# In 5 Schritten zur Cyber-Widerstandsfähigkeit für Endpunkte, die jede Geschäftsführung überzeugt

Malwarebytes

# Einleitung

Das Fundament jeder Organisation sind deren Mitarbeiter – sie sind der Motor für Wachstum, der von den Daten betrieben wird, die sie auf ihren Laptops, Tablets und Mobiltelefonen erstellen und speichern und auf die sie über Datenzentren und Cloudserver zugreifen.

Es sollte CISOs nicht überraschen, dass **60 Prozent aller Unternehmensdaten auf Mitarbeiterendpunkten gespeichert sind.**[1] Und Internetkriminelle nehmen verstärkt die wertvollen Daten auf diesen Unternehmensendpunkten ins Visier. Denn sie wissen, dass diese ihnen höhere Erträge bringen können als Angriffe auf Privatpersonen. So verzeichneten Unternehmen **einen Anstieg von Cyberangriffen von 235 Prozent.** Noch besorgniserregender ist der Umstand, dass es 2018 einen mehr als sechsfachen Anstieg von Trojaner-Schadsoftware zum Datendiebstahl, wie Emotet und TrickBot, sowie einen fünffachen Anstieg von Ransomware, wie Troldesh, gab.[2]

Die Aufgabe jedes CISO ist der Schutz der Organisation und die Minimierung der Risiken für den Geschäftsbetrieb im Fall eines Angriffs. Ein einzelner erfolgreicher Angriff auf einen Endpunkt kann die Mitarbeiterproduktivität unterbrechen und den Geschäftsbetrieb zu einem abrupten Stillstand bringen. In einer Zeit, in der sich die CISOs nicht mehr darauf vorbereiten, *falls* es eine Sicherheitsverletzung gibt, sondern *wenn* ein erfolgreicher Angriff stattfindet, ist es für die Organisationen wichtiger denn je, proaktive Maßnahmen für die Cyber-Widerstandsfähigkeit von Endpunkten zu ergreifen.

[1] Helpnetsecurity. Is GDPR-regulated data lurking in unexpected pockets of your organization? Februar 2018. [2] Malwarebytes. Cybercrime Tactics and Techniques Research Report. April 2019.

Malwarebytes

**200 % mehr**

**Cyberangriffe auf Unternehmen im Jahr 2019 als im Jahr 2018**

Durch die Cyber-Widerstandsfähigkeit von Endpunkten werden die Auswirkungen eines Cyberangriffs minimiert und die Mitarbeiterendpunkte sowie Betriebssysteme wiederhergestellt, um die Geschäftskontinuität zu gewährleisten.
**CISOs müssen mehr als nur Schutzmaßnahmen ergreifen. Vielmehr müssen sie eine Cyber-Widerstandsfähigkeit von Endpunkten durch Umsetzung der folgenden fünf Punkte sicherstellen:**

1. **Vorbereitung**
2. **Schutz**
3. **Isolierung**
4. **Bereinigung**
5. **Untersuchung**

# 1 Vorbereitung

Wenn es um die Cyber-Widerstandsfähigkeit von Endpunkten geht, gilt das alte Sprichwort „Sei gefasst auf das Schlimmste und erhoffe das Beste“. Mit einer guten Vorbereitung wird dafür gesorgt, dass die Incident-Response-Methoden Ihrer Organisation kompromisslos angewendet werden. Mit der Durchführung von Lückenanalysen wird beispielsweise sichergestellt, dass ein Unternehmen die Auswirkungen von Vorfällen eindämmen kann. Dies geschieht, indem Cloud- und On-Premise-Netzwerke, Endpunktsysteme und Anwendungen so schnell wie möglich wieder in einen fehlerfreien Zustand zurückversetzt werden.

**Es ist ausgesprochen wichtig, dass gut vorbereitete und flexible Mitarbeiter bei einem Angriff auf Ihre Organisation schnell und wirksam reagieren können.**

## ENTSCHEIDENDE RAHMENBEDINGUNGEN

CISOs sollten die Vorbereitung als Ausgangspunkt für die Erarbeitung eines Plans zur Cyber-Widerstandsfähigkeit betrachten, womit die Bereitschaft von Menschen, Prozessen und Technologien bewertet wird. Im Rahmen der Vorbereitung müssen Sie Ihre kritischen Assets identifizieren und sicherstellen, dass Ihr Incident-Response-Team (IR-Team) weiß, **welche Prozesse, Endpunkte und Systeme von entscheidender Bedeutung sind, damit das Unternehmen im Fall eines Angriffs seinen Betrieb fortsetzen kann.**

Zwar trägt das IR-Team die Hauptverantwortung für die Vorbereitung, insgesamt sollten diese Aufgaben jedoch vom gesamten Unternehmen unterstützt werden. Holen Sie bei der Planung wichtige Personen aus verschiedenen Abteilungen ins Boot. Hierzu gehören Personal, Finanzen, Marketing, Kundendienst, IT und Sicherheit. Mit ihnen zusammen müssen Vorgehensweisen für Kommunikationseskalationswege erarbeitet werden. Organisationen unterliegen einem dauernden Entwicklungs- und Änderungsprozess. Deshalb ist es auch wichtig, regelmäßig Red-Team-Übungen durchzuführen, um den Bereitschaftsgrad Ihres Unternehmens zu testen und zu bewerten.

## EMPFEHLUNGEN

**Für die Sicherheit der Endpunkte sind folgende Maßnahmen und Informationen erforderlich:**

- Investieren Sie in eine Plattform zum Schutz von Endpunkten, die sich problemlos mit der bestehenden Infrastruktur für das IT-, Sicherheits-, Schwachstellen- und Bedrohungsmanagement integrieren lässt.
- Erstellen Sie eine Asset-Map, mit der die kritischsten Daten mit höchster Priorität identifiziert werden, die auf Endpunkten, im Netzwerk und in der Cloud gespeichert sind.
- Erarbeiten Sie einen Incident-Response-Plan, Richtlinien und Verfahrensweisen, mit denen die Beseitigung der Schadsoftware von Endpunkten auf der Grundlage der Unternehmenskritikalität priorisiert wird.
- Erfassen und verteilen Sie die Kontaktinformationen wichtiger Mitarbeiter sowie der Mitarbeiter mit Bereitschaftsdienst.
- Führen Sie mindestens einmal pro Jahr Red-Team-Incident-Response-Übungen bis hin zur vollständigen Beseitigung der Schadsoftware von Endpunkten durch.

# 2 Schutz

Internetkriminelle setzen bei einem erfolgreichen Angriff mehrere Vektoren ein. Am wirksamsten lässt sich den vielfältigen Angriffsmethoden mit einer Diversifizierung der Schutzmaßnahmen entgegenwirken. Ein engmaschiges Netz aus kompatiblen und signaturlosen Technologien verhindert, dass bekannte und unbekannte Schadsoftware ausgeführt und am Endpunkt eingeschleust wird. Und wenn wir in den letzten zwei Jahrzehnten eines gelernt haben, dann, dass die Angreifer sich immer gern noch ausgeklügeltere Methoden einfallen lassen.

**Die beste Verteidigung gegen die Bedrohungen von heute und morgen bietet ein Endpunktschutz, bei dem zum Durchbrechen der Angriffskette mehrere Techniken zum Einsatz kommen.**

## ENTSCHEIDENDE RAHMENBEDINGUNGEN

Mitarbeiter arbeiten auf ganz unterschiedliche Arten mit ihren Endpunkten. Bedrohungsakteure versuchen, überall einen Einstieg zu finden. CISOs müssen die Mechanismen zur Absicherung der Endpunkte also ganzheitlich betrachten, um einen lückenlosen Schutz sicherzustellen. **Durch den Internet-Schutz wird verhindert, dass Ihre Mitarbeiter auf bösartige Websites, Werbenetzwerke und IPs zugreifen.** Dies schützt insbesondere gegen Malvertising, MalSpam, Phishing, Botnets, Adware, PUPs und Schadsoftwareserver.

**Der Schutz der Endpunkte muss auch Fähigkeiten zur Anwendungshärtung enthalten.** Dabei werden Techniken eingesetzt, die verhindern, dass die Endpunkte aufgrund von Softwareschwachstellen kompromittiert werden. Sobald eine Anwendung geschützt ist, kann sie nicht über eine ihrer aktuellen oder zukünftigen Zero-Day-Schwachstellen ausgenutzt werden.

**Beim Schutz der Endpunkte spielen auch Bedrohungsdaten eine entscheidende Rolle.** Die Schutzschichten sollten von Bedrohungs-Feeds auf der Grundlage von Endpunkt-Beseitigungstelemetrie, Honeypots und menschlicher Intelligenz betrieben werden. Bedrohungsdaten, die in hohem Maß von aktiven Endpunkt-Incident-Responses vertreten werden, erzeugen eine informierte Telemetrie von Daten über neueste Schadsoftware und andere Bedrohungen.

**Entscheidend ist, dass für den Schutz Ihrer Endpunkte gleichzeitig mehrere Techniken zum Einsatz kommen. Dadurch wird nämlich verhindert, dass Schadsoftware erfolgreich am Endpunkt eingeschleust werden kann.** Dies sollte eine Mischung aus statischen und dynamischen Methoden umfassen, wie regelbasierte Erkennung und Analysen auf der Grundlage von Verhalten, künstlicher Intelligenz oder maschinellem Lernen.

# EMPFEHLUNGEN

## Für die Sicherheit der Endpunkte sind folgende Maßnahmen und Informationen erforderlich:

- Internet-Schutz, um zu verhindern, dass Benutzer auf bösartige Websites zugreifen können
- Anwendungshärtung, um das Potenzial für Reverse Engineering oder Manipulation von Apps, die am Endpunkt installiert sind, zu verringern
- Entschärfung von Exploits, indem Versuche, Schwachstellen auszunutzen und Code aus der Ferne am Endpunkt auszuführen, blockiert werden
- Verhaltensüberwachung und Analyse von Anwendungen, um sicherzustellen, dass sie nicht zum Infizieren des Endpunkts missbraucht werden
- Maschinelles Lernen zur Erkennung von Anomalien, womit Viren und Schadsoftware auf der Grundlage von Abweichungen gegenüber bekannten und unbeschädigten Dateien identifiziert werden
- Payload-Analyse, die heuristische und auf Verhaltensanalysen basierende Regeln anwendet, um ganze Familien bekannter und relevanter Schadsoftware zu identifizieren
- Integration der Bedrohungsdatentelemetrie von Endpunkten mit Systemen für das IT-, Sicherheits-, Schwachstellen- und Bedrohungsmanagement, um eine schnelle Response auf Angriffe zu ermöglichen

# 3 Isolierung

Ein erfolgreicher Angriff geschieht schnell. Automatisierte Schadsoftware kann innerhalb weniger Sekunden nach der Ausführung verheerenden Schaden anrichten, indem sie sich lateral vom „Patienten Null“ bewegt, um andere Endpunkte in Ihrem Netzwerksegment zu infizieren. Deshalb sind Isolierungsfähigkeiten für eine wirksame Cyber-Widerstandsfähigkeit von Endpunkten von entscheidender Bedeutung. Traditionelle Sicherheitskontrollen mit einem festen Perimeter, wie Firewalls und Systeme zur Erkennung einer Eindringung, können zwar verhindern, dass Angriffe in das Netzwerk gelangen. Gegen die laterale Bewegung einer Infektion sind sie allerdings machtlos.

**Durch das Eindämmen eines Angriffs am Endpunkt wird die weitere Verbreitung gestoppt. Außerdem verschafft dies dem IR-Team die dringend notwendige Gelegenheit sicherzustellen, dass seine Maßnahmen in den wichtigsten Bereichen angewendet werden, um für eine wirksame Response zu sorgen.**

# 3 Isolierung



## ENTSCHEIDENDE RAHMENBEDINGUNGEN

Isolationsbasierte Fähigkeiten schaffen einen Luftspalt zwischen dem kompromittierten Endpunkt und den anderen Systemen in Ihrer Organisation. **Um eine zuverlässige Cyber-Widerstandsfähigkeit von Endpunkten zu erzielen, sind die Mittel erforderlich, mit denen die Infektion durch Netzwerk-, Geräte- und Prozessisolation eingedämmt werden kann.** Diese Eindämmungsmechanismen verhindern darüber hinaus eine Rückmeldung der Schadsoftware zum Ausgangspunkt für eine Command-and-Control-Kommunikation, damit sie keinen weiteren Schaden anrichten kann.

Automatisierung ist in diesem Kontext von wesentlicher Bedeutung. Ein entscheidender Faktor bei der Verbesserung der Incident-Response-Prozesse ist die Verkürzung der mittleren Zeitdauer bis zur Response (MTTR) oder der Verweildauer. Methoden zur automatisierten Isolierung können in diesem Bereich einen wichtigen Beitrag leisten. Außerdem **sind Ransomware-Infektionen zwischen 2018 und 2019[3] um 195 Prozent angestiegen. Organisationen müssen also die Wiederherstellung nach Ransomware-Angriffen als Anforderung für die Endpunktisolierung aufnehmen.** Diese Fähigkeit sollte Just-in-Time-Endpunktsicherungen umfassen, die es Ihnen ermöglichen, die Uhr zurückzudrehen und die Auswirkungen eines Ransomware-Angriffs zunichte zu machen.

[3] Ebenda

# 3 Isolierung



## EMPFEHLUNGEN

**Die nachstehende Liste enthält Werkzeuge und Prozesse für das Isolieren von Endpunkten. Wir empfehlen Investitionen in folgenden Bereichen:**

- Netzwerkisolierung, die alle vom Endpunkt ausgehenden Prozesse daran hindert zu kommunizieren
- Prozessisolierung, die neue Prozesse daran hindert, am Endpunkt zu starten
- Geräteisolierung, die eine weitere Interaktion verhindert, um den Schaden zu begrenzen
- Ransomware Rollback, womit der frühere Zustand des Geräts wiederhergestellt wird, auch bei einem Angriff an einem langen Wochenende

# 4 Bereinigung

Organisationen verlassen sich zur Bereinigung von mit Schadsoftware infizierten Endpunkten häufig auf Reimaging – eine teure Methode, die laut einiger Aussagen mehr als 1000 USD pro Endpunkt kostet. Einige IR-Teams verwenden Werkzeuge zur Entfernung von Schadsoftware, um Endpunkte nacheinander manuell zu reparieren. Bei einem schweren Angriff bieten zeitaufwändige Bereinigungsmethoden keine akzeptable oder kurze Response-Zeit. So **behaupten 21 Prozent aller Sicherheitsexperten, dass ihr größtes Hindernis für eine wirksame Incident Response darin bestehe, dass die Erkennung und Behebung eines Vorfalls zu lange dauere.**[4]

**Um eine optimale Cyber-Widerstandsfähigkeit der Endpunkte zu erreichen, müssen Sie es Ihrem IR-Team ermöglichen, durch eine Orchestrierung über die Management-Workflows der IT-Systeme hinweg aktiv reagieren zu können, um Endpunkte skaliert zu reparieren und die MTTR Ihrer Organisation beträchtlich zu verringern.**

[4] SANS Institute. 2018 SANS Incident Response Survey. 2019.

# 4 Bereinigung



## ENTSCHEIDENDE RAHMENBEDINGUNGEN

**Technologien, die eine gründliche und automatisierte Bereinigung bieten, stellen den vertrauenswürdigen Zustand Ihrer Endpunkte vor der Infektion wieder her.** Die meisten Lösungen beseitigen nur aktive Schadsoftwarekomponenten, anstatt für eine komplette Beseitigung zu sorgen.

Um eine aktuelle Cyber-Widerstandsfähigkeit Ihrer Endpunkte zu erlangen, sollten die Fähigkeiten zur Endpunktbereinigung eine Erkennung und Entfernung dynamischer und verwandter Artefakte umfassen. Bei der Bereinigung muss eine zugehörige Sequenzierung angewendet werden, um sicherzustellen, dass Mechanismen, durch die Schadsoftware auf dem Endpunkt verbleibt, dauerhaft entfernt werden. **Fortschrittliche Bereinigungsmethoden ermöglichen Ihrer Organisation eine nützliche Schadsoftware-Identifikation und vollständige Entfernung.**

# EMPFEHLUNGEN

**Organisationen sollten zur Optimierung der Endpunktbereinigung die folgenden Mechanismen und Prozesse verwenden:**

## Aktive Reaktionsfähigkeiten

- Geplantes Scannen von Endpunkten und Scannen nach Bedarf
- Nicht verbleibende, entfernbare Endpunktbereinigungsagenten
- Anwender und Richtlinien mit detaillierten Bereinigungsaufgaben und der Fähigkeit, den Endpunkt automatisch wiederherzustellen
- Sequenzierungen, die Bedrohungsartefakte, die zur primären Payload gehören, identifizieren und gründlich entfernen

## Fähigkeiten zur Orchestrierung von Unternehmensendpunkten

- Integration mit vorhandenen Werkzeugen zur Sicherheitsorchestrierung, die Sichtbarkeit bieten, und die Möglichkeit zum Koordinieren, Melden und Ausführen der Bereinigungsarbeiten
- Cloudbasiertes Management von Endpunkten mit Angriffsmuster- und -behebungs-Maps für das koordinierte Verfolgen des Fortschritts von Red Teams
- Gruppenbasierte Richtlinien und Bereitstellungswerkzeuge zum Implementieren von Endpunktbefehlen und Versenden von Systemupdates

# 5 Untersuchung

Ausgeklügelte Schadsoftware bleibt lange nach der erstmaligen Erkennung im System. Ruhender Code bleibt auf infizierten Geräten verborgen und wartet geduldig auf den richtigen Moment zum Zuschlagen. Untersuchungen dauerhafter Bedrohungen wurden häufig als Luxus betrachtet, den sich nur die wirklich großen Unternehmen mit Red Teams, komplexen analysegetriebenen Technologien und ausgereiften SOC-Operationen leisten konnten. Kostengünstige Marktplätze im Darknet ermöglichen es den Internetkriminellen mittlerweile jedoch, Organisationen jeder Größenordnung ins Visier zu nehmen. Deshalb müssen kleine wie große Unternehmen Zugang zu Werkzeugen haben, die es ihnen ermöglichen, kostengünstig Untersuchungen durchzuführen, die das Netzwerk nach einem Angriff wiederherstellen, und proaktiv Untersuchungen anzustellen, um einen nicht infizierten Zustand aufrechtzuerhalten, statt darauf zu warten, bis eine Payload aktiviert wird.

**Bei der Durchführung von Untersuchungen sollte davon ausgegangen werden, dass Bedrohungen bestehen. Dadurch werden die Cyber-Widerstandsfähigkeit von Endpunkten und der Sicherheitszustand allgemein deutlich verbessert.**

## ENTSCHEIDENDE RAHMENBEDINGUNGEN

Um Untersuchungen zum Bestandteil einer Widerstandsstrategie für Endpunkte zu machen, müssen Organisationen Datensätze problemlos per Querverweis miteinander in Beziehung setzen können, um einen Kontext zu erhalten, und Beziehungen mit anderen Einheiten oder historischen Aktivitäten identifizieren können. Untersuchungen sind für die Cyber-Widerstandsfähigkeit von entscheidender Bedeutung und müssen eine agile Datenexploration mit visuellen Daten-Maps unterstützen, die es Ihren IR-Teams ermöglichen, betroffene Endpunkte, Daten, Benutzer sowie andere Details zum Bedrohungsakteur zu identifizieren.

**Ihre Endpunkt-Sicherheitslösung sollte es Ihrem Incident-Response-Team ermöglichen, durch geplante Scans proaktiv nach kürzlich erkannten Bedrohungsindikatoren (IOCs) zu suchen. Im Durchschnitt verbringen Internetkriminelle 191 Tage im Netzwerk, bevor sie erkannt werden.**[5] Mit Untersuchungsmechanismen zum Auffinden von Bedrohungen in Endpunkten wird sichergestellt, dass Sie diese verborgenen Bedrohungen finden.

[5] Ponemon. 2018 Cost of Data Breach Study. Juli 2018.

# 5 Untersuchung



## EMPFEHLUNGEN

**Ihre Methoden zur Endpunktuntersuchung sollten die folgenden Werkzeuge und Prozesse umfassen:**

- Geplantes Scannen von Endpunkten und Scannen bei Bedarf zum Auffinden individueller IOC-Bedrohungen
- Vom Benutzer initiierte Bereinigungs-Scans, die durch Integration mit Ihren vorhandenen Werkzeugen für das Management von IT-Systemen aktiviert werden
- Kontinuierliche Überwachung auf verdächtige Dateien und Prozessereignisse, Netzwerkverbindungen und Registry-Aktivitäten
- Asset-Management, bei dem Endpunktdaten (z. B. installierte Software, Updates und Startprogramme) erfasst und angezeigt werden
- Visuelle Grafiken zur Untersuchung von Prozessen, die von einer Bedrohung hervorgebracht wurden, und wohin diese sich lateral bewegt hat

# Schlussfolgerung

Auf eines können Sie sich verlassen: Internetkriminelle werden Ihre Techniken immer weiter ausbauen und ausfeilen. Unternehmen aller Größen müssen sich auf einen erfolgreichen Angriff einstellen. In der heutigen Welt sich auflösender Perimeter stellt der Endpunkt nun die erste Verteidigungslinie gegen Sicherheitsverletzungen dar. Für die CISOs bedeutet dies, dass die Cyber-Widerstandsfähigkeit von Endpunkten nicht länger ein Luxus ist, sondern eine absolute Notwendigkeit.

**Mit einer Strategie zur Erlangung von Cyber-Widerstandsfähigkeit für Endpunkte, die Vorbereitung, Schutz, Isolierung, Bereinigung und Untersuchung umfasst, werden die Auswirkungen eines Cyberangriffs minimiert. Außerdem wird damit sichergestellt, dass Ihr IR-Team schnell reagieren kann, um die Systeme wiederherzustellen und die Geschäftskontinuität aufrechtzuerhalten.**

# Malwarebytes: Wir machen die Cyber-Widerstandsfähigkeit von Endpunkten zur Realität

**Malwarebytes ermöglicht es Unternehmen, Cyber-Widerstandsfähigkeit von Endpunkten zu erlangen und aufrechtzuerhalten – indem Sicherheitsexperten die Werkzeuge zur Verteidigung gegen Angriffe erhalten, die sie für Vorbereitung, Schutz, Isolierung, Bereinigung und Untersuchung brauchen.**

Unsere Lösung basiert auf mehreren Analyseebenen und fortgeschrittenem maschinellen Lernen. Damit wird ein individueller Schutz gegen Angriffe bereitgestellt, der den nächsten Schritt eines Angreifers vorhersagt und die richtigen Schutzmechanismen am Angriffspunkt anwendet. Darüber hinaus stellt Malwarebytes den CISOs einen kostengünstigen Ansatz für die Cyber-Widerstandsfähigkeit von Endpunkten zur Verfügung, die mit führenden Werkzeugen für das IT- und Systemmanagement integriert ist, darunter ServiceNow, Splunk und Phantom. Außerdem werden infizierte Endpunkte mit granularen Isolierungskontrolloptionen eingedämmt, indem Netzwerkkommunikation, neue Prozesse und der vollständige Zugang zu den Endpunkten blockiert werden.

**Nach der Isolierung können Sicherheitsexperten den Vorfall wirksam mit nur einem Klick beheben – dabei werden die Schadsoftware und alle Angriffsspuren beseitigt, die mittels unserer proprietären Linking-Engine-Technologie erkannt wurden.** Mit einem Ransomware-Rollback-Schutz von bis zu 72 Stunden werden verschlüsselte, gelöschte oder modifizierte Dateien wiederhergestellt. So werden der Endpunkt und die wertvollen Daten wieder in einen bekannten, fehlerfreien Zustand zurückversetzt, ohne teures Reimaging einsetzen zu müssen. Zu guter Letzt deckt Malwarebytes auch die letzte Phase der Cyber-Widerstandsfähigkeit ab, und zwar mit einfachen Werkzeugen für Sicherheitsexperten auf jedem Niveau – nicht nur für jene mit einem Doktortitel. Mit diesen Werkzeugen können schnell und mühelos proaktive und kostengünstige Untersuchungen durchgeführt werden.

# Machen Sie den ersten Schritt in Richtung Cyber-Widerstandsfähigkeit von Endpunkten

Wenn Sie nähere Informationen darüber wünschen, wie Sie Cyber-Widerstandsfähigkeit von Endpunkten mit Malwarebytes erlangen können, besuchen Sie:

**malwarebytes.com/business/endpointprotectionandresponse/**