming von Programmen und Deskops können Benutzer eine Verbindung zu einer Sitzung herstellen, die im Rechenzentrum des Unternehmens oder in der Cloud gehostet wird. Für den Endbenutzer sieht die gehostete Sitzung wie sein gewohnter Desktop aus. Alle Daten befinden sich jedoch innerhalb des virtualisierten Systems, wo auch die Verarbeitung stattfindet.

Remote Desktop-Sitzungen (RDP) gelten als das größte Einfallstor für Ransomware[8]. Bei richtiger Konfiguration lässt sich damit allerdings eine nützliche Sandbox zwischen dem Endpoint und den Unternehmenssystemen schaffen, wie die weit verbreitete Verwendung von RDP innerhalb des Unternehmensnetzwerks belegt.



Durch eine Verschärfung der folgenden Sicherheitsmaßnahmen für Endpoints lassen sich dieselben Vorteile für Remote-Mitarbeiter erzielen:

- **Einführung einer strengen Passwortpolitik, um Brute-Force-Angriffe zu verhindern**
- **Durchgängige Verwendung einer Mehrfaktor-Authentifizierung, um zu verhindern, dass Sitzungen gehackt werden**
- **VPN-Verbindungen für den gesamten Datenverkehr zwischen Endpoint und RDP-Servern**
- **Bewertung und Verschärfung der Firewall-Regeln am Netzwerkperimeter, um nicht autorisierte Verbindungen zu unterbinden**
- **Einsatz von EDR-Sicherheitstools zur Bewertung von Aktivitäten, um verdächtige Vorgänge automatisch zu erkennen und zu blockieren**
- **Auswahl von nicht standardmäßigen RDP-Verbindungsports, um Hacking-Versuche zu erschweren**

Letztendlich geht es darum, Hacker und Malware daran zu hindern, sich in die RDP-Verbindung und -Sitzung zu hacken. Und dagegen muss der Endpoint des Benutzers gesichert werden.

5. Schulungen für Endbenutzer

Mitarbeiter sind das wertvollste Kapital eines jeden Unternehmens und können einen wesentlichen Beitrag zur Eindämmung von Ransomware leisten – sofern sie wissen, was zu tun ist. Alle Mitarbeiter sollten regelmäßig geschult werden, damit sie potentielle Cyberangriffe erkennen und wissen, wie sie sich verhalten müssen. Jeden Tag klicken 2 % aller Mitarbeiter auf einen Phishing-Link[9]. Für Ransomware sind die Zahlen vermutlich ähnlich.

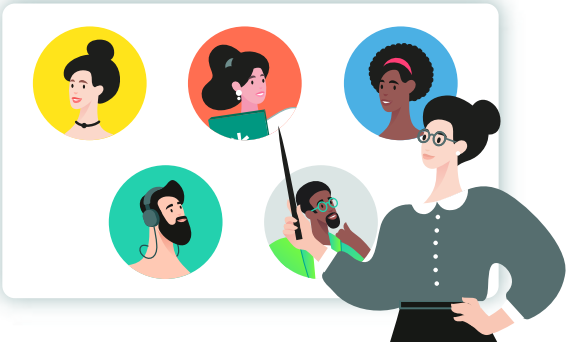
Schulungen müssen nicht nur interaktiv und praxisorientiert sein, sondern auch regelmäßig stattfinden, denn die Bedrohungen für die Cybersicherheit entwickeln sich ständig weiter. Mit einer Präsentation zum Thema Phishing-Mails und verdächtige Programmdateien wird es nicht getan sein, dazu verliert das Gehörte viel zu schnell an Aktualität (und gerät in Vergessenheit). Das müssen Sie bei der Planung von Cybersicherheitsschulungen für Remote-Mitarbeiter berücksichtigen:

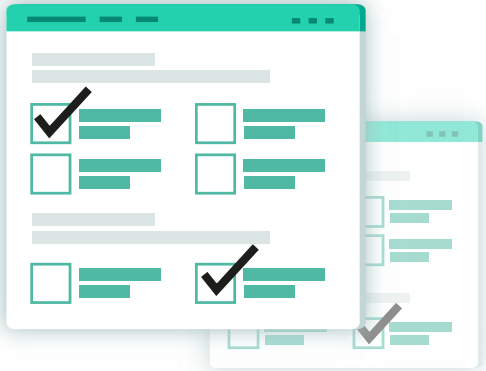
[8] How to secure RDP from ransomware attackers – Emsisoft – https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9] Mobile Security Index 2020 Report – Verizon – https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Schulungen genau auf Ihre Anforderungen anpassen

Die effektivsten Ransomware-Angriffe zielen auf ganz bestimmte Personen und Funktionen ab. Dieselbe Vorgehensweise bietet sich daher auch für Schulungen an. Mitarbeiter aus den Bereichen Buchhaltung, Marketing, Personalwesen und Führungskräfte sind mit jeweils anderen Angriffsarten konfrontiert, so dass eine Schulung auf die zu erwartenden Bedrohungen abgestimmt sein sollte.



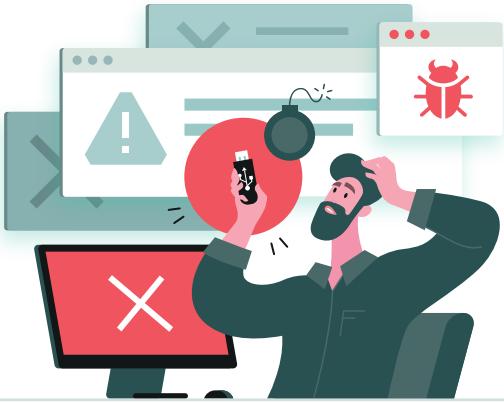


Wissen abfragen

Wissen an sich genügt nicht, man muss es auch praktisch anwenden können – gerade wenn so viel auf dem Spiel steht. Mit routinemäßigen, regelmäßigen Tests können Sie sicherstellen, dass Ihre Mitarbeiter das Gelernte bei Bedarf in die Praxis umsetzen können. Routinemäßige Bewertungen weisen darüber hinaus auf Wissenslücken oder Weiterbildungsbedarf hin und tragen zur Verbesserung der Sicherheitslage Ihres Unternehmens bei.

Nicht nur über Phishing

Phishing und schädliche Anhänge sind das offensichtlichste Einfallstor für Ransomware. Es gibt jedoch noch andere Faktoren, die Ihre Endnutzer beachten müssen. Infizierte Wechseldatenträger, schädliche Webseiten und die Überlappung von beruflichen und privaten Aktivitäten können Malware Zugang zum Endpoint und damit zum gesamten Unternehmensnetzwerk verschaffen. Sie müssen sicherstellen, dass Ihre Mitarbeiter auch für diese potentiellen Probleme geschult sind.



Unterhaltsam (und/oder interessant) gestalten

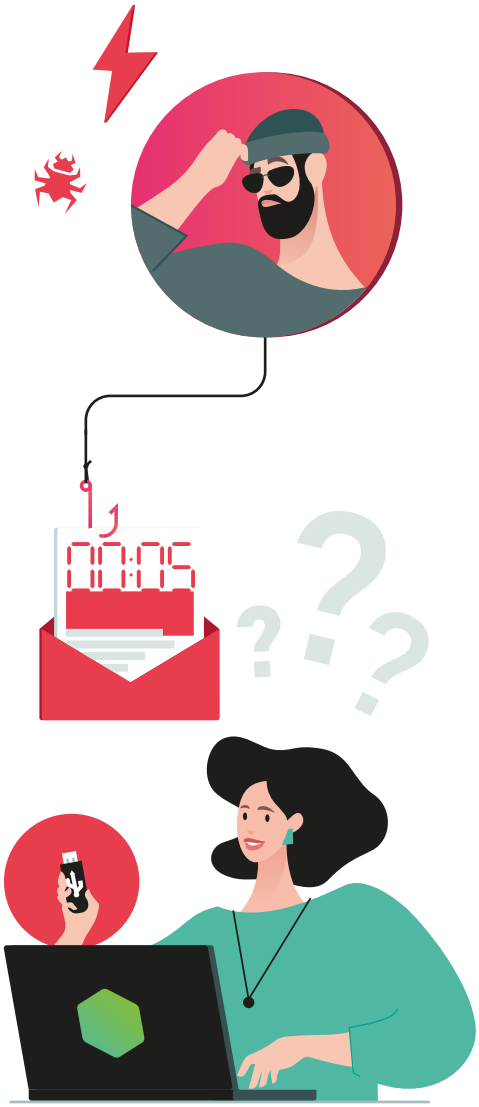
Cybersicherheit kann ein ziemlich trockenes Thema sein, vor allem, wenn sie nicht zur Kernkompetenz gehört. Dass Ihre Endbenutzer die wöchentlichen Briefings des US National Cyber Awareness System lesen (oder verstehen), ist daher eher unwahrscheinlich. Mit spielerischen Elementen können Sie Ihre Mitarbeiter motivieren, vor allem, wenn es um schwer zu vermittelnde Konzepte geht. Indem Sie Ziele setzen, den Wettbewerb fördern und für Spaß an der Sache sorgen, bleiben Ihre Mitarbeiter am Ball und können ihr Wissen und ihre Kompetenzen stetig ausbauen.

Die Investition in Ihre Endbenutzer ist ein wichtiger Schritt zur Verbesserung Ihres Endpoint-Schutzes. Den menschlichen Faktor auf ein Minimum zu reduzieren, ist tatsächlich die effektivste Form der Ransomware-Prävention. Ganz nebenbei können derart geschulte Mitarbeiter bereits im Frühstadium einer Ransomware-Infektion eingreifen, deren Ausbreitung verhindern und die Folgen für das Unternehmen begrenzen.

6. Incident Response-Planung

Es mag erstaunlich scheinen, aber 32 % der Unternehmen verfügen über keinen Reaktionsplan für den Umgang mit Cybersicherheitsvorfällen wie zum Beispiel einem Ransomware-Ausbruch[10]. Diese Unternehmen gehen ein hohes Risiko ein: Die Frage ist nicht ob, sondern wann.

Mit der Aufstellung eines Incident Response-Plans können Unternehmen Schwachstellen bewerten und geeignete Maßnahmen zu ihrer Beseitigung ergreifen. Ein solcher Plan führt auch zu einer Beschleunigung Ihrer Reaktionsfähigkeit – ein entscheidender Faktor im Umgang mit Ransomware, wo jede Sekunde zählt.



Jeder Plan zur Wiederherstellung von Endpoints (Disaster Recovery, DR) muss zwar auf Ihr Unternehmen zugeschnitten sein, sollte aber Folgendes beinhalten:

- **Eine Kommunikationsstrategie.** Sie müssen dafür sorgen, dass die richtigen Informationen zum richtigen Zeitpunkt bei den Betroffenen ankommen. Und dass Ihre Remote-Mitarbeiter Kontakt zu Experten herstellen können, die ihnen im Anfangsstadium einer Infektion helfen können.
- **Einen Angriffsplan.** Sie brauchen ein System, um dem Angriff einen Schweregrad zuzuweisen, um dann entsprechend handeln zu können. Werden Sie Lösegeld zahlen oder versuchen, die Daten aus dem Backup wiederherzustellen?
- **Zugängliche Dokumentation.** Es ist sehr wahrscheinlich, dass Ihre Mitarbeiter infolge der Endpoint-Infektion nicht auf Playbooks oder Anleitungen zur Ransomware-Bekämpfung zugreifen können. Sie müssen dafür sorgen, dass es immer eine Möglichkeit gibt, an diese Informationen zu kommen, auch wenn die Unternehmenssysteme ausgefallen sind.
- **Anleitung für Mitarbeiter.** Unmittelbar nach Auftauchen des Problems sollte dem Remote-Mitarbeiter ein Spezialist zugewiesen werden, der ihm weiterhelfen kann. Dieser Spezialist kann mit ihm die ersten Maßnahmen zur Schadensbegrenzung und Wiederherstellung durchgehen und, falls die Situation es erfordert, Daten für den Bericht an die Aufsichtsbehörden aufnehmen.
- **Erhöhte Wachsamkeit.** Sobald eine Ransomware-Infektion auf einem Remote-Endpoint festgestellt wird, muss Ihr IT-Sicherheitsteam die Überwachung und Berichterstattung verstärken, um festzustellen, ob auch zentrale Systeme betroffen sind. Nach Bedarf kann auch der Disaster Recovery-Plan in Gang gesetzt werden.

Mit einem gut durchdachten Disaster Recovery-Plan kann Ihr Unternehmen die Folgen von Malware wirksam reduzieren – und im Idealfall die Ausbreitung eindämmen, lange bevor das Schadprogramm an wichtige Systeme und Daten herankommt.

[10] Cyber Security Breaches Survey 2021 – Britisches Ministerium für Digitales, Kultur, Medien und Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Fazit

IT-Führungskräfte äußern schon seit vielen Jahren Bedenken hinsichtlich Fernarbeit – und das zu Recht. Die jüngsten Ereignisse haben jedoch die Art, wie wir arbeiten, grundlegend verändert. Homeoffice und Fernarbeit sind zu einem festen Bestandteil unseres Berufslebens geworden.

Gleichzeitig gehört Ransomware zu den Standardtools von Cyberkriminellen. Angriffe auf Unternehmen finden immer häufiger statt und sind in der Ausführung effektiv. Die Folgen können verheerend sein. Vor dem Hintergrund der zusätzlichen Angriffsflächen, die der Wechsel ins Homeoffice schafft, ist vermutlich jedes Unternehmen irgendwann davon betroffen.

Der Schutz von Endpoints vor Ransomware sollte daher eine strategische Priorität sein. Im Falle eines Falles könnte es ansonsten für Ihr Unternehmen zu spät sein.

Die in diesem Dokument beschriebenen sechs Faktoren sollen als Orientierungshilfe dienen, wie sich Unternehmen besser auf Ransomware-Angriffe vorbereiten können. Wenn Sie diese Faktoren berücksichtigen, wird sich der Sicherheitsstatus Ihrer Endpoints sofort verbessern:

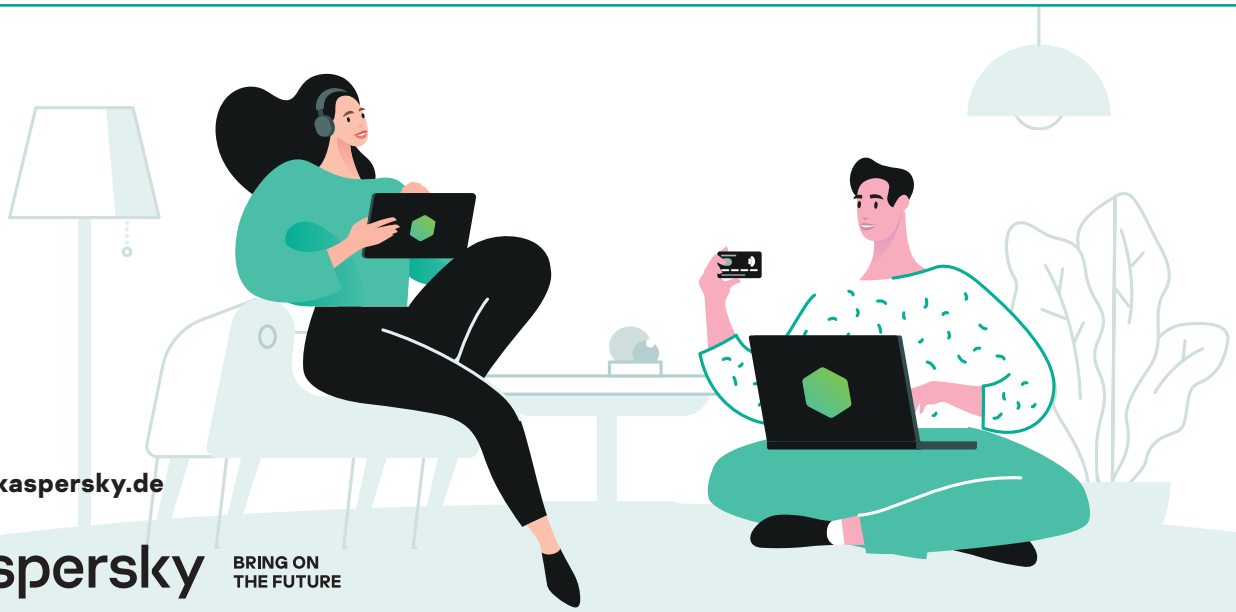
1. Erkennung und Beseitigung von Malware
2. Gerätekonfiguration
3. Datensicherungen und Wiederherstellung von Daten
4. Auslagerung
5. Schulung
6. DR-Planung

Wenn Sie mehr über den Schutz von Mitarbeitern im Homeoffice – und des Unternehmens als Ganzes – vor Ransomware erfahren möchten, steht Ihnen Kaspersky gern zur Seite. Mit unserer Cloud-nativen Lösung Kaspersky Optimum Security können Sie Ihren Schutz durch effektive Bedrohungserkennung und -abwehr sowie Sicherheitsüberwachung rund um die Uhr gegen neue, unbekannte und versteckte Bedrohungen ausbauen – und zwar ganz ohne hohe Kosten oder Komplexität. Mehr Schutz. Mehr Transparenz. Mehr Kontrolle.

Mehr Informationen finden Sie unter https://go.kaspersky.com/de_optimum

Weitere Informationen:

The story of the year: ransomware in the headlines
How to know what level of endpoint protection you need
EDR-Leitfaden
Erhöhte Cybersicherheit für Remote-Teams dank System Hardening



www.kaspersky.de

kaspersky BRING ON THE FUTURE

© 2022 AO Kaspersky Lab.
Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.