Dezember 2016

Threats-Report

McAfee Labs

Das Sicherheitskontrollzentrum (SOC)

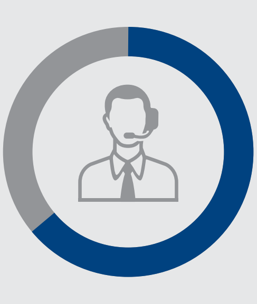
Der aktuelle Stand und Zukunftspläne für das Sicherheitskontrollzentrum

Fast neun von zehn Unternehmen verfügen über ein SOC.

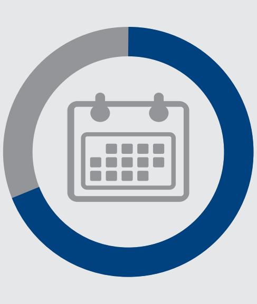
91 %
der großen Unternehmen verfügen über ein SOC.

84 %
der mittleren Unternehmen verfügen über ein SOC.

74 %
der Unternehmen nähern sich dem Ziel proaktiver und optimierter Sicherheitsabläufe, doch 26 % gehen noch reaktiv vor und verfolgen Ad-hoc-Ansätze bei ihren Sicherheitsabläufen, der Bedrohungssuche und der Reaktion auf Zwischenfälle.



64 %
der Unternehmen lassen sich bei ihren Sicherheitsabläufen in gewissem Umfang von Anbietern verwalteter Sicherheits-Services unterstützen.



69 %
verwenden heute eine SIEM-Lösung. 45 % der Unternehmen ohne SIEM beabsichtigen, ein solches System in den nächsten 12 bis 18 Monaten zu implementieren.

93 %
Die meisten Unternehmen sehen sich von der Meldungsflut überwältigt, und 93 % sind nicht in der Lage, alle relevanten Bedrohungen zu untersuchen.

65 %
der Unternehmen mit SOC haben formelle Abläufe für die Bedrohungssuche.

Wachstumsbereiche für die Zukunft – Verbesserung folgender Funktionen:

Reaktion
Reaktion auf bestätigte Angriffe, einschließlich Koordinierung, Eindämmung, Beseitigung und Verhinderung von erneutem Auftreten

Erkennung
Erkennung von Anzeichen für potenzielle Angriffe, einschließlich der Konzentration auf relevante Ereignisse sowie Meldungen, Untersuchung und Priorisierung

Untersuchung
Untersuchung potenzieller Angriffe, einschließlich Bestimmung des vollen Ausmaßes und der Folgen eines Angriffs

Rückblick auf ein Jahr Ransomware

Im Jahr 2016 gab es einen drastischen Anstieg bei der Anzahl der Ransomware-Angriffe. Zudem erlebten wir erhebliche technische Weiterentwicklungen bei Ransomware. Die Sicherheitsbranche schlägt zurück.

Die wichtigsten technischen Weiterentwicklungen bei Ransomware in diesem Jahr:

Festplatten-verschlüsselung
Teilweise und vollständige Festplattenverschlüsselung

Variable Lösegeldbeträge
Forderungen basierend auf dem Zahlungsvermögen des Opfers

Webseiten-verschlüsselung
Verschlüsselung von Webseiten, die von legitimen Anwendungen genutzt werden

Techniken zur Sandbox-Erkennung
Erkennung und Umgehung von Sicherheits-Sandboxes, in denen verdächtiger Code geprüft wird

80 %
Ende des 3. Quartals verzeichneten wir einen Anstieg der neuen Ransomware-Varianten seit Jahresbeginn von 80 Prozent, sodass in diesem Jahr bisher 3,9 Millionen Varianten erfasst wurden.

Exploit-Kits
Raffiniertere Exploit-Kits zur Verbreitung von Ransomware

Ransomware-as-a-Service
Angreifer bezahlen Dienstanbieter für die Nutzung von Infrastruktur und Ransomware

Die Sicherheitsbranche schlägt zurück.

Zusammenarbeit

NO MORE RANSOM!

No More Ransom!
Diese Organisation wurde im Juli gegründet und bietet Informationen zu Schutzmaßnahmen, Unterstützung bei Untersuchungen sowie Entwicklung von Entschlüsselungs-Tools.

Aktionen von Strafverfolgungsbehörden

WildFire
Stilllegung der Ransomware

Shade
Stilllegung der Ransomware

„Trojanisierte" legitime Software

Trojaner infizieren legitimen Code und verbergen sich, um so lange wie möglich unentdeckt zu bleiben und größtmögliche Wirkung zu entfalten.

Vorteile für Trojaner

Anschein der Seriosität
Schaddaten werden hinter bekannten Marken verborgen, was den Anschein der Seriosität verstärkt.

Verhindert Entdeckung
Legitime Software verhindert die Entdeckung bei Sicherheits-Scans und forensischen Analysen.

Beständigkeit ohne zusätzlichen Aufwand
Die Trojanisierung legitimer Anwendungen bietet Beständigkeit ohne zusätzlichen Aufwand.

Möglichkeiten zur Trojanisierung legitimer Anwendungen

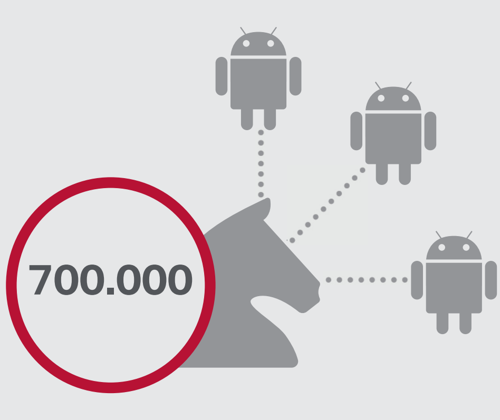
Änderungen
von interpretiertem, dekompiliertem oder Open-Source-Code

Patches
ausführbarer Daten während des Downloads per Man-in-the-Middle-Angriff

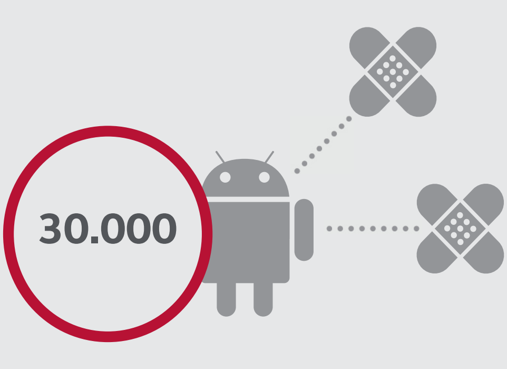
Kombination
sauberer und böswilliger Dateien mithilfe von Binder- oder Joiner-Tools

Änderungen ausführbarer Dateien
mithilfe von Patch-Programmen, die die Nutzbarkeit der Anwendung nicht gefährden

Vergiftung
des Master-Quellcodes, vor allem bei verbreiteten Bibliotheken



700.000
Im 3. Quartal wurden mehr als 700.000 trojanisierte Binärdateien aus drei Android-Malware-Familien gefunden.

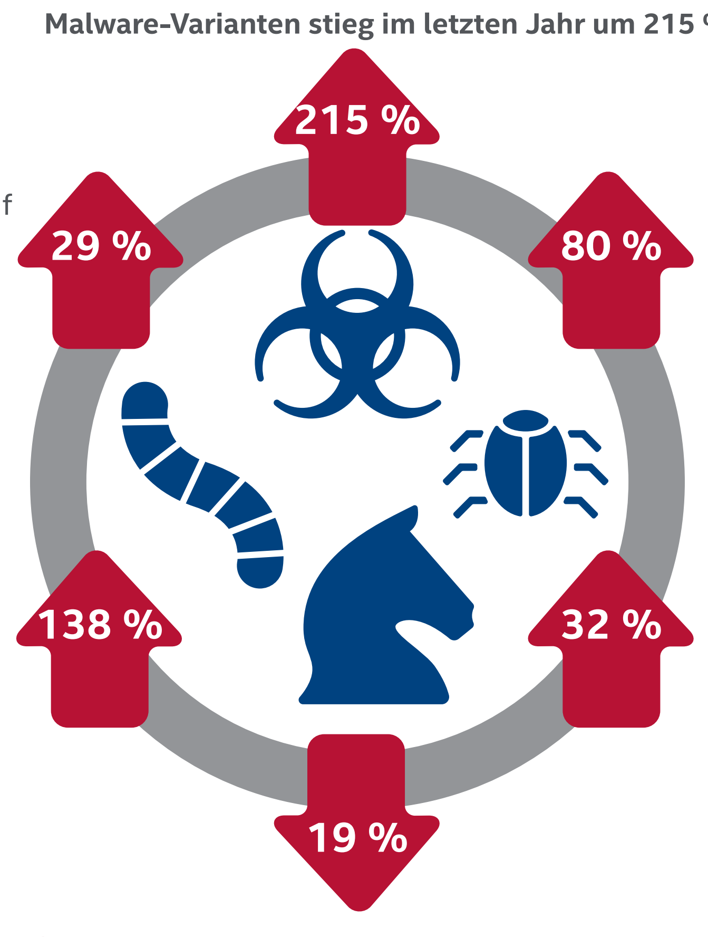


30.000
Im 3. Quartal wurden 30.000 Android-Binärdateien mithilfe von zwei beliebten Backdoor-Patch-Kits trojanisiert.

Statistische Bedrohungsdaten

Pro Minute werden 245 neue Bedrohungen erkannt. Das entspricht mehr als 4 pro Sekunde.

Mac OS-Malware
Obwohl die Zahlen im Vergleich mit Windows-Bedrohungen weiterhin niedrig sind, stieg die Anzahl der neuen Mac OS-Malware-Varianten im 3. Quartal um 65 %. **Die Gesamtzahl der Mac OS-Malware-Varianten stieg im letzten Jahr um 215 %.**



Malware
Die Anzahl neuer Malware-Varianten fiel im 3. Quartal auf 32 Millionen. Das sind 21 % weniger als im 2. Quartal. **Die Gesamtanzahl stieg jedoch im letzten Jahr um 29 % auf 644 Millionen Varianten.**

Ransomware
Die Gesamtanzahl der Ransomware-Varianten stieg im 3. Quartal um 18 % und **im Jahr 2016 bis zum jetzigen Zeitpunkt um 80 %.**

Mobilgeräte-Malware
Die Anzahl neuer Malware-Exemplare für Mobilgeräte – fast 2 Millionen – erreichte im 3. Quartal den höchsten jemals erfassten Wert. **Die Gesamtzahl der Mobilgeräte-Malware-Varianten stieg im letzten Jahr um 138 %.**

Makro-Malware
Die Anzahl der Makro-Malware-Varianten nimmt weiterhin stark zu. **Die Gesamtzahl der Makro-Malware-Varianten stieg im letzten Quartal um 32 %.**

Spam-Botnets
Die Zahl der vom Kelihos-Botnet generierten Spam-E-Mails fiel im 3. Quartal um 97 %, dafür nahm die Aktivität des Necurs-Botnets um 554 % zu. **Insgesamt fiel die Zahl der Spam-E-Mails aus Botnets im 3. Quartal um 19 %.**

McAfee Global Threat Intelligence

McAfee GTI erhielt täglich durchschnittlich 44,1 Milliarden Anfragen.

57 Millionen
Die Zahl der von McAfee GTI erfassten böswilligen URLs **sank von 100 Millionen pro Tag im 2. Quartal auf 57 Millionen pro Tag im 3. Quartal.**

32 Millionen
Die Zahl der von McAfee GTI erfassten potenziell unerwünschten Programme zeigte eine geringfügige Zunahme vom 2. zum 3. Quartal. Im Vergleich zwischen dem 3. Quartal 2015 und dem 3. Quartal 2016 gab es jedoch einen dramatischen Rückgang. **Im 3. Quartal 2016 beobachteten wir 32 Millionen pro Tag – im Vergleich zu 175 Millionen täglich im 3. Quartal 2015.**

150 Millionen
Die Zahl der von McAfee GTI erfassten böswilligen Dateien **stieg von 104 Millionen pro Tag im 2. Quartal auf 150 Millionen pro Tag im 3. Quartal**. Im letzten Jahr verzeichneten wir in diesem Zeitraum einen Rückgang.

27 Millionen
Die Zahl der von McAfee GTI erfassten riskanten IP-Adressen zeigte einen **leichten Rückgang von 29 Millionen pro Tag im 2. Quartal auf 27 Millionen pro Tag im 3. Quartal**. Dies war ein erheblich geringerer Rückgang als der zwischen dem 2. und 3. Quartal des Jahres 2015.

McAfee Labs Threats-Report: Dezember 2016

Den vollständigen Report finden Sie unter www.mcafee.com/December2016ThreatsReport.

1941_1016_info_threats-report-dec-2016