Keine Angst vor „Emotet“

Der Trojaner „Emotet“ gilt als die derzeit gefährlichste Cyberbedrohung für Unternehmen weltweit. Denn ein Emotet-Angriff ist besonders tückisch: Hat dieser Virus einmal den Weg auf einen Rechner gefunden, können Hacker weitere Schadsoftware beliebig oft nachladen. Die Sorge bei vielen Unternehmen ist daher groß. Dabei kann man sich mit geeigneten IT-Sicherheitslösungen sehr gut vor dem Angreifer schützen.

Das Unternehmen Krauss-Maffei hat es getroffen, den Aluminiumhersteller Hydro Norsk auch, und jüngst wurde der Maschinenbauer Pilz zum Opfer: Hacker haben die gesamten Firmendaten verschlüsselt und eine Lösegeldforderung an die Unternehmen geschickt. Tagtäglich werden Unternehmen auf diese Weise erpresst. Laut einer Cybersecurity-Studie des TÜV ist jeder fünfte IT-Sicherheitsvorfall ein Ransomware-Angriff – nur die prominentesten Beispiele kommen in die Schlagzeilen.

Immer häufiger steckt hinter solchen Erpressungsangriffen die Schadsoftware Emotet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft Emotet in Verbindung mit Ransomware in seinem aktuellen Lagebericht als eine der größten Bedrohungen für Unternehmen ein. Emotet wird vom BSI sogar als „eine der größten Cyberbedrohungen der Welt“ bezeichnet.

Durch Emotet- und Ransomware-Angriffe entstehen Unternehmen enorme Kosten – auch wenn kein Lösegeld fließt: Ein Großteil der IT-Systeme muss heruntergefahren werden, um eine Verbreitung der Schadsoftware zu vermeiden und die Mitarbeiter müssen eigentlich automatisierte Arbeitsprozesse plötzlich wieder manuell ausüben, was die Geschäftsabläufe enorm verlangsamt. Zudem ist die Website der betroffenen Unternehmen häufig tagelang nicht erreichbar. Dem norwegischen Aluminiumhersteller Hydro Norsk ist auf diese Weise ein Schaden von rund 40 Millionen Euro entstanden.

Was macht Emotet so gefährlich?

Emotet ist ein Türöffner. Ist der Trojaner einmal installiert, können die Hacker völlig ungehindert weitere Schadprogramme nachladen. Deswegen stellen Emotet-Angriffe eine ganz neue Qualität von Cyberverbrechen dar: Einmal eingeschleust, ist das angegriffene Unternehmen verschiedensten Angriffsszenarien ausgeliefert. Professionelle Hacker-Banden können auf diese Weise langfristige Angriffsszenarien planen und angegriffene Rechner zu Bot-Netzen zusammenführen. Mit diesen lassen sich beispielweise DDos-Angriffe ausüben. Dabei werden massenhaft Anfragen an eine Webseite gerichtet, bis deren Service zusammenbricht. Buchungssysteme, Online-Shops und Online-Banken werden auf diese Weise lahmgelegt.

Sehr häufig nutzen Hacker Emotet als Vorbereitung für Ransomware-Angriffe. Mit Hilfe von Emotet lassen sich aber auch Tools nachladen, die einen Fernzugriff auf den Rechner ermöglichen, um Daten auszuspionieren, zu manipulieren oder zu entwenden. Betroffene Unternehmen merken meist zu spät, dass sie Opfer eines solchen Angriffs geworden sind – z. B. dann, wenn interne Daten im Internet auftauchen. Das kann mitunter zu einem immensen Imageschaden und Vertrauensverlust bei den Kunden führen.

Wie gelangt Emotet in das IT-System?

Emotet wird mithilfe gefälschter E-Mails, sogenannter Phishing-E-Mails, auf Unternehmensrechnern eingeschleust. Diese sehen heute so echt aus, dass es nur schwer ist, sie als Fälschungen zu erkennen. Hinter dem Versand stecken professionelle Hacker-Banden, die in regelmäßigen Abständen eine regelrechte Phishing-Flut initiieren. Die Malware wird über eine angehängte Datei eingeschleust. Der Trick: Der Empfänger wird aufgefordert, bestimmte Einstellungen am PC vorzunehmen – bspw. die Makros einer Word-Datei zu aktivieren. Wer dieser Aufforderung nachkommt, lädt – ohne es zu wissen – Emotet auf seinen PC. In seltenen Fällen ist die Schadsoftware bereits in das angehängte Dokument verpflanzt. Einmal angeklickt oder heruntergeladen, ist das System infiziert.

Angriffsziel Personalabteilungen

Ein häufiges Angriffsziel sind Personalabteilungen. Denn Bewerbungsschreiben eignen sich besonders gut zum Phishing. Der Grund: Jede Bewerbung ist individuell und somit zunächst nicht auffällig – das machen sich Cyberkriminelle zunutze.

Sobald ein Rechner befallen ist, meldet sich Emotet beim Server des Hackers zurück. Dieser weiß dann, dass der Angriff erfolgreich war und kann weitere Malware ein-

Autor:
Clemens A. Schulz,
Director Desktop Security
Rohde & Schwarz Cybersecurity GmbH
www.rohde-schwarz.com/cybersecurity

schleusen. Parallel dazu liest Emotet Inhalte aus Outlook-Postfächern des befallenen Systems aus – das sogenannte „Outlook-Harvesting“. Die gesammelten Informationen nutzen die Täter zur weiteren Verbreitung der Schadsoftware. Opfer erhalten bspw. gefälschte Antworten eines bekannten Kontaktes. Das führt dazu, dass der Spam echt wirkt und mit hoher Wahrscheinlichkeit geöffnet wird.

Wie kann sich ein Unternehmen vor Emotet schützen?

Aufgrund der hohen Zahl an professionellen Phishing-E-Mails reichen Mitarbeiterschulungen zum Schutz vor Emotet nicht aus. Fehler lassen sich kaum vermeiden – die Folgen eines Angriffs sind jedoch enorm. Auch Antivirenlösungen und klassische Firewalls können den Schädling nicht abhalten. Stattdessen braucht es Sicherheitslösungen, die nicht nur auf Angreifer reagieren, sondern diese „proaktiv“ aus dem IT-System fernhalten.

Internetzugang sichern

Um einen PC vor Emotet zu schützen, sollte vor allem der Internetzugang gesichert werden. Am konsequentesten ist das durch eine Trennung von Internet und internem Netzwerk möglich – denn dann kann Schadsoftware nicht in das Basisbetriebssystem eindringen. Praktisch umsetzen lässt sich das mit einem virtuellen Browser: Als Erweiterung zur hardwarebasierten Komponente wird dazu eine softwarebasierte virtuelle „Surfumgebung“ geschaffen. Die Nutzer arbeiten mit einer vom Betriebssystem separierten Maschine. Der Vorteil: Anstatt – wie bei Antivirenprogrammen – Schadcodes zu erkennen, werden alle potenziell gefährlichen Aktivitäten in diesem virtuellen Browser isoliert. Jeder Browserstart beseitigt die Schädlinge und versetzt den Browser in seinen Ausgangszustand.

Strikte Trennung

Selbst wenn Emotet über einen USB-Stick einen Weg ins Netzwerk findet, ließe sich der Angriff aufhalten: Um den Schädling zu aktivieren und weitere Schadsoftware nachzuladen, wäre der Zugang zum Internet notwendig, welcher jedoch durch die strikte Trennung bei einem virtuellen Browser nicht möglich ist. Auch infizierte Dokumente lassen sich in dieser gesicherten Umgebung betrachten: Falls es sich um einen toxischen Anhang handelt, kann dieser nicht auf das Betriebssystem des PCs zugreifen.

Rundumpakete

Zugang zum Unternehmensnetzwerk gewinnen die Angreifer heute allerdings nicht nur über PCs vor Ort. Schon längst nutzen Mitarbeiter zunehmend Notebooks, Tablets, Smartphones und IoT-Geräte im Ökosystem der IT-Abteilungen. Um auch diese Geräte, die mit unternehmenseigenen IT-System verknüpft sind, zu schützen, eignen sich Rundumpakete: Ein sicherer VPN-Client schützt die Netzwerkkommunikation des Endgerätes über das Internet. Entscheidend für die Sicherheit ist auch, dass der VPN-Client zu keinem Zeitpunkt den Zugriff des Gerätes auf ein ungeschütztes Netzwerk – wie bspw. einen Hotspot – erlaubt. Eine zusätzliche Festplattenvollverschlüsselung sorgt dafür, dass das Gerät lokale Daten sicher speichert. Wird die Lösung durch einen virtualisierten Browser ergänzt, sind die Endgeräte auch vor Angriffen aus dem Internet geschützt. Setzt man dabei auf softwarebasierte Sicherheitslösungen sind teure Zusatzgeräte nicht erforderlich.

Und wenn es zu spät ist?

Ein Emotet-Befall bleibt meist unentdeckt, bis es zu Folgeangriffen kommt. Handelt es sich um Ransomware, sollten Unternehmen auf keinen Fall den Lösegeldforderungen nachkommen. Denn jede erfolgreiche Erpressung motiviert den Angreifer weiterzumachen. Zusätzlich finanzieren Lösegelder die Weiterentwicklung von Schadsoftware und fördern deren Verbreitung. Zudem gibt es keine Garantie dafür, dass die Daten nach der Zahlung wieder freigeschaltet werden.

Das BSI empfiehlt, stattdessen Strafanzeige zu erstatten. Denn polizeiliche Ermittlungen ermöglichen Untersuchungen, die Betroffene selbst meist nicht durchführen können, wie etwa die Überwachung verdächtiger Server. Zusätzlich sollten Betroffene infizierte Rechner umgehend vom Netz trennen, um den Schaden möglichst einzugrenzen. ◄