Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

ÜBER GEFÜHLE IN DER WIRTSCHAFT ● PORTRÄT EINES ALLEINUNTERHALTERS ● STIMMUNG AUF DEM ARBEITSMARKT IST GEKIPPT ● CLAAS LAHMANN: WIE ARBEIT GLÜCKLICH MACHT ● P3: DAS DILEMMA DER GEMEINNÜTZIGKEIT ● JONI STUDIO: EIN KNOPF FÜR ALLE ● JAFFA: KOCHEN GEGEN DEN HASS ● WIE DIE WEINBRANCHE DEM TREND TROTZT ● ERFOLGREICHES PILOTPROJEKT: REGION DER LEBENSRETTER

9 770262 777279 02

#02/2025
E2014
6,50 Euro

Am liebsten gut

Schwerpunkt Stimmung

Die unsichtbare Gefahr wächst weiter

Dass viele Betriebe derzeit ihren Fokus auf Effizienz und Kosteneinsparungen richten, nutzen Cyberkriminelle gezielt aus. Der jüngste BSI-Lagebericht zeigt eindrücklich, dass sich die Bedrohungslage im digitalen Raum weiter verschärft hat.

Tobias Leinweber ist als Nachfolger von Julian Sayer Vorstand für Vertrieb, Marketing und Entwicklung der Continum AG. Neben eignen Cloud-Lösungen made in Germany ist der Freiburger Clouddienstleister Azure, AWS- sowie IONOS Partner und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.

Schadsoftware, Phishing-Kampagnen und Angriffstools sind mittlerweile über das Darknet als Dienstleistung erhältlich, Cybercrime-as-a-Service sozusagen. Dadurch sinkt die Einstiegshürde für Cyberkriminelle drastisch, denn so können auch technisch weniger versierte Akteure hochentwickelte Angriffe durchführen. Gleichzeitig treibt künstliche Intelligenz diese Entwicklung weiter voran. KI-generierte Phishing-Mails sind kaum noch von echten zu unterscheiden, Deepfake-Technologien erleichtern Identitätsdiebstahl, und automatisierte Schadsoftware kann sich unbemerkt in Netzwerken verbreiten. Auch APT-Gruppen (Advanced Persistent Threats) intensivieren, oft mit staatlicher Unterstützung, ihre Aktivitäten und setzen Unternehmen gezielt unter Druck.

Als besonders bedrohlich hebt der Lagebericht 2024 des Bundesamts für Sicherheit in der Informationstechnik (BSI) Folgendes hervor: Bei Ransomware sind die Angriffe zunehmend professionell organisiert. Kriminelle agieren arbeitsteilig als Betreiber, Initial Access Broker oder Affiliates, wobei Zugangsdaten gezielt gehandelt werden. Auch im Bezug auf DDoS (Distributed Denial-of-Service) nehmen Angriffe in Umfang und Intensität stark zu. Selbst große Infrastrukturbetreiber wurden bereits attackiert, was die Verwundbarkeit von IT-Systemen verdeutlicht. Schließlich hebt das BSI Lieferkettenangriffe hervor. Mittelständische Unternehmen werden als Einfallstor genutzt, um größere Organisationen zu infiltrieren und zu kompromittieren.

Regulatorische Maßnahmen wie NIS-2, DORA oder der Cyber Resilience Act setzen neue Maßstäbe und sollen das allgemeine Cybersicherheitsniveau anheben. NIS-2 nimmt dabei deutlich mehr Unternehmen in die Pflicht als frühere Vorschriften. Betroffen sind große und mittlere Betriebe aus 18 kritischen Sektoren wie Energie, Finanzen, Logistik und digitale Dienste. Zudem müssen Unternehmen sicherstellen, dass auch ihre Lieferketten die neuen Sicherheitsstandards erfüllen, was viele Dienstleister und Zulieferer in die Pflicht nimmt.

Solche regulatorischen Vorgaben schaffen eine solide Grundlage. Es reicht aber nicht aus, sich allein darauf zu verlassen. Unternehmen sollten IT-Sicherheit als strategischen Vorteil begreifen, aktiv in ihre Resilienz investieren und ihre Mitarbeitenden für Risiken sensibilisieren. Angesichts der aktuellen Lage ist nicht die Frage, ob ein Angriff stattfindet, sondern wann. Wer vorbereitet ist, kann wirtschaftliche und operative Schäden minimieren, den Geschäftsbetrieb im Ernstfall schnell wiederherstellen und sich langfristig einen Wettbewerbsvorteil sichern. Der BSI-Lagebericht ist erneut ein Weckruf – und eine klare Aufforderung zum Handeln.

Foto: PR