Handbuch
für erfolgreiche
DATEN-SICHERHEIT

www.tannwald.com

TANNWALD MEDIA

Inhalt

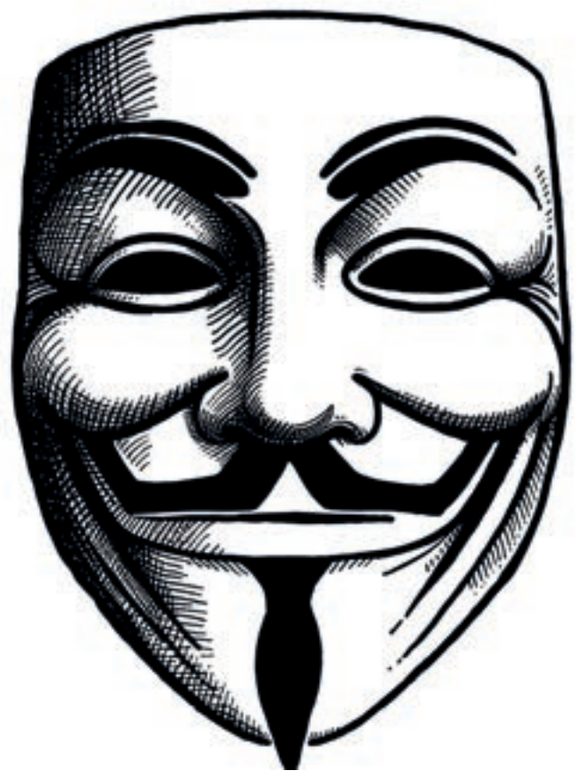
Wer will an Ihre Daten?

1

Konzerne nutzen Ihre Daten, um Geld zu machen.

Kriminelle verkaufen Ihre Informationen oder nutzen diese aus.

Ihre **Gegner** wollen Ihnen schaden.

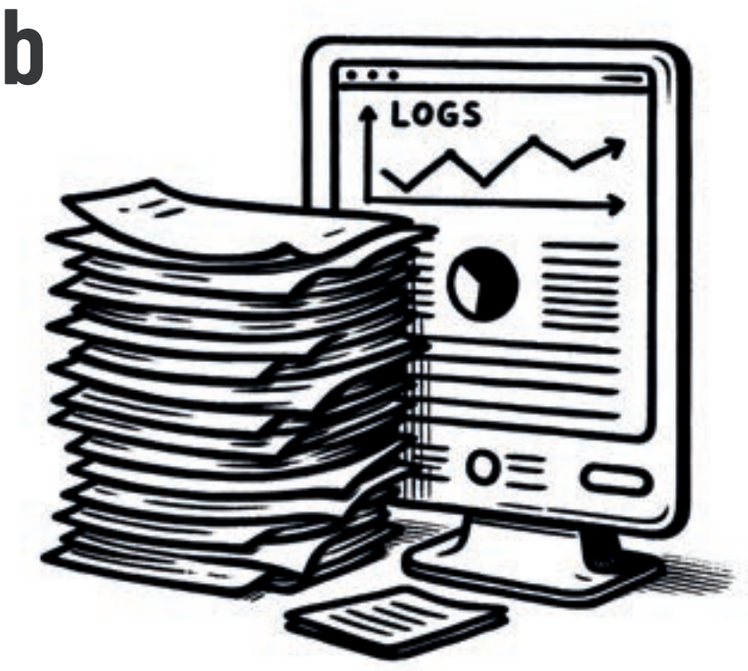


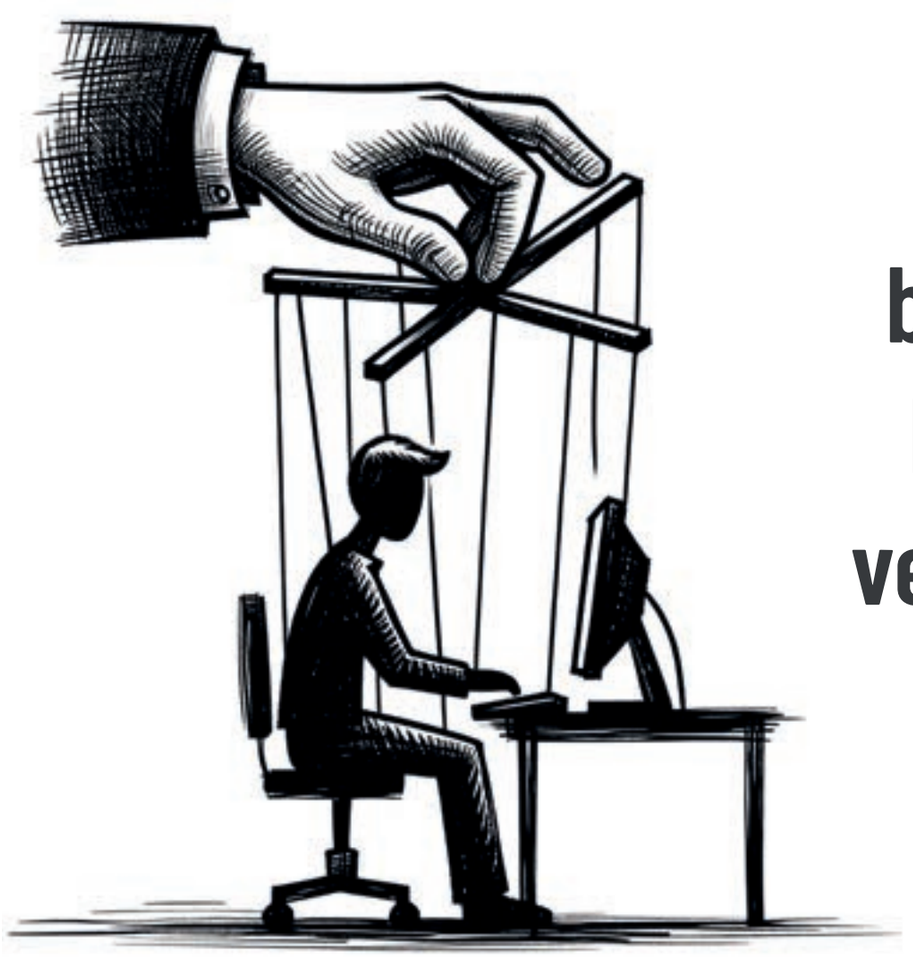
2

Wie kommt man an Ihre Daten?

Logs & Metadaten

Logs sind Aufzeichnungen von Ereignissen oder Prozessen innerhalb eines Systems, während Metadaten Informationen über andere Daten liefern, wie z.B. Zeitstempel oder Standorte.





Social Engineering

bezeichnet die Manipulation von Personen, um sie zur Preisgabe vertraulicher Informationen oder zur Durchführung bestimmter Aktionen zu bewegen.

Dumpster Diving

bezieht sich auf das Durchsuchen von Müll nach nützlichen Informationen wie Dokumenten, Datenträgern oder Notizen.

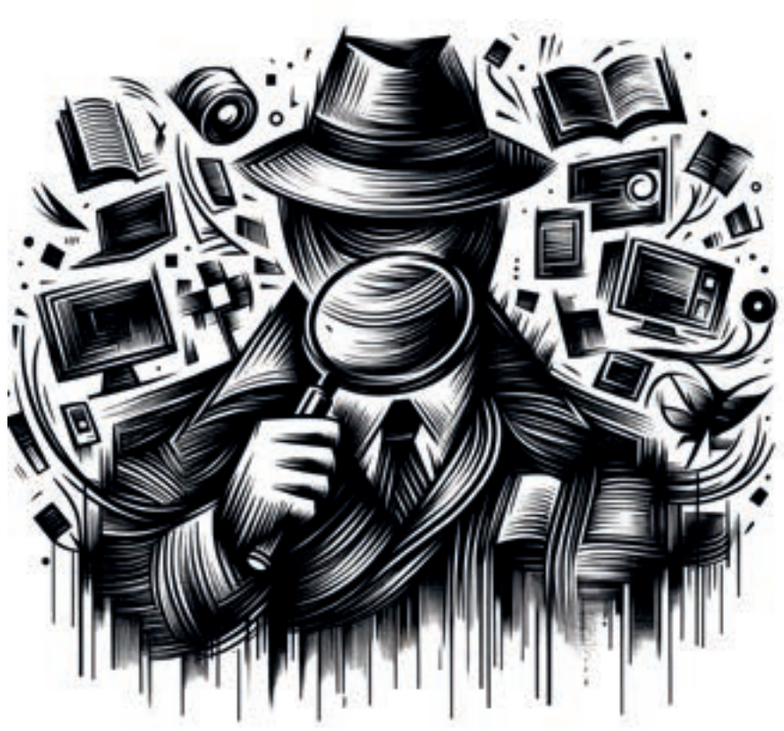
www.tannwald.com

TANNWALD MEDIA

3

OSINT

„Open Source Intelligence“ bezeichnet die Sammlung und Analyse von Informationen aus öffentlich zugänglichen Quellen.



Phishing

Phishing ist ein Cyberangriff, bei dem Täter über gefälschte Kommunikation (z.B. E-Mails oder Nachrichten) vertrauliche Daten von Opfern erlangen.

Gesetze und Überwachung

Staatliche Behörden dürfen unter gesetzlich geregelten Bedingungen auf Ihre privaten Daten zugreifen.

www.tannwald.com

TANNWALD MEDIA

Datenschutz
Grundsätze

4

Die drei Vs

Grundsätzliche Vorkehrungen zum Datenschutz sind das Verstecken, das Vernichten oder das Verschlüsseln der Daten.

Verstecken

muss sich nicht nur auf die eigenen vier Wände beziehen. Verschlüsselte Backups wichtiger Daten können bspw. bei Familie und Freunden sicher verwahrt werden.

Vernichten

Daten auf Speichermedien müssen fachgerecht überschrieben werden. Defekte Datenträger sollten physikalisch zerstört werden. Nutzen Sie für Dokumente einen Aktenvernichter.

www.tannwald.com

TANNWALD MEDIA

Erfolgreich Verschlüsseln

5

VPN (NordVPN etc.)

Ein Virtual Private Network wie NordVPN verschlüsselt und leitet ihre Internetverbindung über einen entfernten Server um, um ihre Online-Privatssphäre und Sicherheit zu verbessern.

Messenger

Verwenden Sie Messenging-Dienste wie WhatsApp, Signal, Threema, oder geheime Chats bei Telegram, die eine Ende-zu-Ende-Verschlüsselung bieten.

HTTPS

**(Hypertext Transfer Protocol Secure) findet man in der Adresszeile des Browsers als Teil der URL.
Es signalisiert, dass die Verbindung zu dieser Netzseite verschlüsselt ist.**

6

TLS (E-Mails)

(Transport Layer Security)
ist ein Sicherheitsprotokoll,
das Datenübertragung im Internet
verschlüsselt und schützt.

Datenträger

Das verschlüsseln von Festplatten
im Alltag ist essenziell.
Mit Verschlüsselungsprogrammen
wie FileVault oder VeraCrypt wird
der Zugang ohne passenden Schlüssel
oder Passwort gesperrt.

WLAN

Meiden Sie WPS und nutzen
Sie stattdessen WPA2 bzw. WPA3.
Richten Sie ein separates Netzwerk
für Gäste ein. Das Passwort sollte über
mindestens 20 Zeichen verfügen.

Metadaten

Dateien wie PDFs und Fotos, die direkt online
gehostet werden, enthalten Metadaten.
Diese können persönliche Informationen,
wie bspw. GPS-Koordinaten enthalten.
Lassen Sie sich diesbezüglich von
Tannwald Media beraten.

www.tannwald.com

TANNWALD MEDIA

7

Sichere Passwörter

Komplexität

Ein sicheres Passwort enthält Groß- und Kleinbuchstaben, Zahlen, sowie Sonderzeichen. Es sollte aus mindestens 12, idealerweise aus 18 Zeichen bestehen.

Passwort-Manager

sind Programme, die alle Ihre Passwörter sicher speichern und Ihnen ermöglichen, diese mit einem starken Master-Passwort abzurufen.

MFA

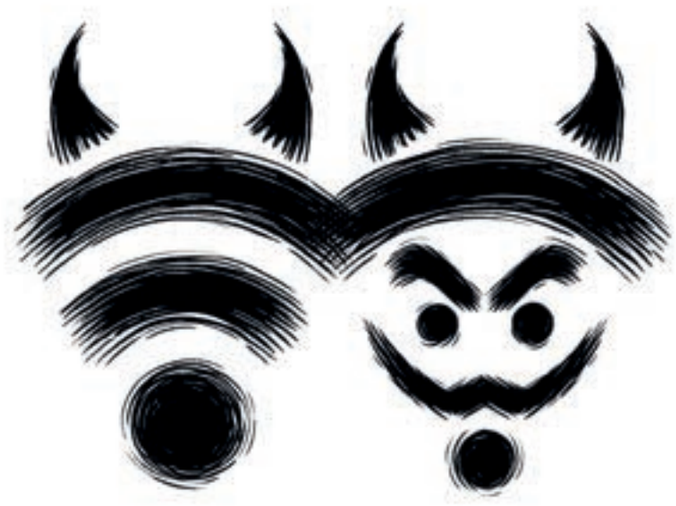
Mehrfaktorenauthentifizierung fordert Sie auf, mindestens zwei Nachweise zur Verifizierung Ihrer Identität bereitzustellen, bevor Sie Zugang erhalten.

Datenschutz unterwegs

8

HotSpots & freie WLANS

sollten gemieden werden, da sie oft ungesichert sind, die Verbindungen aufgezeichnet werden und der Datenstrom manipuliert werden kann.



Evil Twin

Ein „Evil Twin“ ist ein betrügerischer WLAN-Zugangspunkt, der legitim erscheint, aber von Cyberkriminellen eingerichtet wurde, um persönliche Daten von Nutzern zu stehlen.

Standortermittlung

Deaktivieren Sie die Standort-ermittlungsdienste auf Ihrem Gerät. Nutzen Sie VPN-Dienste, um die eigene IP-Adresse zu verschleiern. Verwenden Sie ggf. ein „Dumbphone“ ohne Standortermittlungsdienste.

www.tannwald.com

TANNWALD MEDIA

Weitere Vorkehrungen

9

Clouds

Wenn Sie Daten in einer Cloud speichern, bedeutet dies, dass Sie Ihre Daten auf einem fremden Computer speichern. Dieser kann Sicherheitslücken wie unzureichende Verschlüsselung aufweisen.

Webhosting

Anonymes Webhosting ist durch nicht nachverfolgbare Zahlungs- und Registrierungsmethoden möglich. Beliebt sind Offshore-Hosts in Ländern wie Island und der Schweiz.

Kryptowährungen

bieten den Vorteil der dezentralen Transaktionsabwicklung ohne traditionelle Banken, was Anonymität bietet.

10

Privates & Geschäftliches

sollte grundsätzlich getrennt werden. Nutzen Sie separate Geräte, Konten und Datenträger, um sich vor Cyberangriffen zu schützen.

So wenig wie möglich

und so viel wie nötig. Umso weniger Anwendungen, Accounts etc. Sie nutzen, desto geringer ist das Risiko für Missbrauch Ihrer Daten und Datenlecks.

Datenschutz Checkliste

11

1. Passwortwechsel

Ändern Sie regelmäßig (alle 3 Monate) Ihre Passwörter, um die Sicherheit Ihrer Konten zu erhöhen. ☐

2. Software-Updates

Installieren Sie Software-Updates sofort, um bekannte Sicherheitslücken zu schließen ☐

3. Antivirus-Überprüfung

Nutzen Sie ein aktuelles Antivirus-Programm, bspw. Norton AntiVirus, um Ihren Computer vor Malware zu schützen. ☐

4. WLAN

Vermeiden Sie die Nutzung öffentlicher WLANs für sensible Aktivitäten. Nutzen Sie VPNs, bspw. NordVPN. ☐

5. Datensicherung

Erstellen Sie regelmäßige Backups ihrer Daten, um im Falle eines Datenverlustes abgesichert zu sein. ☐

6. Überprüfung der Berechtigungen

Erstellen Sie regelmäßige Backups Ihrer Daten, um im Falle eines Datenverlustes abgesichert zu sein. ☐

7. Physikalische Sicherheit

Bewahren Sie Ihre Geräte sicher auf und vernichten Sie zu entsorgende Unterlagen fachgemäß. ☐

8. Vorsicht bei E-Mails und Anhängen

Öffnen Sie keine Anhänge unbekannter E-Mail-Adressen, um Phishing-Angriffe zu vermeiden. ☐

9. Sicherheit von Netzseiten

Besuchen Sie ausschließlich sichere Netzseiten, die HTTPS verwenden. ☐

10. Privates & Geschäftliches

Halten Sie berufliche und private Daten strikt getrennt, um beide Bereiche optimal zu schützen. ☐

www.tannwald.com

TANNWALD MEDIA

Noch Fragen?

Wir beraten Sie gern!

TANNWALD MEDIA

Kontakt

Tel.: 0341 9899 5414

Mobil: 0152 3777 0340

Mail: info@tannwald.com

Instagram: @tannwald_media

www.tannwald.com