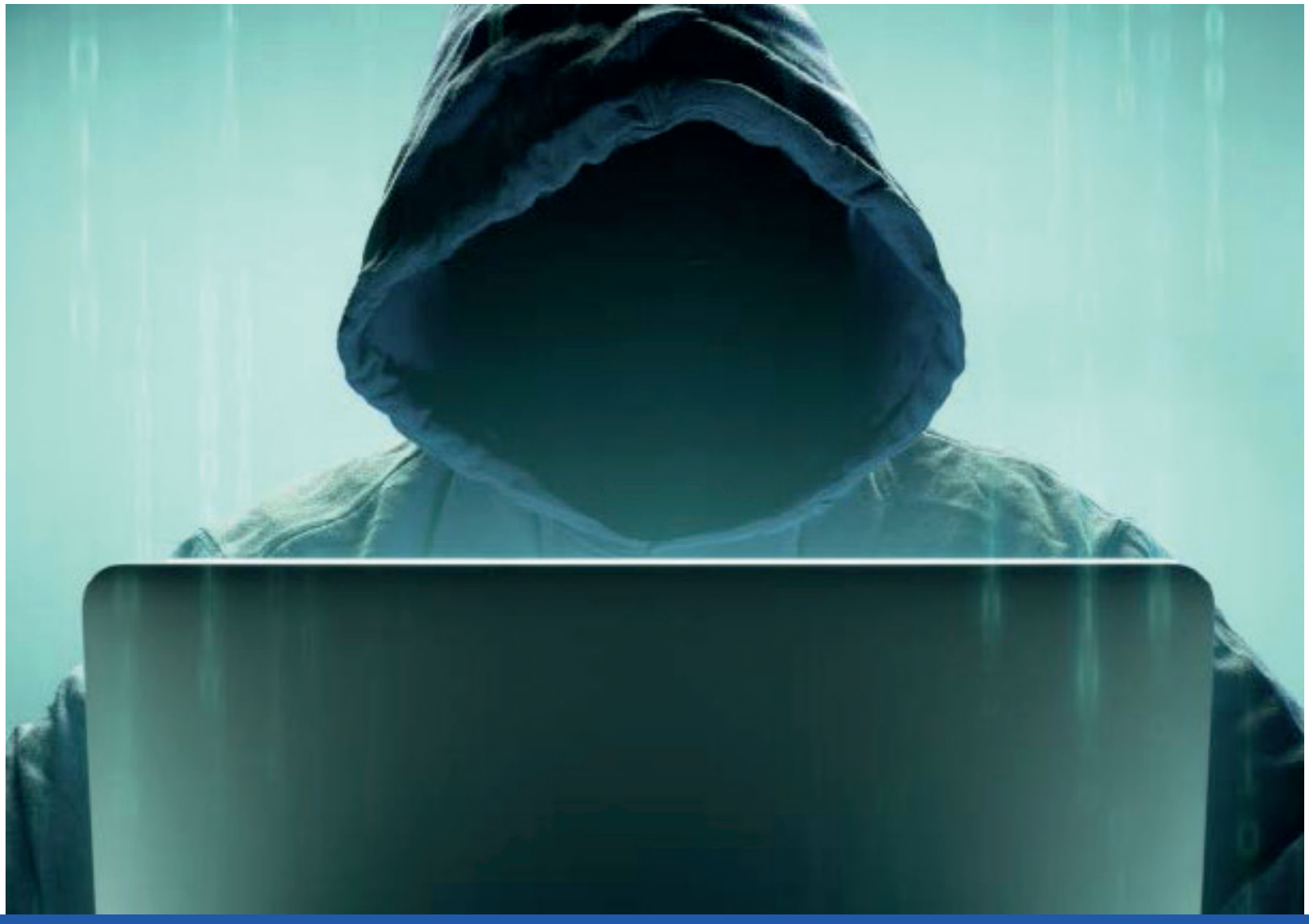


Ransomware-Angriffe vermeiden: die besten Tipps

Ontrack®

1. E-Mail-Sicherheit ist das A und O

Laut McAfee sind **Phishing-E-Mails** nach wie vor einer der Haupteintrittspunkte von Ransomware-Viren, insbesondere bei gezielten Angriffen.

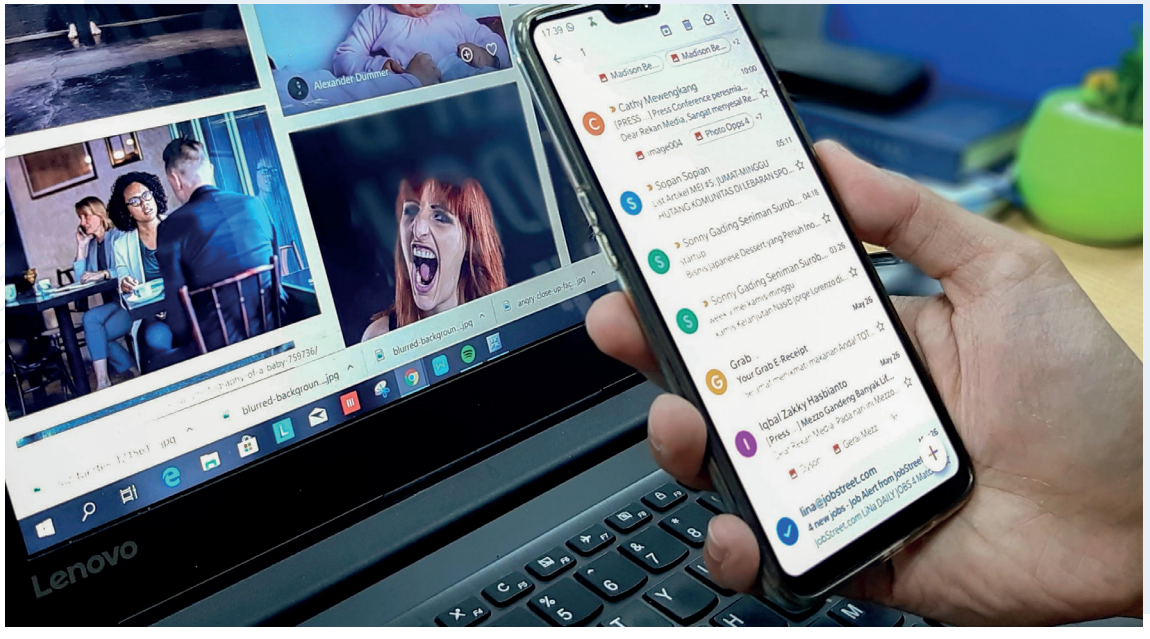
Daher ist es für alle, die ein Netzwerk betreiben oder eine Verbindung zum Internet herstellen, unerlässlich, diese primäre Schwachstelle zu schützen.

Meistens wird ein Ransomware-Angriff dadurch ausgelöst, indem der Benutzer eine – scheinbar – normale E-Mail öffnet, die den Virus in einem Dokument, Foto, Video oder einer anderen Art von Datei enthält.

Die meisten Hacker brauchen heutzutage gar nicht viel Kenntnisse, um Malware-Code in eine Datei einzufügen. Es gibt zahlreiche Artikel und YouTube-Tutorials mit Anleitungen dazu.

Öffnen Sie **niemals**, eine E-Mail von einem **unbekannten Absender**.

Wenn Sie eine E-Mail von einer unbekannten Quelle erhalten, informieren Sie Ihren IT-Experten, um die Infrastruktur Ihres Unternehmens nicht zu gefährden.



Ontrack®

2. Machen Sie Ihr Netzwerk und Ihre IT-Umgebung sicher.

Wenn Ransomware einen einzelnen Computer infiziert, ist dies zweifellos ein ernstes Problem. Wenn diese sich jedoch über das gesamte Netzwerk ausbreitet, kann sie sich nicht nur zu einem Albtraum für die IT-Abteilung entwickeln, sondern auch das gesamte Unternehmen gefährden.

Unternehmen sollten zwingend prüfen, ob eine Datensicherheitssoftware implementiert ist, die alle eingehenden E-Mails überprüft, bevor der beabsichtigte Empfänger sie erhält.

So wird das Risiko, dass sich ein Virus in einem Unternehmensnetzwerk ausbreitet, drastisch verringert.

Außerdem sollten Unternehmen Netzwerksicherheitssoftware installieren, die das Netzwerk automatisch auf Bedrohungen überwacht. Die Lösung warnt Administratoren auch, wenn bei einem Ransomware-Angriff versucht wird, große Mengen von Dateien über das Netzwerk zu verschlüsseln.

Last but not least: Aktualisieren Sie Ihre Software und Betriebssysteme immer mit den neuesten Patches, sobald diese verfügbar sind. Wie so oft schon erwähnt, sind Hacker mit ihren Angriffen nur dann erfolgreich, wenn das Opfer Lücken in seiner IT Security aufweist.

3. Schulung der Mitarbeiter

Ein Ransomware-Angriff ereignet sich meist völlig unvorhgesehen und unvorbereitet. Deshalb sollte jeder Mitarbeiter genau wissen, was bei einem Ransomware-Angriff zu tun ist. Dies gilt auch für Führungskräfte und IT-Verantwortliche.

Protokolle für den Umgang mit Ransomware-Angriffen sollten nicht nur Teil eines Business-Continuity-Plans für das Management und IT-Experten sein, sondern es sollten Leitlinien zur Vorgehensweise bei einem Angriff für jeden Mitarbeiter schnell verfügbar sein.

Diese Tipps können einfach, aber effektiv sein, zum Beispiel

- Trennen Sie die Verbindung von Computern zum Internet und zum internen Netzwerk.
- Fahren das infizierte Gerät ordnungsgemäß herunter und rufen Sie sofort die IT-Sicherheit an

IT-Experten sollten sich kontinuierlich über die neuesten Entwicklungen im Bereich Cybersicherheit und Hacking informieren. So sollte es ein absolutes Muss sein, an Schulungen teilzunehmen, die neuesten Blog-Nachrichten zu lesen oder sich über die neuesten Entwicklungen in diesem Bereich und Lücken in Netzwerk- oder Softwarelösungen zu informieren.

Ontrack®

4. Sichern Sie das Remote Desktop Protocol (RDP) Ihres Unternehmens

Bei den Remote Services wird üblicherweise das Remote-Desktop-Protokoll (RDP) verwendet. Während im Jahr 2018/19 die BlueKeep CVE 2019 0708 als kritische Schwachstelle bekannt wurde, können nun aktuelle Microsoft-Patches diese schließen. Heutzutage ist die Verwendung gestohlener und gekaufter RDP-Zugangsdaten und altmodisches Phishing eine Gefahr.

Wenn Ihre Organisation kein RDP verwenden muss, ist es am besten, wenn Sie es durch eine sicherere Lösung ersetzen. Ist dies nicht möglich, sollten folgende Maßnahmen ergriffen werden:

- Verwenden Sie ein VPN, um auf das RDP Ihrer Organisation zuzugreifen. Dieses stellt eine sichere Verbindung zwischen dem Unternehmen und dem Internet her. Der gesamte Datenverkehr wird über einen verschlüsselten virtuellen Tunnel gesendet, der verhindern soll, dass Cyberkriminelle nach der Brute-Force-Methode in ein System eindringen können.
- Stellen Sie sicher, dass Sie eine Zwei-Faktor-Authentifizierung eingerichtet haben.
- Die Mitarbeiter, die wichtige interne Services warten, sollten über die maximalen Zugriffsrechte verfügen, die sie benötigen. Jeder Mitarbeiter, der auf kritische Systeme oder Backups zugreift, sollte eine Zwei-Faktor-Authentifizierung eingerichtet haben.
- Haben Sie einen aktuellen Notfallplan, um sicherzustellen, dass Sie bei einer Kompromittierung Ihres RDP eine Sicherungskopie aller kritischen Daten haben.

Ontrack®

5. Stellen Sie sicher, dass Sie über ein aktuelles Backup verfügen

Ein hochsicheres Backup ist ein entscheidendes Element, um Ihr Unternehmen auf einen Ransomware-Angriff vorzubereiten. Ontrack empfiehlt:

Implementieren einer Sicherungs- und Wiederherstellungsplan für alle kritischen Daten mithilfe der **3-2-1-Strategie**

3: Aufbewahren von mindestens drei Kopien der Daten

2: Speichern der Daten auf zwei ver schiedenen Medientypen

1: Sichern einer Kopie Ihrer Backups außerhalb des Unternehmens

› Regelmäßiges Testen der Backups, um eine ordnungsgemäße Konfiguration sicherzustellen und so Auswirkungen einer Datenverletzung zu begrenzen

› Isolieren kritischer Sicherungen vom Netzwerk („Air Gap“) bzw. in einen Cloud Speicher

› Implementieren von Cppy-on-Write-Dateisystemen (NetApp WAFL – Linux ZFS) oder WORM-Features in NAS-Systemen oder Appliances

› Patchen von kritischen Betriebssystemen sowie Antiviren-, Sicherheits- und Backup-Software so schnell wie möglich

› Einrichten von kontinuierlichen Schulungen zu Cybersicherheit für Benutzer und Administratoren, um Phishing-E-Mails zu identifizieren

Ontrack®

Wie reagieren, wenn man von einer Ransomware-Attacke getroffen wird?

Wenn Ransomware aus irgendeinem Grund Ihre Verteidigungslinien durchdringt, sollten Sie Folgendes tun:

- **Niemals das Lösegeld bezahlen!**
  Die Kriminellen zu bezahlen, ist keine Garantie dafür, dass Sie Ihre Daten zurückerhalten. In vielen Fällen (und auf jeden Fall, wenn es sich um „Ranscam"- oder Wiper-Malware handelt) erhalten Sie Ihre Daten sowieso nicht zurück, sodass Sie nicht nur die Daten verlieren, sondern auch jede Menge Geld!

- Einige Computerspezialisten sind möglicherweise in der Lage, verlorene Daten wiederherzustellen. Dies ist jedoch riskant. Wenn etwas schiefgeht, könnten Ihre Daten für immer zerstört sein.

- **Überprüfen Sie Ihr Backup!**
  Selbst wenn Sie nach einem Ransomware-Angriff kein Backup mehr haben, sollten Sie die Möglichkeit einer Wiederherstellung niemals ausschließen. Mögliche Lösungen hängen von der Art des Mediums oder Speichersystems und dem Typ der Ransomware ab.

Ontrack®

24/7

0800 10 12 13 14
www.ontrack.com/de

0800 880 100
www.ontrack.ch

0800 644 150
www.ontrack.com/at