# Was ist eine Datenschutzverletzung?

Eine Datenschutzverletzung bzw. ein Datenleck ist jeder **Vorfall**, bei dem unbefugt auf vertrauliche oder sensible Informationen zugegriffen wurde. Datenschutzverletzungen sind das Ergebnis eines Cyberangriffs, bei dem sich Kriminelle **unbefugten Zugang** zu einem Computersystem oder Netzwerk verschaffen und die darin enthaltenen privaten, sensiblen oder vertraulichen personenbezogenen und finanziellen Daten der Kunden oder Benutzer stehlen.

Das **U.S. Department of Justice** definiert eine Datenschutzverletzung als „Verlust der Kontrolle, Kompromittierung, unbefugte Offenlegung, unbefugte Aneignung, Zugriff zu einem unbefugten Zweck oder sonstiger unbefugter Zugriff auf physische oder elektronische Daten.“

**Häufige Cyberangriffe, die bei Datenschutzverletzungen verwendet werden**, sind:

* Ransomware
* Malware
* Phishing
* Denial-Of-Service

Abseits der Cyberangriffe gibt es beispielsweise Insider-Leaks, Zahlungskartenbetrug, Verlust oder Diebstahl von physischen Festplatten mit Dateien sowie menschliches Versagen.

# Ransomware

[Ransomware](https://www.varonis.com/blog/ransomware-guide/) ist Software, die sich Zugang zu wichtigen Daten verschafft und den Zugriff auf diese unmöglich macht. Dateien und **Systeme werden gesperrt** und es wird ein **Lösegeld**, meist in Form von Kryptowährung, verlangt.

**Häufige Ziele:** Unternehmen und Betriebe

# Malware

[Malware](https://www.varonis.com/blog/malware-protection-defending-data-with-varonis-security-analytics/), gemeinhin als „bösartige Software“ bezeichnet, ist ein Begriff, unter den Programme und Code fallen, **die auf schädliche Weise in Systeme eindringen**. Malware ist darauf ausgelegt, Ihren Computer oder Ihre Software zu schädigen, und tarnt sich häufig als Warnung vor Schadsoftware. Durch die „Warnung“ wird versucht, Benutzer davon zu überzeugen, verschiedene Arten von Software herunterzuladen. Obwohl Malware die physische Hardware des Systems nicht beschädigt, kann sie **Daten stehlen**, **verschlüsseln** oder die **Kontrolle über Computerfunktionen** übernehmen.

Malware kann eindringen, wenn Sie **gehackte Websites** besuchen, infizierte Dateien herunterladen oder E-Mails von einem Gerät öffnen, auf dem **kein Malware-Schutz** vorhanden ist.

**Häufige Ziele**: Privatpersonen und Unternehmen

# Phishing und Spear Phishing

[Phishing](https://www.varonis.com/blog/phishing-attacks/) ist eine der **gängigsten Methoden**, mit denen sich Hacker Zugang zu sensiblen oder vertraulichen Informationen verschaffen. Beim Phishing werden **betrügerische E-Mails** versendet, die den Anschein erwecken, von einem bekannten Unternehmen zu stammen. Ziel ist es, die Empfänger dazu zu verleiten, entweder auf einen **bösartigen Link** zu klicken oder einen **infizierten Anhang** herunterzuladen, um dann meistens finanzielle oder vertrauliche Daten zu stehlen.

Unter **Spear Phishing** (dt: „Speer“) versteht man einen **gezielten Angriff** auf eine bestimmte Person oder Mitarbeiter eines **spezifischen Unternehmens**. Am häufigsten werden hochrangige Mitarbeiter mit Zugang zu potenziell attraktiven Informationen oder auch Administratoren angegriffen.

Spear Phishing ist besonders gefährlich: Cyberkriminelle sammeln akribisch Informationen über das Opfer und machen ihm den „Köder“ beabsichtigt noch schmackhafter. Denn mittlerweile ist eine gut aufgebaute Phishing-E-Mail kaum noch von einer legitimen E-Mail zu unterscheiden.

**Häufige Ziele**: Privatpersonen und Unternehmen

# Denial of Service (DoS)

[Denial of Service](https://www.varonis.com/blog/what-is-a-ddos-attack/) ist ein Cyberangriff, bei dem der Täter versucht, einen Rechner oder eine Netzwerkressource für die vorgesehenen Benutzer **nicht verfügbar zu machen**, indem er die Funktion eines mit dem Internet verbundenen Hosts vorübergehend oder auf unbestimmte Zeit unterbricht. In der Regel wird dies erreicht, indem der angegriffene Rechner oder die angegriffene Ressource **mit unnötigen Anfragen überflutet** wird. Dadurch werden die **Systeme überlastet** und es wird verhindert, dass einige oder alle normalen Anfragen beantwortet werden.

**Häufige Ziele**: Websites / Dienste, die auf wichtigen Webservern gehostet werden, wie z. B. Banken

Quelle: Nach <https://blog.varonis.de/statistiken-zu-datenschutzverletzungen/> Abg. am 20.9.2021

# Aufgaben:

Schreiben Sie sich eine eigene Definition für die fünf Cyberangriffe!

Ransomware: Schadsoftware, die Daten verschlüsselt und ein Lösegeld für die Entschlüsselung fordert.

Malware: Bösartige Software, die Systeme schädigen oder Daten stehlen kann.

Phishing: Betrügerische E-Mails, die versuchen, sensible Informationen zu stehlen.

Spear Phishing: Gezielte Phishing-Angriffe auf bestimmte Personen oder Unternehmen.

Denial of Service (DoS): Angriff, der einen Rechner oder eine Netzwerkressource für Benutzer unzugänglich macht.

Ordnen Sie jeweils einen der fünf Cyberangriffe zu (auf die Linie schreiben)!

Ihr Vater bekommt einen Anruf von „Microsoft“, sein System sei gefährdet…

Phishing

Man fragt mich am Telefon nach persönlichen Vorlieben und Gewohnheiten anderer Mitarbeiter.

Spear-Phishing

Einige meiner Dateien haben plötzlich alle die Endung.crypt.

Ransomware

Ein Mitarbeiter erhält einen Anruf vom IT-Administrator. Nach etwas

Fachchinesisch und dem Aufbau von Druck macht er klar, dass er für die

Behebung eines dringenden technischen Problems das Passwort benötigt.

Phising

Der Zugriff auf die Webseite meines Onlineshops ist unmöglich/verlangsamt.

Denial of Service

2020 hat Spotify für eine nicht veröffentlichte Anzahl seiner Nutzer die Passwörter zurückgesetzt, nachdem ihre Kontodaten durch eine Software-Sicherheitslücke offengelegt worden waren.  
Malware

Viele Nutzer bestätigen ihre Ebay-Zugangsdaten auf dubiosen Seiten, obwohl klar ist, dass Ebay die eigentlich hätte haben sollen. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Hacker legten das Schließsystem des Hotels Jägerwirt in Kärnten lahm, so dass im voll ausgebuchten Vier-Sterne-Haus die Türen zu den Hotelzimmern nicht mehr zu öffnen sind.  
 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Das Botnetz Mirai sorgt im Oktober 2016 für massive Ausfälle im gesamten Internet. Dienste wie Twitter oder Paypal sind nicht mehr erreichbar. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_