PRESSEMITTEILUNG

Thema Cryptolocker:

# Panda Security veröffentlicht ‘Security Guide zum Schutz vor Cyber-Erpressung’

*Duisburg, den 22. März 2016* – Um Unternehmen effektiv davor zu schützen, Opfer von Cyber-Erpressung zu werden, reicht eine Maßnahme allein meist nicht aus. Vielmehr bedarf es einer Kombination aus moderner IT-Sicherheitstechnologie, klaren Unternehmensrichtlinien zur Nutzung der digitalen Infrastruktur sowie der Sensibilisierung der Mitarbeiter für die aktuelle Cyber-Gefahrenlage.

Aus diesem Grund hat Panda Security jetzt einen **Security Guide zum Schutz vor Cyber-Erpressung** veröffentlicht. Das 22-seitige Whitepaper bietet Erläuterungen zur Arbeitsweise neuer Erpresser-Malware wie Cryptolocker, ‚Locky‘ & Co. Es gibt Tipps, was zu tun ist, wenn Unternehmen Opfer einer Cyber-Erpressung geworden sind. Zudem erhalten die Leser einen Überblick über die häufigsten Malware-Typen sowie fünf wichtige Empfehlungen zum Schutz vor Cyber-Angriffen.

## Cyber-Erpressung: die derzeit angesagteste Hackermethode

Die Erpresser-Malware Cryptolocker (und ihre Varianten, wie zum Beispiel ‚Locky‘ CryptoWall, TeslaCrypt usw.) ist derzeit eine der am weitesten verbreiteten Malware-Typen. Nicht nur Krankenhäuser waren in jüngster Zeit von ihr betroffen, sondern auch Verwaltungs- und Regierungsinstitutionen sowie alle Arten von Firmen wurden bereits Opfer des Verschlüsselungstrojaners.

Der Prozess der Cyber-Erpressung beginnt dabei stets damit, dass der Trojaner bestimmte Dateien auf dem Computer seines Opfers bzw. in einem Unternehmensnetzwerk verschlüsselt. Sobald die Verschlüsselung abgeschlossen ist, erhält das Opfer eine E-Mail mit der Aufforderung, ein Lösegeld für die gekidnappten Daten zu zahlen. Stimmt der Nutzer den Zahlungsbedingungen zu, erhält er (meist) eine E-Mail mit dem Code zur Entschlüsselung der Daten.

Allerdings ist die Zahlung des Lösegeldes keinesfalls eine Garantie dafür, dass der Entschlüsselungscode auch tatsächlich funktioniert oder dass der Betroffene in Zukunft nicht erneut zum Erpressungsopfer wird. Daher empfiehlt Panda Security den

Opfern, das geforderte Lösegeld keinesfalls zu zahlen, da sie auf diese Weise das Geschäftsmodell „Cyber-Erpressung“ nur noch fördern. Stattdessen sollten die betroffenen Unternehmen unbedingt Anzeige bei den Strafverfolgungsbehörden erstatten.

## Vorbeugende Maßnahmen sind der beste Schutz vor Cyber-Erpressung

Am besten schützen sich Firmen vor Erpresser-Malware, indem sie vorab eine Reihe von geeigneten Sicherheitsmaßnahmen ergreifen. Dazu gehört eine Schutzlösung, die in der Lage ist, fortschrittliche Bedrohungen zu erkennen und zu blockieren. Hier bietet Panda Security beispielsweise seine neue Cyber-Sicherheitslösung Panda Adaptive Defense 360. Diese nutzt laut Marktforschungsinstitut Gartner eine derzeit einzigartige Kombination aus Endpoint Protection (EPP)- und Endpoint Detection and Response (EDR)-Fähigkeiten, und ist so in der Lage, Unternehmen vor gezielten und Zero-Day-Angriffen oder anderen fortschrittlichen Bedrohungen zu schützen – einschließlich Cryptolocker und all seiner Varianten.

Zusätzlich sollten Unternehmen weitere Maßnahmen ergreifen, um einen optimalen Schutz ihres digitalen Netzwerkes zu erreichen: Zum Beispiel sollten sie ihre Mitarbeiter für die Cyber-Gefahren sensibilisieren, Richtlinien für die Nutzung des Internets erstellen, ihre Systeme stets auf dem neuesten Stand halten sowie interne Protokolle entwickeln, um die gesamte Unternehmenssoftware zu kontrollieren.

## Weitere Informationen zum Schutz vor Cyber-Erpressung:

Den vollständigen **Security Guide zum Schutz vor Cyber-Erpressung** lesen Sie hier: http://pandanews.de/wp-content/uploads/Security-Guide-zum-Schutz-vor-Cyber-Erpressung_03.2016.pdf

Hintergrundinformationen über Cryptolocker lesen Sie in unserem FAQ-Artikel mit dem Titel **Cryptolocker kann jeden treffen** unter http://pandanews.de/cryptolocker-kann-jeden-treffen-was-sie-ueber-die-malware-wissen-sollten-und-wie-unternehmen-sich-schuetzen-koennen/

Informationen zu **Panda Adaptive Defense 360** erhalten Sie unter http://www.pandasecurity.com/germany/enterprise/solutions/adaptive-defense-360/

Ein kurzes **Informationsvideo zu Adaptive Defense 360** (2:51 min) sehen Sie auf unserem YouTube-Kanal unter https://www.youtube.com/watch?v=65DArPOD5Ik

Detaillierte **Informationen zur Arbeitsweise von Verschlüsselungstrojanern** (‚Locky' & Co) sowie eine **Live-Demonstration,** wie und warum **Panda Adaptive Defense 360** Unternehmen davor schützt, bietet Ihnen unser Webcast-Streaming unter https://www.youtube.com/watch?v=Xq9d-kLNanA

## Über Panda Security

Seit seiner Gründung 1990 in Bilbao kämpft Panda Security gegen alle Arten von Internet-Angriffen. Als Pionier der Branche reagierte das IT-Sicherheitsunternehmen mit verhaltensbasierten Erkennungsmethoden und der Cloud-Technologie auf die neuen Anforderungen des Marktes. Dank der speziellen Cloud-Technologien greifen User via Internet auf die weltweit größte Signaturdatenbank zu und erhalten schnellen und zuverlässigen Virenschutz ohne lokales Update. Das Unternehmen hat seinen Hauptsitz in Spanien und direkte Präsenzen in mehr als 80 Ländern sowie Millionen von Kunden auf der ganzen Welt. Die Produkte werden in über 23 Sprachen übersetzt. Die Mission des Unternehmens ist es, die Komplexität zu vereinfachen sowie neue und verbesserte Lösungen zu entwickeln, um das digitale Leben der Anwender zu schützen.

## Pressekontakt:

Kristin Petersen
Presse & PR

PAV Germany GmbH
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg

Tel: +49 2065 961 352
Fax: +49 2065 961 195
Kristin.Petersen@de.pandasecurity.com
www.pandanews.de
www.pandasecurity.com/germany/