Wirksamer Schutz vor digitaler Erpressung

Ransomware ist auf dem Vormarsch – vermehrt auch in Unternehmen. Abhilfe schafft eine integrale Sicherheitslösung von Kaspersky Lab, die unterschiedliche Technologien kombiniert und auf allen betroffenen Infrastrukturebenen wirkt.

Ransomware, auch Cryptolocker oder Cryptomalware genannt, wird zunehmend zum Problem. Waren anfangs vor allem Privatanwender von der erpresserischen Verschlüsselung ihrer Daten betroffen, zielen Cryptomalware-Attacken heute immer mehr gegen Unternehmen und gehören mittlerweile zu den drei gravierendsten Sicherheitsproblemen von KMU. Werden kleine und mittelständische Unternehmen Opfer eines Ransomware-Angriffs, entsteht ein durchschnittlicher Schaden von rund 100 000 Franken (bedingt durch den Datenverlust, die Anstrengungen für die Wiederherstellung und entgangene Geschäfte).

Auf die Erpressung einzugehen und das geforderte Lösegeld zu zahlen – bei Unternehmen meist viel mehr als die paar hundert Franken, die Erpresser von Privatanwendern verlangen –, bringt oft gar nichts: Mindestens ein Fünftel der KMU, die der Forderung nachkamen, erhielten ihre Daten niemals zurück.

Am Anfang steht der Nutzer

Entschärfen lässt sich das Ransomware-Problem durch verschiedene Massnahmen. So sollten etwa die Mitarbeitenden zum äusserst vorsichtigen Umgang mit E-Mails und Links zu unbekannten Websites angeregt werden. Methoden wie Phishing oder Social Engineering, mit deren Hilfe der Schadcode auf die betroffenen Systeme gelangt, werden jedoch immer raffinierter. Auch eine E-Mail, die unverdächtig aussieht und vorgeblich von einem bekannten Absender stammt, kann als Einfallstor für Cryptolocker dienen. Und wie schnell klickt man einen gefälschten Link zu angeblich interessanten Informationen an – kaum ein Anwender kann sich zu hundert Prozent zurückhalten.

Kein Schutz ohne Sicherheitslösung

Eine stets aktuell gehaltene Sicherheitslösung, die sich nebst der Abwehr konventioneller Viren und Würmer sowie der Abwehr fortgeschrittener Attacken speziell auch um Ransomware kümmert, ist deshalb unabdingbar – so wie die ganzheitliche Sicherheitslösung von Kaspersky Lab, die bereits seit 2014 Funktionen zum Schutz vor Cryptomalware beinhaltet und kontinuierlich ausgebaut wird. Ausschlaggebend sind dabei mehrstufige Schutzmechanismen, die sowohl unterschiedliche Infrastrukturelemente wie Arbeitsstationen und Server abdecken als auch mit einer gezielten Kombination von Erkennungs- und Abwehrtechnologien arbeiten. So nutzt Kaspersky Lab ausser dem gängigen Blacklisting von als schädlich erkannten Absendern und Websites auch proaktives Machine-Learning, das bisher unbekannte Angriffe erkennt. All diese Technologien nutzen die globalen Big-Data-Analysefunktionen des Kaspersky Security Network (KSN).

Vielfältige Schutzfunktionen

Einige Beispiele aus dem Arsenal der Sicherheitslösungen von Kaspersky Lab: Mit Sicherheitskontrollen lässt sich die Nutzung von unerwünschten Geräten und Websites einschränken, ebenso der Start von nicht vertrauenswürdigen Programmen. Die Gefahr von Malware-Angriffen wird damit generell minimiert. Noch weiter geht «Application Privilege Control». Damit kann der Zugriff von Programmen auf bestimmte Ressourcen inklusive Nutzer- und Systemdateien gezielt geregelt werden. Wenn kein Schreibzugriff besteht, kann auch Ransomware diese Dateien nicht mehr verschlüsseln. Der automatische Exploit-Schutz sorgt dafür, dass Malware keine Schwachstellen im Betriebssystem sowie in häufig angegriffenen Programmen ausnutzen kann. Der «System Watcher» erkennt gefährliche Programmprozesse anhand von Aktivitätsmustern und blockiert schädliche Aktionen. Und die serverbasierten Anti-Cryptor-Funktionen verhindern, dass Daten auf gemeinsam genutzten Ressourcen (z. B. Fileserver) durch eine infizierte Workstation verschlüsselt werden.

ANTI-RANSOMWARE VON KASPERSKY LAB: DIE HIGHLIGHTS

- Schutz für alle Endpoints – PCs, Macs, Server, Mobilgeräte, virtuelle Server und Desktops (VDI)
- Abgestimmte Kombination verschiedener Erkennungs- und Abwehrtechnologien
- Big-Data-Analytics und Machine Learning für umfassende Schadcode-Erkennung
- Aktivitätsmonitor mit Cryptomalware-Countermeasures-Technologie
- Sicherheit für Mailserver (Exchange, Linux Mail, Lotus Domino)
- Programmkontrolle, Webkontrolle, Anti-Phishing

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch