PRESSEMITTEILUNG / INTERVIEW

Erpressungstrojaner WannaCry

Experte mahnt: Unternehmenskultur muss sich ändern

- Ransomware in bis dato unbekannter Dimension
- Altsysteme sind Schwachstellen
- Interview mit Albert Ludwig, Comma Soft AG

Bonn, 23.05.2017 – Weltweit Hunderttausende infizierte Betriebssysteme: Ransomware wie jüngst WannaCry verbreitet sich schnell, unkontrolliert und unberechenbar. Das kriminelle Programm traf erstmals neben Privatpersonen und wirtschaftlich orientierten Unternehmen in großem Umfang auch die Betreiber von kritischen Infrastrukturen wie etwa Krankenhäuser in Großbritannien und die Deutsche Bahn. Für Albert Ludwig, Manager des Competence Centers Infrastructure Platforms beim Bonner Data Business- und IT-Consulting-Spezialisten Comma Soft, kommt der Vorfall wenig überraschend.

Frage: Die Ransomware „WannaCry“ hat eine bekannte Sicherheitslücke von Microsoft ausgenutzt, für die es bereits ein Patch gab. Dass Betriebssysteme nicht auf dem neuesten Stand sind, passiert immer wieder. Wieso konnte WannaCry entgegen früherer Ransomware-Attacken eine so große Reichweite erzielen?

Ludwig: WannaCry nutzte zwei Angriffsvektoren: Zum einen wurde der Trojaner durch den Versand von sehr gut gefälschten Emails

mit einem infizierten Anhang verbreitet. Zum anderen hat sich der Schädling über bereits infizierte Rechner verbreitet, indem er die genannte Sicherheitslücke genutzt hat.

Frage: Reicht es zum Schutz vor Attacken, Betriebssysteme und Antivirenprogramme regelmäßig zu aktualisieren?

Ludwig: Grundsätzlich sollten Anwender natürlich nach wie vor alle Systeme und Antivirenprogramme aktualisieren. Dies bietet jedoch keinen hundertprozentigen Schutz wie im Fall von sogenannten Zero-Day-Attacken, die auf bisher unbekannte Sicherheitslücken abzielen.

Frage: Was ist durch Ransomware betroffenen Firmen zu raten?

Ludwig: Zuerst sollten sie die infizierten Systeme identifizieren und bereinigen. Danach ist es wichtig, die Ausbreitung des Trojaners zu stoppen, um weiteren Schaden zu verhindern. Dies geschieht durch gezielte Abschaltung der Verbreitungswege wie beispielsweise Netzwerksegmente, Clients aber auch Server. Wenn eine Wiederherstellung der verschlüsselten Daten etwa durch ein Backup nicht möglich ist, sollten Anwender das chiffrierte Material dennoch aufbewahren. Der Verschlüsselungsalgorithmus des Trojaners wird voraussichtlich in absehbarer Zeit entschlüsselt.

Frage: Jeder kennt die Gefahr. Warum scheitert die Umsetzung von Security-Maßnahmen in Unternehmen noch immer so häufig?

Ludwig: Angriffe auf Sicherheitslücken erfolgen in immer kürzeren Abständen und lassen somit IT-Abteilungen immer weniger Zeit, entsprechende Updates einzuspielen. Außerdem gilt die höchste Priorität der IT der Unterstützung der Geschäftsprozesse. Oft ist

der schnelle Ablauf zunächst wichtiger als die Sicherheit der Struktur. Zudem betreiben viele Unternehmen Anwendungen, die auf veralteten Technologien beruhen und für die die Hersteller keine Updates mehr entwickeln. Ebenso sind trotz häufiger Angriffe und zahlreicher Medienmeldungen noch immer viele Benutzer zu sorglos, wenn beispielsweise eine E-Mail von einem unbekannten Absender stammt.

Frage: Wie können Unternehmen wirksame Schutzmechanismen gegen Cyberattacken aufbauen?

Ludwig: Im ersten Schritt sollten Unternehmen ihre IT homogenisieren, denn je weniger differenziert die Systeme sind, desto geringer fällt die Vielfalt der Angriffsvektoren aus. Insbesondere sind die bereits erwähnten Altsysteme zu beseitigen. Außerdem empfiehlt es sich, alle Systeme regelmäßig zu patchen und in unterschiedliche Netzsegmente, DMZ, Firewalls usw. aufzuteilen. Außerdem sollten Unternehmen prüfen, ob unsignierte Office-Makros auf ihren Clients deaktiviert werden können. Hinweise auf die typischen Verhaltensweisen von Ransomware wie beispielswiese massive Schreib- und Löschvorgänge können Monitoring-Maßnahmen geben. Zudem helfen professionelle Partner bei der proaktiven Suche nach Schwachstellen in der IT und reduzieren somit die Verwundbarkeit. Unternehmen sollten außerdem Vorgehensweisen und Prozesse planen, um bei einem Angriff strukturiert vorzugehen.

In diesem Sinne muss sich die Unternehmenskultur vielerorts ändern und insbesondere den verantwortlichen IT-Mitarbeitern die Möglichkeit geben, ohne Sorge um die eigene Karriere mögliche Schwachstellen zu melden. Zudem ist es ratsam, das Personal

eigens für das Thema Sicherheit durch regelmäßige Informationen und Schulungen zu sensibilisieren.

Über Albert Ludwig:

Albert Ludwig ist Competence Center Manager bei der Comma Soft AG, einem Bonner IT-Unternehmen mit Fokus auf Data Business-, IT-Consulting und Softwareentwicklung. Ludwigs Schwerpunkt liegt auf der Beratung zur Informationssicherheit von Unternehmen.

Weitere Infos: https://www.comma-soft.com/cmc-fuer-sicherheit/workshop-counter-ransomware/

Über die Comma Soft AG:

Die Comma Soft AG – „The Knowledge People“ wurde 1989 von Stephan Huthmacher gegründet. Seitdem hat sich das Unternehmen einen Namen als „Digital Think Tank“ und innovatives IT-Consulting- und Software-Haus gemacht. Comma Soft unterstützt Kunden bei der Umsetzung der digitalen Transformation ihrer Geschäftsmodelle. Das Leistungsspektrum umfasst Data Science-, Analytics-, IT-Strategie, IT-Architektur und Security-Consulting sowie die dazu passenden Software-Produkte und Lösungen. Sowohl große und mittelständische Unternehmen in der DACH-Region als auch zahlreiche DAX-Konzerne bauen auf die 27-jährige Erfahrung von Comma Soft im Enterprise-Umfeld. 135 Mitarbeiter sorgen am Stammsitz in Bonn und bei den Kunden vor Ort dafür, dass Projekte agil und wertschöpfend umgesetzt werden.

Kontakt für Journalisten & Redaktionen:

Malte Limbrock
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-630
Fax: +49 (0)228 / 30412-639
limbrock@agentur-sputnik.de
www.sputnik-agentur.de

Hagen Thiele
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-633
Fax: +49 (0)228 / 30412-639
thiele@sputnik-agentur.de
www.sputnik-agentur.de