RISIKEN KENNEN - RISIKEN MANAGEN

> Eilmeldung! Kryptotrojaner WannaCry weltweit auf dem Vormarsch

WAS IST PASSIERT?

Es war ein aufregendes Wochenende für IT-Administratoren und Sicherheitsspezialisten weltweit. Eine Malware namens WannaCry verbreitete sich seit Freitagnachmittag weltweit mit rasender Geschwindigkeit. Betroffen sind Windows-PCs, die nicht mit aktuellen Patches versorgt sind. Auf Screenshots verzweifelter Anwender ist eine Bitcoin-Adresse zu sehen, an die 300 US-Dollar zu überweisen sind. Ob die Täter nach Zahlungseingang den Geschädigten auch helfen ist jedoch zweifelhaft – die Anzahl der Betroffenen ist so hoch, dass eine Kommunikation mit den Erpressern kaum möglich ist. Zahlen sollte man daher nicht!

Zu den bekanntesten Opfern des Trojaners gehört die Deutschen Bahn: Einige Anzeigetafeln zeigten unfreiwillig die Infektion mit WannaCry an. Aber auch englische Krankenhäuser und französische Produktionsstätten waren stark betroffen.

WAS IST ZU TUN?

Wenn in Ihrer Firma keine aktuellen Windowsupdates installiert sind, sollte sofort ein Administrator ausrücken und die PCs schützen, bevor es zum Schaden kommt. Denn die Malware verbreitet sich nicht nur über E-Mails mit Anhängen wie in den zuletzt bekannt gewordenen Fällen Goldeneye oder Locky, die bereits weltweit für immense Schäden gesorgt haben.

WannaCry ist noch gemeiner: Der Kryptotrojaner nutzt zusätzlich eine Schwachstelle des sogenannten SMB-Dienstes, der in den Büros u.a. für die weit verbreiteten „Netzlaufwerke“ genutzt wird und daher fast immer aktiviert ist. So kann der Trojaner sich im Netzwerk von PC zu PC ausbreiten, ohne dass es einer Nutzeraktion oder eines Öffnen von E-Mails bedarf. Es ist zu befürchten, dass dies ab heute in vielen Büroumgebungen der Fall sein wird, wenn die PCs wieder eingeschaltet werden. Insbesondere, wenn die oft mobilen Mitarbeiter ins Büro kommen, die ihre nicht aktualisierten Notebooks (zuletzt in öffentlichen WLANs eingebucht) ins Firmennetz einbringen, ist mit Infektionen zu rechnen. Nicht selten wird auch die Geschäftsführung betroffen sein, die sich am ehesten gegen „lästige“ Update-Politiken im Unternehmen wehren kann.

WIE GEHT ES WEITER?

Derzeit sieht es so aus, dass die Verbreitung der Malware temporär gestoppt wurde, nachdem Sicherheitsforscher eine Domain anmeldeten, die der Trojaner abfragt, und auf diese Weise unbeabsichtigt eine Unterbrechungsfunktion aktivierten. Die Forscher wollten Daten sammeln und entdeckten den Mechanismus rein zufällig. Dieser nun aktivierte Schutz ist jedoch nicht überall gegeben, da einige Netzwerke diese Verbindung nicht zulassen. Zudem ist mit Varianten von WannaCry zu rechnen, die ohne diese Unterbrechungsfunktion agieren. Keinesfalls kann Entwarnung gegeben werden!

Es ist daher immens wichtig, dass die Windows-PCs in Ihrem Netzwerk auf den aktuellen Stand gebracht werden – und das am besten, bevor der Büroalltag beginnt und sich der Trojaner auch in Ihrem Netz ausbreitet und Daten vernichtet.

WIE KANN MAN SICH SCHÜTZEN?

Neben der bereits angesprochenen aktuellen Betriebssystem-Software sind es in erster Linie regelmäßige und gut geplante Datensicherungen, die vor Schäden durch Kryptotrojaner schützen. Wer seine Daten selbst wiedereinspielen kann, muss kein Lösegeld zahlen und kann die Folgen eines Angriffes minimieren. Backup-Konzepte sind jedoch komplex und sollten daher sehr sorgfältig geplant und am besten von nicht involvierten Fachleuten überprüft werden (Mehraugenprinzip). Auch regelmäßige Restore-Tests sind Pflicht! Denn eine Datensicherung, die nie getestet wurde, ist ein fahrlässiges Spiel mit dem Feuer – und Fahrlässigkeit hat in gut geführten Unternehmen keinen Platz.

DECKT DIE CYBER-POLICE DEN SCHADEN?

Die Infektion mit WannaCry löst den Versicherungsfall unter der Cyber-Versicherung aus. Betroffene Deckungsbausteine könnten sein:

- Aufwendungen für IT-Forensik-Kosten und weitere Beratungskosten
- Wiederherstellungskosten für die betroffenen IT-Systeme und Daten
- Ertragsausfälle oder Mehrkosten für die provisorische Aufrechterhaltung des Betriebes bei Stillständen in der Produktion Erpressungsgelder

Die Cyber-Versicherung bietet so einen weitreichenden Schutz gegen Schäden durch WannaCry.

WIE SIEHT ES MIT DEN OBLIEGENHEITEN AUS?

In einigen Policen ist ein Patch-Management, das eine zeitnahe Installation von Sicherheitsupdates und – patches sicherstellt, als vertragliche Obliegenheit verankert. Hier muss nach den Umständen des Einzelfalles geprüft werden, ob eine Obliegenheitsverletzung in dem Sinne vorliegt, dass tatsächlich keinerlei planvolles Patch-Management gegeben ist, oder lediglich punktuell und versehentlich vergessen wurde, das betreffende Update aufzuspielen oder aus anderen Gründen das Update nicht erfolgte.

Nach dem Vorfall bei der Telekom im November des letzten Jahres ist dies der nächste großflächige Angriff, der zu versicherten Schäden führen kann. Die Cyber-Versicherung entwickelt sich nach wir vor mit rasanter Geschwindigkeit.

Bitte sprechen Sie uns bei weiteren Fragen gerne an.