it-daily.net

Kriegsgeschehen in der Ukraine erhöht weltweites Risiko für Cyberangriffe

15. März 2022

Der russische Angriffskrieg gegen die Ukraine verschärft weltweit das Risiko für großflächige und gezielte Cyberattacken. Hohes Schadenspotenzial für Kritische Infrastrukturen (KRITIS) und private Unternehmen sind die Folge.

„Bereits seit der Annexion der Krim im Jahr 2014 sind verstärkt Angriffe auf wichtige Einrichtungen in der Ukraine zu beobachten, die zum Beispiel die Strom- und Wasserversorgung betreffen. Malware-Attacken wie BlackEnergy, Industroyer und NotPetya haben gezeigt, wie zerstörerisch sie sein können“, sagt Ulrich Brüll, Director Cyber Resilience & Consulting Services bei der xevIT GmbH, Mitgliedsunternehmen des

Digitalisierungsverbunds Innovation Alliance. Marcel Sievers, Information Security Specialist bei der pco GmbH & Co. KG, ergänzt: „Es ist zu befürchten, dass die neue militärische Eskalation Cyberrisiken auf eine neue Stufe hebt, auch wenn sich diese aktuell noch eher auf die Ukraine beschränken."

xevIT und pco sind Mitgliedsunternehmen der Innovation Alliance, die als Kompetenzverbund zu IT-Sicherheitskonzepten berat und die präventive und fortlaufende Überwachung und Bekämpfung von Cyberattacken begleitet.

Incident Response wird wichtiger

Der Angriffserkennung kommt derzeit eine eminente Rolle zu. Mechanismen, um Anomalien und Angriffe frühzeitig zu erkennen, fehlen jedoch noch breitflächig – nicht nur im KRITIS-Sektor, sondern in vielen Wirtschaftsunternehmen. „Entsprechende Softwarelösungen wie SIEM-Systeme sind teils vorhanden, um volle Sichtbarkeit auf Netzwerkaktivitäten zu erlangen. Es mangelt aber vielerorts an Spezialisten, die Incidents analysieren und entsprechende Reaktionen ableiten", sagt Brüll. Laut Innovation Alliance betrifft die derzeitige Sicherheitslage fast jedes Wirtschaftsunternehmen. Während öffentliche Betreiber attackiert werden, um Versorgungssysteme lahmzulegen, nehmen die Angreifer private Unternehmen ins Visier, um mit Ransomware Daten zu verschlüsseln und zu erpressen.

Nur 20 Prozent der Krankenhäuser gelten als KRITIS-Betreiber

Betreiber Kritischer Infrastrukturen sind laut IT-Sicherheitsgesetz dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der von ihnen betriebenen kritischen Strukturen zu treffen. Allerdings zählen derzeit circa 80 Prozent der Krankenhäuser in Deutschland aufgrund der Höhe der durchgeführten stationären Patientenbehandlungen nicht zum KRITIS-Sektor und unterliegen damit nicht den Anforderungen aus dem IT-Sicherheitsgesetz. Bei Angriffen auf Gesundheitseinrichtungen nutzen Cyberkriminelle verstärkt vernetzte medizintechnische Geräte wie Operationsroboter als Brückenköpfe, um IT-Infrastrukturen zu kontrollieren. Mit leistungsfähigen Netzwerkzugangslösungen lassen sich Netzwerke in Zonen isolieren und effektive Zugangskontrollen ermöglichen. Ziel ist es, Angriffsflächen zu verkleinern und die Verbreitung von Angriffen so einzuschränken.

Netzwerkzugänge absichern, User sensibilisieren

Da viele Angriffe die Interaktion mit einem User benötigen, empfiehlt die Innovation Alliance, verstärkt User-Awareness-Schulungen durchzuführen. So lassen sich Mitarbeiter in Bezug auf die erhöhte Gefahrenstufe sensibilisieren.

Auch eine gut gewartete IT-Infrastruktur, aktuelle Webserver, Notfallpläne im Fall eines Cyberangriffs sowie die Einführung von Multi-Faktor-Authentifizierungen für Außenzugänge sind wirksame Maßnahmen. Ausgelagerte Security Operations Center, sogenannte SOC, helfen dabei sowie auch bei der Durchführung von Penetrationtests und einem wirksamen Incident Response Management. „Das Gros der IT-Dienstleister ist derzeit sehr gut ausgelastet. Wir empfehlen Firmen, Serviceverträge abzuschließen, um im Security-Notfall zügig Hilfe zu erhalten“, sagt Sievers.

www.innovationalliance.de