netzwerk südbaden

Wie geht’s?

Schwerpunkt Gesundheit

Februar 2024 | Preis: 6,00 Euro | E 2014 www.netzwerk-suedbaden.de

9 770262 777279 02

Das regionale Wirtschaftsmagazin

CONTINUM

ALARMSTUFE ROT IM CYBERSPACE

Foto: ZVG

Der aktuelle Bericht des Bundesinstituts für Sicherheit in der Informationstechnik (BSI) enthüllt eine historische Bedrohungslage und Evolution der Cyberkriminalität in Deutschland.

Das Lagebild zur Cybersicherheit in Deutschland skizziert eine besorgniserregende Situation, wie der jüngste BSI-Lagebericht aufzeigt. Die Bedrohung im Cyberraum hat ein historisch hohes Niveau erreicht. Ransomware bleibt die größte Bedrohung. Allerdings lässt sich eine Verschiebung der Angriffsziele beobachten. Es werden nicht mehr nur große Unternehmen, sondern zunehmend auch kleinere Organisationen, staatliche Institutionen und Kommunen angegriffen, was direkte Auswirkungen auf Bürgerinnen und Bürger haben kann.

Bemerkenswert ist das Phänomen des organisierten Verbrechensmodells „Cybercrime-as-a-Service" (CaaS), das eine Professionalisierung der virtuellen Verbrechen begünstigt. Cyberkriminelle verkaufen dabei ihre Werkzeuge, Fachkenntnisse und Dienstleistungen an andere. Damit können auch Personen ohne spezielle technische Fähigkeiten cyberkriminell tätig werden. Gegen Bezahlung im sogenannten Darknet bekommen sie Zugriff auf eine Vielzahl illegaler Dienstleistungen, wie finanziellen Betrug, Malware- oder DDoS-Angriffe, Ransomware, Phishing und Social Engineering. Für solche kriminellen Dienstleistungen sind CaaS-Anbieter strukturell nach dem Vorbild legaler Unternehmen aufgebaut und bieten alles für Angriffe an – vom technischen Support bis zu Hosting-Diensten.

Der BSI-Lagebericht 2023 hebt mehrere kritische Punkte und Lösungsansätze hervor. Eine Checkliste:

Ransomware: Sie bleibt die dominierende Bedrohung, mit durchschnittlich 250.000 neuen Schadprogramm-Varianten täglich. Es gab einen Anstieg um 24 Prozent bei identifizierten Schwachstellen in Softwareprodukten, von denen 15 Prozent als kritisch eingestuft werden.

Phishing-E-Mails: Diese stellen weiterhin ein großes Problem dar, insbesondere zur Erlangung von Authentisierungsdaten, vor allem bei Banken und Sparkassen.

Unternehmenssicherheit: Im Jahr 2023 wurden durchschnittlich alle fünf Tage Unternehmen in Deutschland verschlüsselt und zwei Ransomware-Angriffe pro Monat auf Kommunalverwaltungen oder kommunale Betriebe verzeichnet.

Cyber-Resilienz: Der Bericht betont die Wichtigkeit von gesteigerter Cyber-Resilienz und empfiehlt Standardisierung, Zentralisierung und Automatisierung zur Abwehr von Angriffen.

Präventive Maßnahmen: Empfohlen werden regelmäßige Sicherheitsupdates, zentrale Überwachung, Automatisierung der IT-Infrastruktur, Einsatz von IT-Sicherheitsprodukten wie Firewalls und Antiviren-Schutz sowie regelmäßige Datensicherungen an mehreren Standorten.

Training der Mitarbeitenden: Schulungen und Sensibilisierung der Angestellten gegenüber Schadsoftware und Phishing-E-Mails werden als beste Schutzmaßnahme hervorgehoben.

Der BSI-Bericht zur IT-Sicherheitslage in Deutschland 2023 wurde am 2. November 2023 in der Bundespressekonferenz vorgestellt. BSI-Präsidentin Claudia Plattner und Bundesinnenministerin Nancy Faeser gaben dabei einen umfassenden Überblick über aktuellen Bedrohungen im Cyberraum. Als Mitglied der Bundesarbeitsgruppe für Cybersicherheit des Wirtschaftsrats arbeitet Continum tatkräftig an der Entwicklung von solchen gemeinsamen Lösungsansätzen und Sicherheitskonzepten mit, um der wachsenden Bedrohung entgegenzuwirken.

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung der Continum AG. Das Freiburger Hostingunternehmen ist AWS-, Microsoft Azure sowie IONOS Partner und unterstützt Unternehmen auf dem sicheren Weg in die Cloud