

IT-Sicherheit

29. Oktober 2020

TÜV SÜD: Das sind die Cybersecurity-Trends 2021

München. Das New Normal erfordert von Unternehmen auch in der Cybersecurity, bisherige Konzepte, Strukturen und Prozesse zu überdenken und neue Lösungen zu finden. Die Experten von TÜV SÜD Sec-IT nennen wichtige Trends und Entwicklungen, auf die Unternehmen und deren IT-Sicherheitsabteilungen im kommenden Jahr achten sollten.

„Das New Normal verlangt von Unternehmen einen Anpassungsprozess“, erklärt Stefan Vollmer, Chief Technology Officer (CTO), TÜV SÜD Sec-IT. „Auch künftig werden großen Teile der Belegschaft mobil arbeiten. Remote-Zugriffe auf Unternehmensdaten und Anwendungen in der Cloud nehmen weiter zu. Die Konzepte für Zugangsmanagement, der daraus resultierende Aufwand im Datenschutz, sowie natürlich auch die IT-Sicherheit beim Arbeiten im Homeoffice müssen daran angepasst werden.“ Vor dem Hintergrund dieser Entwicklung sehen die Experten von TÜV SÜD Sec-IT folgende Cybersecurity-Trends für das Jahr 2021:



1. Fachkräftemangel: Automatisierung kann helfen

Bereits vor der Pandemie herrschte ein Fachkräftemangel in der IT-Security, die [Cybersecurity Workforce Studie der \(ISC\)²](#) von 2019 geht von einem Bedarf von vier Millionen Fachleuten weltweit aus. Darum müssen sich Unternehmen zunehmend nach automatisierten Lösungen umsehen, die es erlauben, das vorhandene Personal zu entlasten und die Ressourcen besser auf den Schutz vor neuen Bedrohungen und die Entwicklung neuer Strategien zu verteilen, während kleinere Aufgaben selbstständig vom System erledigt werden.

2. Lieferketten besser absichern

Lockdowns und neue Regularien haben besonders Zulieferer dazu genötigt, neue Wege zu gehen und bisherige Prozesse umzustrukturieren. Produzierende Gewerbe werden von den Umständen gefordert, mehr und mehr Prozesse teilweise oder komplett zu digitalisieren. Ein wichtiger Faktor wird dabei das intelligente Vernetzen und Fernsteuern mehrerer Geräte über das Internet-der-Dinge (IoT). Um solche IoT-Geräte vor externen Angriffen zu schützen, muss die Entwicklung und die Absicherung standardisiert werden und objektiv prüf- und zertifizierbar sein.

3. Cloud Security wird wichtiger

Um Fernzugriffe und mobiles Arbeiten zu vereinfachen, verlegen viele Unternehmen Anwendungen und Services in die Cloud. Dadurch steigt auch der Schutzbedarf der Plattformen. Ein Weg, um den Umzug in die Cloud sicherer zu gestalten, ist eine vorherige Analyse und Beratung durch unabhängige Experten. Im Anschluss ist es allerdings imperativ, die Sicherheit der Cloud-Lösungen durch regelmäßige und umfangreiche Penetrationstests auf eventuelle Lücken zu überprüfen.

4. Automatisiertes Phishing

Quantität ist besser als Qualität – diesen Slogan schreiben sich Cyberkriminelle nach wie vor auf die Fahne. Entsprechend ist eine der größten Gefahren für Unternehmen weiter das breite Netz, das Cyberkriminelle mit Phishing per Mail oder über soziale Medien auswerfen. Mitarbeiter müssen durch gezielte Security Awareness Trainings auf diese Gefahren und die Tricks der Betrüger aufmerksam gemacht werden und lernen, wie mit diesen Bedrohungen umzugehen ist. Inwieweit Automatisierung auch für die Verteidiger sinnvoll ist, zeigt nicht zuletzt ein [Report](#) von Cofense von 2019.

5. Datenschutz bleibt wichtig

Durch den erhöhten Grad an Digitalisierung werden auch kleine und mittlere Unternehmen mit immer größeren Aufgaben rund um den Schutz der gesammelten und gespeicherten Daten konfrontiert. Entsprechend ist es nicht nur notwendig, diese Daten bestmöglich zu sichern, sondern auch die wichtigsten Anforderungen zum Datenschutz durch die EU-DSGVO zu

kennen. Hierbei kann oftmals eine externe Beratung oder, bei größeren Unternehmen, auch die Auslagerung der Verantwortung an einen extern benannten Datenschutzbeauftragten helfen.

6. Standards sind Basis für Sicherheit

Seit Juni 2019 ist die europäische Verordnung „EU-Cybersecurity Act“ in Kraft. Sie bietet das Rahmenwerk für die EU-weite IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen. Geräte müssten dann bereits während der Konzeption und Produktion einheitliche Sicherheitsanforderungen erfüllen ("Security by Design" und "Security by Default"). Einheitliche Standards auf dieser Basis ermöglichen eine Überprüfung durch unabhängige, neutrale Dritte.

Mehr über die Leistungen der TÜV SÜD Sec-IT GmbH unter [https://www.tuvsud.com/de-de/dienstleistungen/cyber-security](https://www.tuvsud.com/de/de/dienstleistungen/cyber-security).

Hinweis für Redaktionen: Die Pressemeldung und das Bild 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