Kurzvorstellung

# Keine Chance für Ransomware: Schützen Sie Ihre Daten vor der Geiselnahme

Ransomware ist Malware, die die Daten ihres Opfers mittels asymmetrischer Verschlüsselung als Geiseln nimmt. Asymmetrische (öffentlich-private) Verschlüsselung ist eine Form von Kryptografie, bei der ein Schlüsselpaar zum Ver- und Entschlüsseln einer Datei verwendet wird. Der Angreifer generiert das einmalige öffentlich-private Schlüsselpaar für das Opfer, wobei der private Schüssel für die Entschlüsselung der Dateien auf dem Server des Angreifers abgelegt wird. Der Angreifer verspricht dem Opfer, ihm den privaten Schlüssel nach Zahlung eines Lösegeldes auszuhändigen – ein Versprechen, das in der Vergangenheit nicht immer gehalten wurde. Ohne Zugang zu diesem privaten Schlüssel ist es praktisch unmöglich, die in Geiselhaft genommenen Dateien zu entschlüsseln.

## Was ist Ransomware?

Einen detaillierten technischen Einblick in Ransomware erhalten Sie im ***McAfee Labs Threat-Report vom Mai 2015***. Im *McAfee Labs Threat-Report vom November 2014* sagten wir voraus, dass im Jahr 2015 neun schwerwiegende Bedrohungen auftreten würden. In Bezug auf Ransomware sagt McAfee Labs: „Die Methoden zur Verbreitung, Verschlüsselung und Zielsuche von Ransomware werden sich weiterentwickeln.“ Beinahe sofort kam es zu einem rasanten Anstieg der Verbreitung von Ransomware, und es tauchten neue Familien wie Teslacrypt oder Änderungen an aktuellen Familien wie CTB-Locker, CryptoWall und TorrentLocker auf.

Am Anfang der meisten Ransomware-Kampagnen steht ein Phishing-Angriff. Doch die Angriffe werden immer raffinierter. Viele Kampagnen werden inzwischen akribisch im jeweiligen regionalen Kontext der ausgewählten Opfer entwickelt.

intel Security

Zusätzlich sollen neue Techniken die Ransomware noch mächtiger machen:

- **Virtuelle Währungen:** Durch die Nutzung **virtueller Währungen** als Methode zur Lösegeldzahlung können die Angreifer nicht über das herkömmliche Bankensystem verfolgt werden, dessen Geldfluss überwacht werden kann.
- **Tor-Netzwerk:** Durch die Verwendung des **Tor-Netzwerks** können die Angreifer den Standort ihrer Kontroll-Server mit den privaten Schlüsseln ihrer Opfer leichter verbergen. Dank Tor ist es möglich, die kriminelle Infrastruktur langfristig zu nutzen und sie sogar an andere Angreifer zu vermieten, damit diese Partnerkampagnen durchführen können.
- **Wechsel zu Mobilgeräten:** Im Juni 2014 entdeckten Forscher die erste Ransomware-Familie, die Daten auf Android-Geräten verschlüsselt.[1] Pletor verwendet AES-Verschlüsselung, sperrt die Daten auf der Speicherkarte des Telefons und nutzt Tor, SMS oder HTTP, um sich mit den Angreifern in Verbindung zu setzen.
- **Angriff auf Massenspeichergeräte:** Im August 2014 begann Synolocker, NAS-Speicher und Rack-Stationen von Synology anzugreifen.[2] Die Malware nutzt eine Schwachstelle in ungepatchten Versionen der NAS-Server aus, um per Fernzugriff alle Daten mit RSA 2.048-Bit- oder 256-Bit-Schlüsseln zu verschlüsseln.

## Schutz vor Ransomware

Beachten Sie die folgenden Richtlinien und Verfahrensweisen, um sich und Ihr Unternehmen besser vor Ransomware zu schützen.

- **Führen Sie regelmäßig Benutzerschulungen zur Verbesserung des Sicherheitsbewusstseins durch.** Die meisten Ransomware-Angriffe beginnen mit einer Phishing-E-Mail. Daher ist die Sensibilisierung der Benutzer absolut unverzichtbar. Statistiken zeigen, dass von zehn E-Mails, die von Angreifern gesendet wurden, mindestens eine erfolgreich ist. Öffnen Sie keine E-Mails oder Anhänge von unbekannten oder nicht überprüften Absendern.
- **Halten Sie die Systeme auf dem neuesten Patch-Stand.** Viele von Ransomware missbrauchte Schwachstellen können mit Patches geschlossen werden. Halten Sie Betriebssysteme, Java, Adobe Reader, Flash und Anwendungen mit Patches auf dem neuesten Stand. Sie sollten ein Verfahren zur Patch-Installation ausarbeiten und überprüfen, ob die Patches ordnungsgemäß installiert wurden.
- **Seien Sie äußerst vorsichtig, wenn Sie Anhänge öffnen.** Konfigurieren Sie Ihre Virenschutz-Software so, dass E-Mail- und Instant-Messaging-Anhänge automatisch gescannt werden. Sorgen Sie dafür, dass E-Mail-Programme Anhänge nicht automatisch öffnen oder Grafiken automatisch darstellen und dass das Vorschaufenster deaktiviert ist. Öffnen Sie niemals eine E-Mail, die Ihnen unverlangt zugesendet wurde oder einen unerwarteten Anhang enthält – auch dann nicht, wenn die E-Mail von einem bekannten Absender stammt.
- **Fallen Sie nicht auf Phishing-Versuche in Spam-Mails herein.** Klicken Sie nicht auf Links in E-Mails oder Instant Messages.

## So kann Intel Security vor Ransomware schützen

### McAfee Web Gateway

Malvertising, Drive-by-Downloads und böswillige URLs, die in vertrauenswürdige Webseiten eingebettet sind, sind nur einige der Angriffsmethoden, mit denen Ransomware übertragen wird. Der zuverlässige **McAfee Web Gateway** dehnt den Schutz Ihres Unternehmens auf diese Art der Bedrohung aus.

- **McAfee Gateway Anti-Malware Engine:** Die signaturlose Absichtsanalyse filtert in Echtzeit gefährliche Inhalte aus dem Web-Datenverkehr heraus. Emulation und Verhaltensanalyse bieten präventiven Schutz vor Zero-Day-Bedrohungen und gezielten Angriffen. McAfee Gateway Anti-Malware Engine untersucht Dateien und blockiert das Herunterladen durch den Benutzer, falls sich die Dateien als böswillig erweisen.
- **Integration von McAfee Global Threat Intelligence (McAfee GTI):** Der Echtzeit-Datendienst McAfee GTI bietet Datei- und Web-Reputation sowie Web-Kategorisierungsinformationen und schützt so vor den neuesten Bedrohungen, da McAfee Web Gateway alle Verbindungsversuche zu bekannt böswilligen Webseiten sowie zu Webseiten blockiert, die böswillige Werbenetzwerke nutzen.

### McAfee Email Gateway

Eine wichtige Frage für Unternehmen ist, ob eine E-Mail im Posteingang eines Benutzers legitim ist oder ob sich dahinter ein Phishing-Angriff verbirgt, der Ransomware verteilen soll. **McAfee Email Gateway** bietet verschiedene Funktionen, die Schutz vor den immer raffinierteren Phishing-Angriffen bieten.

- **ClickProtect:** Diese Funktion wehrt Bedrohungen durch eingebettete URLs in E-Mails ab, indem die URLs zum Klick-Zeitpunkt gescannt werden. Dabei werden die URL-Reputation überprüft sowie eine proaktive Emulation mithilfe der Gateway Anti-Malware Engine durchgeführt.
- **Integration von McAfee Advanced Threat Defense:** Durch die statische und dynamische Code-Analyse verdächtiger Dateien, die an E-Mails angehängt sind, kann hochentwickelte und verschleierte Malware entdeckt werden, sodass böswillige Dateien den Posteingang gar nicht erst erreichen.
- **Integration von McAfee GTI:** Durch die Kombination von Daten aus dem lokalen Netzwerk mit Reputationsinformationen, die über McAfee GTI bereitgestellt werden, bietet die Lösung den lückenlosesten erhältlichen Schutz vor eingehenden Bedrohungen, Spam und Malware.

### McAfee Advanced Threat Defense

**McAfee Advanced Threat Defense** ist eine mehrschichtige Malware-Erkennungslösung, die mehrere Analysemodule kombiniert. Die Module wenden signatur- und reputationsbasierte Analysen, Echtzeit-Emulation und vollständige statische Code- sowie dynamische Sandbox-Analysen an. McAfee Advanced Threat Defense schützt vor verbreiteter Ransomware wie CTB-Locker oder CryptoWall.

- **Erkennung auf Signaturbasis:** Erkennt Viren, Würmer, Spyware, Bots, Trojaner, Buffer Overflows sowie komplexe Angriffe. Die umfangreiche KnowledgeBase, die derzeit mehr als 150 Millionen Signaturen (inklusive CTB-Locker, CryptoWall und den entsprechenden Varianten) enthält, wird von McAfee Labs gepflegt.
- **Erkennung auf Reputationsbasis:** Über den McAfee GTI-Service werden Informationen zur Datei-Reputation abgerufen, damit auch neue Bedrohungen erkannt werden.
- **Statische Analyse und Emulation in Echtzeit:** Bietet statische Echtzeitanalyse und Emulation zur schnellen Erkennung von Malware und Zero-Day-Bedrohungen, die von Signatur- oder Reputations-basierten Verfahren nicht erkannt werden.

- **Vollständige statische Code-Analyse:** Führt ein Reverse Engineering des Datei-Codes durch, um alle Attribute und Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen. Umfassende Entpackfunktionen öffnen gepackte und komprimierte Dateien jedes Typs, um Malware vollständig zu analysieren und einzustufen, sodass Ihr Unternehmen weiß, welche Gefahren von einer bestimmten Malware ausgehen.
- **Dynamische Sandbox-Analyse:** Hierbei wird Datei-Code in einer virtuellen Ausführungsumgebung ausgeführt und das Verhalten beobachtet. Dabei werden die virtuellen Umgebungen so konfiguriert, dass sie mit Host-Umgebungen Ihres Unternehmens übereinstimmen – unabhängig davon, ob Sie benutzerdefinierte Betriebssystemabbilder von Windows 7 (32- und 64-Bit-Versionen), Windows XP, Windows Server 2003, Windows Server 2008 (64-Bit Version) oder Android benötigen.

**McAfee Threat Intelligence Exchange**

Sie benötigen eine Informationsplattform, die sich an Ihre Umgebung anpassen lässt. Dank der Erkennung unmittelbarer Bedrohungen wie unbekannter Dateien oder Anwendungen, die in der Umgebung ausgeführt werden, kann **McAfee Threat Intelligence Exchange** die Anfälligkeit für diese Art von Angriffen erheblich verringern. Die Blockierung unbekannter oder neuer ausführbarer Dateien bietet präventiven Schutz vor Ransomware.

- **Umfassende Bedrohungsanalyse:** Die umfassenden Bedrohungsdaten von weltweiten Datenquellen können unkompliziert angepasst werden. Dabei kann es sich um Feeds von McAfee GTI oder Drittanbietern handeln, die mit lokalen Bedrohungsdaten aus Echtzeit- sowie Verlaufsereignissen kombiniert und über Endgeräte, Gateways sowie andere Sicherheitskomponenten weitergegeben werden.
- **Ausführungsschutz und Behebung:** McAfee Threat Intelligence Exchange kann unbekannte Anwendungen daran hindern, in der Umgebung ausgeführt zu werden. Wenn eine Anwendung, die sich später als böswillig herausstellt, zuvor ausgeführt wurde, kann McAfee Threat Intelligence Exchange die laufenden Prozesse dieser Anwendung in der gesamten Umgebung deaktivieren. Dabei greift die McAfee-Lösung auf ihre leistungsfähigen Funktionen zur zentralen Verwaltung und Richtliniendurchsetzung zurück.
- **Sichtbarkeit:** McAfee Threat Intelligence Exchange kann alle gepackten ausführbaren Dateien und deren Start in der Umgebung sowie alle anschließend stattfindenden Veränderungen verfolgen. Dieser Einblick in die Aktionen von Anwendungen oder Prozessen ab der Installation bis zum aktuellen Zeitpunkt ermöglicht schnellere Reaktionen und Behebungsmaßnahmen.
- **Kompromittierungsindikatoren:** Die Hash-Werte bekannt gefährlicher Dateien werden in McAfee Threat Intelligence Exchange importiert, um Ihre Umgebung mithilfe von Richtliniendurchsetzungen gegen diese Bedrohungen zu immunisieren. Wenn diese Kompromittierungsindikatoren in der Umgebung entdeckt werden, kann McAfee Threat Intelligence Exchange alle Prozesse und Anwendungen blockieren, die mit dem Indikator in Zusammenhang stehen.

**McAfee VirusScan Enterprise**

Mit **McAfee VirusScan Enterprise** ist das Erkennen und Abwehren von Ransomware äußerst einfach. McAfee VirusScan Enterprise nutzt das preisgekrönte McAfee-Scan-Modul zum Schutz Ihrer Dateien vor Viren, Würmern, Rootkits, Trojanern und anderen hochentwickelten Bedrohungen.

- **Präventiver Schutz vor Angriffen:** Durch die Verzahnung von Malware-Schutztechnologien und Eindringungsschutz können Exploits abgewehrt werden, die mithilfe von Buffer Overflows Schwachstellen in Anwendungen angreifen.

- **Unschlagbare Malware-Erkennung und -Bereinigung:** Die erweiterte Verhaltensanalyse schützt vor Bedrohungen wie Rootkits und Trojanern. Mithilfe von Techniken wie der Blockierung von Ports und Dateinamen, der Sperrung von Ordnern bzw. Verzeichnissen und Freigaben sowie der Verfolgung und Blockierung von Infektionen wird Malware schon im Ansatz aufgehalten.
- **Echtzeitsicherheit mit McAfee GTI:** Die Plattform für die branchenweit umfassendsten Bedrohungsdaten bietet Schutz vor bekannten und neuen Bedrohungen aus allen Sektoren – Dateien, Web, E-Mails und Netzwerk.

**McAfee Network Security Platform**

**McAfee Network Security Platform** ist für die Durchführung tiefgehender Netzwerkdatenverkehr-Überprüfungen ausgelegt. McAfee Network Security Platform kombiniert fortschrittliche Analysetechniken, um Angriffe z. B. von Ransomware zu erkennen und abzuwehren, die über Netzwerkprotokolle wie Tor, IRC u. a. kommunizieren will. Zu diesen Techniken gehören unter anderem die vollständige Analyse der Protokolle, des Verhaltens und der Bedrohungs-Reputation sowie die erweiterte Malware-Analyse.

- **Umfassender Malware-Schutz:** Die Lösung kombiniert McAfee GTI-Datei-Reputationsdaten sowie Datei-Tiefenanalysen mit JavaScript-Überprüfungen und umfasst ein signaturloses hochentwickeltes Malware-Analysemodul zur Erkennung und Abwehr von Zero-Day-Bedrohungen, angepasster Malware sowie anderen verborgenen Angriffen.
- **Hochentwickelte Analysetechniken:** Die Lösung umfasst die vollständige Analyse der Protokolle, der Bedrohungs-Reputation und des Verhaltens zur Erkennung sowie Abwehr bekannter und Zero-Day-Angriffe im Netzwerk.
- **Integration von McAfee GTI:** Kombiniert Echtzeit-Datei-Reputations-, IP-Reputations- und Standort-Feeds mit detaillierten Kontextdaten zu Benutzern, Geräten und Anwendungen, um schnell und präzise auf Angriffe aus dem Netzwerk reagieren zu können.
- **Security Connected:** Dank der zuverlässigen Integration von McAfee Advanced Threat Defense kann die McAfee Network Security Platform verdächtige Dateien, die in überwachtem Datenverkehr gefunden wurden, an McAfee Advanced Threat Defense übermitteln und dann gemäß den von McAfee Advanced Threat Defense zurückgegebenen Angaben zulassen oder ablehnen.

Der Schutz vor dem Diebstahl wertvoller Daten aus Ihrem Unternehmen stellt eine gewaltige Aufgabe dar, insbesondere wegen der zunehmenden Bedeutung von Ransomware als Angriffsvektor. Mit der Technologie von Intel Security kann sich Ihr Unternehmen sowohl auf den Endgeräten als auch im Netzwerk präventiv vor Bedrohungen wie Ransomware schützen.

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee, das McAfee-Logo und VirusScan sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2015 McAfee, Inc. 61980brf_ransomware_0615

**McAfee. Part of Intel Security.**
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com