WatchGuard
Endpoint Security

# Entkommen Sie dem Ransomware-Labyrinth

Ransomware ist eine sich ständig weiterentwickelnde Form von Malware. Sie zielt darauf ab, geschäftskritische Daten zu stehlen und sie anschließend zu verkaufen oder Dateien auf einem Gerät zu verschlüsseln, wodurch alle Dateien und die Systeme, die auf ihnen beruhen, unbrauchbar werden. Böswillige Akteure fordern dann Lösegeld für die Entschlüsselung.

Die Anzahl und Häufigkeit von Ransomware-Angriffen nimmt von Jahr zu Jahr dramatisch zu, während die Vorfälle, die für Schlagzeilen sorgen, sich an Umfang und Reichweite immer mehr ausweiten. Ransomware-Banden nehmen auch die Geschäftspartner ihrer Hauptopfer ins Visier. Sie zwingen sie zur Zahlung eines Lösegelds, um Datenverluste oder durch den Angriff verursachte Geschäftsunterbrechungen zu verhindern.

# Herkömmliche Endpoint-Schutzwerkzeuge sind einfach nicht mehr die beste Verteidigung

**+95%**

Ransomware-Angriffe sind 2023 im 2. Quartal um 11 % und im Vergleich zum Vorjahr um 95 % gestiegen[1]

**+2**

Duale Ransomware-Angriffe nutzen eine Kombination aus Verschlüsselung, Exfiltration und finanziellen Verlusten, um die Opfer zur Zahlung von Lösegeldforderungen zu zwingen[2]

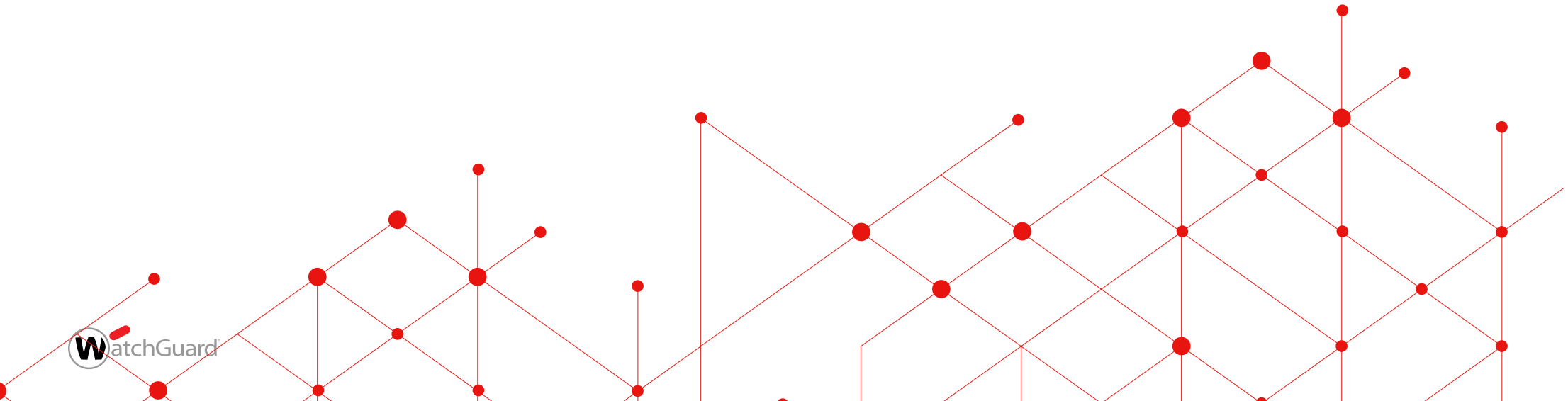
**10–15 Mal**

die Kosten für die Wiederherstellung und die daraus resultierende Ausfallzeit nach einem Ransomware-Angriff können 10 bis 15 Mal höher sein als das Lösegeld[3]

**#1**

Ransomware ist weiterhin eine der häufigsten Angriffsarten bei Sicherheitsverstößen im Jahr 2023[4]

1. Dark Reading - Q3 2023 Global Ransomware Report
2. FBI Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends
3. How to Prepare for Ransomware Attacks | Gartner
4. Verizon – DBIR: 2023 Data Breach Investigations Report



# Ist Ihr Unternehmen angemessen geschützt?

Ransomware ist vielleicht die bisher lukrativste Methode der Cyberkriminalität. Das heißt, die Art und Weise, wie Cyberkriminelle aus den Daten ihrer Opfer einen Wert schöpfen, verändert sich deutlich. Bei Ransomware müssen sich die Angreifer nicht länger auf den Diebstahl von Daten konzentrieren, die sie leicht weiterverkaufen können. Sie machen sich stattdessen die Bedeutung dieser Daten für das Opfer zunutze.

Auch wenn die Daten inhaltlich vielleicht nicht sensibel sind, können sie für das betroffene Unternehmen geschäftskritisch sein. Indem sie die Daten als Geiseln halten und ein Lösegeld für ihre Rückgabe fordern, können Angreifer Daten zu Geld machen, für die sie möglicherweise keine sonstige Verwendung hatten.

Aufgrund dieses Paradigmenwechsels rücken eine Vielzahl von Organisationen, von denen sich viele lange Zeit für zu klein hielten, um ein attraktives Ziel für Cyberangriffe zu sein, fest ins Fadenkreuz von Cyberkriminellen.

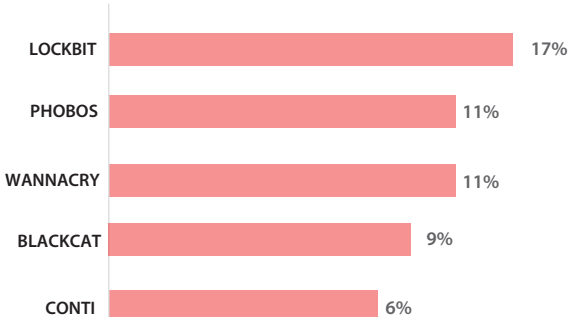
Bei Ransomware müssen sich die Angreifer nicht länger auf den Diebstahl von Daten konzentrieren, die sie leicht weiterverkaufen können. Sie machen sich stattdessen die Bedeutung dieser Daten für das Opfer zunutze.

WatchGuard

# Ransomware: Hinter den Kulissen

Heutige Cyberangreifer verwenden ausgefeilte Taktiken, um herkömmliche Ransomware-Erkennungsmaßnahmen zu umgehen und sich in der Alltäglichkeit und Komplexität der Umgebung ihrer Ziele zu verstecken. Bei ihren Bewegungen durch das Netzwerk verfolgen sie das Ziel, Daten zu stehlen, Ransomware zu installieren, Daten zu verschlüsseln und Schaden anzurichten. Sobald sie haben, was sie brauchen, drohen sie mit dem Verkauf oder der Weitergabe exfiltrierter Daten oder Authentifizierungsinformationen, falls das Lösegeld nicht gezahlt wird.

## Wichtigste Ransomware-Varianten und deren Häufigkeit[5]




5. IBM – X-Force Threat Intelligence Index 2023

Ransomware-as-a-service, Spear-Phishing, Angriffe auf ungepatchte Systeme, doppelte Erpressung und Angriffe über die Lieferkette waren die fünf wichtigsten anfänglichen Infektionsvektoren, die zur Verbreitung von Ransomware in kompromittierten Netzwerken eingesetzt wurden.[5]

6. Gemeinsames Gutachten zeigt die zunehmende globale Bedrohung durch Ransomware auf

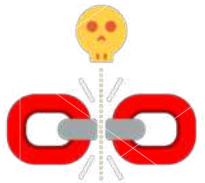
## Die wichtigsten Ransomware-Trends:

**Ransomware-as-a-service**

**Spear-Phishing**

**Angriffe auf ungepatchte Systeme**

**Doppelte Erpressung**



**Angriffe über Lieferketten**

# Der Lebenszyklus eines Ransomware-Angriffs I

Ransomware folgt einem Angriffsmuster[6], das die folgenden Phasen umfasst. In den meisten Fällen reichen wenige Minuten zur Ausführung des Angriffs. Selbst die harmloseste Aktion kann dazu führen, dass der Endpoint zum Opfer von Ransomware wird und die sensiblen oder geschäftskritischen Dateien zur Geisel einer Erpressung werden.

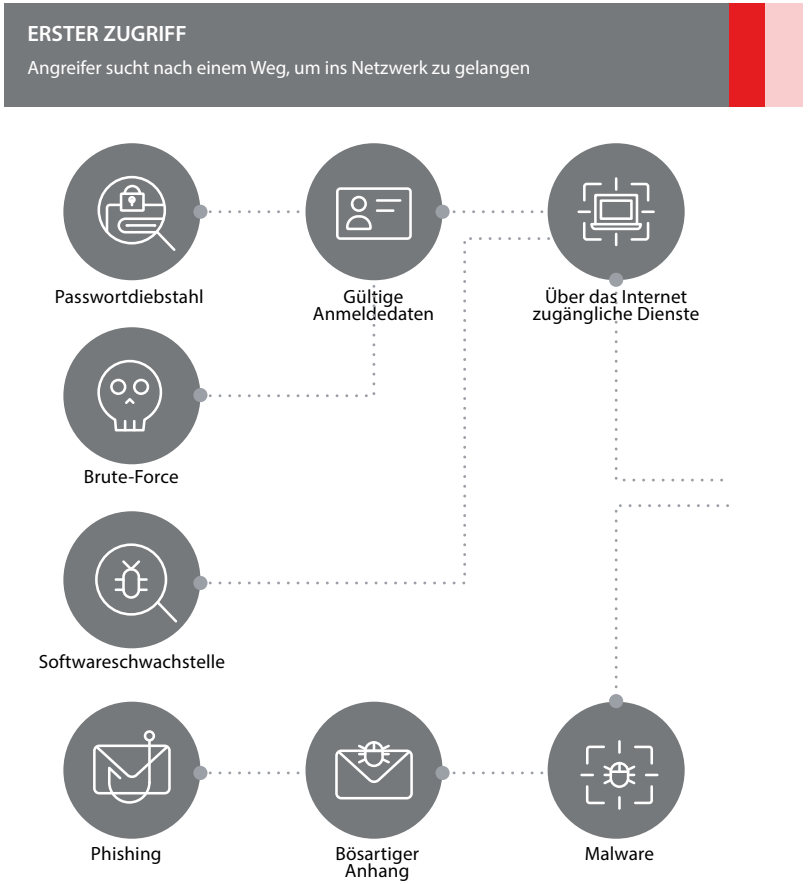
## Erster Zugriff

In der ersten Phase des Angriffs versuchen die Cyberkriminellen, im Netzwerk des Unternehmens fest Fuß zu fassen. In den meisten Fällen verschaffen sie sich Zugang über einen der folgenden Infektionsvektoren: Passwortdiebstahl, Brute-Force, Software-Schwachstellen oder Phishing. Nachdem sich der Angreifer eingeschlichen hat, versucht er, kritische Identitäten ausfindig zu machen und Anmeldedaten zu erlangen, mit denen er unter Umgehung herkömmlicher Schutzmaßnahmen weiter vordringen kann.

Gängige Ransomware-Angriffe verwenden verschiedene Formen von Malware, z. B. handelsübliche oder benutzerdefinierte Malware (zur Wiederverwendung heruntergeladen oder gekauft). Malware wird in der Regel über Spear-Phishing-E-Mails verbreitet, die bösartige Anhänge enthalten.

Bei diesen Anhängen handelt es sich häufig um Trojaner in Form von Office- oder PDF-Dokumenten mit eingebetteter Ransomware. Sobald sie geöffnet werden und sofern die Ausführung von Makros erlaubt ist, können sie ihre Nutzlast ausführen und versuchen, Malware auf den Computer zu laden, auf dem das Dokument geöffnet wurde. Ransomware scheint oft aus legitimen Quellen zu stammen, z. B. von Finanzinstituten, staatlichen Stellen oder Benutzern innerhalb der eigenen Organisation.

Wir haben auch viele Ransomware-Vorfälle beobachtet, die damit begannen, dass Angreifer Schwachstellen in über das Internet zugänglichen Diensten ausnutzten. Häufig waren dies Fernzugriffssysteme wie Remote Desktop Protocol (RDP), Virtual Protection Networks (VPNs) und andere Betriebssysteme oder Software-Schwachstellen von Drittanbietern. Einige Angreifer versuchen auch, durch Brute-Force-Methoden Zugangsdaten zu erzwingen und legen es gezielt auf schwache und leicht zu erratende Benutzernamen und Kennwörter an. Die meisten Ransomware-Varianten nutzen mehrere Infektionsvektoren.



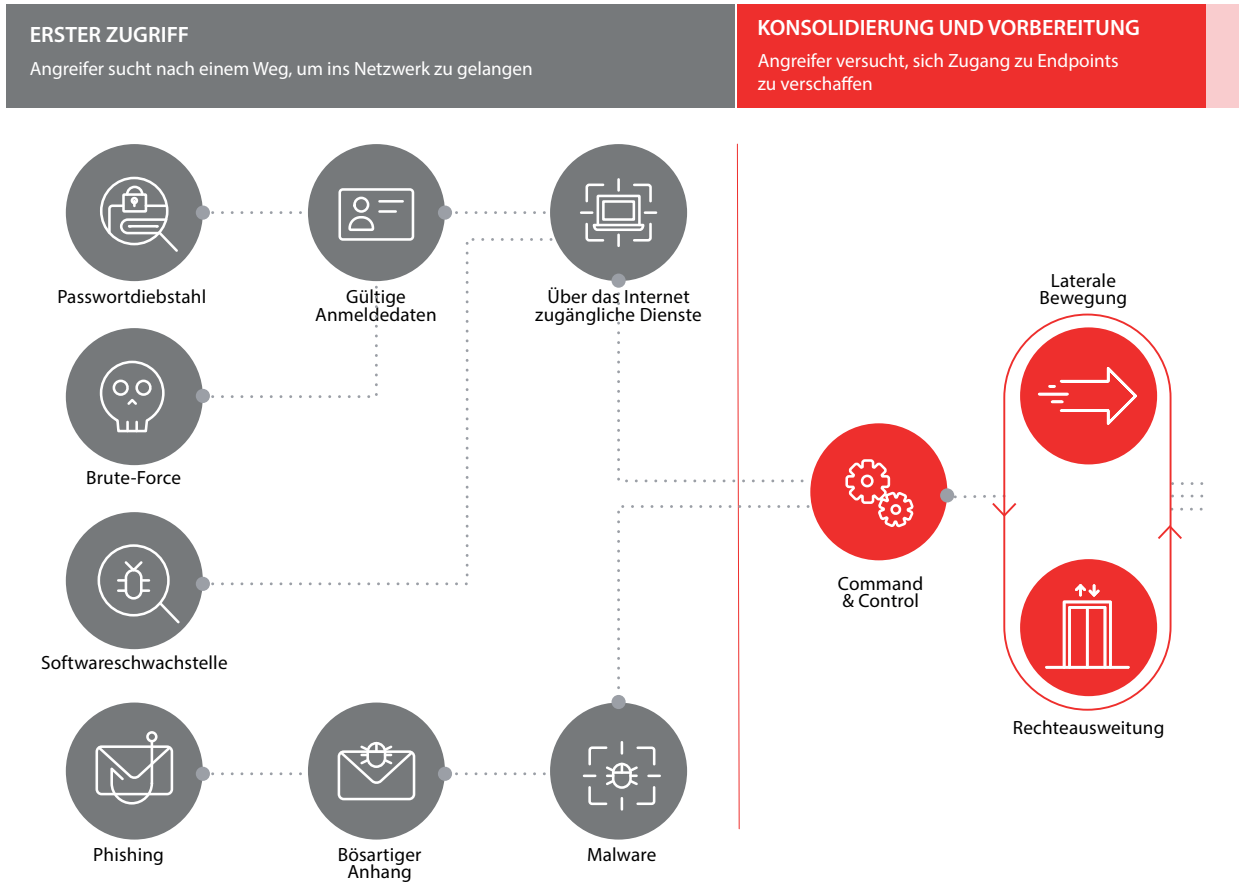

6. How ransomware happens and how to stop it (so entsteht Ransomware und so kann man sie stoppen) – certnz

# Der Lebenszyklus eines Ransomware-Angriffs II

## Konsolidierung und Vorbereitung

Haben Bedrohungsakteure sich Zugang zum Netzwerk verschafft, benötigen sie eine Reihe von Werkzeugen, um den Angriff durchzuführen. Sie dringen entweder mit Malware ein, die ein Paket mit allen für den Angriff erforderlichen Werkzeuge enthält, oder sie laden nach dem Eindringen die erforderlichen Tools herunter. Dazu stellen Sie eine Kommunikation mit einem Command-and-Control-Server (C2) her, um mit den nächsten Angriffsschritten fortzufahren. Diese Kommunikation erfolgt meist über vertrauenswürdigen Datenverkehr wie DNS.

C2-Tools können auch dazu verwendet werden, andere Endpoints im Netzwerk zu finden, auf Geräten zu verbleiben und diese Aktivitäten zu verschleiern.



# Der Lebenszyklus eines Ransomware-Angriffs II

**Hacker verwenden für die Durchführung der Angriffe viele Werkzeuge, z. B:**

- Erkundungstools, die dem Angreifer helfen, herauszufinden, wo er sich im Netzwerk befindet und welche Konten weiter ins Visier genommen werden können. Beispiele: Nmap, Process Hacker und BloodHound
- „Credential Dumping"-Tools, die dabei helfen, die Anmeldedaten anderer privilegierter Konten zu kompromittieren, mit denen der Angreifer sich dann innerhalb des Netzwerks weiter bewegen kann. Beispiele: Mimikatz und ProcDump
- Integrierte Programme wie PowerShell, Windows Management Instrumentation (WMI) und PsExec. Sicherheitsforscher konnten feststellen, dass WMI- und PSExec-Befehle zum Löschen lokaler Sicherungskopien und PowerShell zum Erstellen bösartiger Hintertüren verwendet wurden.

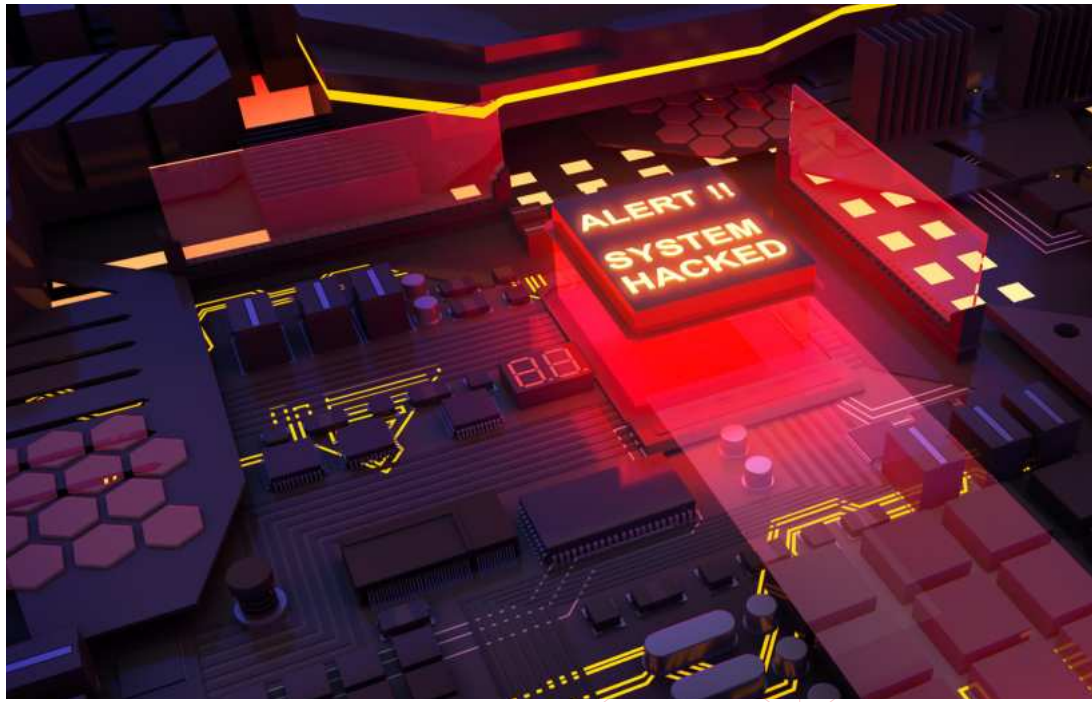
## Laterale Bewegung und Rechteausweitung

Cyberkriminelle bewegen sich innerhalb des Netzwerks lateral, um anfällige privilegierte Konten zu finden. Sobald der Angreifer Zugriff auf ein Konto, ein Netzwerk oder eine Ressource erhält, eskaliert er den Angriff, indem er diesen Zugriff nutzt, um sich durch die Infrastruktur zu bewegen. In dieser Phase bahnen sich die Angreifer üblicherweise einen Weg zu den wichtigsten Daten, indem sie Sicherheitsschichten durchbrechen und sich zusätzliche Privilegien verschaffen.

Eine der häufigsten Techniken, die bei Ransomware-Angriffen beobachtet werden, ist die Ausnutzung von Administratorkonten. Administratorkonten sind kritische Ziele, da Organisationen in der Regel ein gemeinsames Kennwort für alle lokalen Administratorkonten verwenden. Durch die Erlangung von Administratorrechten können Angreifer die Sicherheitskonfigurationen herkömmlicher AV- und EDR-Lösungen manipulieren. Ihr Ziel dabei ist es, Sicherheitskontrollen zu deaktivieren, eine Erkennung zu vermeiden und eine Nutzlast auf den Endpoint des Opfers herunterzuladen und zu installieren.

Der Zugriff auf Domain-Controller ermöglicht es ihnen außerdem, mit einem Schlag Malware auf alle Systeme im Netzwerk zu übertragen. Angreifer wenden Reihe von Taktiken an, um Domänen-Administratorrechte zu erlangen, darunter Techniken wie Kerberoasting, Pash-the-Hash-Angriffe und Diebstahl von im SYSVOL-Ordner gespeicherten Kennwörtern.

Um sicherzustellen, dass die Opfer ihre Daten nicht einfach aus ihren Backups wiederherstellen können, werden bei den meisten Ransomware-Angriffen die Backups zerstört.

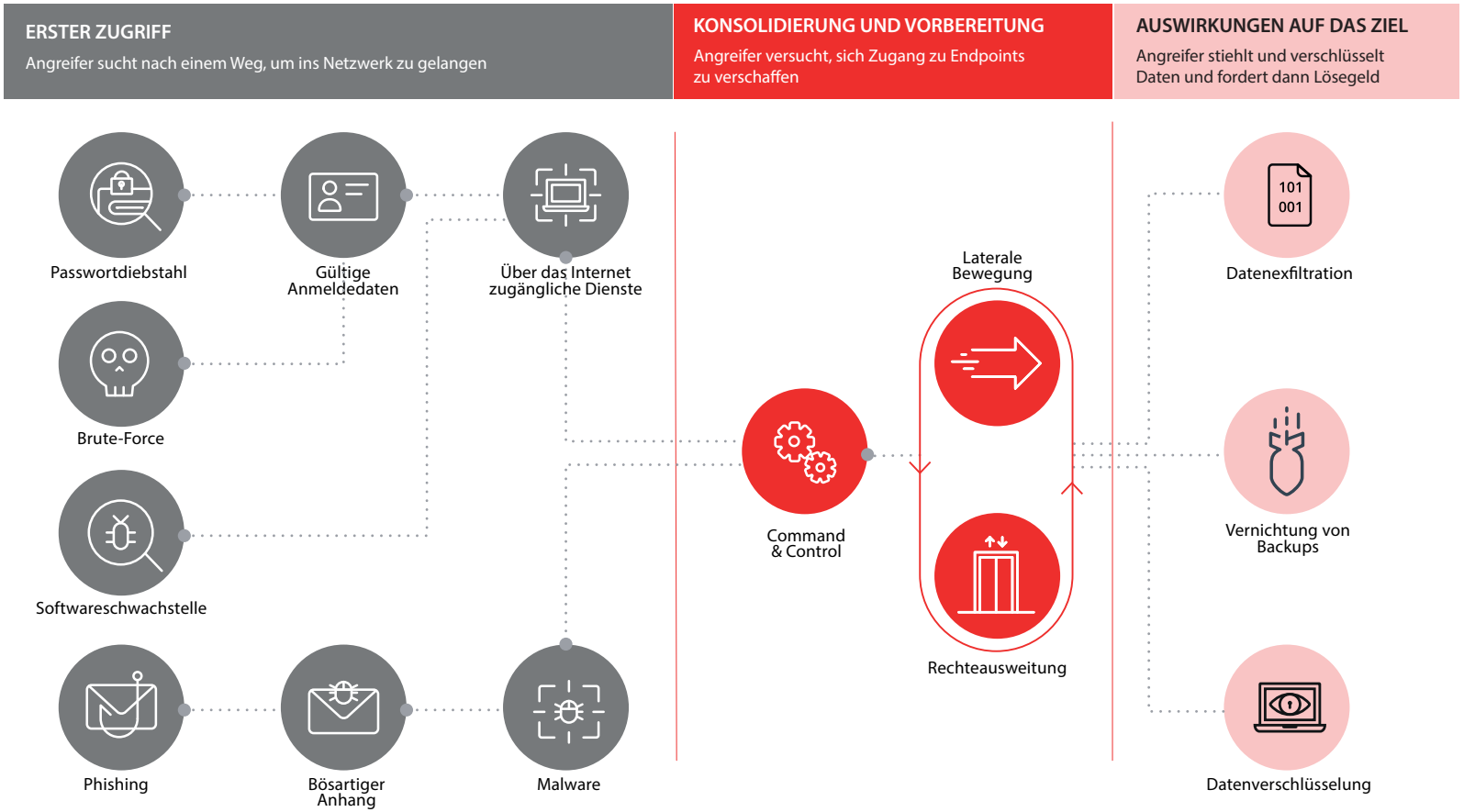


# Der Lebenszyklus eines Ransomware-Angriffs III

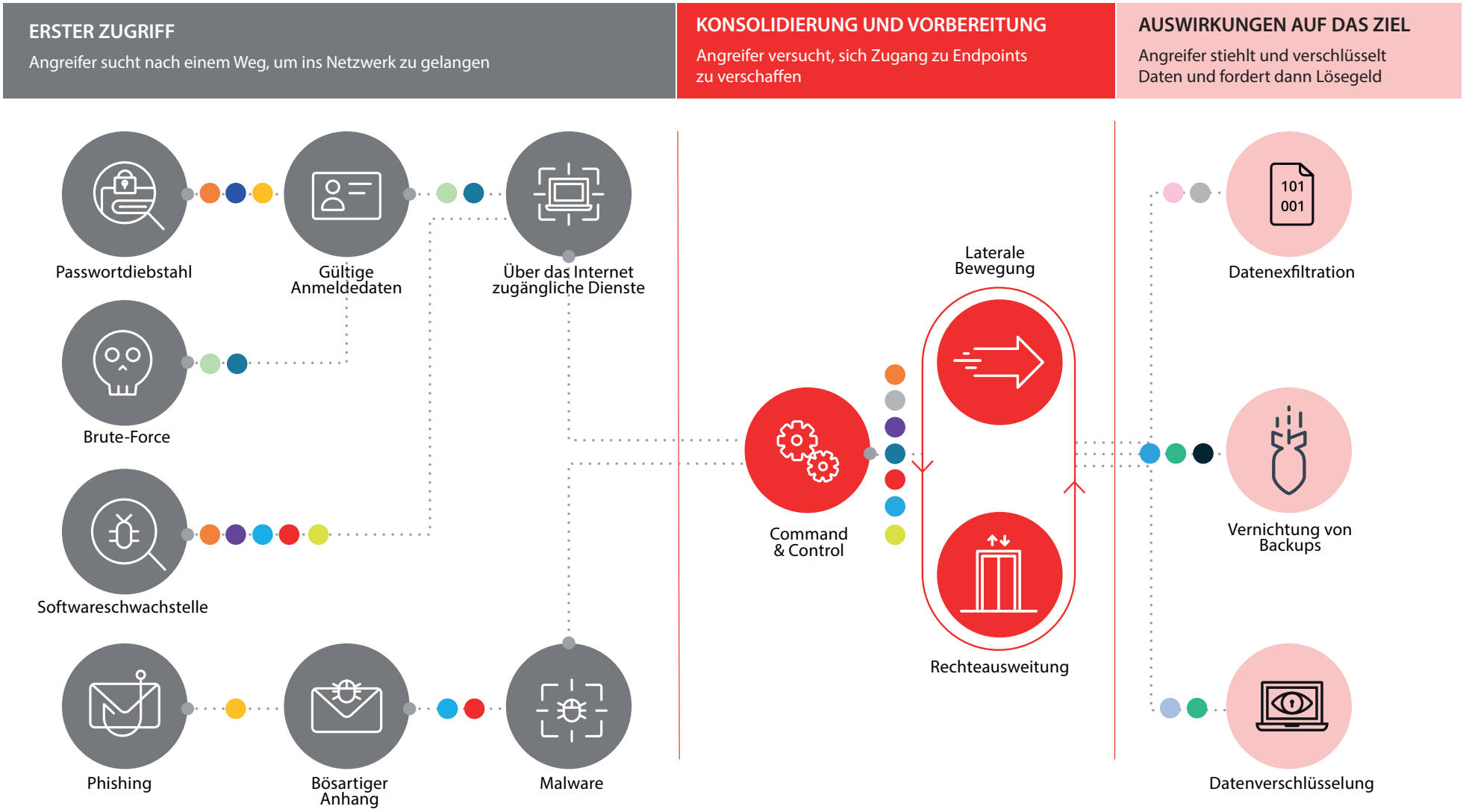
## Auswirkungen auf das Ziel

In dieser letzten Phase des Angriffs wurde die Ransomware heruntergeladen und auf dem System des Opfers installiert. Sie beginnt nun mit der Ausführung der vorgesehenen Aufgaben Sobald der Angreifer den kritischen Schutz des Systems deaktiviert hat, versucht er, sensible Informationen auf dem Endgerät zu exfiltrieren, Backups der Organisation zu zerstören und schließlich Systeme und Daten zu verschlüsseln.

An diesem Punkt verweisen Lösegeldhinweise oder Sperrbildschirme das Opfer auf die Zahlungsaufforderung des Hackers (in der Regel Kryptowährung) und andere Details, um sicherzustellen, dass das Opfer die Anweisungen des Hackers befolgt. Diese Details beinhalten oft einen Betrag in Kryptowährung als Gegenleistung für den Zugriff auf die Dateien des Opfers oder eine zweite Zahlung, um die Angreifer an der Weitergabe oder dem Verkauf der Daten zu hindern.



# Verhindern von Ransomware mit WatchGuard Endpoint Security



### Verhindern Sie Vorfälle, noch bevor sie eintreten

Gerade bei Ransomware-Angriffen ist es besonders wichtig, den Angriff zu verhindern, bevor er stattfindet. Wenn die Ransomware erst einmal in Ihrer Organisation ist und mit der Verschlüsselung der Dateien auf Ihren Laptops, Computern und Servern beginnt, kann es zu spät sein. Die mit einem Ransomware-Angriff verbundenen Kosten sind enorm, daher ist die beste Verteidigung die Prävention.

Unsere einzigartige Schutzebene enthält verschiedene Schutzebenen und eine Vielzahl fortschrittlicher Technologien, die vor Ransomware schützen.

### Verwenden Sie ein starkes Passwort-Manager-System

Die Sicherheit von Passwörtern ist für den Schutz der Daten Ihrer Organisation von entscheidender Bedeutung. Viele Unternehmen versäumen es jedoch, die richtige Verwendung und Verwaltung von Passwörtern in ihren Teams zu implementieren. Diese einfache Verteidigungslinie kann die Wahrscheinlichkeit eines Ransomware-Angriffs oder eines anderen Cyberangriffs drastisch verringern. Organisationen, die einem robusten Passwortverwaltungssystem Priorität einräumen, werden bei der Verhinderung eines Angriffs erfolgreicher sein.

Mit Password Manager können Administratoren alle Passwörter unter einem Hauptschlüssel verwalten, Formulare schnell und einfach automatisch ausfüllen, Passwörter synchronisieren und aktualisieren, Duplikate vermeiden und Schlüssel mit militärischem Sicherheitslevel bereitstellen.

### Implementieren Sie eine Multifaktor-Authentifizierung (MFA)

Ransomware-Angriffe beginnen in der Regel mit dem Diebstahl von Benutzerdaten, die einem Angreifer Zugang zum Netzwerk oder zu einem sensiblen Geschäftskonto verschaffen. AuthPoint, unsere Multi-Faktor-Authentifizierungslösung (MFA), stellt sicher, dass Angreifer alleine mit gestohlenen Zugangsdaten nicht dorthin gelangen können, wo sie nicht hingehören. Sie verlangt stattdessen zusätzliche Faktoren zum Nachweis der Identität eines Benutzers. Auf diese Weise werden die Auswirkungen verlorener und gestohlener Kennwörter minimiert, während gleichzeitig Transparenz über den Benutzerzugang gewährleistet wird.

Selbst wenn ein Berechtigungsnachweis kompromittiert wird, können unbefugte Benutzer die zweite Authentifizierungsanforderung nicht erfüllen und sind nicht in der Lage, auf den betreffenden physischen Raum, das Computergerät, das Netzwerk oder die Datenbank zuzugreifen.

*Hinweis: Unternehmen, die eine Cyberversicherung abschließen möchten, müssen nachweisen, dass sie E-Mails, Server, Fernzugriff und sensible Daten mit MFA schützen.*

### Kontextuelle Erkennung

Unsere Endpoint Security-Produkte beinhalten eine verhaltensbasierte Erkennung zur Verhinderung und Blockierung von dateilosen Angriffen, die auf in Office-Dateien eingebetteten Skripten basieren, sowie von Angreifern, die LotL-Techniken (living-off-the-land) verwenden.

Sie erkennt, wenn vorhandene Anwendungen am Endpoint missbraucht werden und versuchen, die Sicherheitskontrolle zu umgehen und sich Zugriff auf das System zu verschaffen oder lateral auf andere Endpoints überzugehen. Dies ist ein äußerst wirksamer Schutz gegen Exploits, die Schwachstellen in Webbrowsern und anderen häufig angegriffenen Anwendungen wie Java, Adobe Reader, Adobe Flash, Office usw. ausnutzen.

Unsere Produkte enthalten Hunderte von kontextbezogenen Erkennungen, um Angriffe kontextabhängig zu stoppen. Alle diese Erkennungen sind proaktiv, da sie nicht auf Signaturdateien oder anderen reaktiven Technologien beruhen.

Ein Teil des Kontexts wird von Windows AMSI (Antimalware Scan Interface) bezogen. Durch die Verwendung von AMSI erhalten unsere Lösungen Telemetriedaten und zusätzliche Informationen über die Ausführung von Skripten und Makros. Der Schutz wird somit verbessert, ohne die Computerleistung zu beeinträchtigen.

### Decoy-Dateien

Decoy-Dateien sind Honeypots, mit denen überwacht wird, ob bestimmte von unseren Lösungen bereitgestellte Dateien geändert werden. Falls diese Dateien geändert werden, wird ein Ereignis an unsere Engine zur Verhaltenserkennung gesendet. Sehr wahrscheinlich wird diese Aktion so eingestuft, dass die Ransomware als Root-Prozess beendet wird, wodurch die Verschlüsselung der Datei auf den Endpoints verhindert wird.

### Anti-Exploit-Technologie

Die Anti-Exploit-Technologie ist ein wichtiger Schutz zur Verhinderung lateraler Bewegungen. Mit ihr werden unsere EDR-Lösungen um virtuelle Patching-Funktionen erweitert. Sie ergänzt die Patch-Management-Lösungen, indem sie vor nicht gepatchten Anwendungen oder solchen Anwendungen schützt, die das Ende ihres Wartungszeitraums erreicht haben, wie z. B. Windows XP oder Windows 7.

Im Gegensatz zu anderen Lösungen umfasst unser Anti-Exploit generische Erkennungsfunktionen, die auf dem anomalen Verhalten ausgenutzter Prozesse basieren.

### Zero-Trust Application Service

Unsere EDR-Produkte sind die einzige Lösung auf dem Markt, die laufende Prozesse zu 100 % klassifiziert. Jede unbekannte Anwendung wird blockiert, bis sie von unseren Technologien des maschinellen Lernens (99,98 %) oder von unseren Cybersicherheitsexperten weltweit (0,02 %) als vertrauenswürdig eingestuft wird. Und das alles geschieht in Echtzeit für unbekannte Anwendungen. Zusätzlich bieten unsere Produkte die Flexibilität, autorisierte Software mit detaillierten Regeln für jene Organisationen hinzuzufügen, die ihre eigene Software entwickeln.

Diese Schutzebene ermöglicht es uns, Malware-basierte Angriffe unter Kontrolle zu halten. Sie ist zudem unerlässlich für bereits infizierte Organisationen, um Angriffe mit lateraler Bewegung innerhalb des Netzwerks zu stoppen.

### RDP-Schutz

Der RDP-Schutz ist Teil des Threat Hunting Service und steht allen Kunden zur Verfügung, die unsere EDR-Lösungen erwerben.

Unter gezielten Cyberangriffen auf Unternehmen werden RDP-Brute-Force-Angriffe von Angreifern am häufigsten eingesetzt, insbesondere wenn die Systeme direkt dem Internet ausgesetzt sind. Unsere EDR-Lösung erkennt und schützt Netzwerkcomputer vor Angriffen, die das RDP (Remote Desktop Protocol) als Infektionsvektor nutzen.

Wenn ein durch unsere Lösungen geschützter Computer viele RDP-Verbindungsversuche erhält, die aufgrund ungültiger Anmeldeinformationen fehlschlagen, versetzt die Schutzsoftware den Computer in den Modus „RDP-Erstangriffseindämmung". In diesem Modus wird der RDP-Zugriff auf den Computer von IPs außerhalb des Kundennetzwerks blockiert, die in den letzten 24 Stunden eine große Anzahl von Verbindungsversuchen gesendet haben.

Wenn ein durch unsere EDR-Lösungen geschützter Computer einen erfolgreichen Anmeldeversuch von einem Konto erhält, der zuvor aufgrund ungültiger Anmeldedaten fehlgeschlagen ist, gilt dieses Konto als kompromittiert. Als Schutzmechanismus werden alle externen RDP-Verbindungen, die in den letzten 24 Stunden mindestens einmal eine Verbindung mit dem Zielcomputer erstellen wollten, blockiert.

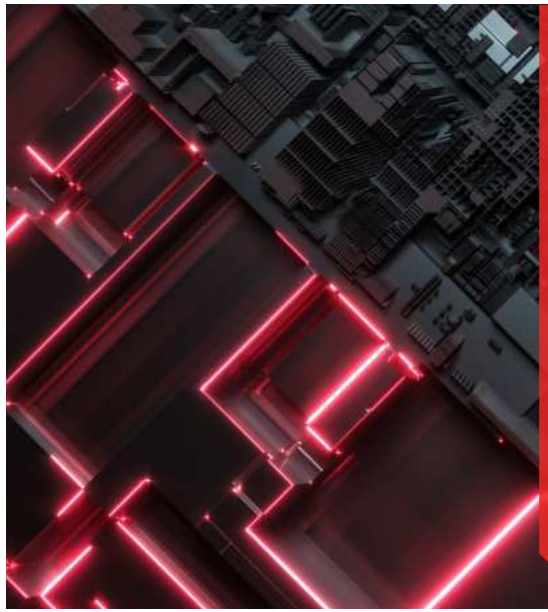
### Anti-Malware-Technologien

Wie viele andere Antiviren-Lösungen der nächsten Generation enthalten auch unsere Endpoint Security-Lösungen Signaturdateien, Zugang zu unserem Echtzeitschutz zu unserer kollektiven Intelligenz sowie heuristische Technologien, die Deep Learning nutzen, um Ransomware-Angriffe zu verhindern, die keine LotL-Techniken (living-off-the-land) verwenden.

### Schutz vor Manipulationen

Viele Ransomware-Angriffe versuchen, den auf den Endgeräten installierten Schutz auszuschalten, bevor sie versuchen, sich über das Netzwerk auszubreiten und Dateien im gesamten Unternehmen zu verschlüsseln. Es ist wichtig, einen Manipulationsschutz gegen Hacker einzubauen, die versuchen, Dienste und Prozesse zu stoppen oder anzuhalten.

Unsere Manipulationsabwehr verwendet proprietäre Technologien, darunter 2FA für den Konsolenzugriff und den sicheren Startmodus von Windows, um den physischen Zugriff auf autorisierte Personen zu beschränken und unbefugte Änderungen zu vermeiden. Sie nutzt außerdem die ELAM-Technologie (Early Launch Anti-Malware) unter Windows 10 und höheren Betriebssystemversionen.



Hacker sind ständig auf der Suche nach Lücken und Hintertüren, die sie ausnutzen können. Indem Sie Ihre Systeme sorgfältig aktualisieren, minimieren Sie Ihre Anfälligkeit für bekannte Schwachstellen.

### Patches zur Verringerung der Angriffsfläche

Hacker sind ständig auf der Suche nach Lücken und Hintertüren, die sie ausnutzen können. Sie minimieren Sie Ihre Anfälligkeit für bekannte Schwachstellen, indem Sie Ihre Systeme sorgfältig aktualisieren.

Ransomware wie WannaCry und Petya nutzte ungepatchte Sicherheitslücken, um sich weltweit zu verbreiten. Die Ransomware-Angriffe Locky und Cerber nutzten eine Schwachstelle in Adobe Flash, um sich auf den Workstations der Opfer zu verbreiten.

Sie können viele Angriffe verhindern, indem Sie sicherstellen, dass Betriebssysteme (Windows, macOS und Linux) und Anwendungen von Drittanbietern aktualisiert und gepatcht werden. Es ist wichtig, frühzeitig und häufig, mindestens einmal im Monat, zu patchen, um kritische Sicherheitslücken zu schließen.

### Anti-Phishingschutz

Phishing per E-Mail ist eine der häufigsten Methoden, um einen Ransomware-Angriff zu starten. Das Blockieren von Phishing-URLs verringert die Wahrscheinlichkeit, dass ein Benutzer auf einen Link klickt, den er nicht anklicken sollte.

### Threat Hunting Service

Selbst eine robuste EDR-Lösung kann sich nicht bei allen Erkennungen auf Präventionstechnologien verlassen ... manchmal braucht es einfach ein menschliches Gehirn, um einen Hacker zu erkennen. Dies gilt insbesondere seit dem Aufkommen von dateilosen Living-off-the-land-Angriffen.

Unser Threat Hunting Service erkennt ungewöhnliche Verhaltensweisen und verdächtige Aktivitäten und kategorisiert diese mit hoher Sicherheit und ohne Fehlalarme als Angriffsindikatoren (IoAs). In der Regel handelt es sich um Angriffe in einem frühen Stadium oder in der Phase der Ausbeutung, bei denen keine Malware verwendet wird.

### Schutz vor Netzwerkangriffen

Ransomware-Vorfälle beginnen häufig damit, dass Angreifer Schwachstellen in über das Internet zugänglichen Diensten ausnutzen. Wenn die Hacker erfolgreich sind und die Organisation bereits infiziert ist, muss der Angriff innerhalb des Netzwerks aufgehalten werden.

Mit Network Attack Protection werden Bedrohungen erkannt und verhindert, indem der Netzwerkverkehr in Echtzeit gescannt wird, wodurch Angriffe, die Schwachstellen in über das Internet zugänglichen Diensten ausnutzen, und solche, die innerhalb des internen Netzwerks auftreten, verhindert werden.

Hacker nutzen häufig Angriffsmethoden und Exploits wie EternalBlue, BlueKeep oder DCShadow. Durch den Einsatz dieser Technologie sind wir in der Lage, derartige Angriffe frühzeitig zu verhindern.

### Isolieren Sie Ihre Endpoints, um den Angriff einzudämmen

Im Falle einer Ransomware-Infektion versucht der Angreifer, das gesamte Netzwerk zu infizieren. Sie können den Angriff eindämmen, indem Sie die betroffenen Endpoints isolieren und verhindern, dass es durch Ausnutzung der Schwachstelle, Verwendung gestohlener Anmeldedaten, Sich-selbst-kopieren und Verwendung des KMU-Protokolls usw. zu lateralen Bewegungen von einem Rechner zum anderen kommt.

Es wäre hilfreich, wenn Sie so schnell wie möglich Patches installieren würden, um die Auswirkungen des Angriffs zu minimieren und die Anzahl der verschlüsselten Dateien in Ihrer Organisation zu verringern.

Isolierte Computer können mit unseren Servern kommunizieren, so dass Sie weiterhin die Sicherheit aller Endpoints verwalten können. Sie können sogar einige Ausnahmen hinzufügen und ihnen erlauben, mit bestimmten Prozessen zu kommunizieren, die Sie für die Wiederherstellung benötigen.

### Aktivieren Sie alle Präventionsmethoden

Um das Risiko auf allen Computern zu beseitigen, müssen Sie den richtigen Schutzstatus beibehalten, Fehlkonfigurationen vermeiden, Anzeichen für Angriffe archivieren, ausstehende kritische Patches anwenden und dafür sorgen, dass alle Schutzebenen aktiv sind. Darüber hinaus ist es notwendig, den Sperrmodus im erweiterten Schutz zu aktivieren, um zu verhindern, dass unbekannte Anwendungen unabhängig von ihrer Quelle ausgeführt werden.

### Wenden Sie Wiederherstellungsmaßnahmen mit „Schattenkopien“ an

Viele Ransomware-Angriffe gehen noch einen Schritt weiter und versuchen, neben der Verschlüsselung von Dateien auch alle Arten von Backups zu zerstören, die von den Kunden erstellt wurden.

Mit unserer Endpoint-Sicherheitslösung können Sie mithilfe der Betriebssystemtechnologie Schattenkopien erstellen, die wir mit unserer Anti-Manipulations-Technologie schützen. Dadurch sind Sie in der Lage, Informationen nach einer Ransomware-Infektion wiederherzustellen.

IT-Profis verwenden die Schattenkopien, um Dateien nach kritischen Systemausfällen wiederherzustellen. Diese Technologie eignet sich aber auch hervorragend zur Wiederherstellung von Dateien, die durch Ransomware verschlüsselt wurden.

Im Gegensatz zu anderen Lösungen, die Kopien jeder verschlüsselten Datei erstellen und dabei viel Speicherplatz verbrauchen, sind Schattenkopien nur für die Speicherung der Unterschiede optimiert. Die Wahrscheinlichkeit, dass der Speicherplatz knapp wird, ist also minimal. Mit unserer Lösung können Sie den Prozentsatz des für Schattenkopien vorgesehenen Speicherplatzes konfigurieren, obwohl die standardmäßig zugewiesenen 10 % in den meisten Fällen ausreichen sollten.

# 10 Wege zur Verteidigung gegen einen Ransomware-Angriff

1

Führen Sie regelmäßig Backups von wichtigen Daten, Systembildern und Konfigurationen durch. Testen Sie Ihre Backups und bewahren Sie sie extern und offline auf, wo Angreifer sie nicht finden können.

2

Verwenden Sie eine Multi-Faktor-Authentifizierung (MFA). Legen Sie sichere Passwörter fest und setzen Sie sie durch; verwalten Sie sie über einen Passwort-Manager.

3

Beschränken Sie den Zugriff auf Ressourcen über interne Netzwerke und setzen Sie einen zeitbasierten Zugriff für privilegierte Konten durch. Schränken Sie Berechtigungen ein, entziehen Sie Endbenutzern lokale Administratorrechte und blockieren Sie die Installation von Anwendungen durch Standardbenutzer.

4

XDR

Fügen Sie XDR-Funktionen hinzu, um die Bedrohungsanalyse zu beschleunigen. Mehr Lösungen desselben Anbieters, die in XDR integriert werden, bewirkt eine bessere Visualisierung und größeren Schutz.

5

Patchen Sie alles, patchen Sie frühzeitig und patchen Sie häufig, um alle Betriebssysteme und Software auf dem neuesten Stand zu halten. Ransomware-Angriffe wie WannaCry und NotPetya nutzten ungepatchte Sicherheitslücken, um sich weltweit zu verbreiten.

6

Implementieren Sie einen robusten Anti-Phishing-Schutz mit verschiedenen Sicherheitsebenen am Endpoint und am Perimeter.

7

Sichern Sie den Fernzugriff ab, indem Sie unnötige RDP-Verbindungen deaktivieren und sich für Ratenbegrenzung, 2FA, VPN oder andere Tools entscheiden. Bevor Sie einen VPN-Zugriff zulassen, überprüfen Sie, ob alle Endpoints, die auf die Unternehmens- oder WLAN-Netzwerke zugreifen, ausreichend

8

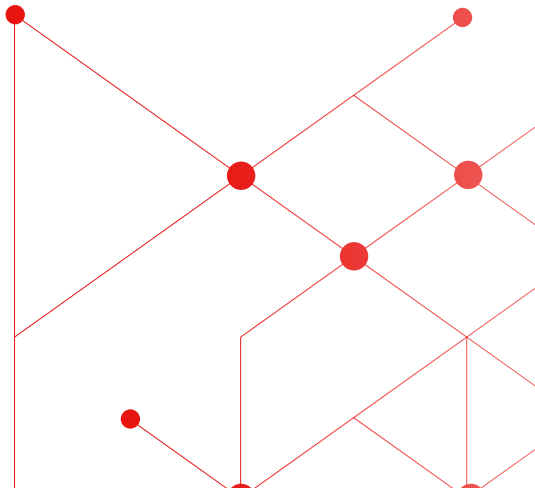
Stellen Sie sicher, dass der Manipulationsschutz aktiviert ist – Ryuk und andere Ransomware-Bedrohungen versuchen, Ihren Endpoint-Schutz zu deaktivieren.

9

Überwachen Sie Warnungen und reagieren Sie auf diese. Erwägen Sie die Implementierung fortschrittlicher Endpointsicherheitslösungen, wie z. B. EDR, die einen Zero-Trust-Schutzmodellansatz mit mehreren Verteidigungsebenen umfassen.

10

Sensibilisieren Sie die Benutzer für die Risiken von Phishing und klären Sie sie über die Gefahren von Social Engineering als Teil der besten Cybersicherheitspraktiken auf.



WatchGuard

Ransomware-Angriffe nehmen zu und sind ausgeklügelter als je zuvor. Für Cyberkriminelle stellen sie ein nachhaltiges und lukratives Geschäftsmodell dar. In manchen Fällen ist es einfacher und günstiger, das Lösegeld zu zahlen, als die Daten aus dem Backup wiederherzustellen. Die Zahlung des Lösegelds ist jedoch keine Garantie dafür, dass die Dateien des Opfers wiederhergestellt werden oder dass das System wieder zugänglich ist. Der Endpoint bleibt außerdem weiterhin infiziert.

Herkömmliche Schutzmethoden, die sich auf Malware-Signaturen stützen, reichen gegen Ransomware-Bedrohungen nicht aus. Tatsächlich entwickeln Angreifer ihre Ransomware so, dass sie herkömmliche Schutzebenen umgehen. Diesen Gefährdungen sollte mit einer umfassenden Sicherheitslösung begegnet werden, die auf die neuesten Bedrohungen reagiert.

---

**Jetzt ist es an der Zeit, Ihre Organisation mit WatchGuard Endpoint Security vor diesen Bedrohungen zu schützen – bevor der nächste Ransomware-Angriff Sie trifft.**

# WatchGuard-Portfolio

### Netzwerksicherheit

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

### Secure Wi-Fi

Die sicheren WLAN-Lösungen von WatchGuard sind eine richtungsweisende Neuerung für den Markt von heute: Sie schaffen eine sichere, geschützte WLAN-Umgebung, eliminieren den Verwaltungsaufwand und ermöglichen beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

### Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können Sie die passwortbasierende Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones“ als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen.

### Endpoint-Sicherheit

WatchGuard Endpoint Security ist ein cloudnatives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung WatchGuard EPDR verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

### Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von mehr als 250.000 Kunden. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB www.watchguard.com