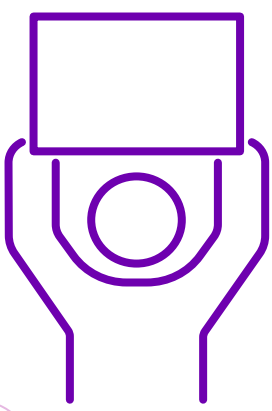
HISCOX
WISSEN VERSICHERT.

Sechs aktuelle Cyber-Risiko-Trends

1 Bedrohungen durch Insider-Täter

Die erhöhte Inflation hat auch indirekt Auswirkungen auf die Cybersicherheit für Unternehmen. Denn Insider-Angriffe häufen sich auch, wenn Mitarbeiter in finanziellen Schwierigkeiten stecken. Außerdem kann die Unzufriedenheit der Mitarbeiter wegen stagnierender Löhne oder drohender Entlassungen zu Datenextraktion und -schmuggel führen.

2 Angriffe durch Aktivisten

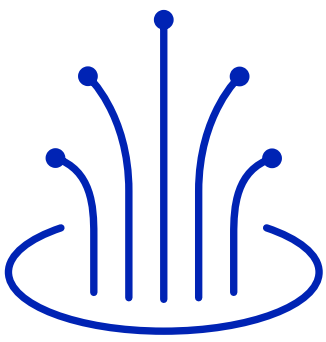


Der Angriffskrieg in der Ukraine wird auch verstärkt im Internet ausgetragen. Beispielsweise ist die sogenannte “IT-Armee der Ukraine” als Cyber-Aktivistenarmee eine der ersten ihrer Art und könnte damit ein Vorbild für andere Aktivisten darstellen. In welche Richtung werden sich diese Gruppierung und Nachahmer in Zukunft orientieren? Bereits 2022 wurden etwa die Klimaproteste immer dramatischer es ist damit zu rechnen, dass auch hier die Aktivisten künftig vermehrt auf Cyberangriffe zurückgreifen könnten.

3 Zersplitterung von Ransomware-Gruppierungen

Eine kontinuierliche Bedrohung sind die Ransomware-Banden. Hier zeichnet sich seit 2022 allerdings eine Veränderung ab: Die Gruppierungen setzen nach wachsendem Druck durch die Strafverfolgungsbehörden inzwischen vermehrt auf Anonymität und agieren in kleineren Gruppen, die regional und branchenspezifisch vorgehen. Auch bei den extrem hohen Lösegeldforderungen ist ein Rückgang zu sehen, da diese oft für Schlagzeilen sorgen und damit unerwünschte Aufmerksamkeit auf die Gruppierungen lenken.

4 Physische Angriffe auf Datenkabel



Trotz aller Schutzvorkehrungen im Bereich Cyberrisiken gibt es Schwachstellen, gegen die Unternehmen weitgehend machtlos sind. Die physische Infrastruktur, die die weltweite Internetverbindung gewährleistet, wird immer wieder Ziel von Angriffen. Im letzten Jahr gab es mehrere Angriffe auf die Unterseekabel, ohne dass Verantwortliche ermittelt werden konnten. Die Motivation hinter diesen Angriffen ist nicht zweifelsfrei geklärt, was die Angriffe umso besorgniserregender macht.

5 Gefahr von Stromausfällen

Schon im vergangenen Jahr warnten mehrere Regierungen vor Stromausfällen. Grund hierfür war der Beginn des Russland-Ukraine-Kriegs, welcher die globalen Energieversorgungsketten nachhaltig schwächt. Nach wie vor ist die Gefahr von Stromausfällen nicht gebannt. Datenzentren und Remote-Arbeit können betroffen sein, aber auch Büros und Fabriken. Für den Fall der Fälle gilt es also auch hier, Vorkehrungen zu treffen, da Stromausfälle natürlich auch die Cybersicherheit negativ beeinflussen können.

6 Mehr Sicherheit durch passwortlose Authentifizierung

Um die Sicherheit von physischen Geräten zu gewährleisten, werden die Multi-Faktor-Authentifizierung und die passwortlose Anmeldung mit biometrischen Merkmalen zum neuen Standard für Cybersicherheit werden – Apple, Microsoft und Google machen es mit ihrem “Fast ID Online”-Standrt vor. Eine Umstellung ist schon heute ratsam, da diese zusätzlichen Vorkehrungen die Benutzerfreundlichkeit sowie Cybersicherheit in Unternehmen erhöhen.

22334 03/23