Wie Cyberkriminelle mit Erpressungssoftware Unternehmen angreifen.

Die 7 häufigsten Wege.

Die Gefahr eines „Ransomware“ Angriffs auf österreichische Unternehmen sowie Behörden und staatsnahe Unternehmen wird zunehmend größer. Der Begriff (deutsch: Erpressungssoftware) steht für ein Schadprogramm, das Rechner bis zur Zahlung einer Summe sperrt. Das Besondere ist, dass Akteure parallel dazu mit Benutzern in Kontakt treten (Social Engineering) und das Ziel verfolgen, Daten auf allen Computern eines IT-Netzwerkes zu verschlüsseln. So werden ganze Unternehmen und Behörden lahmgelegt. Hacker verkaufen heute maßgeschneiderte Ransomware an andere Cyberkriminelle und erhalten eine Gewinnbeteiligung. Diese Arbeitsteilung führt zu innovativeren Liefermethoden und mehr Angriffen. Wir geben Ihnen hier einen Überblick über die häufigsten Ransomware-Angriffe.

1. PHISHING & SOCIAL ENGINEERING

Die häufigste Methode einen Endpunkt mit Ransomware zu infizieren, sind Phishing-E-Mails. Cyberkriminelle nutzen dafür personalisierte Informationen, um Vertrauen zu gewinnen. Ihr Ziel ist es Opfer dazu zu bringen, Anhänge zu öffnen oder auf Links zu klicken, um bösartige Dateien herunterzuladen.

2. KOMPROMITTIERTE WEBSITES

Hier genügt es, wenn das Opfer eine Website besucht, die auf eine andere Seite umleitet. Auf dieser wird man aufgefordert eine schädliche Software herunterzuladen. Solche Webumleitungen sind besonders schwer zu erkennen.

3. MALVERTISING & WEB BROWSER

Im Fall ungepatchter Sicherheitslücken im Browser können Cyberkriminelle auch über gewöhnliche Werbung auf Websites einen bösartigen Code einfügen, der die Ransomware herunterlädt, sobald die Werbung erscheint.

4. EXPLOIT-KITS UND BENUTZERDEFINIERTE MALWARE

Exploit-Kits sind bösartige Toolkits mit Schadcodes, die auf Schwachstellen in Browser-Plugins wie Java und Adobe Flash abzielen. Bekannte Ransomware wie „Locky“ und „CryptoWall“ wurden über Exploit-Kits auf gefälschten Websites verbreitet.

5. INFIZIERTE DATEIEN UND ANWENDUNGEN HERUNTERLADEN

Jede downloadbare Datei kann für Ransomware verwendet werden. Kein Wunder, dass Software auf illegalen Tauschbörsen häufig betroffen ist. Oft nutzen Hacker aber auch legitime Websites, um infizierte Dateien anzubieten.

6. MESSAGING-ANWENDUNGEN ALS INFEKTIONSVEKTOREN

In Messaging-Apps wie WhatsApp und Facebook Messenger tritt Ransomware als Grafik (SVG) getarnt auf. Ruft man die infizierte Bilddatei auf, leitet sie auf eine scheinbar legitime Website weiter. Diese fordert Nutzer auf, eine Installation zu akzeptieren, die Schadsoftware an Kontakte des Opfers weiterleitet.

7. PASSWORTATTACKEN AUF TERMINALSERVICES

Ransomware wie „SamSam“ kompromittiert Endgeräte direkt. Dafür startet sie einen Brute-Force-Angriff (Zugriff mit User- und Passwortkombinationen). Haben die Angreifer Erfolg, erlangen sie volle Kontrolle über den Computer und können die Ransomware einschleusen.

DIE BESTE HILFE GEGEN RANSOMEWARE: CYBERDEFENCE AS A SERVICE

Das Security Team der CYBERCONTACT-CERT GmbH erkennt in Echtzeit den Eintritt der Erpressungssoftware und stoppt, klassifiziert und entfernt sie frühzeitig. Anschließend stellt es in wenigen Minuten den Ursprungszustand der Systeme her und sorgt dafür, dass das Unternehmen wieder voll geschäftsfähig ist. Es sichert Beweise, dokumentiert den Ablauf des Angriffs und liefert Maßnahmen zur Optimierung der Sicherheitsinfrastruktur sowie präventive Cyberdefence Intelligence Services. **Mehr auf cybercontact.at**

Alexander Franz, Geschäftsführer Cybercontact

cyber[contact].at
INFORMATION SECURITY & CERT-TEAM