

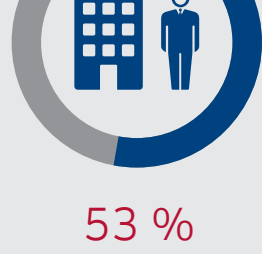


Threat-Report

McAfee Labs

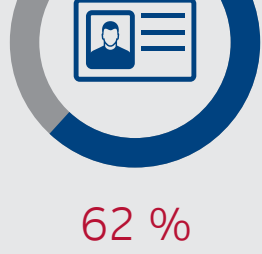
Informationsdiebstahl

Datenverlust: Wer ist wie und warum davon betroffen?



53 %

aller Kompromittierungen werden von Personen außerhalb des angegriffenen Unternehmens entdeckt.



62 %

aller Datenpannen betreffen Kunden- oder Mitarbeiterdaten.



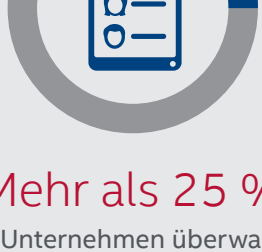
Fast 40 %

aller Datenverluste sind mit dem Gebrauch physischer Medien verbunden.



68 %

aller Vorfälle beinhalten meldepflichtigen Datenverlust.



Mehr als 25 %

aller Unternehmen überwachen nicht den Zugriff auf Mitarbeiter- oder Kundendaten.



Nur 37 %

aller Unternehmen nutzen Endgeräteüberwachung, inkl. Benutzeraktivität und physische Medien.

Krise in der Notaufnahme

Ransomware infiziert Krankenhäuser.

Ransomware-Autoren greifen Krankenhäuser aus folgenden Gründen an:



Veraltete Systeme

Veraltete Krankenhausysteme verfügen über nur unzureichende Sicherheitsvorkehrungen.



Medizinische Geräte

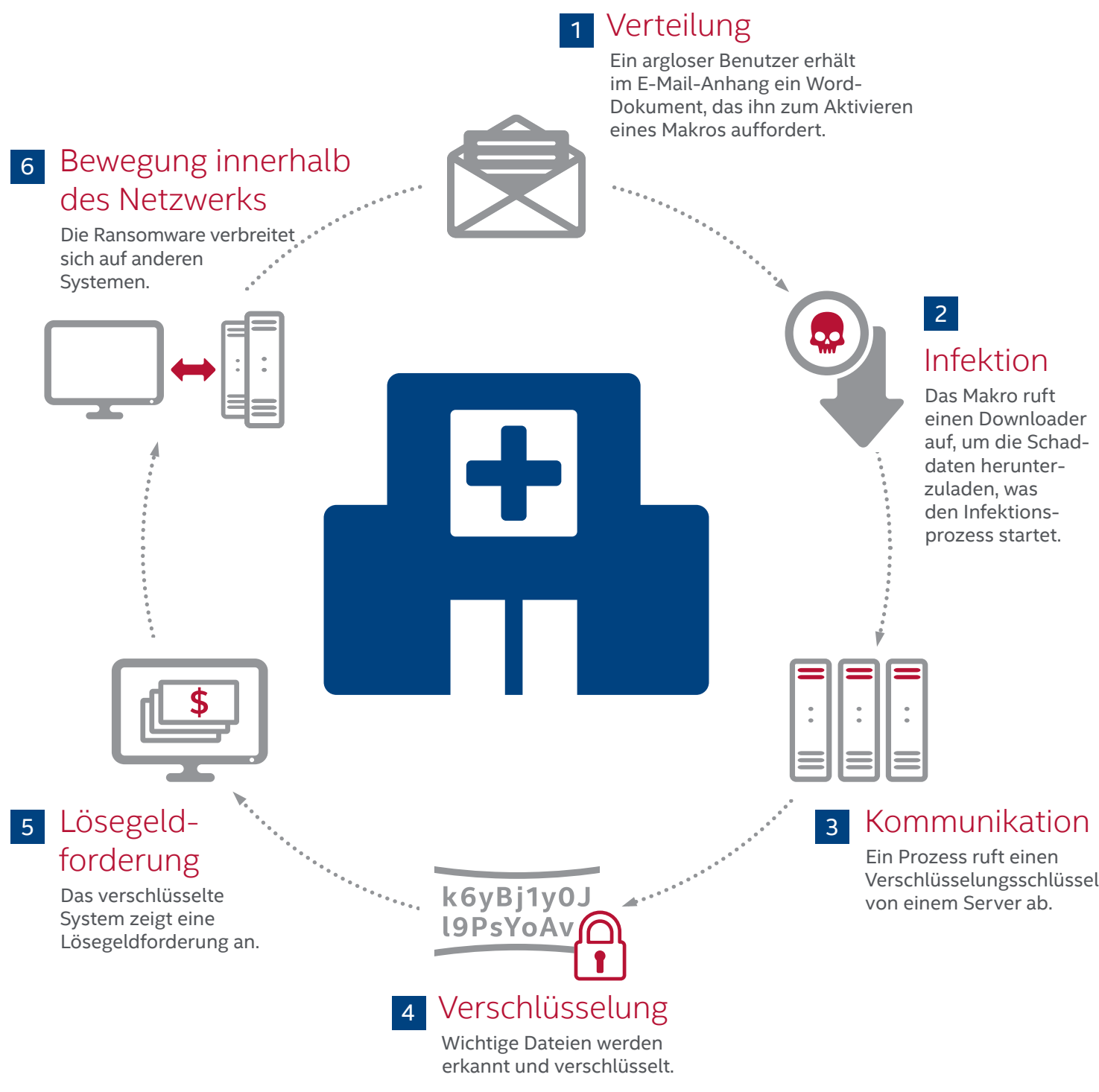
Medizinische Geräte werden kaum oder gar nicht abgesichert.



Patientenbetreuung

Sie benötigen schnellen Zugriff auf Informationen für bestmögliche Patientenbetreuung.

Stufen eines Ransomware-Angriffs auf ein Krankenhaus



19 Krankenhäuser

Mindestens 19 Krankenhäuser wurden im 1. und 2. Quartal mit Ransomware infiziert.



17.000 USD

Ein kalifornisches Krankenhaus zahlte im 1. Quartal 17.000 US-Dollar zur Wiederherstellung seiner Dateien und Systeme – und konnte erst nach fünf Arbeitstagen die Arbeit wieder aufnehmen.



100.000 USD

Intel Security entdeckte, dass im 1. Quartal bei einer ähnlichen Angriffsserie auf Krankenhäuser 100.000 US-Dollar Lösegeld erbeutet wurden.

Analysen

Maschinelles Lernen zur Abwehr von Angriffen.

Beim maschinellen Lernen werden Analysen automatisiert, mit denen Computer über die Zeit dazulernen.



Präskriptive Analysen

„Diese Empfehlung wird gegeben, weil ein bestimmtes Ereignis eintreten wird.“



Deskriptive Analysen

„Was ist geschehen?“



Prädiktive Analysen

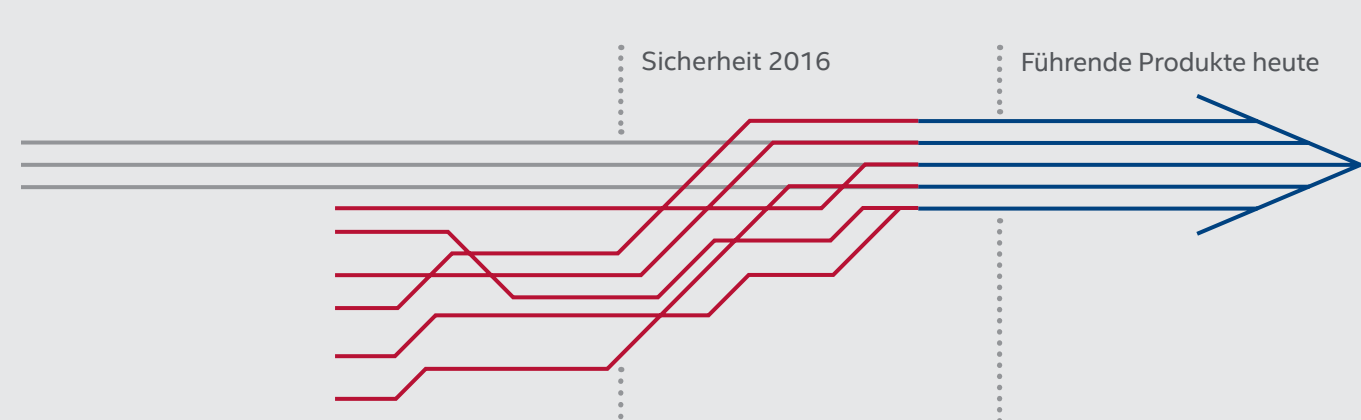
„Was wird geschehen?“



Diagnostizierende Analysen

„Warum ist das geschehen?“

Die Evolution der Analyse



1.0

Analysen 1.0

- Interne Quellen, strukturierte Datensätze
- Deskriptive und diagnostische Analysen
- Reaktiv, aber nützlich

2.0

Analysen 2.0

- Big Data: umfangreich, komplex, unstrukturiert
- Daten aus internen und externen Quellen

3.0

Analysen 3.0

- Nutzt lernfähige Algorithmen mit Big Data, Deep Learning und Cognitive Computing
- Schnelle proaktive Erkennung und Untersuchung

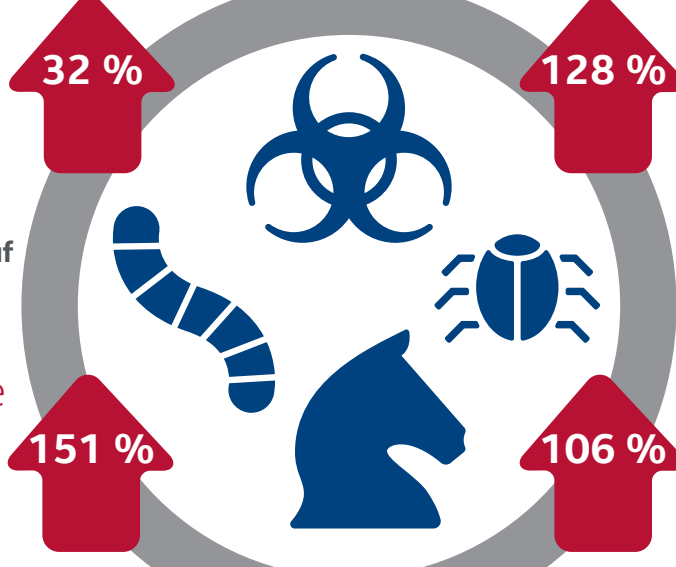
Quelle: Übernommen vom International Institute for Analytics.

Statistische Bedrohungsdaten

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

Malware

Die Anzahl neuer Malware-Exemplare – 41 Millionen – ist im 2. Quartal der zweithäufigste jemals erfasste Wert. Der Malware-Bestand von McAfee Labs wuchs im vergangenen Jahr um 32 % auf über 600 Millionen Varianten.



Ransomware

Die Anzahl neuer Ransomware-Exemplare – über 1,3 Millionen – erreichte im 2. Quartal den höchsten jemals erfassten Wert. Die Gesamtzahl der Ransomware-Varianten stieg im letzten Jahr um 128 %.

Mobilgeräte-Malware

Die Anzahl neuer Malware-Exemplare für Mobilgeräte – über 2 Millionen – erreichte im 2. Quartal den höchsten jemals erfassten Wert. Die Gesamtzahl der Mobilgeräte-Malware-Varianten stieg im letzten Jahr um 151 %.

Makro-Malware

Neue Downloader-Trojaner sind im 2. Quartal für einen Anstieg von 200 % bei neuer Makro-Malware verantwortlich gewesen. Die Gesamtzahl der Makro-Malware-Varianten stieg im letzten Jahr um 106 %.

McAfee Global Threat Intelligence

McAfee GTI erhielt täglich durchschnittlich 48,6 Milliarden Anfragen.



100 Millionen

Die Zahl der von McAfee GTI erfassten böswilligen URLs stieg leicht im Jahresvergleich auf 100 Millionen pro Tag im 2. Quartal.



30 Millionen

Die Zahl der von McAfee GTI erfassten potenziell unerwünschten Programme sank im Jahresvergleich um 83 % auf 30 Millionen pro Tag im 2. Quartal.



104 Millionen

Die Zahl der von McAfee GTI erfassten böswilligen Dateien sank im Jahresvergleich um 77 % auf 104 Millionen pro Tag im 2. Quartal.



29 Millionen

McAfee GTI registrierte den höchsten Anstieg bei riskanten IP-Adressen in den letzten zwei Jahren um 128 % im Quartalsvergleich auf 29 Millionen pro Tag.



McAfee Labs Threat-Report: September 2016

Den vollständigen Report finden Sie unter www.mcafee.com/September2016ThreatsReport.

