Informationssicherheit

Lagebild 2021 der IT-Sicherheit

Mit der Bedeutung der IT steigt deren Komplexität und damit verändert sich auch die Gefährdungslage. Das BSI bezeichnet die Sicherheitslage in Deutschland als angespannt bis kritisch und empfiehlt entsprechende Gegenmaßnahmen.

Die Digitalisierung prägt uns Tag für Tag. Immer mehr Prozesse in der Bank werden automatisiert und mit anderen Prozessen vernetzt. Zahlreiche Innovationen eröffnen Potenziale für neue IT-Projekte wie z. B. die Themen künstliche Intelligenz und Blockchain. Daneben verändert sich die Arbeitswelt durch äußere Einflüsse, aktuell sehr geprägt durch die Corona-Pandemie. Entsprechend steigt die Komplexität und verändert sich die Gefährdungslage. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet deshalb u. a. jährlich über die Lage der IT-Sicherheit in Deutschland. Vor kurzem wurde der Bericht für das Jahr 2021 veröffentlicht.

Die IT-Sicherheitslage in Deutschland wird demnach als angespannt bis kritisch bezeichnet.

Anstieg bei Schadsoftware und Cyber-Erpressungen

Maßgeblichen Anteil an der Einschätzung trägt die immer schneller werdende Produktion von Schadsoftware. Im Berichtszeitraum betrug alleine der durchschnittliche tägliche Zuwachs an neuen Schadprogramm-Varianten etwa 394.000. Im Vorjahreszeitraum lag die Anzahl bei 250.000.

Aber auch die Ausweitung der Lösegelderpressung auf Basis von Cyber-Angriffen – in der Regel mit Verschlüsselungstrojanern – ist atemberaubend. Inzwischen nehmen auch Schweigegelderpressung unter Androhung der Enthüllung kompromittierender Informationen und Schutzgelderpressung unter Androhung eines DDoS-Angriffs zu (Distributed Denial of Service, bewirkt z. B. eine Überlastung bzw. Nichterreichbarkeit des Netzwerks oder der Internetseite).

Identitätsdatendiebstahl und Missbrauch bleiben insgesamt konstant, jedoch werden diese – meist über sogenannte Phishing-Mails ausgeführten – Angriffe zum Teil besser auf aktuelle Themen angepasst, um den Nutzer zur Preisgabe seiner Daten zu überreden. So nehmen die Mails häufig auf aktuelle Themen Bezug, z. B. Corona-Hilfen, Änderung der Gesetzgebung und insbesondere bei Bankkunden konkrete regionale Themen wie Fusionen und Filialschließungen.

Corona als zusätzlicher Stressfaktor in der IT-Sicherheit

Die Corona-Pandemie war überhaupt ein wichtiger Treiber, denn die Situation bot zahlreiche neue Angriffsmöglichkeiten. Allen voran konnten Angriffe via Social Engineering (Beeinflussung eines Menschen, um sein Handeln zu manipulieren) erfolgreich abgesetzt werden. Die neue Arbeitssituation im Homeoffice verunsicherte Mitarbeiter und manchmal fehlte dann auch der Kollege „gegenüber“, um die „komisch wirkende Mail“ zu besprechen. Hinzu kam der Druck, den Digitalisierungsprozess schnell zu beschleunigen, um die Handlungsfähigkeit während der Pandemie zu erhalten. So mussten mit den Kontakteinschrän-

144 MIO.
neue Schadprogramm-Varianten

+22%
gegenüber 2020:
117,4 MIO.

DURCHSCHNITTLICH
394.000
neue Schadprogramm-Varianten pro Tag
2020: 322.000

IM HÖCHSTWERT
553.000
2020: 470.000

Quelle: Die Lage der IT-Sicherheit in Deutschland 2021 (bund.de)

kungen zahlreiche Remote-Arbeitsplätze eingerichtet und neue Kommunikationssysteme genutzt werden. Entsprechend stiegen auch die Angriffe auf Videokonferenzsysteme.

Zur Erhöhung der IT-Sicherheit im Homeoffice empfiehlt das BSI folgende Maßnahmen:

- Nutzung von VPN-Verbindungen (Virtual Private Network)
- Absicherung der Zugänge durch Mehr-Faktor-Authentifizierung
- Verwaltung mobiler Endgeräte über ein MDM (Mobile Device Management)
- Awareness-Maßnahmen für Mitarbeiter
- Regelmäßige Übung von Cyber- und IT-Notfällen

Insbesondere dem letzten Punkt wurde im Bankenbereich mit der Veröffentlichung der BAIT und des dort enthaltenen neuen Kapitels 10 IT-Notfallmanagement Rechnung getragen.

IT-Sicherheit als Wettbewerbsvorteil

Das Fazit überschreibt das BSI mit „Digitalisierung braucht Sicherheit". Entwicklungen und Veränderungen in Gesellschaft und Wirtschaft müssen mit entsprechenden Sicherheitsmaßnahmen einhergehen. Die größte Bedrohung stellt derzeit die Cyber-Erpressung dar. Als größte Herausforderung wird der Umgang mit Schwachstellen in IT-Systemen genannt.

Dabei sollte Cyber- bzw. IT-Sicherheit als Wettbewerbsvorteil in den Fokus rücken. Denn: „Informationssicherheit schafft Vertrauen, und sie schafft Akzeptanz bei Verbraucherinnen und Verbrauchern." ▬

AUTOR UND ANSPRECHPARTNER

Michael Switalla
Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de