ESET-Analyse: Ransomware bleibt in Unternehmen eine unterschätzte Gefahr Schlagzeilen machen andere Angriffstrends - doch Ransomware bleibt die grösste Bedrohung

Cryptomining, Cyber-Spionage oder Angriffe auf kritische Infrastrukturen: So lauten die Top-Cyber-Gefahren des Jahres 2018 - zumindest, wenn man die mediale Aufmerksamkeit als Massstab nimmt. Bei Unternehmen, die von Cyberkriminellen attackiert wurden, stellt sich ein ganz anderes Bild dar: Hier sorgt nach wie vor Ransomware für Angst, Schrecken und enorme Schäden. Seit 2017, wo Attacken mit dieser Erpressersoftware allein für ein Viertel aller Schadensfälle verantwortlich waren, will die Flut der Angriffe nicht verebben. Stephen Cobb, Senior Security Researcher beim IT-Sicherheitsspezialisten ESET, hat das Problem Ransomware genauer unter die Lupe genommen. In seinem Whitepaper "Ransomware - Eine Gefahr für Unternehmen" auf dem Security-Portal stellt er die wichtigsten Angriffsvektoren, Bedrohungsarten und Gegenmassnahmen vor.

Ransomware entwickelt sich rasant weiter

Tatsächlich ist die Gefahr durch Ransomware aktuell grösser denn je. Vor allem in den letzten beiden Jahren haben Cyberkriminelle ihre Methoden perfektioniert, um Erpressersoftware auf Systeme aufzuspielen. Im Vergleich zu früher, als Kriminelle viele Nutzer um verhältnismässig geringe Summen erpressen wollten, gehen sie nun wesentlich gezielter vor. Sie konzentrieren sich auf einen eher kleinen Kreis von besonders attraktiven Opfern, deren Daten einen besonders hohen Wert haben und von denen sich deshalb grosse Summen erpressen lassen.

Das Whitepaper stellt besonders drei Angriffsvektoren in den Fokus:

1. RDP-Attacken, die Geräte angreifen, auf denen Software mit Remote Desktop Protocol (RDP) läuft. Ein typischer RDP-Endpoint ist etwa ein Datenbank-Server. Das Protokoll verwenden nach Daten von Shodan über 3 Millionen Systeme im Internet.
2. E-Mail-Attacken, bei denen Ransomware über Mail-Anhänge auf Systeme eingeschleust wird.
3. Angriffe, die über die Supply Chain verbreitet werden. Hier werden beispielsweise Software-Unternehmen attackiert, um Schadcode mithilfe von deren Updates in die Breite zu streuen.

Attraktive Opfer: Ã–ffentliche Hand und Unternehmen

Organisationen der Ã–ffentlichen Hand sind von Ransomware-Attacken ebenso betroffen wie Unternehmen. Das wahre Ausmass der Schäden lässt sich anhand von Medienberichten nur schwer beziffern - zu selten berichten Unternehmen über erfolgreiche Cyber-Angriffe auf ihre IT-Infrastruktur. Managed Service Provider und Anbieter von Security-Software bestätigen unisono, dass Ransomware weiterhin eine grosse und vor allem potentiell kostspielige Gefahr für alle Branchen darstellt.