NEUE AUSGABE

KnowBe4
Human error. Conquered.

RANSOMWARE

Handbuch zur Datenrettung

Wie Sie sich vor Ransomware-Angriffen schützen und Ihre Daten wiederherstellen

Inhaltsverzeichnis

EINFÜHRUNG

Ransomware ist extrem schädlich. Angriffe mit Ransomware werden von Unternehmen und Cybersicherheitsexpert:innen gleichermaßen gefürchtet. Diese Sorge ist nicht unbegründet. Innerhalb von Sekunden kann die geschäftskritische IT-Infrastruktur einer Organisation für Wochen oder Monate in die Knie gezwungen werden, sodass alle Geschäftsprozesse zum Erliegen kommen. Manche Daten und Systeme sind möglicherweise für immer verloren. Bis zur vollständigen Wiederherstellung kann unter Umständen mehr als ein Jahr vergehen. Die Nachwirkungen für Kunden sind meist noch lange nach dem technischen Wiederherstellungsprozess spürbar.

Das FBI verfolgt über 100 verschiedene Ransomware-Banden (https://www.reuters.com/technology/fbi-says-it-is-investigating-about-100-types-ransomware-wsj-2021-06-04/). Die meisten davon operieren von Ländern aus, in denen sich Cyberkriminelle vor dem Zugriff durch die Strafverfolgungsbehörden aus dem Wohnsitzland des Opfers sicher fühlen können. Trotz großer Bemühungen von Sicherheitsexpert:innen ist Ransomware weiter auf dem Vormarsch (https://blog.knowbe4.com/ransomware-attacks-in-2021-have-increased-nearly-three-fold-in-the-first-half-of-the-year).

Der finanzielle Schaden, der durch Ransomware verursacht wird, ist erschreckend. Laut Cyberthreat Defense Report 2021 (https://info.knowbe4.com/research-2021-cyberthreat-defense-report) wurden in nur einem Jahr bis zu 68 % der befragten Organisationen durch Ransomware geschädigt. Der Ransomware-Sicherheitsanbieter Coveware berichtet, dass im dritten Quartal 2021 ein durchschnittliches Lösegeld (engl. „ransom“) von 139 739 US-Dollar gezahlt wurde (https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts). Manche Organisationen zahlten als Lösegeld sogar bis zu zweistellige Millionenbeträge.

Gewöhnlich liegen die Kosten für die Wiederherstellung um ein Vielfaches über den gezahlten Beträgen. Laut einem Cybersicherheitsanbieter wurden 2020 weltweit 18 Milliarden US-Dollar an Lösegeld gezahlt, während sich die Gesamtkosten auf mehrere 100 Milliarden US-Dollar beliefen (https://blog.emsisoft.com/en/38426/the-cost-ofransomware-in-2021-a-country-by-country-analysis/). Ein anderer Cybersicherheitsanalyst geht davon aus, dass die mit Ransomware verbundenen Kosten bis 2031 die Marke von 250 Milliarden US-Dollar übersteigen.

WAS IST RANSOMWARE?

Ransomware kann auf vielerlei Weise für Bedrohung und Schaden sorgen. Meist drohen Kriminelle damit, den Zugriff auf wichtige Daten und Systeme einzuschränken und/oder sensible Daten erst nach Zahlung eines Lösegelds wieder freizugeben. Zu den häufigsten Auswirkungen eines Ransomware-Angriffs zählen:

- Ausfallzeiten und Wiederherstellungskosten infolge einer Verschlüsselung von Daten und Systemen
- Diebstahl vertraulicher Daten von einer Organisation unter Androhung der Veröffentlichung
- Diebstahl von Anmeldedaten der Organisation, von Mitarbeitenden, Kund:innen
- Nutzung der kompromittierten Systeme des Opfers und Ausnutzung des guten Rufs des Opfers, um Kund:innen und Geschäftspartner:innen zu schädigen
- Öffentliche Rufschädigung des Opfers

Durch die Medien wurde der Begriff „doppelte Erpressung“ geprägt. Damit ist gemeint, dass Ransomware-Banden Daten nicht nur verschlüsseln, sondern auch mit der Veröffentlichung der Daten drohen. Der Schaden eines durchschnittlichen Ransomware-Angriffs ist für die betroffene Organisation oft sehr gravierend.

Inzwischen umfassen über 80 % aller Ransomware-Angriffe eine solche „doppelte Erpressung“ sowie den Diebstahl von Daten und Anmeldedaten.

Ransomware-Hacker:innen verwenden hauptsächlich die folgenden Methoden, um einen Computer zu infizieren: Phishing-E-Mails, ungepatchte Programme, Erraten von Passwörtern, Passwortdiebstahl, kompromittierte Anbieter, schädliche Onlinewerbung und kompromittierte Software-Downloads.

Wenn der Ransomware-Angriff erfolgreich ist und die Dateien verschlüsselt und/oder gestohlen wurden, wird ein Bildschirm oder eine Webseite mit Informationen zur Zahlung des Lösegelds angezeigt. Dieses muss gezahlt werden, um die Daten und Anmeldedaten wieder freizugeben bzw. deren Offenlegung zu verhindern. Hacker:innen setzen oft eine Frist von unter einer Woche, nach deren Ablauf sich der Zahlungsbetrag automatisch erhöht oder die Verschlüsselung permanent bestehen bleibt und die gestohlenen Daten veröffentlicht oder an andere Cyberkriminelle weitergegeben werden.

Bitcoin und Kryptowährung

Die Zahlung des Lösegelds erfolgt fast ausnahmslos in Form einer Kryptowährung wie z. B. Bitcoin (abgekürzt mit BTC). Bitcoin ist die derzeit bekannteste Kryptowährung und wird zur Zahlung von Ransomware-Lösegeld am häufigsten verlangt. Andere bekannte Kryptowährungen sind z. B. Ethereum, Litecoin, Ripple, Tether, XPR, Dogecoin oder Monero.

Manche Ransomware-Banden nutzen andere Zahlungsarten wie Geschenkgutscheine oder Geldüberweisungsdienste. Bitcoin und Kryptowährungen bleiben jedoch die mit Abstand häufigste Zahlungsmethode. Grund hierfür ist die beinahe garantierte Anonymität. Kryptowährungen können im Internet in die ganze Welt überwiesen werden. Die „Cyberwallets“, die für alle Überweisungen von Kryptowährungen benötigt werden, können zwar eingesehen werden. Wenn sich die beteiligten Parteien jedoch nicht freiwillig zu erkennen geben, bleiben Sender:in und Empfänger:in der Zahlung normalerweise unerkannt. Das macht Kryptowährungen zur idealen Zahlungsmethode für Ransomware-Banden.

TOR (Anonymisierungsnetzwerk)

Ransomware-Banden verlangen oft, dass die gesamte Kommunikation mit dem Opfer über TOR („The Onion Router“) erfolgt. TOR ist ein virtuelles Netzwerk mit einem zugehörigen Browser. Beides dient dazu, den Internetverkehr zu anonymisieren. Der spezielle Browser (TOR-Browser) nutzt ein weltweites Overlay-Netzwerk auf Basis von Onion-Routing. Der gesamte Verkehr wird am Ursprungspunkt verschlüsselt und dann über eine anonymisierte Gruppe von zufällig ausgewählten „TOR-Knoten“ gesendet, bis das gewünschte Ziel erreicht ist. Das TOR-Netzwerk wurde von Grund auf so konzipiert, dass der Ursprungs- und Endpunkt des Verkehrs anonym und verborgen bleibt.

Cyberkriminelle und andere Personen, die ihren Datenverkehr anonymisieren möchten, können über das TOR-Netzwerk kommunizieren oder dort Websites hosten. Eine Rückverfolgung durch Strafverfolgungsbehörden oder Regierungen ist kaum möglich. Dadurch ist TOR nicht nur zum Umgehen von Zensur, sondern auch für kriminelle Zwecke geeignet. Da TOR und Kryptowährungen auf Anonymität ausgelegt sind, ist es Ransomware-Banden möglich, sie für die Interaktion mit ihren Opfern zu nutzen, ohne eine Enttarnung fürchten zu müssen.

Ein paar Fakten zu TOR:

- Im Gegensatz zu .com- oder .net-Domains verwenden Onion-Webadressen die Endung „.onion“.
- TOR-Websites können nicht mit einem gewöhnlichen Internetbrowser aufgerufen werden.
- TOR wurde ursprünglich vom U.S. Naval Research Laboratory und der Defense Advanced Research Projects Agency (DARPA) entwickelt.
- Obwohl TOR-Netzwerk und -Browser die tatsächlichen Standorte und Aktivitäten der Nutzer:innen gut verbergen, können diese in manchen Fällen durch andere Methoden aufgedeckt werden, die oft nicht mit dem TOR-Netzwerk oder -Browser in Verbindung stehen.

Typische Ransomware

Ransomware stellt in der Regel nach dem Eindringen in das System einer Organisation eine Verbindung zu den Servern her, die weitere Befehle übermitteln. Dabei führt die Ransomware oft eigenständig eine Aktualisierung durch, um nicht von Anti-Malware-Software erkannt zu werden und um neue Funktionen und Anweisungen abzurufen. Die Ransomware-Bande wird über das neue Ziel benachrichtigt und kann den programmierten Ablauf der Ransomware starten, neue Anweisungen erteilen oder die Umgebung des Opfers nach Belieben durchsuchen.

Ransomware-Banden setzen oft zusätzliche Malware, Tools und Scripts ein, um sich in der Umgebung des Opfers umzuschauen. Dabei werden beispielsweise E-Mails ausspioniert, um zu ermitteln, bei welchen Daten sich eine Verschlüsselung bzw. ein Diebstahl besonders lohnt. Gewöhnlich wird die finanzielle Situation der Organisation unter die Lupe genommen, um die Höhe des Lösegelds festzulegen. Es soll zwar so viel wie möglich erbeutet werden, der Betrag darf jedoch nicht so abschreckend sein, dass das Opfer am Ende nicht bezahlt. Üblicherweise wird als Lösegeld 2 % des Jahresnettoumsatzes gefordert. Dann werden die Dateien mit der eingeschleusten Ransomware verschlüsselt und die Erpressung beginnt. Die Zeitspanne zwischen dem ursprünglichen Eindringen und der Erpressungsnachricht beträgt oft mehrere Wochen oder Monate.

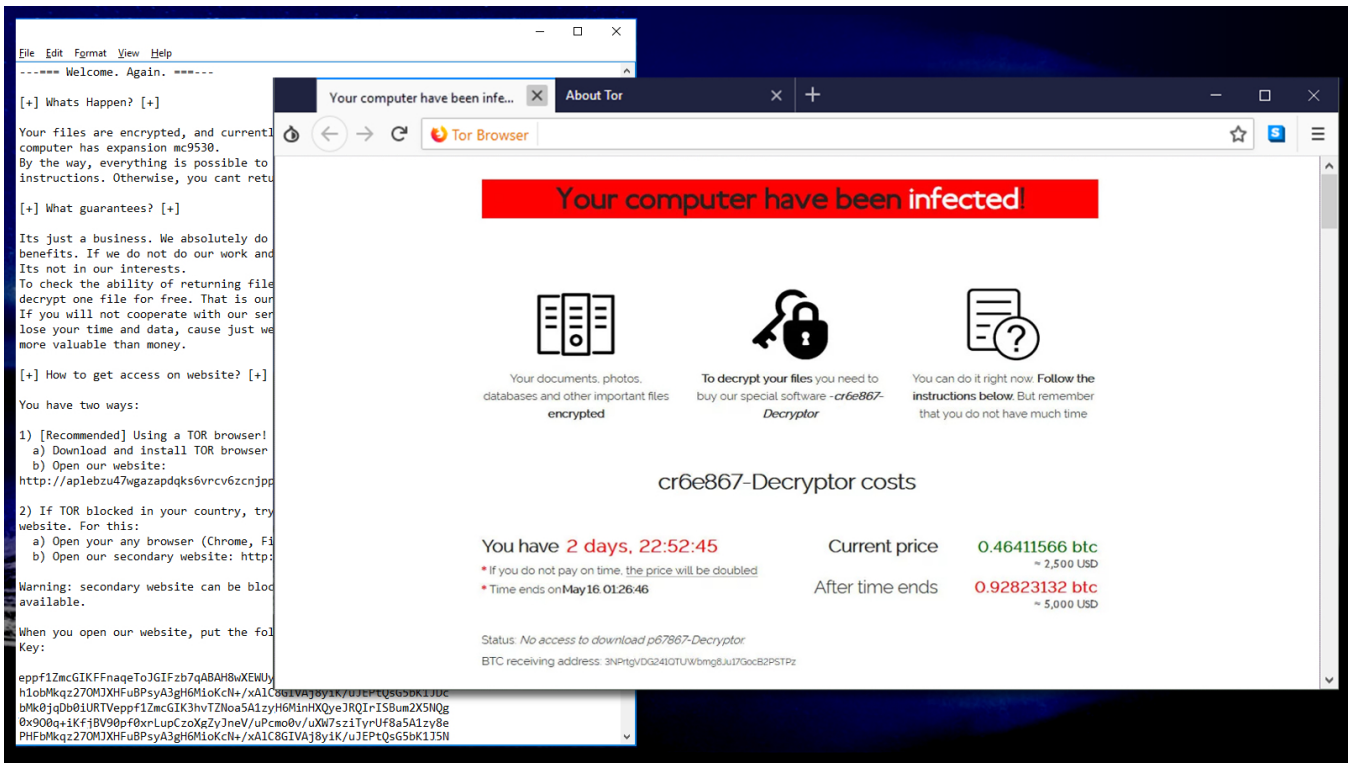
Wenn sich das Opfer entschließt, das Lösegeld zu zahlen, werden nach Zahlungseingang in der Regel eine Entschlüsselungssoftware und/oder Entschlüsselungsschlüssel bereitgestellt. Das Opfer kann dann beginnen, die verschlüsselten Daten wieder zu entschlüsseln. Dies ist oft sehr mühsam. Schließlich versprechen die Hacker:innen, die kopierten Daten und Anmeldedaten nicht zu veröffentlichen.

BIN ICH BETROFFEN?

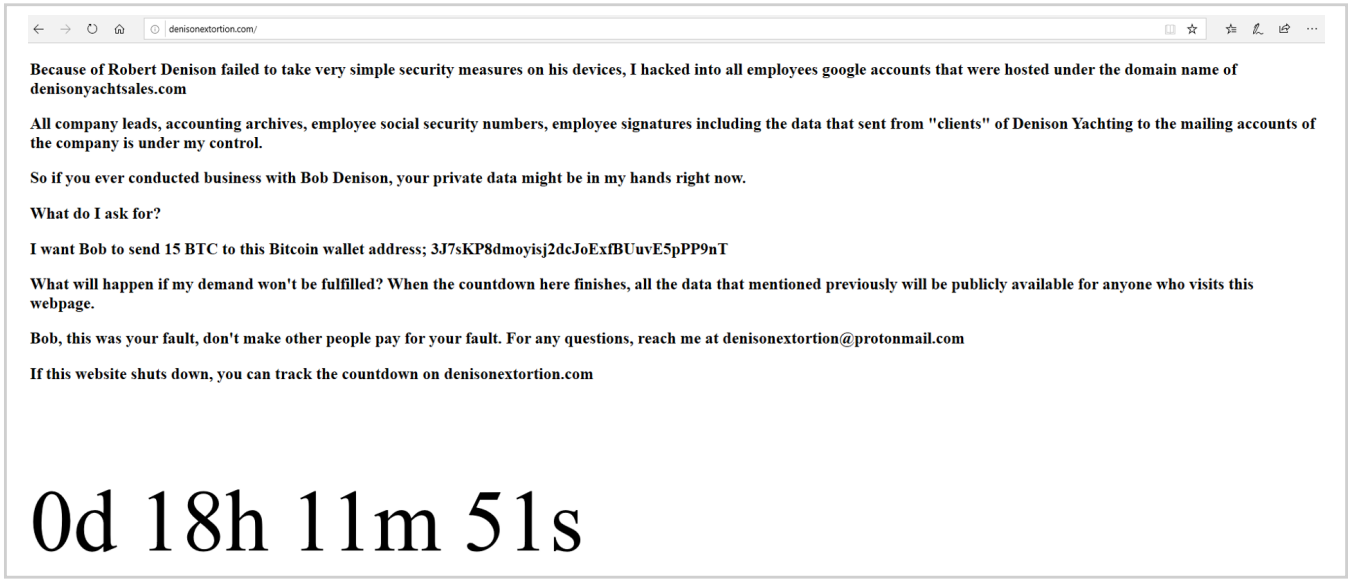
Normalerweise lässt sich recht einfach herausfinden, ob ein System von einem Ransomware-Programm bedroht wird. Folgende Anzeichen treten am häufigsten auf:

- Es kommt zu einem oder mehreren unerklärlichen „Abstürzen“ von ansonsten nicht betroffenen Systemen im selben Netzwerk.
- Eine Ransomware-Nachricht wird angezeigt.
- Dateien können plötzlich nicht mehr geöffnet werden. Stattdessen werden Fehlermeldungen wie „Datei beschädigt“ oder „falsche Dateierweiterung“ angezeigt.
- Sie erhalten über ein Ransomware-Programm oder eine entsprechende Website eine Warnung mit einem Countdown, nach dessen Ablauf das geforderte Lösegeld erhöht wird oder die Dateien nicht mehr entschlüsselt werden können.
- Eine Warnmeldung des Ransomware-Programms wird angezeigt, die sich nicht mehr schließen lässt.
- In allen Verzeichnissen werden Dateien mit Namen wie SO ENTSCHLÜSSELN SIE DATEIEN.TXT oder ANWEISUNGEN_ZUR_ENTSCHLÜSSELUNG.HTML angezeigt.

Beispiel eines Ransomware-Bildschirms der Ransomware Sodinokibi:



Beispiel einer Ransomware-Nachricht auf einer infizierten Kundenwebsite, in der die Veröffentlichung von Daten angedroht wird:



DIE GÄNGIGSTEN METHODEN FÜR EINEN RANSOMWARE-ANGRIFF

Cyberkriminelle setzen vor allem zwei Methoden für ihre schädlichen Angriffe auf Geräte und Organisationen ein:

- Social Engineering
- Ungepatchte Software

Dies ist auch bei Ransomware-Angriffen der Fall. Eine Zeit lang waren auch andere Malware- und Hacking-Methoden populär (z. B. Bootviren, Viren auf USB-Sticks usw.). Social Engineering und ungepatchte Software sind jedoch seit über drei Jahrzehnten eindeutiger Spitzenreiter und liegen meist auf Platz eins oder zwei der häufigsten Exploit-Methoden.

Dass schädliche Hacker- und Malware-Angriffe häufig aufgrund von Social Engineering und ungepatchter Software erfolgreich sind, wurde bereits in zahlreichen Artikeln und Whitepapers behandelt. Hier finden Sie einige Beispiele:

- https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense
- https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks
- https://blog.knowbe4.com/cyberheistnews-vol-11-14-heads-up-phishing-remains-the-most-common-form-of-attack
- https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

Sofern entsprechende Kenntnisse nicht bereits vorhanden sind, kann jede Organisation davon profitieren, sich mehr auf die Bekämpfung von Social Engineering und Phishing sowie auf das regelmäßige Patchen der Umgebung zu konzentrieren. Denn so kann das Gesamtrisiko, einem Cyberangriff zum Opfer zu fallen, am effizientesten verringert werden.

Im KnowBe4-Whitepaper *The Root Causes of Ransomware* (https://info.knowbe4.com/wp-root-causes-ransomware) wird darauf eingegangen, dass Social Engineering und ungepatchte Software für Ransomware-Banden die häufigsten Angriffsvektoren bleiben, um sich Zugriff auf die Geräte und Netzwerke ihrer Opfer zu verschaffen. Speziell bei Ransomware-Angriffen spielen jedoch noch weitere Angriffsvektoren eine Rolle. Diese sind in der Übersichtstabelle zu den Umfrageergebnissen weiterer Ransomware-Sicherheitsanbieter aufgeführt (siehe auch KnowBe4-Whitepaper *The Root Causes of Ransomware*):

Name des Reports	Social Engineering	RDP	Ungepatchte Software	Erraten von Passwörtern	Diebstahl von Anmel-dedaten	Remote-server-Angriff	Dritter	USB	Sons-tiges
Coveware Report	30 %	45 %	18 %	–	–	–	–	–	5 %
Statista	54 %	20 %	–	–	10 %	–	–	–	–
Artikel im Forbes Magazine	1.	3.	2.	–	–	–	–	–	–
Datto's Report	54 %	20 %	–	21 %	10 %	–	–	–	–
Hiscox Cyber Readiness	65 %	–	28 %	19 %	39 %	–	34 %	–	–
Sophos Report	45 %	9 %	–	–	–	21 %	9 %	7 %	9 %
Durchschnitt	50 %	24 %	23 %	20 %	20 %	21 %	22 %	7 %	7 %

Obwohl viele Angriffsvektoren von den verschiedenen Sicherheitsanbietern unterschiedlich kategorisiert werden, wird deutlich, dass Ransomware-Banden häufig noch einen dritten Angriffsvektor verwenden: Passwortangriffe. Dabei meldet sich die Ransomware-Bande entweder mit zuvor gestohlenen Anmeldedaten auf den Geräten des Opfers an oder errät die entsprechenden Anmeldedaten.

Nach der Anmeldung werden dann weitere Exploits gestartet und möglicherweise weitere Teile des Netzwerks kompromittiert. Die Mehrheit der Ransomware-Angriffe lässt sich damit auf drei Angriffsvektoren zurückführen:

- Social Engineering
- Ungepatchte Software
- Passwortangriffe

Im Folgenden werden einige zugehörige Angriffe beschrieben:

Social Engineering per E-Mail

Beim mit Abstand häufigsten Social-Engineering-Szenario geht eine unerwartete E-Mail mit einem harmlos erscheinenden Anhang ein (oder mit einer URL, hinter der sich eine schädliche Datei verbirgt). Häufig senden Hacker:innen Dateien mit mehreren Dateierweiterungen (z. B. datei.jpg.exe), um den eigentlich gesendeten Dateityp zu verbergen. Wenn Nutzer:innen eine E-Mail mit einem Anhang oder einem Software-Download-Link erhalten und den Anhang öffnen oder die Software herunterladen und installieren, ohne die Echtheit und die Absicht der Quelle zu überprüfen, kann dies direkt eine Ransomware-Infektion nach sich ziehen. Es handelt sich um die gängigste Methode, mit der Ransomware auf dem Computer eines Opfers installiert wird.

Versteckter Drive-by-Download

Ransomware-Angriffe können auch mithilfe „versteckter Drive-by-Downloads“ erfolgen. Dabei besuchen Nutzer:innen schädliche oder kompromittierte Websites, die Schwachstellen in ungepatchten Softwareprogrammen ausnutzen. Das Opfer bemerkt normalerweise nicht, dass ein Angriff erfolgt ist und der Computer kompromittiert wurde (daher der Begriff „versteckt“).

Ungepatchte Server oder Dienste

Häufig suchen Hacker:innen nach anfälligen, ungepatchten Softwareprogrammen auf dem Computer oder im Netzwerk des Opfers, die die Ausführung von schädlichem Code ermöglichen. Bei diesem und dem vorherigen Beispiel kann der Angriff durch die Nutzer:innen und die Organisation verhindert werden, indem anfällige Software offensiv identifiziert und gepatcht wird.

Kostenlose Software

Eine weitere gängige Methode zum Infizieren von Computern besteht darin, kostenlose Versionen von Software anzubieten. Bei kostenloser Software kann es sich z. B. um „gecrackte“ Versionen teurer Spiele oder Software, kostenlose Spiele, „Mods“ für Spiele, pornografische Inhalte, Bildschirmschoner oder betrügerische Software, die angeblich Cheats bei Onlinespielen oder die Umgehung der Bezahlschranke einer Website ermöglicht, handeln. Sobald Nutzer:innen darauf eingehen, können die Hacker:innen alle Firewall- oder E-Mail-Filter umgehen. Schließlich wurde die Datei von ihnen freiwillig heruntergeladen! Um ein Beispiel aus der Realität heranzuziehen: Bei einem Ransomware-Angriff wurde die Beliebtheit des Spiels Minecraft ausgenutzt und den Spieler:innen wurden kostenlose „Mods“ (begehrte Programmmodifikationen) angeboten. Bei der Installation dieser „Mods“ wurde auch eine Ransomware-Version installiert, die einige Wochen später aktiviert wurde.

Remotedesktopprotokoll (RDP)

Bei RDP-Sitzungen (Remotedesktopprotokoll) unter Microsoft Windows werden ebenfalls häufig Netzwerke infiziert. RDP-Sitzungen dienen dazu, sich remote bei einem Microsoft Windows-Computer anzumelden. Dadurch können Administrator:innen/Nutzer:innen den Computer so bedienen, als würden sie davor sitzen. Die Technologie kommuniziert in der Regel über den TCP-Port „3389“. Viele Organisationen lassen RDP-Datenverkehr aus dem Internet über ihre Firewall zu, damit autorisierte Personen remote auf Computer zugreifen können. Hacker:innen wissen genau, wie Sie diese ungeschützten Computer mit RDP angreifen können, um Malware in Netzwerke einzuschleusen.

Normalerweise funktioniert ein RDP-Exploit über Schwachstellen aufgrund fehlender Patches oder über das Erraten von Passwörtern, da die Opfer sehr schwache Passwörter gewählt und/oder keine Kontosperrung aktiviert haben. In anderen Fällen melden sich Angreifer:innen mit einem gestohlenen oder gekauften legitimen Passwort über RDP an. RDP-Exploits bleiben oft länger unbemerkt als andere Angriffsmethoden, da sich autorisierte Nutzer:innen und Administrator:innen ebenfalls über RDP anmelden und die meisten Angriffserkennungssysteme nicht zwischen einer legitimen Anmeldung und einer nicht legitimen Anmeldung unterscheiden können.

Sobald das Ransomware-Programm bzw. die Bande den Zugriff auf das erste Gerät im Netzwerk hergestellt hat, kann die Bande einfach auf weitere Geräte innerhalb der Organisation zugreifen, ohne entdeckt zu werden.

ICH BIN VON RANSOMWARE BETROFFEN. WAS SOLL ICH TUN?

Wenn Sie feststellen, dass Sie Opfer eines Ransomware-Angriffs sind, müssen Sie umgehend Maßnahmen einleiten. In der folgenden Grafik sind die einzelnen Schritte aufgeführt:

Die Schritte werden im Folgenden ausführlich beschrieben.

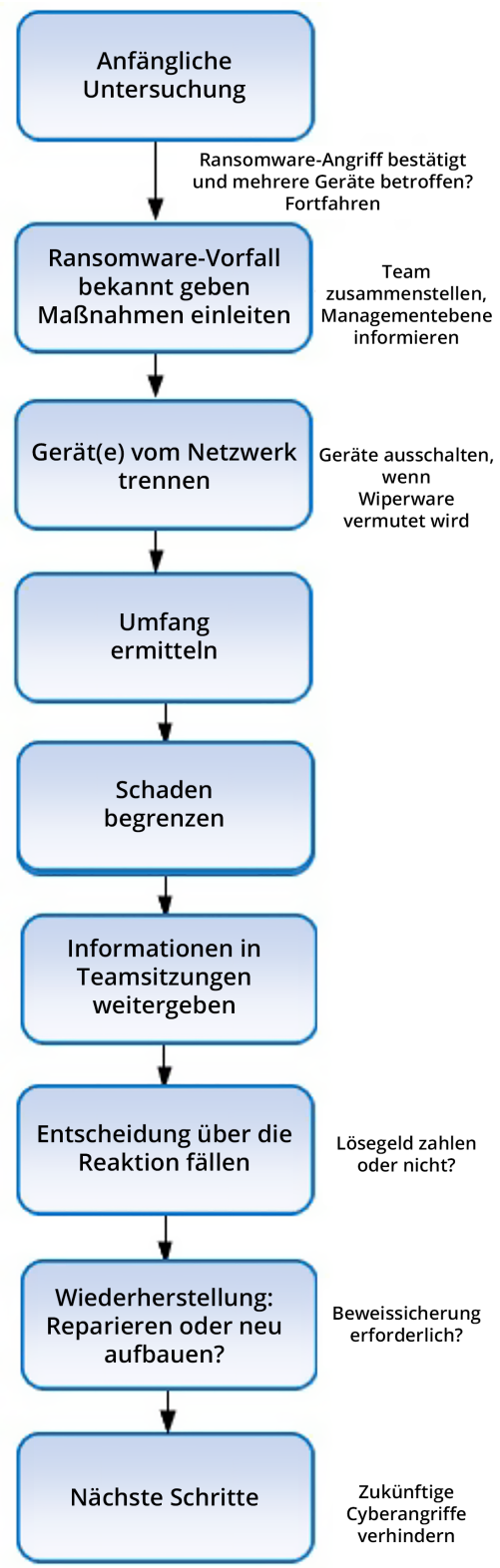
1 | Anfängliche Untersuchung

Alle potenziellen Ransomware-Angriffe beginnen mit der Meldung eines verdächtigen Computerereignisses durch eine oder mehrere Personen. Möglicherweise erhalten Sie sogar eine Ransomware-Nachricht oder verschlüsselte Dateien. Beides deutet mit hoher Wahrscheinlichkeit auf einen Ransomware-Angriff hin. Durch die anfängliche Untersuchung soll bestätigt werden, dass es sich wirklich um einen Ransomware-Angriff handelt. Beispielsweise sind nicht alle Ransomware-Nachrichten Angriffsversuche. Es kann sich auch um einen Hoax handeln, bei dem keine Dateien verschlüsselt werden. Möglicherweise wurden zufällig verschlüsselte Dateien von einem früheren Vorfall gefunden. Manchmal weist eine anfängliche Untersuchung mit hoher Wahrscheinlichkeit auf Ransomware hin, die Diagnose kann jedoch nicht zu 100 % bestätigt werden.

Ein bestehender Verdacht auf einen Ransomware-Angriff kann anhand von zwei wichtigen Punkten bestätigt oder verworfen werden. Ist bei dem gemeldeten verdächtigen Vorfall tatsächlich Ransomware im Spiel (es handelt sich also nicht um einen Hoax)? Sind mehrere Geräte betroffen? Wenn nur ein Gerät betroffen ist und bei keinem anderen Gerät ein Ransomware-Exploit vermutet wird oder bestätigt worden ist, ist es möglicherweise zu früh, „offiziell“ von einem Ransomware-Vorfall zu sprechen. Dann wäre eine umfassende Reaktion mit allen verfügbaren Ressourcen erforderlich.

Viele Organisationen entdecken ein Ransomware-Programm beim ersten Eindringen, noch bevor es sich verbreiten oder Dateien verschlüsseln kann. Es muss dennoch ermittelt werden, ob die Ransomware bereits mehrere Computer infiziert hat. Eine Ausbreitung muss möglichst unterbunden werden. Wenn ein Exploit „nur“ auf einem Computer sicher bestätigt wird, muss noch nicht das gesamte Incident-Response-Team involviert werden. Sofern diesbezüglich Zweifel bestehen, sollten Sie auch einen Einzelvorfall wie einen Angriff auf mehrere Computer behandeln und sich weiter an den Ransomware-Reaktionsplan halten.

Wird die Infektion eines weiteren Geräts bestätigt, müssen Sie davon ausgehen, dass sich die Ransomware auf alle mit dem Netzwerk verbundenen Geräte innerhalb der Organisation verbreitet hat. In diesem Fall müssen Sie eine umfassende Reaktion auf den Ransomware-Angriff einleiten.



2 | Ransomware-Vorfall bekannt geben

Geben Sie einen Ransomware-Vorfall offiziell bekannt, sobald mehrere Geräte von Ransomware betroffen sind. Das bedeutet, dass eine umfassende Reaktion auf den Vorfall mit allen verfügbaren Ressourcen erforderlich ist. Die Geschäftsleitung muss über alle bereits bekannten Details in Kenntnis gesetzt werden. Die Rechtsabteilung muss benachrichtigt und so schnell wie möglich aktiv eingebunden werden. Alle Mitglieder des Incident-Response-Teams müssen informiert werden und nach weiteren Anzeichen für einen Ransomware-Angriff und die Ausbreitung der Ransomware suchen. Die Teammitglieder dokumentieren, was überprüft wird und wonach gesucht wird. Die Ergebnisse werden ebenfalls festgehalten. Dabei wird davon ausgegangen, dass jedes Asset im Netzwerk befallen ist und sich unter der Kontrolle der Ransomware-Bande befindet. Die Assets werden überprüft und bei einer Infektion bereinigt oder wiederhergestellt. Alle vorhandenen Passwörter müssen als kompromittiert angesehen werden. Selbst wenn sich in einem Netzwerk nur ein kompromittiertes Gerät befindet, muss das gesamte Netzwerk bis zur Bereinigung und Wiederherstellung als nicht vertrauenswürdig angesehen werden.

Alle vorhandenen Passwörter müssen als kompromittiert angesehen werden.

Die gesamte Organisation sollte auf alternative, zuvor vereinbarte Kommunikationsmittel umsteigen, wobei die betroffenen Netzwerke und Assets ausgeschlossen sind. In der Regel bedeutet dies, dass die Kommunikation des Incident-Response-Teams bis auf Weiteres über Mobiltelefone und/oder externe Messaging-Anwendungen erfolgt. Über ein möglicherweise kompromittiertes Asset darf in keinem Fall kommuniziert werden. Incident-Response-Team, Geschäftsleitung und Rechtsabteilung müssen bis auf Weiteres das alternative Kommunikationsmittel verwenden. Die gesamte Kommunikation mit Dritten außerhalb der betroffenen Organisation muss über die Rechtsabteilung erfolgen, da diese Kommunikation ggf. einem besonderen rechtlichen Schutz unterliegt und im Falle von Gerichtsverfahren oder Untersuchungen gegenüber anderen Parteien nicht ohne Weiteres offengelegt wird. Gehen Sie davon aus, dass die Angreifer:innen jegliche vorherige Kommunikation über das kompromittierte Netzwerk und die verbundenen Assets kennen.

Legen Sie ein alternatives Kommunikationsmittel fest, das im Falle eines Ransomware-Angriffs für die Reaktion und Wiederherstellung verwendet wird.

3 | Gerät(e) vom Netzwerk trennen

Wurde auf einem Gerät ein Ransomware-Exploit bestätigt, trennen Sie dieses Gerät sofort vom Netzwerk (gemeint sind alle kabelgebundenen und drahtlosen Verbindungen). Wurden mehrere Geräte von Ransomware befallen, müssen Sie die Netzwerkfunktionen auf allen möglicherweise betroffenen Geräten deaktivieren. Dies umfasst die Internetverbindung sowie eingehende und ausgehende Netzwerkpunkte. Wägen Sie ab, ob Sie alle Geräte vom Netzwerk trennen, selbst wenn derzeit nur auf einem Gerät ein Exploit bestätigt wurde. So verringern Sie das Risiko einer weiteren Ausbreitung der Ransomware und Übernahme der Kontrolle durch die Ransomware-Bande.

Einige Organisationen sorgen – manuell oder mithilfe automatisierter Methoden – für eine Trennung vom Netzwerk, indem die Netzwerkfunktionen auf jedem möglicherweise befallenen Gerät deaktiviert werden. Meist ist es jedoch einfacher, die gemeinsam genutzte Netzwerkausrüstung (z. B. Router, Switches, VLANs, WLAN-Router usw.) zu deaktivieren. Die Netzwerkfunktionen können auf jedem Gerät einzeln deaktiviert werden. Dies nimmt in der Regel jedoch mehr Zeit in Anspruch – und wenn das Netzwerk wieder hochgefahren wird, muss der Netzwerkzugriff bei jedem Gerät auch wieder einzeln aktiviert werden. Trennen Sie jegliche Speichergeräte wie USB-Sticks oder externe Festplatten.

Wenn Sie die Netzwerkfunktionen auf einem mit dem Netzwerk verbundenen Gerät deaktivieren müssen, deaktivieren Sie die Netzwerkfunktionen, sofern möglich, auf einem gemeinsam genutzten Netzwerkgerät.

Schalten Sie Geräte nicht aus. Löschen Sie nichts und „bereinigen“ Sie (zu diesem Zeitpunkt) keine Dateien, etwa mit Antivirus-Software. Dies ist wichtig für spätere Schritte, da es andernfalls zu Problemen kommen kann, etwa bei der Wiederherstellung oder Beweissicherung.

Es gibt zwei wichtige Ausnahmen von dieser Regel. Wenn die Dateiverschlüsselung auf einem Computer gerade erst begonnen hat (d. h. die meisten Dateien wurden noch nicht verschlüsselt) oder wenn Sie das Vorhandensein von „Wiperware“ vermuten, können Sie die betroffenen Geräte sofort ausschalten (ohne diese „ordnungsgemäß herunterzufahren“). Bei Wiperware handelt es sich um Malware, mit der Datenträgerinformationen oder Dateien einfach gelöscht, beschädigt oder verschlüsselt werden können, ohne dass im Anschluss eine einfache Wiederherstellung möglich ist. Selbst dann, wenn ein Lösegeld verlangt und bezahlt wurde. Manchmal wird Malware als Ransomware ausgegeben, obwohl es sich tatsächlich um Wiperware handelt. Ein Beispiel mit besonders gravierenden Auswirkungen ist der Angriff auf Tausende ukrainische Unternehmen mit dem Wiperware-Programm Petya (https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine). Der Angriff verursachte einen Schaden von mehreren 100 Millionen bis Milliarden US-Dollar. Bei Petya wurde eine Nachricht ähnlich wie bei einem Ransomware-Angriff angezeigt und Geld gefordert.

Leider lässt sich zu Beginn eines Angriffs nur sehr schwer bestimmen, ob es sich um Ransomware oder Wiperware handelt. Insbesondere dann, wenn Wiperware als Ransomware ausgegeben wird. Glücklicherweise ist dies jedoch selten der Fall. Wenn also Malware festgestellt wird, die sich wie Ransomware verhält und als Ransomware ausgegeben wird, dann sollte ein Incident-Response-Team diese auch wie Ransomware behandeln. Behalten Sie das Risiko von Wiperware jedoch stets im Hinterkopf.

4 | Umfang ermitteln

Nun müssen Sie genau ermitteln, wie viel von Ihrer Infrastruktur kompromittiert wurde, was verschlüsselt/beschädigt wurde und ob Daten und/oder Anmeldedaten entwendet wurden. Bei der Untersuchung eines Exploits muss das ermittelnde Team alle ungewöhnlichen oder ungeklärten neuen Prozesse, Dienste oder Daemons ausfindig machen und melden. Wenn Sie den Umfang der Verschlüsselung bestimmen möchten, müssen Sie auch Folgendes in die Untersuchung einbeziehen:

- Freigegebene oder nicht freigegebene Laufwerke oder Ordner
- Netzwerkspeicher jeglicher Art
- Cloudspeicher (DropBox, Google Drive, Microsoft OneDrive, AWS usw.)
- Externe Festplatten
- USB-Sticks mit wertvollen Dateien

Erfassen Sie die oben genannten Ressourcen und suchen Sie nach Anzeichen für Verschlüsselung. Dies ist aus mehreren Gründen wichtig: Zunächst um den Umfang und die Ausbreitung des Ransomware-Programms zu ermitteln. Was wurde verschlüsselt? Darüber hinaus sind Sie bei Nutzung einer Cloudlösung wie DropBox, Microsoft OneDrive oder Google Drive möglicherweise in der Lage, aktuelle unverschlüsselte Versionen Ihrer Dateien einfach wiederherzustellen. Sofern ein Sicherungssystem eingerichtet ist, müssen Sie außerdem wissen, welche Dateien gesichert wurden, welche Dateien wiederhergestellt werden müssen und was nicht gesichert wurde. Wenn Sie schließlich dazu gedrängt werden, ein Lösegeld zu zahlen, müssen die Laufwerke wieder angeschlossen werden, damit die Ransomware mit der Entschlüsselung beginnen kann.

Sie können den Umfang auch ermitteln, indem Sie nach einem von der Ransomware erstellten Registrierungseintrag oder einer Dateiliste suchen, in dem bzw. in der alle verschlüsselten Dateien aufgeführt sind. Ransomware dokumentiert, welche Dateien von ihr verschlüsselt wurden. Nur so ist nach der Zahlung des Lösegelds klar, welche Dateien entschlüsselt werden müssen und welche Schlüssel benötigt werden. Oft handelt es sich bei diesen Listen um Registrierungseinträge oder Nachverfolgungsdateien. Da jede Ransomware-Version anders ist, sollten Sie im Internet nach Informationen über die Version suchen, von der Sie betroffen sind. Stimmen Sie Ihre Untersuchung dann auf die Ergebnisse Ihrer Recherche ab.

Es gibt auch Tools, mit denen Sie alle verschlüsselten Dateien in Ihrem System auflisten können.

- In unserer Ransomware-Wissensdatenbank finden Sie Links zu Entschlüsselungstools.

Ermitteln Sie, ob Daten oder Anmeldedaten kopiert wurden. Ist dies der Fall, ermitteln Sie den Umfang (soweit möglich). Oft finden Sie diese Angaben in der Ransomware-Nachricht selbst. Dort wird angegeben, welche Daten kopiert wurden oder welche Informationen über die gestohlenen Daten die Hacker:innen auf Websites oder Blogs veröffentlicht haben. Überprüfen Sie Ihre Protokolle und Tools zum Schutz vor Datenverlust (Data Leak Prevention, DLP) auf Informationen über gestohlene Daten. Suchen Sie nach großen, nicht autorisierten Archivdateien (z. B. ZIP, ARC usw.), die Ihre Daten enthalten und die als Zwischenspeicherung vor dem anschließenden Kopiervorgang angelegt wurden. Schauen Sie in allen Systemen nach. Möglicherweise finden Sie dort Hinweise, ob große Datenmengen aus dem Netzwerk heraus kopiert wurden. Suchen Sie nach Malware, Tools und Scripts, die möglicherweise zum Suchen und Abgreifen von Daten verwendet wurden. Ob Ihre Daten und Anmeldedaten gestohlen wurden, erfahren Sie am ehesten von der Ransomware-Bande selbst. Halten Sie also Ausschau nach entsprechenden Nachrichten. Wenn die Ransomware-Bande behauptet, sie sei im Besitz Ihrer Daten oder Anmeldedaten, dann zweifeln Sie nicht daran. Es kommt nicht oft vor, dass jemand blufft.

Anmerkung: Dennoch sollten Sie von einer Ransomware-Bande, die behauptet, Ihre Daten und/oder Anmeldedaten gestohlen zu haben, einen entsprechenden Beweis fordern. Meist wird ein entsprechender Beweis vorgelegt. Es ist möglich, dass die gestohlenen Dateien nicht besonders wichtig sind. Dies ist jedoch nur selten der Fall. Es ist für die zukünftige Wiederherstellung jedoch wichtig zu wissen, was gestohlen wurde und was nicht.

Sie sollten für jedes betroffene Gerät oder zumindest für einen Großteil der betroffenen Geräte (sofern sehr viele Geräte betroffen sind) eine umfassende forensische Analyse durchführen. Versuchen Sie, alle schädlichen Aktivitäten und Prozesse aufzudecken. Ransomware-Banden installieren neben dem eigentlichen Ransomware-Exploit meist noch viele weitere schädliche Programme und Scripts. Nur mit einer gewissenhaften und gründlichen forensischen Analyse erhalten Sie einen Überblick über das vollständige Ausmaß des Angriffs. Beauftragen Sie für diesen Teil der Untersuchung eine Person, die in forensischer Analyse geschult ist. Belassen Sie die betroffenen Geräte dabei möglichst unberührt. Erstellen Sie mithilfe von Tools für die forensische Analyse Kopien von Speichergeräten und dem Arbeitsspeicher betroffener Geräte und ermitteln Sie dann, welche Teile davon schädlich sind.

Art/Version der Ransomware ermitteln

Sie sollten genau wissen, mit welchem Ransomware-Programm Sie es zu tun haben. Jede Ransomware folgt einem grundlegenden Muster, wenn es darum geht, Daten und/oder Anmeldedaten zu verschlüsseln oder zu stehlen und dann ein Lösegeld innerhalb einer bestimmten Frist einzufordern. Wenn Sie die Version kennen, von der Sie betroffen sind, stehen Ihnen mehr Informationen zur Verfügung, auf die Sie Ihre Entscheidung stützen können.

Einige Ransomware-Versionen verlangen ein höheres Lösegeld als andere. Und manche Versionen bieten neben Bitcoin auch andere Zahlungsoptionen an. Wieder andere Ransomware-Versionen sind bekanntermaßen fehlerhaft, sodass nach der Zahlung des Lösegelds keine zuverlässige Entschlüsselung erfolgt. Manche Ransomware-Banden sind dafür bekannt, dass sie zu ihrem Wort stehen und kompetent sind. Informationen über das Ransomware-Programm und die jeweilige Version sind bei der Wiederherstellung hilfreich.

Es besteht eine kleine Chance, dass es für die Version, von der Sie betroffen sind, ein Entschlüsselungstool oder einen veröffentlichten Entschlüsselungsschlüssel gibt, mit dem Sie Ihre Dateien ohne Zahlung des Lösegelds zurückerhalten. Darauf sollten Sie sich jedoch nicht verlassen. Für den Fall, dass Sie zu den Ersten gehören, die von einer neuen Ransomware-Version betroffen sind, können die von Ihnen bereitgestellten Informationen dabei helfen, Ihre Umgebung wiederherzustellen und zukünftige Opfer der gleichen Ransomware-Version vor Schaden zu bewahren.

Es muss auch ermittelt werden, was in welchem Ausmaß betroffen ist. Welche Geräte sind in welchem Ausmaß von dem Exploit betroffen? Sind nur bestimmte Gerätetypen betroffen (z. B. nur Geräte unter Microsoft Windows)? Beschränkt sich der Ransomware-Angriff auf einen Standort oder sind mehrere Standorte betroffen? Welche Ressourcen sind nicht betroffen? Um den Umfang des Schadens zu ermitteln und eine geeignete Reaktion festzulegen, ist es meist genauso wichtig zu wissen, welche Ressourcen nicht betroffen sind. Können Sie ermitteln, ob Daten oder Anmeldedaten gestohlen wurden? Können Sie den Ursprung des Exploits bestimmen?

Sind die Datensicherungen weiterhin sicher und zuverlässig? Viele Opfer von Ransomware lehnen Verhandlungen mit der Ransomware-Bande zunächst ab, da sie fälschlicherweise davon ausgehen, durch ihre Datensicherungen „geschützt“ zu sein. In vielen Fällen können die nach Auffassung der Opfer sicheren und zuverlässigen Datensicherungen jedoch gelöscht oder beschädigt werden. Das Team muss sich darauf verlassen können, dass Vorgaben zuverlässig sind und nicht revidiert werden müssen. Vermeiden Sie eine solche Situation. Lassen Sie Ihre Datensicherungen testen und bestätigen Sie, dass alle relevanten Sicherungen sicher und zuverlässig sind, bevor Sie den Status der Datensicherungen dem Incident-Response-Team melden. Gehen Sie davon aus, dass Ihre Sicherungen beschädigt und unzuverlässig sind, bis das Gegenteil bewiesen ist. Für den Fall, dass Ihre Sicherungen sicher und zuverlässig sind – wie lange dauert schätzungsweise die zuverlässige Wiederherstellung aller betroffenen Geräte und Dienste anhand dieser Sicherungen? Viele Organisationen mussten feststellen, dass eine Wiederherstellung der betroffenen Daten und Dienste – sogar bei einer sicheren und zuverlässigen Datensicherung – Hunderte oder Tausende Jahre in Anspruch nehmen würde.

Da bei den meisten Ransomware-Angriffen Daten und Anmeldedaten entwendet werden, ist eine Datensicherung nicht ausreichend, um alle Risiken auszuräumen.

In dieser Phase sollten Sie so viele Informationen wie möglich in Erfahrung bringen.

5 | Schaden begrenzen

Wenn der Schaden auf irgendeine Weise begrenzt werden kann, sollten diesbezügliche Maßnahmen ergriffen werden (unter Einhaltung der Anforderungen für die Beweissicherung). Eine Möglichkeit besteht darin, das Netzwerk sowie alle direkt verbundenen Speichergeräte zu trennen. Eine weitere besteht darin, Geräte auszuschalten, auf denen Dateien gerade verschlüsselt werden. Viele Opfer schalten diese Geräte jedoch erst aus, wenn sicher ist, dass dadurch unverschlüsselte/unbeschädigte Daten gerettet werden können.

Kompromittierte Passwörter ändern

Der Schaden lässt sich auch begrenzen, indem alle eventuell kompromittierten Passwörter für alle Dienste, auf die die Angreifer:innen Zugriff haben, geändert werden. Viele Dienste werden über das Internet bereitgestellt und können nicht deaktiviert werden, wie z. B. öffentliche cloudbasierte Dienste. Opfer müssen davon ausgehen, dass alle Passwörter, die zwischen dem Ransomware-Exploit und dem aktuellen Zeitpunkt gespeichert und verwendet wurden, gestohlen wurden. Das betrifft Anmeldedaten für die betroffenen Geräte und das Netzwerk genauso wie Passwörter der Organisation, der Mitarbeitenden sowie der Kund:innen, sofern über die betroffene Umgebung ein Kundenportal zugänglich war. Stellen Sie eine Liste aller eventuell kompromittierten Passwörter zusammen, um diese dann im Rahmen einer gemeinsamen Aktion schnellstmöglich zu ändern. Normalerweise ist für das Zurücksetzen von Passwörtern eine vorherige Koordination und Planung notwendig. Bei einem Vorfall zählt jedoch jede Sekunde, um keine weiteren Schäden zu riskieren.

Die Passwörter der direkt betroffenen Geräte und Netzwerke, die Sie getrennt bzw. deaktiviert haben, müssen erst zurückgesetzt werden, wenn die Geräte und Dienste wiederhergestellt werden. Alle möglicherweise betroffenen Passwörter sollten geändert werden, bevor die Ransomware-Bande auf die betroffenen Dienste zugreifen kann (d. h. wenn der Netzwerkzugriff wiederhergestellt wird).

6 | Informationen in Teamsitzungen weitergeben

Jetzt ist der richtige Zeitpunkt, eine Teamsitzung über das zuvor festgelegte alternative Kommunikationsmittel oder in einem sicheren Konferenzraum abzuhalten. In dieser Sitzung können Sie Erkenntnisse über den Umfang des Ransomware-Vorfalls austauschen. Welche Ressourcen sind betroffen und welche sind nicht betroffen? Was wurde verschlüsselt? Wurden Daten und Anmeldedaten gestohlen? Wie konnte das Ransomware-Programm in die Umgebung eindringen?

ANMERKUNG: Einige Organisationen haben für diese Sitzungen schon Konferenzräume mit kompromittierten Video- oder Telefonsystemen genutzt, sodass die Angreifer:innen die Möglichkeit hatten, die Wiederherstellungspläne auszuspionieren.

Zu diesem Zeitpunkt werden oft externe Parteien hinzugezogen. Geschäftsleitung, Rechtsabteilung und Marketing-/PR-Abteilung (soweit vorhanden) sollten den Teilnehmenden mitteilen, welche Informationen außerhalb der Gruppe weitergegeben werden dürfen. Erinnern Sie alle Beteiligten daran, dass vertrauliche Informationen nicht weitergegeben werden dürfen und der festgelegte Vorfallreaktionsplan einzuhalten ist. Es ist nicht ungewöhnlich, dass sich Mitarbeitende ohne vorherige Genehmigung mit externen Parteien austauschen, da sie davon ausgehen, eine solche Kommunikation wird toleriert oder sogar gutgeheißen. Fragen Sie nach, ob sich jemand außerhalb der Gruppe über den Vorfall unterhalten hat. Das kommt häufig vor – auch dann, wenn diese Kommunikation untersagt wurde. Fragen Sie nach, was besprochen wurde und wer am Gespräch beteiligt war.

Mit diesem Schritt soll sichergestellt werden, dass alle bisherigen Erkenntnisse im Team ausgetauscht werden, alle auf dem gleichen Stand bezüglich Auswirkung und Umfang des Vorfalls sind und alle die nächsten Schritte vor Augen haben. Alle Teammitglieder sollten die Möglichkeit haben, ihre Einschätzung darzulegen und anderen zu widersprechen, wenn sie glauben, dass die vorgetragenen Informationen falsch oder unvollständig sind. Es ist auch in einem Incident-Response-Team normal, dass verschiedene Meinungen vorherrschen oder ein einzelnes Mitglied über mehr Informationen als das übrige Team verfügt.

Außerdem muss die Geschäftsleitung und/oder Rechtsabteilung zu diesem Zeitpunkt entscheiden, ob externe Parteien wie Branchenaufsichts- und Strafverfolgungsbehörden oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert werden. In den USA ist die Bundesbehörde CISA im Bereich Cybersicherheit tätig und koordiniert die Abwehr von Cyberangriffen und Wiederherstellung. Viele Länder verfügen über ähnliche Behörden für Cybersicherheit. Opfer von Ransomware-Angriffen in Deutschland sollten sich an die zuständige Behörde wenden, wenn sie Unterstützung benötigen. Opfer erhalten nützliche Informationen, Rat und einen zusätzlichen Rechtsschutz. Informieren Sie jetzt auch Ihre Versicherung, wenn Sie über eine Versicherungspolice für Vorfälle wie diesen verfügen. Die Entscheidung, ob externe Parteien eingebunden werden, wird von der Geschäftsleitung und der Rechtsabteilung getroffen. Letztere übernimmt dann die Kommunikation.

7 | Entscheidung über die Reaktion fällen

Sobald die ersten Informationen und der Umfang des Angriffs bekannt sind, müssen Sie sich entscheiden:

- Entweder Sie zahlen das Lösegeld.
- Oder Sie zahlen das Lösegeld nicht.

Die Entscheidung, ob das Lösegeld gezahlt wird, muss immer von der Geschäftsleitung und der Rechtsabteilung getroffen werden. Wenn sich Ihre Organisation entschließt, das Lösegeld nicht zu zahlen, können Sie direkt mit dem Versuch der Wiederherstellung beginnen.

Wenn Sie sich entschließen, das Lösegeld zu zahlen, besteht kein Grund für Scham oder Schuldgefühle. Ransomware-Banden machen es Ihnen so schwer wie möglich, ohne Lösegeldzahlung davonzukommen. Schätzungsweise 40 bis 60 % der Opfer von Ransomware zahlen das Lösegeld. Es ist für viele betroffene Organisationen die schnellste und kostengünstigste Möglichkeit, den normalen Geschäftsbetrieb wieder aufzunehmen bzw. zu verhindern, dass gestohlene Daten und Anmeldedaten offengelegt werden. Dabei stellen viele Opfer fest, dass ihre Datensicherungen nicht so sicher und wirksam sind wie gedacht. Wenn eine Versicherung in den Vorfall involviert und entscheidungsbefugt ist, wird in den meisten Fällen das Lösegeld gezahlt – mit der Absicht, die Ausfallzeiten und Gesamtkosten zu verringern.

Wenn Sie sich entschlossen haben, das Lösegeld zu zahlen, müssen Sie entscheiden, wer mit der Ransomware-Bande verhandelt (interne oder externe Person), wie viel die Organisation bereit ist zu zahlen (sofern nicht der gesamte geforderte Betrag gezahlt wird) und wie die Kryptowährung beschafft wird, die für die Zahlung wahrscheinlich erforderlich ist (mehr dazu weiter unten).

Wenn Sie (oder die Versicherung) sich entschließen, das Lösegeld zu zahlen, sollten Sie nicht den gesamten geforderten Betrag zahlen. Üblicherweise sind die von Ransomware-Banden gestellten Forderungen etwas übertrieben und können heruntergehandelt werden. Es ist nicht ungewöhnlich, dass der von Ransomware-Banden ursprünglich geforderte Betrag am Ende halbiert wird. Es ist jedoch auch nicht ungewöhnlich, dass Ransomware-Banden mehr Geld verlangen, wenn sie sich aus irgendeinem Grund respektlos behandelt fühlen.

In jedem Fall sollte das Lösegeld (ganz unabhängig vom ausgehandelten Betrag) erst dann gezahlt werden, wenn die Bande einen Beweis vorgelegt hat, dass die Daten mit ihrem Entschlüsselungsprogramm oder -schlüssel in einer für die Organisation nützlichen Weise wieder entschlüsselt werden können. Gelegentlich erfolgt entgegen der Behauptungen der Ransomware-Bande keine Entschlüsselung oder diese funktioniert nicht so wie angekündigt, da Ransomware-Programme meist nicht ausführlich getestet werden.

Kann es sein, dass die Zahlung von Lösegeld gesetzwidrig ist?

Ja. Wenn sich Opfer für die Zahlung des Lösegelds entscheiden, muss zuerst sichergestellt werden, dass dieses Vorgehen nicht gegen das Gesetz verstößt. Beispielsweise veröffentlichte das Office of Foreign Assets Control (OFAC) des Finanzministeriums der USA am 1. Oktober 2020 eine Mitteilung (https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf), dass Personen und Organisationen, die nach einem Ransomware-Angriff das geforderte Lösegeld zahlen, sowie deren Helfer:innen mit rechtlichen Konsequenzen rechnen müssen. An einige frühere sowie aktive Ransomware-Banden darf kein Geld gezahlt werden (zumindest nicht von Unternehmen, die an US-Gesetze gebunden sind).

Auf der SDN-Liste mit „Specially Designated Nationals and Blocked Persons“ des OFAC stehen unter anderem: Evgeniy Mikhailovich Bogachev, der Entwickler von Cryptolocker, einem frühen Ransomware-Programm; zwei Iraner wegen erheblicher Unterstützung einer schädlichen Cyberaktivität und der Nutzung von zwei Digitalwährungsadressen in Verbindung mit der Ransomware SamSam; die nordkoreanische Lazarus-Bande, Urheber der Ransomware WannaCry sowie die beiden Ransomware-Banden Bluenoroff und Andariel. Wer Lösegeld an Personen und Gruppen auf der OFAC-Liste zahlt, muss mit Bußgeld und Strafen rechnen, selbst wenn dem Opfer nicht bekannt war, dass sich die Ransomware-Bande auf der Liste befindet.

Holen Sie daher vor der Zahlung von Lösegeld immer Rechtsbeistand ein. Wenden Sie sich an einen Dienst, der das Geld nachverfolgen und Ihnen sagen kann, ob sich die Ransomware-Bande auf der OFAC-Liste befindet. Elliptic und Chainalysis sind Unternehmen, die Überweisungen mit Kryptowährungen nachverfolgen. Es gibt auch offizielle Stellen, die eine Aussage dazu treffen können, ob die Zahlung des Lösegelds legal ist. Es schadet nie, das BSI, das BKA oder Strafverfolgungsbehörden über einen Vorfall zu informieren. Überlassen Sie die endgültige Empfehlung Ihrem Rechtsbeistand.

8 | Wiederherstellung: Reparieren oder neu aufbauen?

Egal, ob Sie das Lösegeld zahlen oder nicht – Sie müssen entscheiden, ob die betroffenen Systeme und Daten REPARIERT oder NEU AUFGEBAUT werden sollen.

Nur REPARIEREN

Viele Opfer mit begrenzten finanziellen Mitteln und Ressourcen, die zudem unter Zeitdruck stehen, müssen die betroffenen Geräte und Dienste mit minimalem Einsatz so schnell wie möglich wieder zum Laufen bringen. Es wird alles daran gesetzt, die gesamte Malware sowie schädliche Modifizierungen zu entfernen, alle betroffenen Passwörter zu ändern, die kompromittierten Systeme wieder in einen funktionsfähigen Zustand zu versetzen (oft durch Entschlüsselung der verschlüsselten Dateien) und dann so schnell wie möglich wieder in den regulären Betrieb überzugehen. Dieses Vorgehen bei der Wiederherstellung ist in der Regel schnell und kostengünstig. Dabei besteht jedoch das Risiko, dass schädliche Dateien übersehen werden, sodass die Bande (oder zukünftige Angreifer:innen) erneut eindringen können.

Kompletter NEUAUFBAU

Die sicherste (und normalerweise teuerste) Option besteht darin, alle Geräte und Dienste im Netzwerk vollständig neu aufzubauen (und/oder auszutauschen), komplett neue Anmeldedaten einzurichten und sicherzustellen, dass alte Schwachstellen ausgeräumt werden. Häufig nutzen Opfer eines Ransomware-Angriffs die Ausfallzeit dazu, Infrastrukturen ohne die Schwachstellen oder Fehler der Vergangenheit komplett neu aufzubauen. Viele richten neue Softwareprogramme ein, aktualisieren vorhandene Programme und nutzen neue Computersicherheitsprogramme sowie Multi-Faktor-Authentifizierung. Es kann sein, dass sich diese neu aufgebauten Infrastrukturen vollkommen von der vorherigen Infrastruktur der Organisation unterscheiden.

Beweise sichern

Viele Opfer müssen aus rechtlichen Gründen alle möglichen Beweise für den Ransomware-Angriff sichern. Daher werden alle Maßnahmen, ob Reparatur oder Neuaufbau, auf neuen Geräten durchgeführt (zumindest am Anfang). Das Opfer kann auch eine vollständige Datensicherung der aktuell betroffenen Systeme durchführen, diese auf ähnlichen Geräten wiederherstellen und dann die Reparatur oder Wiederherstellung auf den neuen Geräten durchführen. (Die alten Geräte bleiben bis auf Weiteres unberührt.) Andere Opfer erstellen forensische Kopien (von Arbeitsspeicher und Speichermedien) und führen die Wiederherstellung anschließend auf den vorhandenen betroffenen Geräten aus. Die Geschäftsleitung und die Rechtsabteilung müssen entscheiden, ob eine Reparatur oder ein Neuaufbau der richtige Weg und ob eine Beweissicherung erforderlich ist.

Ganz egal, ob Sie sich für eine Reparatur oder einen Neuaufbau entscheiden – es ist äußerst aufwendig, Ihre Umgebung wiederherzustellen und ein sicheres Weiterarbeiten zu gewährleisten. Wenn nicht bereits geschehen, sollten Sie eine Business-Impact-Analyse (BIA) durchführen und entscheiden, welche Dienste in welcher Reihenfolge wiederhergestellt werden müssen, um die Wiederherstellung optimal zu gestalten und den Gesamtschaden zu verringern. Bei beiden Optionen binden Sie sehr wahrscheinlich externe Parteien in den Wiederherstellungsprozess ein.

Zugrundeliegende Infrastruktur neu aufbauen

Wenn feststeht, welche Anwendungen und Dienste vorrangig wiederhergestellt werden sollen, muss in den meisten Fällen zuerst die gesamte zugrundeliegende Infrastruktur (z. B. IP-Adressverwaltung, DHCP, DNS, Active Directory, Sicherheitsdienste und -tools) auf einen bekannten einwandfreien Zustand zurückgesetzt werden. Dies ist meist die Grundvoraussetzung für die Wiederherstellung von Anwendungen. Manche Anwendungen werden möglicherweise in externen Clouds oder anderen nicht betroffenen Infrastrukturen gehostet und können somit leicht wieder online gestellt werden. In anderen Fällen muss eventuell tage- oder wochenlang an der zugrundeliegenden Infrastruktur gearbeitet werden, bevor Anwendungen wieder zum Laufen gebracht werden können.

Selbstverständlich kann es auch sein, dass die betroffene Organisation mit der Reparatur einiger Systeme und Dienste beginnt und dann feststellt, dass eine Reparatur nicht mehr möglich und ein Neuaufbau erforderlich ist – oder umgekehrt. Denken Sie daran, dass eine Reparatur normalerweise schneller und billiger ist, jedoch eine höhere Wahrscheinlichkeit für einen weiteren Angriff besteht. Dies ist bei einem Neuaufbau genau umgekehrt. Versuchen Sie, die richtige Entscheidung für Ihre Organisation zu treffen.

Verschlüsselte Dateien sichern (optional)

Verschlüsselte Dateien sollten vor der Wiederherstellung gesichert werden. Wenn Sie das Lösegeld zahlen und die Ransomware-Bande Ihnen ein Programm oder Schlüssel für die Entschlüsselung sendet, nehmen Sie für den ersten Test zur Wiederherstellung nicht die verschlüsselten Dateien, sondern eine Kopie dieser Dateien. Häufig funktioniert die erste Wiederherstellung nicht und die Dateien werden bei diesem Versuch teilweise sogar so beschädigt, dass eine spätere Entschlüsselung nicht mehr möglich ist. Seriöse Teams für Ransomware-Wiederherstellung erstellen immer eine Kopie der betroffenen Dateien. Die Wiederherstellung wird dann an der Kopie der verschlüsselten Dateien vorgenommen.

Sichern Sie die verschlüsselten Dateien auch dann, wenn Sie sich entschließen, das Lösegeld nicht zu zahlen.

Dieses Vorgehen ist absolut richtig. Denn es kann sein, dass die entsprechenden Entschlüsselungsschlüssel zu einem späteren Zeitpunkt entdeckt oder veröffentlicht werden. Es haben sich bereits zahlreiche Ransomware-Entwickler:innen – ob aus schlechtem Gewissen oder aus Angst – dazu entschlossen, alle verschlüsselten Dateien ihrer Opfer wieder herzustellen. Die Chance ist zwar gering, ganz auszuschließen ist ein solcher Glücksfall jedoch keineswegs.

Verhandeln und/oder Lösegeld zahlen

Folgende Frage wird hinsichtlich der Lösegeldzahlung am häufigsten gestellt: „Werden diese Kriminellen meine Dateien tatsächlich entschlüsseln, wenn ich zahle?“ Die Antwort ist etwas komplexer. Im Grunde lautet die Antwort: „Ja“. Fast immer wird eine Möglichkeit zur Entschlüsselung der Dateien angeboten. Letztendlich befinden sich Hacker:innen in einem moralischen Dilemma. Sie möchten Geld von Ihnen und bieten daher technische Unterstützung, um die Zahlung zu erleichtern. Wenn bekannt wird, dass Hacker:innen nach der Lösegeldzahlung die Dateien NICHT zuverlässig entschlüsseln, verlieren sie an Glaubwürdigkeit. Zukünftige Opfer würden bei einer Internetrecherche schnell herausfinden, dass es zwecklos ist zu zahlen. Die einzige Möglichkeit, Opfer zur Zahlung zu bewegen, besteht also ironischerweise darin, Wort zu halten und die Dateien nach der Lösegeldzahlung zu entschlüsseln.

Andererseits haben Sie es nicht mit einem Fortune 500-Unternehmen zu tun, das seinen Ruf gegenüber Aktionär:innen verteidigen oder einen Quartalsbericht vorlegen muss. Wahrscheinlich handelt es sich um eine osteuropäische Ransomware-Bande, die nicht gleich nervös wird, wenn der Entschlüsselungsvorgang bei manchen ihrer Opfer nicht funktioniert. Nach der Zahlung des Lösegelds ist es durchaus möglich, dass die kriminellen Entwickler:innen der Ransomware, von der Sie betroffen sind, nicht mehr reagieren. Ein gewisses Risiko bleibt immer bestehen. Die Systeme sind von Grund auf robust und redundant konzipiert, da die Banden Gegenwehr einplanen und ihr „Geschäft" fortführen möchten.

Wenn alle bisherigen Punkte geklärt sind, sollten Sie sich mit den Details zur eigentlichen Lösegeldzahlung befassen. In diesem Dokument wird davon ausgegangen, dass das Lösegeld in Form von Bitcoin zu zahlen ist. Sie finden weiter unten eine schrittweise Anleitung, wie Sie Bitcoin beschaffen und die entsprechenden Zahlungen vornehmen. Diese Informationen sind vor allem dann relevant, wenn Sie bisher noch nichts mit Bitcoin zu tun hatten.

Anweisungen zur Zahlungsmethode finden

Bei den meisten Ransomware-Programmen werden die Informationen zur Zahlungsmethode auffällig dargestellt bzw. sehr deutliche Anweisungen erteilt. Üblicherweise wird direkt auf dem Ransomware-Bildschirm ein Link zu den Anweisungen eingeblendet. Möglicherweise finden Sie die entsprechenden Anweisungen auch in einer Datei, die ANWEISUNGEN_ZUR_ENTSCHLÜSSELUNG.TXT oder ähnlich benannt ist. Unabhängig von der Ransomware-Version, von der Sie betroffen sind, enthalten die Anweisungen drei Informationen:

- wie viel Geld gezahlt werden soll
- wohin das Geld überwiesen werden soll
- wie viel Zeit für die Zahlung noch verbleibt (Countdown)

Sobald diese Informationen vorliegen, müssen Sie herausfinden, wie Sie das Lösegeld zahlen.

Bitcoin beschaffen

Zuerst müssen Sie ein Konto bei einer Kryptobörse einrichten, an der Bitcoin gehandelt wird und an der Sie Bitcoin kaufen können. Normalerweise stellt das kein Problem dar. Ihnen bleibt jedoch möglicherweise wenig Zeit zur Zahlung des Lösegelds, sodass die Dinge etwas schwieriger sind. Sie müssen also eine Börse finden, bei der Sie schnell an Bitcoin kommen. Um sich auf einen solchen Vorfall vorzubereiten, können Sie auch jetzt schon ein entsprechendes Konto einrichten.

- In unserer Ransomware-Wissensdatenbank finden Sie weitere Informationen darüber, wie Sie Bitcoin beschaffen.

ANMERKUNG: Wenn es sich bei der geforderten Kryptowährung nicht um Bitcoin handelt, können Sie das Wort Bitcoin durch jede andere Kryptowährung ersetzen.

Die Auswahl der Börse ist mitunter schwierig. Einige setzen ein Konto bei einer Bank voraus, während es sich bei anderen Börsen um Broker-Websites handelt, auf denen Personen Bitcoin kaufen und verkaufen. In manchen Fällen findet die Abwicklung sogar persönlich statt. In jedem Fall muss ein Konto erstellt werden. KnowBe4 verfügt über ein Konto bei http://www.CoinBase.com.

Sobald Sie ein Konto erstellt haben, haben Sie wahrscheinlich auch eine Cyberwallet-Adresse. Diese Adresse benötigt die Person, von der Sie Bitcoin kaufen. Bitcoin kann mit verschiedenen Zahlungsarten gekauft werden. Einige Kryptobörsen verlangen die Verknüpfung eines Bankkontos. Bei solchen Börsen dauern die Transaktionen jedoch in der Regel länger (bis zu vier Tage bei neuen Konten). Möglicherweise steht Ihnen jedoch nicht so viel Zeit zur Verfügung. Auf Broker-Websites für Bitcoin wie http://www.LocalBitcoins.com können Sie lokale Verkäufer:innen kontaktieren und nach Zahlungsarten filtern. Auf diese Weise erhalten Sie wahrscheinlich am schnellsten Bitcoin.

Kaufen Sie am besten einen etwas höheren Bitcoin-Betrag als den geforderten Betrag, um Kursschwankungen und/oder Transaktionsgebühren einzukalkulieren.

TOR-Browser installieren (ggf. optional)

Wenn Sie mit dem TOR-Browser nicht vertraut sind, finden Sie zu Beginn dieses Dokuments einen Abschnitt mit Informationen zu TOR und dessen Funktionsweise. Die Navigation funktioniert fast genauso wie Sie es bei einem gängigen Browser gewohnt sind. Der TOR-Browser kann über die Adresse http://www.torproject.org heruntergeladen werden. Laden Sie den TOR-Browser von keiner anderen Website herunter.

Installieren Sie den Browser und öffnen Sie ihn. Er sieht ähnlich wie andere Browser aus, die Sie kennen. Mit dem TOR-Browser können Sie im TOR-Netzwerk gehostete Websites aufrufen. Ransomware-Banden hosten ihre Websites oft temporär im TOR-Netzwerk, sodass Sie gezwungen sind, die Website mit den Zahlungsanweisungen über den TOR-Browser aufzurufen. Die Hacker:innen können die Website sofort abschalten, sobald sie ihren Zweck erfüllt hat, und so eine öffentliche Nachverfolgung (wie beim normalen Hosting im World Wide Web möglich) verhindern.

Die „Adresse" der Website, die Sie von der Ransomware-Bande erhalten, kann ein sehr seltsames Format haben und befindet sich normalerweise in den Entschlüsselungsanweisungen oder auf dem Hauptbildschirm.

Beispiele für Adressen von TOR-Websites:
kprrj4jalkparf4p.onion/rqla 7yulv7filqlrycpqrkrl.onion

Lösegeld zahlen

Sobald sich genügend Bitcoin in Ihrer Bitcoin-Wallet befinden und Sie den Nachweis haben, dass die Entschlüsselung funktioniert, können Sie die geforderten Bitcoin an die Wallet der Ransomware-Bande senden. Normalerweise benötigen Sie Folgendes, um das Lösegeld zu zahlen:

- eine Webadresse zum Anzeigen der speziellen Ransomware-Zahlungsanweisungen (Dies kann eine TOR-Adresse sein.)
- die Bitcoin-Wallet-ID des Hackers bzw. der Hackerin, um den geforderten BTC-Betrag zu überweisen
- je nach Ransomware-Version die Transaktions-ID oder den „Hash", der beim Senden der BTC an die Wallet des Hackers bzw. der Hackerin generiert wurde

Bei vielen Ransomware-Versionen müssen Sie eine Website im TOR-Netzwerk aufrufen, die allein für die Zahlung Ihres Lösegelds erstellt wurde. Geben Sie die Webadresse in den TOR-Browser ein. Befolgen Sie einfach die Anweisungen auf der Website, um die Wallet-ID zur Überweisung des Bitcoin-Betrags zu erhalten. Bei der Wallet-ID handelt es sich üblicherweise um eine lange Zeichenfolge aus Ziffern und Buchstaben, die in den Ransomware-Zahlungsanweisungen oder auf dem Bildschirm mit den Zahlungsinformationen zu finden ist.

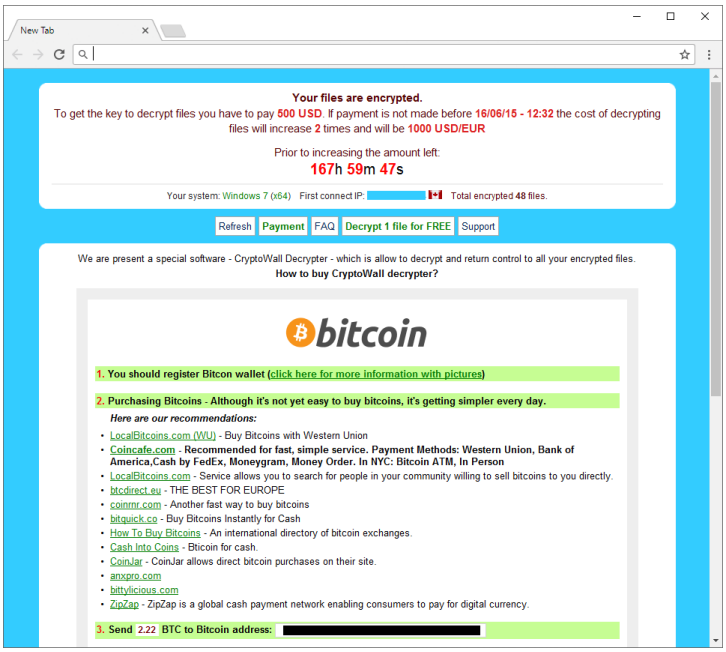
Beispiel einer Bitcoin-Wallet-Zeichenfolge:
19eXu88pqN30ejLxfei4S1alqbr23pP4bd

Anmerkung: Rufen Sie Ransomware-Websites nur auf, wenn es absolut notwendig ist. Oft wird der Countdown erst beim ersten Aufruf aktiviert. Opfer haben eventuell mehr Zeit zum Reagieren auf den Ransomware-Vorfall, wenn sie die Auslösung des Countdowns verhindern.

Nachdem Sie sich bei Ihrem Konto an der Kryptobörse angemeldet und die Bitcoin an die Wallet des Hackers bzw. der Hackerin überwiesen haben (Dauer: etwa 20 bis 40 Minuten), erhalten Sie normalerweise einen Hash, der die Transaktion bestätigt. Dabei handelt es sich wieder um eine lange Zeichenfolge aus Ziffern und Buchstaben.

Meist reicht es aus, den Bitcoin-Betrag zu senden, damit Sie von den Hacker:innen den Entschlüsselungsschlüssel für Ihre Dateien erhalten. Je nach Ransomware-Version müssen Sie zusätzlich noch die Hash-ID der Transaktion an die Hacker:innen senden. Üblicherweise befindet sich auf dem Ransomware-Bildschirm ein Feld, in dem Sie die Hash-ID der Transaktion eingeben bzw. einfügen können.

Beispiel des Zahlungsbildschirms der Ransomware CryptoWall:



Ihre Dateien entschlüsseln

Nach der Zahlung des Bitcoin-Betrags an die Hacker:innen müssen Sie möglicherweise mehrere Stunden warten, bis die Transaktion verarbeitet wurde. Ist dies geschehen, sollten Sie von den Hacker:innen die spezielle ausführbare Datei mit den Schlüsseln erhalten, mit denen Sie Ihre Dateien entschlüsseln können.

WICHTIG: Stellen Sie vorab sicher, dass alle externen Laufwerke, USB- oder auch Netzwerkspeichergeräte, die zum Zeitpunkt des Angriffs angeschlossen waren, auch aktuell angeschlossen und aktiviert sind. Wenn die Ransomware nicht in der Lage ist, die verschlüsselten Dateien zu finden, können diese auch nicht entschlüsselt werden. Stellen Sie außerdem sicher, dass alle freigegebenen Ordner den gleichen Pfad wie zum Zeitpunkt des Angriffs aufweisen. Dies gilt ebenso für externe Festplatten oder USB-Sticks.

Die meisten Ransomware-Opfer haben Probleme, alle Dateien wiederherzustellen bzw. in ihren ursprünglichen Zustand zurückzuversetzen, selbst wenn sie das Lösegeld zahlen und den Entschlüsselungsschlüssel oder das -programm erhalten. Selbst wenn die Dateien vollständig entschlüsselt werden, können sie oft nicht in ihrer ursprünglichen Form verwendet werden, da die anderen Dateien zu einem anderen Zeitpunkt verschlüsselt wurden und somit nicht synchronisiert sind. Eine Wiederherstellung ist mit Erfolgen und Misserfolgen verbunden. Es ist jedoch die Ausnahme, dass eine betroffene Organisation alle Dateien wiederherstellen kann und das System ohne viel Aufwand wie vor dem Ransomware-Angriff funktioniert. Dennoch haben Opfer, die ihre Dateien entschlüsseln können, immer noch weniger Aufwand als Opfer, die keine Datensicherung haben und das Lösegeld nicht zahlen. Betroffene Organisationen mit umfangreichen Datensicherungen erzielen die besten Ergebnisse bei der Wiederherstellung der Dateien (sofern diese zeitnah erfolgt).

9 Nächste Schritte: Zukünftige cyberkriminelle Vorfälle verhindern

Unabhängig davon, ob Sie von Ransomware betroffen waren oder nicht, ist der Schutz des Netzwerks vor dieser Art von Angriffen inzwischen integraler Bestandteil jedes Frameworks für Netzwerksicherheit für Einzelpersonen wie für Unternehmen. Dieser Schutz ist unverzichtbar. Und wenn Sie bereits betroffen waren, versuchen Sie, aus Ihren Fehlern zu lernen. Es ist an der Zeit, Gegenmaßnahmen zu treffen und proaktive Schritte zu unternehmen, um solche und ähnliche Vorfälle zukünftig zu verhindern.

Sie sollten mindestens Folgendes tun:

- Organisieren Sie ein wirksames Security Awareness Training in Verbindung mit simulierten Phishing-Angriffen, um die Phish-prone™ Percentage unter Ihren Mitarbeitenden deutlich zu verringern. Es ist wichtig, eine Bedrohung als solche erkennen zu können, bevor sie zu Ausfallzeiten führt.
- Installieren und warten Sie hochwertige Antivirus- oder EDR-Software (Endpoint Detection and Response) als zusätzliche Verteidigungslinie. Verlassen Sie sich jedoch nicht blind darauf. Die Software hinkt den Malware-Entwicklungen meist hinterher.
- Wenden Sie alle wichtigen Patches innerhalb von zwei Wochen nach Veröffentlichung durch den Anbieter an.
- Nutzen Sie überall, wo es möglich ist, eine starke Multi-Faktor-Authentifizierung (MFA) sowie starke, eindeutige Passwörter, die nicht für mehrere Websites oder Dienste gleichzeitig eingesetzt werden.
- Konfigurieren Sie hochwertige Sicherungs-/Wiederherstellungssoftware und testen Sie die Wiederherstellungsfunktion regelmäßig.

Defense-in-Depth-Strategie

Zum Schutz vor Eindringlingen und Angriffen müssen die wichtigsten Verteidigungslinien gesichert werden.

Wenn Sie sich ein Computernetzwerk als eine Reihe von Linien vorstellen, die von Malware oder Viren überschritten werden müssen, besteht die äußerste Linie aus den Nutzer:innen. Um in ein Netzwerk einzudringen, ist in der Regel nur die Interaktion einer Nutzerin oder eines Nutzers erforderlich. Erst NACHDEM eine Nutzerin oder ein Nutzer auf einen schädlichen Link geklickt oder eine schädliche Website besucht hat, kommen die sekundären und tertiären Verteidigungsmaßnahmen zum Einsatz (Firewalls und Antivirus-Software).

Security Awareness Training

Mitarbeitende kommen nicht mit der Absicht zur Arbeit, auf Links in Phishing-E-Mails zu klicken und ihre Computer zu infizieren. Jedoch benötigen Mitarbeitende ein grundlegendes Sicherheitsbewusstsein, um Warnsignale zu erkennen und schädliche Links/Software von rechtmäßigem Datenverkehr unterscheiden zu können. Dies werden Ihnen viele IT-Expert:innen bestätigen können. Die Bedrohungslage nimmt weiter zu und es werden stets neue Malware und Tricks eingesetzt, um Mitarbeitende zu täuschen. Diese müssen sich nicht nur bezüglich IT- und E-Mail-Sicherheit kontinuierlich weiterbilden, sondern auch in Bezug auf neue Angriffsmethoden und -vektoren. Inzwischen wissen wahrscheinlich alle, dass es keinen nigerianischen Prinzen gibt, der sein Geld loswerden will, sondern es sich dabei um eine Betrugsmasche handelt.

Was ist aber, wenn „Birthe Loose“ von der „Steuerberatungskanzlei“ Ihnen versehentlich eine Gehaltstabelle sendet? Nicht alle hinterfragen die zweifelhafte Quelle einer gut gemachten Phishing-E-Mail, besonders wenn diese einen interessanten Anhang wie „Gehaltsabrechnung_für_Q4.zip“ enthält. Die Personalabteilung empfängt möglicherweise 20 Lebensläufe am Tag. Nur einer davon muss mit böswilliger Absicht gesendet worden sein, um einen Sicherheitsvorfall zu verursachen.

Hacker:innen versuchen immer häufiger, Mitarbeitende mithilfe von „Social Engineering“ dazu zu bringen, auf schädliche Links zu klicken oder schädliche Software zu installieren. Das Security Awareness Training und die Phishing-Simulationen von KnowBe4 beschäftigen sich nicht nur mit softwarebasierten Angriffsvektoren und Warnsignalen, sondern auch mit physischer Sicherheit. Sicherheitstraining von Mitarbeitenden ist ein fundamentaler Baustein bei der Sicherung Ihres Netzwerks.

Simulierte Phishing-Angriffe

Training ist der erste Schritt zum Festigen der ersten Sicherheitsebene. In Verbindung mit simulierten Phishing-Angriffen werden Nutzer:innen zusätzlich darin geschult, stets wachsam zu bleiben, sodass ein erfolgreicher Phishing-Versuch oder E-Mail-Angriff extrem unwahrscheinlich wird.

Mit den simulierten Phishing-Kampagnen von KnowBe4 können Sie heute vollständig randomisierte und anpassbare simulierte Phishing-Angriffe an beliebig viele Nutzer:innen in Ihrer Umgebung senden. Es ist wichtig, dass alle aufmerksam gegenüber solchen Angriffen sind und bleiben. Durch die bloße Kenntnis von den simulierten Phishing-Angriffen werden Nutzer:innen die in ihrem Posteingang eingehenden Nachrichten noch aufmerksamer betrachten. Sie wissen, dass sie sich nicht ausschließlich auf die „Antivirus-Software“ oder die „IT“ verlassen können – stattdessen werden sie aktiv getestet. Außerdem können etwaige Unachtsamkeiten oder versehentliche Klicks als Gelegenheit genutzt werden, um das Training zu wichtigen Warnsignalen weiter zu vertiefen. Die Folgen eines Klicks auf eine simulierte Phishing-E-Mail sind deutlich weniger drastisch als bei einem tatsächlichen Phishing-Angriff.

Ein weiterer Vorteil simulierter Phishing-Angriffe besteht in der sofortigen Sensibilisierung für aktuelle Bedrohungen. Durch simulierte Phishing-Angriffe bekommen Sie beispielsweise eine Vorstellung davon, wie die Nutzer:innen auf Malware und Phishing-E-Mails reagieren, die in ähnlicher Form von Ransomware-Banden eingesetzt werden. Auf diese Weise können Sie Schwachstellen unmittelbar erkennen und Nutzer:innen über aktuelle Bedrohungen informieren, damit diese wissen, worauf sie achten müssen. KnowBe4 verfügt über eine ständig aktualisierte Liste von Ransomware und E-Mail-Vorlagen aus aktuellen Vorfällen, mit denen Sie prüfen können, ob die Nutzer:innen in Ihrer Umgebung anfällig für Phishing-Versuche sind.

Wenn Sie bei vier wichtigen Punkten Ihre Hausaufgaben erledigen, können Sie das Risiko für Exploits von Cyberkriminellen wie Ransomware-Angriffe deutlich senken. Es handelt sich um folgende vier Punkte:

- Verhindern von Social Engineering, z. B. durch Security Awareness Training und simulierte Phishing-Angriffe
- Patchen von Software
- Einsetzen von MFA, soweit möglich
- Verwenden starker und eindeutiger Passwörter, sofern der Einsatz von MFA nicht möglich ist

Computer- und Netzwerksicherheitsteams sollten zahlreiche weitere Gegenmaßnahmen umsetzen. Oft sind es jedoch diese vier grundlegenden Maßnahmen, denen nicht genügend Aufmerksamkeit gewidmet wird, sodass Hacker:innen, Malware und Ransomware-Banden erfolgreich in Geräte und Umgebungen eindringen und Schaden anrichten können.

Wir hoffen, dass Sie die in diesem Dokument aufgeführten Schritte in Ihren Ransomware-Reaktionsplan einbinden können. Wir hoffen natürlich auch, dass Sie und Ihre Organisation niemals Opfer eines Ransomware-Exploits werden. Sollte es doch dazu kommen, finden Sie in diesem Handbuch Tipps zur weiteren Vorgehensweise, Wiederherstellung und Verhinderung zukünftiger Sicherheitsvorfälle.

KnowBe4

Checkliste zur Reaktion auf Ransomware-Angriffe

SCHRITT 1: Anfängliche Untersuchung

- [ ] a. Ermitteln, ob es sich wirklich um einen Ransomware-Angriff handelt
- [ ] b. Ermitteln, ob mehrere Geräte betroffen sind

Wenn ja, fortfahren:

SCHRITT 2: Ransomware-Vorfall bekannt geben und Maßnahmen einleiten

- [ ] a. Ransomware-Vorfall bekannt geben
- [ ] b. Auf zuvor vereinbarte, alternative Kommunikationsmittel umsteigen
- [ ] c. Teammitglieder, Geschäftsleitung und Rechtsabteilung benachrichtigen

SCHRITT 3: Gerät(e) vom Netzwerk trennen

- [ ] a. Netzwerk deaktivieren (über die Netzwerkgeräte, sofern möglich)
- [ ] b. Geräte ausschalten, wenn Wiperware vermutet wird

SCHRITT 4: Umfang des Exploits ermitteln

Auf folgende Anzeichen achten:

- [ ] a. Zugeordnete oder freigegebene Laufwerke
- [ ] b. Cloudspeicher: DropBox, Google Drive, OneDrive usw.
- [ ] c. Netzwerkspeichergeräte jeglicher Art
- [ ] d. Externe Festplatten
- [ ] e. USB-Speichergeräte jeglicher Art (UBS-Sticks, Memory Sticks, angeschlossene Telefone/Kameras)
- [ ] f. Zugeordnete oder freigegebene Ordner von anderen Computern

Ermitteln, ob Daten oder Anmeldedaten gestohlen wurden

- [ ] a. Protokolle und DLP-Software auf Anzeichen von Datenlecks prüfen
- [ ] b. Nach ungewöhnlich großen Archivdateien (z. B. ZIP, ARC usw.) suchen, die vertrauliche Daten enthalten und die möglicherweise als Zwischenspeicherung angelegt wurden
- [ ] c. Nach Malware, Tools und Scripts suchen, die möglicherweise zum Durchsuchen und Kopieren von Daten verwendet wurden
- [ ] d. Das deutlichste Anzeichen für einen Ransomware-Datendiebstahl ist eine Nachricht von der angreifenden Ransomware-Bande, in der Sie über den Diebstahl Ihrer Daten und/oder Anmeldedaten informiert werden.

Ransomware-Version ermitteln

- [ ] a. Um welche Ransomware-Version/-Art handelt es sich? Zum Beispiel: Ryuk, Dharma, SamSam usw.

SCHRITT 5: Schaden begrenzen

- [ ] a. Bei der anfänglichen Untersuchung sollte auch versucht werden, alle entdeckten Schäden so weit wie möglich einzudämmen.

SCHRITT 6: Informationen in Teamsitzungen weitergeben

- [ ] a. Das Ziel besteht darin, das Team über alle Erkenntnisse wie Umfang und Ausmaß des Schadens zu informieren.

SCHRITT 7: Entscheidung über die Reaktion fällen

- [ ] a. Lösegeld zahlen oder nicht?
- [ ] b. Reparieren oder neu aufbauen?
- [ ] c. Externe Parteien hinzuziehen?
- [ ] d. Branchenaufsichts- und Strafverfolgungsbehörden, BSI, BKA usw. informieren?

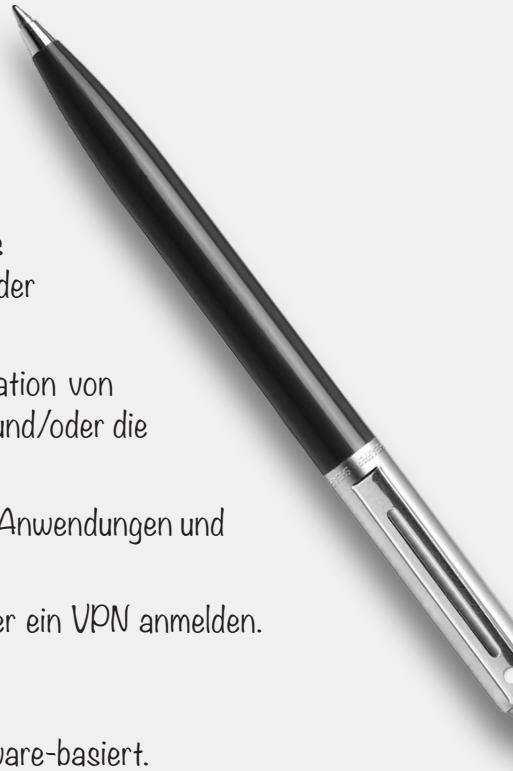
SCHRITT 8: Umgebung wiederherstellen

- [ ] a. Nur Reparatur oder kompletter Neuaufbau
- [ ] b. Beweissicherung erforderlich?
- [ ] c. Anhand einer Business-Impact-Analyse ermitteln, welche Geräte und Systeme in welchem Zeitraum wiederhergestellt werden sollten
- [ ] d. Zuerst die geschäftskritische Infrastruktur wiederherstellen

SCHRITT 9: Nächste Schritte

Zukünftige Cyberangriffe verhindern

- [ ] a. Social Engineering abwenden
- [ ] b. Software patchen
- [ ] c. Multi-Faktor-Authentifizierung (MFA) verwenden, sofern möglich
- [ ] d. Starke, eindeutige Passwörter verwenden
- [ ] e. Antivirus- oder EDR-Software (Endpoint Detection and Response) verwenden
- [ ] f. Anti-Spam-/Anti-Phishing-Software verwenden
- [ ] g. Software zum Schutz vor Datenverlust (Data Leak Prevention, DLP) verwenden
- [ ] h. Umfangreiche Datensicherungen mit regelmäßigen Tests durchführen



Erste Verteidigungslinie: Software

- [ ] 1. Stellen Sie sicher, dass Sie über eine Firewall verfügen und diese verwenden.
- [ ] 2. Implementieren Sie Anti-Spam- und/oder Anti-Phishing-Software. Dies ist mithilfe von Software oder dedizierter Hardware wie SonicWALL- oder Barracuda-Geräten möglich.
- [ ] 3. Stellen Sie sicher, dass alle in Ihrer Organisation die neueste Generation von Endpunktschutz und/oder Endpunktschutzmaßnahmen wie Whitelists und/oder die Echtzeitsperrung ausführbarer Dateien verwenden.
- [ ] 4. Sorgen Sie für ein äußerst diszipliniertes Patchverfahren, bei dem alle Anwendungen und Betriebssystemkomponenten mit Schwachstellen aktualisiert werden.
- [ ] 5. Stellen Sie sicher, dass sich alle Nutzer:innen, die remote arbeiten, über ein VPN anmelden.

Zweite Verteidigungslinie: Datensicherungen

- [ ] 1. Implementieren Sie eine Sicherungslösung: Software- und/oder Hardware-basiert.
- [ ] 2. Stellen Sie sicher, dass für alle Daten, auf die Sie zugreifen oder die gespeichert werden müssen, eine Sicherung durchgeführt wird, auch von mobilen bzw. USB-Speichergeräten.
- [ ] 3. Achten Sie darauf, dass Ihre Daten nach der Sicherung sicher, redundant und leicht zugänglich sind.
- [ ] 4. Testen Sie regelmäßig die Wiederherstellungsfunktion Ihres Sicherungs-/Wiederherstellungsverfahrens. Testen Sie die Datenintegrität physischer Sicherungen und die Durchführbarkeit von Wiederherstellungen für Online-/Softwaresicherungen zumindest für Dateien der letzten drei oder vier Monate. Cyberkriminelle können monatelang in Ihren Netzwerken lauern und Ihre Sicherungen kompromittieren.

Dritte Verteidigungslinie: Diebstahlschutz für Daten und Anmeldedaten

- [ ] 1. Implementieren Sie Tools zum Schutz vor Datenverlust (Data Leak Prevention, DLP).
- [ ] 2. Verwenden Sie das Prinzip der geringsten Berechtigungen, um Dateien, Ordner und Datenbanken zu schützen.
- [ ] 3. Aktivieren Sie Systemprotokolle, um Datenbewegungen nachzuverfolgen.
- [ ] 4. Analysieren Sie den Netzwerkverkehr, um ungewöhnliche Datenbewegungen zwischen Computern und Netzwerken zu erkennen.
- [ ] 5. Verschlüsseln Sie nicht verwendete Daten, um unbefugtes Kopieren zu erschweren.

Vierte und letzte Verteidigungslinie bzw. die „Last Line of Defense“: Nutzer:innen

- [ ] 1. Informieren Sie Ihre Nutzer:innen in professionellem Security Awareness Training, worauf sie achten müssen, um das Herunterladen/Ausführen schädlicher Anwendungen zu verhindern.
- [ ] 2. Ihre E-Mail-Filter übersehen 5 bis 10 % der schädlichen E-Mails. Führen Sie daher regelmäßig simulierte Phishing-Angriffe durch, um Nutzer:innen für aktuelle Bedrohungen zu sensibilisieren (am besten mindestens einmal im Monat).

Weitere Ressourcen

Ransomware Simulator
Mit diesem Simulator finden Sie heraus, wie anfällig Ihr Netzwerk gegenüber Ransomware-Angriffen ist.

Phishing Security Test (kostenlos)
Mit diesem kostenlosen Test erhalten Sie einen Eindruck davon, wie anfällig Ihre Nutzer:innen gegenüber Phishing sind (Phish-prone-Wert).

Phish Alert Button (kostenlos)
Mit diesem Tool können Mitarbeitende ab sofort Phishing-Angriffe mit nur einem Klick sicher melden.

Email Exposure Check (kostenlos)
Welche Ihrer E-Mail-Anmeldedaten wurden bereits offengelegt? Werden Sie aktiv, bevor es die Cyberkriminellen tun.

Domain Spoof Test (kostenlos)
Finden Sie heraus, ob Hacker:innen E-Mail-Adressen Ihrer Domain spoofen können.

CEO-Fraud-Handbuch
Durch CEO-Betrug sind bereits Verluste von mehr als 3 Milliarden US-Dollar entstanden. Informieren Sie sich, damit Sie nicht das nächste Opfer werden. Das CEO-Fraud-Handbuch bietet einen umfassenden Überblick, wie Daten von Führungskräften kompromittiert werden, wie solche Angriffe verhindert werden können und was Opfer tun müssen.

Über KnowBe4

KnowBe4 ist Anbieter der weltweit größten Plattform für Security Awareness Training und Phishing-Simulationen. Der Faktor Mensch wurde bei Sicherheitsschulungen bisher deutlich vernachlässigt. In den umfangreichen KnowBe4-Programmen werden Mitarbeitende über die andauernden Gefahren von Social Engineering aufgeklärt und erfahren, wie sie ihr Unternehmen schützen können.

Der neue Ansatz kombiniert elementare Tests auf Basis realer Angriffsszenarien, kurzweilige interaktive Trainings, kontinuierliches Assessment anhand von simulierten Phishing-Versuchen, Vishing-Angriffe sowie aussagekräftige Reports, um Unternehmen durch sicherheitsbewusstes Handeln besser vor tatsächlichen Angriffen zu schützen.

Weltweit nutzen Zehntausende von Unternehmen aus unterschiedlichsten Branchen – darunter auch stark reglementierte Bereiche wie Finanzwesen, Gesundheitswesen, Energiebranche, öffentliche Verwaltung und Versicherungswesen – die KnowBe4-Plattform, um Nutzer in die Lage zu versetzen, kompetente Entscheidungen hinsichtlich Cybersicherheit zu treffen.

Weitere Informationen finden Sie auf www.KnowBe4.de.

KnowBe4
Human error. Conquered.

KnowBe4 Germany | Stubenrauchstr. 72 | 12161 Berlin – Deutschland | knowbe4.de |

Tel.: +49 30 34 64 64 60 | E-Mail: kontakt@knowbe4.com

04C01K05