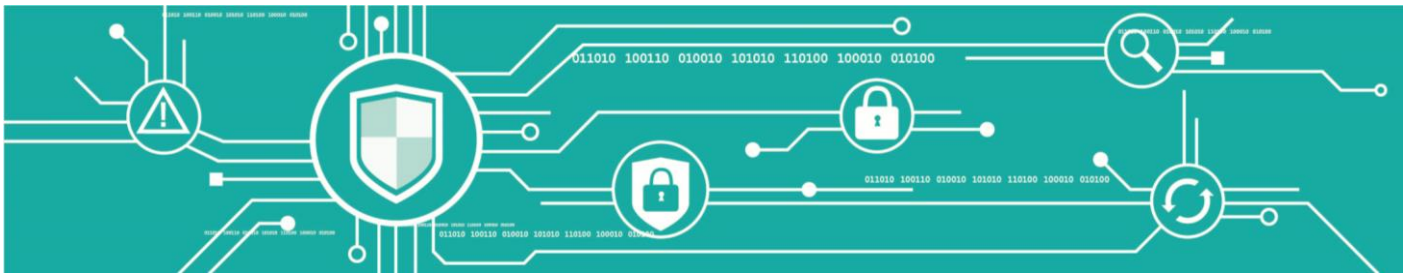

Weltweite Ransomware-Attacke

Server-Admins erleben gerade ein Deja-Vu: Wenige Wochen nach der WannaCry Ransomware wütet erneut eine Erpressersoftware weltweit. Sie nutzt die selbe Schwachstelle, die bereits vor wenigen Wochen zum Einsatz kam - und ist trotz eines vorhandenen Patches extrem erfolgreich. Der initiale Angriffsvektor scheinen möglicherweise manipulierte Dokumente zu sein, die an Personalabteilungen verschickt wurden.

Was wissen wir über den Petya/NotPetya-Ausbruch

Keine zwei Monate nach der aufsehen-erregenden Attacke des Erpressungs-trojaners WannaCry rollt eine zweite Ransomware-Welle um den halben Globus. Dabei scheint es sich, wenigstens dem Anschein nach, um eine neue Version des Trojaners Petya zu handeln. Ziemlich schnell wurde Sicherheitsforschern, die den Ausbruch untersuchten, allerdings klar, dass es sich bei den Angreifern diesmal wohl nicht um einfache Erpresser handelt. Die neue Petya-Variante scheint Erpressung nur als Vorwand zu verwenden – eigentlich geht es wohl darum, möglichst viel Chaos zu erzeugen und Firmen lahmzulegen. Alles deutet auf eine politisch motivierte Cyberattacke hin.

Ziel scheint die Ukraine zu sein, die zuerst und am härtesten getroffen wurde. Dabei stellt der Angriff eine ganz neue Qualität der Cyberattacken dar.
Schaut man sich den Infektionsweg des neuen Trojaners an, wird deutlich, dass der Schadcode um einiges raffinierter ist als die ursprüngliche Ransomware. Nicht nur, dass die Entwickler die wurmartige Verbreitung über die SMB1-Lücke der NSA (ETERNALBLUE) von WannaCry übernommen haben, sie haben ausserdem weitere clevere Verbreitungsmethoden eingebaut.
Im krassen Unterschied dazu sind allerdings die Bezahlmöglichkeiten für Opfer im Gegensatz zu Petya ziemlich verkümmert. Eine fest-eingebaute Bitcoin-Adresse und einzige Mail-Adresse als Kontakt zu den Erpressern wirkt gegenüber dem ausgeklügelten Web-Interface von Vorgänger - Goldeneye gradezu stümperhaft. Was unter anderem dazu geführt hat, dass der Zahlungsweg zu den Angreifern sehr schnell unterbunden wurde.

Auswirkungen und Gefahren

Das alles legt die Vermutung nahe, dass es sich um einen politisch-motivierten Angriff handelt, der Chaos stiften will und dass sich die NotPetya-Angreifer nur als Petya-Erpresser ausgeben. Sie nutzen den Vorwand der Erpressung, um den Verdacht von sich abzulenken. Ob es sich bei den Angreifern um staatliche Hacker handelt, ist allerdings bei weitem nicht klar. Denkbar sind auch andere Akteure, die zwar politisch motiviert sind, aber dennoch unabhängig von staatlichen Regierungen agieren. Neben Organisationen in der Ukraine haben die Angreifer dabei auch viele grosse Firmen in Deutschland, Schweiz, dem Vereinigten Königreich und den USA in Mitleiden-schaft gezogen. Es ist durchaus denkbar. dass dieser Kollateralschaden willentlich in Kauf genommen wurde oder sogar Teil des Plans für den Ausbruch war.

Nach einer bestimmten Zeit (standardmässig sind das 40 Minuten) starten sich infizierte Rechner neu. Nun verrichtet der Trojaner sein zerstörerisches Werk. Die Liste der verschlüsselten Dateien ist, im Gegensatz zu vielen anderen Kryptotrojanern, relativ kurz. Darunter sind komprimierte Archive, PDF-Dokumente, Office-Dateien, Mail-Ordner, Virtuelle Maschinen und Backup-Dateien.

Infektion und Verschlüsselung durch NotPetya funktioniert sowohl auf 32- als auch auf 64-Bit-Windows-Rechnern. Nachdem der Trojaner seine zerstörerische Arbeit durchgeführt hat, versucht er, seine Spuren zu verwischen.

Was kann ich unternehmen, wenn ich infiziert wurde?

Wer Hinweise darauf hat, dass ein System von NotPetya infiziert wurde, sollte dieses umgehend vom Strom trennen. Unter Umständen verhindern Sie so, dass Daten verschlüsselt werden. Schon verschlüsselte Festplatten sollte man aufbewahren. Mit etwas Glück entdecken Sicherheitsforscher nach einiger Zeit Fehler in der Verschlüsselung des Trojaners und es wird ein Werkzeug veröffentlicht, mit dem man seine Daten retten kann. Die beste Verteidigung gegen Bedrohungen wie Petya, NotPetya und ihre fiesen Verwandten sind allerdings aktuelle Backups.

Update Service
Mit dem Update Service übernimmt Rittmeyer das testen und installieren der Patches und Hotfix von Microsoft. Besonders für das Betriebssystem wird empfohlen, in regelmässigen Abständen alle verfügbaren Sicherheitsupdates zu installieren, um bekannte Sicherheits-lücken zu schliessen.

Backup Service
Das Daten-Backup von Rittmeyer ist eine vollständige, Cloudintegrierte Lösung. Gespeichert werden dabei nicht nur die Leitsystemdaten, wie beim manuellen Backup üblich, sondern auch die jeweilige Anlagekonfiguration mit allen Einstel-lungen. Diese Sicherung ist immer aktuell, da sie täglich durchgeführt wird.

ICT-Security
Sollte trotzdem etwas passieren, unterstützen wir Sie gerne mit unseren zertifizierten ISO-27001-Security-Experten.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity