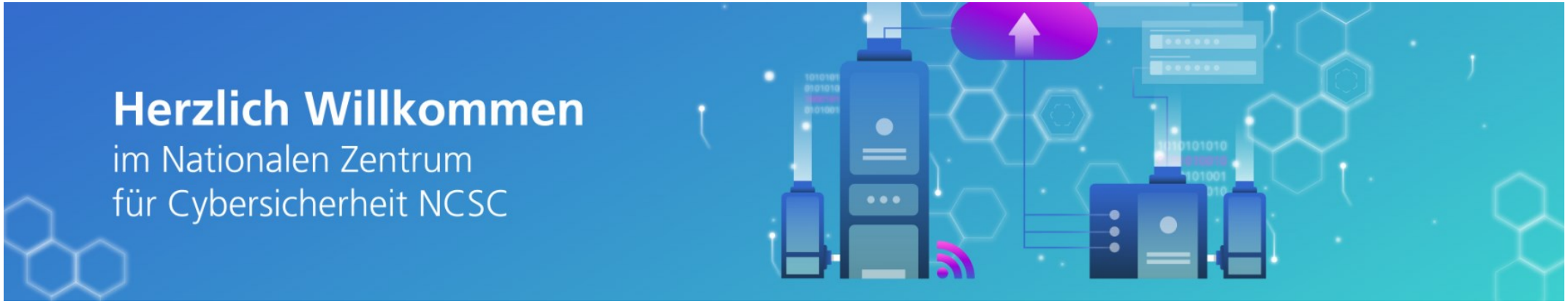
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
Swiss Government Computer Emergency Response Team (GovCERT.ch)

Schutz kritischer Infrastrukturen und Internet Hygiene in der Schweiz



10. Februar 2023

$ whoami

Neue Zürcher Zeitung

Ausmass verharmlost? Der Cyberangriff auf die Stadt Bülach ist schwerwiegender, als bisher kommuniziert

Seit Sonntag steht die Stadtverwaltung von Bülach still. Grund dafür ist ein krimineller Angriff auf die IT-Infrastruktur. Vermutlich wurden zentrale Daten der Verwaltung gestohlen.

Lukas Mäder

21.07.2022, 16.15 Uhr

Hören Merken Drucken Teilen

Neue Zürcher Zeitung

Ausmass verharmlost? die Stadt Bülach ist sc bisher kommuniziert

Seit Sonntag steht die Stadtverwalt ist ein krimineller Angriff auf die IT- zentrale Daten der Verwaltung gest

Lukas Mäder

21.07.2022, 16.15 Uhr

Höre

Blick

WIRTSCHAFT

Wirtschaft | Hacker-Angriff auf Swissport beeinträchtigt den Flugbetrieb

Flugbetrieb gestört

Hacker-Angriff auf Swissport!

Swissport wurde Opfer eines Hacker-Angriffs. Die Systeme waren beeinträchtigt. Flugzeuge blieben am Boden, konnten erst mit Verspätung abheben. Swissport bestätigt den Vorfall.

Publiziert: 04.02.2022 um 09:32 Uhr | Aktualisiert: 04.02.2022 um 12:46 Uhr

9

Neue Zürcher Zeitung

Ausmass verharmlost? die Stadt Bülach ist sc bisher kommuniziert

Seit Sonntag steht die Stadtverwalt ist ein krimineller Angriff auf die IT- zentrale Daten der Verwaltung gest

Lukas Mäder

21.07.2022, 16.15 Uhr

Höre

watson

Schweiz International Wirtschaft Sport Leben Spass Digital Wissen Blogs Quiz Videos Promotionen

Blick

WIRTSCHAFT

Wirtschaft | Ha

Flugbetrieb

Hack Swiss

Swissport wurde beeinträchtigt. Fl abheben. Swisspo

Publiziert: 04.02.2022 um 0

Ransomware-Attacke auf Migros-Tochter: Hacker drohen mit Leak, Sprecher beschwichtigt

9

Neue Zürcher Zeitung

watson

Schweiz International Wirtschaft Sport Leben Spass Digital Wissen Blogs Quiz Videos Promotionen

IT INSIDE IT

INSERIEREN JOBPORTAL

Aus
die
bis

Seit
ist ei
zentr

Lukas
21.07.2

Schoggifabrikant Läderach von Ransomware-Attacke beeinträchtigt

Von Christian Wingeier, 6. September 2022 um 16:32

SECURITY LÄDERACH CYBERANGRIFF RANSOMWARE DETAILHANDEL SCHWEIZ

mware-Attacke auf s-Tochter: Hacker dro- it Leak, Sprecher be- chtigt

9

Neue Zürcher Zeitung

IT INSIDE IT

Schoggifabrikant Läderach v
beeinträchtigt

Von Christian Wingeier, 6. September 2022 um 16:32

SECURITY LÄDERACH CYBERANGRIFF RA

Aus
die
bis

Seit
ist ei
zentr

Lukas
21.07.2

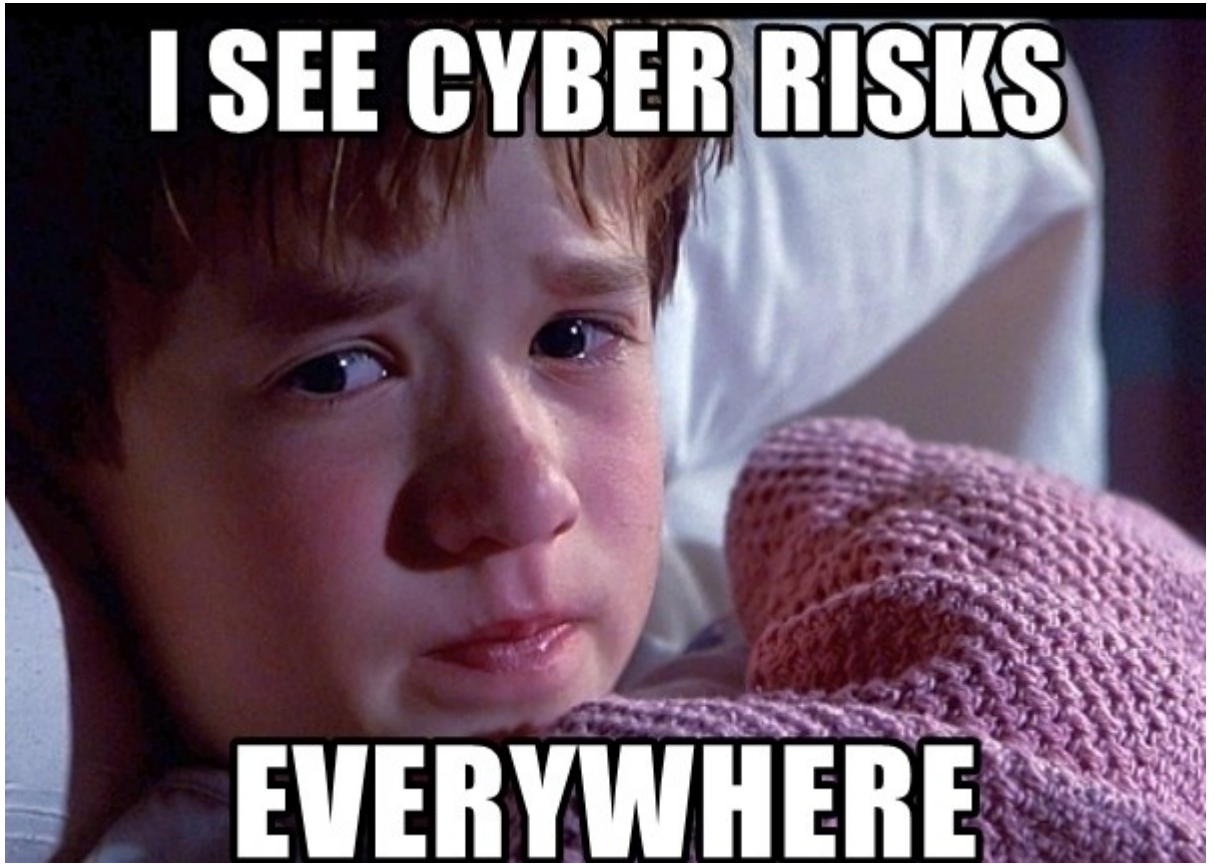
watson 4° DE | FR

Spass Digital Wissen Blogs Quiz Videos Promotionen

are-Attacke auf
chter: Hacker dro-
eak, Sprecher be-
gt

9

Cyber, Cyber, Cyber



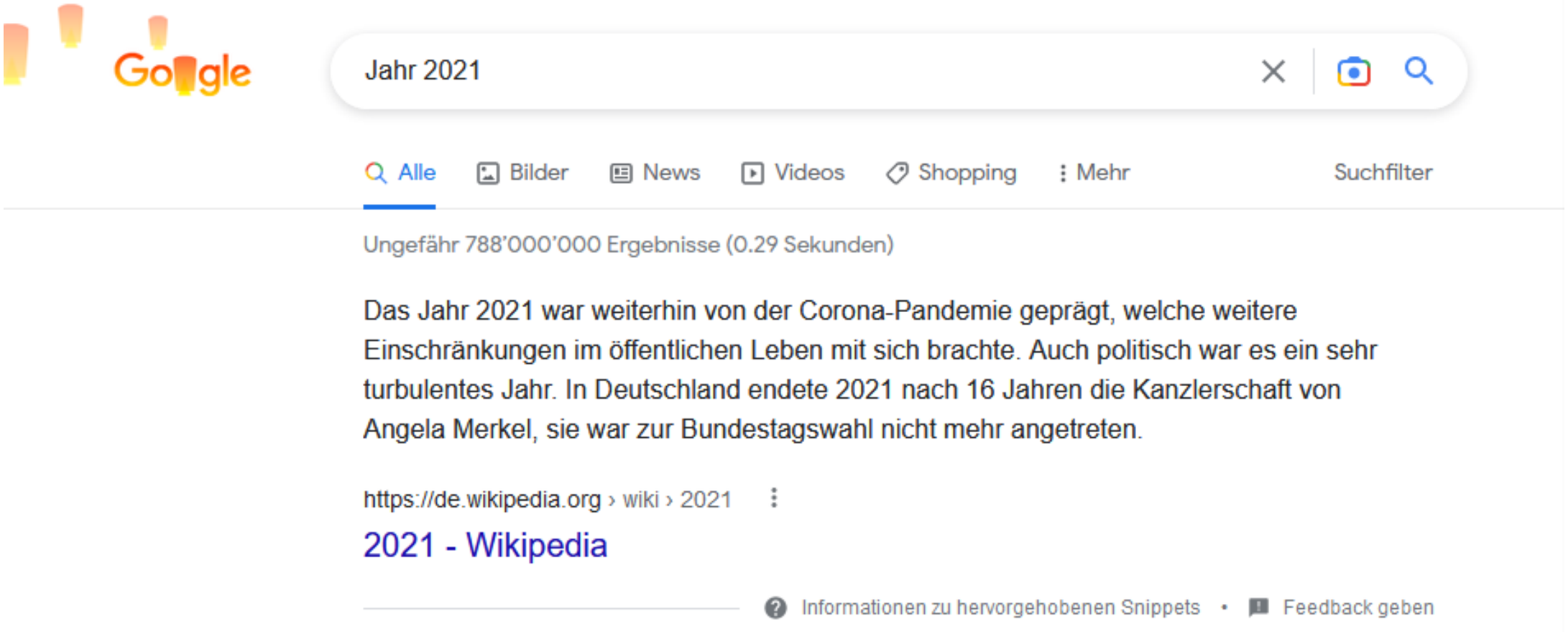
Cybersicherheit ist keine Raketenwissenschaft

1. Was tut das NCSC?

Was tut das NCSC?

- Prävention:
  - Sensibilisierung der Öffentlichkeit, Wirtschaft und Behörden
  - Präventive technische Massnahme mit Stakeholdern
- Detektion:
  - Sensorik
  - CERT-Austausch (national, international)
- Reaktion:
  - Incident Response (Erste Hilfe)
  - Technische Analysen

2021?


Google
Jahr 2021
Alle
Bilder
News
Videos
Shopping
Mehr
Suchfilter
Ungefähr 788'000'000 Ergebnisse (0.29 Sekunden)
Das Jahr 2021 war weiterhin von der Corona-Pandemie geprägt, welche weitere Einschränkungen im öffentlichen Leben mit sich brachte. Auch politisch war es ein sehr turbulentes Jahr. In Deutschland endete 2021 nach 16 Jahren die Kanzlerschaft von Angela Merkel, sie war zur Bundestagswahl nicht mehr angetreten.
https://de.wikipedia.org › wiki › 2021
2021 - Wikipedia
Informationen zu hervorgehobenen Snippets
Feedback geben

2021: Exchange, Pulse VPN, SonicWALL…

heise online heise+ Jetzt 1 Monat gratis testen

Alert!

ProxyShell: Massive Angriffswelle auf ungepatchte Exchange-Server

Die Lücken sind bekannt, Patches da – trotzdem sind tausende Exchange-Server angreifbar. Nun rollt eine massive Angriffswelle, die die Schwachstellen ausnutzt.

22.08.2021 13:47 Uhr | Security

Von Günter Born

RAPID7

Active Exploitation of Pulse Connect Secure Zero-Day (CVE-2021-22893)

Apr 21, 2021 | 3 min read | Caitlin Condon

Last updated at Wed, 21 Apr 2021 20:36:39 GMT

On Tuesday, April 20, 2021, security firm FireEye published detailed analysis of multiple threat campaigns targeting Ivanti's Pulse Connect Secure VPN. According to FireEye's analysis, threat actors have been leveraging multiple techniques to bypass single- and multi-factor authentication on Pulse Secure VPN devices, establish persistence across updates, and maintain access via webshells. The focus of the analysis is on threats to U.S. defense networks, but Pulse Secure devices are also a perennially popular target for exploitation across a broad range of organizations' networks.

2021: Exchange, Pulse VPN, SonicWALL…

Herausforderung #1:

- Identifikation von verwundbaren Gerätschaften

2021: Exchange, Pulse VPN, SonicWALL…

Herausforderung #2:

- Identifikation der Betreiber*innen

2021: Exchange, Pulse VPN, SonicWALL…

Herausforderung #3:

- Effiziente Benachrichtigung der Betreiber*innen

Identifikation von Anschlussinhaber*innen

Der Bundesrat › Bundesrecht

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Fedlex
Die Publikationsplattform des Bundesrechts

780.1

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

(BÜPF)

vom 18. März 2016 (Stand am 1. Juni 2022)

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,

gestützt auf die Artikel 92 Absatz 1 und 123 Absatz 1 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom 27. Februar 2013[2],

beschliesst:

Art. 21 Auskünfte über Fernmeldedienste

[1] Die Anbieterinnen von Fernmeldediensten liefern dem Dienst folgende Angaben über bestimmte Fernmeldedienste:

a. Name, Vorname, Geburtsdatum, Adresse und, falls bekannt, Beruf der Teilnehmerin oder des Teilnehmers;

b.[35] die Adressierungselemente nach Artikel 3 Buchstabe f des Fernmeldegesetzes vom 30. April 1997[36] (FMG);

c. die Arten der Dienste;

d. weitere vom Bundesrat bezeichnete Daten über Fernmeldedienste; diese Daten können administrativer oder technischer Natur sein oder die Identifikation von Personen erlauben;

e. bei Kundenbeziehungen ohne Abonnementsverhältnis: zusätzlich Abgabestelle und Name und Vorname der Person, welche das für den Zugang zum Fernmeldedienst erforderliche Mittel abgegeben hat.

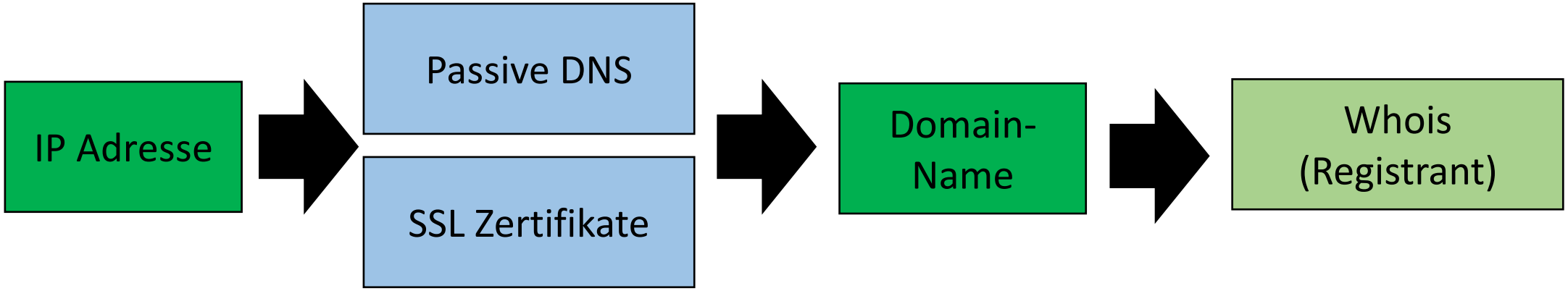
Identifikation von Anschlussinhaber*innen

Art. 1 Sachlicher Geltungsbereich

[1] Dieses Gesetz gilt für die Überwachung des Post- und Fernmeldeverkehrs, die angeordnet und durchgeführt wird:

a. im Rahmen eines Strafverfahrens;
b. zum Vollzug eines Rechtshilfeersuchens;
c. im Rahmen der Suche nach vermissten Personen;
d. im Rahmen der Fahndung nach Personen, die zu einer Freiheitsstrafe verurteilt wurden oder gegen die eine freiheitsentziehende Massnahme angeordnet wurde;
e.[3] im Rahmen des Vollzugs des Nachrichtendienstgesetzes vom 25. September 2015[4] (NDG);
f.[5] im Rahmen von Mobilfunklokalisierungen nach dem Bundesgesetz vom 21. März 1997[6] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS).

Identifikation von Anschlussinhaber*innen



Identifikation von Anschlussinhaber*innen

Identifikation von Anschlussinhaber*innen

Der Bundesrat › Bundesrecht

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Fedlex
Die Publikationsplattform des Bundesrechts

784.104.2

Verordnung über Internet-Domains

(VID)

vom 5. November 2014 (Stand am 1. Januar 2021)

Der Schweizerische Bundesrat,

gestützt auf die Artikel 13*a* Absatz 3, 28 Absätze 2, 3, 4 und 6, 28*e*, 48*a* Absatz 2, 59 Absatz 3, 62 und 64 Absatz 2 des Fernmeldegesetzes vom 30. April 1997[1] (FMG),[2]

verordnet:

– **Art. 46[45] Bereitstellung von Daten**

[3] Sie gewährt jeder Person, die ein überwiegendes legitimes Interesse glaubhaft macht, kostenlos Zugang zu den in der RDDS-Datenbank (WHOIS) enthaltenen Personendaten der Halterin oder des Halters des betreffenden Domain-Namens.

Benachrichtigung von Anschlussinhaber*innen

- Problematik:
  - Spamfilter
  - Veraltete Adressangabe (Email Adresse existiert nicht mehr)
  - Misstrauen gegenüber unseren Emails

Benachrichtigung von Anschlussinhaber*innen

Switzerland hosted resources daily report

Generated at Tue, 16 Nov 2021 00:55:02 UTC

Summary

Found 943 unsecured databases in the last 24h, 178.7 MB in 455,714 rows.

Host	Port	Source	Country	Priority	Infected	Leak rows	Leak size
			Switzerland	high	false	455,637 rows	132.0 MB
			Switzerland	medium	false	77 rows	46.7 MB
			Switzerland	critical	false	0 rows	0 B
			Switzerland	critical	false	0 rows	0 B
			Switzerland	critical	false	0 rows	0 B
			Switzerland	critical	false	0 rows	0 B

Benachrichtigung von Anschlussinhaber*innen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Höchste Zeit, die Sicherheitslücken bei Microsoft Exchange-Server zu schliessen

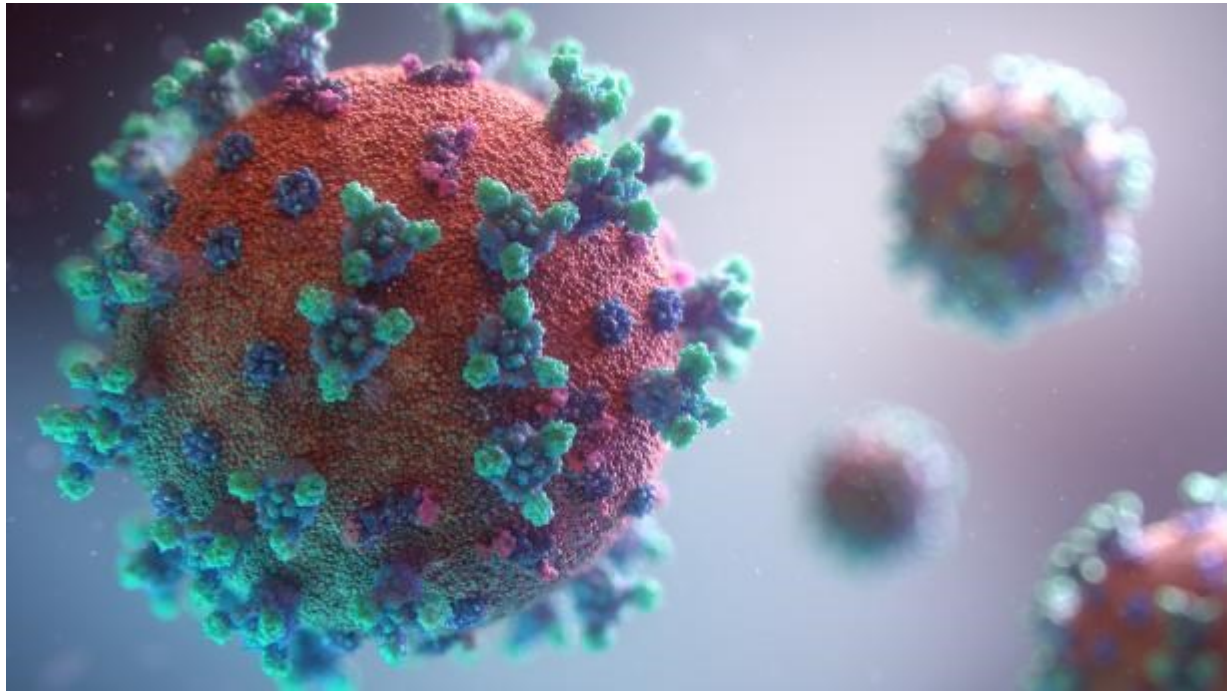
16.02.2022 - Das NCSC ruft Unternehmen und Gemeinden eindringlich dazu auf, die Sicherheits-Patches für die Microsoft Exchange-Server einzuspielen. Die seit langem bekannten Sicherheitslücken werden von Cyberkriminellen aktiv ausgenutzt, um beispielsweise Verschlüsselungstrojaner einzuschleusen.

NCSC ruft auf, die Sicherheits-Patches einzuspielen

Das NCSC hat im letzten Jahr über 4500 Unternehmen und Gemeinden per E-Mail über die Verwundbarkeit informiert und eine Anleitung zur Behebung dieser Sicherheitslücke mitgesandt. Doch trotz mehrmaligem Nachfassen, haben noch nicht alle Betroffenen die notwendigen Massnahmen ergriffen. In den vergangenen Tagen erhielt das NCSC von internationalen Partnern Hinweise, dass dutzende Unternehmen und Gemeinden die Sicherheits-Updates noch immer nicht eingespielt haben.

Benachrichtigung von Anschlussinhaber*innen

Benachrichtigung von Anschlussinhaber*innen



Benachrichtigung von Anschlussinhaber*innen

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [1/4]

NCSC MA:
«Grüäzi, ich bräuchte 1’000 Einschreiben-Etiketten.»

Postangestellte/r:
«So viele haben wir nicht. Wir können Ihnen aber 80 mitgeben.»

NCSC Mitarbeiter radelt mit dem Velo in die Nachbarsgemeinden…

Benachrichtigung von Anschlussinhaber*innen

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [2/4]

NCSC MA:
«Grüäzi, ich hätte hier 500 Briefe zum Einschreiben.»

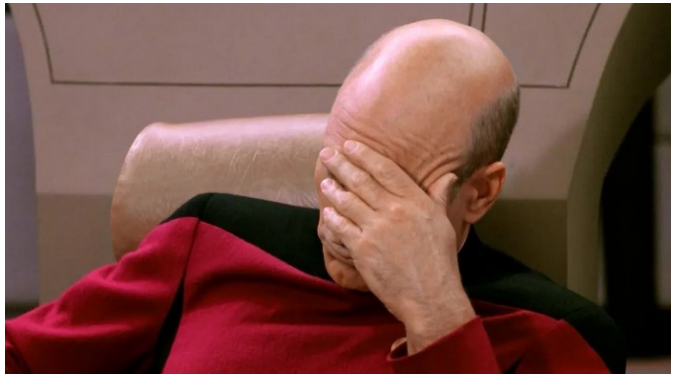
Postangestellte/r:
«Tut mir leid, wir nehmen maximal 10 Briefe pro Sendung an.»

NCSC Mitarbeiter radelt (erneut) mit dem Velo in die Nachbarsgemeinden…

Benachrichtigung von Anschlussinhaber*innen

- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [3/4]

NCSC MA:
«Vorsicht! Sie haben eine Infektion in Ihrem Netzwerk, welche höchstwahrscheinlich zu einer Verschlüsselung mit Ransomware führt.»



Opfer:
«Annahme des Einschreiben verweigert.»

Benachrichtigung von Anschlussinhaber*innen

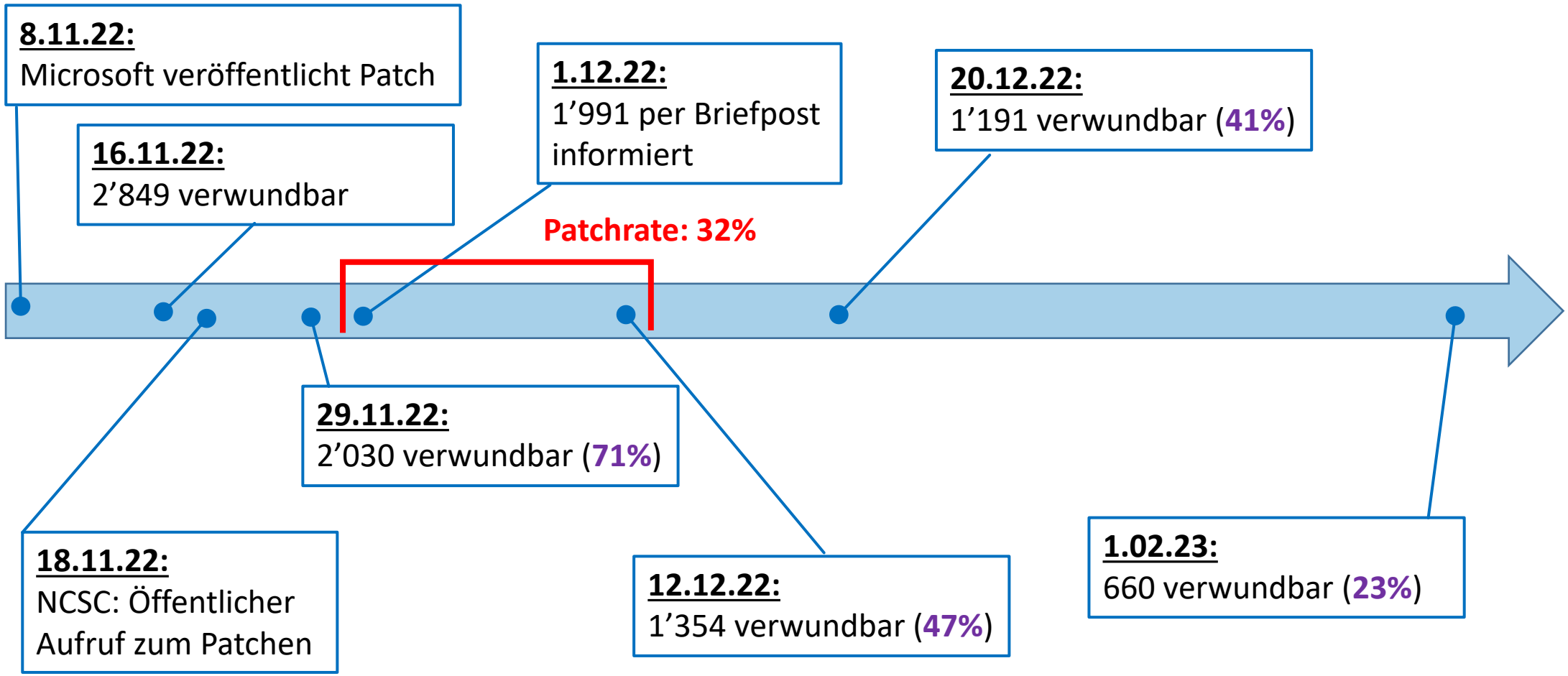
- Wie der Briefversand im Jahr 2022 (nicht) funktioniert… [4/4]

NCSC MA:
«Vorsicht! Sie haben eine Infektion in Ihrem Netzwerk, welche höchstwahrscheinlich zu einer Verschlüsselung mit Ransomware führt.»

Opfer:
«Sendung nicht abgeholt, Abholfrist abgelaufen.»

2. Wie sinnvoll ist die Benachrichtigung auf dem Postweg?

ProxyNotShell (CVE-2022-41082)



ProxyNotShell (CVE-2022-41082)

- Briefzustellung (Total: 1’991):
  - Empfänger existiert nicht (3%)
  - Brief nicht abgeholt (0.5%)
  - Annahme verweigert (0.1%)

Vielen Dank für Ihre Aufmerksamkeit!