Presseinformation

KRITIS-Studie: Cybersecurity-Bedrohung für Unternehmen wächst

[Essen, 26. April 2023] **Welchen Gefahren sind Unternehmen Kritischer Infrastrukturen (KRITIS) derzeit ausgesetzt? Wo liegen ihre größten Herausforderungen? Und welche Rolle spielen Systeme zur Angriffserkennung dabei? Um diese und weitere Fragen zu beantworten, hat das Research- und Beratungsunternehmen techconsult im Auftrag der secunet Security Networks AG mehr als 120 KRITIS-Unternehmen im Rahmen der Studie „Angriffserkennung in Unternehmen Kritischer Infrastrukturen – wie deutsche KRITIS-Unternehmen mit den steigenden IT- und OT-Risiken umgehen“ befragt.**

Die Ergebnisse zeigen, dass 79 Prozent der Unternehmen die aktuelle Bedrohungslage als wachsend bis stark wachsend einschätzen. Auch vor diesem Hintergrund hat die Bundesregierung 2021 das IT-Sicherheitsgesetz 2.0 auf den Weg gebracht, um die Bevölkerung vor Cyberangriffen und ihren Folgen zu schützen. Ab 1. Mai 2023 müssen betroffene Unternehmen den Einsatz von Systemen zur Angriffserkennung in ihrer IT-Infrastruktur, die zur Aufrechterhaltung der kritischen Versorgungsdienstleistungen unabdingbar ist, nachweisen. Obwohl solch ein System für andere Bereiche nicht verpflichtend ist, planen 71 Prozent der befragten KRITIS-Unternehmen, auch beispielsweise in der Büro-IT entsprechende Systeme zur Angriffserkennung zu etablieren. Bereits 21 Prozent haben ein derartiges System vollständig sowohl in den Pflichtbereichen als auch darüber hinaus eingeführt. 45 Prozent der Befragten planen die Einführung noch dieses Jahr und rund ein Drittel (33 Prozent) in den nächsten ein bis drei Jahren.

Presseinformation

Prävention gegen Cyberrisiken scheitert häufig an fehlender Kompetenz

59 Prozent der befragten Unternehmen stufen sich als kompetent bis sehr kompetent beim verpflichtenden Melden von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein, 56 Prozent bei der Prävention gegen Cyberrisiken. Bei jeweils über 40 Prozent der Unternehmen besteht somit noch Verbesserungspotenzial hinsichtlich der Umsetzung der gesetzlichen Meldepflicht bei Sicherheitsvorfällen an das BSI. Dabei schätzt jedes zweite befragte Unternehmen (50 Prozent), dass IT-Sicherheitsvorfälle zu Kompromittierung sensibler und kritischer Daten führen würden. 45 Prozent befürchten bei einem Vorfall den Ausfall von für das Gemeinwesen relevanten Anlagen und 46 Prozent Umsatzeinbußen.

IT-Fachkräftemangel bleibt größte Herausforderung

Mehr als jedes zweite KRITIS-Unternehmen (59 Prozent) sieht den Mangel an IT-Fachpersonal als eine der größten Herausforderungen für die kommenden zwei Jahre. Dieses Fachpersonal fehlt, um die Anpassungen und die Umsetzung der Regularien und Vorgaben zu bewältigen. Ein weiterer Schmerzpunkt ist für 44 Prozent der Befragten die Schwachstellenanalyse im Netzwerk, die jedoch essenziell für weitere Maßnahmen zur Steigerung der Abwehr von Cyberangriffen ist. Weitere Herausforderungen sind mit 30 Prozent die Absicherung von kritischen Komponenten im Internet of Things (IoT) oder Industry Control Systems (ICS), die Inbetriebnahme notwendiger Security-Lösungen (28 Prozent) sowie die Erbringung von Nachweisen zur Informationssicherheit (23 Prozent).

Über die Studie:

Die Studie „Angriffserkennung in Unternehmen Kritischer Infrastrukturen – wie deutsche KRITIS-Unternehmen mit den steigenden IT- und OT-Risiken umgehen" wurde im Januar 2023 von techconsult durchgeführt.

Presseinformation

Mit Hilfe eines strukturierten Fragebogens wurden branchenübergreifend 121 KRITIS-Unternehmen in Deutschland befragt.

Alle Ergebnisse der Studie finden Sie unter dem folgenden Link: https://www.secunet.com/studie-2023-angriffserkennung-in-unternehmen-kritischer-infrastrukturen

Sollten Sie weitere Grafiken zur Studie benötigen, steht Ihnen das secunet Presseteam gerne unter presse@secunet.com zur Verfügung.

Pressekontakt

Patrick Franitza
Pressesprecher

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen/Germany
Tel.: +49 201 5454-1234
Fax: +49 201 5454-1235
E-Mail: presse@secunet.com
http://www.secunet.com

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im SDAX gelistet und erzielte 2022 einen Umsatz von rund 347 Mio. Euro.

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

Weitere Informationen finden Sie unter www.secunet.com.