Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

MANUFAKTUREN: KLEINE CHARGEN, GROSSE LEIDENSCHAFT ● OLIVIER NASTI: JÄGER DES GUTEN GESCHMACKS ● BETRIEBS-RESTAURANTS: GUT ESSEN, BESSER SCHAFFEN ● OBSTGROSSMARKT MITTELBADEN: APFEL AUF ACHSE ● WASCHBÄR: DAS ENDE EINES PIONIERS ● KNOLL FEINMECHANIK: AUTOMATISIERUNG FÜR DEN SKISCHLIFF ● SEILEREI HAAS: HANDWERK MIT HALT ● DIETENBACH: „WIR WERDEN ALLE BRAUCHEN“ ● AUSSTELLUNG: GABRIELE ENGELHARDTS KEHLER BERGE

9 770262 777279 10

#10/2025
E2014
6,50 Euro

Was uns schmeckt

Schwerpunkt Kulinarik

Sicherheit beginnt bei jedem Einzelnen

Der Oktober steht im Zeichen der Cyber sicherheit: Der Cyber Security Awareness Month ruft dazu auf, gemeinsam Verant- wortung zu übernehmen. Denn jede(r) kann einen Beitrag leisten, die Welt ein Stück sicherer zu machen, zumal die digitale Bedrohung immer weiter wächst.

Tobias Leinweber ist 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.

Der jüngste Cybervorfall mit massiven Einschränkungen im Flugverkehr hat erneut gezeigt, wie real die Bedrohung durch Cyberangriffe ist. Die Auswirkungen sind längst nicht mehr nur technischer Natur – sie treffen unsere Wirtschaft, unsere Infrastruktur und unseren Alltag. Der Lagebericht 2024 des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eindeutig: Die Bedrohungslage in Deutschland wird als „angespannt bis kritisch" eingeschätzt. Während große Konzerne massiv in ihre Sicherheitsarchitektur investieren, geraten zunehmend kleine und mittelständische Unternehmen in den Fokus professioneller Angreifer. Ransomware-Angriffe zählen weiterhin zu den größten Gefahren, ebenso wie Phishing-Kampagnen, infizierte E-Mail-Anhänge und sogenannte Zero-Day-Exploits, bei denen bisher unbekannte Schwachstellen gezielt ausgenutzt werden. Viele Vorfälle entstehen nicht durch technische Mängel - sondern durch kleine menschliche Fehler aufgrund von Unwissenheit – mit oft gravierenden Folgen.

Denn Cybersicherheit ist keine rein technische Herausforderung mehr. Sie beginnt bei den Menschen: mit jedem Klick, jedem Passwort, jeder Entscheidung, jedem herausgezögertem Softwareupdate. Und sie endet nicht in der IT-Abteilung. Gerade in Zeiten hybrider Arbeitsmodelle, zunehmender Digitalisierung und Vernetzung, wachsender Angriffsflächen und immer raffinierterer Angriffe ist es entscheidend, dass alle im Unternehmen Verantwortung übernehmen - von der Werkstudentin bis zum Geschäftsführer.

Deshalb muss Cybersicherheit im Alltag mitgedacht werden. Die Wahl sicherer Passwörter, der bewusste Umgang mit sensiblen Daten, das kritische Hinterfragen verdächtiger E-Mails: All das trägt zur Sicherheit bei. Doch es funktioniert nur, wenn Cybersicherheit im Unternehmen sichtbar und verständlich kommuniziert wird. Sie darf kein Tabuthema sein, sondern muss aktiv angesprochen, erklärt und regelmäßig trainiert werden. Nur wer versteht, worauf es ankommt, kann im Ernstfall richtig handeln.

Gleichzeitig gilt: Awareness allein reicht nicht aus. Denn auch bei hoher Aufmerksamkeit lassen sich nicht alle Risiken vermeiden. Entscheidend ist, wie gut ein Unternehmen auf Sicherheitsvorfälle vorbereitet ist – organisatorisch und technisch. Wer schnell reagieren, Schäden begrenzen und Systeme wiederherstellen kann, schützt nicht nur Daten, sondern sichert auch den laufenden Betrieb und die eigene Reputation.

Dazu braucht es klare Prozesse, geschulte Zuständigkeiten und moderne Infrastrukturen, die Ausfallsicherheit und Wiederherstellbarkeit mitdenken. Backup- und Recovery-Strategien, Netzwerksegmentierung, Monitoring, Alarmierung und ein funktionierendes Notfallmanagement sind heute keine Kür mehr, sondern Pflichtbestandteile einer verantwortungsvollen Cyber-Resilience-Strategie. Wem dazu die Kapazität fehlt, der sollte auf Dienstleister setzen, die sich tagtäglich genau um diese Themen kümmern.

Der Cyber Security Awareness Month ist weit mehr als eine PR-Kampagne. Er ist eine Einladung zum Umdenken. Wer Cybersicherheit nicht nur als technische Maßnahme, sondern als gesamtunternehmerische Aufgabe versteht, stärkt langfristig Vertrauen – nach innen wie nach außen. Denn am Ende beginnt Cybersicherheit nicht mit einer Software oder einem Dienstleister. Sie beginnt bei jedem Einzelnen. Und sie wirkt am effektivsten, wenn alle mitmachen.

Fotos: PR