Presseinformation

Cybererpressung kann man vorbeugen

Mit einer geeigneten Backup- und Disaster Recovery-Strategie können auch Daten nach unentdeckten Cyberangriffen wiederhergestellt werden

- Nach den aktuellen erpresserischen Trojaner-Angriffen erkannten Virenscanner die Gefahr erst, als der Befall schon fortgeschritten war – das ist für viele Unternehmen jedoch zu spät
- Erste betroffene Krankenhäuser lassen sich auf Lösegeldzahlung ein, um auf Daten wieder zugreifen zu können
- Sicheres Auslesen selbst von befallen Daten und die Wiederherstellung der Systeme müssen in der Backup- und Disaster Recovery-Strategie verankert sein

Weyarn, 19.02.2016 – Die Internetkriminalität nimmt immer neue Formen an. Die aktuellen Cyberattacken auf Krankenhäuser und Unternehmen, bei denen mittels der Verschlüsselungs-Trojaner „Locky“ und „TeslaCrypt“ Daten verschlüsselt und von den Kriminellen nur gegen Lösegeld wieder freigegeben werden, sind ein neues Niveau auf das sich die IT-Abteilungen einstellen müssen. Selbst über eine Woche nach Bekanntwerden hatten laut Googles Virenwarndienst „VirusTotal“ nur drei von 54 Virenscanner diesen neuen Trojaner erkannt. Dabei treibt der Trojaner schon seit Wochen sein Unwesen und verschlüsselte im Hintergrund unbemerkt Daten. In den USA haben sich schon erste betroffene Krankenhäuser auf die Zahlung eingelassen, um auf wichtige Patientendaten wieder zugreifen zu können. Die SEP AG, deutscher Hersteller von plattformunabhängigen Hybrid Backup- und Disaster Recovery-Lösungen, gibt als Experte auf diesem Gebiet folgende Ratschläge, wie Unternehmen den Erpressungen durch eine Datensicherungsstrategie vorbeugen können. Dadurch können nach einer Trojaner-Infektion Daten sicher zurückgeholt und der laufende Betrieb zügig wiederhergestellt werden.

1. Nur so lässt sich die Totalverschlüsselung der (Backup-)Daten verhindern

Neben den klassisch einzuhaltenden Backup-Szenarien, also wöchentliche Komplettsicherung aller Daten (Full-Backup) und täglichen Sicherung der zwischenzeitlich geänderten Daten (Inkrementelles Backup) sind weitere Maßnahmen nötig:

- Die Backup-Daten müssen mittels Medienbruch auf einem separaten Bandlaufwerk (Tape) und wenn möglich, an einem anderen Ort aufbewahrt werden.
- Der Aufbewahrungszeitraum sollte angesichts der unentdeckten Ausbreitungsdauer verlängert werden.

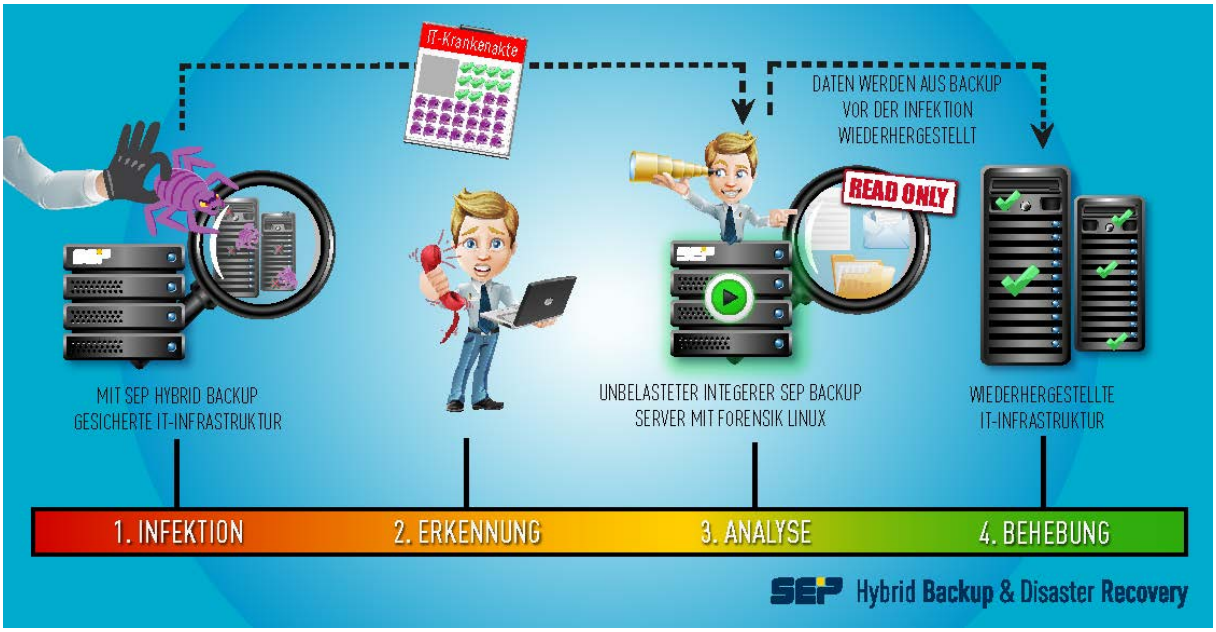
- Die eingesetzte Backup-Software muss die Verwaltung von Ladern und Wechseldatenträgern beherrschen.

2. Schritte nach dem Angriff

Ist, wie im aktuellen Fall, ein Angriff passiert und möglicherweise infizierte Daten in den Sicherungsdatensatz gelangt, besteht sofortiger Handlungsbedarf.

- So muss zunächst der Zeitpunkt des Angriffs eingegrenzt werden.
- Dann setzt die Datenwiederherstellung an. Die Lösung von SEP ist in der Lage einzelne Backups eines beliebigen Sicherungszeitpunktes auf einem abgeschotteten System wiederherzustellen.
- Im sogenannten Read-Only-Modus können auf bereinigten Backup-Festplatten die Daten von Wechselmedien, wie beispielsweise Bandlaufwerken, eingelesen und analysiert werden, ob darin doch noch ein Befall zu verzeichnen ist.
- Wenn der Verschlüsselungsbefehl der Cyberkriminellen noch nicht zur Ausführung gekommen ist, lassen sich so zumindest die Daten lesen. SEP sesam unterstützt dabei Forensik Linux-Distributionen wie beispielsweise KALI, die speziell für die Analyse nach einem Cyber-Angriff entwickelt wurden. So ist es möglich, dass jedes Backup, egal von welcher Quelle, auf einem Linux- oder Windows Backup-Server oder auch Remote-Device-Server geöffnet werden kann und überprüfbar ist.
- Die Schadsoftware hat während der Forensik-Analyse keine Möglichkeit, das integrere System zu infizieren.
- Ist der letzte sichere Datensatz gefunden, werden die Systeme damit sauber wiederhergestellt und der Betrieb der IT-Systeme kann wieder normal anlaufen.
- Vorher müssen die Abwehrmechanismen nochmals überprüft werden, um einen neuerlichen Angriff auszuschließen.

Infografik:
Ablauf der Wiederherstellungs-Maßnahmen nach einem Cyberangriff



Erläuterung der Infografik:

1. Infektion hat stattgefunden.
2. Sie wird von den IT-Administratoren erkannt.
3. Anhand der Backups analysieren, wann der Befall stattfand und wie die Ausbreitung verlaufen ist. Und durch Vergleiche der Sicherungssätze erkennen, wo sich die Schadsoftware befindet. Dazu werden Daten Betriebssystem-übergreifend verfügbar gemacht. Dies erfolgt auf einem abgeschotteten, integren System, beispielsweise mit Hilfe von Forensik Linux KALI.
   - Die Backup-Daten werden von Wechselmedien (Bandlaufwerken) auf bereinigte Backup-Festplatten eingelesen und Read-Only gemountet.
   - Vergleich von Datensätzen von verschiedenen Zeitpunkten.
   - Sichere Datensätze werden erkannt und wiederhergestellt.
4. Das System kann wieder anlaufen und der IT-Betrieb ist wieder lauffähig.

Über SEP AG

Die SEP AG ist Hersteller von Backup- und Disaster Recovery-Lösungen zum Schutz von plattformübergreifenden, heterogenen IT-Umgebungen. Die Datensicherungslösung „SEP sesam“ ist „Made in Germany“ und sichert ein breites Spektrum an virtuellen Umgebungen, Betriebssystemen, Anwendungen und Datenbanken. Die universelle Unterstützung komplexer Systemumgebungen hebt die SEP-Lösung stark von denen der Mitbewerber ab. Dadurch ist eine Konsolidierung mehrerer

Backup-Systeme zu einer zentral verwalteten Hybrid Backup-Lösung möglich. Mit den SEP-Lösungen werden unternehmenskritische Daten jederzeit verfügbar gehalten, was Zeit spart und damit den Kapitalbedarf und die Betriebskosten reduziert.

Seit 1992 entwickelt und vertreibt die SEP AG unternehmensweite Datensicherungslösungen und hat ihren Hauptsitz in Weyarn bei München. Eine Niederlassung mit Support- und Vertriebsteam befindet sich zudem in den USA. Die SEP AG hat ein starkes Partner-Netzwerk und setzt beim Vertrieb zu 100 Prozent auf Wiederverkäufer. Zu den Kunden in mehr als 50 Ländern zählen Aldi Nord, SPIEGEL-Verlag, Stadtwerke Potsdam, Port of San Diego, TU Wien und die Georgetown University.

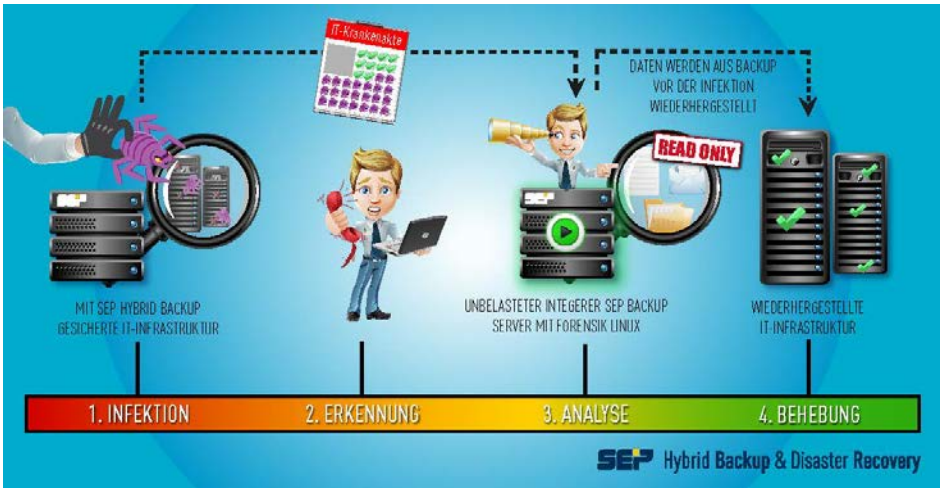
Weitere Informationen unter www.sep.de

30-Tage Vollversion von SEP sesam inkl. kostenlosem Support
http://www.sep.de/download

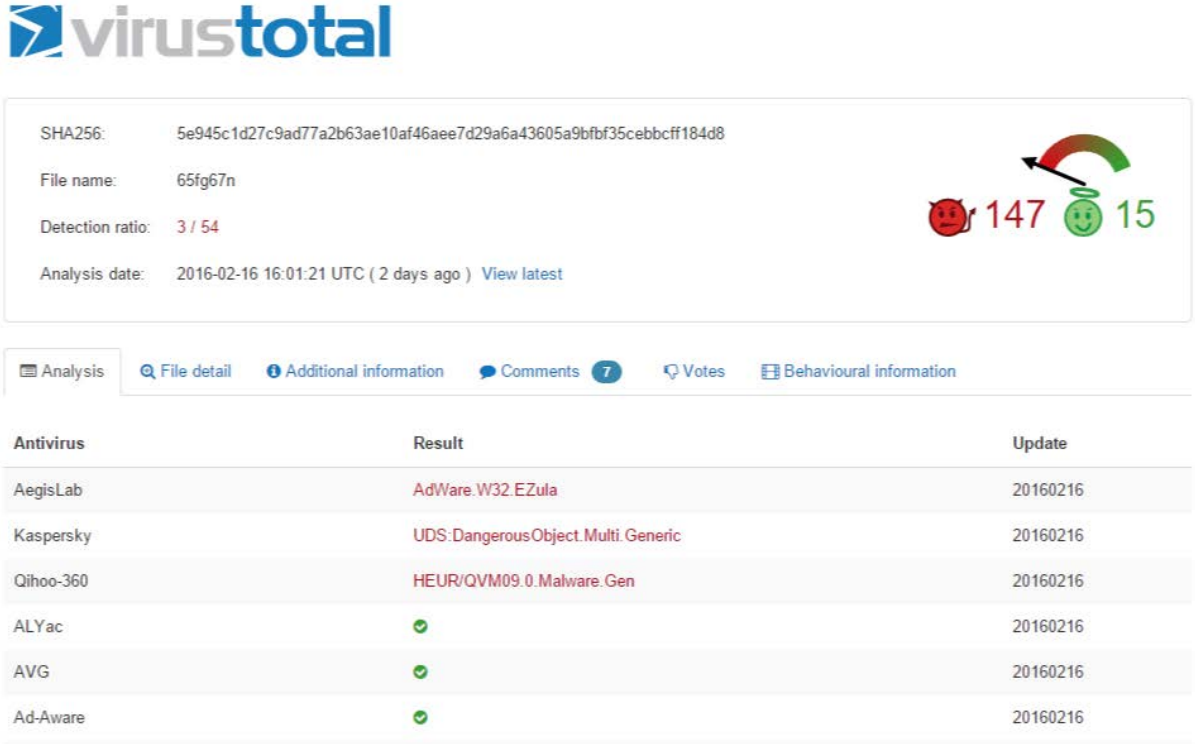
Social Media
Twitter: http://www.twitter.com/SEPHybridBackup
LinkedIn: https://www.linkedin.com/company/846856
Facebook: www.facebook.com/SEPHybridBackup
YouTube: www.youtube.com/user/SEPsesam/

Kundenreferenzen
http://www.sep.de/de/referenzen/

Bildmaterial



Infografik: Ablauf der Wiederherstellungs-Maßnahmen bei einem Cyberangriff
https://www.dropbox.com/s/vyv9e775kip8ydm/Wiederherstellung_nach_Trojanerbefall_SEP_AG.pdf
(Hochaufgelöste PDF-Datei, ca. 3 MB)



SHA256: 5e945c1d27c9ad77a2b63ae10af46aee7d29a6a43605a9bfbf35cebbcff184d8

File name: 65fg67n

Detection ratio: 3 / 54

Analysis date: 2016-02-16 16:01:21 UTC (2 days ago) View latest

147 15

Analysis | File detail | Additional information | Comments 7 | Votes | Behavioural information

Antivirus	Result	Update
AegisLab	AdWare.W32.EZula	20160216
Kaspersky	UDS:DangerousObject.Multi.Generic	20160216
Qihoo-360	HEUR/QVM09.0.Malware.Gen	20160216
ALYac	✓	20160216
AVG	✓	20160216
Ad-Aware	✓	20160216

Screenshot VirusTotal.com (Google) vom 16.02.2016 – über eine Woche nach dem Bekanntwerden der ersten Angriffe, haben erst 3 von 54 Virenscannern den Trojaner erkannt
https://www.dropbox.com/s/jau7893nrmzzfx8/2016-02-16_Antivirus-VirusTotal.png
Link zum Status vom 16.02.2016:
https://www.virustotal.com/en/file/5e945c1d27c9ad77a2b63ae10af46aee7d29a6a43605a9bfbf35cebbcff184d8/analysis/1455638481/

Logo SEP AG
http://www.sep.de/fileadmin/user_upload/Logos/SEP/SEP_HybridBackup-sub_cmyk.zip
(Formate jpg-, ai- und eps-Datei, 4c, als ZIP ca. 250 KB)

Hinweis
Die Meldung ist zum Abdruck freigegeben. Bei Veröffentlichung bitten wir um einen kurzen Hinweis an beleg@veritaspr.de bzw. Zusendung eines Belegexemplars. Vielen Dank!

Kontakt
SEP AG
Ziegelstraße 1
83629 Weyarn
Telefon: +49 8020 180-0
Fax: +49 8020 180-666
E-Mail: info@sep.de

Pressekontakt
David Schimm
Veritas Public Relations
Telefon: +49 8024 467 3132
Mobil: +49 179 5944745
E-Mail: presse@sep.de