Internet-Kriminalität

Praxisfälle und Prävention

Lukas Fässler
Rechtsanwalt & Informatikexperte
Zugerstrasse 76B
CH-6340 Baar
www.fsdz.ch
faessler©fsdz.ch

Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | E-Mail sekretariat@fsdz.ch

Impressum Datenschutzbestimmungen

Hinweis schliessen

Umsetzung der DSGVO

Als Anwaltskanzlei mit Schwerpunkt vor allem im Datenschutzrecht ist uns ein verantwortungsbewusster Umgang mit Ihren personenbezogenen Daten wichtig. FSDZ Rechtsanwälte & Notariat AG verzichtet vollständig auf den Einsatz von Social Media-Plugins, Websiteanalyse-Diensten und Anzeigen sowie Marketing-Diensten (keine Cookies, keine Google Analytics etc.). Sie können ohne Angabe von personenbezogenen Daten unsere Webseite besuchen.

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

Jetzt unkompliziert Video-Konferenz vereinbaren

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
sekretariat@fsdz.ch
Karte Google Maps

Rechtsanwalt
lic. iur. Lukas Fässler
Telefon +41 41 727 60 80
faessler@fsdz.ch

Rechtsanwältin & Notarin
lic. iur. Carmen de la Cruz
Telefon +41 41 727 60 80
sekretariat@fsdz.ch

Aktuell bei FSDZ

CAS Cybersecurity & Information Risk

Lukas Fässler

Rechtsanwalt und Informatikexperte, Certified Software Asset Manager IAITAM Inc.

faessler@fsdz.ch
+41 41 727 60 80
+41 79 209 24 32

Profil

1975 – 1980
Studium an der Universität Fribourg/CH

1982
Anwaltspatent des Kantons Luzern

1982 – 1984
Gerichtsschreiber am Amtsgericht Hochdorf

1984 - 1987
Gerichtsschreiber am Verwaltungsgericht Luzern

1987 - 1992
EDV-Beauftragter im Gerichtswesen Kanton Luzern

1992 - 1997
Informatikchef des Kantons Luzern

1997
Selbständiger Spezialanwalt seit September 1997

1999 - 2000
Universität Zürich, Nachdiplomstudium, Internationales Wirtschaftsrecht (Spezialisierungskurs Immaterialgüterrecht, Technologie- und Informationsrecht)

2017
"Certified Software Asset Manager IAITAM Inc." bei der International Association of Information Techology Asset Managers Inc. in Amerika

Verwaltungsratsmandate

- Verwaltungsratspräsident AR Informatik AG (IT-Service-Dienstleisterin für Kanton und Gemeinden AR)
- Verwaltungsratsvizepräsident Informatik-LeistungsZentrum OW/NW (IT-Service-Dienstleisterin für Kantone OW und NW sowie alle Gemeinden dieser Kantone)
- Verwaltungsrat der Health Info netz AG (HIN Security Services im Gesundheitswesen)

- Verwaltungsratspräsident FSDZ Rechtsanwälte & Notariat AG, Baar
- Verwaltungsratspräsident e-comtrust international AG, Baar

- Präsident Verein Schweizerische Städte- und Gemeinde-Informatik SSGI (2005-2025)
- Verwaltungsrat der Eisenbahnbetriebslabor Schweiz AG (2022 – 2025)

Dozententätigkeiten

- **Universität Basel:**
  - Master of Marketing Management, eCommerce-Recht EU und CH

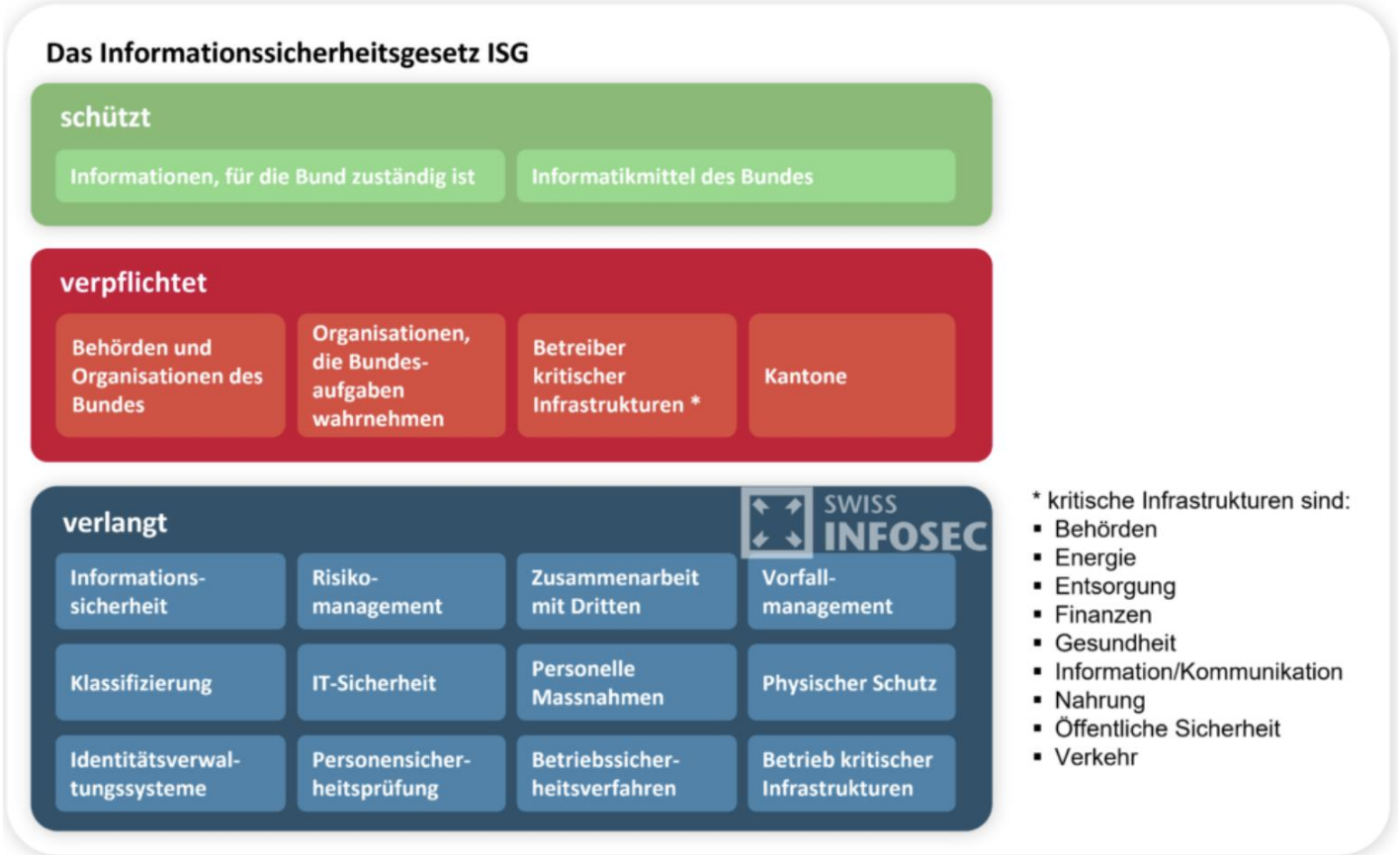
- Universität Bern/Lausanne:
  - Master of Advanced Studies for Archival an Information Management

- **Fachhochschule Nordwestschweiz in Basel:**
  - CAS eCommerce und Online-Marketing
  - CAS Information Security & Risk Management
  - CAS IT Service Management & IT Controlling
  - CAS Operational Risk Management
  - Seminar IT Leadership
  - Praxis-Seminar DSGVO und CH E-DSG
  - Seminar öffentliches Beschaffungsrecht

- **Fachhochschule Nordwestschweiz in Olten:**
  - CAS Data und Information Management

Gesetze

- Neues unternehmerisches Risiko
- Informationssicherheit (neue Gesetzesgrundlage ISG; neue Meldepflichten per 1.5.2025)
- Datensicherheit (verschärfte Gesetzesgrundlage DSG per 1.9.2023)



Praxisfälle: Cyberangriffe

Cyberangriff auf Comparis

Comparis-Hacker hatten Zugang zu Nutzerdaten

Aktualisiert um 08:28 Uhr

https://www.srf.ch/news/wirtschaft/cyberangriff-auf-comparis-comparis-hacker-hatten-zugang-zu-nutzerdaten

Cyberkriminalität

Emil Frey-Gruppe wurde Opfer von Cyberangriff

Mittwoch, 12.01.2022, 01:44 Uhr

https://www.srf.ch/news/schweiz/cyberkriminalitaet-emil-frey-gruppe-wurde-opfer-von-cyberangriff

Hacker legen einzige Zeitungspapierfabrik der Schweiz lahm – Folgen nicht absehbar

https://www.watson.ch/digital/schweiz/744582672-hacker-legen-einzige-zeitungspapierfabrik-der-schweiz-lahm-mit-folgen

Hackerangriff auf die Rothenburger Auto AG Group

Die Auto AG Group mit Sitz in Rothenburg wurde Opfer eines Hackerangriffs. Die Täterschaft ist bisher unbekannt.

27.08.2019, 17.26 Uhr

Merken Drucken Teilen

Cyberangriff auf NZZ

Hackerangriff trifft verschiedene Systeme der NZZ und CH Media

Ziel der Attacke seien diverse Dienste der Medien-Unternehmen gewesen. Der Angriff wurde aber frühzeitig erkannt.

Freitag, 24.03.2023, 16:00 Uhr

Praxisfälle: Unfälle mit verheerenden Schäden

Cloud-Rechenzentrum der OVN in Strassburg am 10.3.2021

Praxisfälle: Cyber-Erpressungen gegen Lösegeld (Bitcoin)

Praxisfälle: Cyber-Erpressungen gegen Lösegeld (Bitcoin)

- Wie verheerend ein Cyberangriff auf Basis-Infrastrukturen sein kann, hat der Fall der Colonial Pipeline im Mai 2021 in den USA gezeigt:
  - Betreiberfirma musste Rohrleitung abschalten
  - Benzinversorgung an der Ostküste wurde knapp
  - Ransomware-Angriff mit Systemverschlüsselung und Lösegeld-Erpressung
    - Hacker dringen durch Sicherheitslücken in IT-Systeme der Unternehmung ein und verschlüsseln und kopieren wichtige Daten. Für Herausgabe des Schlüssels verlangen sie ein Lösegeld (primär in Bitcoins). Oftmals drohen die Täter auch mit der Veröffentlichung von sensiblen (Kunden- oder Geschäfts-) Daten.
  - Es wurden 4.4 Mio Dollar Lösegeld in Bitcoin bezahlt

https://www.tagesschau.de/wirtschaft/unternehmen/colonial-pipeline-loesegeld-hacker-angriff-ransomware-101.html

Praxisfälle: Cyber-Erpressungen gegen Lösegeld (Bitcoin)

CYBERATTACKE

FBI nimmt Pipeline-Hackern Lösegeld ab

Der Hackerangriff auf die größte Benzin-Pipeline hat die Verletzlichkeit der US-Infrastruktur offengelegt. Immerhin wurde den Erpressern nun ein Teil ihrer Beute abgejagt.

Der stellvertretende FBI-Direktor Paul Abbate erläuterte das Verfahren: Das in der Digitalwährung Bitcoin gezahlte Lösegeld sei bei der Überprüfung zahlloser anonymer Transaktionen in einer digitalen Geldbörse (Wallet) aufgespürt worden. 75 Bitcoin - nach damaligem Wert 4,4 Millionen Dollar - hatte das Versorgungsunternehmen Colonial Pipeline den Hackern bezahlt. 63,7 Bitcoin davon konnte das FBI beschlagnahmen - wegen des Absturzes der digitalen Währung in den vergangenen Wochen mit einem heutigen Wert von 2,3 Millionen Dollar. Es ist das erste Mal, dass eine eigens zum Einsatz gegen Ransomware und digitale Erpressung gegründete Einheit des Ministeriums Lösegeld beschlagnahmt hat.

"Das war ein Angriff auf eine unserer wichtigsten nationalen Infrastrukturen", sagte Lisa Monaco. Hinter der Tat vermutet die US-Regierung Hacker der Gruppe DarkSide aus Russland.

https://www.srf.ch/news/schweiz/cyberkrimina
hackerangriff-auf-die-gemeinde-montreux

Quelle:
https://www.srf.ch/news/schweiz/cyberkriminalitaet-hackerangriff-auf-die-gemeinde-montreux

News > Schweiz >

Cyberkriminalität

Hackerangriff auf die Gemeinde Montreux

Montag, 11.10.2021, 08:17 Uhr
Aktualisiert um 11:33 Uhr

Tausende persönliche Daten im Darknet: Die Cyberattacke auf Rolle ist gravierender als von den Behörden kommuniziert

Seit dem Angriff auf die Waadtländer Gemeinde sind sensitive Informationen über Bürger, Mitarbeiter und Unternehmen frei zugänglich. Die Hacker wollten Lösegeld. Der Bund ist eingeschaltet.

Gemeinde	Ort (Kanton)	Jahr	Vorfalltyp
Bad Zurzach	AG	März 2021	Ransomware, Betriebsstillstand
Rolle	VD	Sommer 2021	Ransomware, Datenexfiltration
Niederwil	AG	Mai 2023	Account-Hack (MOVEit-Lücke)
Rüegsau	BE	Mai 2023	EDV-Unterbruch via Dienstleister
Zollikofen	BE	Nov. 2023	Ransomware-Angriff
Saxon	VS	(2023?)	Ransomware bei Vormundschaftsbehörde

Praxisfälle: Cyber-Erpressungen gegen Lösegeld (Bitcoin)

Hackerangriff legt Login von Schweizer Medienportalen lahm

Nach einem Cyberangriff ist die von etlichen Schweizer Medien genutzte Login-Plattform Onelog nicht verfügbar.

Schweizer Medien-Login nach Cyber-angriff weiter offline

Die Plattform Onelog bleibt ausser Betrieb. Das volle Ausmass des Angriffs ist noch nicht bekannt.

Schweizer Medienplattform Onelog

Cyberangriff auf Stiftsbezirk St. Gallen: Es war Ransomware

Von Philipp Anz, 29. Oktober 2024, 14:59

SECURITY CYBERANGRIFF RANSOMWARE VERWALTUNG KANTON ST. GALLEN

Foto: Bistum St. Gallen

Über den Angriff auf katholische Institutionen in St. Gallen werden neue Details bekannt. Systeme wurden verschlüsselt, eine Lösegeldforderung ist eingegangen.

Am vergangenen Wochenende wurden die kirchlichen Institutionen im Kanton St. Gallen Opfer eines Cyberangriffs. Betroffen sind zahlreiche Einrichtungen des Stiftsbezirks wie unter anderem das Bischöfliches Ordinariat, die Katholische Administration, die Stiftsbibliothek, das Seminar St. Wiborada und die Pensionskasse der Diözese St. Gallen.

Stiftsbezirk St.Gallen

Ausweitung der Untersuchungstätigkeit auf die Xplain AG

Bern, 14.07.2023 - Der EDÖB weitet seine Untersuchungstätigkeit auf die Xplain AG aus.

Gemäss seiner Pressemitteilung vom 21. Juni 2023 hat der EDÖB am 20. Juni 2023 eine formelle Untersuchung gegen die Bundesämter für Polizei sowie Zoll- und Grenzsicherheit unter anderem wegen der im Zusammenhang mit der Xplain AG angezeigten Verletzung der Datensicherheit eröffnet. Inzwischen hat der EDÖB von weiteren Informationen zu diesem Vorfall Kenntnis genommen, die ihn dazu bewogen haben, seine Untersuchungstätigkeit am 13. Juli 2023 auf die Firma Xplain auszudehnen.

Kanton Waadt kündigt Xplain-Vertrag

Von Reto Vogt, 8. Februar 2024, 17:24

POLITIK & WIRTSCHAFT BESCHAFFUNG KANTON WAADT XPLAIN

Foto: zVg

Xplain wurde von der Waadtländer Polizei mit der Modernisierung des IT-Systems beauftragt. Daraus wird nichts mehr. Xplain will prüfen, ob die Kündigung rechtens ist.

Am 7. Februar beschloss der Waadtländer Staatsrat, den Vertrag mit Xplain mit sofortiger Wirkung zu kündigen, um die "finanziellen und betrieblichen Risiken einzugrenzen", wie der Kanton in einer Mitteilung schreibt.

Durch den Cyberangriff auf Xplain wurde die Durchführung von Odyssée "erheblich gestört", was zu Verzögerungen geführt habe, wie es in der Mitteilung des Kantons weiter heisst. Bekannt ist das schon seit Herbst 2023, schon damals äusserten Mitglieder des Kantonsparlaments Bedenken.

Der Lieferant habe ausserdem "Probleme mit der Produktqualität", was zu "ernsthaften Zweifeln an seiner Fähigkeit führte, die ursprünglich vereinbarten Leistungen zu erbringen", schreibt der Kanton in ungewohnter Schärfe. Der Kanton arbeitet mit dem aktuellen System weiter, bis ein neuer Lieferant feststeht. Es bleibe aber eine Modernisierung erforderlich.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Schlussbericht und Empfehlungen

vom 25. April 2024

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

in Sachen Xplain AG

aufgrund Ransomware-Vorfall

gemäss

Artikel 29 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (aDSG) in Verbindung mit Artikel 70 Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG)

https://www.newsd.admin.ch/newsd/message/attachments/87361.pdf

Hackerangriff auf die Firma Concevis: Auch die Bundesverwaltung ist betroffen

Bern, 14.11.2023 - Das Software-Unternehmen Concevis wurde Opfer eines Ransomware-Angriffes, bei dem sämtliche Server der Firma verschlüsselt wurden. Unter den entwendeten Daten befinden sich nach aktuellem Kenntnisstand mutmasslich auch ältere, operative Daten der Bundesverwaltung. Die vertieften Analysen laufen derzeit noch.

Die Firma Concevis, eine Schweizer Anbieterin von Softwarelösungen für öffentliche Verwaltungen (Bund, Kantone, Städte), den Finanzsektor und Unternehmen aus der Industrie und Logistik, ist Opfer eines Ransomware-Angriffs geworden. Die Angreifer entwendeten Daten und verschlüsselten danach sämtliche Server der Firma. Nachdem die Firma der Lösegeldforderung nicht nachgekommen ist, drohen die Angreifer mit der Veröffentlichung der Daten im Darknet.

Cyberangriff auf die Stiftung Radix: Auch Daten der Bundesverwaltung sind betroffen

30.06.2025- Die Stiftung Radix wurde Opfer eines Ransomware-Angriffs. Beim Angriff sind Daten abgeflossen und wurden verschlüsselt. Zu den Kunden der Stiftung Radix gehören auch verschiedene Bundesstellen. Die Daten wurden im Darknet publiziert und werden nun von den betroffenen Stellen analysiert.

CYBERATTACKEN

Vor Bürgenstock-Konferenz: Zahl der russischen Hackerangriffe auf Schweizer Computer nimmt massiv zu

Seit der Ankündigung der Ukraine-Friedenskonferenz auf dem Bürgenstock ist die Zahl russischer Cyberangriffe rasant angestiegen.

09.06.2024 08:13

Identitätsmissbrauch mit künstlicher Intelligenz

Schweizerisches Strafgesetzbuch 311.0

Art. 179decies 242 Seit 1.9.2023 in Kraft

Identitätsmiss-brauch

Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird auf Antrag mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.

Künstliche Intelligenz: SVP-Glarner fälscht Arslan-Aussage 18.10.2023

- Der in der Strafbestimmung statuierte Nachteil für den durch den Identitätsmissbrauch Betroffenen muss eine gewisse Schwere erreichen und kann materieller oder immaterieller Natur sein.

- Die Absicht, beim Betroffenen einen massiven Ärger auszulösen, kann als Nachteilsabsicht bereits ausreichen.

Wegen Fake-Video

Staatsanwaltschaft darf gegen SVP-Nationalrat Glarner ermitteln

Freitag, 27.06.2025, 14:05 Uhr
Aktualisiert um 15:48 Uhr

- Gegen den Aargauer SVP-Nationalrat Andreas Glarner darf strafrechtlich ermittelt werden.
- Es geht um den Fall eines mit künstlicher Intelligenz generierten Videos.
- Die zuständige Parlamentskommission hat die Immunität von Glarner definitiv aufgehoben.

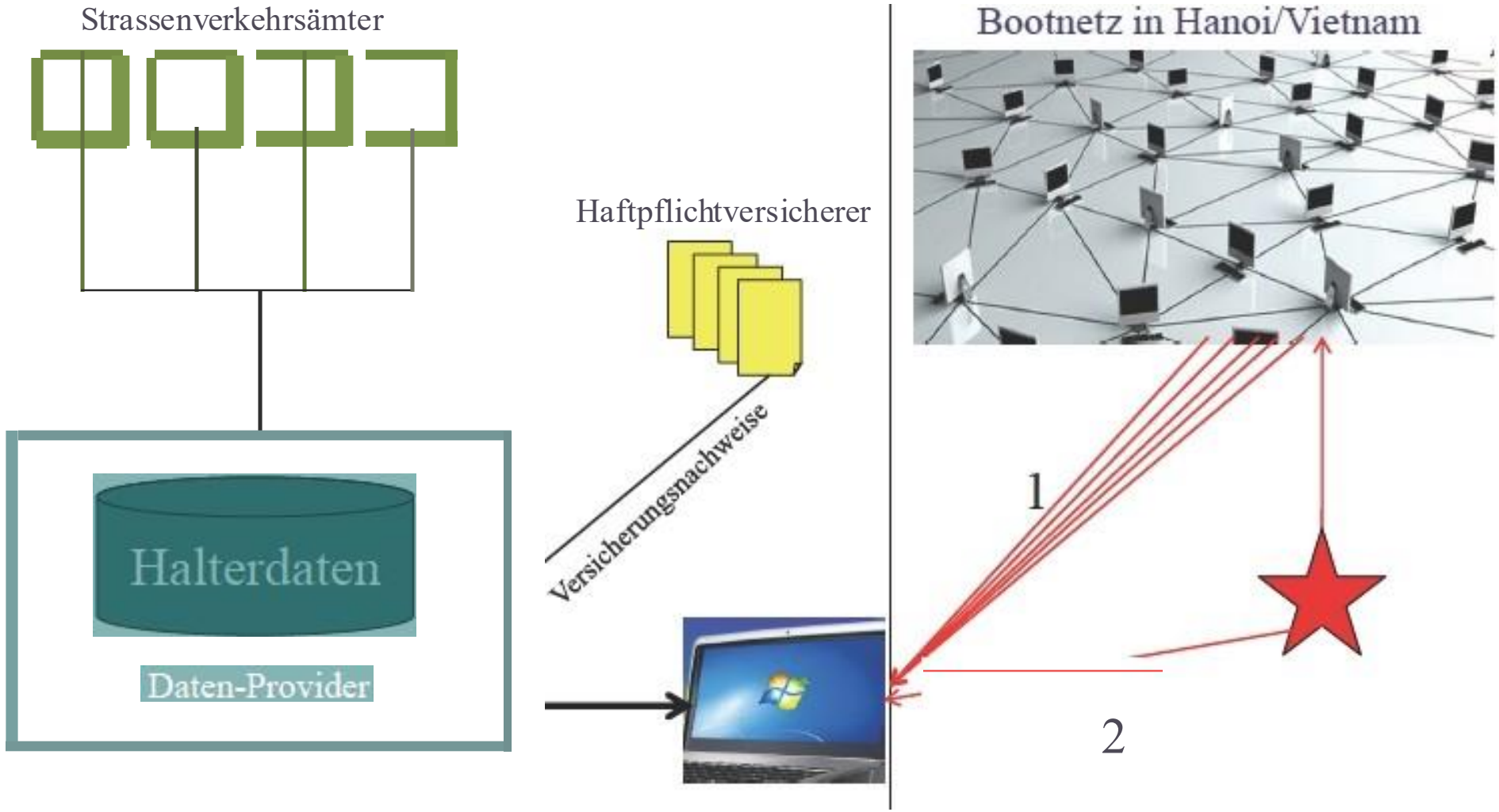
Mit 8 zu 2 Stimmen schliesst sich die Rechtskommission des Ständerats (RK-S) dem Entscheid der Immunitätskommission des Nationalrats (IK-N) an, wie Kommissionspräsident Daniel Jositsch (SP/ZH) in Bern vor Medien mitteilt.

Cyberangriff auf Strassenverkehrsämter und Halterdaten

Diebstahl Halterdaten

[redacted] gibt Autonummern einen Namen: Wer einen Autohalter personalisieren möchte, dem bietet sich ab sofort für CHF 0.80 pro Anfrage eine neue Möglichkeit. [redacted] ist eine vollautomatische Plattform, welche die rasche Abfrage der Fahrzeughalterdaten per SMS ermöglicht: Autokennzeichen eintippen, SMS an [redacted] senden und innerhalb weniger Sekunden erscheint die Antwort auf dem Display. Einfacher und schneller geht es nicht. Vorerst bietet [redacted] den Dienst für die folgenden acht Kantone an: BL, LU, NE, NW, OW, TI, VS und ZG. Weitere sollen bald folgen.

Cyberangriff auf Strassenverkehrsämter und Halterdaten



Cyberangriff auf Strassenverkehrsämter und Halterdaten

InfoGuard
SWISS CYBER SECURITY

InfoGuard
SWISS CYBER SECURITY

2 INVESTIGATIVE FINDINGS

2.1 Intrusion Timeline

InfoGuard established the following timeline in Table 1. based on investigative results. InfoGuard lists all timestamps in Universal Coordinated Time (UTC)

DATE	EVENT
2020-04-14	Execution of CopyData.exe and Upload.cmd on TS99
2020-04-23	Execution of UploadBackup.exe and Upload.cmd in a TeamViewer session on TS97
2020-04-30	Execution of UploadBackup.exe on TS99
2020-06-12	Execution of UploadBackup.exe in a TeamViewer session on TS97
2020-06-30	Execution of UploadBackup.exe, Notepad.exe and cmd.exe in a TeamViewer session on TS97
2020-07-01	The Attacker had a TeamViewer Session on TS97
2020-07-02	Two TeamViewer sessions, in the second was UploadBackup.exe and Notepad.exe executed on TS97
2020-08-12	Execution of UploadBackup.exe in a TeamViewer session on TS82

KANTON LUZERN
Amtsgericht Luzern-Land

Abteilung II
Präsident Trüeb, Amtsrichterin Unternährer, Meier und Ersatzrichter Dätwyler,
Gerichtsschreiberin Wigger

Urteil vom 6. Dezember 2010

Rechtsspruch

1. M.W. ist schuldig der mehrfachen unbefugten Datenbeschaffung nach Art. 143 Abs. 1 StGB, begangen in mittelbarer Täterschaft vom 20.5.2008 bis 31.7.2008.

2. M.W. wird in Anwendung von Art. 34, Art. 42 Abs. 1, Art. 44 Abs. 1, Art. 47, Art. 49 Abs. 1 und Art. 51 StGB mlt einer Geldstrafe von Fr. 8'800.00, 80 Tagessätzen zu je Fr. 110.00 bestraft unter Anrechnung von zwei Tagessätzen erstanden aus der zweitägigen Untersuchungshaft vom 19.11.2008 bis 20.11.2008. Die Geldstrafe wird bedingt ausgesprochen bei einer Probezeit von 2 Jahren.

3. Zusätzlich wird in Anwendung von Art. 42 Abs. 4 und Art 106 StGB eine Busse von Fr. 1'750.00 ausgesprochen. Die Ersatzfreiheitsstrafe beträgt 16 Tage.

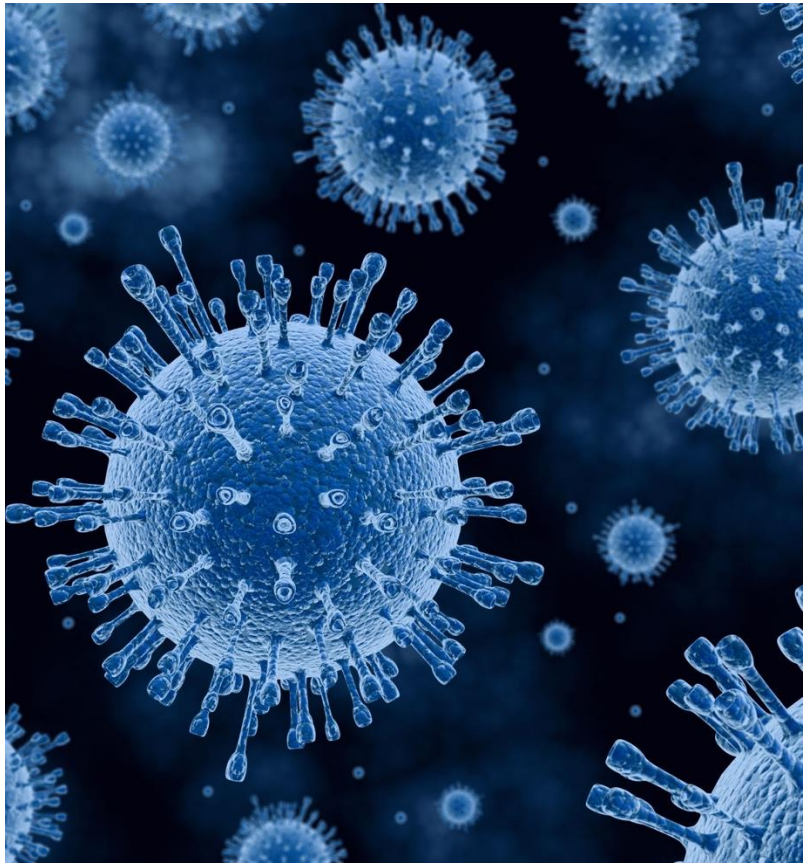
Was passiert bei einem Ransomware-Angriff? | fuzo explains

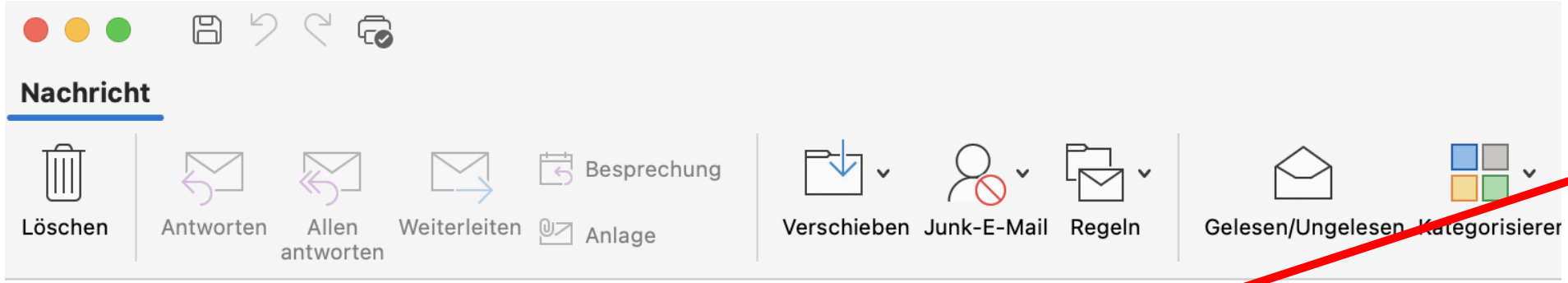
YouTube · FUTUREZONEat · 09.12.2021

YouTube

Ablauf eines Ransomware-Angriffs

- Angreifer infiltrieren Netzwerke durch Phishing-E-Mails oder Analyse-Tools zu offenen Ports.
- Ransomware wird heruntergeladen und installiert sich heimlich.
- Dateien werden verschlüsselt, um Zugriff zu verwehren.
- Opfer erhalten Lösegeldforderungen zur Entschlüsselung.
- Daten können für immer verloren sein, wenn kein Lösegeld gezahlt wird oder sie werden im Darknet mit medialem Aufwand publiziert.





Final Reminder: Corporate INTL - 2025 Annual Who's Who Handbook

Jessica Eddy <jessicaeddy@corp-intl.com>

An: Lukas Fässler

Diese Nachricht scheint eine Junk-E-Mail zu sein. Links und andere Funktionen können nicht verwendet werden.

Dear Lukas Fässler,

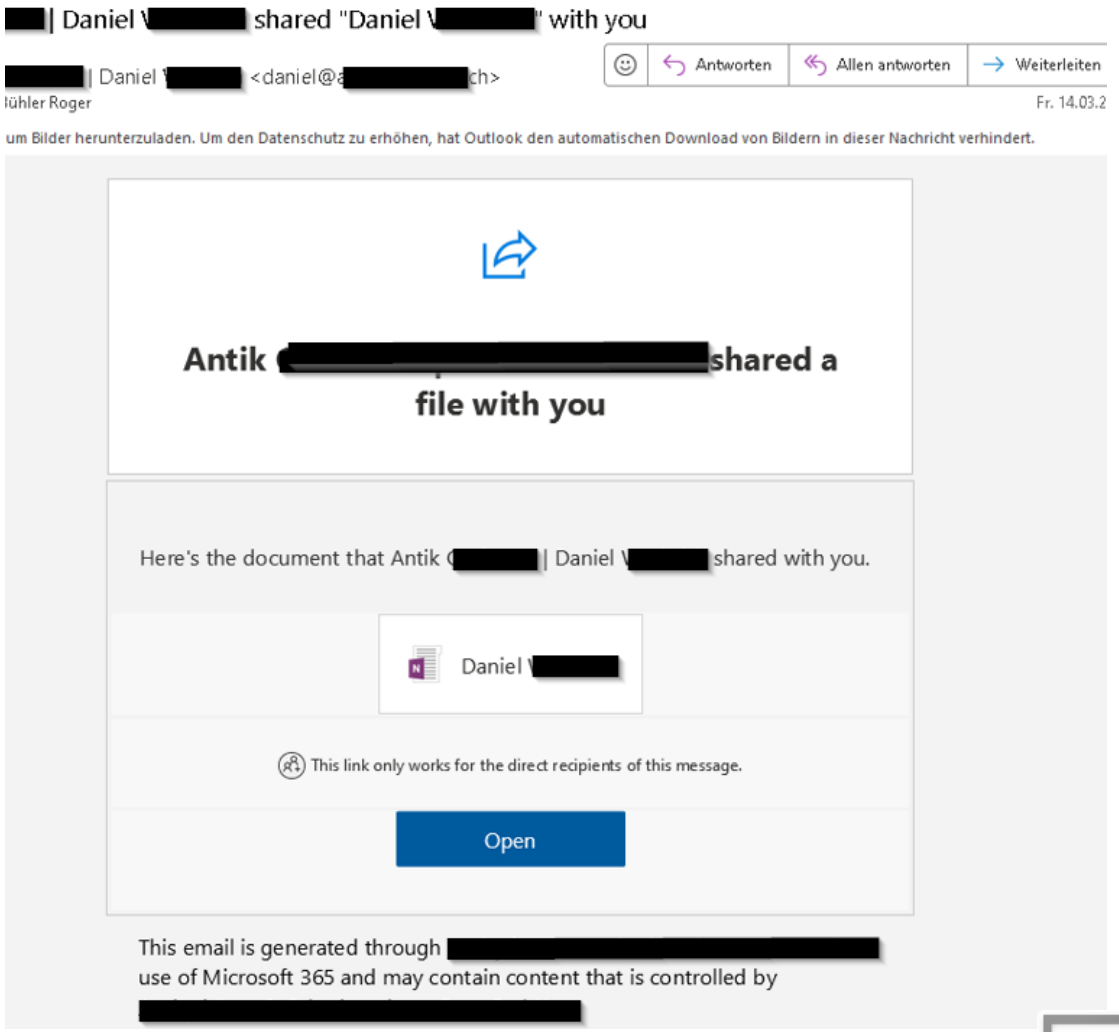
I sent the below email to you on 29th April regarding the 2025 Corporate INTL 'Who's Who - Find an Adviser Handbook'.

I have been asked to send you a **final reminder** as our research panel have recommended that we feature you within the 2

As with our previous annual Handbook publications since 2006, the 2025 'Who's Who - Find an Adviser Handbook' will be p
and Handbook section of the Corporate INTL website www.corp-intl.com with a total circulation of over 187,000 individuals

AiTM-Attacken in der Zentralschweiz (Adversary-in-the-Middle)

Ein **"Adversary-in-the-Middle" (AitM)** ist ein Angreifer, der sich heimlich zwischen zwei kommunizierende Parteien positioniert, um deren Kommunikation **abzuhören, zu manipulieren oder umzuleiten**, ohne dass diese es merken.



AiTM-Attacken auf KMU in der Zentralschweiz

- Insbesondere KMU betroffen
- Einzelne Accounts von Kunden eines Unternehmens werden gefisht
- Recht zuverlässige Erkennung durch MS Defender möglich

AiTM-Attacken in der Zentralschweiz (Adversary-in-the-Middle)

- **Geschenkkarten** Betrug
- Klar ersichtliche, falsche Absender
- Existierende, **echte** Mailboxen
- 2 bekannte erfolgreiche Fälle (1x Kanton NW, 1x Kanton OW)

Von: A. R.-S. <a.r.ch1@outlook.com>
Gesendet: Thursday, May 1, 2025 8:57:47 AM
An: [redacted]@ow.ch
Betreff:

Guten Morgen [redacted],

Hast du eine Minute Zeit? Du must ine Aufgabe für mich erledigen. Ich kann nicht telefonieren, ich habe heute mehrere Meetings, also schreib einfach hier zurück.

Mit freundlichen Grüßen
A. R.-S.

Von: A. R.-S. <a.r.ch1@outlook.com>
Gesendet: Thursday, May 1, 2025 8:57:47 AM
An: [redacted]@ow.ch
Betreff:

.....kaufe mir rasch 50 Gutscheine (WishCards) zu CHF 20.— ……..

….. und schick mir schnell die Codes der gescannten Karten rüber ……

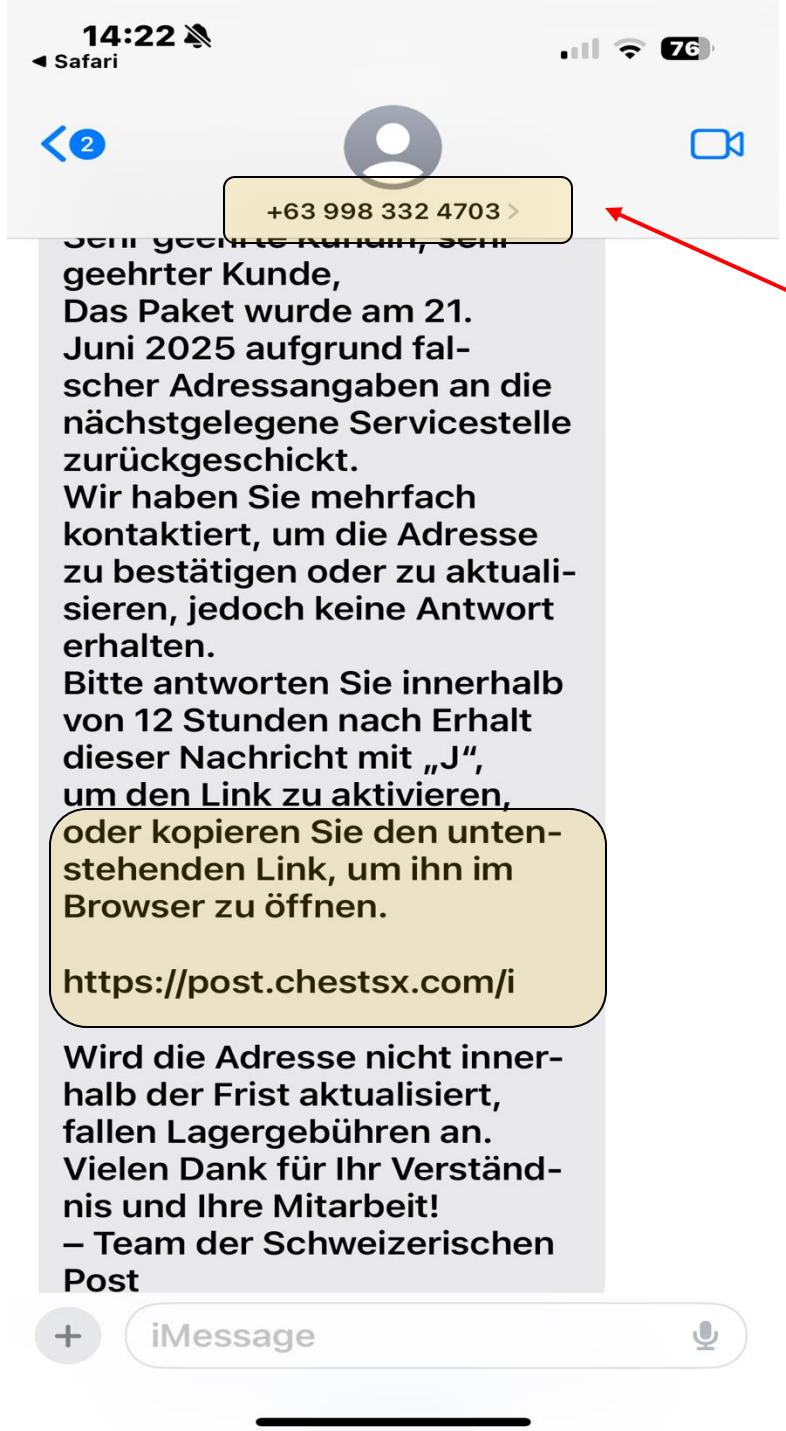
ZVG/LUZERNER POLIZEI

Zu erkennen sind falsche Codes gemäss Luzerner Polizei auch daran, dass sie oft Rechtschreibfehler haben oder der Druck minderwertig sei. Auch sind sie über die originalen Kleber geklebt.

Aus dem Archiv: QR-Code-Betrug auch auf Parkplätzen in der Deutschschweiz

01:18 min, aus **Espresso** vom 03.10.2024

srf.ch


14:22
Safari
76
2
+63 998 332 4703
geehrter Kunde,
Das Paket wurde am 21. Juni 2025 aufgrund falscher Adressangaben an die nächstgelegene Servicestelle zurückgeschickt.
Wir haben Sie mehrfach kontaktiert, um die Adresse zu bestätigen oder zu aktualisieren, jedoch keine Antwort erhalten.
Bitte antworten Sie innerhalb von 12 Stunden nach Erhalt dieser Nachricht mit „J“, um den Link zu aktivieren, oder kopieren Sie den untenstehenden Link, um ihn im Browser zu öffnen.
https://post.chestsx.com/i
Wird die Adresse nicht innerhalb der Frist aktualisiert, fallen Lagergebühren an.
Vielen Dank für Ihr Verständnis und Ihre Mitarbeit!
– Team der Schweizerischen Post
iMessage

RFID Skimming

RFID-Skimming ist **eine Form des elektronischen Datendiebstahls, bei der Kriminelle mit mobilen Lesegeräten Daten von RFID-Chips unbemerkt auslesen, um an persönliche oder finanzielle Informationen zu gelangen**.

Wie funktioniert RFID-Skimming?

RFID-Chips:

RFID (Radio-Frequency Identification) ist eine Technologie, die verwendet wird, um Objekte automatisch zu identifizieren, oft in Karten oder Ausweisen.

Lesegeräte:

Kriminelle nutzen kleine, tragbare Lesegeräte, die in der Lage sind, die Daten von RFID-Chips in der Nähe auszulösen und auszulesen.

Datendiebstahl:

Die Kriminellen nähern sich mit dem Lesegerät deinen persönlichen Gegenständen (Geldbörse, Ausweis, etc.), oft in überfüllten Bereichen, wo deine Aufmerksamkeit abgelenkt ist, und lesen unbemerkt die Daten ab.

Prävention

Gesicherte Backup-Konzepte: 3-2-1 Regel

Die 3-2-1 Regel ist eine weit verbreitete und bewährte Strategie für Backups, die darauf abzielt, Daten effektiv vor Verlust zu schützen. Sie besagt, **dass man drei Kopien seiner Daten erstellen soll, diese auf zwei verschiedenen Medien speichern und eine Kopie an einem externen Standort aufbewahren soll.**

Erläuterung der 3-2-1 Regel:

3:

Erstellung von mindestens drei Kopien der Daten. Dies umfasst das Original und zwei Backups.

2:

Speicherung der Backups auf zwei verschiedenen Medien. Dies kann beispielsweise eine lokale Festplatte und ein USB-Stick oder ein lokales NAS-Gerät und ein Cloud-Speicher sein.

1:

Speicherung einer Kopie an einem externen Standort, der geografisch vom Hauptstandort getrennt ist. Dies kann ein Cloud-Speicher oder ein Backup-Server an einem anderen Standort sein.

Lindt Museum – Vorsicht vor Fake Seiten beim Ticket-Kauf

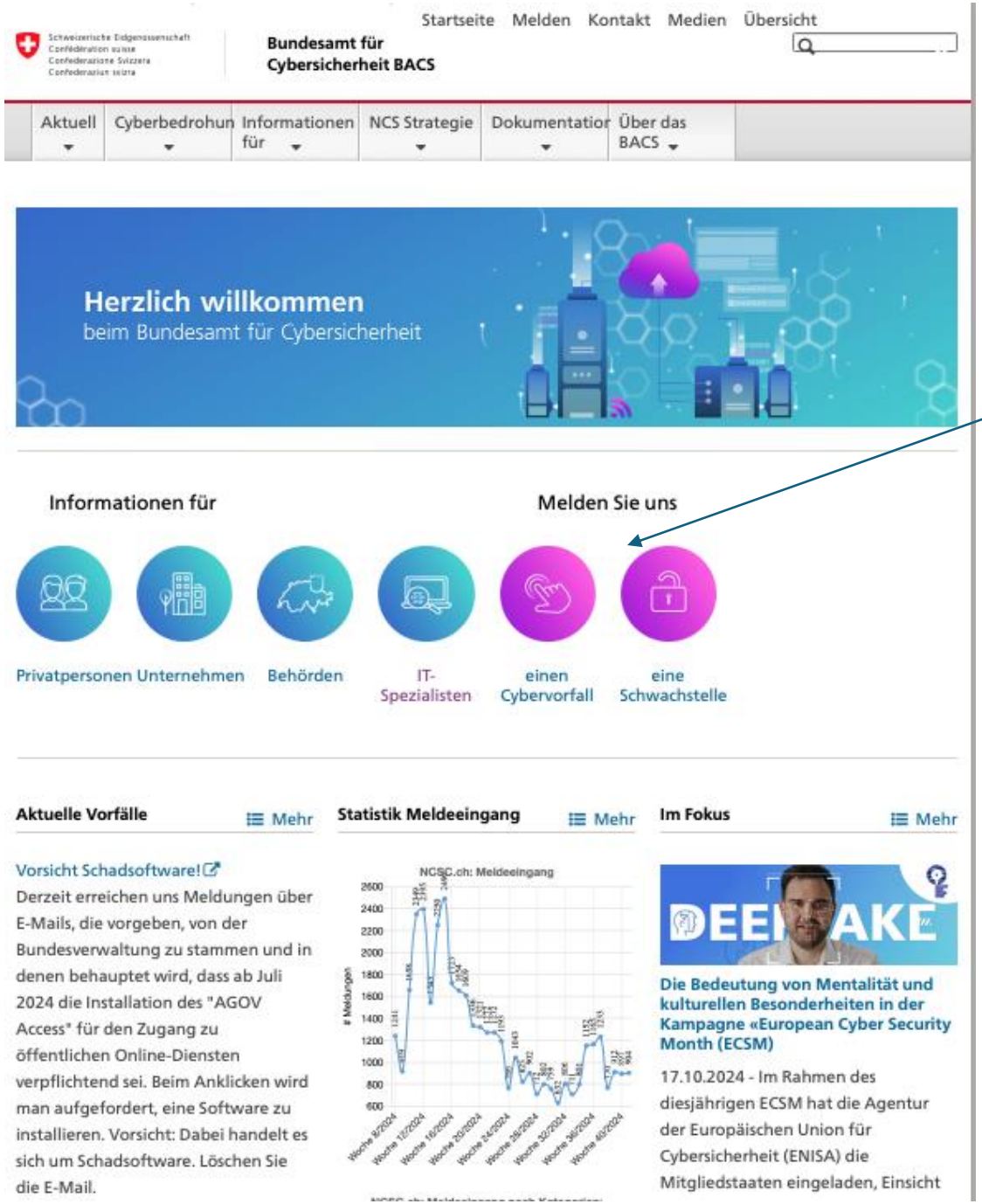
So läuft der Betrug ab

- Online-Käufe beginnen oft mit einer Google-Suche. So auch hier: Wenn Sie hier Begriffe rund um das Thema „Lindt Home of Chocolate“ eingeben, werden Ihnen ganz oben mehrere bezahlte Suchergebnisse angezeigt.
- Betrüger nutzen die Online-Werbeplattform Google Ads gezielt, um Interessierte auf ihre gefälschten Lindt-Webseiten zu lenken. Sobald Betroffene auf den betrügerischen Seiten Tickets bestellen und Ihre Kreditkartendaten eingeben, wird die Kreditkarte unrechtmässig belastet.

So schützen Sie sich

- Kaufen Sie Ihre Tickets immer nur auf der offiziellen Website: https://www.lindt-home-of-chocolate.com/de/. Geben Sie die genaue Adresse am besten direkt in Ihr Browserfenster ein.
- Wenn Sie eine Suchmaschine nutzen möchten, vermeiden Sie gesponserte Anzeigen und prüfen Sie alle Suchergebnisse genau, bevor Sie Ihre Bestellung aufgeben.


National Cyber Security Centre Switzerland NCSC
40.513 Follower:innen
4 Tage •
Betrüger missbrauchen offizielle Handelsregisterdaten
Mithilfe von gefälschten Websites, die jenen legitimer Unternehmen ähnlich sehen, versuchen Betrüger, ihre Opfer in die Falle zu locken. Wie sie sich dabei Angaben aus öffentlich einsehbaren Informationsquellen wie z.B. dem Zentralen Firmenindex (Zefix) zunutze machen, lesen Sie im aktuellen Wochenrückblick. #bacs_wochenrückblick #cybersicherheit #cyber
https://lnkd.in/ecQtV_FH


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Bundesamt für Cybersicherheit BACS
Startseite Melden Kontakt Medien Übersicht
Aktuell
Cyberbedrohun
Informationen für
NCS Strategie
Dokumentatior
Über das BACS
Herzlich willkommen
beim Bundesamt für Cybersicherheit
Informationen für
Melden Sie uns
Privatpersonen
Unternehmen
Behörden
IT-Spezialisten
einen Cybervorfall
eine Schwachstelle
Aktuelle Vorfälle
Mehr
Vorsicht Schadsoftware!
Derzeit erreichen uns Meldungen über E-Mails, die vorgeben, von der Bundesverwaltung zu stammen und in denen behauptet wird, dass ab Juli 2024 die Installation des "AGOV Access" für den Zugang zu öffentlichen Online-Diensten verpflichtend sei. Beim Anklicken wird man aufgefordert, eine Software zu installieren. Vorsicht: Dabei handelt es sich um Schadsoftware. Löschen Sie die E-Mail.
Statistik Meldeeingang
Mehr
NCSC.ch: Meldeeingang
Meldungen
Im Fokus
Mehr
Die Bedeutung von Mentalität und kulturellen Besonderheiten in der Kampagne «European Cyber Security Month (ECSM)
17.10.2024 - Im Rahmen des diesjährigen ECSM hat die Agentur der Europäischen Union für Cybersicherheit (ENISA) die Mitgliedstaaten eingeladen, Einsicht

Scan-Blocker für Kreditkarten und Bankkarten

RFID Secure-Card

MENGENRABATT

CHF 14.95 inkl. MwSt.

Ab 2 Stück CHF 13.95
Ab 3 Stück CHF 12.95
Ab 5 Stück CHF 11.95
Ab 10 Stück CHF 9.95

Sofort lieferbar | Schnellversand

1 In die Kiste

Warnungen von Geschäften

MIGROS

Schütze dich vor Cyberkiminalität

So kannst du dich schützen:

Nutze Passkeys

Melde dich mit Passkeys an, indem du einfach dein Gerät entsperrst, via Gesichtserkennung, Fingerabdruck, PIN oder Muster. Ganz ohne Passwort oder Anmelde-Codes. Passkeys sind von Grund auf sicher und resistent gegen Phishing. Um Passkeys einzurichten, gehe in die Sicherheitseinstellungen in deinem Migros Account.

Gib auf dein Passwort acht

Falls du Passkeys nicht nutzen möchtest oder kannst und weiterhin ein Passwort verwendest, sei achtsam. Wir fragen dich am Telefon oder per E-Mail nie nach deinem Passwort. Die einzige Seite, auf der du dich in deinem Migros Account anmeldest, beginnt wie folgt:

https://login.migros.ch/

Betrugsseiten weichen immer davon ab.

Im Zweifelsfall Passwort ändern & Infoline kontaktieren

Du bist auf eine Betrugs-E-Mail hereingefallen oder hast dein Passwort auf einer Betrugsseite eingegeben? Das kann jedem passieren. Schnelles Handeln ist jetzt wichtig. Ändere umgehend dein Passwort oder - falls nicht mehr möglich - kontaktiere unsere Infoline.

KI und ihre Gefahren

Im Zusammenhang mit Meta AI

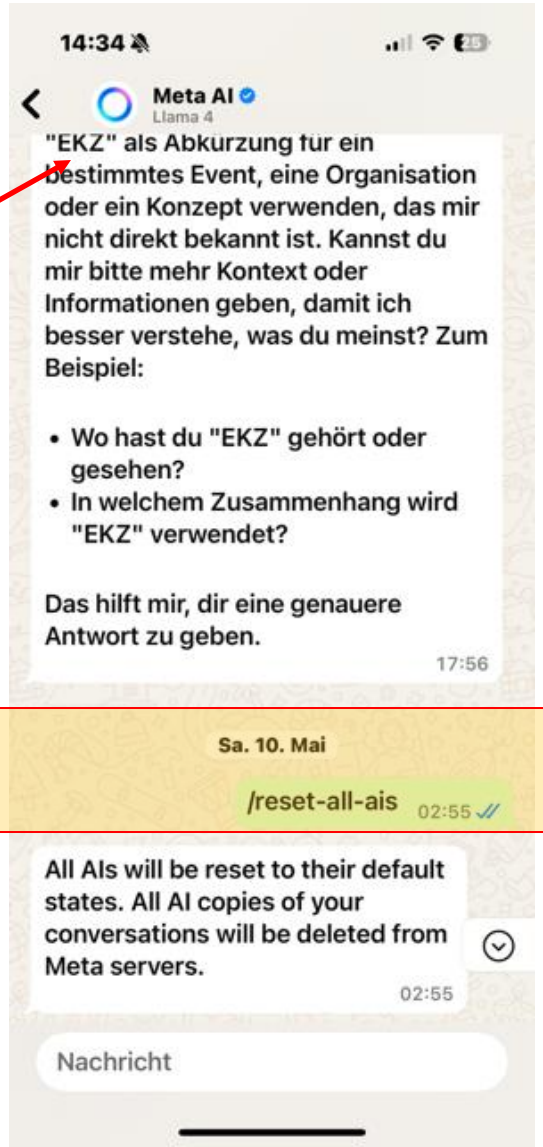
Meta plant, ab dem 27. Mai öffentliche Nutzerdaten für KI-Training zu verwenden.
Nach dem Ablauf der Frist besteht keine Möglichkeit zum Widerruf mehr.

DATENSCHUTZ

Frist abgelaufen – so fressen Instagram und Facebook Ihr digitales Leben

https://www.giessener-anzeiger.de/produktempfehlung/meta-nutzt-ihre-daten-fuer-ki-nur-tage-zeit-zum-widersprechen-zr-93745281.html

WhatsApp
integrierte KI-Funktion



Wie die «Grossen» die KI monetarisieren

Der Monetäre Aspekt und wie die «Grossen» vorgehen…

https://www.deraktionaer.de/artikel/aktien/microsoft-jetzt-wird-es-teuer-20373225.html

Microsoft: Jetzt wird es teuer

Foto: FinkAvenue/iStockphoto

Microsoft | Copilot | Office | Preissteigerung

0:00 / 0:00

17.01.2025 · Lukas Meyer

Die Monetarisierung von KI schreitet in großen Schritten voran. Microsoft integriert Copilot-KI in seine Office-Suite und hebt die Preise um bis zu 43 Prozent an. Für den Tech-Riesen ein lukrativer Schritt, der das Umsatzwachstum antreiben soll – und Anlegern attraktive Perspektiven eröffnet.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Vorschläge zu Business-Continuity-Strategien (BC-Strategien)

Hilfsmittel zum BSI-Standard 200-4

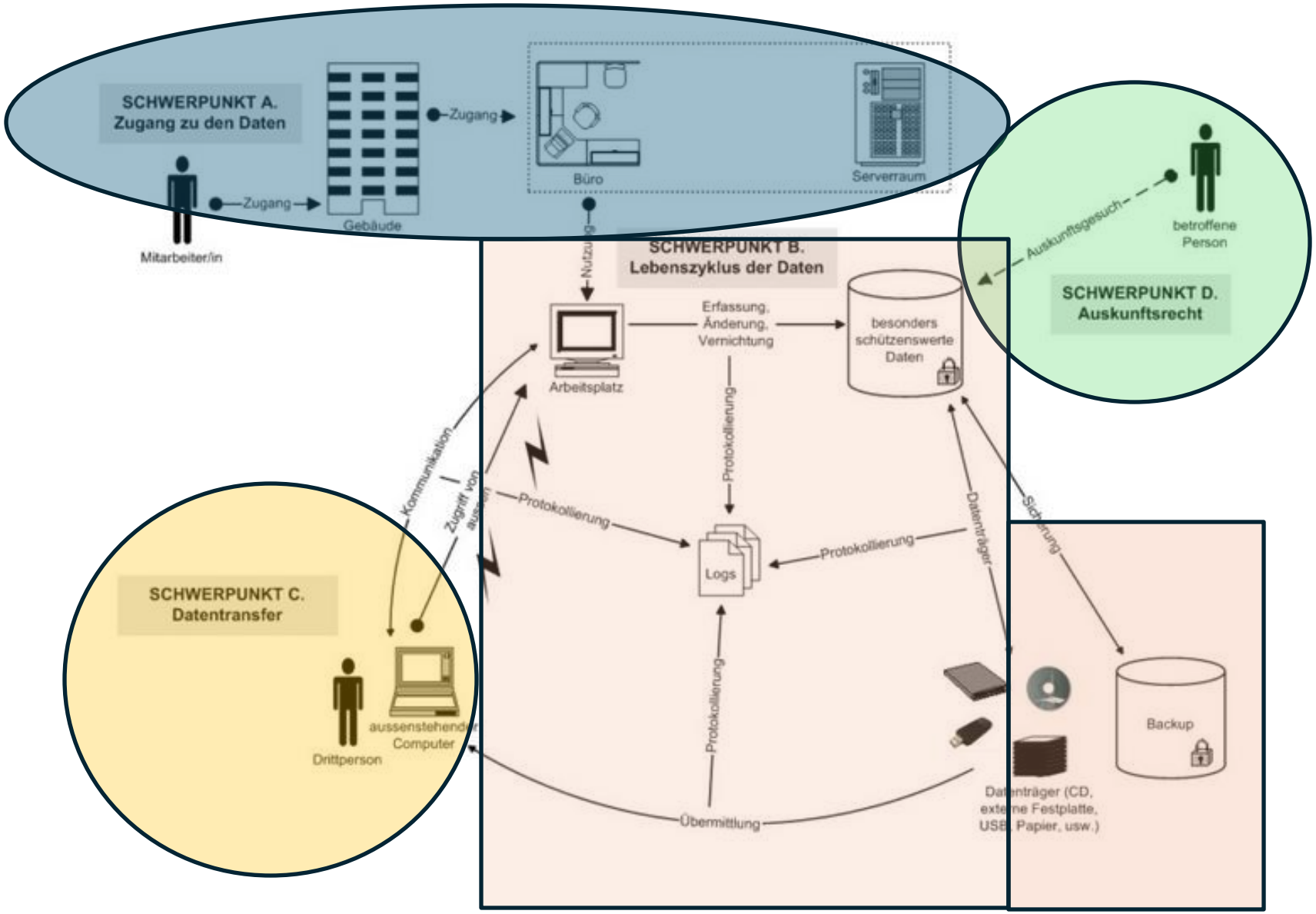
Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)

- A. Zugang zu den Daten
- B. Lebenszyklus der Daten
- C. Datentransfer
- D. Auskunftsrechte

15. Januar 2024

INHALTSVERZEICHNIS

1 Einleitung ... 4
1.1 Datenschutzgesetz ... 4
1.2 Begriffe ... 5
1.3 Allgemeine Grundsätze ... 6
1.4 Funktionen ... 7
1.5 Technische und organisatorische Massnahmen ... 7
1.6 Hilfsmittel ... 7
2 Datenbearbeitung ... 9
2.1 Datenschutz-Folgenabschätzung ... 9
2.1.1 Pflicht zur Erstellung einer DSFA ... 10
2.1.2 Ausnahmen von der Pflicht zur Erstellung einer DSFA ... 10
2.1.3 Datenschutzberaterin oder Datenschutzberater ... 10
2.1.4 Bestandteile einer DSFA ... 11
2.2 Verzeichnis ... 11
2.3 Meldung von Verletzungen ... 12
2.4 Verantwortliche im Ausland ... 13
3 Rechte und Pflichten ... 15
3.1 Informationspflicht ... 15
3.2 Rechte der betroffenen Personen ... 16
3.2.1 Auskunftsrecht ... 17
3.2.2 Recht auf Datenherausgabe oder -übertragung ... 18
3.2.3 Recht auf Vernichtung der Personendaten ... 19
3.2.4 Recht auf Berichtigung der Personendaten ... 19
3.2.5 Recht auf Verbot der Bearbeitung von Personendaten ... 19
3.2.6 Recht auf Verbot der Bekanntgabe von Personendaten ... 20
3.2.7 Recht auf Mitteilung der Massnahmen betreffend Personendaten ... 20
3.3 Reproduzierbarkeit der Verfahren ... 20
4 Bundesorgane ... 22
4.1 Gesetzliche Grundlagen ... 22
4.2 Datenbearbeitung für nicht personenbezogene Zwecke ... 22
4.3 Bekanntgabe ... 23
4.4 Verzeichnis der Datenbearbeitungen ... 23
4.5 Meldung von Verletzungen der Datensicherheit ... 23
4.6 Automatisierte Einzelentscheidungen ... 23
4.7 Informationspflicht ... 24
4.8 Rechte der betroffenen Personen ... 24
4.9 Protokollierung ... 24
4.10 Bearbeitungsreglement ... 24
5 Datenschutz ... 26
5.1 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen ... 26
5.2 Pseudonymisierung ... 27
5.3 Anonymisierung ... 28
5.4 Generalisierung ... 30
5.5 Minimierung ... 31
5.6 Randomisierung ... 31
5.7 Homomorphe Verschlüsselung ... 32
5.8 Synthetische Daten ... 32
6 Infrastruktur ... 33
6.1 Sicherheit der Räumlichkeiten ... 33
6.2 Sicherheit der Serverräume ... 34
6.3 Sicherheit der Arbeitsplätze ... 34
6.4 Cloud-Nutzung ... 35
6.5 Zur Vertiefung ... 36
7 Zugriff und Bearbeitungen ... 37
7.1 Zugriffsverwaltung ... 37
7.2 Identifizierung und Authentifizierung ... 37
7.3 Zugang zu den Daten ... 38
7.4 Zugang von ausserhalb der Organisation ... 39
7.5 Zur Vertiefung ... 39
8 Lebenszyklus der Daten ... 40
8.1 Datenerfassung ... 40
8.2 Verschlüsselung ... 41
8.3 Sicherheit der Datenträger ... 42
8.4 Datensicherung ... 42
8.5 Datenvernichtung ... 43
8.6 Sicherheits- und Schutzstufe ... 43
8.7 Protokollierung ... 45
8.8 Bearbeitungsreglement ... 46
9 Datenaustausch und -übermittlung ... 48
9.1 Netzsicherheit ... 48
9.2 Verschlüsselung von Mitteilungen ... 49
9.3 Digital Unterzeichnen von Mitteilungen (signieren) ... 50
9.4 Übergabe von Datenträgern ... 51
9.5 Protokollierung des Datenaustauschs ... 52
9.6 Datenbekanntgabe ins Ausland ... 52
9.7 Bearbeitung durch Auftragsbearbeiter ... 53
10 Schlussbemerkungen ... 54
11 Referenzen ... 55



Quelle:
https://www.mll-news.com/edoeb-veroeffentlicht-leitfaden-zu-den-technischen-und-organisatorischen-massnahmen-des-datenschutzes/

Präventiv-Massnahmen gegen Ransomware-Angriffe

- Unternehmen brauchen zwingend einen **Cyber-Security-Plan**
- **Periodische Schulung** aller Mitarbeitenden (inkl. Nachweisdokument über Teilnahme)
- **Automatische Sicherheits-Updates** für PC/Server/übrige IT-Infrastrukturen (wie Firewalls, Netzwerk-Komponenten) durchführen lassen
- Antiviren-Software installieren und aktuell halten
- Datensicherung aller geschäftsrelevanten Daten nach der **3-2-1 Regel**
- **Datensicherung auf separaten (nicht netzwerkverbundenen) Festplatten**
- Keine Mails öffnen mit
  - suspektem Inhalt
  - unbekannter Absenderadresse
  - Anfragen nach Accountnamen oder Passworten nie beantworten.
  - Oft ist ein telefonischer Rückruf an den Absender sehr hilfreich und aufschlussreich.

Tipps für den sicheren Umgang:

- **Sichere Webseiten:** Achten Sie darauf, dass die URL mit "https://" beginnt und berücksichtigen Sie die Wahl des Online-Anbieters.

- **Daten schützen:** Geben Sie Ihre Zahlungsmitteldaten, Login-Informationen oder Sicherheitscodes nie an Dritte weiter oder auf betrügerischen Webseiten ein.

- **Kritisch sein:** Klicken Sie nicht auf Links oder Anhänge in Mails, SMS/Chats oder Social Media Nachrichten von Absendern mit beispielsweise vielen Rechtschreibefehler oder mit einer fehlenden persönlichen Anrede.

Cyberversicherungen

- Sinnvoll ja oder nein?

- Lesen Sie die Allg. Versicherungsbedingungen (AVB), welche zur Cyberversicherung mitgegeben werden, aufmerksam durch.
- Oft zeichnen sich Cyberversicherungen von der Vertragserfüllung frei, wenn der Versicherte vorsätzlich oder grobfahrlässig gehandelt hat.
- Cyberversicherungen wehren immer zuerst ab und verweisen auf mindestens Grobfahrlässigkeit beim Versicherten.
- Dann müssen SIE gegen die Versicherung auf Erfüllung klagen (??)

Besten Dank

Lukas Fässler
Rechtsanwalt & Informatikexperte

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76B
CH-6340 Baar
Tel. +41 +41 727 60 80

www.fsdz.ch
faessler@fsdz.ch