CYBER SECURITY REPORT |2022

**LaCTiS - Your expert in Cyber Security!**



We are happy, to Cyber Secure you.

Die digitale Transformation bietet den meisten Unternehmen viele neue und bedeutende Chancen.Schnell wird jedoch klar, dass diese Transformation auch Risiken herbeiführen kann. Dabei ist fast jeder, also Unternehmen, öffentliche Institutionen, andere Organisationen sowie Privatpersonen das Ziel von Cyber-Attacken.Die Bedrohungslage nimmt stetig zu. Ziel sind die sensiblen und wertvollen Daten. Cyber Security wird in vielen deutschen Unternehmen vernachlässigt. Oft können die Unternehmen die Risiken der Cyberkriminalität nicht abschätzen.Die Angst vor Cyberkriminalität ist meist nicht groß genug.Betrachtet man im Gegenzug dazu erfasste Fälle von Cyberkriminalität in den letzten zehn Jahren in Deutschland, so kann man die Cyberkriminalität geradezu als Wachstumsbranche bezeichnen. Neben den Hobby-Hackern gibt es mittlerweile professionelle Anbieter, die ihre Hacker-Servicesals Dienstleistung anbieten.Besonders kleine und mittelständische Unternehmen stehen im Visier von Cyberkriminiellen. Denn diese haben meist unterdurchschnittliche Sicherheitsvorkehrungen.

# Schaden durch Hacks

# **Enstehung von Datenlecks**

Daten sind ein wertvolles Gut. Unternehmen haben oft unmengen an Daten gespeichert, die für viele Hacker interessant sind. Größere Plattformen, die bspw. Kreditkartendaten oder Sozialversicherungsdaten gespeichert haben bieten sich für Hacker als besonders attraktiv an. Datenlecks können bspw. durch Phising-Mails, infizierte USB-Sticks, Schwachstellen von Software, oder auch Mitarbeitende enstehen

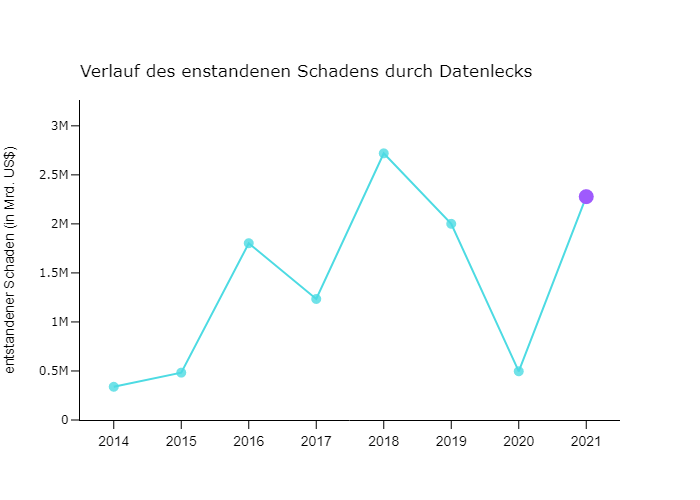


Abbildung 1: Data Breaches über die letzten 8 Jahre

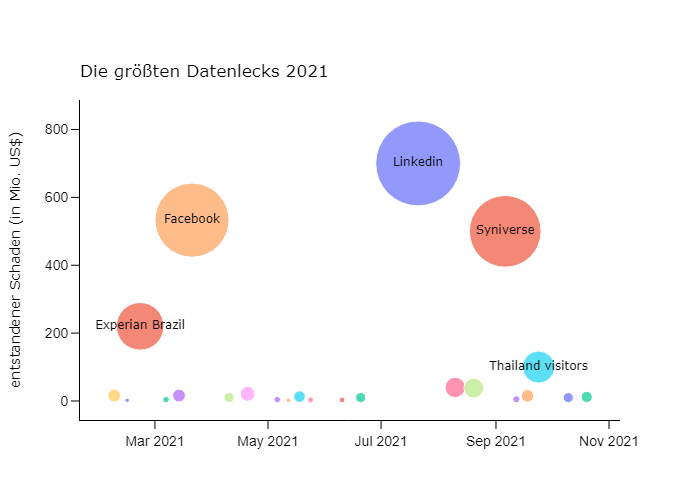


Abbildung 2: Data Breaches im Jahr 2021

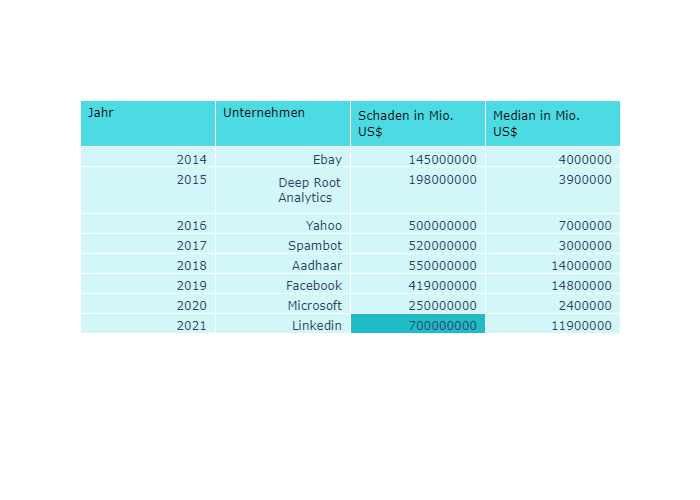


Tabelle 1: Unternehmen mit dem höchsten Schaden durch Data Breaches von Jahr 2014 bis 2021 inklusive der Mediane

# Cyber Attacken

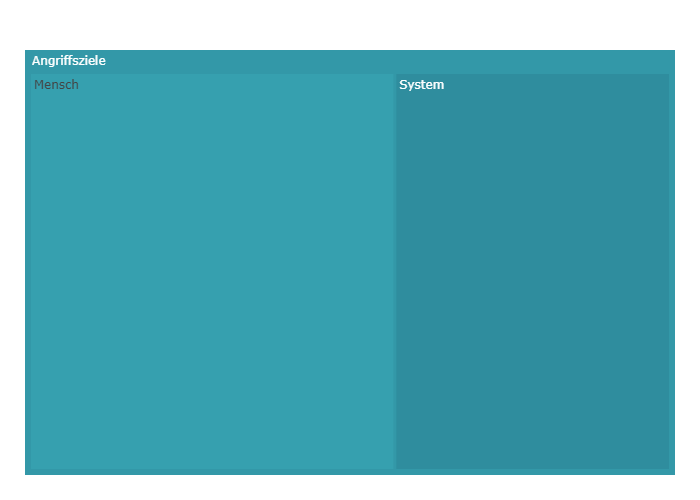


Abbildung 3: Cyber Attacken nach Angriffsvektor Mensch und System aufgeteilt

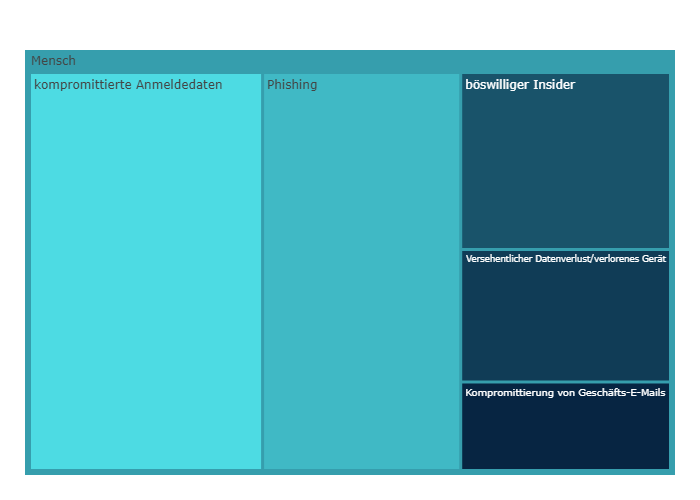


Abbildung 4: Cyber Attacken mit Angriffsvektor Mensch

Da zur Authentifizierung von Benutzern eines Informationssystems vorwiegend Kennwörter verwendet werden, ist das Abgreifen von Kennwörtern eine gängige und effektive Angriffsmethode. Zugriff auf das Kennwort einer Person erhalten Angreifer, indem sie sich auf dem Schreibtisch des Opfers umsehen, die Netzwerkverbindung „abhören“, um unverschlüsselte Kennwörter abzugreifen, Social-Engineering-Techniken nutzen, sich Zugriff auf eine Kennwortdatenbank verschaffen oder auch einfach raten. Bei der letzten Methode können Angreifer nach dem Zufallsprinzip oder systematisch vorgehen.

Von Phishing spricht man, wenn Betrüger E-Mails verschicken, welche darauf abzielen, heikle Informationen und Daten vom Empfänger zu erlangen. In der Regel erwecken die Mails den Anschein, von seriösen Unternehmen oder sogar offiziellen Institutionen und Dienstleistern (Polizei, Versicherungen, etc.) zu stammen. Im Text wird dem potenziellen Opfer oft mitgeteilt, dass sein Konto gefährdet sei, woraufhin es angewiesen wird, auf einen Link zu klicken, um vertrauliche Informationen zur Überprüfung des Kontos anzugeben.

# Phising

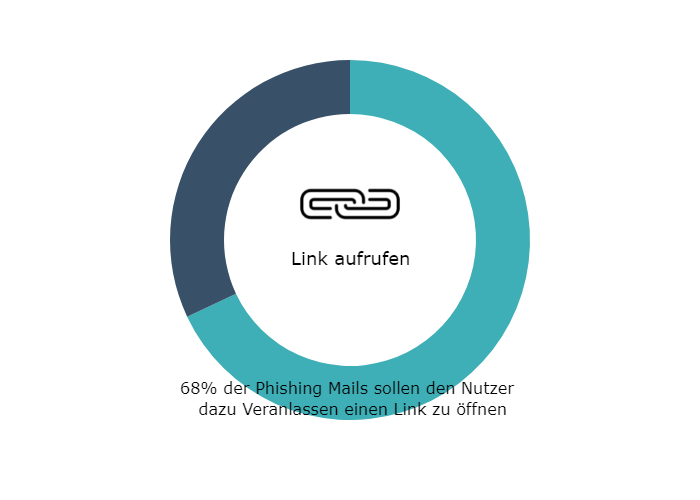


Abbildung 5: Phising via Link

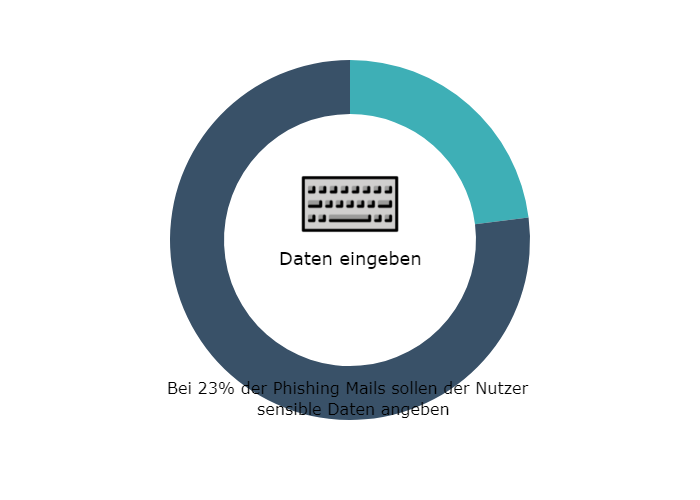


Abbildung 6: Phising via Input

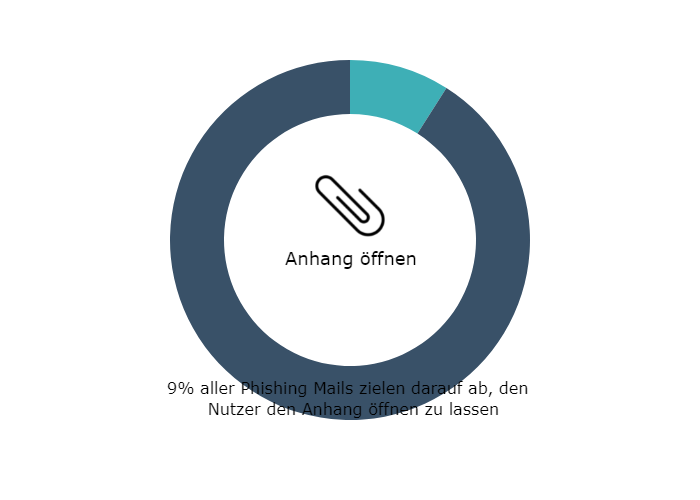


Abbildung 6: Phising via Anhang

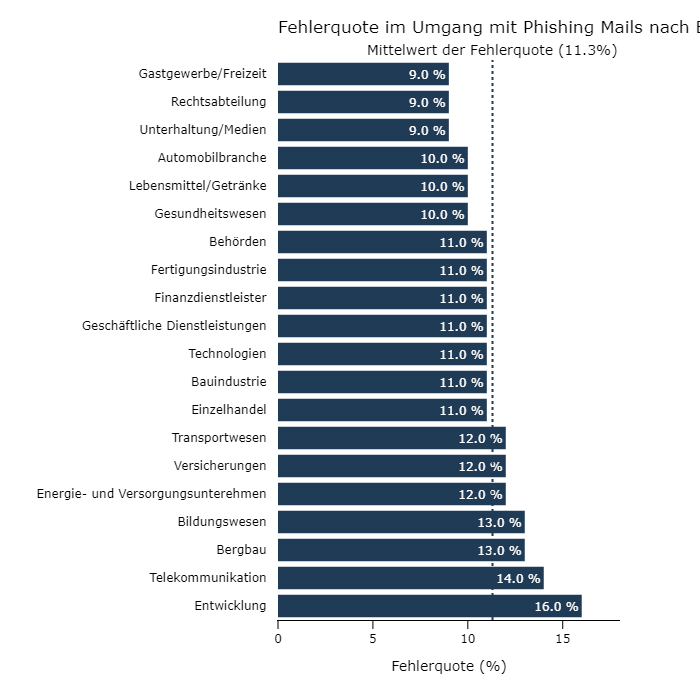


Abbildung 7: Phising nach Branche

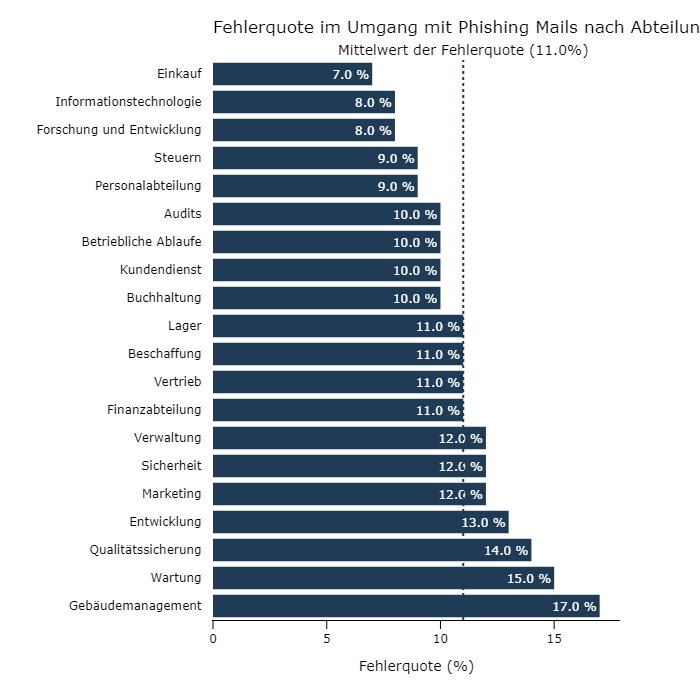


Abbildung 7: Phising nach Branche

# Passwortsicherheit

Ein häufiger Angriffsvektor in Bezug auf Passwörter ist das erraten von diesen durch ausprobieren Dabei wird durch systematisches Ausprobieren jeglicher Kombinationen versucht das richtige Passwort zu ermitteln. Diese Art von Angriff wird auch Brute-Force-Angriff genannt. Hierbei werden alle Kombinationen von möglichen Passwörtern hintereinander automatisch ausprobiert, bis das korrekte Passwort gefunden wurde. Meist führt dieses Verfahren zum Erfolg, wenn die Anzahl der möglichen Kombinationen, klein sind. So können alle Möglichkeiten in nur kurzer Zeit ausprobiert werden. Aus diesem Grund sollte die Anzahl der Zeichen so groß wie wie möglich sein. Außerdem sollte das Passwort eine definierte Länge haben. So kann die Zeit bzw. Rechenleistung, die gebraucht wird, um ein Passwort zu identifizieren, den Nutzen das Passwort zu kennen, übersteigen. (Pohlmann, 2019)

**Verwendetes Alphabet und die Länge von Passwörtern**

Durch das verwendete Alphanet und dabei nutzbaren Zeichen wird die Anzahl der möglichen Kombinationenb bei einer bestimmten Passwortlänge berechnet. Die Passwortlänge bezieht sich dabei auf die Anzahl der genutzten Elemente. Die Komplexität der automatischen Suche wird due die Anzahl der möglichen Kombinationen beschrieben. Siehe dazu Tabelle 2. (Pohlmann, 2019)

Mögliche Kombinationen = ZeichenanzahlPasswortlänge

Hinweis: Es wird angenommen, dass 1 Milliarde Versuche in einer Sekunde getätigt werden können

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Verwendetes Alphabet | Anzahl der möglichen Zeichen | Länge des Passworts | Anzahl der möglichen Kombinationen | Zeit der vollständigen Suche |
| 0-9 | 10 | 6 | 1.000.000 | 1 s |
| 6 | 100.000.000 | 100 s |
| 10 | 10.000.000.000 | 2,8 h |
| A-Z, a-z, 0-9 | 10 | 6 | 1.000.000 | 1 s |
| 6 | 100.000.000 | 100 s |
| 10 | 10.000.000.000 | 2,8 h |
| A-Z, a-z, 0-9, ()[]{}?!$%&/=\*+~,.;:<>-\_ | 10 | 6 | 1.000.000 | 1 s |
| 6 | 100.000.000 | 100 s |
| 10 | 10.000.000.000 | 2,8 h |

Tabelle 2: Mögliche Zeichen des verwendeten alphabets und die Länge von Passwörtern (Quelle: Pohlmann, 2019)

In Tabelle 2 wird deutlich, dass die Länge des Passworte und auch die Anzahl der Zeichen der verwendeten Alphabete eine ausschlaggebende Rolle spielen

**Meist verwendete Passwörter**

Die meist verwendeten Passwörter lassen sich in elf Kategorien einteilen. Namen, machohafte Begriffe und einfache alphanumerische Zeichenketten sind die meist verwendeten Passwortkategorien (information is beautiful, 2021b)

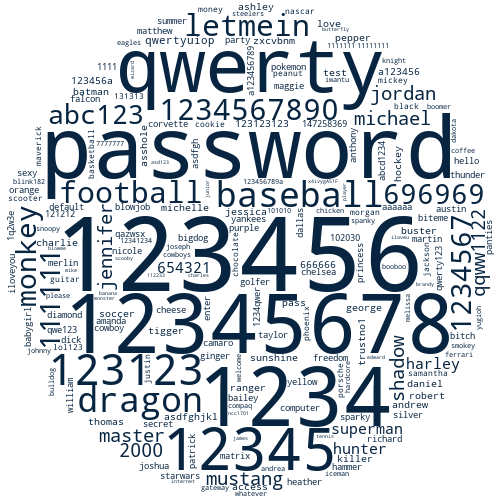


Abbildung 8: Wordcloud zu den meist genutzten Passwörtern (Quelle: information is beautiful, 2021b)

Neben Datenlecks sind schlecht gewählte Passwörter die größte Sicherheitslücke. Hacker können mit Hilfe automtischer Programme tausende Zeichenkombinationen in wenigen Sekunden testen. Ein gutes Passwort ist mindestens zehn Zeichenlang, enthält Buchstaben, Zahlen sowie Sonderzeichen und ist für jede Plattform unterschiedlich. Zur Unterstützung beim der Erstellung von Passwörtern hift die Satzregel. Dabei wird sich ein Satz überlegt. Zum Beispiel: Mein kleiner Kater Findus spielt gerne im Garten und ist sechs Jahre alt. Für ihr Passwort nehmen sie von jedem Wort ausschließlich den ersten Buchstaben und ersetzen bspw. und mit dem &-Zeichen. Aus dem Beispielsatz würde dann folgendes Passwort entstehen: MkKFsgiG&i6Ja. (Verbraucherzentrale, 2021)