Ein Unternehmen der

enviaM-Gruppe

Whitepaper

Cybersicherheit ist Chefsache.

Wissenswertes zur Geschäftsführer-haftung bei Cyberangriffen.

Vorwort

Aufgrund der akuten Bedrohungslage im digitalen Raum hat die Europäische Union in den letzten Jahren die Vorschriften zur Cybersicherheit immer weiter verschärft. Und was viele Geschäftsführer, Vorstände und Aufsichtsräte weiterhin nicht wissen, ist die Tatsache, dass sie im Fall der Fälle oftmals persönlich für ein Versäumnis im Bereich Cybersecurity haften. So können Cyberattacken auf ein Unternehmen daraus resultieren, dass die Geschäftsführung es schlicht und ergreifend vergessen hat, die rechtlichen Vorschriften im Hinblick auf die Cybersicherheit zu erfüllen. Klar, dass es dann kaum eine Chance gibt, sich der Verantwortung und persönlichen Haftung zu entziehen. Die drohenden Bußgelder können dabei immens hoch sein und zusätzlich zu dem verursachten Schaden durch den Angriff eine existenzielle Bedrohung für das Unter-nehmen darstellen.

In diesem Whitepaper möchten wir die aktuelle Bedrohungslage erörtern und auf relevante Richtlinien rund um das Thema Cybersicherheit hinweisen. Auch zeigen wir auf, wie Geschäftsführer und andere Führungskräfte im Unternehmen ihrer Verantwortung nachkommen können.

Inhalt

1. Akute Bedrohungslage

203 MRD EURO SCHADEN

.... erlitten deutsche Unternehmen allein im Jahr 2022 ....

1.1. Unter Cyber-Dauerbeschuss: Erhöhte Bedrohungslage für Unternehmen im digitalen Zeitalter.

Die Gefahr im Bereich Cybersicherheit in Deutschland hat sich drastisch erhöht, nicht zuletzt auch mit dem Beginn des russischen Angriffskriegs gegen die Ukraine. So stuft das Bundesamt für Sicherheit in der Informationstechnik (BSI), die höchste Behörde für Cybersicherheit, die Bedrohung im Cyberraum als so hoch wie nie zuvor ein.[1]

Insgesamt zeigt sich, dass die Cybersicherheit in Deutschland und weltweit zu einer immer drängenderen Herausforderung wird, die sowohl finanzielle als auch organisatorische Auswirkungen auf Firmen und Organisationen haben kann. Aktuelle Zahlen, Daten und Fakten dokumentieren den Ernst der Lage und die oftmals existenzielle Bedrohung für kleine und große Unternehmen.

Zunahme von Schadprogrammen und Schwachstellen

- Zwischen Juni 2021 und Mai 2022 verzeichnete das BSI[2] 116,6 Millionen neue Varianten von Schadprogrammen.
- In diesem Zeitraum wurden 15 Millionen Schadprogramm-Infektionen gemeldet.
- Zudem wurden 20.174 Schwachstellen in Software-Produkten identifiziert.

Hinterhältige Ransomware-Attacken häufen sich

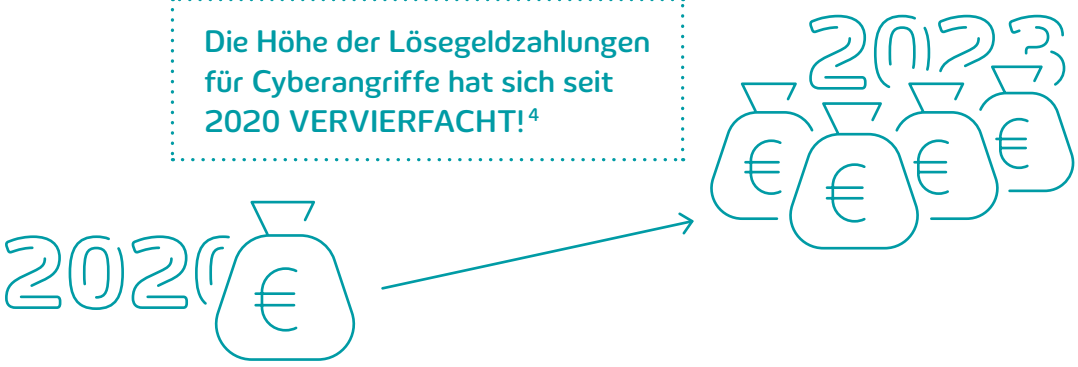
- Ransomware-Angriffe sind eine der größten Gefahren für die Cybersicherheit im Business-Bereich.
- Kriminelle verschlüsseln die Daten und Systeme ihrer Opfer und erpressen Lösegeld.
- Zusätzlich drohen sie damit, sensible Daten zu veröffentlichen, wenn das Lösegeld nicht gezahlt wird.

1 https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
2 https://www.prosoft.de/blog/bsi-lagebericht-2022-zur-it-sicherheit-in-deutschland/

Verheerende Auswirkungen auf die Wirtschaft

- Im Jahr 2021 wurden 84 % der deutschen Unternehmen Opfer von Cyberangriffen.
- Der entstandene Schaden für die deutsche Wirtschaft belief sich auf insgesamt 203 Milliarden Euro.[3]

Die Höhe der Lösegeldzahlungen für Cyberangriffe hat sich seit 2020 VERVIERFACHT![4]



Langwierige Erholung und hohe Kosten

- Unternehmen benötigen durchschnittlich einen Monat, um sich von einer Ransomware-Attacke zu erholen.
- Die durchschnittlichen Kosten einer solchen Attacke belaufen sich auf etwa 1,3 Millionen Euro.
- Aufgrund des langen Bereinigungsprozesses können die Kosten jedoch noch deutlich höher ausfallen.

Kontinuierliche Bedrohungslage

- In naher Zukunft ist keine Entspannung der Cyber-Bedrohungslage absehbar.
- Die zunehmende Digitalisierung, Automatisierung und Vernetzung bieten Angreifern immer wieder neue Angriffsflächen.
- Um diesen Gefahren entgegenzuwirken, müssen Unternehmen ihre Cybersecurity-Fähigkeiten kontinuierlich verbessern.

1.2. Erschreckend kreative Cyberattacke: Phishing-Angriff nutzt Google Authenticator zur Umgehung von Multi-Faktor-Authentifizierung.

Ein kürzlich bekannt gewordener Cyberangriff auf Retool, ein Anbieter von Low-Code-Entwicklungsplattformen, enthüllte die Ausnutzung der Cloud-Synchronisation des Google Authenticators. Der Angreifer verwendete gezielte Phishing-SMS, um Mitarbeiter von Retool zu täuschen. Nachdem ein Mitarbeiter auf einen gefälschten Link geklickt und einen vermeintlichen Anruf vom IT-Team erhalten hatte (tatsächlich ein Deepfake), konnte der Angreifer einen Multi-Faktor-Authentifizierungscode (MFA) erlangen.

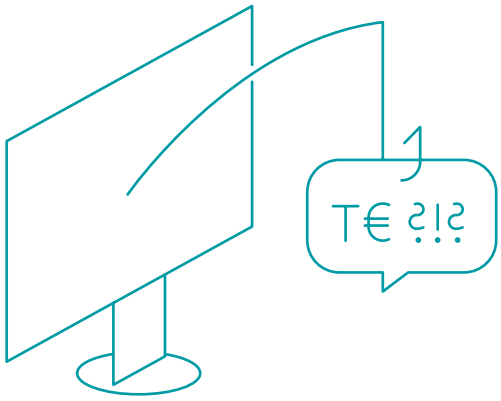
Die Synchronisierungsfunktion des Google Authenticators ermöglichte es dem Angreifer, Zugriff auf interne Systeme von Retool zu erhalten. Das Unternehmen warnte vor diesem neuen Angriffsvektor und betonte die Standardaktivierung der Cloud-Synchronisation ohne einfache Deaktivierungsmöglichkeit für Nutzer und Administratoren.[5]

3 https://bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
4 https://www.heise.de/news/Warum-Cybergangster-mit-Ransomware-immer-hoehere-Loesegelder-erpressen-6121767.html
5 https://retool.com/blog/mfa-isnt-mfa

1.3. Gefährliches Sixpack: Diese Angriffstrends gefährden täglich unzählige Unternehmensleben.

1. Künstliche Intelligenz
Cyberkriminelle maximieren mit KI-basierten Angriffsmethoden wie Deepfakes und Voice Cloning ihre Gewinne. Effektiv schützen kann sich nur, wer mit der rasanten Entwicklung mithält.

2. Perfide Phishing-Methoden
Der Dauerbrenner, der den Kriminellen Milliarden einbringt. Mit Social-Engineering-Taktiken wie Business E-Mail Compromise[6] oder Romance Scam spielen die Angreifer immer versierter mit menschlichen Verhaltensmustern. Und es werden immer ausgereiftere Methoden entwickelt.



3. Skrupelloses Multichannel Phishing
Oft greifen Kriminelle über mehrere Kanäle gleichzeitig an, um an persönliche Anmeldedaten und andere sensible Daten zu gelangen.

4. Hinterhältige Ransomware-as-a-Service
Ransomware ist eine äußerst lukrative Spielwiese für Kriminelle. Illegale Verschlüsslungstools gibt es bereits für kleines Geld im Darknet.

5. Unerwartetes Versagen der Multifaktor-Authentifizierung
Die intelligente Multifaktor-Authentifizierung galt lange als effektive Schutzmaßnahme. Mittlerweile haben Angreifer auch diese Hürde genommen und als Angriffsvektor missbraucht.

6. Erschöpfte Security-Teams
Stress, überforderte Mitarbeitende und niedrige Budgets in Kombination mit unterbesetzten IT-Sicherheitsabteilungen schaffen ideale Verhältnisse für erfolgreiche Cyberangriffe.