Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

JULIAN SCHUSTER: DER WUNSCHKANDIDAT ● VAKANT: DEM SC FEHLT DERZEIT EIN FUSSBALLGOTT ● „WIE PROFIS“: INTERVIEW MIT ZWEI KAPITÄNINNEN ● INDUSTRIE 4.0: CONTINENTAL-TOCHTER WÄCHST IN FREIBURG ● FURTWANGEN: KLEINE STADT MIT GROSSEM ANGEBOT ● BUNT, STARK, GROSS: KÜNSTLERINNEN IN RIEGEL ● KONJUNKTUR: DER INDUSTRIE GEHT ES NICHT GUT ● MÜLLHEIM: VERDACHT DER ABZOCKE

9 770262 777279 08

#08/2024
E2014
6,50 Euro

Die alte Bescheidenheit

Schwerpunkt SC Freiburg

Strengere Maßnahmen, höhere Strafen

Die Europäische Union setzt der wachsenden Bedrohung im Netz eine Weiterentwicklung ihrer Network and Information Security Directive (NIS-2) entgegen. Ist das ein Boost für unsere Sicherheit oder ein neues Bürokratiemonster?

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.

Die Cybersicherheitslage hat sich aufgrund globaler Konflikte in einer immer digitaleren Welt enorm zugespitzt. Innerhalb der EU ist das Cyber-Sicherheitsniveau in vielen Bereichen oft unzureichend. Abhilfe soll nun die NIS-2 Richtlinie schaffen. Tut sie das?

Wen betrifft NIS-2?

In erster Linie richtet sich NIS-2 an große und mittlere Einrichtungen beziehungsweise an Unternehmen aus insgesamt 18 Sektoren mit entweder hoher Kritikalität, also beispielsweise Energie und Bankenwesen, mit sonstiger Kritikalität, unter anderem Post- und Kurierdienste, oder Anbieter digitaler Dienste. Als mittleres Unternehmen gelten dabei Einrichtungen, die mindestens 50 Mitarbeitende beschäftigen oder einen Jahresumsatz von mehr als 10 Millionen Euro erzielen. Doch die Richtlinie geht noch einen entscheidenden Schritt weiter.

Aufgrund der wachsenden Bedrohung durch Supply-Chain-Attacken müssen betroffene Einrichtungen künftig sicherstellen, dass auch Unternehmen in ihrer Lieferkette den Anforderungen der NIS-2 gerecht werden. Auch Lieferanten und Dienstleister betroffener Unternehmen werden somit künftig indirekt die Standards von NIS-2 erfüllen müssen, unabhängig von ihrer Größe oder ihrem Sektor. Damit sind deutlich mehr Unternehmen betroffen als bei der bisherigen NIS-Verordnung.

Was bedeutet NIS-2 für betroffene Unternehmen?

Diese direkt und indirekt betroffenen Unternehmen müssen höheren Anforderungen im Hinblick auf Risikomanagement, Sicherheitsmaßnahmen und Business Continuity gerecht werden. Das heißt, sie müssen erstens robuste Sicherheitsvorkehrungen implementieren und regelmäßig aktualisieren – einschließlich Prävention, Detektion und Reaktion auf Cybervorfälle. Zweitens erhöht sich die Verantwortung der Geschäftsführung. Sie ist für die Einhaltung der Cybersicherheitsanforderungen verantwortlich und muss sicherstellen, dass alle notwendigen Maßnahmen zur Erfüllung der NIS-2-Anforderungen umgesetzt werden. Drittens gibt es Meldepflichten. Sicherheitsvorfälle müssen schnell an die zuständigen Behörden gemeldet werden, was effiziente Prozesse und klare Kommunikationswege erfordert. Den Behörden ermöglicht dies ein umfassendes Lagebild. Und viertens drohen bei Verstößen empfindliche Geldstrafen und Sanktionen. So sehen sich „besonders wichtige“ Unternehmen mit Strafzahlungen in Höhe von mindestens 10 Millionen Euro oder 2 Prozent des weltweiten Vorjahresumsatzes konfrontiert, „wichtige“ Unternehmen mit mindestens 7 Millionen Euro oder 1,4 Prozent des weltweiten Vorjahresumsatzes.

Die Vielzahl an direkt und indirekt betroffenen Unternehmen, die strengen Maßnahmen sowie die hohen Strafen unterstreichen das Bestreben der EU, mit NIS-2 ein hohes gemeinsames Cyber-Sicherheitsniveau sicherzustellen und so den EU-Binnenmarkt zu stärken. Gerade bei den bisher nicht betroffenen ist der Handlungsbedarf groß. Mit der EU-weiten Inkraftsetzung der NIS-2-Richtlinie am 16. Januar 2023 und der Frist zur Überführung in deutsches Recht bis 17. Oktober 2024 bleibt Unternehmen nur noch wenig Zeit, die teils langwierigen notwendigen Maßnahmen zu ergreifen und sich auf die neuen Anforderungen vorzubereiten.

Foto: PR