Adaptive Defense 360

KEINE CHANCE FÜR CRYPTOLOCKER

WARUM ADAPTIVE DEFENSE 360 SIE ZUVERLÄSSIG SCHÜTZT

Panda Security lässt Cryptolockern keine Chance

Cyber-Erpressung ist derzeit eine der angesagtesten Hackermethoden: Kaum ein Tag vergeht, an dem nicht über neue Ransomware-Angriffe berichtet wird. Dabei machen die fiesen Verschlüsselungstrojaner mit den Namen Cryptolocker, Locky, TeslaCrypt oder Petya vor kaum einem Ziel halt. Krankenhäuser waren bereits in großem Stil betroffen, ebenso wie Verwaltungs- und Regierungsinstitutionen, Firmen aller Art und Größe und auch Privatanwender.

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 Meldung mit einer Zahlungsaufforderung, direkt auf dem Bildschirm des betroffenen Gerätes. 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.

Was können Firmen tun, um sich vor Ransomware-Attacken zu schützen?

Panda Security hat die Antwort auf die jüngsten Entwicklungen im Bereich der Cyberattacken: Adaptive Defense 360, ein neuentwickeltes IT-Schutzsystem auf höchstem technischen Niveau, das – durch eine lückenlose und kontinuierliche Überwachung aller laufenden Prozesse innerhalb eines Firmennetzwerkes – in der Lage ist, Cryptolocker und seine Varianten zu stoppen.

Dabei ist Adaptive Defense 360 wesentlich mehr als eine klassische Antimalware-Lösung. Es ist ein Managed Service, der permanent alle Anwendungen und Prozesse, die auf den Endpoints oder Servern ausgeführt werden, überwacht und – je nach Einstellung – jeden unbekannten Prozess innerhalb eines Systems automatisch blockiert. Dieses permanente Prozess-Monitoring, in Verbindung mit einer intelligenten Big-Data-Analyse in der Collective Intelligence von Panda Security, ermöglicht die automatische Klassifizierung aller laufenden Prozesse. Diese Vorgehensweise sorgt dafür, dass auf einem mit Adaptive Defense 360 geschützten System bekannte oder unbekannte Schadsoftware nicht ausgeführt werden kann.

Adaptive Defense 360: Vier Säulen für Ihre Sicherheit

Automatische Prävention

Blockiert Anwendungen und isoliert Systeme, um zukünftige Angriffe zu verhindern.

Automatische Erkennung

Targeted Attacks und Zero-Day-Angriffe werden in Echtzeit und ohne Signaturdateien blockiert.

Automatische Desinfektion

Entfernung von Malware mit einem Klick oder automatisch, um die Arbeitslast der Administratoren zu reduzieren.

Automatische Forensik

Forensische Informationen für die detaillierte Analyse jedes Angriffsversuchs. Nachverfolgbarkeit und Transparenz jeder Aktion, die von laufenden Anwendungen ausgeführt wird.

Adaptive Defense 360 im Überblick

UMFASSENDE EPP-FÄHIGKEITEN

Adaptive Defense 360 enthält Panda Endpoint Protection Plus, die fortschrittlichste EPP-Lösung von Panda inklusive:

- Wiederherstellungsmaßnahmen
- Zentralisierte Gerätesteuerung: Verhinderung von Malware-Eintritt und Datenverlust durch Sperren von Gerätetypen
- Webfilterung und -überwachung
- Mailfilterung und -überwachung
- Endpoint Firewall und vieles mehr

UMFASSENDER UND STABILER SCHUTZ

Adaptive Defense 360 bietet zwei Betriebsmodi:

- Hardening-Modus: Es dürfen alle Anwendungen laufen, die als Goodware klassifiziert wurden, sowie die Programme, die noch durch Panda Security und die automatisierten Systeme analysiert werden müssen. Jedoch werden alle unbekannten Programme, die aus dem Internet heruntergeladen wurden, blockiert.
- Lock-Modus: Es darf ausschließlich Goodware ausgeführt werden. Dies ist die beste Schutzform für Unternehmen, die einen „Nullrisiko"-Ansatz bei der Sicherheit haben.

SCHUTZ FÜR GEFÄHRDETE BETRIEBSSYSTEME UND ANWENDUNGEN

Systeme wie Windows XP, die nicht länger vom Hersteller unterstützt werden und deshalb ungepatcht und ungeschützt sind, fallen Zero-Day-Angriffen und Bedrohungen der neuesten Generation leicht zum Opfer.
Zudem nutzen 90 Prozent der Malware Schwachstellen in Anwendungen wie Java, Adobe, Microsoft Office sowie in Browsern.
Adaptive Defense 360 nutzt Kontext- und Verhaltensregeln um sicherzustellen, dass Unternehmen in einer sicheren Umgebung arbeiten können, sogar wenn diese Betriebssysteme nutzen, die nicht mehr aktualisiert werden.

INTEGRATION IN SIEM

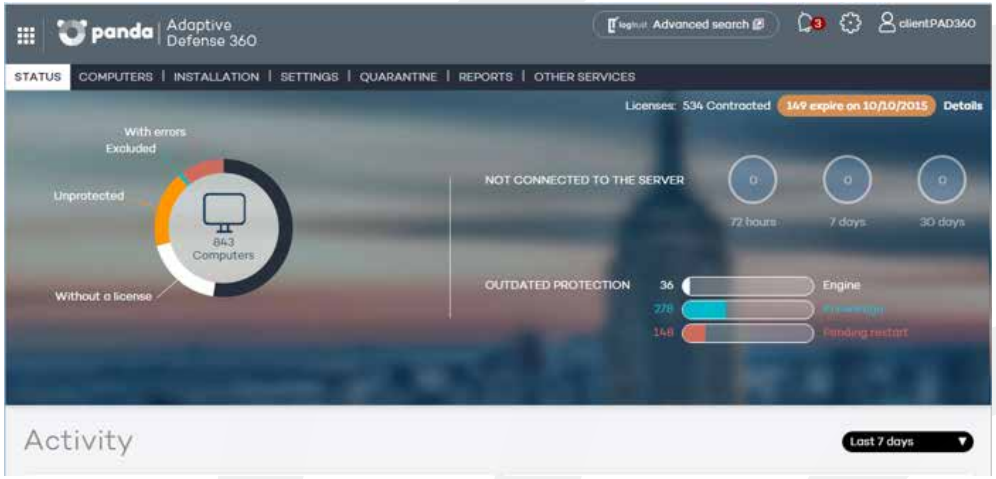
Adaptive Defense 360 integriert sich in SIEM (Security Information and Event Management) Lösungen, um detaillierte Daten über die Aktivitäten aller auf dem System laufenden Anwendungen zu liefern.
Für Kunden ohne SIEM enthält Adaptive Defense 360 optional ein komplettes SIEM-Tool zur Visualisierung und forensischen Analyse dessen, was alle Prozesse im System bzw. Kundennetzwerk auslösen.

FORENSISCHE INFORMATIONEN

- Übersichten aller ausgeführten Aktionen geben einen klaren Überblick über alle Ereignisse, die von der Malware verursacht wurden.
- Heatmaps geben visuelle Informationen über die geografische Herkunft der Malware-Verbindungen, erstellte Dateien und vieles mehr.
- Software mit bekannten Schwachstellen, die im Kundennetzwerk installiert wurde, wird lokalisiert.

STÄNDIGE INFORMATIONEN ÜBER DEN NETZWERKSTATUS

Es werden umgehend Warnmeldungen ausgegeben, sobald Malware im Kundennetzwerk identifiziert wird. Ein umfassender Bericht liefert Informationen zum Ort, den angegriffenen Computern und den von der Malware ausgeführten Aktionen.
Berichte über die täglichen Service-Aktivitäten werden per E-Mail versandt.



pandasecurity.com

Damit jeder sicher alles anklicken kann: Panda Adaptive Defense 360

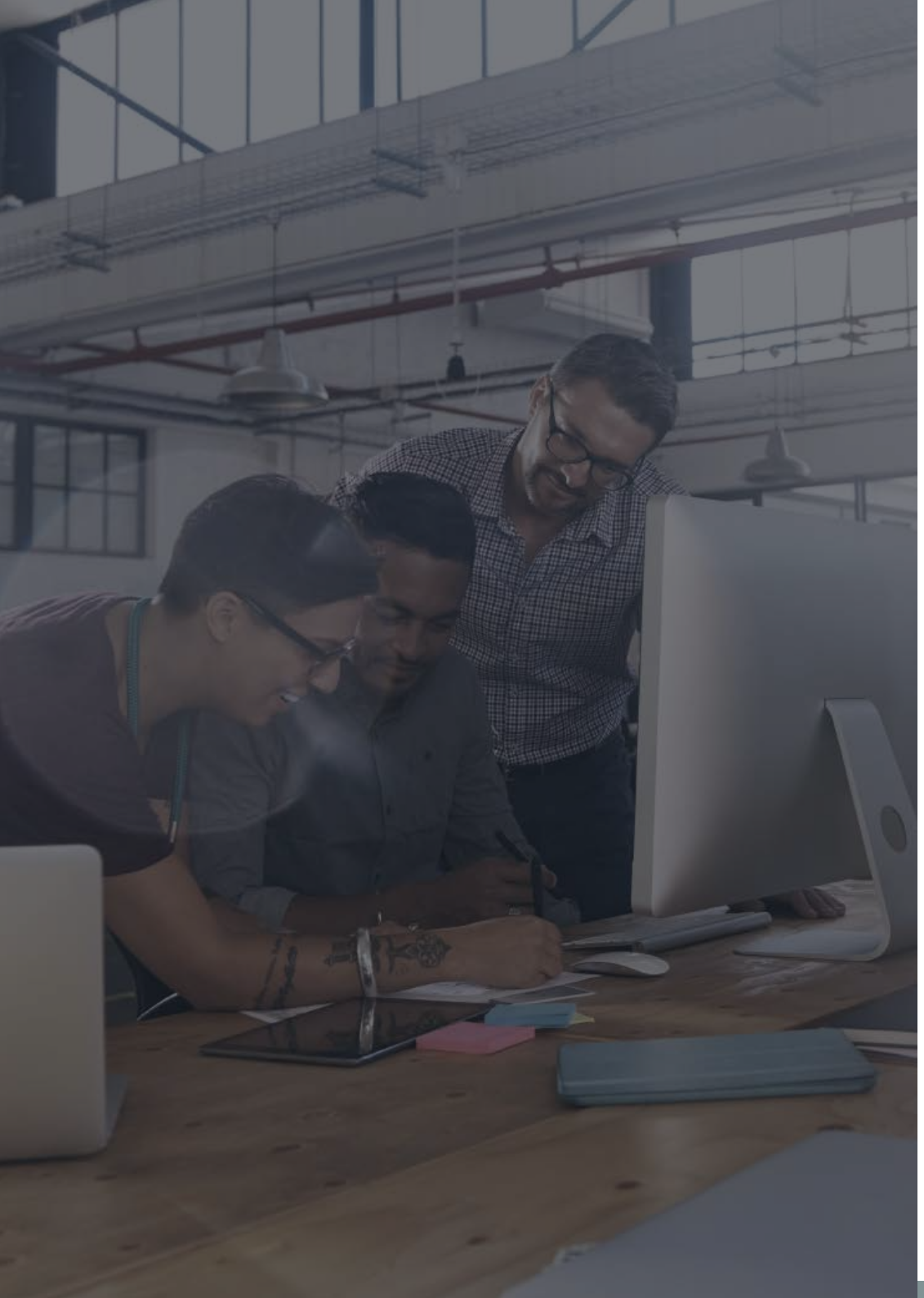
Mit dem Schutz von Panda Adaptive Defense 360 können die User alle Anwendungen und Applikationen in einem Netzwerk bedenkenlos starten.

Anders gesagt: Mit Adaptive Defense 360 müssen sich Unternehmen keine Sorgen mehr machen, dass ihre Mitarbeiter durch das unbedachte Anklicken einer E-Mail oder Webseite das komplette IT-System der Firma lahmlegen. Dieser IT-Schutz gibt Cryptolocker & Co keine Chance.

Weiterführende Informationen

Eine ausführliche Produktvorstellung von Panda Adaptive Defense 360 - entweder in Form eines Live-Webcasts oder als aufgezeichnete Streaming-Version - finden Sie unter http://pandainside.de/panda-academy/webcast/

Ein ebenfalls dort hinterlegter Webcast mit dem Titel ‚Cryptolocker – Hintergründe zu Locky & Co' bietet zudem ausführliche Hintergrundinformationen zur Arbeitsweise von modernen Cryptolockern und den Gründen, warum traditionelle, blacklist-basierte Antivirenlösungen gegen die modernen Ransomware-Exemplare machtlos sind.



Panda Security, Visionär in der IT-Sicherheitsbranche

Panda Security ist einer der führenden europäischen IT-Security-Entwickler und gehört zu den Pionieren im Geschäft mit der digitalen Sicherheit. Das Unternehmen hat seinen Hauptsitz in Spanien und direkte Präsenzen in mehr als 50 Ländern sowie Millionen von Kunden auf der ganzen Welt. Die Produkte werden in über 23 Sprachen übersetzt.

Über einen Zeitraum von ca. fünf Jahren haben Panda-Experten die moderne und derzeit einzigartige IT-Security-Lösung Adaptive Defense 360 entwickelt. Sie ist kompatibel mit Windows-Betriebssystemen und wird kurzfristig auch für Android-Geräte erhältlich sein.

Im magischen Quadranten des renommierten Marktforschungsinstituts Gartner nimmt Panda Security bereits seit mehreren aufeinanderfolgenden Jahren eine Führungsposition im Bereich „Visionäre“ ein. Denn Panda gelingt es immer wieder, die Entwicklungen der neuesten Technologien im IT-Security-Bereich entscheidend voranzutreiben. Gartner bestätigt: „Panda Security verbessert die cloud-basierte IT-Technologie rapide, indem es den Kunden zahlreiche hochentwickelte Features für alle Stufen des ‚Security Life Cycle‘ bietet.“*

* Quelle: Gartner Magic Quadrant für Endpoint Protection Platforms, 22.12.2014


panda