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 Phishing-Mails, infizierte USB-Sticks, Schwachstellen von Software, oder auch Mitarbeitende enstehen. (AVG, 2019)

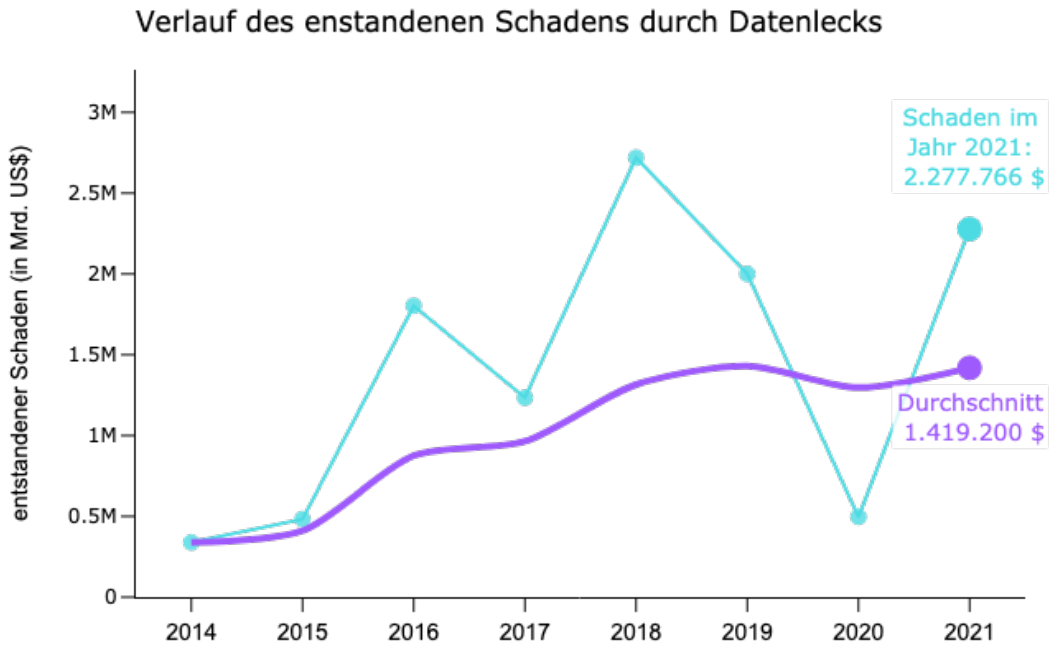


Abbildung 1: Datenlecks über die letzten 8 Jahre inklusive Durchschnitt (Quelle: information ist beautiful, 2021a)

In den letzten Jahre ist Summe der Schäden, die durch Datenlecks in den Unternehmen entstanden sind gestiegen (siehe dazu Abbildung 1 und Tabelle 1). Dies hat unter Anderem den Grund, dass Unternehmen immer häufiger Angegriffen werden und durch die Digitalisierung die Menge der Daten in den Unternehmen stetig steigt. Viele Daten die vor einigen Jahren noch lokal in den Unternhemen in Papierform vorlagen, werden heutzutage digitalisiert auf großen Servern gespeichert. Wo es Hackern früher noch gar nicht möglich war auf Daten zuzugreifen, besteht heut für diese ein rießiges Potenzial.

Jahr	Unternehmen	Schaden in Mio. US$	Mittelwert in Mio. US$
2014	Ebay	145	18
2015	Deep Root Analytics	198	19
2016	Yahoo	500	55
2017	Spambot	520	49
2018	Aadhaar	550	66
2019	Facebook	419	47
2020	Microsoft	250	19
2021	Linkedin	700	91

Tabelle 1: Unternehmen mit dem höchsten Schaden durch Data Breaches von Jahr 2014 bis 2021 inklusive der Mittelwerte (Quelle: information ist beautiful, 2021a)

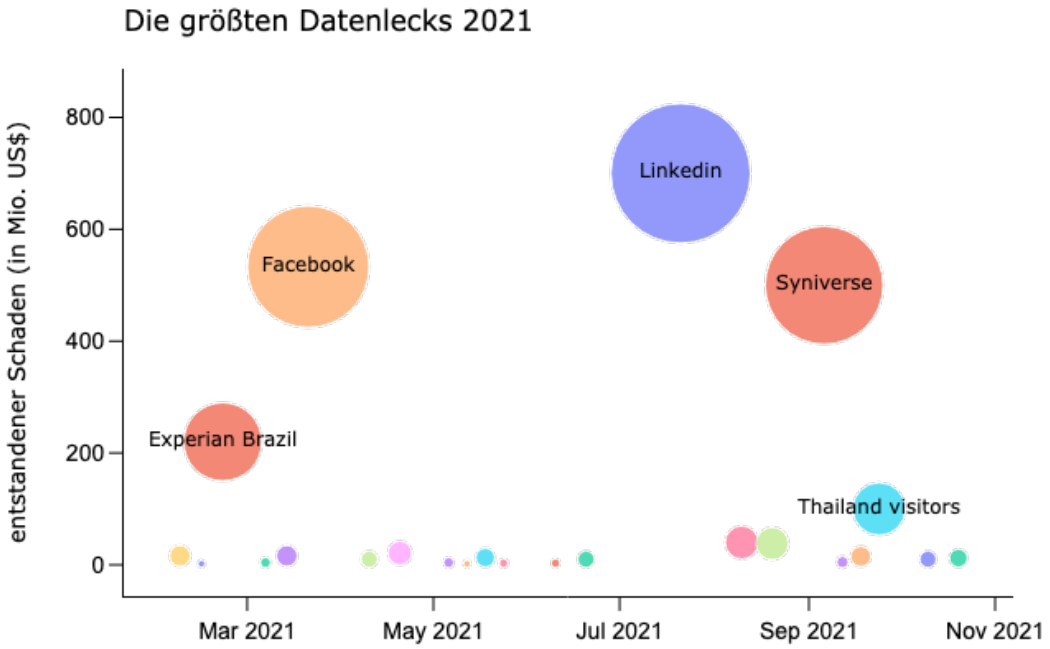


Abbildung 2: Data Breaches im Jahr 2021 (Quelle: information ist beautiful, 2021a)

Gerade bei größeren Unternehmen, die viele Daten speichern, sind die Schäden am höchsten. Haben es die Angreifer geschafft Zugriff zu erlangen, können sie meist direkt viele Daten abgreifen. Oft sind Unternehmen betroffen, die viele personenbezogene Daten speichern, wie bspw. Facebook und Linkedin.

Cyber Attacken

Hacker haben verschiedene Angriffsziele. Zunächst denkt man dabei an Hackerangriffe auf Systeme, bei dem der Angreifer die Schwächen des System ausnuzt. Allerdings können auch Menschen in das Ziel von Hackern geraten. Dabei ist das Ziel oft, Menschen zu manipulieren oder sie bestimmte Handlungen ausführen zu lassen, sodass der Angreifer Zugang zum System bekommt.

Im Jahr2021ist die Aufteilung der Cyberattacken 55 % Mensch und 45 % System.

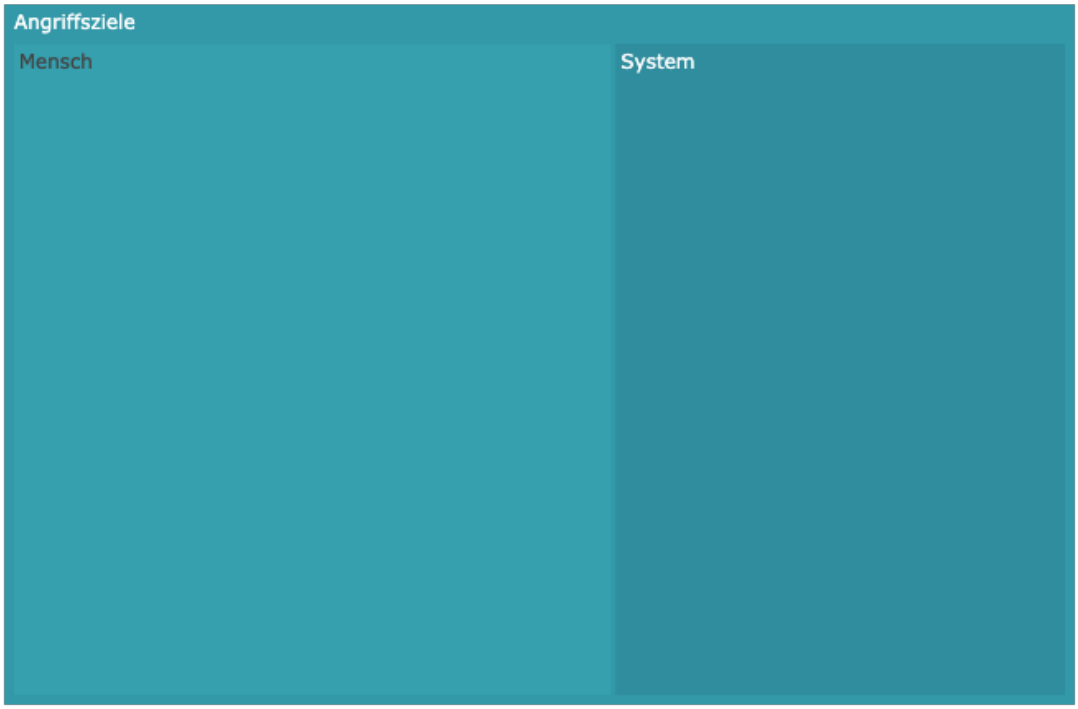


Abbildung 3: Cyber Attacken nach Angriffsvektor Mensch und System aufgeteilt (Quelle: IBM, 2021)

Systemschwächen sind häufig Ziele von Hackern. Dabei können alle möglichen Systeme angegriffen werden, die mit dem Internet verbunden sind. Um mögliche Schwachstellen in Systemen zu finden können externe Sicherheitsfirmen beauftragt werden, die einen Angriff simuliert.

Angriffsvektor Mensch

Menschliches Fehlverhalten sind eine häufige Ursache für Datenlecks. Meist rührt das Fehlverhalten von Unwissenheit oder Unachtsamkeit. Gegen Unachtsamkeit und mutwilliges böswilliges Verhalten kann leider schwer etwas unternommen werden. Aber

gegen Unwissenheit helfen Schulungen und Sensibilisierungskurse, die maßgeblich zum Schutz des Unternehmens beiträgt.

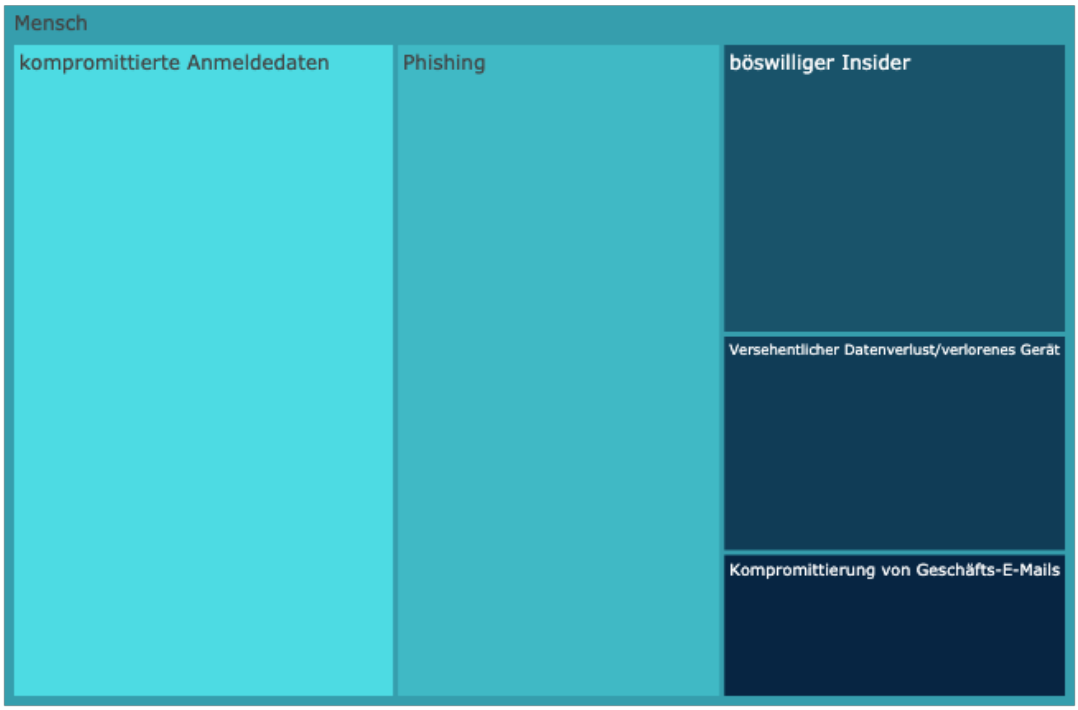


Abbildung 4: Cyber Attacken mit Angriffsvektor Mensch (Quelle: IBM, 2021)

Verteilung der Cyber Attacken mit Angriffsvektor Mensch

- Kompromittierte Anmeldedaten: 36 %
- Phishing: 30 %
- Böswilliger Insider: 14 %
- Versehentlicher Datenverlust/verlorenes Gerät: 10 %
- Kompromittierung von Geschäfts-E-Mails: 7 %

Im folgenden werden die zwei größten Angriffsvektoren beim Angriffvektor Mensch näher beschrieben.

Angriffsvektor Kompromittierte Anmeldedaten

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.

Angriffsvektor Phishing

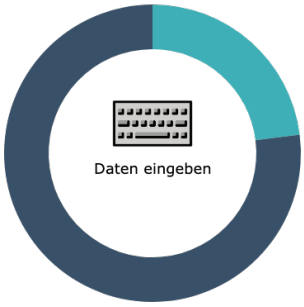
Von Phishing spricht man, wenn Betrüger E-Mails verschicken, welche darauf abzielen, heikle Informationen und Daten vom Empfänger zu erlangen. In der Regel erwecken die Mails den Anschein, von seriösen Unternehmen oder sogar offiziellen Institutionen und Dienstleistern (Polizei, Versicherungen, etc.) 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.Mehr zu Phishing ist im folgenden Kapitel zu finden.

Phishing

Die meist verbreitesten Arten von Phishing sind, das Senden eines URL-Hyperlinks, die Anfrage einer Dateneingabe und ein an eine E-Mail angefügter Anhang. Dabei sind Phishing Anriffe am meisten verbreitet. Die Angreifer sind über die letzten Jahre immer erfinderischer geworden. Oft verstecken sich Angreifer hinter weit verbreitete und vertrauenswürdige Diensten und täuschen so ihre Opfer, indem sie sich als echt ausgeben. Zu den meist verwendeten Themen von Phishing gehören bspw. Mircosoft Teams-Anfragen, Coronavirus-Alarmmeldungen aber auch Starbucks-Bonus oder UPS-Versandbenachrichtugnen. Oft versuchen Angreifer ihre Opfer mit raffinierten Themen wie kostenlosen Angeboten, Rabatten oder Ticketvorverkäufen zu überzeugen. (Proofpoint, 2021)

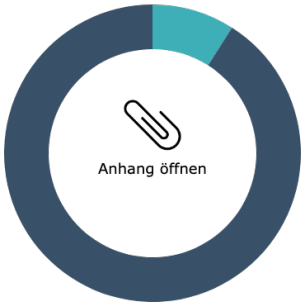
68% der Phishing Mails sollen den Nutzer dazu Veranlassen einen Link zu öffnen

Abbildung 5: Phishing via Link (Quelle: Proofpoint, 2021)



Bei 23% der Phishing Mails sollen der Nutzer sensible Daten angeben

Abbildung 6: Phishing via Input (Quelle: Proofpoint, 2021)



9% aller Phishing Mails zielen darauf ab, den Nutzer den Anhang öffnen zu lassen

Abbildung 6: Phishing via Anhang (Quelle: Proofpoint, 2021)

Im Folgenden werden die Fehlerquoten für 20 verschiedene Branchen und Abteilungen dargestellt.Die Fehlerquote bezieht sich dabei auf das Fehlverhalten bei Phishing-Angriffen durch bspw. auf öffnen eines URL-Hyperlinks. (Proofpoint, 2021)Der Gesamtdurchschnitt über alle Branchen hinweg lag bei 11 % (siehe Abb. 7). Bei den Abteilungen lag der Durchschnitt bei 11% (siehe Abb. 8).

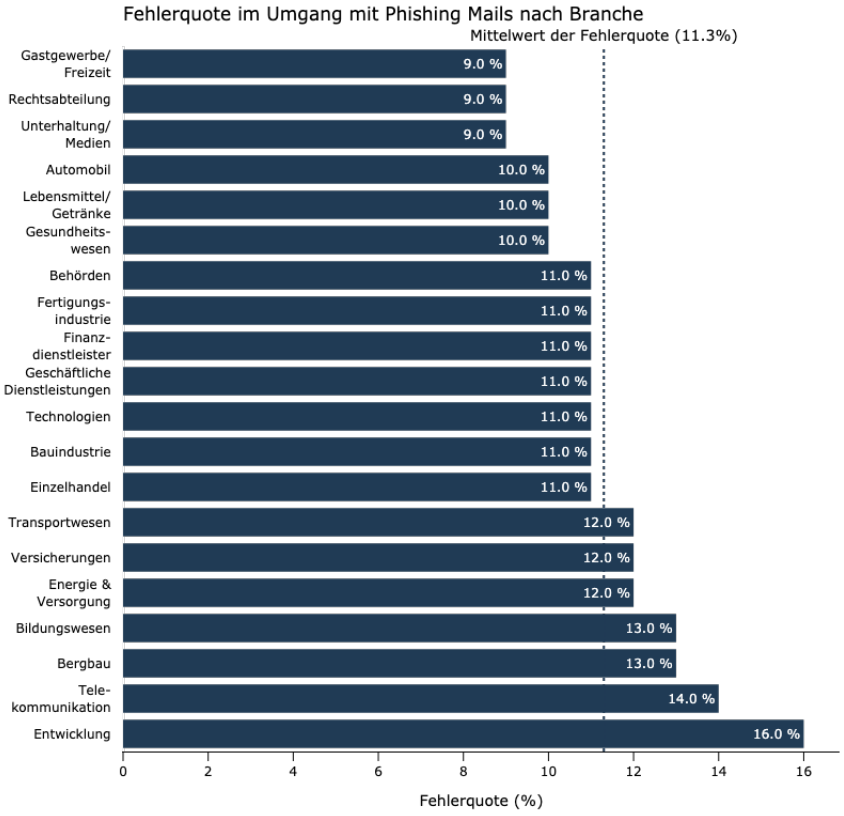


Abbildung 7: Phishing nach Branche

Fehlerquoten betrachtet auf einzelnen Abteilungsebene legt einen ausführlichen Überblick über mögliche Schwachstellen im Unternehmen. Angreifer haben meist einzelne Posteingänge und E-Mail-Aliase im Blick für einen Angriff. Eine Fehlerquote auf Unternehmensebene allein stellt nicht dar, bei welchen Teams oder Aufgabenbereiche möglicherweise Probleme auftreten. (Proofpoint, 2021)

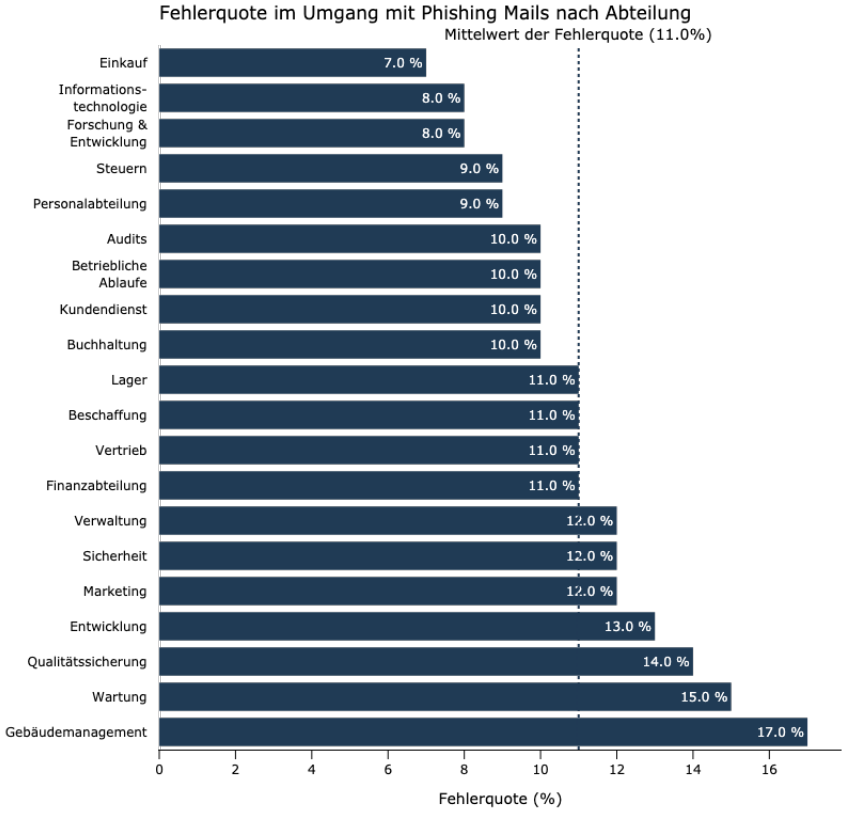


Abbildung 8: Phishing nach Branche (Quelle: Proofpoint, 2021)

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)

$$\text{Mögliche Kombinationen} = \text{Zeichenanzahl}^{\text{Passwortlänge}}$$

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

Verwendetes Alphabet	Anzahl der möglichen Zeichen	Länge des Pass-worts	Anzahl der möglichen Kombinationen	Zeit der vollständigen Suche
0-9	10	6	1.000.000	0,001 s
		8	100.000.000	0,1 s
		10	10.000.000.000	10 s
A-Z, a-z, 0-9	10	6	56.800.235.584	56 s
		8	218.340.105.584.896	12 h
		10	839.299.365.868.340.224	26 Jahre
A-Z, a-z, 0-9, 0[]{}?!$%& =*+~,.;:<>-_	10	6	404.567.235.136	11 min
		8	2.992.179.271.065.856	13 h
		10	22.130.157.888.803.070.976	1700 Jahre

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)

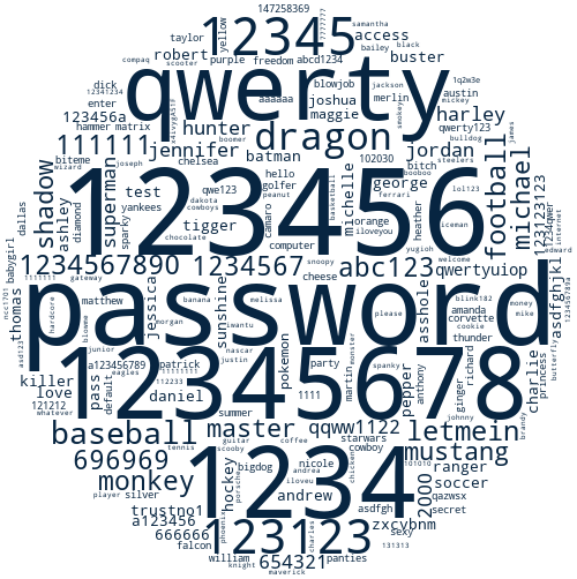


Abbildung 9: Wordcloud zu den meist genutzten Passwörtern (Quelle: information is beautiful, 2021b)

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)