ROHDE&SCHWARZ

PRESSEINFORMATION

München, 11. August 2021

Ransomware: So können sich Unternehmen wirklich schützen

Eine aktuelle Studie des Digitalverbands BITKOM bewertet Ransomware als Haupttreiber für den enormen Anstieg an Cyberattacken. Die Erpresserangriffe verursachen bei den Betroffenen einen enormen wirtschaftlichen Schaden. Doch Unternehmen und Behörden sind nicht wehrlos: Es gibt durchaus wirksame Möglichkeiten, sich vor Ransomware-Attacken zu schützen.

Autor: Dr. Falk Herrmann, CEO von Rohde & Schwarz Cybersecurity

Bei einem Ransomware-Angriff verlangen Cyberkriminelle ein Lösegeld, um zuvor gestohlene oder verschlüsselte Daten wieder freizugeben. Solche Erpresserangriffe sind längst Teil eines lukrativen, kriminellen Geschäftsmodells. Keine Branche, Region oder Unternehmensgröße ist heute davor gefeit und mit jeder Weiterentwicklung der Angriffe steigen die Lösegeldforderungen. Sie liegen nicht selten bei einer Höhe von 1 Millionen Euro und mehr. Das Bundeskriminalamt (BKA) bezeichnet Ransomware-Angriffe daher als größte Cybercrime-Bedrohung für deutsche Unternehmen und öffentliche Einrichtungen überhaupt.

Der Präsident des Digitalverbands BITKOM, Achim Berg, warnt: „Die Wucht, mit der Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Unternehmen aller Branchen und Größen.“ In einer aktuellen Studie hat der Digitalverband BITKOM aufgezeigt, dass Ransomware Haupttreiber des enormen Anstiegs von Cyberangriffen im vergangenen Jahr ist. Die so verursachten Schäden hätten sich im Vergleich zu den Vorjahren 2018/2019 mehr als vervierfacht (+358 Prozent). Aktuell sehe jedes zehnte Unternehmen (neun Prozent) seine geschäftliche Existenz durch Cyberattacken bedroht.

Wie gelangt Ramsomware in das Netzwerk?
Ransomware-Angriffe werden häufig über File-Sharing-Netzwerke und Phishing-E-Mails verbreitet – versteckt in Bildern oder als ausführbare Dateien im Anhang von E-Mails. WannaCry, einer der bekannteren Ransomware-Angriffe, nutzte eine Schwachstelle in einem Protokoll von Microsoft, wodurch jeder ungepatchte, mit dem Internet verbundene Computer für eine Infektion anfällig wurde. Andere Angriffe nutzen ungesicherte Remote-Desktop-Dienste. In Zeiten von Remote Work und Homeoffice bieten sich daher besonders viele Schwachstellen.

Wie sollten Unternehmen auf einen Ransomware-Angriff reagieren?
Ist die Geschäftsfähigkeit durch einen Angriff bedroht, sehen sich viele Unternehmen genötigt, zu zahlen – in der Annahme schnell wieder Zugriff auf unternehmenskritische Daten und Informationen zu erlangen. Doch es gibt keine Garantie dafür, dass die Daten nach der Zahlung wieder freigeschaltet werden. Das BKA rät daher: Unternehmen, die von einem Erpresserangriff betroffen sind, sollten auf keinen Fall den Lösegeldforderungen nachkommen. Jede erfolgreiche Erpressung animiert den Angreifer, weiterzumachen. Lösegelder finanzieren zudem die Weiterentwicklung von Schadsoftware und fördern deren Verbreitung.

Die Polizei informieren
Im Falle eines Ransomware-Angriffs sollten Unternehmen stattdessen die Erpressungsnachricht auf dem Bildschirm fotografieren und eine Anzeige bei der Polizei erstatten. Alle infizierten Computer sollten dann so schnell wie möglich voneinander, vom gemeinsamen Speicher und vom Netzwerk getrennt werden. Um die Daten wiederzuerlangen kann es helfen, den Rechner neu aufzusetzen und Daten-Backups aufzuspielen.

Um juristische Konsequenzen zu verhindern, sollten Unternehmen zudem prüfen, ob sie

- den Angriff beim BSI (Bundesamt für Sicherheit in der Informationstechnik) melden müssen. Anbieter digitaler Dienste wie Online-Marktplätzen, Suchmaschinen und Cloud-Computing-Diensten sind verpflichtet, ein IT-Sicherheitsniveau gemäß „dem Stand der Technik“ zu erfüllen. Vorfälle sind laut § 8c BSI-Gesetz zu melden.

- den Angriff der Aufsichtsbehörde melden müssen. Durch den Angriff kann der Schutz personenbezogener Daten bedroht sein, wenn keine Backups von ihnen vorliegen. Das wäre ein Verstoß gegen die EU-DSGVO. Erpresser können ausgespähte und kriminell verschlüsselte Daten zudem an Dritte verkaufen oder drohen damit, wodurch die Vertraulichkeit der personenbezogenen Daten nicht mehr gewährleistet ist. Auch das ist ein Verstoß gegen die EU-DSGVO und wird mit empfindlichen Geldstrafen geahndet.

Wie können sich Unternehmen vor einem Ransomware-Angriff schützen?
Die gute Nachricht ist: Unternehmen und Behörden können sich vor Ransomware schützen bzw. die Gefahr eines Angriffs minimieren. Und zwar mit folgenden Maßnahmen:

- Sicherheitslücken schließen: Softwarehersteller veröffentlichen regelmäßig so genannte Patches. Mir diesen Programmkorrekturen lassen sich bekannte Fehler in Programmen ausbessern oder Sicherheitslücken schließen. Patches sollten regelmäßig und zeitnah auf alle Geräte im IT-Netzwerk eines Unternehmens aufgespielt werden. Dies ist die beste Absicherung gegen jede Art von Hacking-Versuchen, also auch gegen Ransomware. Regelmäßige Software-Updates sind ein weiterer wichtiger Schutzmechanismus gegen Cyberangriffe und Ransomware.

- Keine veralteten Systeme: Das Alter der Geräte spielt eine wichtige Rolle für die Netzwerksicherheit. Veraltete Systeme mit nicht mehr unterstützten Betriebssystemen – wie Windows XP – sollten keinesfalls in einem mit dem Internet verbundenen Netzwerk laufen.

- Vertrauensvolle Links nutzen: Anhänge oder Links, die nicht zweifelsfrei sicherer Herkunft sind, sollten auf keinen Fall geöffnet werden. Die Mitarbeiter müssen entsprechend geschult werden.

- Verifizierte Download-Quellen: Mitarbeiter sollten niemals Programme aus dem Internet herunterladen, die nicht von verifizierten Stellen angeboten sind.

- Daten mit Backups sichern: Regelmäßige Backups auf externen Datenträgern sichern den Zugang zu unternehmenskritischen Daten.

Zusätzlich gibt es eine Reihe von sehr wirksamen IT-Sicherheitstechnologien mit denen sich Ransomware-Angriffe abwehren lassen.

- **Der wichtigste Schutz ist die Absicherung des Internetzugangs.** Denn das Internet ist für Angreifer das Einfallstor Nummer Eins. Möglich ist das mit einem virtuellen Browser. Dieser erlaubt das Surfen im Internet, ohne, dass Hacker Zugriff auf die Unternehmensnetzwerke erlangen können. Der „R&S®Browser in the Box“ von Rohde & Schwarz Cybersecurity schließt die Sicherheitslücke „Internet“, indem er eine „digitale“ Quarantäne für Hackerangriffe ermöglicht: Die Ransomware-Software wird isoliert, bevor sie ausgeführt werden kann. Dieser Mechanismus schützt auch vor Angriffen via E-Mail-Anhängen oder Webkonferenzen mit Mikrofonnutzung und Webcam-Unterstützung. Der Schutz des „R&S®Browser in the Box“ wirkt sogar in beide Richtungen: Es kann keine Schadsoftware über das Internet auf den Rechner gelangen – aber auch selbst, wenn Malware auf einen anderen Weg auf den PC gelangt, ist es nicht möglich, Daten über das Internet abzugreifen (Data Leakage Prevention). Weitere Informationen: https://www.rohde-schwarz.com/de/produkte/cybersicherheit/secure-web-browser/secure-web-browser_232366.html

- **Remote-Arbeit & Homeoffice absichern:** Nutzen Remote-Arbeitende das Internet über private oder öffentliche WiFi-Netzwerke oder andere ungesicherte Netze, können ihre Endgeräte infiziert oder kompromittiert werden. Wenn sie dann später mit demselben Gerät auf Unternehmens- oder Behördennetzwerke zugreifen, verbreitet sich diese Infektion. Verhindern lässt sich das mit einer hochsicheren VPN-Verbindung wie dem R&S®Trusted VPN Client. Der VPN Client schafft eine sichere und verschlüsselte Verbindung über unsichere Netze, wie zum Beispiel das Internet. Weitere Informationen: https://www.rohde-schwarz.com/de/produkt/tvpnc-produkt-startseite_63493-677632.html

- **Webanwendungen schützen:** Die Online-Infrastruktur in Unternehmen wächst stetig und webbasierte Anwendungen gehören längst zum Alltag. Doch sie erhöhen die Zahl der möglichen Sicherheitslücken. Mit einer Web Application Firewall lassen sich solche Webanwendungen überwachen und rechtzeitig patchen. Weitere Informationen: https://www.rohde-schwarz.com/de/produkte/cybersicherheit/web-application-firewall/web-application-firewall_250809.html

Ansprechpartner:
Eva Wagenbach, Tel.: +49 (0) 221 801087 89, Fax: +49 (0)221 801087 77, E-Mail: ew@moeller-pr.de
Kontakt für Leser:
Esther Ecke, Tel.: +49 (0) 30 65 884 - 222, E-Mail: pr-cybersecurity@rohde-schwarz.com

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity ist ein führendes IT-Sicherheitsunternehmen, das digitale Informationen und Geschäftsprozesse von Unternehmen und öffentlichen Institutionen weltweit vor Cyberangriffen schützt. Der IT-Sicherheitsexperte bietet innovative Datensicherheitslösungen für Cloud-Umgebungen, erweiterte Sicherheit für Websites, Webanwendungen und Webservices sowie Netzwerkverschlüsselung und Endpoint-Sicherheit. Die vertrauenswürdigen Sicherheitslösungen werden nach dem Security-by-Design-Ansatz entwickelt und verhindern Cyberangriffe proaktiv. Weitere Informationen unter www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz

Der Technologiekonzern Rohde & Schwarz zählt mit seinen führenden Lösungen aus den Bereichen Test & Measurement, Technology Systems sowie Networks & Cybersecurity zu den Wegbereitern einer sicheren und vernetzten Welt. Vor mehr als 85 Jahren gegründet, ist der Konzern für seine Kunden aus Wirtschaft und hoheitlichem Sektor ein verlässlicher Partner rund um den Globus. Zum 30. Juni 2020 betrug die weltweite Zahl der Mitarbeitenden rund 12.300. Der unabhängige Konzern erwirtschaftete im Geschäftsjahr 2019/2020 (Juli bis Juni) einen Umsatz von 2,58 Milliarden Euro. Firmensitz ist München.