Cybersicherheitsvorfälle

Wann soll ich einen Vorfall der Polizei melden?

Was ist ein Cybersicherheitsvorfall?

Ein Cybersicherheitsvorfall ist ein absichtlicher **Angriff auf** die

- **Vertraulichkeit,**
- **Verfügbarkeit**
- und/oder **Integrität**

von Daten/IT-Systemen, der Betroffene im **großen Ausmaß**[1] beeinträchtigt.

Warum soll ich einen Vorfall der Polizei melden?

1. **Aufklärung der Straftat.** Meist handelt es sich um **Offizialdelikte**, die von Strafverfolgungsbehörden von Amts wegen verfolgt werden, wie z.B.:
   - Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)
   - Datenbeschädigung (§ 126a StGB)
   - Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)
   - Erpressung (§ 144 StGB)
2. **Schadenswiedergutmachung** (wenn Täterschaft ausgeforscht ist)
3. **Anzeigenbestätigung** für Versicherung
4. **Absicherung gegenüber Dritten** (wegen etwaiger Schadensforderungen)
5. **Unterstützung der polizeilichen Ermittlungsarbeit** (neue Daten können neue Ermittlungsansätze ergeben => erhöht die Wahrscheinlichkeit der Tataufklärung)

Was tut die Polizei?

1. **Strafverfolgung/Ausforschung der Täterschaft** mit den Mitteln der digitalen Ermittlungen, digitalen Forensik und klassischen Ermittlungsarbeit
2. **Cyber-Prävention:** Wissen generieren, teilen und vermitteln
3. **Interne Verständigungen** durchführen (Berichtspflichten)

---

1 Zum Beispiel großes mediales Aufsehen, längere Zeit andauernde Beeinträchtigung, Wertqualifikation.

Welche Aufgaben übernimmt die Polizei nicht? (exemplarische Aufzählung)

1. Datenwiederherstellung von gelöschten Daten
2. Entschlüsselung von Daten
3. IT-Sicherheit von Betroffenen überprüfen und verbessern
4. Consulting/Training
5. Produktempfehlungen aussprechen
6. Meldepflichten des Betroffenen übernehmen

Beweismittelsicherung – was kann relevant sein?

1. **Logdateien** (mit IP-Adressen und Zeitstempel, Windows Event Logs, etc.)
2. **Datenträger-Images** („Patient Null“ -> erstes angegriffenes Gerät)
3. **Schadsoftware**
4. Informationen zu **Tools, welche die Täterschaft verwendet (hat)**
5. **E-Mail-Adressen der Täterschaft** bzw. E-Mail-Schriftverkehr im Original (inkl. E-Mail-Header)
6. **Etwaige Erpresserschreiben**
7. **Zahlungsinformationen** (Kryptowährungsadressen, Bankkonten, Informationen über verwendete bargeldlose Zahlungsmittel, …)

Wie anzeigen?

Jede gerichtlich strafbare Handlung kann **auf jeder Polizeidienststelle** angezeigt werden. Die rasche Übermittlung von digitalen Beweismitteln spielt dabei eine wichtige Rolle. Technisch fachkundige Polizistinnen und Polizisten, sogenannte Bezirks-IT-Ermittlerinnen und IT-Ermittler, unterstützen je nach Verfügbarkeit. Ist Ihr Unternehmen Teil der kritischen Infrastruktur (= Teil der ACI-Liste), weisen Sie bei der Anzeige darauf hin.

post@dsn.gv.at
dsn.gv.at

Impressum
Medieninhaber: Bundesministerium für Inneres,
Direktion Staatsschutz und Nachrichtendienst (DSN)
1010 Wien, Herrengasse 7, +43 1 531 26-0
Layout: Abteilung I/C/10/a – Strategische Kommunikation und Kreation
Fotos: Adobe Stock
Hersteller: Digitalprintcenter des BMI, 1010 Wien, Herrengasse 7
Wien, 2023