# Schutz vor moderner Malware



cirosec

# Schutz vor moderner Malware

Die Zeiten, in denen man sich mit klassischen signaturbasierten Virenscannern erfolgreich vor Malware schützen konnte, sind vorbei. Nicht nur die Hersteller fortschrittlicher Malware-Erkennungswerkzeuge weisen darauf hin: Auch unabhängige Sicherheitsberater und sogar Hersteller herkömmlicher Antiviruslösungen bestätigen dies.

Die Ursache dafür ist einerseits Malware, die sich so schnell ändert, dass die Virenscanner in Unternehmen auch bei mehrmals täglicher Aktualisierung nie aktuell genug sind. Andererseits wird häufig professionelle und individuelle Malware im Rahmen von gezielten Angriffen beziehungsweise bei APTs eingesetzt. Für sie gibt es meist noch keine Signaturen und sie umgeht sogar aktiv Sicherheitsprodukte oder deaktiviert diese.

Als Lösungsmöglichkeit bietet der Markt heute viele verschiedene technische Ansätze im Bereich Erkennung und Reaktion, doch auch neue Präventionsmechanismen.

Um erkennen zu können, wie gut Ihr Unternehmen vor aktueller Malware geschützt ist und mit welchen Maßnahmen beziehungsweise Techniken dieser Schutz am sinnvollsten auf das von Ihnen benötigte Niveau angehoben werden kann, bieten wir Ihnen die Erstellung eines Malware-Schutzkonzepts an.

# UNSER ANGEBOT

## Workshop

In einem ersten Workshop erfassen wir zunächst den Ist-Stand in Bezug auf den Malware-Schutz in Ihrem Unternehmen. Dies beinhaltet unter anderem folgende Aspekte:

- Vorhandene Policies und Richtlinien mit Bezug zu Malware-Schutz
- Bisherige Maßnahmen zur Sensibilisierung von Geschäftsleitung, Führungskräften und Mitarbeitern
- Vorhandene Filterungseinstellungen von Mail-Attachments und Webinhalten: Umgang mit ausführbaren Dateien, Flash, Office-Dokumenten und Batch- bzw. Skriptdateien in Mails und Webdownloads
- Kontrolle externer Schnittstellen wie USB und Regelung des Umgangs mit mobilen Datenträgern
- Vorhandene AV-Produkte
- Andere Sicherheitslösungen auf den Endgeräten und Servern
- Relevante Sicherheitstechniken in der Firewall-Umgebung und im internen Netzwerk

Zudem geben wir Ihnen im Rahmen des Workshops einen Überblick über die aktuelle Bedrohungslage sowie über die heute verfügbaren Methoden zur Erkennung und Blockierung von Malware.

Dabei werden neben den klassischen technischen Ansätzen wie Virenscanner, lokale Firewalls, Host-IDS/Host-IPS, Application Whitelisting oder Device Control vor allem die moderneren Ansätze wie Exploit Mitigation, Isolationstechniken (ReCoBS, Sandboxing und Mikrovirtualisierung), Next-Generation-AV mit neuronalen Netzen/KI sowie Verhaltensanalyse auf dem Endgerät vorgestellt.

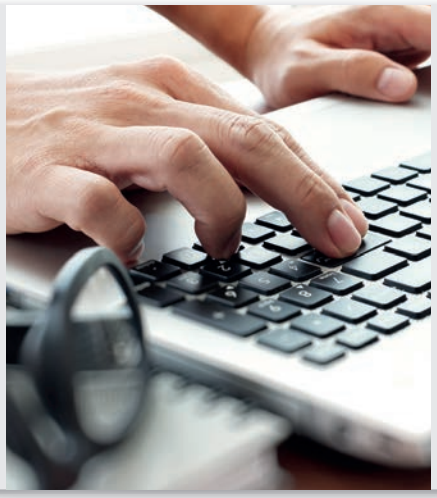
# UNTERSTÜTZUNG DURCH CIROSEC

## Analyse

Anhand der gesammelten Informationen bewerten wir den technischen Ist-Stand und die vorhandenen Regelungen des Malware-Schutzes mithilfe einer Wirksamkeitsmatrix.

Darin bilden wir die vorhandenen Maßnahmen und Techniken hinsichtlich ihrer Wirksamkeit gegen die verschiedenen Angriffsvektoren und Wirkmechanismen moderner Malware ab. Aus dieser Matrixdarstellung geht dann hervor, wo die tatsächlichen Schwachpunkte in der bisherigen Situation liegen und an welchen Stellen eine Verbesserung sinnvoll ist.

Die Matrix bildet auch die Grundlage für die Analyse und die Bewertung möglicher neuer Schutzmaßnahmen. Hier zeigen wir klar auf, wo die potenziellen neuen Lösungen eine Verbesserung der Situation bewirken könnten, wo Redundanzen liegen und wo keine Verbesserung erreicht würde.



## Erstellung eines Konzepts

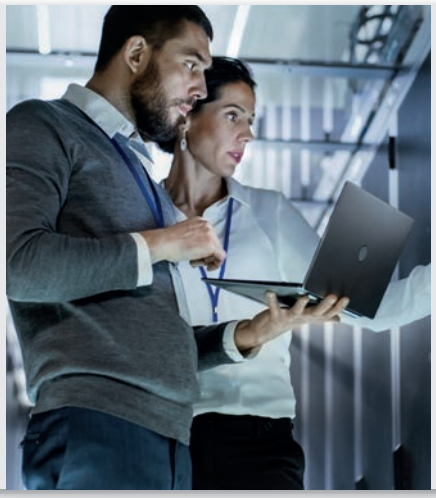
Auf Basis der strukturiert hergeleiteten Wirksamkeitsmatrix erarbeiten wir einen nachvollziehbaren Vorschlag für eine wirtschaftliche und auch wirksame Verbesserung des Schutzes vor Malware. Dabei werden neben den technischen Maßnahmen auch organisatorische Aspekte wie Richtlinien und Sensibilisierung berücksichtigt.

Optional ergänzen wir die zunächst herstellerneutrale technologische Empfehlung um eine Abbildung der empfohlenen Techniken auf Hersteller und Produkte, die diese Techniken implementieren. Diese Konkretisierung kann dann auch um typische Preise und Betriebsaufwände ergänzt werden.

| Wirkmechanismus | [redacted] | | [redacted] | | [redacted] | | [redacted] | |
|---|---|---|---|---|---|---|---|---|
| | Gezielt | Standard | Gezielt | Standard | Gezielt | Standard | Gezielt | Standard |
| [redacted] | | | | | | | | |
| [redacted] | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | | | | | | | | |
| [redacted] | 🔴 | 🟡 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🔴 | 🟡 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🔴 | 🟡 | 🟡 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🟡 | 🟢 | 🟢 | 🟢 | 🔴 | 🔴 | 🔴 | 🔴 |
| [redacted] | | | | | | | | |
| [redacted] | 🔴 | 🔴 | 🔴 | 🔴 | 🔴 | 🔴 | 🟡 | 🟡 |
| [redacted] | 🟢 | 🟢 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🟢 | 🟢 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🔴 | 🔴 | 🔴 | 🔴 | 🔴 | 🔴 | 🟡 | 🟡 |
| [redacted] | 🔴 | 🔴 | 🔴 | 🔴 | 🔴 | 🔴 | 🟡 | 🟡 |
| [redacted] | 🟢 | 🟢 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🟢 | 🟢 | 🔴 | 🔴 | 🟢 | 🟢 | 🟢 | 🟢 |
| [redacted] | 🟢 | 🟢 | 🔴 | 🔴 | 🟡 | 🟡 | 🟢 | 🟢 |
| [redacted] | 🟢 | 🟢 | 🔴 | 🔴 | 🟡 | 🟡 | 🟢 | 🟢 |
| | | | | | | | | |
| **Umgehbarkeit** | 🟡 | | 🟡 | | 🟡 | | 🟢 | |

🔴 kein Schutz/gering
🟡 mittel
🟢 hoch/sehr hoch/schwer

# ÜBER CIROSEC

Unsere erfahrenen IT-Sicherheitsspezialisten prüfen die IT-Landschaft unserer Kunden, beraten sie herstellerneutral und setzen Lösungen kompetent um.

Unser Team zeichnet sich durch seine zahlreichen Experten aus, die als Buchautoren oder Referenten bekannt sind und die Kunden mit technischem und strategischem Sachverstand individuell beraten. Darüber hinaus verfügen wir über langjährige Erfahrung in der Konzeption und Integration von Sicherheitsprodukten in komplexen Umgebungen.

Das Angebotsspektrum umfasst:

- Konzepte, Reviews und Analysen
- Durchführung von Audits und Penetrationstests
- Managementberatung (ISO 27001, Risikomanagement, Erstellung von Prozessen, Policies, Richtlinien)
- Incident Response und Forensik
- Konzeption, Evaluation und Implementierung von Lösungen
- Trainings

# TRAININGS BEI CIROSEC

## Trainings & Seminare

Wir bieten Ihnen Seminare und Trainings, in denen Ihnen unsere erfahrenen Berater den richtigen Umgang mit den modernen Technologien und neuen Sicherheitsthemen vermitteln.

Bei allen Trainings steht der Praxisbezug im Vordergrund. So steht jedem Teilnehmer jeweils ein Notebook mit zahlreichen Werkzeugen zur Verfügung, sodass er das vermittelte Wissen direkt anhand vieler Übungen und Beispielszenarien praktisch umsetzen kann.

Die Trainings und Workshops finden sowohl in Stuttgart, Köln, München und Hamburg als auch bei Kunden direkt vor Ort als Inhouse-Schulungen statt.

Die Vorteile eines Trainings bei cirosec liegen auf der Hand:

- Erfahrung und Wissen aus erster Hand
- Praxisnahe Schulung durch Berater von cirosec
- Lösungsorientierte Vorgehensweise

v01CRS-17-2737-DE170719 · Bildquellen: istockphoto, shutterstock

cirosec GmbH | Heilbronn | Deutschland
T +49 7131 59455-0 | F +49 7131 59455-99 | www.cirosec.de

cirosec