Die Lage der IT-Sicherheit in Deutschland 2024/2025

Trends der Cyber-Security

Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) spricht im aktuellen Berichtszeitraum von einer angespannten Lage. Besonders besorgniserregend sind die zunehmende Professionalisierung und Spezialisierung der Cyberkriminellen. Dieser Trend ermöglicht es den Kriminellen, ihre Angriffe effizient durchzuführen. Hierbei setzt man vor allem auf die Ausnutzung der Zero-Day-Schwachstellen. Für diese Art von Schwachstellen existieren aktuell keine Sicherheitsupdates, weshalb Cyberkriminelle diese verwenden, um in Systeme einzudringen und Daten zu stehlen.

Der Lagebericht identifiziert drei Hauptzielgruppen von Cyberangriffen:

- Kleine und mittlere Unternehmen (KMU)
- IT-Dienstleister
- Kommunen

Die Angriffe auf IT-Dienstleister sind besonders besorgniserregend, weil diese in der Regel einen Zugang zu den Systemen ihrer Kunden besitzen – ein einzelner erfolgreicher Angriff kann so weitreichende Folgen haben.

Das BSI sieht in DDoS-Angriffen und Ransomware die Hauptbedrohung für Unternehmen und öffentliche Einrichtungen. Bei einem DDoS-Angriff (Distributed Denial of Service) überfordert ein Angreifer eine Website, einen Server oder eine Netzwerkressource mit sehr vielen Anfragen (Überlast). Der Begriff Ransomware steht für eine Art von Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld (englisch: Ransom) verlangt. Entweder sperrt ein solches Schadprogramm den kompletten Zugriff auf das System oder es verschlüsselt bestimmte Nutzer- beziehungsweise Unternehmensdaten. Kleine und mittlere Unternehmen sowie Kommunen, Universitäten und Forschungseinrichtungen wurden überproportional häufig angegriffen.[1]

Als besonders schwerwiegendes Sicherheitsereignis aus 2024 kann der Crowdstrike-Vorfall genannt werden, bei dem ein fehlerhaftes Update eines Sicherheitsprodukts von CrowdStrike zu weltweiten IT-Ausfällen mit erheblichen wirtschaftlichen Schäden führte. Dieser Vorfall zeigt deutlich, wie abhängig moderne Unternehmen von funktionierender IT-Infrastruktur sind und wie weitreichend sich Störungen auswirken.

Für das Jahr 2025 prognostizieren Experten, dass Sicherheitsbedrohungen weiter stark ansteigen werden. Gewisse Trends sind jetzt schon erkennbar:

Noch professionellere Ransomware-Angriffe

Da es sich bei bis zu 20 Prozent aller Verstöße um Ransomware-Angriffe handelt, ist diese Sicherheitsherausforderung seit über einem Jahrzehnt[2] ein weitverbreitetes Risiko. Ihr Bedrohungspotenzial wird in naher Zukunft noch größer werden. Es gibt schon jetzt weit über

Bild: kras99/stock.adobe.com

100 Ransomware-Familien, die zeigen, dass sich dieser Angriffsvektor ausbreitet und an Raffinesse zunimmt.[3]

Cloud-Security

Sicherheitsexperten haben im europäischen Wirtschaftsraum eine steigende Zahl an Untersuchungen von Vorfällen festgestellt, die auf Fehlkonfigurationen, unzureichende Überwachung, die Wiederverwendung von Anmeldeinformationen und schwache Sicherheitspraktiken in nicht verwalteten Cloud-Umgebungen zurückzuführen sind. Viele Unternehmen ziehen ihre Systeme sehr schnell in die Cloud um, was die damit verbundenen Probleme und Herausforderungen durch die Aufteilung der Verantwortlichkeiten zwischen Geschäftsführung, Entwicklung, IT-Betrieb und IT-Sicherheit verschärft. Unternehmen müssen der Cloud-Sicherheit Vorrang einräumen, um sensible Daten zu schützen und das Vertrauen der Kunden zu erhalten.[4]

KI (Künstliche Intelligenz)

Abschließend muss auch das Thema „Künstliche Intelligenz“ angesprochen werden. Denn die Angriffe mithilfe von KI werden in Qualität und Quantität weiter steigen. Das liegt unter anderem daran, dass entsprechende Tools immer leichter zugänglich sind. Experten gehen davon aus, dass Cyber-Akteure im Jahr 2025 zunehmend KI-basierte Tools einsetzen werden, um ihre Online-Operationen zu verbessern und zu unterstützen.[4]

Mittels KI realisierte Deepfakes könnten dabei beispielsweise für sehr realistische Phishing-Angriffe genutzt werden. Deepfakes beschreiben Methoden zur Manipulation medialer Identitäten, wie beispielsweise Videos, Bilder, Audios und Texte.
Durch die Manipulation der Videos, Bilder oder Stimmen sind verschiedene Bedrohungsszenarien denkbar:

- Überwindung biometrischer Systeme: Insbesondere bei Fernidentifikationsverfahren (z. B. der Spracherkennung über das Telefon oder der Videoidentifikation) scheinen solche Angriffe erfolgversprechend.
- Social Engineering: Deepfake-Verfahren können außerdem dazu verwendet werden, gezielte Phishing-Angriffe durchzuführen, um Informationen zu gewinnen.

Auch kann ein Angreifer mittels dieser Technologie in Anrufen/Videoanrufen die Stimme und/oder das Aussehen der Führungskräfte nachahmen, um so einen Geldtransfer zu initiieren („CEO-Fraud“).[5]

Autoren: Markus Vollmuth (Informationssicherheitsberater und DIN ISO 27001 Lead Auditor bei der atarax Unternehmensgruppe) und Rico Seyd (Stv. Leiter Standortpolitik bei der IHK zu Coburg)

[1] Die Lage der IT-Sicherheit in Deutschland 2024
[2] www.isaca.org/resources/infographics/ransomware-incident-management
[3] www.isaca.org/resources/news-and-trends/industry-news/2025/cybersecurity-trends-to-watch-in-2025
[4] cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025?hl=en
[5] www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Regionale Datenbank für Automobil-Zulieferer: der IHK-AutomotiveFinder

Die Automobilzulieferindustrie durchläuft derzeit eine tiefgreifende Transformation, die nicht nur den Markt, sondern auch die gesamte Wertschöpfungskette maßgeblich verändert. Während traditionelle Märkte zunehmend an Bedeutung verlieren, entstehen zugleich innovative und zukunftsorientierte Geschäftsfelder. Diese Dynamik zwingt Unternehmen dazu, ihr Produkt- und Dienstleistungsportfolio kontinuierlich zu überdenken und anzupassen, um wettbewerbsfähig zu bleiben.

In diesem komplexen und schnelllebigen Umfeld leistet der IHK-AutomotiveFinder einen essenziellen Beitrag.

Die Plattform wurde speziell für die Bedürfnisse der Automobilzulieferindustrie angepasst, um Markttransparenz zu erhöhen und die Wettbewerbsfähigkeit von Unternehmen, insbesondere kleinen und mittelständischen, zu stärken. Sie bietet eine umfassende Datenbank, die Hersteller, Zulieferer, industrienahe Dienstleister sowie Anbieter von Forschung- und Entwicklungslösungen integriert. Der IHK-AutomotiveFinder erleichtert mit einer leistungsstarken Suchfunktion und Filtern die schnelle Identifikation passender Geschäftspartner und stärkt durch detaillierte Unternehmensprofile die Marktpräsenz. Zudem fördert er Innovationen, indem er den Zugang zu FuE-Anbietern erleichtert und so Innovationsprozesse beschleunigt, die für die aktuelle Transformation entscheidend sind. Die IHK zu Coburg unterstützt im Verbundprojekt „transform_EMN“ die breite Einbindung der kleinen und mittleren Unternehmen in den Transformationsprozess.

Wenn auch Sie Interesse daran haben, Ihr Unternehmen in der Datenbank zu präsentieren und Ihre Sichtbarkeit zu steigern sowie gezielt Kontakte zu Geschäftspartnern und Innovatoren zu knüpfen, dann registrieren Sie sich gerne hier:

ihk-automotivefinder.de

KONTAKT

RICO SEYD
09561 7426-46
rico.seyd@coburg.ihk.de