ROHDE&SCHWARZ

PRESSEINFORMATION

München, 2. November 2021

Cybercrime: 5 aktuelle Angriffstrends

Der aktuelle BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2021“ warnt, dass die Gefahr für Unternehmen drastisch zunimmt, von Cyberattacken getroffen zu werden. Vor allem Kritische Infrastrukturen und finanzstarke Unternehmen seien gefährdet. Rohde & Schwarz Cybersecurity fasst die fünf wichtigsten neuen Angriffstrends zusammen und erklärt, wie man sich schützen kann.

1. Neue Erpressungsvarianten

In den vergangenen zwölf Monaten haben sich cyberkriminelle Erpressungsmethoden spürbar ausgeweitet – das ist ein zentrales Ergebnis des BSI-Berichtes „Die Lage der IT-Sicherheit in Deutschland 2021“. Solche Ransomware-Angriffe spielen seit mehreren Jahren eine zunehmende Rolle bei der Bedrohung von Unternehmen. Das BKA bezeichnete in seinem aktuellen Lagebericht Ransomware-Angriffe sogar als die größte Cybercrime-Bedrohung für deutsche Unternehmen und öffentliche Einrichtungen überhaupt. Bei einem Ransomware-Angriff verlangen Cyberkriminelle ein Lösegeld, ehe sie zuvor verschlüsselte Daten wieder freigeben.

Das BSI erkennt aber auch neue Varianten der Erpressungsangriffe. Laut aktuellem Lagebericht nehmen auch Schutzgeld- und Schweigegelderpressungen zu. Bereits im Herbst 2020 sei eine weltweite Kampagne von Cybererpressern zu beobachten gewesen, die unter Androhung von Distributed-Denial-of-Service-Angriffen (DDoS-Angriffen) Schutzgelder von zahlungskräftigen Opfern erpressten. Bei DDoS-Angriffen werden Webseiten so stark mit Anfragen attackiert, dass sie nicht mehr erreichbar sind. Auch kommt es vermehrt zu Schweigegelderpressungen, bei denen Daten nicht mehr nur verschlüsselt, sondern auch abgezogen werden. Die Angreifer drohen mit der Veröffentlichung der Daten, falls nicht gezahlt wird.

2. Erpresser wählen finanzstarke Opfer gezielt aus

Als „Big Game Hunting“ – Großwildjagd – wird der gezielte Erpressungsangriff auf finanzstarke Unternehmen bezeichnet. Die Höhe des Lösegelds machten die Angreifer dabei beispielsweise an öffentlich verfügbaren Informationen über ihre Opfer, wie etwa der Unternehmensgröße oder den Quartalszahlen fest, schreibt das BSI in seinem Bericht. Außerdem würden Netzwerke von Unternehmen vor dem eigentlichen Angriff ausspioniert, um geeignete Ziele auszumachen. Dabei kommen mehrstufige Angriffsstrategien zum Einsatz. Das BSI beschreibt diese wie folgt: Zunächst wird der Trojaner Emotet eingeschleust. Er dient als Türöffner. Daraufhin wird die Schadsoftware „Trickbot“ nachgeladen, um das Netzwerk auszuspionieren, Passwörter auszuspähen und Konten einzusehen. Bei besonders lohnenswerten Zielen wurde dann die Ransomware „Ryuk“ aufgespielt und Lösegeld erpresst. Clemens A. Schulz von Rohde & Schwarz Cybersecurity warnt: „Der Emotet-Virus ist zwar inzwischen stillgelegt. Es ist jedoch nur eine Frage der Zeit, bis neue – womöglich noch mächtigere – Varianten solcher Türöffner auftauchen.“

3. Massenhaft neue Virusvarianten

Laut BSI nahm die Zahl neuer Schadprogrammvarianten im letzten Berichtszeitraum täglich um durchschnittlich etwas mehr als 394.000 zu. Das entspricht einer Steigerung von 22 Prozent. Zeitweise wurden Spitzenwerte von täglich 553.000 neuen Varianten erreicht. Diese Zahlen machen deutlich, wie stark der Cybercrime-Markt gewachsen ist und wie professionell die Akteure vorgehen. Schulz erklärt, warum Varianten so gefährlich sind: „Gängige Firewalls und Antivirenprogramme können nur Malware stoppen, die ihnen bereits bekannt ist. Je größer die Zahl neuer und unbekannter Angriffsarten, desto größer ist die Wahrscheinlichkeit, dass diese unbemerkt in die IT-Netze von Unternehmen gelangen.“

4. Angreifer setzen auf Doppelschlag

Das BSI hat beobachtet, dass Angreifer während eines laufenden Angriffs zusätzliche Angriffe auf ein Unternehmen starten. So setzen einzelne Angreifer etwa während der Verhandlung eines Lösegelds zusätzlich DDoS-Angriffe ein, um das Opfer weiter unter Druck zu setzen. Wenn beispielsweise ein Online-Versandhändler aufgrund eines Ransomware-Angriffs auf eine Webpräsenz ausweicht, die weniger gegen DDoS-Angriffe geschützt ist, würde ein DDoS-Angriff auf diese Präsenz die Bewältigung des Ransomware-Angriffs noch zusätzlich erschweren.

5. Kritische Infrastrukturen besonders gefährdet

Das BSI nennt mehrere Beispiele, bei denen Kritische Infrastrukturen (KRITIS) in jüngerer Zeit schwer von einem Cyberangriff getroffen wurden. So erfolgte im September vorigen Jahres der Angriff auf das Universitätsklinikum Düsseldorf. Mit gravierenden Konsequenzen: Das Krankenhaus musste sich für 13 Tage von der Notfallversorgung abmelden. Ein weiteres spektakuläres Beispiel war der Angriff auf den Pipeline-Betreiber „Colonial Pipeline“ im Mai dieses Jahres – mit immensen Auswirkungen auf die Versorgungslage mit Treibstoff in den USA. **Eine aktuelle Studie von Techconsult** unterstreicht die hohe Gefährdung von KRITIS-Unternehmen: Demnach sind bereits 35 Prozent aller Unternehmen, die zu den KRITIS zählen, in den vergangenen zwölf Monaten Opfer eines Angriffs aus dem Internet geworden.

Wie können sich Unternehmen vor diesen Angriffstrends schützen?

Die gute Nachricht ist: Man kann sich gegen diese neuen Cybercrime-Attacken schützen. Eine zentrale Rolle spielt dabei die Absicherung des Internets – denn 70 Prozent der Hackerangriffe kommen aus dem World Wide Web. Der beste Schutz vor Angriffen aus dem Internet ist ein virtueller Browser, wie der R&S®Browser in the Box. Kommt dieser zum Einsatz, haben auch neue Virusvarianten keine Chance, denn die Lösung setzt nicht auf ein reaktives Erkennen und Abwehren, sondern auf eine proaktive Isolation. „Auf keinen Fall sollten Unternehmen alleine auf die Vorsicht der Mitarbeiter setzen“, warnt Schulz. „E-Mails mit schädlichen Anhängen werden immer professioneller. Der Fehler eines einzigen Mitarbeiters, der einen solchen Anhang versehentlich öffnet, kann dazu führen, dass ein ganzes Unternehmen oder eine Behörde offline genommen werden muss.“

Neben der Absicherung des Internets sollten weitere Schutzmaßnahmen vorgenommen werden – bspw. die Verschlüsselung der Endgeräte, eine hochsichere VPN-Verbindung und die Absicherung des heimischen WLANs. Eine Web Application Firewall verhindert zudem, dass die Website zum Einfallstor für Ransomware wird und sie kann DDos-Angriffe stoppen. „Mit einem solchen 360-Grad-Schutz erschweren Unternehmen einen Angriff erheblich“, betont Schulz. „Die Täter werden abgeschreckt und suchen sich stattdessen ein leichteres Opfer.“

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 hoheitlichen und privatwirtschaftlichen Kunden mit besonderen Sicherheits- und Zulassungsanforderungen Schutz vor den sich stetig ändernden Cyberbedrohungen bietet. Der Pionier hochsicherer Verschlüsselungstechnologien liefert Hochgeschwindigkeits-Netzwerkverschlüsselung, zero-trust-basierte Endpoint-Sicherheit sowie innovative Datenschutzlösungen für Cloud-Umgebungen und Webanwendungen. Die meisten dieser Produkte sind vom BSI für die Absicherung VS-NfD-eingestufter Daten zugelassen. Diese vertrauenswürdigen Sicherheitslösungen unterstützen die Anwender auf dem Weg in eine sichere und digitalisierte Welt und leisten damit einen wesentlichen Beitrag zur digitalen Souveränität. 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.