LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Behörden in Liechtenstein – Gemeinsam für Cyber-Sicherheit

13. November 2024 – Liechtensteiner Braustube

Agenda

1. Kurze Vorstellung der Behörden
2. Prävention
3. Fallbeispiel einer Ransomware-Attacke
4. Wie unterstützen Behörden? Welche Pflichten haben Unternehmen?
5. Q&A
6. Apéro

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Vorstellung der Behörden

Datenschutzstelle Fürstentum Liechtenstein

8 Mitarbeitende

- **5 Juristinnen / Juristen**
- **2 IT-Experten**
- **1 Assistentin**

Landespolizei Kommissariat Digitale Kriminalität

- Gegründet 1.1.2021
- 4 Mitarbeitende

- Fachbereich IT-Forensik: Forensische Sicherung digitaler Spuren
- Fachbereich IT-Ermittlung: Ermittlungen zu Straftaten im Cybercrime-Bereich
  Ziel: Identifikation und Lokalisation der unbekannten Täterschaft

Stabsstelle Cyber-Sicherheit

Die Stabsstelle Cyber-Sicherheit des Fürstentums Liechtenstein ist die zentrale Anlaufstelle für sämtliche Belange im Umgang mit Cyber-Risiken.

Sie fungiert als Drehscheibe, Vermittlungs- und Verbindungsstelle für die Bevölkerung, die Wirtschaft, der kritischen Infrastrukturen sowie der Staatsorgane.

Gegründet: Oktober 2020

Operativ tätig: Februar 2022

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Prävention

SCS - CSIRT

Vorbereitung

- Systeme kennen
- Vorfälle erkennen können
- Sicherheitskonzepte haben
- Verantwortliche identifizieren
- Kommunikation planen
- Dinge klären, die man klären kann
- …

Vorbereitung

IT-Sicherheits- und Datenschutzstandards sowie einschlägige Richtlinien können helfen.

Warn- und Informationsdienst (WID)

- Regelmässige Warnungen & Infos an
  - KRITIS
  - LI-Unternehmen
- Niederschwelliger Zugang über einfache Registrierung
- Ziel: Berücksichtigung in der Risikobewertung/Behebung

https://csirt.li

Vulnerability Intelligence (nicht nur)

Quellen:

- Mailing-Listen
- Infos von Partner-Organisationen
- Einschlägige IT-Security-Webseiten
- Sicherheitsforscher (u.a. auf Social Media)
- …

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Cybersicherheit BACS

CERT Bund

heise security

CERT.at

Jan 11

Kritische Sicherheitslücken in Ivanti Connect Secure und Ivanti Policy Secure - aktiv ausgenützt

Sicherheitsforscher:innen haben in Produkten der Firma Ivanti zwei schwere Sicherheitslücken entdeckt, deren kombinierte Ausnutzung entfernte, unauthentifizierte Ausführung von Code ermöglichen.

Weiterlesen →

CSA SINGAPORE

ALERTS

Active Exploitation of Zero Day Vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secu...

11 Jan 2024

Ivanti has released security updates to address two zero-day vulnerabilities impacting Ivanti Connect Secure and Ivanti...

Warnmeldung

gem. Kriterien des CSIRT:

- weit verbreitete Soft- oder Hardware
- Schwachstelle leicht ausnutzbar (Ferne, unauthentisiert)

aus anderen Gründen relevant

Spezifische Schwachstellenhinweise (SSH)

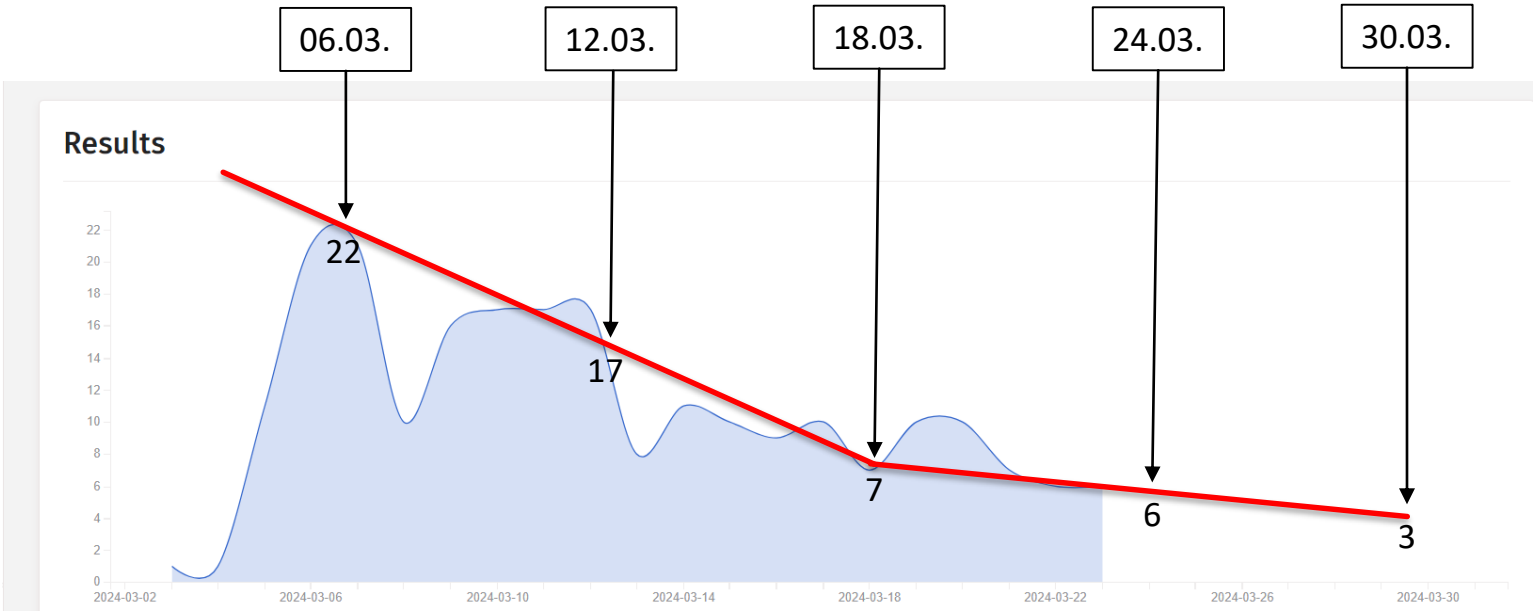
- Gezielte Warnungen zu konkret angreifbaren Systemen oder Fehlkonfigurationen, auf Basis
  - Scan-Ergebnisse von Partnern
  - Eigene Suche in der LI-Domain
- Mitteilung an ISP/IT-Dienstleister/Betr.
- Ziel: Berücksichtigung in der Risikobewertung/Behebung

https://csirt.li

Cyber-Hygiene-Massnahme…

… zur **Verhinderung der Kompromittierung**

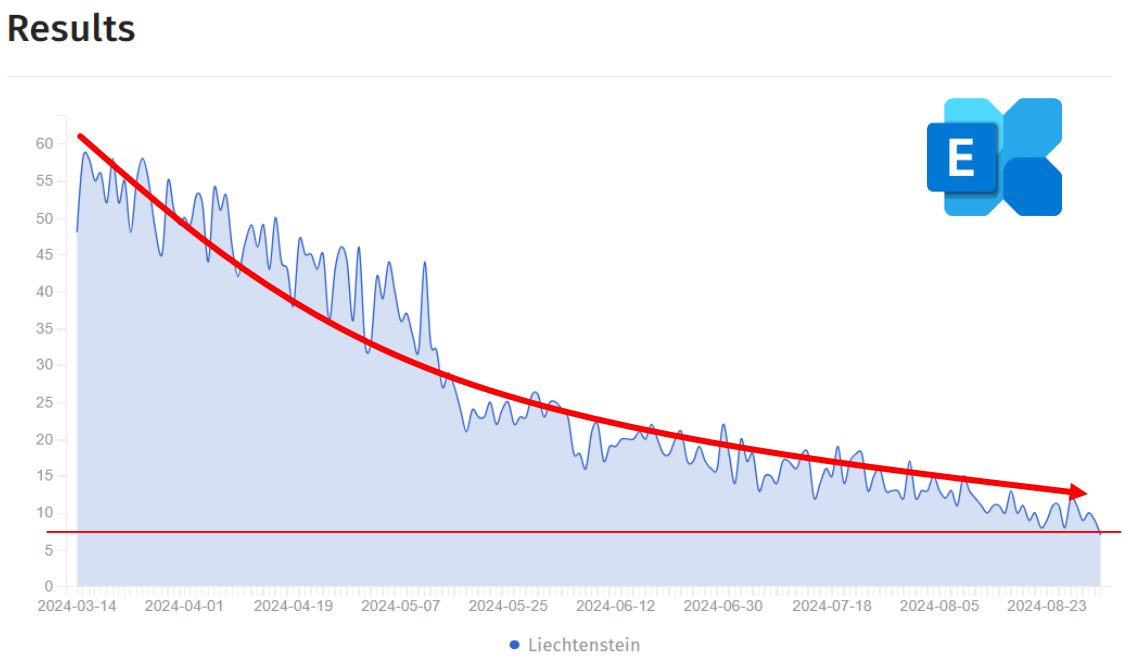
FORTINET
CVE-2024-21762



CSIRT.LI

Cyber-Hygiene-Massnahme…

… zur **Verhinderung der Kompromittierung + im Sinne des digitalen Ökosystems**



Monitoring

Monitoring von Echtzeitdaten und kontinuierlichen Statistiken mit dem Ziel

- Lageeinschätzung
- Erkennung von Angriffen

https://csirt.li

- Detektion
- Alarmierung
- Koordination
- Kooperation
- Warnung
- Analyse
- Reporting

regierung.li/medienportal-medium/16182/232241/0/medienmitteilung

REGIERUNG
DES FÜRSTENTUMS LIECHTENSTEIN

English Kontakt Datenschutz

Menü

Medienportal | Medienanlässe | **Medienmitteilungen** | Fotoservice | RegierungsTV | Filmbeiträge

Montag, 8.7.2024

DDoS-Angriff: Website der Liechtensteinischen Landesverwaltung www.llv.li nicht erreichbar

Seit Montag, 8. Juli 2024, ca. 12 Uhr, ist die Website der Liechtensteinischen Landesverwaltung www.llv.li nicht erreichbar. Auch die Website der Regierung www.regierung.li war von einem Angriff betroffen. Der Ausfall konnte zwischenzeitlich behoben werden. Grund dafür sind sogenannte DDoS-Angriffe auf die Provider der LLV sowie der Regierung. Die Angriffe wurden rasch bemerkt und entsprechende Massnahmen und Abklärungen wurden eingeleitet.

Eine pro-russische Hackergruppe hat sich zu den Angriffen auf die Websites bekannt.

DDoS steht für "Distributed Denial of Service". Bei einem DDoS-Angriff geht es darum, Websites und Anwendungen mit gezielten und verteilten Anfragen zu überlasten, damit diese nicht mehr erreichbar sind. Ein Datenabfluss findet bei einem solchen Angriff nicht statt.

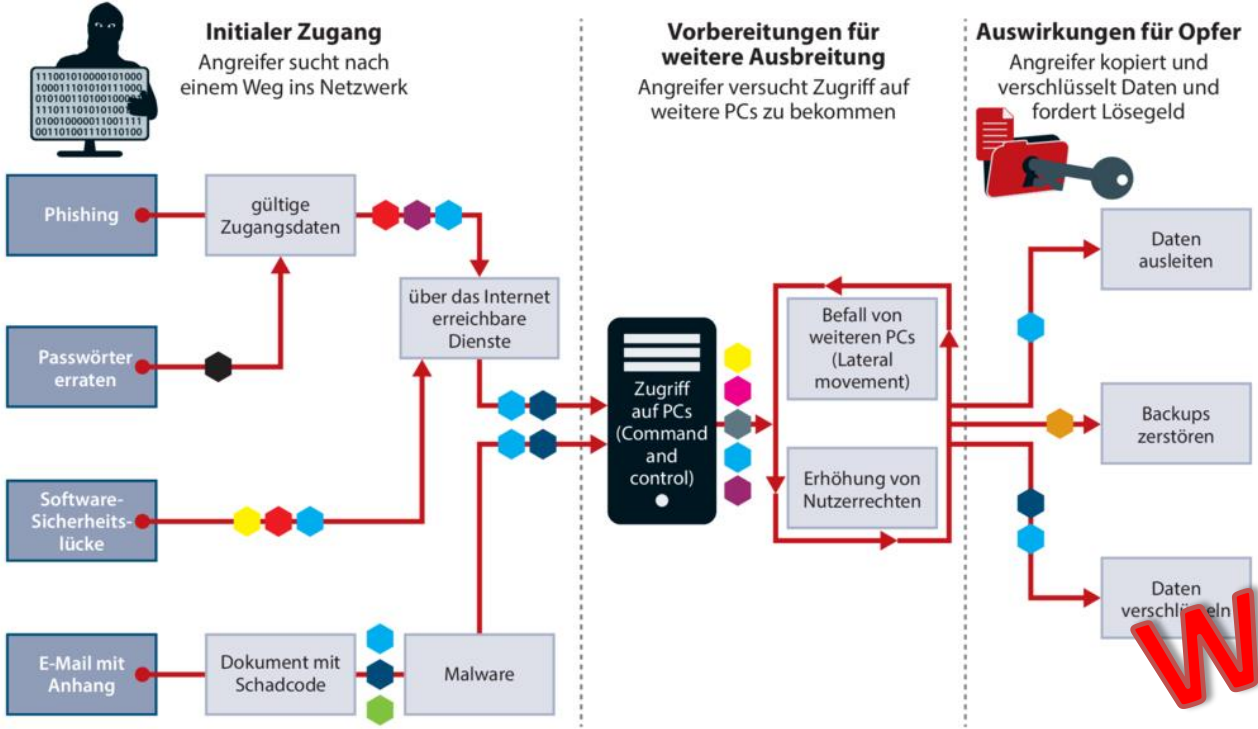

FIRST
Improving Security Together
TI
CENTRE FOR CYBERSECURITY BELGIUM
LHC
Luxembourg House of Cybersecurity
CERT.at
BSI
CSIRTs NETWORK
Switch_

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Fallbeispiel einer Ransomware-Attacke

Fallbeispiel: Ransomware-Angriff

- Ransomware = Art von Schadprogramm, das Zugriff auf Daten oder System einschränkt oder unterbindet
- Für Freigabe wird ein Lösegeld (englisch: Ransom) verlangt
- Daten gestohlen und anschliessend verschlüsselt
- Erpresserschreiben: z.B. 1 Mio in BTC innert 2 Tagen



Was nun?

Quelle:
c’t magazin für computer technik
https://www.heise.de/ct/

Fallbeispiel: Ransomware-Angriff

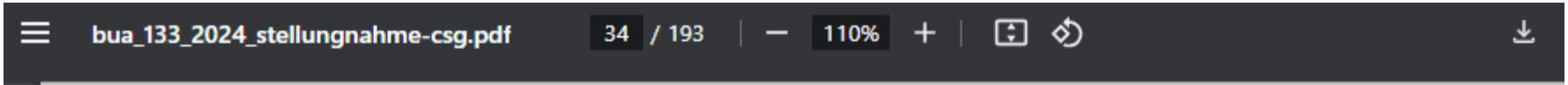
Was nun?

- Eigenverantwortung
- Ablauf gemäss vorher überlegten Abläufen
- Wir als Behörden unterstützen

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Melde-/Berichtspflichten

SCS - CSIRT



Art. 6

Berichtspflichten

1) Wesentliche und wichtige Einrichtungen haben erhebliche Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit unverzüglich zu melden.

2) Für die Zwecke der Meldung nach Abs. 1 haben die betroffenen Einrichtungen der Stabsstelle Cyber-Sicherheit Folgendes zu übermitteln:

Berichtspflicht nach Art. 6 RevCSG

1. Frühwarnung (unverzüglich bis max. 24h) – Art. 6 Abs. 2 Bst. a
2. Meldung (unverzüglich bis max. 72h) – Art. 6 Abs. 2 Bst. b
3. Zwischenbericht (auf Ersuchen der SCS) – Art. 6 Abs. 2 Bst. c
4. Abschlussbericht (innert 1 Monat nach Meldung, s. Pkt. 2) – Art. 6 Abs. 2 Bst. d

Art. 9

Freiwillige Meldung

1) Jede Einrichtung kann Sicherheitsvorfälle, Cyberbedrohungen oder Beinahe-Vorfälle der Stabsstelle Cyber-Sicherheit melden.

2) Die freiwillige Meldung muss weder die Identität der Einrichtung noch Informationen, die auf diese schliessen lassen, enthalten.

C. Computer-Notfallteam (CSIRT)

Art. 20

Zweck und Aufgaben

1) Zur Gewährleistung der Cybersicherheit wird bei der Stabsstelle Cyber-Sicherheit ein CSIRT eingerichtet. Ihm obliegen insbesondere:

a) gegebenenfalls das zur Verfügung stellen von zur Bewältigung eines Sicherheitsvorfalls nützlichen Informationen oder Orientierungshilfen für die Durchführung möglicher Abhilfemassnahmen nach Eingang von Meldungen über Risiken oder Sicherheitsvorfälle nach Art. 6 und 9;

Meldungen über sicherheitsrelevante Ereignisse

- 2022: 29 Meldungen
- 2023: 34 Meldungen
- bis 25. Oktober 2024: 54 Meldungen

Meldekanäle

Internetseite Stabsstelle Cyber-Sicherheit unter …

- «Sicherheitsvorfall melden»
  - https://formulare.llv.li/formserver_SCS/start.do?generalid=SCS_MFC
- «CSIRT Kontakt»
  - Links zum Kontakt- oder Meldeformular
  - verschlüsselte / vertrauliche Kommunikation (PGP, S/MIME, Post)

Zusammenarbeit mit anderen Behörden

- An DSS: keine Weitergabe
- An LP: keine Weitergabe
- An andere Stellen oder Behörden: keine Weitergabe

Zusammenarbeit nur mit Einverständnis der betroffene Firma oder Privatperson

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Melde-/Berichtspflichten

DSS

Meldepflicht nach Art. 33 und 34 DSGVO

1. **Hat eine Datenschutzverletzung stattgefunden?**

   Wenn ja: genaue Abklärung der Verletzung (z.B. welche Daten sind betroffen? Wie viele Betroffene gibt es?).

   -> Ausgangspunkt ist eine Verletzung des Schutzes personenbezogener Daten. Siehe Art. 4 Abs. 12 DSGVO

Meldepflicht nach Art. 33 und 34 DSGVO

2. Besteht voraussichtlich *ein Risiko* für die Rechte und Freiheiten natürlicher Personen?

- Wenn ja: Meldung der Verletzung innerhalb von 72 Stunden an die zuständige Datenschutzaufsichtsbehörde. **Vorläufige Meldung möglich!**
- Wenn nein: Interne Dokumentation der Verletzung und Begründung, warum voraussichtlich kein Risiko für die Betroffenen besteht.
- Wenn zweifelhaft: Kontaktaufnahme mit der Datenschutzstelle.

Meldepflicht nach Art. 33 und 34 DSGVO

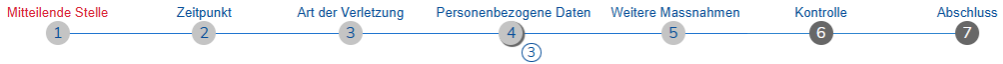
3. Besteht voraussichtlich *ein hohes Risiko* für die Rechte und Freiheiten natürlicher Personen?

- Wenn ja: Unverzügliche Benachrichtigung der betroffenen Personen.
- Wenn nein: Interne Dokumentation der Verletzung und Begründung, warum voraussichtlich kein hohes Risiko für die Betroffenen besteht.
- Wenn zweifelhaft: Kontaktaufnahme mit der Datenschutzstelle.

Wie kann die Meldung erfolgen?

- Meldung einer Datenschutzverletzung (Online-Formular / PDF-Datei)
- Notification of a personal data breach to the Data Protection Authority (EN) (Online-Formular)

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzstelle (Art. 33 DSGVO)



Zusammenarbeit mit anderen Behörden

Etablierter Prozess mit SCS

- Eingelangte Meldungen gem. Art. 33 werden von der DSS auf Relevanz für SCS geprüft;
- Falls definierte Kriterien laut Prozess erfüllt sind, erfolgt eine anonymisierte Meldung an SCS;
- Bei Bedarf werden nach Rücksprache mit dem Verantwortlichen (der meldenden Stelle), detailliertere Informationen an SCS übermittelt.

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Information und Anzeige

LP

Kontakt zu Landespolizei

- Information → Zeitnah zur Sicherung digitaler Spuren
- Anzeige → persönlich am Schalter

Information und Anzeige sind freiwillig - wird jedoch empfohlen!

Empfehlung der Landespolizei

- Kein Lösegeld bezahlen
- Keine Unterstützung krimineller Organisationen
- Keine Garantie, dass Daten tatsächlich freigegeben werden
- Hohe Wahrscheinlichkeit eines erneuten Angriffs

Was macht die Landespolizei?

- Digitale Spuren suchen, sichern und analysieren
- Ermittlungsansätze suchen (E-Mail-Adressen, IP-Adressen, Domain, Telefonnr. usw.)

- Anfragen bei Providern oder Kryptobörsen

- Grösste Herausforderungen: Täter meist im Ausland und technisch sehr versiert

Nationale und Internationale Zusammenarbeit

NEDIK
Kantonspolizeien Schweiz

DK

Verschiedene Behörden, u.a.:
Amt für Informatik
Amt für Kommunikation
Datenschutzstelle
Stabstelle Cyber-Sicherheit
Stabstelle Financial Intelligence
Stabstelle Finanzplatzinnovation
Fachgruppe Medienkompetenz

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

SWITCH

EUROPOL
EC3 | European Cybercrime Centre

INTERPOL

FBI-Verbindungs-
büro Bern

FMA
Finanzmarktaufsicht
Liechtenstein

Zusammenarbeit mit anderen Behörden

- An DSS: keine Weitergabe
- An SCS: anonymisierte Weitergabe

- Vertiefte Zusammenarbeit nur mit Einverständnis der betroffene Firma oder Privatperson

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Fazit

- Cyber-Sicherheit: **Prävention** ist ein entscheidender Faktor;

- Treten Sie bei **Cyber-Sicherheitsvorfällen** mit der **Landespolizei in Kontakt** und erstatten Sie Anzeige;

- Nutzen Sie bei Bedarf, hinsichtlich der Meldepflicht nach Art. 33 DSGVO, die Möglichkeit der Einreichung einer **vorläufigen Meldung**.

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Kontaktdaten

Kontaktdaten

Stabsstelle Cyber-Sicherheit

Zollstrasse 45
9490 Vaduz
Liechtenstein

T +423 236 63 11
info.scs@llv.li / team@csirt.li
https://scs.llv.li / https://csirt.li

Datenschutzstelle

Kirchstrasse 8
9490 Vaduz
Liechtenstein

T +423 236 60 90
info.dss@llv.li
www.datenschutzstelle.li

Landespolizei

Gewerbeweg 4
9490 Vaduz
Liechtenstein

T +423 236 71 11
info@landespolizei.li
www.landespolizei.li

LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN

Literaturhinweise

Literaturhinweise (1/3)

- **Meldeformular (Art. 33 DSGVO)**: https://www.datenschutzstelle.li/services-und-downloads/formulare#MeldungDatenschutzVerletzung

- **Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten** https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf

Literaturhinweise (2/3)

- **Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäss der DSGVO**
  https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_de_0.pdf

Literaturhinweise (3/3)

- **Cybercrime-Police: Ein Engagement der Kantonspolizei Zürich**
  https://www.cybercrimepolice.ch

- **Schweizerische Kriminalprävention:**
  https://www.skppsc.ch