Trojaner haben keine Chance

Detlev Spierling

Um die Gefahr von Ransomware-Attacken einzudämmen, setzt der rheinland-pfälzische Kreis Bad Dürkheim auf die neuartige Schutz-Software CryptoSpike und ist damit zu einem bundesweiten Vorreiter bei der IT-Sicherheit avanciert.

Kryptotrojaner oder Ransomware sind eine besonders aggressive Form der Online-Erpressung. „Die Online-Kriminellen kapern die Computer ihrer Opfer, drohen mit der Sperrung des Bildschirms oder nehmen die Daten quasi in Geiselhaft – Freilassung nur nach Geldzahlung. Betroffene sind Krankenhäuser, Stadtverwaltungen oder Smartphone-Nutzer weltweit“, schrieb die FAZ im März 2016. Eine Ransomware-Attacke kostet oft mehr als zehnmal so viel wie das geforderte Lösegeld – nämlich im Schnitt 40.500 Euro. „Das durchschnittlich geforderte Lösegeld liegt bei 3.700 Euro pro Angriff“, berichtete das Fachmagazin IT-Business in seiner Online-Ausgabe am 15. November 2018 unter Berufung auf eine weltweite Umfrage eines IT-Herstellers unter 2.400 Managed Service Providern. Die aus einer Attacke resultierenden Umsatzverluste durch Ausfallzeiten können sogar geschäftsbedrohende Ausmaße annehmen.

Daher setzt der Landkreis Bad Dürkheim – als erste regionale Gebietskörperschaft in Deutschland – seit Kurzem auf einen neuartigen Schutz gegen Ransomware-Attacken auf FileServer-Ebene und ist damit bundesweit Vorreiter bei der IT-Sicherheit. Die Schutz-Software namens CryptoSpike wurde von dem jungen österreichischen IT-Unternehmen ProLion speziell für die leistungsfähigen Speichersysteme des US-amerikanischen Anbieters NetApp entwickelt, die auch in Bad Dürkheim eingesetzt werden.

Kreis Bad Dürkheim ist vor Trojanern gut geschützt.

CryptoSpike schützt Speichersysteme von NetApp wirksam und proaktiv auf der FileServer-Ebene nach einem dreistufigen Konzept, das auf der Erkennung von Verhaltensmustern basiert: Sobald das System während einer Transaktion in Echtzeit eine Anomalie bei einer Dateiendung, einem Dateinamen oder im Verhalten eines Anwenders entdeckt, schlägt es Alarm und sperrt den Lese- und Schreibzugriff des betreffenden Mitarbeiters. Der User befindet sich dann sozusagen in IT-Quarantäne und kann keinen weiteren Schaden anrichten.

Implementiert wurde die IT-Security-Lösung im Kreis Bad Dürkheim von Christian Ruppert, der mit seinem im Jahr 2011 gegründeten IT-Consulting-Unternehmen in Ingelheim am Rhein vor allem für mittelständische Unternehmen arbeitet. „Die IT-Lösungen, die wir vorstellen, können wir bis ins Detail selbst planen, optimieren, umsetzen und weiter betreuen. Dabei ist es unser oberstes Ziel, eine hohe Kundenzufriedenheit zu erreichen“, so Ruppert.

Der Experte, der herstellerübergreifend mit allen führenden Hard- und Software-Anbietern zusammenarbeitet und auf eine über 15-jährige IT-Erfahrung zurückblickt, installierte CryptoSpike Anfang Mai 2018 bei der Kreisverwaltung Bad Dürkheim. Bevor das System Anfang August produktiv ging, wurde zunächst in einer ausführlichen Test- und Lernphase die Funktionalität auf Herz und Nieren geprüft. Dabei wurden Malware-Angriffe mittels PowerShell-Skripten nachgestellt und erfolgreich abgewehrt.

Der Informationssicherheitsbeauftragte der Kreisverwaltung Bad Dürkheim, Ferdinand Hecht, lobt

Schutz in drei Stufen

Wie die Software CryptoSpike genau arbeitet, erklärt im Interview Robert Graf, Gründer und Geschäftsführer von ProLion.

Herr Graf, warum kann ein Ransomware-Angriff so große Schäden verursachen?

Nach einschlägigen Schätzungen wird weltweit etwa alle 40 Sekunden ein Unternehmen mit Ransomware infiziert. Moderne Ransomware-Varianten können sich wie ein Wurm im Netzwerk weiterverbreiten, ohne dass der Anwender dafür interagieren muss oder es merkt.

Wie kann Ihre Lösung solche Ransomware-Angriffe verhindern?

CryptoSpike entdeckt Ransomware-Angriffe durch drei aufeinander abgestimmte Konzepte. Dazu zählt die Whitelist, die alle in einem Unternehmen oder einer Organisation erlaubten Dateiendungen enthält. Diese werden bei Installation unserer Lösung automatisch aus dem Storage-System von NetApp ausgelesen. Ergänzend gibt es eine Blacklist, die aktuell rund 1.800 bekannte Ransomware-Dateiendungen oder -Dateinamen enthält und täglich aktualisiert wird. Hinzu kommt der entscheidende Teil – der Learner als dritte Sicherheitsstufe von CryptoSpike. Dieser analysiert Muster (Patterns) des Benutzerverhaltens in einem Unternehmen oder einer Verwaltung. Dazu werden die letzten 50.000 Transaktionen im Netzwerk erfasst und in der White-Patterns-List gespeichert. Ebenso gibt es die Black-Patterns-List mit Verhaltensmustern aus aktuellen Ransomware-Angriffen.

Link-Tipp

Weitere Informationen unter:

- **www.prolion.at**

Wie reagiert CryptoSpike bei einem erkannten Ransomware-Angriff?

Zunächst liefert CryptoSpike die wichtigste Information: Wo sind welche Dateien betroffen? Das Unternehmen erhält Informationen über den Pfad und die Anzahl der durch Ransomware verschlüsselten Dateien. Bei irrtümlicher Sperre kann der User mit einem Klick wieder entsperrt und die Patterns können gegebenenfalls angepasst werden. Bei einem Ransomware-Angriff kann so schnell analysiert werden, wo schadhafte Programme

Robert Graf

laufen. Sobald der Mitarbeiter nach Bereinigung entsperrt wird, unterstützt CryptoSpike den Recovery-Prozess mit einer Exportliste der betroffenen Dateien, sodass diese über die regelmäßig erstellten Snapshots des NetApp-Systems schnell wiederhergestellt werden können.

Was kostet CryptoSpike?

CryptoSpike wird pro NetApp-Storage Controller lizenziert. Die Kosten für ein NetApp-Speicher-Cluster, bestehend aus zwei so genannten Nodes, belaufen sich inklusive 36 Monate Wartung auf netto 8.800 Euro. Die Installation ist in zwei bis drei Tagen erfolgreich abgeschlossen. Die jährlichen Kosten liegen damit bei unter 3.000 Euro.

Interview: Detlev Spierling

vor allem den geringen Aufwand für die CryptoSpike-Installation während des laufenden, produktiven Betriebs seiner Behörde sowie die einfache Bedienung der IT-Lösung. „Mit dieser effektiven technischen Schutzmaßnahme haben wir das Risiko eines Ransomware-Befalls ganz entscheidend vermindert. Darüber hinaus setzen wir natürlich auch weiterhin eine Firewall und einen Viren-Scanner ein und haben die Nutzung von Browser-Plug-Ins begrenzt, die ja häufig zum Einfallstor für Malware werden“, betont Hecht sein umfangreiches Sicherheitskonzept. Zu diesem gehört auch die Sensibilisierung aller Mitarbeiter der Verwaltung, mit E-Mail-Anhängen entsprechend vorsichtig umzugehen.

Detlev Spierling ist freier IT-Fachjournalist aus Oberursel (Taunus).