Neue Zürcher Zeitung

GASTKOMMENTAR

Schadsoftware und Datenschutz – die Firewall Mensch

Jeder einzelne Nutzer sollte sich selber als Glied in der Kette zum Schutz der im Unternehmen bearbeiteten Daten sehen.

Michael Valersi
13.9.2017, 05:30 Uhr

In jüngerer Zeit sahen wir zahlreiche spektakuläre Angriffe von Ransomware. «Wanna Cry» im Frühjahr 2017 und keine zwei Monate später «Not Petya» sind sicherlich jene, die am meisten Aufsehen erregten – auch deswegen, weil Firmen und Privatpersonen auf der ganzen Welt gleichermassen von Schadsoftware betroffen waren, die Daten verschlüsselte und die Betroffenen erpresste. Gerade durch die Berichterstattung in de Medien sollte inzwischen bekannt sein, dass jeder von einem Cyberangriff betroffen sein kann, und dies ungeachtet dessen, ob sich jemand selbst als lukratives Angriffszie sieht oder nicht.

Elf Antworten zur Cyberattacke «Wanna Cry»

Michael Schilliger

Ransomware – vorausgesetzt, die Nutzer oder die Unternehmen haben mit einer entsprechenden Back-up-Strategie vorgesorgt – ist unter Umständen eine teure, aber grundsätzlich beherrschbare Situation. Eigentlich macht sie einen sehr geringen Antei der im Umlauf befindlichen Schadsoftware aus. Der Grossteil schlummert unerkannt auf den Rechnern der Nutzer und gewährt Angreifern Zugriff auf sämtliche darauf gespeicherten vertraulichen und persönlichen Daten. Da diese Infektionen einem Betroffenen nicht unmittelbar auffallen, besitzen sie ein weit höheres Schadenspotenzial – etwa durch die Möglichkeit des Diebstahls von Passwörtern und Zugangsdaten sowie Finanz- oder anderen unternehmenswichtigen Daten.

Regelmässige Software-Updates, Firewalls, Angrifferkennungssysteme und viele ander technische Sicherheitsmassnahmen sollten Standard sein. Doch nicht allen Bedrohungen aus dem Internet kann allein mit technischen Massnahmen begegnet werden. Es gibt da noch den Angriffsvektor Mensch, die wohl grösste Schwachstelle. Aufgrund dieser Erkenntnis steht die Sensibilisierung der Nutzer für das Thema IT-Sicherheit und den Datenschutz seit längerem auf der Agenda von Unternehmen. Insbesondere bei jenen, die in irgendeiner Weise vertrauliche oder besonders schützenswerte (personenbezogene) Daten bearbeiten. Es werden Sensibilisierungsveranstaltungen durchgeführt oder die Mitarbeiter zur Teilnahme an E-Learning-Kursen verpflichtet. Dabei ist der Umgang mit E-Mails immer ein Thema; wohl auch, weil E-Mail laut der Melde- und Analysestelle Informationssicherung (Melani)nach wie vor der häufigste Verbreitungsvektor für Schadsoftware ist.

Doch wie praxistauglich sind die Tipps und Vorgaben? Ein Auszug aus einem E-Learning-Kurs zum Thema Umgang mit E-Mails, adressiert an eine Personalabteilung: «E-Mails dürfen nur geöffnet werden, wenn diese absolut vertrauenswürdig erscheine und Anhänge nur, wenn diese erwartet wurden.» Die Frage der Praxistauglichkeit scheint nachvollziehbar, wenn man bedenkt, dass in einer Personalabteilung täglich zi Bewerbungen von Unbekannten womöglich initiativ, ohne konkreten Stellenbezug, au elektronischem Weg eingehen und dabei Anhänge wohl eher die Regel als die Ausnahn sind. Wenig praxistauglich dürfte auch folgende Aufforderung sein: «Verwenden Sie z Weitergabe von Daten immer neue Datenträger (USB-Sticks, CD-ROM oder DVD), die noch nie beschrieben wurden. Sie verhindern dadurch, dass nicht zur Weitergabe bestimmte oder nicht komplett gelöschte Daten aus Versehen mitgegeben werden.»

GASTKOMMENTAR

Mündigkeit und Datenschutz

Thomas Damberger

In der heutigen Zeit ist eine regelmässige Sensibilisierung des Personals in Unternehmen für das Thema Datenschutz und Datensicherheit zweifellos unentbehrlich – die Firewall Mensch. Es kommt dabei nicht darauf an, ob traditionell mit Vorträgen oder mit E-Learning-Werkzeugen sensibilisiert wird. Wesentlich ist jedoch, dass die Tipps und vor allem die verbindlichen Vorgaben praxistauglich sind u ihre Einhaltung vor allem im Unternehmensumfeld auch kontrolliert wird. Die Schulungen sollten auf die jeweilige Zielgruppe und deren Arbeitsumfeld sowie die verwendete Software massgeschneidert sein. Jeder Nutzer sollte sich letztlich als stark Glied in der Kette zum Schutz der in einem Unternehmen bearbeiteten Daten sehen und erkennen, dass jede noch so ausgereifte technische Schutzmassnahme durch falsches Verhalten der Nutzer ausgehebelt werden kann – im Sinne von: «Ich klicke m zur Not wird es der Helpdesk schon richten.» Nein, er wird es nicht richten können!

Michael Valersi ist Informatiker und Datenschutzexperte.

Veraltete Systeme sind eine grosse Gefahr

Die Schadsoftware «Wanna Cry» hat Hunderttausende von Computern lahmgelegt. Viele Firmen sind betroffen. Was ist passiert, und wie können Sie sich schützen? Die wichtigsten Antworten im Überblick.

Michael Schilliger, Christian Steiner

Schweizer Firmen sind gezwungen, Daten ihrer Kunden besser zu schützen – sonst drohen drakonische Strafen

Dem neuen Datenschutzgesetz in der EU sind auch die meisten Schweizer Unternehmen unterworfen. Die Auswirkungen sind nicht zu unterschätzen, und Unterlassungen können ganz schön ins Geld gehen.

Giorgio V. Müller