Ransomware im Karrieremodus

Vom lästigen Quälgeist zur ernstzunehmenden Bedrohung für die Gesellschaft

Alles fängt mal klein an. Auch Ransomware steckte vor zehn Jahren noch in den Kinderschuhen, stieg dann aber rasant die Karriereleiter zur Super-Malware hinauf. Immer raffinierter, jedes Mal krimineller, mit kontinuierlich wachsendem Opferkreis: Ransomware erscheint grenzenlos. Was tun? Sophos-Experte Michael Veit kennt den Feind und empfiehlt eine mehrschichtige Abwehrstrategie.

Wiesbaden, 3. Mai 2017 – Für viele Internetnutzer scheint die heute weit verbreitete Ransomware-Welle aus dem Blauen heraus zu kommen. Doch erste Vertreter der Erpresser-Malware wie z.B. der Trojaner „Cryzip“ sorgten bereits 2006 für Ärger – damals allerdings noch mit einem sehr kleinen und regional begrenzten Aktionsradius. Erst 2013 setzte sich die Schädlingsart mit dem Auftreten des ersten globalen Superstars „CryptoLocker“ in den Köpfen fest.

Dieser und sein Nachfolger „CryptoWall“ machen eine ideale Objektstudie zum Thema „Was macht Ransomware so mächtig?“ möglich. Zuerst war nur Ottonormalverbraucher im Visier der Cyberkriminellen. Doch das Wesen von Ransomware lässt weitaus größere Ziele zu: jeder kann Opfer sein, auch kleine und mittelständische Unternehmen und Abteilungen großer Organisationen. Michael Veit, Technology Evangelist bei Sophos, bringt das „Erfolgsmodell“ Ransomware auf den Punkt: „Für Ransomware-Entwickler war und ist es einfach, ihre Profite schnellen rasant in die Höhe. Laut FBI-Schätzung in 2016 bis zu einer Milliarde US-Dollar. Trotz besserem Schutz und höherer Aufmerksamkeit zeigt Ransomware keinerlei Anzeichen, sich zur Ruhe zu setzen: die Opferzahlen von kleinen Unternehmen, Krankenhäusern, Büchereien, Polizeistationen, Hotels und Verbrauchern steigt kontinuierlich.“

Wie tickt der Feind?

Das Angriffsfeld von Ransomware ist grenzenlos und macht es den Cyberkriminellen einfach, da sie nicht mehr darüber nachdenken müssen, wen sie als nächstes Opfer auswählen sollen. Es wird einfach jeder. Dabei erhöht sich der Preis proportional zu den Unannehmlichkeiten, die die Erpresser dem Opfer zufügen. Der Code gilt den Cyberkriminellen dabei als Indikator: je mehr Zeilen, desto höher der mentale Druck auf das Opfer. Via Social Engineering wird die Lösegeld-Zahlung für den User als der einfachste Weg dargestellt, sich zu befreien.

Doch auch wenn man sich entscheidet, auf die Zahlungsaufforderung einzugehen, heißt das noch lange nicht, dass man auch seine Daten wieder bekommt. Es lässt sich nämlich eine wachsende Unzuverlässigkeit im Hinblick auf die Zahlungs-Abwicklung erkennen, die von den Cyberkriminellen verwendet wird. Entweder, weil die Polizei sie dicht gemacht hat oder weil die Kriminellen sie aufgeben mussten, um

nicht entdeckt zu werden. Schwierig, den „Deal“ dann umzusetzen. So wird die Ransomware zur dauerhaften Lockware.

Die Überlegung, dass Opfer mehrfach hintereinander mit der gleichen Taktik attackiert werden, scheint auf den ersten Blick gegen die eigene Intuition zu sprechen. Bis man den Trick begreift, mit Hilfe von Social Engineering einen Grad von Kontrolle im Kopf des Opfers zu erzwingen. Wenn Kriminelle die Regeln des Spiels schreiben, ist es der Gefangene, der sich an ihre Vorstellung der Realität anpassen muss. Eine entscheidende Verhaltensänderung, die neue Lösungsmöglichkeiten eröffnet. Aber wo finden Unternehmen und Verbraucher Hilfe?

Ransomware-Abwehr auf verschiedenen Ebenen
Bevor man gleich mit konkreter Anti-Ransomware Technologien startet, sollte man als erste Abwehrmaßnahme die grundlegenden Schutzhinweise anwenden. Darunter fallen sowohl flächendeckende Backup-Routinen und regelmäßiges Einspielen der Patches, als auch eine sorgfältige Netzwerk-Trennung von Servern und Workstations und eingeschränkte Nutzerfunktionen. Einige Administratoren blocken die Ausführungsfunktion in Anhängen, aber vergessen diesen Schutz dann für Dokumenten Makros. Makros gehören zu den beliebtesten Zugängen, durch die Cyberkriminelle versuchen, ihre Malware in den meist sehr gut strukturierten Dokumenten zu platzieren. Deswegen: das Öffnen von JavaScript Dateien (.JS) im Notepad als Standard definieren und Microsoft Office 2016 „Protected View“ so konfigurieren, dass Office-Makros automatisch stoppen wenn Dokumente aus dem Internet empfangen werden.

Aufdecken, Blockieren, Wiederherstellen – Intercept X
Für Geschäftskunden bietet Sophos mit Intercept X ein modulares Endpoint Security Produkt an, das vielfältige Sicherheitsmaßnahmen integriert und zugleich den Schutz vor Ransomware, der bereits in bestehenden Endpoint Tools verfügbar ist, verstärkt.
„Intercept X kombiniert dreierlei: Exploit Schutz (in dem es die Techniken abpasst, die Ransomware indizieren, wie zum Beispiel dass man viele Dateien öffnen soll), das Aufspüren von Zero-day Attacken und eine forensische Analyse, die einen Malware-Angriff sogar bis auf seine Quelle entblößen kann“, so Veit, der bei Sophos auch an der Produktentwicklung beteiligt ist.
Sobald Ransomware es schafft, Entschlüsselungsdateien auszuführen, wird umgehend der CrypoGuard Schutz mit seinen Sanierungsmaßnahmen gestartet. Damit besteht die Möglichkeit, Prozesse zurückzusetzen und so eventuelle Schäden rückgängig zu machen. Diese Vorgehensweise unterstreicht die Art und Weise, Ransomware anzugehen: gleichermaßen reaktiv, entlarvend und blockierend.

Und für die Zukunft? Nicht verzagen. Nur schneller sein.
Im Hinblick auf das neue Wachstum von zielgerichteter Ransomware, Ransomware-as-a-Service und der massenhaften Verschlüsselung von unzureichend gesicherten MongoDB-Datenbanken, erscheint es nicht übernervös, sich zu fragen, wo die Ransomware-Reise denn hingehen soll. Doch Veit bleibt zuversichtlich: „Es gilt – wie immer im Leben: nicht vor Angst verzagen, sondern sich der neuen Situation anpassen. Ransomware wird immer raffinierter. Darauf haben wir keinen Einfluss – wohl aber, wie schnell wir die Attacken abwehren. Dieses Bewusstsein und die Anpassungsfähigkeit werden den entscheidenden Vorsprung im Kampf gegen Ransomware ausmachen.“

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de