DDP.IT SERVICES
X
PROSEC

CYBERRESILIENZ UND DIE MACHT DER SICHERHEITSKULTUR

Bedrohung durch Cyberkriminalität

Cyberkriminalität zählt mittlerweile zu den größten kriminellen Märkten weltweit und belegt dabei den dritten Platz im globalen Vergleich.

Die finanziellen Schäden, die durch Cyberangriffe entstehen, werden weltweit auf rund 12 Billionen US-Dollar geschätzt.

Diese enorme Summe verdeutlicht, wie ernst und weitreichend die Bedrohung durch Cyberkriminalität heute ist.

Sie meinen, das betrifft Sie nicht?

Sicherheitslücken in Ihrem Alltag

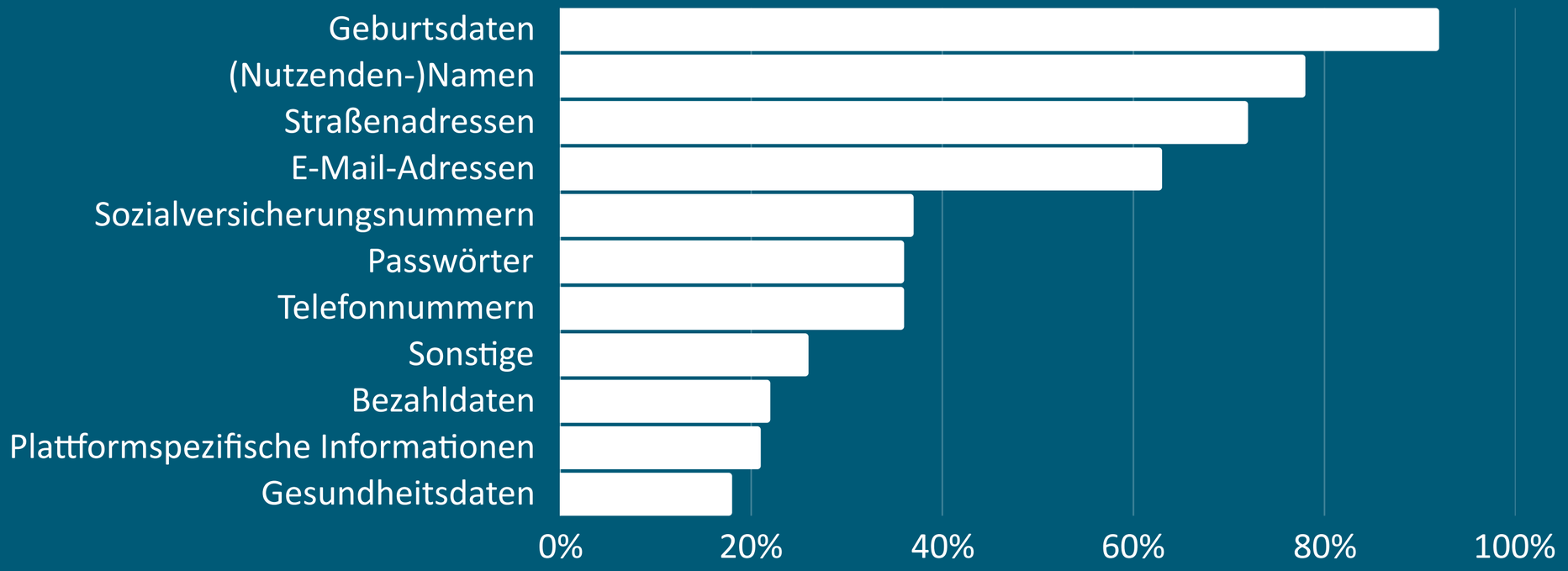
Eine Studie ergab, dass bereits ein Viertel der Drei- und Vierjährigen in Großbritannien ein eigenes Smartphone besitzen[1].

Gerade junge Kinder sind im Umgang mit Smartphones allerdings besonders schutzbedürftig und können die Gefahren von Cyberkriminalität oft noch nicht einschätzen.

Dass auch Sicherheitsbeauftragte noch Nachholbedarf beim Thema Cybersicherheit haben können, zeigt das Beispiel des Louvre in Paris: Das Sicherheitskonzept gründete auf dem Passwort “Louvre”[2].

[1] https://www.theguardian.com/technology/2024/apr/19/quarter-of-uks-three--and-four-year-olds-own-a-smartphone-data-shows
[2] https://www.zeit.de/kultur/2025-11/juwelendiebstahl-paris-sicherheit-louvre-ermittlungen

Datenleaks in Deutschland



Anteile in Prozent. Mehrfachnennungen möglich

Quelle: Leak-Statistik (DLK)

Wie können Sie sich schützen? 6 Take Aways für Ihre Cyberresilienz:

1. Das stärkste Glied sind Sie

Der aufgeklärte, wache und kritisch denkende Mensch ist die stärkste Stelle in der Verteidigungskette. Investieren Sie in Ihr Wissen und das Ihrer Kollegen, denn Awareness ist die effektivste Waffe gegen Social Engineering.

2. Der zweite Faktor

Die Multi-Faktor-Authentifizierung (MFA) ist eine der wirksamsten und einfachsten Schutzmaßnahmen. Aktivieren Sie sie überall dort, wo sie angeboten wird – für E-Mail-Konten, soziale Netzwerke und Unternehmensanwendungen. Ein Passwort allein ist kein ausreichender Schutz mehr.

3. Denken, dann klicken

Entwickeln Sie eine gesunde Skepsis gegenüber unerwarteten E-Mails, Links und Nachrichten. Insbesondere bei dringenden Handlungsaufforderungen, emotionalen Appellen oder verlockenden Angeboten gilt: Halten Sie inne, überprüfen Sie den Absender und denken Sie nach, bevor Sie klicken.

4. Rechte - Chef darf alles?!

Jeder Benutzer und jedes System sollte nur über die Zugriffsrechte verfügen, die für die Erfüllung der jeweiligen Aufgabe absolut notwendig sind. Unnötig weitreichende Berechtigungen erhöhen das Risiko im Falle einer Kompromittierung erheblich.

5. Awareness durch Erfahrung

Sicherheit wird durch Übung erlernt. Nehmen Sie aktiv an Sicherheitsschulungen, Phishing-Simulationen und anderen praktischen Übungen teil. Nur durch die Simulation eines Angriffs lernen Sie, im Ernstfall richtig zu reagieren.

6. #machen

Warten Sie nicht auf Anweisungen, sondern wenden Sie das Gelernte aktiv an – sowohl im beruflichen als auch im privaten Umfeld. Setzen Sie die hier genannten Punkte um und werden Sie zum Multiplikator für eine stärkere Sicherheitskultur.

Noch Fragen?
Wir helfen Ihnen bei Ihrer IT-Sicherheit

Kontaktieren Sie uns noch heute, um mehr über unser Beratungsangebot zu erfahren.

thomas.janzen@ddp-it.de

0261-4066-231

www.ddp-it.de