Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

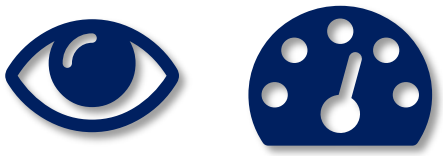
12nach12 Lunch
«Einblicke in die Welt der Cybersicherheit»

20. Oktober 2022 - Nordwestschweizerische Public Relations Gesellschaft NPRG

Daniel W. Seiler, IT-Projektleiter NCSC

Themen

- Aktuelle Lage im Cyberspace
- Das Nationale Zentrum für Cybersicherheit
- What’s next?
- Einige Tipps

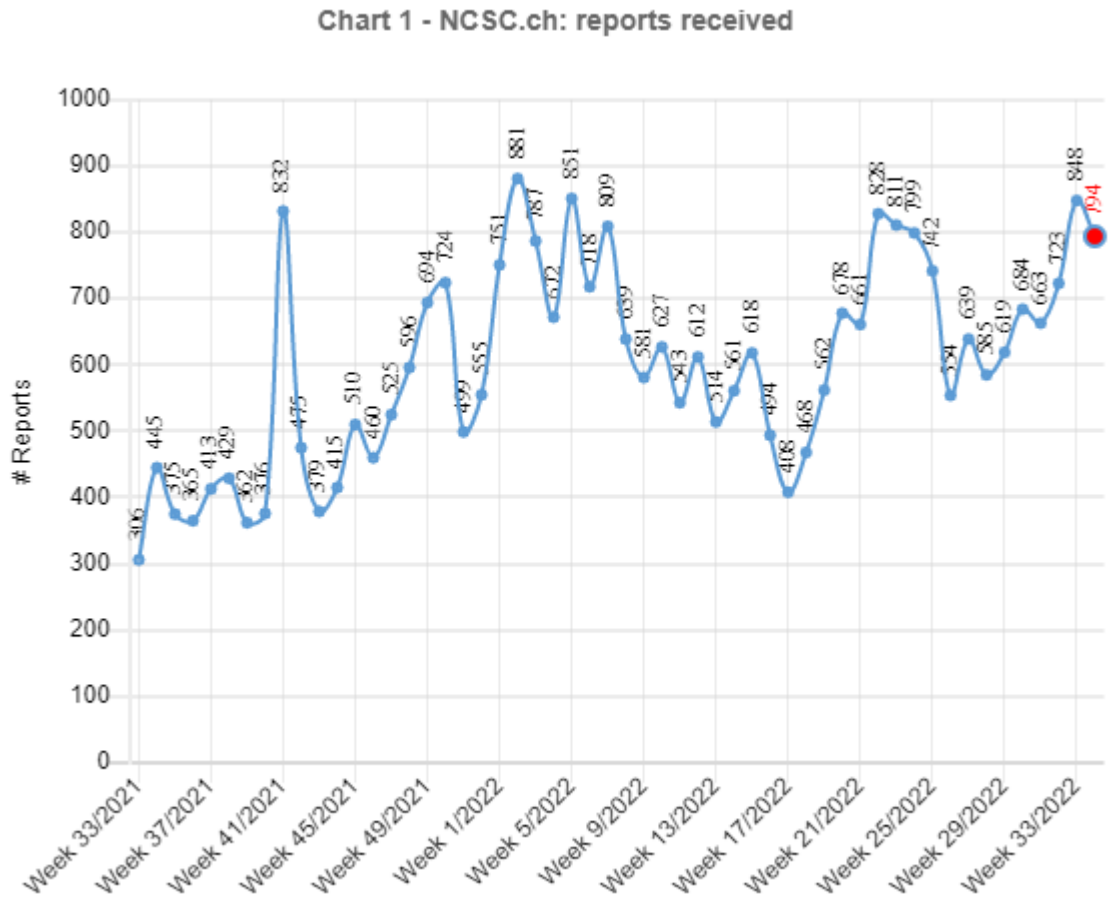


AKTUELLE LAGE IM CYBERSPACE

Meldungen ans NCSC

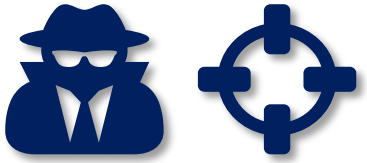
2021

21’714 Meldungen von Unternehmen und Bevölkerung
davon
11362 Betrug
4956 Phishing
908 Malware
312 hacking
43 Datenabflüsse



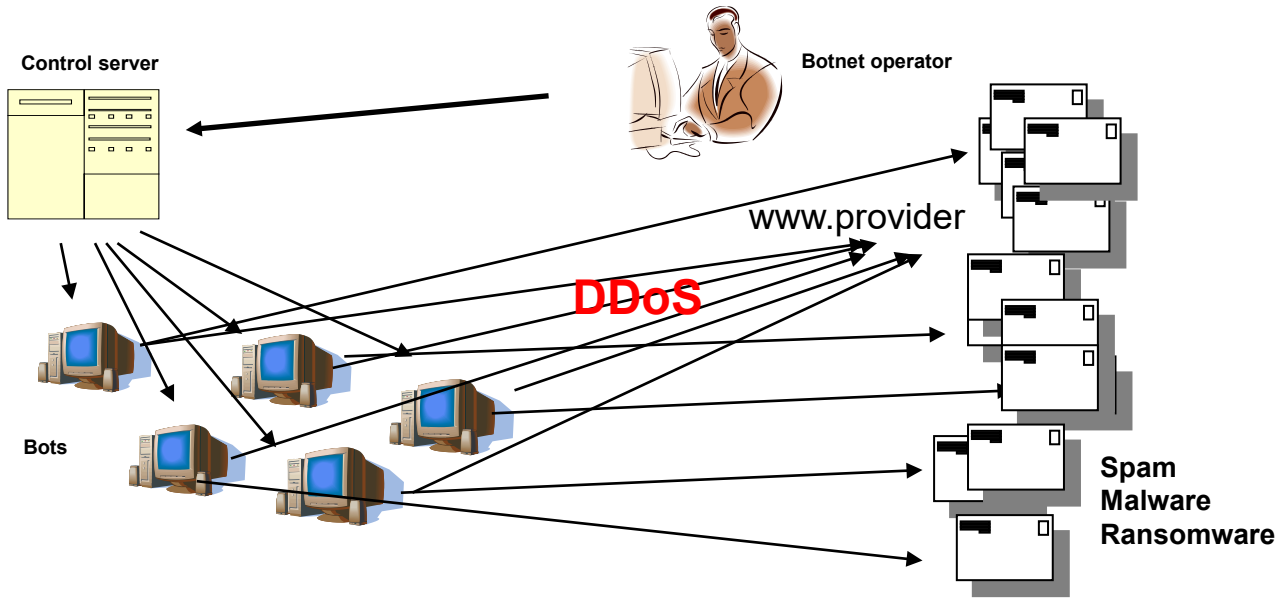
2022 **(01.09.2022)**

23’255 Meldungen von Unternehmen und Bevölkerung
davon
14362 Betrug
2939 Phishing
285 Malware
260 hacking
26 Datenabflüsse



ANGRIFFS-ARTEN UND VEKTOREN

Distributed Denial of Sevice (DDos)



DDoS Angriffe – einfach zu erhalten

Zunahme von DDoS Angriffen

WARUM FÜR 2022 EINE NEUE REKORDZAHL AN DDOS-ATTACKEN PROGNOSTIZIERT WIRD

Veröffentlicht am 30. Mär 2022 | von Michelle Gehri | Cyberrisiken

Stand 2021 Ransomware besonders hoch im Kurs, so stehen die Chancen gut, dass 2022 DDoS die Cyber-Security-Welt erneut stark beschäftigen wird, denn in den letzten Monaten haben DDoS-Angriffe massiv zugenommen. Security-Expert*innen vermuten, dass dies nur die Spitze des Eisbergs war. Das Gefährliche an DDoS: Mit herkömmlichen Mitteln sind diese nur schwer aufzuhalten. Da der Angriff verteilt erfolgt, sprich von verschiedenen Quellen ausgehend, reicht es nicht, eine einzelne Quelle zu blockieren. In diesem Artikel geben wir Ihnen einen Überblick über die Entwicklungen der letzten Monate, erläutern die aktuelle Risikolage und geben eine Empfehlung, wie Sie sich auf die DDoS-Welle vorbereiten können.

Bereits in früheren Artikeln (z.B. hier oder hier) haben wir über die rasche Zunahme an Distributed-Denial-of-Service-(DDoS)-Angriffen* berichtet sowie mögliche Zukunftsszenarien, die bereits damals nicht Gutes verheissen liessen. Nun sind die Befürchtungen eingetroffen. NETSCOUT hat kürzlich die Ergebnisse ihres halbjährlichen Threat Intelligence Reports veröffentlicht. In der zweiten Jahreshälfte 2021 starteten Cyber-Kriminelle rund 4,4 Millionen DDoS-Angriffe, womit sich die Gesamtzahl der DDoS-Angriffe im Jahr 2021 auf 9,75 Millionen beläuft – das entspricht einem Angriff alle drei Sekunden.

Zu ähnlichen Ergebnissen kommen auch Untersuchungen anderer Unternehmen wie beispielsweise des Netzwerk-Anbieters Cloudflare. Dieser berichtet weiter, dass in der zweiten Jahreshälfte 2021 Terabit-starke Angriffe massiv zugenommen haben. Ihr analysierter Spitzenwert: Ein DDoS-Angriff mit knapp zwei Terabits pro Sekunde, der insgesamt lediglich zwei Minuten andauerte und von 15'000 Bots gestartet wurde.

Quelle: InfoGuard AG - Michelle Gehri

Im ersten Quartal 2022 ist die Anzahl an DDoS-Angriffen um das 4,5-fache im Vergleich zum gleichen Vorjahresquartal gestiegen [1]. Des Weiteren war die durchschnittliche Dauer einer Attacke 80 Mal länger als in Q1 2021. Die Experten von Kaspersky sehen es als wahrscheinlich an, dass diese Zunahme der Angriffe auf hacktivistische Aktivitäten zurückzuführen ist.

DDoS (Distributed Denial of Service)-Angriffe zielen darauf ab, die von Unternehmen und Organisationen genutzten Netzwerkressourcen zu unterbrechen und deren ordnungsgemäßen Betrieb zu beinträchtigen. Erfolgreiche Attacken vor allem auf Behörden und auf Institutionen im Finanzbereich haben weitreichendere negative Auswirkungen, da die Nichtverfügbarkeit dieser Dienste die gesamte Bevölkerung betrifft.

Im ersten Quartal 2022 kam es Ende Februar aufgrund der Krise in der Ukraine zu einem plötzlichen Anstieg der Angriffe: Im Vergleich zum vierten Quartal 2021, in dem die Zahl der von Kaspersky-Lösungen erkannten DDoS-Angriffe ihren bisherigen Höchststand erreicht hatte, stieg die Gesamtzahl der DDoS-Angriffe im ersten Quartal 2022 um 46 Prozent. Dies entspricht einem Anstieg um das 4,5-fache. Die Anzahl der intelligenten, fortschrittlichen und zielgerichteten Angriffe wies ebenfalls einen bemerkenswerten Anstieg von 81 Prozent im Vergleich zum vorherigen Höchstwert aus dem vierten Quartal 2021 auf. Die Attacken wurden nicht nur im großem Maßstab durchgeführt, sondern waren auch innovativer. Beispiele hierfür sind eine Website, die das beliebte 2048-Puzzlespiel imitiert, um DDoS-Angriffe auf russische Websites zu gamifizieren, und ein Aufruf zum Aufbau einer freiwilligen IT-Armee, um Cyberangriffe zu erleichtern.

Quelle: Kaspersky

Ransomware

Angriffe mit Erpressungssoftware

Colonial Pipeline: FBI beschlagnahmt Großteil des Lösegeldes

Ein Erpressungstrojaner hatte die Pipeline-Firma erwischt. Sie zahlte Löseg
Form von Bitcoin und hatte Glück im Unglück.

Lesezeit: 1 Min. In Pocket speichern

Das Symbolbild zeigt ein Warnschild über einer anderen unterirdisch verlegten US-Pipeline. (Bil
AJ Sokolov)

Colonial Pipeline droht Millionenbusse

Von Reto Vogt, 10. Mai 2022, 15:27

SECURITY CYBERANGRIFF COLONIAL PIPELINE USA

Benzinknappheit aufgrund Ransomware-Angriff. Foto: Wikimedia / Famartin (CC BY-SA 4.0)

Ein Jahr nach der Ransomware-Attacke auf die amerikanische Öl-Pipeline droht dieser eine Busse von fast einer Million Dollar wegen Verstössen gegen nationale Sicherheitsregeln.

Am 7. Mai 2021 wurde der Ransomware-Angriff auf eine der grössten Öl-Pipelines der USA entdeckt. Man habe daraufhin bestimmte Systeme offline genommen, um die Bedrohung einzudämmen. Dies führte dazu, dass man den gesamten Pipeline-Betrieb vorübergehend gestoppt habe, schrieb Colonial Pipeline dazu.

Der Angriff blieb nicht ohne Folgen: In den USA wurde aufgrund des Ausfalls ein regionaler Notstand ausgerufen. Zudem ging das Management des Unternehmens auf die Forderungen der Ransomware-Bande Darkside ein und hat noch am Tag des Angriffs die Zahlung von 4,4 Millionen Dollar genehmigt. Der Schaden für das Unternehmen war indes wesentlich grösser: CEO Joseph Blount schätzte diesen damals auf mehrere 10 Millionen Dollar.

Busse von knapp 1 Million Dollar droht

Bezahlt wurde die Forderung der Hacker damals, obwohl Regierungen und Experten stets empfehlen, kein Lösegeld zu bezahlen, weil das zu weiteren Hacks einlade.

lte angeblich Lösegeld an Hacker

Pipeline in den USA gibt es Informationen zu einer
'd wieder hochgefahren.

ld: Samuel Corum/Bloomberg)

h dem Hacker-Angriff auf eine
ies in den USA sickern
enschwere Lösegeldzahlung
nachrichtenagentur Bloomberg
schaft Colonial osteuropäischen
ternehmen habe den Betrag nur
n einer nicht zurückverfolgbaren
s es unter Berufung auf zwei mit
. Danach hätten die Hacker
hlüsselung zur Verfügung
setzte Computersystem
h dieses habe nur langsam
line-Betreiber schliesslich auf
nte zurückgegriffen.

FuW-Umfrage

Wie lange gibt es in der Schweiz Strafzinsen auf Cash?

- Nur noch bis diesen Herbst
- Bis Ende 2022
- Noch mehrere Jahre

ABSTIMMEN

Alle Umfragen »

Neue Artikel

HEUTE, 08:59 MÄRKTE
Chinas Wirtschaft schaltet Gang zurück

HEUTE, 08:33 AKTIEN
SMI notiert stabil

HEUTE, 08:08 MÄRKTE
Bitcoin nach Musk-Tweet auf Dreieinhalb-Monats-Tief

HEUTE, 07:49 GESUNDHEIT, SCHWEIZ
Relief-Übernahmeziel APR hat Studie mit Covid-Nasenspray gestartet

HEUTE, 07:43 GESUNDHEIT, SCHWEIZ
Evolva sichert sich weiteres Kapital

Ransomware

Cyberkriminalität *03.02.2020, 10:25 Uhr*

Hackerangriff auf die Amag verübt

Auf die IT des Autohändlers Amag wurde ein Cyberangriff verübt. Die Attacke fällt direkt in die heisse Vorbereitungsphase auf den geplanten Einstieg des Unternehmens in das Online-Business.

Stadler Rail erleidet Cyberangriff

Eine unbekannte Täterschaft hat versucht, den Schienenfahrzeug-Hersteller aus Bussnang zu erpressen. Es ist ihr offenbar gelungen, einen grösseren Abfluss von Daten zu verursachen.

Dominik Feldges
07.05.2020, 19.05 Uhr

Hören Merken Drucken Teilen

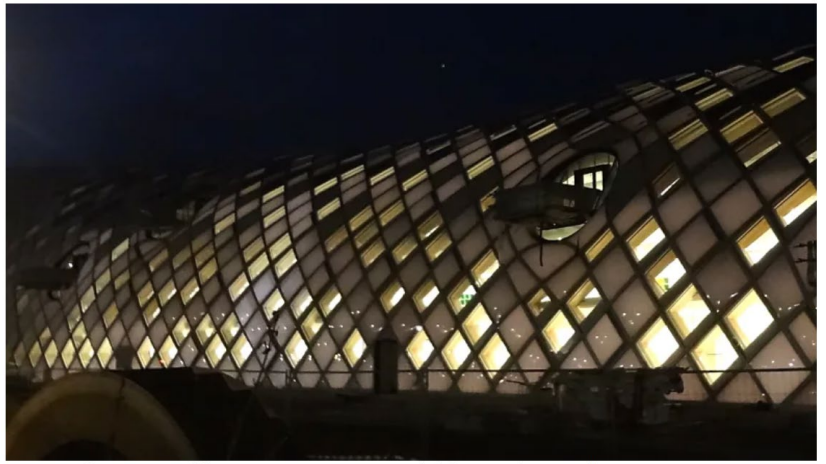
Der Schienenfahrzeug-Hersteller Stadler Rail ist Opfer eines Cyberangriffs geworden.

Gian Ehrenzeller / Keystone

Swatch wurde Opfer eines Cyber-Angriffs

SWATCH, SECURITY, ATTACKE, INDUSTRIE, SCHWEIZ

Von Keystone-sda/mag, 29. September 2020 17:29 Letzte Aktualisierung: 29. September 2020 17:48



Der Swatch-Sitz in Biel (Foto: MHM55, Batiment (...) du Swatch Group à Bienne, Lizenz CC BY-SA 4.0)

Einige IT-Systeme sind nach wie vor down, bestätigt der Konzern auf Nachfragen.

Cyberangriffe auf Gemeinden

Gemeinde Rolle räumt Fehler im Umgang mit Cyberangriff ein

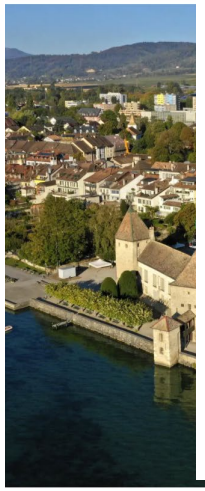
Der Cyberangriff auf die Verwaltung der Waadtländer Gemeinde Rolle hat ein grösseres Ausmass als zunächst bekannt. So wurden geklaute Daten im Darknet gehandelt.

Nach dem Ransomware-Angriff auf die Gemeindeverwaltung von Rolle sind sensible Daten der Bewohnerinnen und Bewohner wie etwa deren AHV-Nummer im Darknet aufgetaucht
(Quelle: Alexey Muzalyev/Wikimedia)

rsönliche Dat
acke auf Rolle
Behörden kom

die Waadtländer Gem
Bürger, Mitarbeiter un
ker wollten Lösegeld.

Hören



Datum: 17.06.2022

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich

Seite: 8
Fläche: 196'668 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 84626405
Ausschnitt Seite: 2/5

Ein Hackerangriff schüttelt eine Gemeinde durch

Das Städtchen Rolle machte vor einem Jahr landesweit Schlagzeilen, weil es Opfer einer Cybererpressung wurde. Der Fall zeigt, wie rasch eine Milizbehörde in der Krise überfordert ist

LUKAS MÄDER, ANTONIO FUMAGALLI

Der Tsunami kam in zwei Wellen. Die erste legte – unbemerkt von der Öffentlichkeit – die Computer der Gemeindeverwaltung Rolle lahm. Die zweite und heftigere Welle stürzte in Form von Medienanfragen über die Gemeindepräsidentin ein. Und brachte sie an ihr Limit.

Am 20. August letzten Jahres publizierte das Newsportal «Watson» einen Artikel: «Schweizer Gemeinde wird gehackt und verschweigt Datendiebstahl». Für Monique Pugnale, die Präsidentin des Städtchens am Genfersee, war die Welt ab diesem Zeitpunkt eine andere. In jenen Tagen jagte eine Krisensitzung die andere, das Handy klingelte pausenlos, im engen, historischen Gemeindehaus gaben sich IT-Experten und Kantonsvertreter die Türklinke in die Hand. Irgendwann konnte Pugnale nicht mehr. Sie wollte im Flur etwas Luft schnappen und stiess dort auf eine Anwohnerin. «Sie sehen müde aus», sagte diese zu ihr. «Halten Sie durch – wir stehen hinter Ihnen!» Für Pugnale war es die «ausgestreckte Hand, die ich brauchte», wie sie heute im Sitzungszimmer erzählt, das während Wochen als Krisenzentrum diente.

Der Cyberangriff im vergangenen Jahr hat Rolle landesweit bekannt gemacht. Der Fall zeigt, wie rasch eine Behörde Opfer von Cyberkriminellen wird – und monatelang mit den Folgen kämpft. Das kann jeder Gemeinde, jeder Schule, jedem Spital in der Schweiz passieren. Und Rolle hatte noch Glück.

Die Attacke zeigt auch, wie wichtig eine transparente Kommunikation ist. Denn im Falle von Rolle hat dieses Versäumnis die Krise noch verschärft. Und vermutlich sind viele andere Organisationen ebenso wenig auf einen Cyberangriff vorbereitet, wie Rolle es war.

Dabei gibt es durchaus Möglichkeiten, sich auf einen Cyberangriff vorzubereiten. Es lohnt sich deshalb, den Fall von Rolle nochmals aufzurollen und vom Anfang bis zum Ende zu erzählen.

Der Angriff

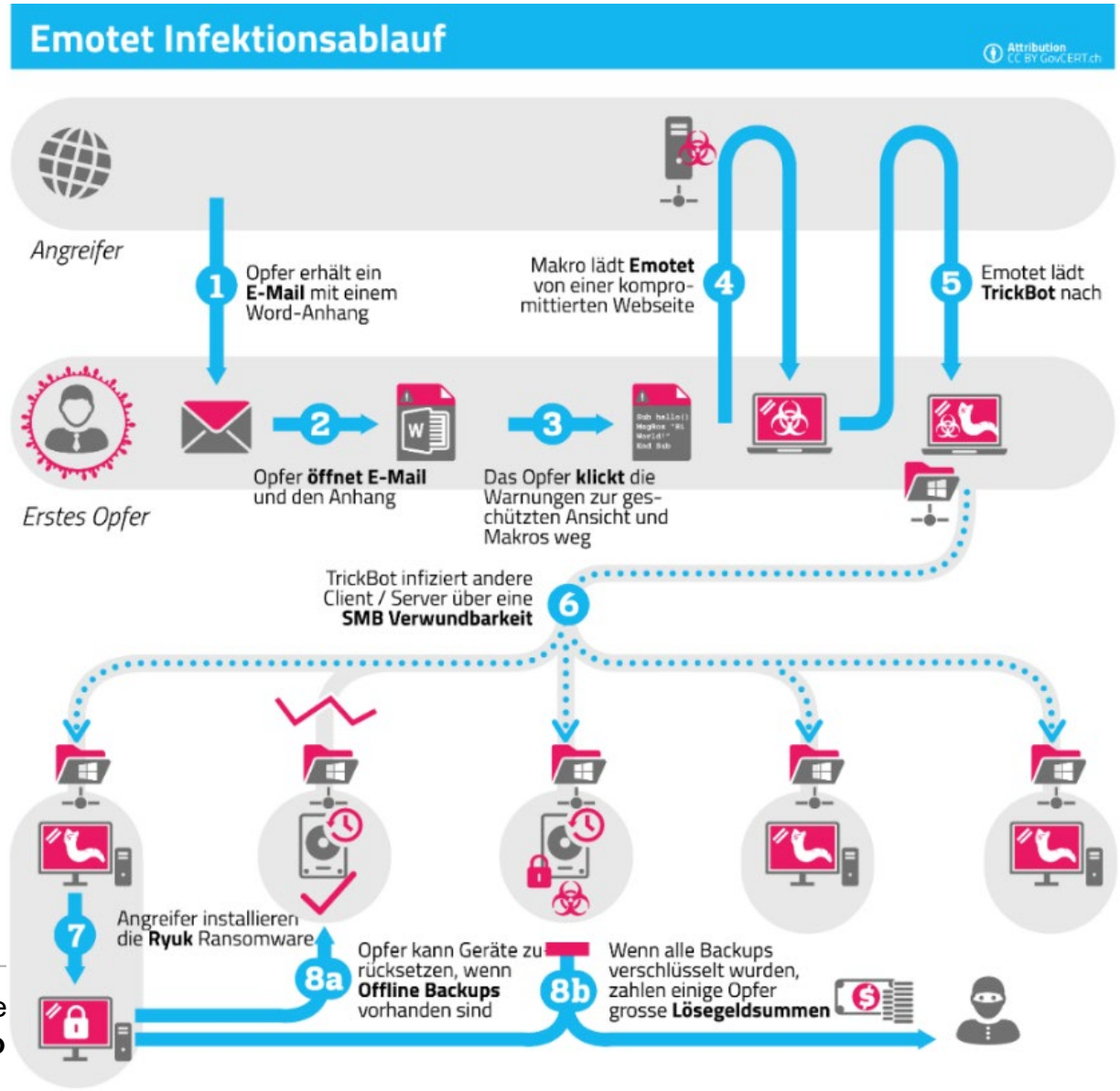
Die erste Welle des Tsunamis trifft Rolle am 30. Mai 2021. Es ist am frühen Sonntagmorgen, als ein Mitarbeiter der externen IT-Firma die Warnung bekommt. Ein Back-up-Server der Gemeindeverwaltung Rolle, für welche die IT-Firma die Informatikinfrastruktur betreibt, hat ein technisches Problem. Als die Firma der Ursache nachgeht, wird bald klar: Rolle ist Opfer eines Cyberangriffs geworden. In der Nacht haben Cyberkriminelle die IT-Systeme verschlüsselt und damit unbrauchbar gemacht. Sie verlangen ein Lösegeld.

Kurz darauf erfährt auch Marielle Vontobel vom Vorfall. Sie ist in der Gemeindeverwaltung seit Jahren zuständig für die Finanzen und die Informatik. Der Informatiker meldet ihr, dass es ein Problem gebe. An eine Hackerattacke dachte sie im ersten Moment nicht. «Ich bin keine Informatikspezialistin», sagt Vontobel heute. Sie wird in den folgenden Tagen rasch lernen, was ein Ransomware-Angriff ist.

In den letzten Jahren hat sich Ransomware zu einem globalen kriminellen Geschäft entwickelt, das Milliardenschäden verursacht. Bei dieser Art von Angriffen dringen die Kriminellen in ein Computernetzwerk ein, stehlen die Daten des Opfers und verschlüsseln die Rechner, um sie unbrauchbar zu machen. Zur Entschlüsselung fordern die Angreifer ein Lösegeld. Zudem drohen sie damit, die entwendeten Daten im Darknet zu veröffentlichen, falls das Opfer nicht bezahlt.

Rolle ist eine kleine Gemeinde mit gut 6000 Einwohnern. Die Gemeindeverwaltung hat 58 Mitarbeiter, das Budget ist begrenzt. Als klar wird, dass die Gemeinde Opfer einer kriminellen Attacke geworden ist, benötigt sie Hilfe. Sie wendet sich an das Nationale Zentrum für Cybersicherheit des Bundes (NCSC), das mit Ratschlägen und dem Kontakt zu einer

Ransomware / Encryption-Malware



Great damage to the point of bankruptcy of a company!

Not only data is being encrypted, but data is also being stolen and threatened with publication in order to lend force to the extortion

Ransomware

2020: 66 gemeldete Fälle
10 von Privatpersonen
56 von Firmen, Verwaltung und Vereinen

2021: 161 gemeldete Fälle
48 von Privatpersonen
113 von Firmen, Verwaltung und Vereinen

2022: 102 gemeldete Fälle
40 von Privatpersonen
62 von Firmen, Verwaltung und Vereinen

Stand 01.09.2022

Woche 25: Zunahme von Meldungen zu Vorfällen mit Verschlüsselungstrojanern (Ransomware)

28.06.2022 - Der Meldeeingang beim NCSC war letzte Woche wieder hoch. Acht Meldungen zu Verschlüsselungstrojanern sogenannte Ransomware rufen in Erinnerung, wie wichtig Vorsichtsmassnahmen zum Schutz vor solchen Angriffen sind.

Ransomware – Vorsorge ist wichtig

Nach fünf Wochen mit einer eher tiefen Zahl an gemeldeten Ransomware-Vorfällen wurden dem Nationalen Zentrum für Cybersicherheti NCSC in der letzten Woche gleich acht Fälle gemeldet. Das erstaunliche: Praktisch hinter jedem Fall steckte eine andere Schadsoftware. So hat das NCSC Meldungen zu Sodinokibi, Lockbit 2.0, Conti, Black.Basta und Deadbolt erhalten.

Grafik 4 - NCSC.ch: Meldungen pro Woche in der Kategorie: Ransomware

Fake-Sextortion

Von: Farrah Jones <farrah.jones@aqkw.cia-gov-int.ga>
Gesendet: Montag, 18. März 2019 03:13
An: [redacted]
Betreff: Central Intelligence Agency - Case #48623971

Case #48623971

Distribution and storage of pornographic electronic materials involving underage children.

My name is Farrah Jones and I am a technical collection officer working for Central Intelligence Agency.

It has come to my attention that your personal details including your email address ([redacted]) are listed in case #48623971.

The following details are listed in the document's attachment:

- Your personal details,
- Home address,
- Work address,
- List of relatives and their contact information.

hans.muster@example.com [mailto:hans.muster@example.com] 04:34

Sicherheitsalarm. Hacker kennen Ihr Passwort: password123

To: password123

Ich habe schlechte Nachrichten für dich.
08.10.2018 - an diesem Tag habe ich Ihr Betriebssystem gehackt und vollen Zugriff auf Ihr Konto erhalten hans.muster@example.com.
An diesem Tag lautete Ihr Kontopasswort (hans.muster@example.com): password123

Wie war es:
In der Software des Routers, mit der Sie an diesem Tag verbunden waren, gab es eine Sicherheitsanfälligkeit.
Ich habe diesen Router zuerst gehackt und meinen bösartigen Code darauf abgelegt.
Bei der Eingabe im Internet wurde mein Trojaner auf dem Betriebssystem Ihres Geräts installiert.

Danach habe ich alle Daten auf Ihrer Festplatte gespeichert (ich habe Ihr gesamtes Adressbuch, den Verlauf der angezeigten Websites, alle Dateien, Telefonnummern und Adressen aller Ihrer Kontakte).

Ich wollte dein Gerät sperren. Und benötigen Sie eine kleine Menge Geld für das Entsperren.
Aber ich habe mir die Websites angesehen, die Sie regelmäßig besuchen, und kam zu dem großen Schock Ihrer Lieblingsressourcen.
Ich spreche von Websites für Erwachsene.

Ich möchte sagen - du bist ein großer Perverser. Sie haben ungezügelte Fantasie!

Danach kam mir eine Idee in den Sinn.
Ich habe einen Screenshot der intimen Website gemacht, auf der Sie Spaß haben (Sie wissen, worum es geht, oder?).
Danach nahm ich Ihre Freuden ab (mit der Kamera Ihres Geräts). Es stellte sich wunderbar heraus, zögern Sie nicht.

Ich bin fest davon überzeugt, dass Sie diese Bilder Ihren Verwandten, Freunden oder Kollegen nicht zeigen möchten.
Ich denke, 317€ sind ein sehr kleiner Betrag für mein Schweigen.
Außerdem habe ich viel Zeit mit dir verbracht!

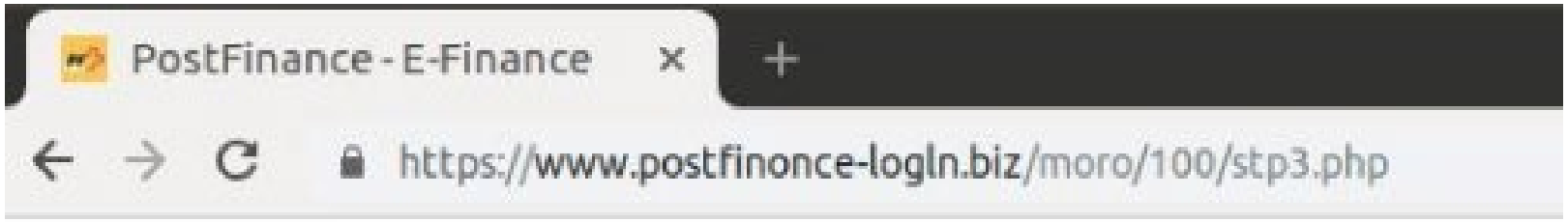
Ich akzeptiere nur Bitcoins.
Meine BTC-Geldbörse: 1Dvd7Wb72JBTbAcfTrxSJCZZuf4tsT8V72

Sie wissen nicht, wie Sie die Bitcoins senden sollen?
Schreiben Sie in einer Suchmaschine "wie Sie Geld an die BTC-Geldbörse senden".
Es ist einfacher als Geld an eine Kreditkarte zu senden!

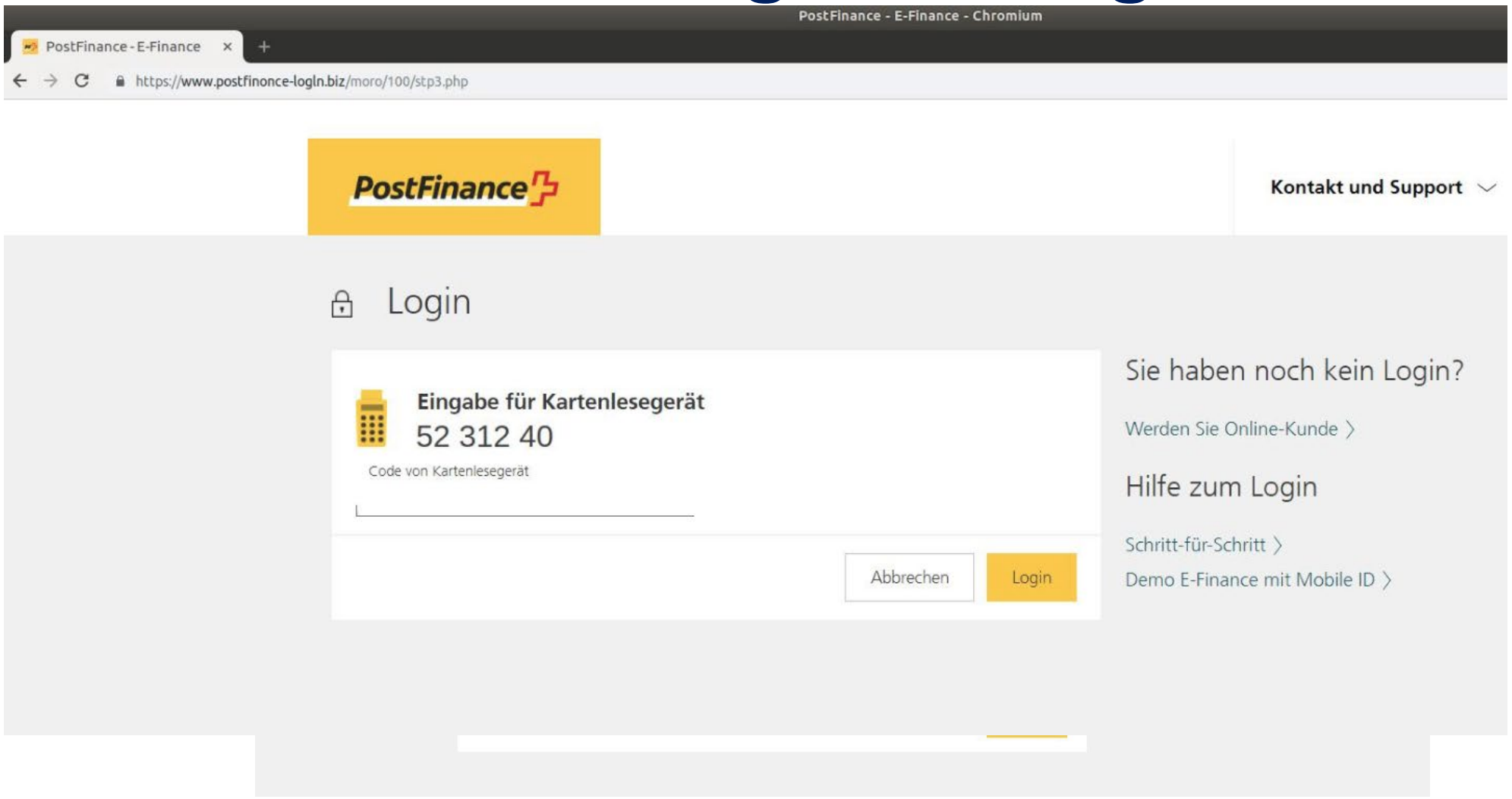
Für die Bezahlung gebe ich Ihnen etwas mehr als zwei Tage (genau 50 Stunden).
Keine Sorge, der Timer startet in dem Moment, in dem Sie diesen Brief öffnen.
Ja, ja .. es hat schon angefangen!

Real-Time e-Banking Phishing

- Mit Real-Time Phishing versuchen Betrüger, Zwei-Faktor Authentisierung und Transaktionssignierungen zu umgehen
- Täterschaft versendet Phishing-Mails im Namen der Bank
- E-Mail enthält einen Link zu einer Phishing-Webseite
- **Nach Eingabe der Zugangsdaten versucht Täterschaft in Echtzeit eine Zahlung auszulösen (während das Opfer noch auf der Phishing-Webseite ist)**



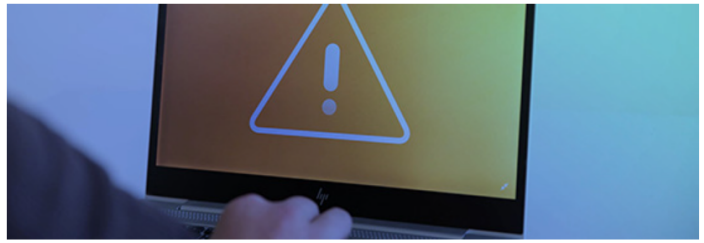
Real-Time eBanking Phishing



Warnungen

MS Exchange-Lücken werden noch immer nicht geschlossen

16.05.2022 - Erneut hat das NCSC über 200 Unternehmen mittels eingeschriebenem Brief über verwundbare Microsoft Exchange-Server informiert und gewarnt. Die Sicherheitslücken sind seit Langem bekannt und werden von Cyberkriminellen aktiv ausgenutzt.



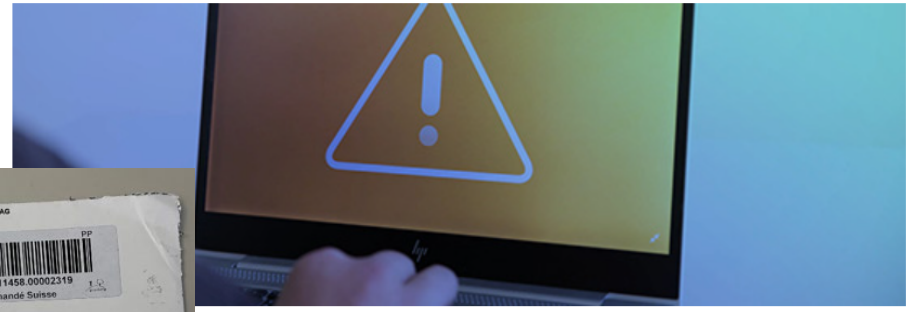
Die Sicherheitslücken bei Microsoft Exchange-Servern sind schon seit einem Jahr bekannt und Patches sind längst verfügbar. Dennoch gibt immer noch zahlreiche Systeme, die verwundbar sind.

Warnung mittels eingeschriebenem Brief

Aus diesem Grund hat das NCSC am Wochenende erneut über 200 Unternehmen und einzelne Gemeinden mit einem eingeschriebenen informiert und vor der Sicherheitslücke gewarnt. An wen die Briefe v wurden, wird vom NCSC aus Sicherheitsgründen nicht bekannt gegel Einige der Unternehmen haben die seit Langem bekannte Sicherheit immer noch nicht gepatcht. Es sind aber auch Unternehmen darunte bereits vor einiger Zeit durch das NCSC informiert worden sind, reagi haben, und die Sicherheits-Updates damals eingespielt haben. Jedoc sie seither keine Patches mehr installiert. Da in der Zwischenzeit neue Sicherheitslücken aufgetaucht sind, sind ihre Systeme wieder verwun und somit potenziell angreifbar.

Wenn Warnungen des Bundes verpuffen

28.04.2022 - Immer wieder kommt es vor, dass adressierte Warnungen des Bundes zu konkreten, akuten Cyberbedrohungen leider ins Leere laufen. Dies führt dazu, dass sich Unternehmen aber auch Privatpersonen unnötigen Gefahren im Cyberraum aussetzen – oftmals mit verheerenden Folgen, wie ein Fall kürzlich gezeigt hat.

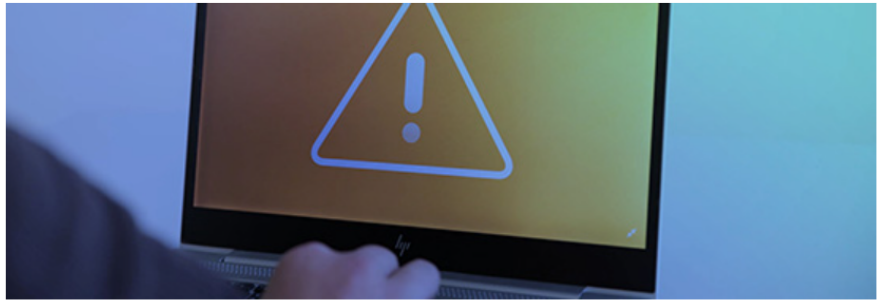


miert und warnt regelmässig öffentlich zu aktuellen gen auf seinen Kanälen, wie Twitter, LinkedIn oder auf der . Ein Grossteil der Warnungen betrifft jedoch nicht die ganze ondern bestimmte Unternehmen. In diesem Fall informiert etroffene Unternehmen direkt per E-Mail, per Telefon und a eingeschriebenen Brief. In vielen Fällen konnten so Lücken hlossen und eine Verschlüsselung und ein Datenabfluss den.

Ukraine

Das NCSC verzeichnet aktuell keinen Anstieg von Cyberangriffen auf die Schweiz

25.02.2021 - Aufgrund der aktuellen Berichterstattung zu möglichen Cyberrisiken im Zusammenhang mit dem Ukraine-Konflikt veröffentlicht das Nationale Zentrum für Cybersicherheit eine Einschätzung zur Cyberlage in der Schweiz. Aktuell sieht das NCSC keine Intensivierung von bedrohlichen Aktivitäten im Cyberraum, die die Schweiz direkt betreffen würden.

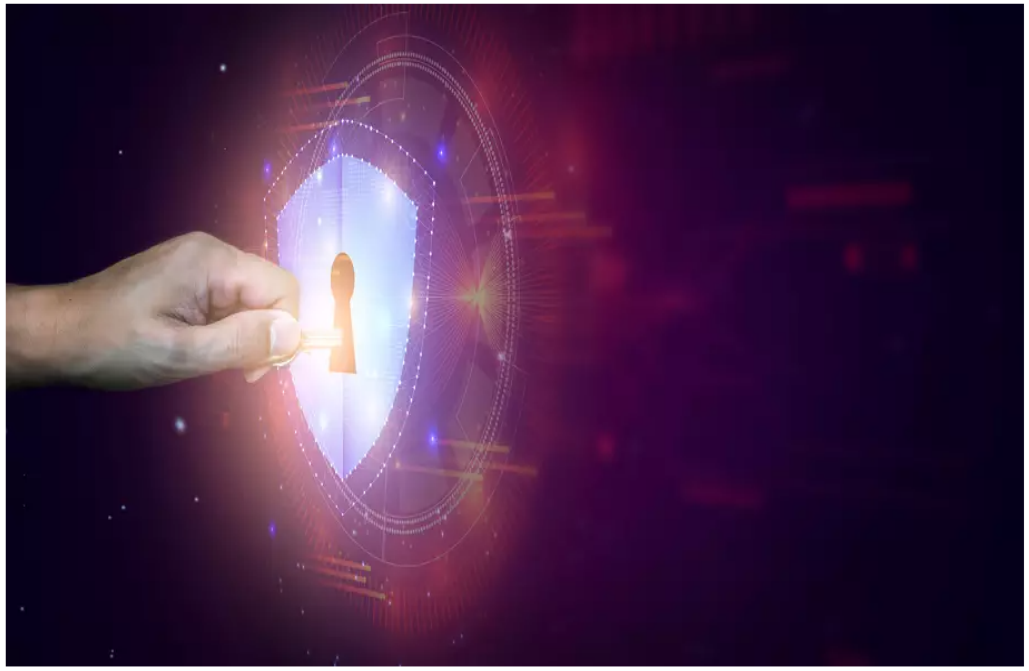


Der Nachrichtendienst des Bundes (NDB) verfolgt und analysiert laufend die aktuelle Cyberbedrohungslage und steht diesbezüglich in engem Kontakt mit dem Nationalen Zentrum für Cybersicherheit (NCSC) sowie internationalen Partnern.

Cybergang Conti: Interne Daten geleakt - 2,8 Milliarden US-Dollar erbeutet

Nachdem die Cybergang Conti sich im Ukraine-Konflikt auf russische Seite stellte, veröffentlichte ein Mitglied interne Chats und Daten der vergangenen Jahre.

Lesezeit: **4 Min.** In Pocket speichern 83



(Bild: Rinrada_Tan/Shutterstock.com)

DAS NATIONALE ZENTRUM FÜR CYBERSICHERHEIT NCSC

Nationales Zentrum für Cybersicherheit

Rechtliche Grundlage:

Die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV)


120.73

Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung

(Cyberrisikenverordnung, CyRV)

vom 27. Mai 2020 (Stand am 1. April 2021)

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Gegenstand

Art. 2 Geltungsbereich

Art. 3 Begriffe

Mitarbeitende:

50 Mitarbeitende (Voll- oder Teilzeitpensum)
(Stand 10.2022)

Auftrag:

Die Wirtschaft, Bildungseinrichtungen und die Verwaltung beim Schutz vor Cyberrisiken zu unterstützen und die Sicherheit der eigenen Systeme zu verbessern

NCS Strategie:

Verantwortlich für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018-2022

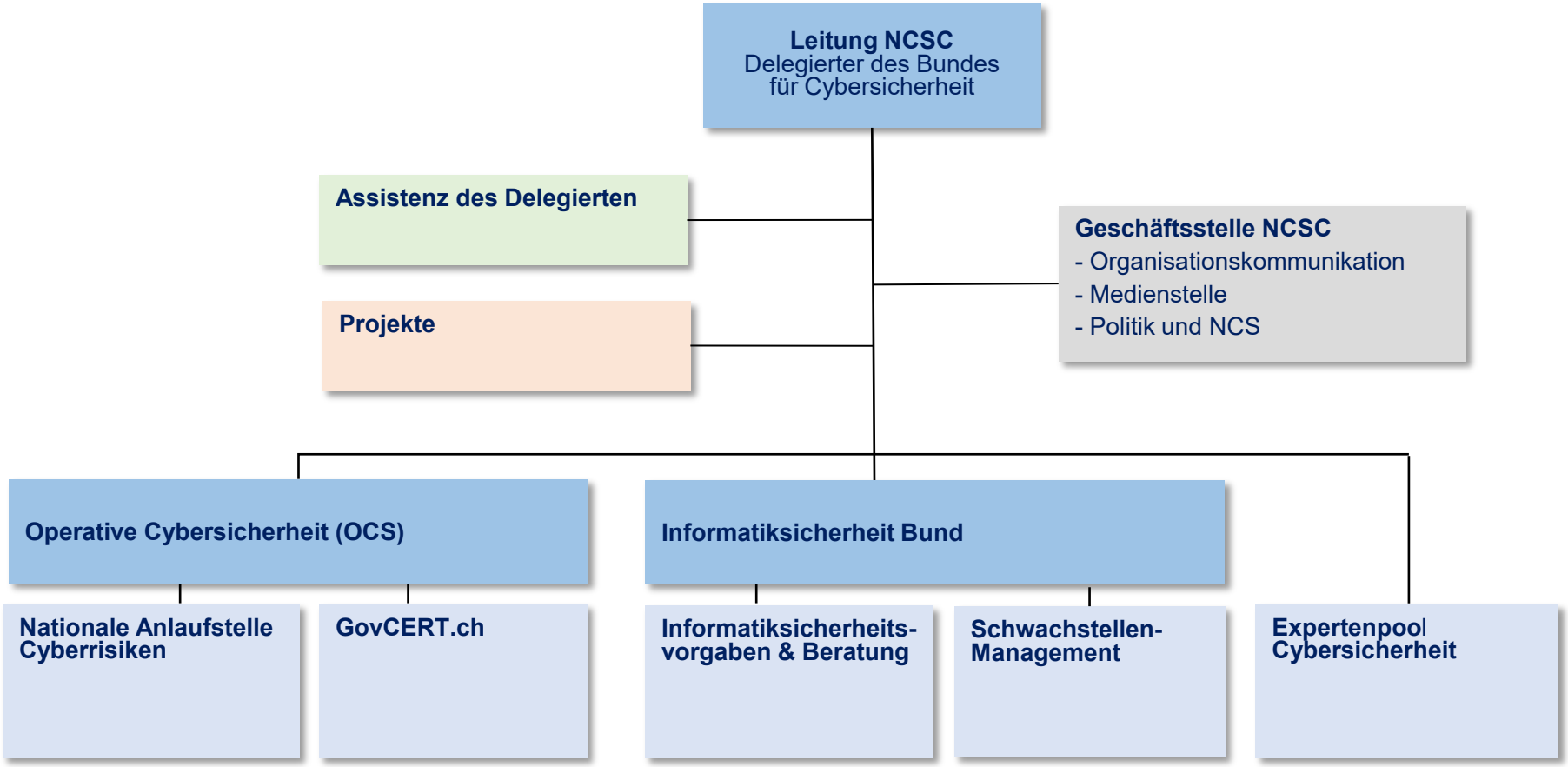
Leiter:

Der Delegierte des Bundes für Cybersicherheit
Florian Schütz

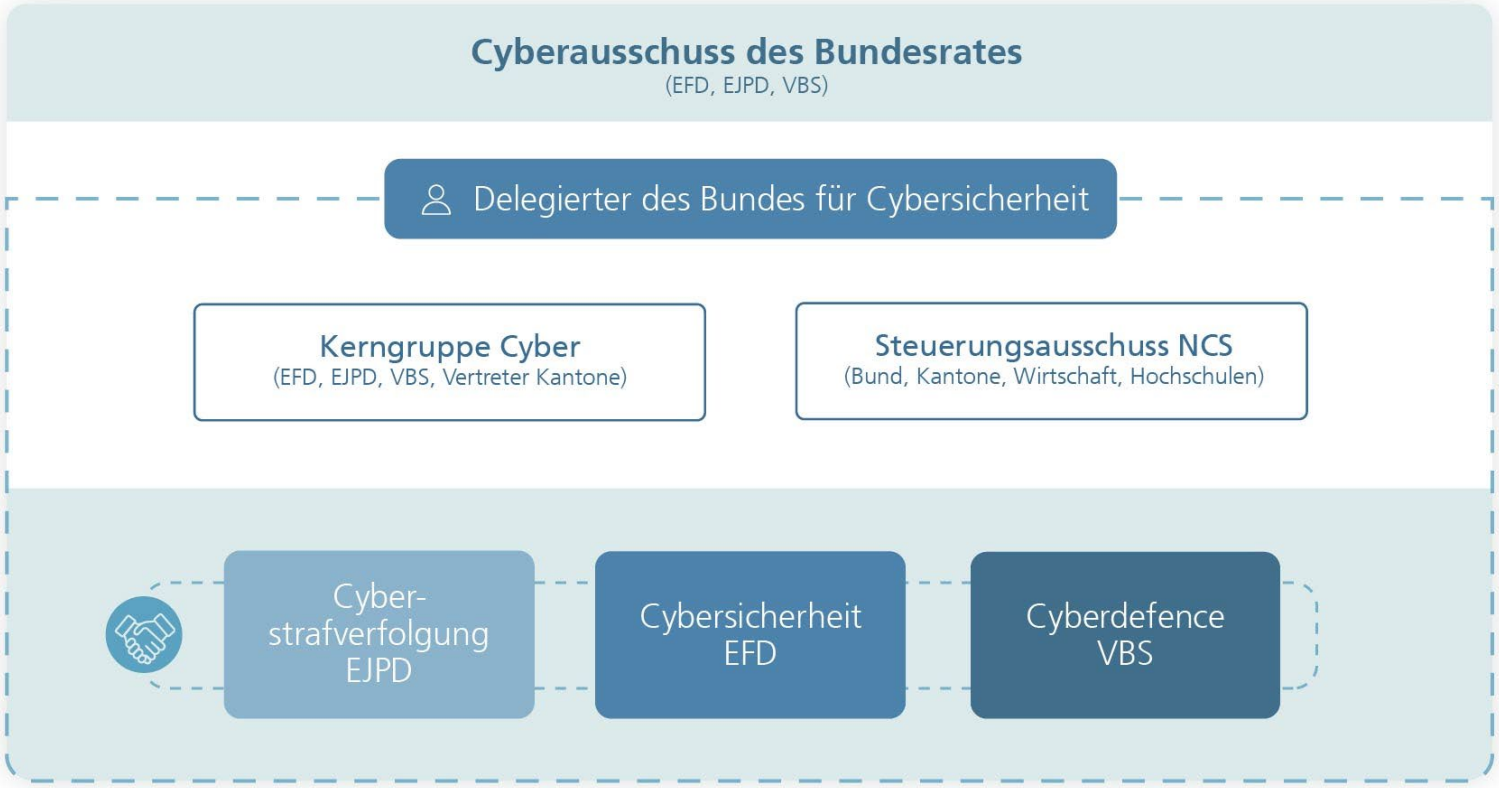
Meldeformular:

Für Cybervorfälle
www.ncsc.admin.ch

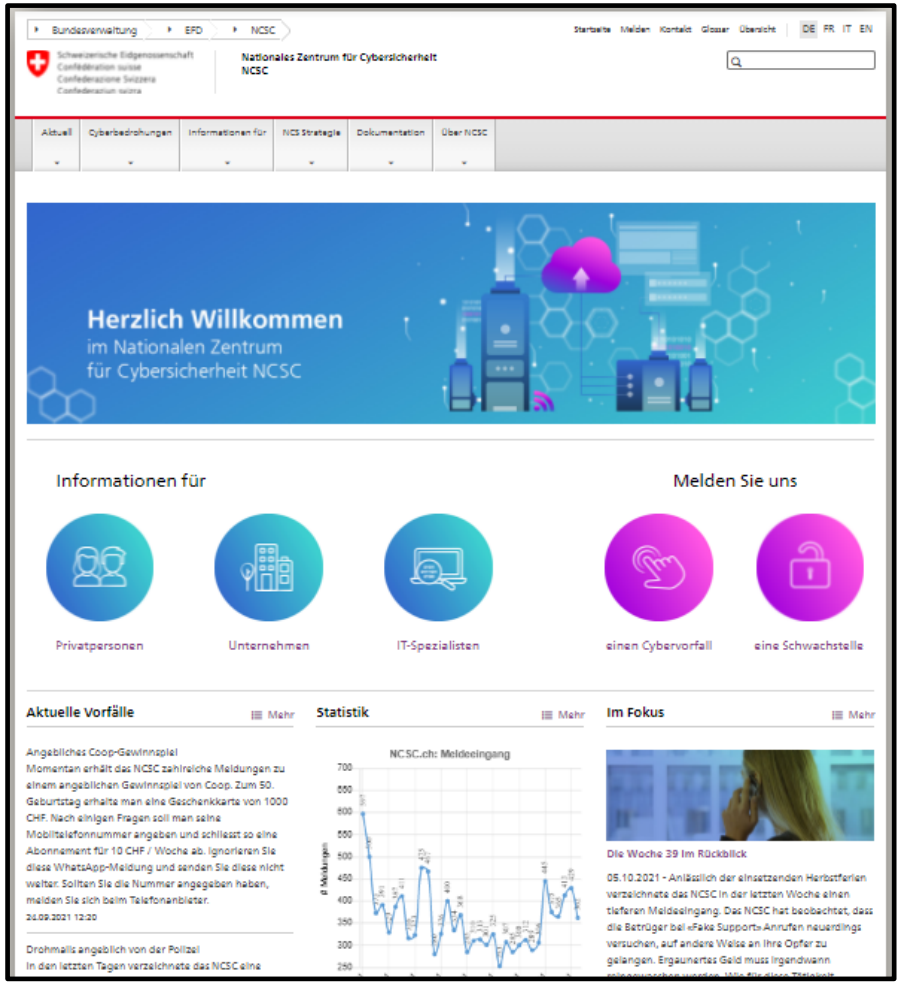
Organigramm NCSC



Organisation des Bundes im Bereich Cyberrisiken



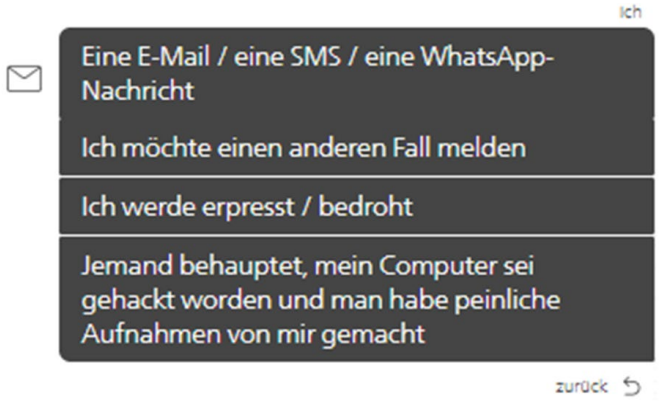
Dienstleistungen des NCSC



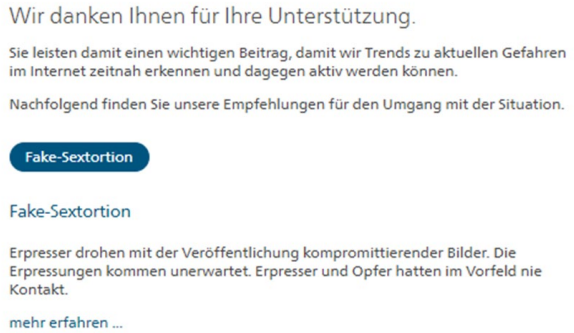
- Generelle Informationen / Trends
- Warnungen zu laufenden Angriffen
- Aktuelle Statistik
- Regelmässige Informationen zu aktuellen Vorfällen
- Halbjahresberichte
- Meldeformular
- Erste-Hilfe Dokumente bei den häufigsten Vorfällen
- IKT-Minimalstandard
- IKT-Branchenstandard
- Exklusive Dienstleistungen für kritische Infrastrukturen

Interaktives Meldeformular

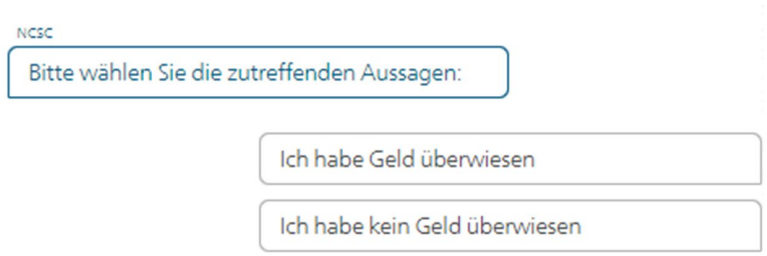
Wenige kurze Fragen führen rasch zur Lösung



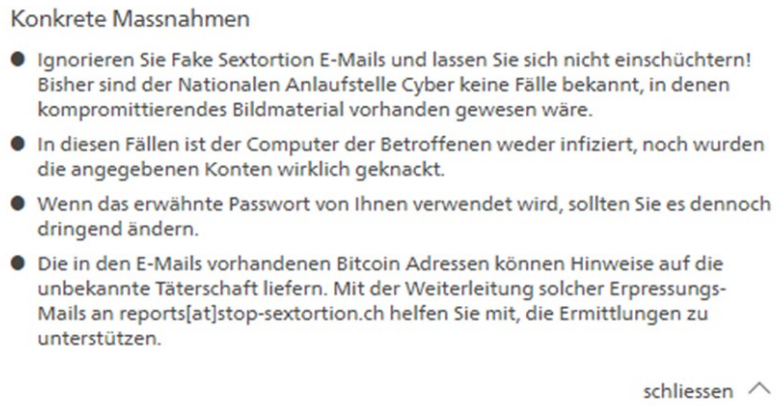
Über 90% Trefferquote



Schaden oder nur Meldung?



Soforthilfe und präventive Massnahmen



Aktuell

Nationale Cyberstrategie: Umsetzung verläuft erfolgreich und wird weiter gestärkt

Bern, 18.05.2022 - Der Bundesrat hat am 18. Mai 2022 den Bericht zur Wirksamkeitsüberprüfung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022» zur Kenntnis genommen und beschlossen, für den Schutz vor Cyberrisiken weitere 25 Stellen zu schaffen.

Die Umsetzung der aktuellen nationalen Cyberstrategie wird Ende 2022 abgeschlossen. Bis dahin wird die Strategie erneuert und auf die aktuelle Bedrohungslage ausgerichtet. Grundlage für diese Arbeiten bildet die Überprüfung der Wirksamkeit der aktuellen Strategie. Diese hat im zweiten Halbjahr 2021 stattgefunden.

Positives Fazit zur Strategieumsetzung

Die Strategie und deren bisherige Umsetzung wurde durch externe Gutachter auf ihre Wirksamkeit überprüft. Das Fazit ist insgesamt positiv. Die Umsetzung verläuft planmässig und hat zu entscheidenden Resultaten geführt: So wurden beispielsweise gemeinsam mit den Hochschulen Standards und Labels entwickelt, welche Organisationen helfen, ihre Cybersicherheit systematisch zu prüfen und zu verbessern. Mit der Schaffung des Nationalen Testzentrums für Cybersicherheit in Zug werden in der Schweiz Fähigkeiten aufgebaut, IT-Produkte vertieft zu analysieren und mit der Vorlage zur Einführung einer Meldepflicht hat der Bund auch einen Vorschlag erarbeitet, wie die Cybersicherheit durch regulative Massnahmen verbessert werden kann. Ein wesentlicher Faktor für die erfolgreiche Erarbeitung und Umsetzung der NCS ist die breite Einbindung von Akteuren aus den Kantonen, der Wirtschaft und der Hochschulen.

Das Nationale Zentrum für Cybersicherheit soll ein Bundesamt werden

Bern, 18.05.2022 - Der Bundesrat hat an seiner Sitzung vom 18. Mai 2022 beschlossen, das Nationale Zentrum für Cybersicherheit (NCSC) in ein Bundesamt zu überführen. Er hat das Eidgenössische Finanzdepartement EFD beauftragt, bis Ende 2022 Vorschläge auszuarbeiten, wie das Amt ausgestaltet und in welchem Departement es angesiedelt werden soll.

Die Bedeutung der Cybersicherheit hat in den vergangenen Jahren auf allen Ebenen stark zugenommen. Der Bundesrat hat bereits 2019 mit der Schaffung des NCSC, das im Generalsekretariat des EFD angesiedelt ist, einen wichtigen Grundstein gelegt. Seither hat sich das NCSC stark weiterentwickelt. Neben dem Ausbau der technischen Fachstelle, dem GovCERT, wurde eine Anlaufstelle für Meldungen von Cybervorfällen aus der Bevölkerung und Wirtschaft aufgebaut sowie ein Schwachstellen-Management etabliert. Mit rund 40 Mitarbeitenden nimmt das NCSC Kernaufgaben beim Schutz der Schweiz vor Cyberbedrohungen wahr. Es unterstützt Betreiber kritischer Infrastrukturen bei der Prävention und bei der Bewältigung von Vorfällen, betreibt die nationale Anlaufstelle für Fragen zur Cybersicherheit für Bevölkerung und Wirtschaft und ist vom Bundesrat als zentrale Meldestelle bei der Einführung der Meldepflicht für Cyberangriffe vorgesehen.

Bundesverwaltung beschafft Plattform für Bug Bounty-Programme

Bern, 03.08.2022 - Um die Cybersicherheit der IT-Infrastruktur zu erhöhen sowie Cyberrisiken effektiv und kosteneffizient zu senken, beschafft der Bund eine zentrale Plattform für Bug Bounty- Programme. Unter der Federführung des Nationalen Zentrums für Cybersicherheit NCSC und in Zusammenarbeit mit Bug Bounty Switzerland AG werden ethische Hacker künftig die IT-Systeme der Bundesverwaltung nach Schwachstellen durchsuchen.

Sicherheitslücken in IT-Systemen gehören zu den häufigsten Einfallstoren bei Cyberangriffen. Umso wichtiger ist es, Schwachstellen so rasch als möglich zu entdecken und zu schliessen. Denn haben Angreifer durch eine Lücke in der Webseite oder in einer Software-Komponente ins System hineingefunden, können sie sich darin potenziell auch ausbreiten und weiteren Schaden anrichten. Standardisierte Sicherheitstests reichen heute häufig nicht mehr aus, um die versteckten Lücken zu finden. Daher sollen in Zukunft ethische Hacker im Rahmen von sogenannten Bug Bounty-Programmen die produktiven IT-Systeme und Applikationen der Bundesverwaltung nach Schwachstellen durchsuchen.

Strategische Ziele NCSC ab 2023

Erarbeitung der Strategie in Zusammenarbeit mit Kantonen, Wirtschaft und Hochschulen

Vier Strategische Ziele:

1. Selbstbefähigung
2. Sichere und verfügbare digitale Dienstleistungen und Infrastruktur
3. Effektive Abwehr von Cyberangriffen und Ahndung der Verursacher
4. Führende Rolle in der internationalen Zusammenarbeit

WHAT’S NEXT?

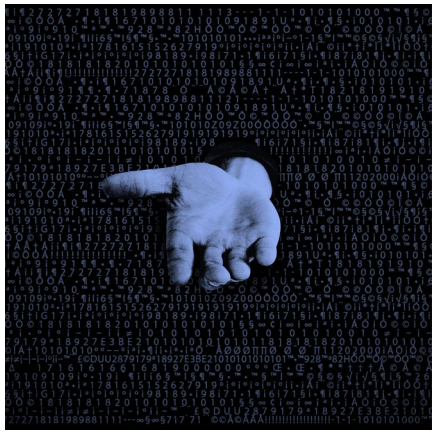
Globale Trends

Ransomware

DDoS

Daten-Diebstahl

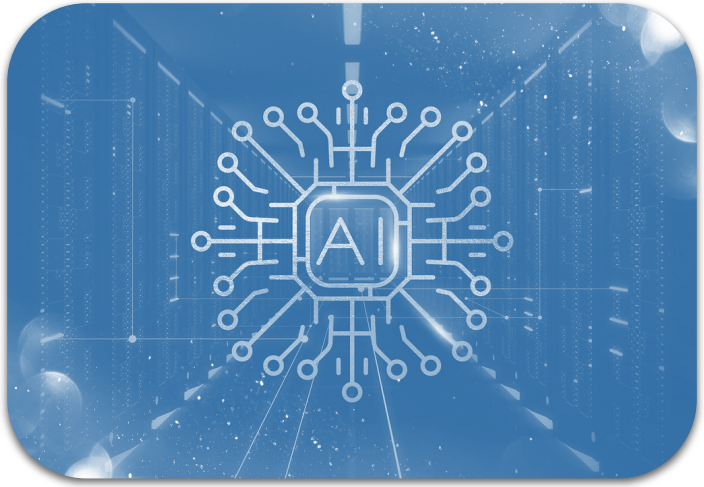
Erpressung



Spionage

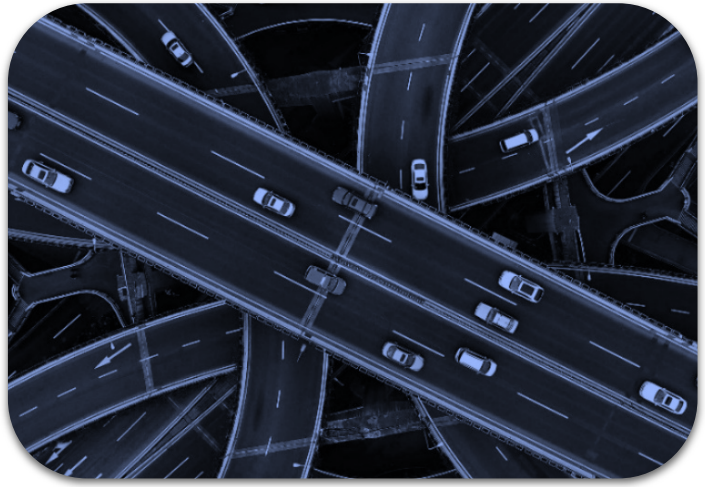
Dienstleister

What is next?



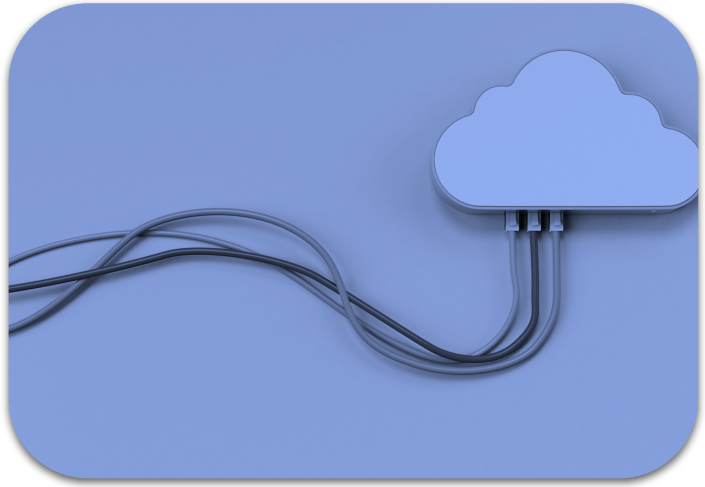
AI (Trainingdata/Entscheidung)

Soziale Netzwerke (Desinformation)



Physische Objekte für Cyberangriffe verwenden (z. B. Verkehrsschilder)

Schallwellen werden als Cyberangriff genutzt (z.B. Übertragung im Ultraschallband)



Immer mehr Produkte werden mit Konnektivität ausgestattet (z. B. Internet der Dinge, 5G), wodurch ehemals analoge Geräte nun anfällig werden

Neue Technologien und gesellschaftliche Veränderungen erweitern die Angriffsfläche für Angriffe

EINIGE TIPPS

Bitte beachten

Aktualisierungen / Updates

- Aktivieren Sie automatische Systemaktualisierungen auf Ihren Geräten
- Stellen Sie sicher, dass Ihr Webbrowser automatische Sicherheitsupdates verwendet

Anti-Virus-Schutz & Firewall

- Windows und Mac OS X Firewalls aktivieren
- Verwenden Sie stets aktuelle Antiviren-Software

Passwortverwaltung

- Verwenden Sie nach Möglichkeit eine Zwei-Faktor- oder Multi-Faktor-Authentifizierung
- Verwenden Sie nur sichere Passwörter
- Verwenden Sie einen Passwort-Manager

Phishing und Betrug

- Öffnen Sie keine E-Mails von Personen, die Sie nicht kennen
- Bewegen Sie den Mauszeiger über einen Link, um zu erfahren, wohin er führt
- Bösartige Links/Mails können auch von bekannten Kontakten stammen, die ebenfalls infiziert wurden

Bitte beachten

Schützen Sie Ihre persönlichen Informationen	Überprüfen Sie Ihre Datenschutzeinstellungen für alle Ihre Konten in den Social Media Apps
Sichere Nutzung Ihrer mobilen Geräte	Erstellen Sie einen schwierigen mobilen Passcode und verwenden Sie biometrische Authentifizierung (z.B. FaceID) Installieren Sie Anwendungen nur aus vertrauenswürdigen Quellen
Regelmäßige Sicherung Ihrer Daten	Bewahren Sie drei Kopien Ihrer Daten auf zwei verschiedenen Datenträgern (lokale und externe Festplatte) und eine Kopie an einem externen Speicherort (Cloud-Speicher) auf.
Öffentliches Wi-Fi	Benutzen Sie kein öffentliches Wi-Fi, ohne ein virtuelles privates Netzwerk (VPN) zu verwenden
Überprüfen Sie Ihre Online-Konten	Mindestens einmal im Monat auf unbekannte Transaktionen und Muster prüfen Aktivieren Sie Transaktionsbenachrichtigungen (SMS/App)

Der Schutz der Schweiz vor Cyberrisiken ist eine gemeinsame Aufgabe von Gesellschaft, Wirtschaft und Staat

Besten Dank für Ihre Aufmerksamkeit

Daniel Seiler
IT-Projektleiter Cybersicherheit

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC