STUDERUS
network technologies

Bedrohung durch Ransomware

In diesem Interview beantwortet der erfahrene Studerus IT- und Kursleiter Hugo Bosshard die häufigsten Fragen zum Thema Ransomware und gibt nützliche Tipps aus erster Hand.

Wie beurteilen Sie die Bedrohungslage mit Ransomware?
Die Gefahr ist sehr gross, wachsend und noch schwer einzuschätzen. In einem Punkt ist man sich beim Thema Ransomware jedoch einig: Die Lösung für sämtliche Probleme in diesem Bereich gibt es leider noch nicht. Offensichtlich ist sich die IT-Industrie dessen bewusst und lässt alle hoffen. Vorerst müssen wir also mit der aktuellen Situation zurechtkommen und uns mit den zur Verfügung stehenden Lösungen möglichst schadlos halten.

Wie kann man das Bewusstsein vor Ransomware bei den Anwendern stärken?
Die Einschätzung der Vertrauenswürdigkeit an einem konkreten Fall ist in unserem Unternehmen zu 100 % schief gelaufen. Eine sehr gut gefälschte Bewerbung wurde als E-Mail über drei Instanzen weitergeleitet. Eine Person öffnete schlussendlich die mit Ransomware befallene Bewerbungsdatei. Dies trotz einer Makrowarnung seitens Word. Glücklicherweise konnte der auf dem Client installierte Virenscanner Schlimmeres verhindern. Im Anschluss an diesen Vorfall führten wir intern einen für alle Mitarbeitenden obligatorischen Security-Kurs durch, in welchem wir den erwähnten Fall offenlegten und daraus lernen konnten. Ich bin davon überzeugt, dass die dafür eingesetzte Zeit einen wesentlichen Beitrag zum korrekten Umgang mit Informationen aus unterschiedlichen Quellen (Mail, Browser usw.) geschaffen hat. In Zukunft werden wir weitere interne Awareness-Schulungen durchführen.

«Die Lösung für sämtliche Probleme in diesem Bereich gibt es leider noch nicht.»

Wie wird Ransomware bereits in einkommenden Mails blockiert?
Als erste Instanz wird auf jeden Fall eine Antispam-Lösung mit integriertem Virenscanner benötigt. Ransomware-Angriffe werden aber zunehmend raffinierter und leider von Spam-Lösungen trotz neuster Sandbox-Technologie oft nicht erkannt. Bei Studerus AG werden alle Mails mit verdächtigen Attachments geblockt und in eine Quarantäne gestellt. Dies hat allerdings Konsequenzen: Die Quarantäne wird von einem IT-Mitarbeiter manuell bedient, der das Mail auf seine Vertrauenswürdigkeit hin überprüft und anschliessend dem Adressaten freigibt. Diese Umsetzung führt zu einem grossen Aufwand, ist in der aktuellen Bedrohungslage jedoch sehr wirkungsvoll. Im Weiteren werden für öffentliche Mailkonten, welche viele allgemeine und potenziell gefährliche Mails behandeln, dedizierte Arbeitsplätze eingesetzt. Der angemeldete Benutzer arbeitet mit stark eingeschränkter Berechtigung auf dem Fileserver. Bei einem Ransomware-Befall wäre der Schaden limitiert und unter Kontrolle.

«Bei Studerus AG werden alle Mails mit verdächtigen Attachments geblockt und in eine Quarantäne gestellt.»

Wie werden Systeme gegen Ransomware möglichst immun?
Ein Muss ist das Patchen von OS-Layer und Applikationen. In diesem Bereich setzen wir kompromisslos auf «Schnelligkeit». Sobald neue Patches von Herstellern zur Verfügung stehen, spielen wir diese so zeitnah wie nur möglich ein. Dies geschieht nicht mehr nur an angrenzenden Wochenenden, sondern auch im Verlauf des Tagesgeschäfts. Grundsätzlich sind wir von dieser Notwendigkeit überzeugt, kämpfen allerdings mit der Erstellung eines verlässlichen Berichts, welcher aufzeigen soll, dass alle Clients den aktuellsten Patch-Level aufweisen.

«Die vielen bekannten Schadensfälle zeigen aber auf, dass sehr oft der Faktor Mensch Schlimmeres hätte verhindern können.»

Was ist bei der Datensicherung mit Backups zu beachten?
Bekannterweise führen bei erfolgreichen Crypto-Attacken oft nur noch die vorhandenen Sicherungen zu den benötigten Daten. Hier haben wir sichergestellt, dass nach einem erfolgten Backup die gesicherten Daten vom Unternehmensnetzwerk getrennt werden.

Welche weiteren Aktionen sind bei der Studerus geplant?
- Einsatz von FW4.20 auf der Firewall Zyxel USG1900 (neu mit GeoIP und SafeSearch)
- Deinstallation diverser SW-Pakete auf den Clients (es soll nur SW zur Verfügung gestellt werden, welche benötigt wird)
- Überarbeitung der internen IT-Richtlinien
- Anpassung der Berechtigungs-Strukturen auf dem Fileserver

Welche weiteren Tipps geben Sie IT-Verantwortlichen?
Die IT-Abteilungen können einen grossen Beitrag zur Sicherstellung eines Betriebs leisten, dies mit dem Einsatz diverser Systeme, welche gut unterhalten und regelmässig auf korrekte Funktionsweise überprüft werden. Die vielen bekannten Schadensfälle zeigen aber auf, dass sehr oft der Faktor Mensch Schlimmeres hätte verhindern können. Somit lohnt es sich, die Mitarbeitenden regelmässig zu schulen und gezielt auf neue Gefahren hin zu informieren. Also, nehmen Sie sich die notwendige Zeit zur Schaffung einer guten Awareness, es lohnt sich! ■

Hugo Bosshard
Leiter IT