Pressemitteilung

Cybersicherheit 7. Dezember 2022

TÜV SÜD: Das sind die Cybersecurity-Trends 2023

München. Neue Gesetze und Regularien sowie geopolitische und wirtschaftliche Krisensituationen wirken sich auch auf die Cybersecurity-Maßnahmen der Unternehmen aus. Weiterbildung bleibt ein entscheidender Erfolgsfaktor. TÜV SÜD nennt aktuelle Trends in der Cybersecurity für das Jahr 2023.

„Cybergefahren sind eines der größten Risiken für Unternehmen“, sagt Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) bei TÜV SÜD. „Durch die Bedrohungslage sowie durch neue Regularien und deren Umsetzung werden Investitionen in Cybersicherheit immer wichtiger. Vor allem Kleine und Mittlere Unternehmen (KMU) achten künftig aber stärker auf die Kosteneffizienz von Cybersecurity-Lösungen“, so Ethiraj. Die folgenden Trends und Entwicklungen in der Cybersecurity werden im Jahr 2023 wichtig:

Kosteneffiziente Cybersecurity-Lösungen

Günstige und effektive Sicherheitslösungen und Services werden im Jahr 2023 stärker nachgefragt. Hier machen sich die Unsicherheit angesichts der allgemeinen Wirtschaftslage sowie negative Effekte durch Pandemie und den Ukraine-Krieg bemerkbar. Vor allem Kleine und Mittlere Unternehmen (KMU)

setzen ihr Budget für IT-Sicherheit daher gezielter ein und hinterfragen die Kosteneffizienz. Um die Lieferketten-Sicherheit zu stärken, sollten Zulieferer zudem nicht durch unterschiedliche Vorgaben zur Cybersecurity belastet werden, sondern möglichst einheitliche Sicherheitsvorgaben und Standards erfüllen.

Regulierungen: Implementierung beginnt

Nachdem einige Gesetze und Regulierungen zur Cybersecurity national und international auf den Weg gebracht wurden, beginnt nun die Phase der Umsetzung. Einige Beispiele: Die EU-Richtlinie über die Netz- und Informationssicherheit (NIS) wird ersetzt durch die NIS-2-Richtlinie, unter anderem mit strengeren Überwachungsmaßnahmen und Meldepflichten sowie EU-weit harmonisierter Sanktionen. Der Gesetzesentwurf zum European Cyber Resilience Act (CRA) schreibt EU-weit erstmalig verpflichtende Maßnahmen für die Cybersicherheit internetfähiger Geräte und Produkte vor. Ab August 2024 umfasst die EU-Verordnung zur Radio Equipment Directive (RED) zudem verpflichtend Cybersicherheit für alle Wireless-Geräte wie Mobiltelefone, Tablets oder Smartwatches. In den USA gab es eine zunehmende Zahl von Durchführungsverordnungen zur Cybersicherheit, die US-Behörden wie CISA dazu veranlassten, an der Umsetzung von Cybersicherheitsanforderungen für mehrere Branchen zu arbeiten. Für alle Regularien gilt: Unternehmen müssen prüfen, ob sie betroffen sind und wie sie entsprechende Änderungen am effizientesten durchführen. Normen und Zertifizierungen durch unabhängige Dritte werden dabei noch wichtiger mit Blick auf die länderübergreifende Umsetzung.

Kritische Infrastruktur (KRITIS) stärker im Fokus

Die Anzahl der Phishing-, Malware- und Ransomware-Attacken steigt stetig und dieser Trend wird andauern. Angesichts der zunehmenden Professionalisierung von Cyberkriminellen sowie virtueller Kriegsführung steht der Schutz Kritischer Infrastruktur deshalb weiter im Mittelpunkt, vor allem in hochsensiblen Bereichen wie Energieversorgung und Gesundheitswesen. Cyber-Resilienz ist ein wichtiger Faktor in der von US-Präsident Biden vorgelegten Nationalen Sicherheitsstrategie. In Deutschland soll ein KRITIS-Dachgesetz kommen, das durch sektorübergreifende Mindestvorgaben das Gesamtsystem widerstandsfähiger macht.

Zielgruppenorientiertes Training

Der menschliche Faktor ist nach wie vor ein neuralgischer Punkt in der Cybersecurity. Neben Technik und Prozessen sind die Mitarbeitenden das dritte relevante Element. Bisher standen vor allem breitangelegte Awareness-Schulungen für die gesamte Belegschaft im Mittelpunkt. Der Trend geht in Zukunft verstärkt zu Trainingsmaßnahmen für konkrete Zielgruppen und deren Bedürfnisse. Dabei geht es auch um die Anforderungen in konkreten Branchen wie Automobil oder Medizintechnik. Auch

Fachexperten und die Führungsebene benötigen regelmäßige Weiterbildung zu Cyberbedrohungen und dem richtigen Verhalten.

Digitales Vertrauen durch Standardisierung

Digitales Vertrauen in KI sicherzustellen ist ein wichtiger Schlüsselfaktor. Normen und Standards werden deshalb relevanter. Auf regulatorischer Seite hat die EU-Kommission im April 2021 den Artificial Intelligence Act vorgelegt. Deshalb müssen nun Diskussionen über KI-Zertifikate und prüfbare Standards geführt werden, um eine möglichst sichere IT-Umgebung aufzubauen. Normierungsorganisationen wie die ISO (Internationale Organisation für Normung) befassen sich damit. Auch die Wirtschaft erarbeitet Vorschläge und Lösungen für mögliche KI-Label. Ein Beispiel ist die Charter of Trust, eine Cybersecurity-Allianz globaler Unternehmen, der auch TÜV SÜD angehört. Ein zentraler Aspekt bei der Entwicklung und dem Einsatz von KI-basierten Anwendungen ist es, sicherzustellen, dass das Vertrauen in digitale Technologien wächst.

Podcast zu den Cybersecurity-Trends 2023

Mehr Hintergrund zu den Cybersecurity-Trends 2023 gibt es in Episode 62 des TÜV SÜD-Podcasts „Safety First". Das englischsprachige Interview mit Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) TÜV SÜD, ist hier verfügbar oder überall, wo es Podcasts gibt.

Informationen zu den Dienstleistungen von TÜV SÜD rund um IT-Sicherheit: https://www.tuvsud.com/cybersecurity.

Hinweis für Redaktionen: Die Pressemeldung und die Grafik in reprofähiger Auflösung sind verfügbar unter www.tuvsud.com/presse.

Pressekontakt:

Sabine Krömer TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail sabine.kroemer@tuvsud.com Internet www.tuvsud.com/de