IT-SECURITY TRENDS 2022

Eine Prognose für Unternehmen aus Deutschland

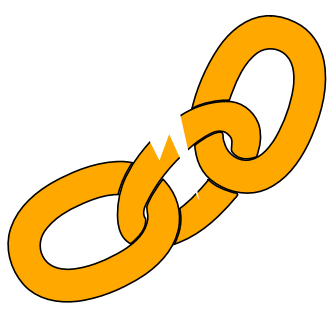
TRENDS, TIPPS UND FAZIT:

Cybercrime-as-a-Service (CaaS)

Cyberstraftaten werden künftig vermehrt in Form von Dienstleistungspaketen angeboten. Cyberkriminelle mithilfe des neuen illegalen Geschäftsmodells CaaS Angriffe ohne jegliche IT-Kenntnisse oder Fähigkeiten realisieren.

Supply-Chain-Attacken

Das Risiko von Attacken auf Lieferketten nimmt zu. Ziel dieser Attacken ist der Angriff auf Unternehmensnetzwerke über Lieferanten oder Drittanbieter. Hierbei wird mangelnde Sorgfalt von Unternehmen in der Überwachung von Lieferketten ausgenutzt.



Cybersecurity Awareness

Die steigende Anzahl an Cyberattacken erfordert zugleich ein steigendes Bewusstsein für Bedrohungen im ganzen Unternehmen. Die Sensibilisierung von Mitarbeitern im Hinblick auf Risiken, zum Beispiel mithilfe von Security-Awareness-Trainings, ist so wichtig wie noch nie zuvor.

Absicherung hybrider Arbeitsplätze

Dies geht mit dem Trend zu hybriden und flexiblen Arbeitsplatzlösungen einher. Zunehmenden Bedrohungen von Remotelösungen entgehen Unternehmen neben dem Einsatz von Schadprogrammen durch die Sicherung von Daten in einer Cloud-Umgebung, wo die Überwachung, Netzwerksicherheit und Aktualisierung gewährleistet wird.

Unser Fazit:

Cyberattacken werden im Jahr 2022 noch ausgeklügelter und es kommen neue Bedrohungen hinzu. Um sich als Unternehmen dagegen zu schützen, hilft ein starkes und ganzheitliches Sicherheitskonzept. Das besteht aus Mitarbeitersensibilisierung, proaktiver Überwachung der IT-Infrastruktur und dem Einsatz der richtigen Schutzprogramme.

Besuchen Sie uns für mehr Infos zu Ihrer IT-Sicherheit auf

www.osite-network.de