Pressemitteilung

Mehr Wert.
Mehr Vertrauen.

Cybersicherheit 16. November 2021

TÜV SÜD: Das sind die Cybersecurity-Trends 2022

München. Cybercrime-as-a-Service, wachsende Awareness und die Absicherung der gesamten Lieferkette zählen zu den wichtigsten Trends in der Cybersicherheit im Jahr 2022. Zudem fordert die steigende Professionalisierung von Cyberkriminellen im Bereich Ransomware eine entsprechende Vorbereitung auf Unternehmensseite.

„Kaseya, SolarWinds, die Colonial Pipeline: Die Attacken im Jahr 2021 haben erneut gezeigt, wie wichtig es ist, Cybersicherheit als Teil der Unternehmenskultur zu etablieren und über die gesamte Lieferkette hinweg zu implementieren“, erläutert Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) bei TÜV SÜD. „Zusätzlich ist Ransomware mittlerweile als Cybercrime-as-a-Service für jeden zugänglich und das inklusive technischen Supports. Cyberkriminelle haben 2021 dafür genutzt, sich neu zu positionieren, zu professionalisieren und ihr Tätigkeitsfeld auszubauen. Daher wird es nun für KMU, Industrie und Behörden wichtig, zu reagieren.“ Entsprechend den Entwicklungen sehen die Security-Experten vom TÜV SÜD die folgenden Trends für das Jahr 2022:

Cybercrime-as-a-Service (CaaS)

Schadsoftware (Ransomware) wird mittlerweile von Cyberkriminellen ähnlich vermarktet wie reguläre Software und haben damit ein Geschäftsmodell geschaffen. Gegen Lizenzgebühren kann Malware gekauft werden, sogar inklusive technischem Support. Dieser Markt wird weiterwachsen. Unternehmen müssen darauf proaktiv reagieren und verstärkt in die Schulung und Awareness ihrer Mitarbeitenden sowie in die Absicherung der technischen Infrastruktur investieren.

Cybersecurity Awareness: Verbraucher sind sensibilisiert

Angriffe auf große Unternehmen und Infrastruktur haben gezeigt, dass die Maßnahmen der Industrie in Sachen Cybersicherheit, beispielsweise bei IIoT, den Methoden der Angreifer deutlich hinterher sind. Hier ist es im Interesse der Industrie selbst, das eigene Bewusstsein für Risiken und Bedrohungen zu schärfen und gemeinsam Anforderungen zu entwickeln, die dabei helfen resilienter gegenüber Angreifern zu werden. Auch Endverbraucher achten bei der Kaufentscheidung vernetzter Produkte zunehmend auf Cybersicherheit, beispielsweise bei IoT-Geräten wie Smartwatches oder anderen Wearables.

Lieferkette: Einheitliche Sicherheitsstandards

Vergangene Vorfälle zeigen, dass besonders die Lieferkette in der Software-Entwicklung noch mehr Awareness für Cyberbedrohungen benötigt. Zudem muss es gemeinsame Standards für sichere Software geben, wie sie beispielsweise von der Charter of Trust gefordert werden, einer globalen Cybersicherheitsallianz in der TÜV SÜD aktives Mitglied ist. Hersteller sollten ihre Partner und Zulieferer bezüglich der Einhaltung neuer Vorschriften unterstützen, um sie zu motivieren.

Globale Harmonisierung: Gemeinsam für mehr Cybersicherheit

„Standards sind das Rückgrat der Cybersicherheit." Dieses Motto muss international gelebt werden und erfordert grenzüberschreitende Zusammenarbeit. Industrie und Gesetzgeber müssen reagieren: Es muss gemeinsam an harmonisierten Mindestanforderungen gearbeitet werden, die über Branchen und Technologien hinweg dafür sorgen, dass Produkte und Services „ab Werk" cybersicher sind. Durch einheitliche und allgemeingültige Standards für Cybersicherheit ist es möglich, das Sicherheitsniveau zu stärken.

Digital Trust: Schutz für KI, Automation und Algorithmen

KI und Automatisierung helfen Unternehmen beispielsweise dabei, Prozesse zu optimieren und den eigenen Datenverkehr zu analysieren, um Angriffe, Datenlecks und -diebstähle frühzeitig zu erkennen. Allerdings sind diese Technologien nur so zuverlässig, wie die Algorithmen dahinter abgesichert

werden. Unternehmen und Organisationen müssen entsprechend umsichtig sein, wie sie diese Technologien schützen. Denn auch Cyberkriminelle nutzen KI zunehmend für ihre Zwecke. Grundlegende Standards zur Cybersicherheit von KI können den Schutz der Infrastruktur und die Datenintegrität unterstützen.

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

Hinweis für Redaktionen: Die Pressemeldung und die Grafik in reprofähiger Auflösung gibt es im Internet 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

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 25.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. www.tuvsud.com/de