März 2016

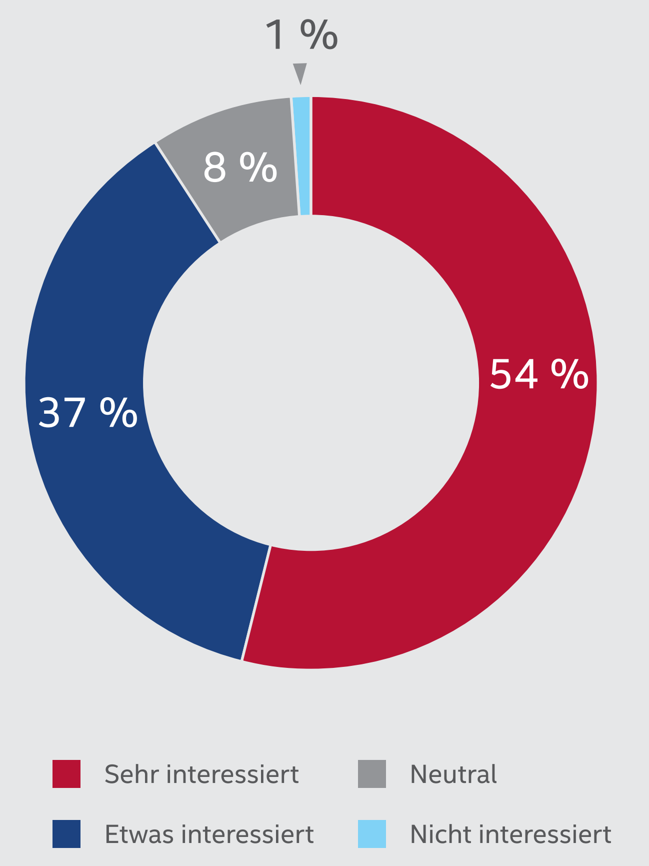
Threat-Report

McAfee Labs

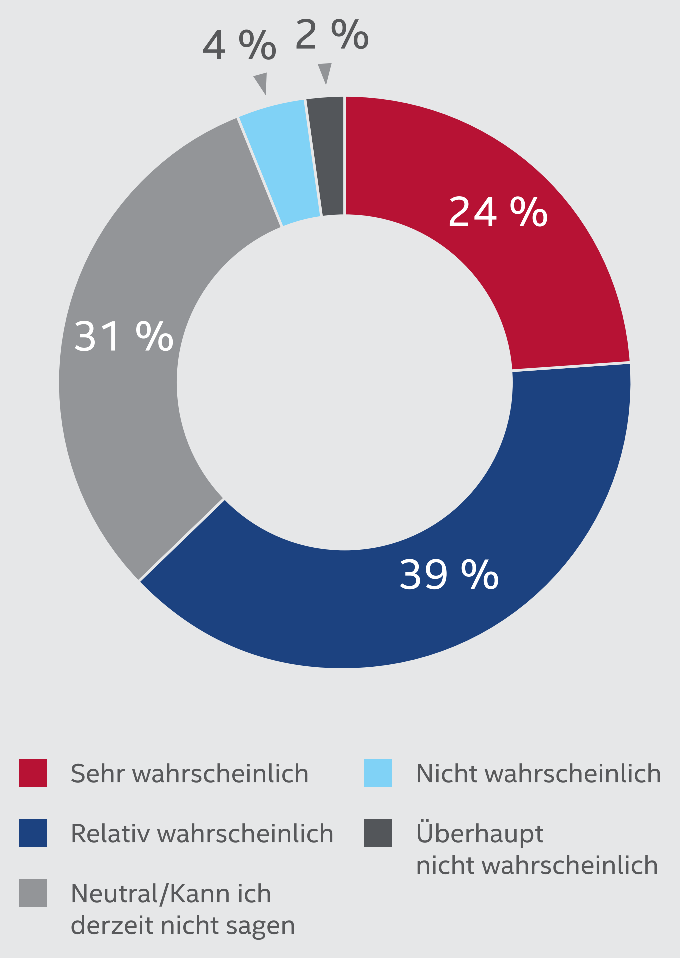
Cyber-Bedrohungsdaten

Intel Security befragte Sicherheitsexperten zum Thema Cyber-Bedrohungsdatenaustausch. 97 % derjenigen, die Cyber-Bedrohungsdaten austauschen, sehen darin einen Mehrwert.

Fast alle Befragten sind an branchenspezifischen Cyber-Bedrohungsdaten interessiert.

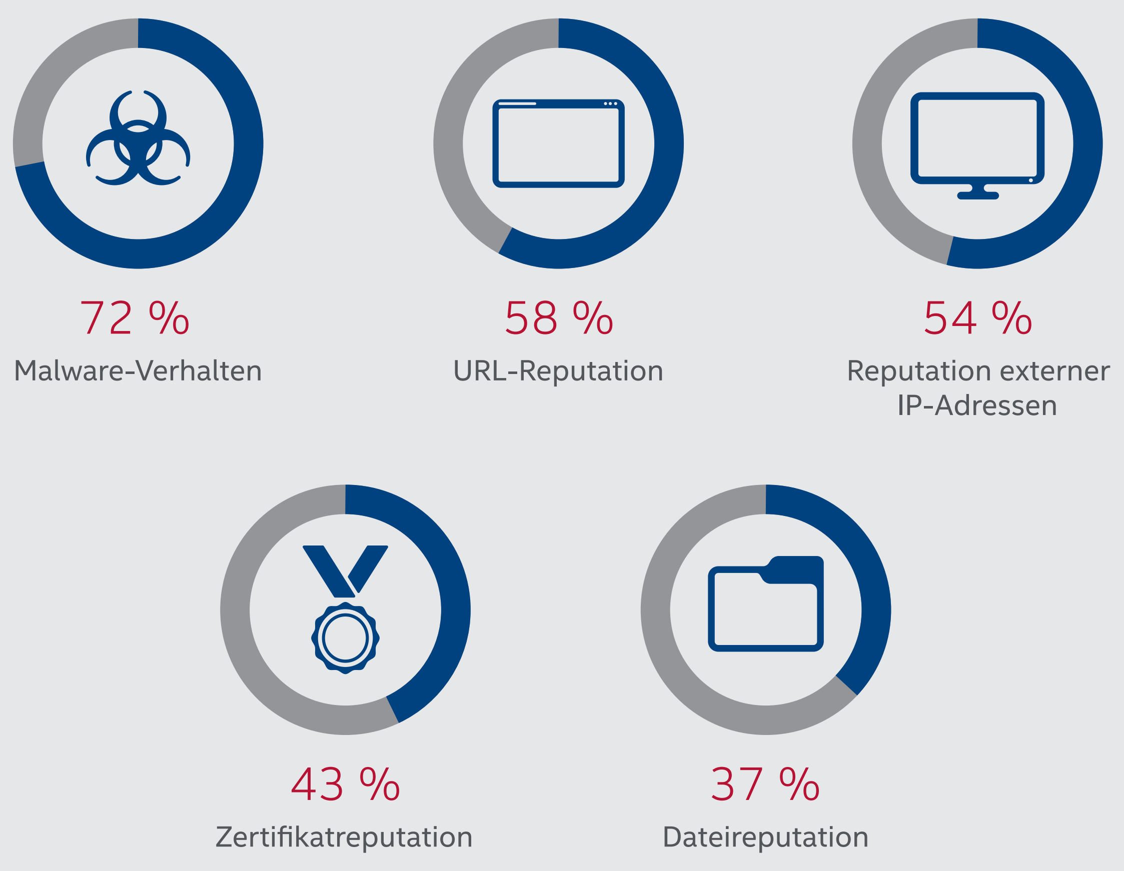


Weitaus weniger sind jedoch zum Austausch von Cyber-Bedrohungsdaten bereit.



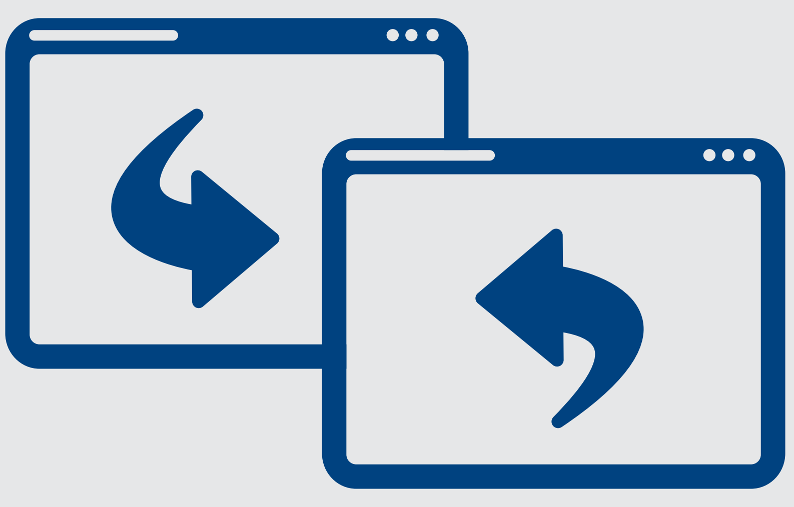
Quelle: Intel Security

Unternehmen sind zum Austausch verschiedener Cyber-Bedrohungsdaten bereit.



Quelle: Intel Security

Warum tauschen Unternehmen keine Cyber-Bedrohungsdaten aus?



Überführung der Angreifer
Einige Informationen sind Teil laufender Untersuchungen.

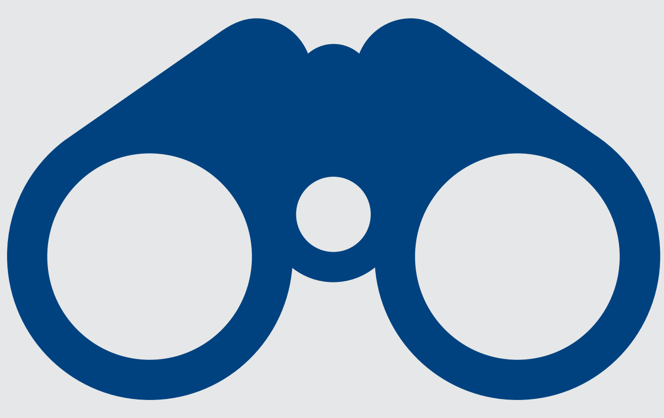
Sorgen über die Rechtmäßigkeit
Die Rechts- und Vertrauensrahmen zum Datenaustausch sind nicht umfassend etabliert.

Richtlinie
Unternehmen verbieten oftmals den Austausch von Daten und selbst von Hash-Werten.

Wie sieht die Zukunft aus?

Bessere Cyber-Bedrohungsdaten
Durch die Verbesserung von Konsistenz, Typ und Qualität wird auch das Verständnis besser.

Standards
Standards wie STIX, TAXII und CybOX werden von Unternehmen und Regierungen weitgehend anerkannt.



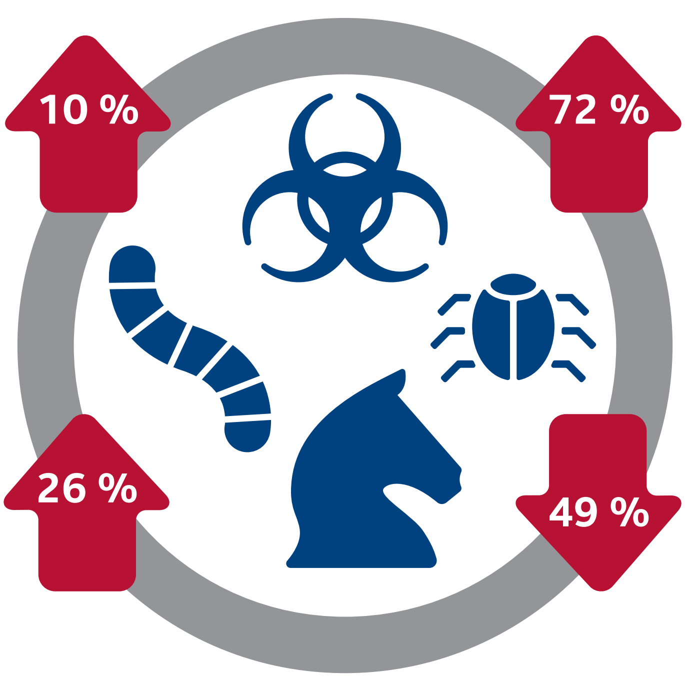
Integrierte Automatisierung
Anbieter von Sicherheitsprodukten entwickeln Technologien, mit denen Cyber-Bedrohungsdaten effizient ausgetauscht und genutzt werden können.

Unternehmen für Cyber-Bedrohungsdatenaustausch
Regierungen unterstützen den Datenaustausch.

Rechtliche Frameworks
Gesetze beschränken die Haftung beim Austausch von Cyber-Bedrohungsdaten.

Statistische Bedrohungsdaten

Pro Minute werden 316 neue Bedrohungen erkannt. Das entspricht mehr als 5 pro Sekunde.



Malware
Nach drei Quartalen des Rückgangs **stieg die Zahl der neuen Malware-Varianten im 4. Quartal um 10 % an**, wobei mit 42 Millionen Varianten der zweithöchste Wert für ein Quartal erkannt wurde.

Ransomware
Im 4. Quartal gab es bei neuen Ransomware-Varianten eine Zunahme um 26 %.

Open-Source-Ransomware-Code und Ransomware-as-a-Service vereinfachen die Angriffe.

Zudem sind Angriffe finanziell profitabel, ohne dass eine große Gefahr für die Angreifer besteht, verhaftet zu werden.

Mobilgeräte-Malware
Im 4. Quartal gab es bei der Zahl neuer Mobilgeräte-Malware-Varianten eine Zunahme um 72 %.

Möglicherweise haben die monatlich von Google herausgegebenen Updates für Android die Angreifer dazu gezwungen, häufiger neue Malware zu entwickeln.

Rootkits
Die Anzahl neuer Varianten fiel im 4. Quartal um 49 %.

Damit setzt sich ein langfristiger, durch 64-Bit-Intel-Prozessoren und 64-Bit-Varianten von Windows verstärkter Abwärtstrend fort.

McAfee Global Threat Intelligence

McAfee GTI erhielt täglich durchschnittlich 47,5 Milliarden Anfragen.

McAfee GTI

157 Millionen
Pro Tag wurden (per E-Mail, Browser-Suchen usw.) **mehr als 157 Millionen Versuche gestartet**, unsere Kunden zur Herstellung einer Verbindung zu riskanten URLs zu verleiten.

353 Millionen
Pro Tag wurden in den Netzwerken unserer Kunden **mehr als 353 Millionen infizierte Dateien entdeckt.**

71 Millionen
Pro Tag versuchten **71 Millionen potenziell unerwünschte Programme**, sich auf den Systemen unserer Kunden zu installieren oder zu starten.

55 Millionen
Pro Tag versuchten unsere Kunden 55 Millionen Mal, sich mit riskanten IP-Adressen zu verbinden, oder solche Adressen versuchten, eine Verbindung mit den Kundennetzwerken herzustellen.

McAfee Labs Threat-Report: März 2016

Den vollständigen Report finden Sie unter www.mcafee.com/March2016ThreatsReport.

McAfee gehört jetzt zu Intel Security.

62290info_qtr-q1-2016_0316