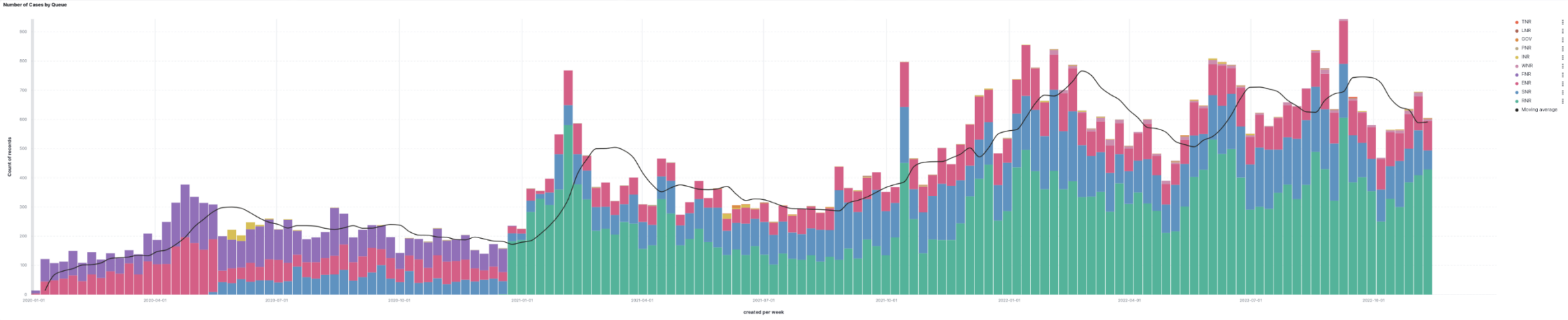
Die aktuelle Cyberbedrohungslage

Pascal Lamia, Stv. des Delegierten für Cybersicherheit und Leiter der operativen Cybersicherheit, NCSC

2000 - 2007	Informatiksicherheitsbeauftragter des Bundes
2008 – 2020	Leiter der Melde- und Analysestelle Informationssicherung MELANI
seit Juni 2020	Stv. des Delegierten des Bundes für Cybersicherheit und Leiter der operativen Cybersicherheit im NCSC

Verlauf der Meldungen 2020 - 2022



rot - E-Mail

violett - altes Meldeformular

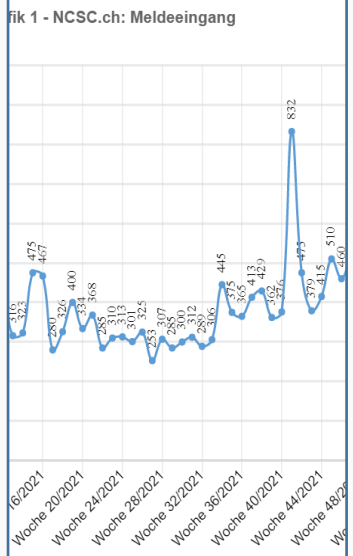
grün - neues Meldeformular

Was wird gemeldet
Meldungen 2020 - heute

Meldungen im Jahr 2022

34’527 Meldungen

davon
20950 Betrug
4487 Phishing
460 Hacking
410 Malware davon 159 Ransomware
39 Datenabfluss



2021
21714 Meldungen

Meldungen im Jahr 2023 (bis 15.2.23)

4820 Meldungen

davon
2931 Betrug
906 Phishing
55 Hacking
39 Malware davon 20 Ransomware
7 Datenabfluss

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!

Fake-Extortion

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

POLICE.CH

CYBERCRIMEPOLICE.CH
Ein Engagement Ihrer Polizei

STRUCTURES EN COLLABORATION FEDPOL – POLICE DE SURETE & GENDARMERIE – DEPARTEMENT FEDERAL DE JUSTICE ET POLICE

Madame, Monsieur

Nous engageons à votre encontre des poursuites judiciaires, peu après une saisie informatique de Cyber-infiltration, pour : **Pédopornographie, Pédophilie, Cyberpornographie, Exhibitionniste...**

Pour votre information, le Législateur a déclaré que, lorsque les crimes et délits envisagés par le Code pénal étaient réalisés grâce à un réseau de télécommunications, les peines pénales prévues seraient aggravées.

A l'issue de l'enquête, nous avons conclu que vous avez commis ces infractions, à savoir la détention, la visualisation, la transmission et la consultation d'images, de vidéos à caractère exhibitionniste, pédopornographique, au moyen d'internet lors de conversation entretenue avec des mineurs de moins de 16 ans.

Au cours de l'investigation, nous avons également observé que des messages érotiques et des scènes d'exhibition, de masturbation étaient pratiquées via des séances de webcam et de discussion instantanée.

Il faut rappeler que, lorsque des contenus obscènes sont exposés d'une telle sorte aux regards des mineurs de moins de 16 ans, cela constitue un délit d'exhibition sexuelle, de pédopornographie, de pédophilie, de cyberpornographie, ces crimes sont sévèrement punis par la Loi.

De nombreux éléments enregistrés par la Cyber-infiltration constituent les preuves considérables de vos infractions.

Veuillez envoyer vos justifications par mail, afin qu'elles puissent être mises en examen et vérifiées ; ceci dans un délai strict de 48 heures. Passé ce délai, nous serons contraints d'adresser notre rapport au Tribunal Judiciaire de votre Région, pour émettre un mandat d'arrêt à votre encontre, qui s'ensuivra d'une arrestation immédiate par la Police de sûreté la plus proche de votre domicile.

Vous serez ensuite fiché au registre national des délinquants sexuels. Dans cette situation, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias

*Veuillez adresser un e-mail à :

Email : infos.cybercriminalite@europolmail.org

NICOLETTA DELLA VALLE
DIRECTRICE DE FEDPOL

- Kontaktaufnahme via Mail
- Einschüchterungen
- In der Regel muss zwischen €3000 – €4000 bezahlt werden

⇒ Mails dem NCSC melden

⇒ Weitere Infos: https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/fake-extortion.html

Zunahme von DDoS Attacken

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

DDoS

KILLNET

Cyberangriffe auf Nato-Webseiten

Das Militärbündnis Nato bestätigte Angriffe auf seine Webseiten. Dahinter werden die pro-russischen Hacktivisten von Killnet vermutet.

in Pocket speichern | merken

13. Februar 2023, 9:42 Uhr, Moritz Tremmel

(Bild: Clker-Free-Vector-Images/Pixabay)

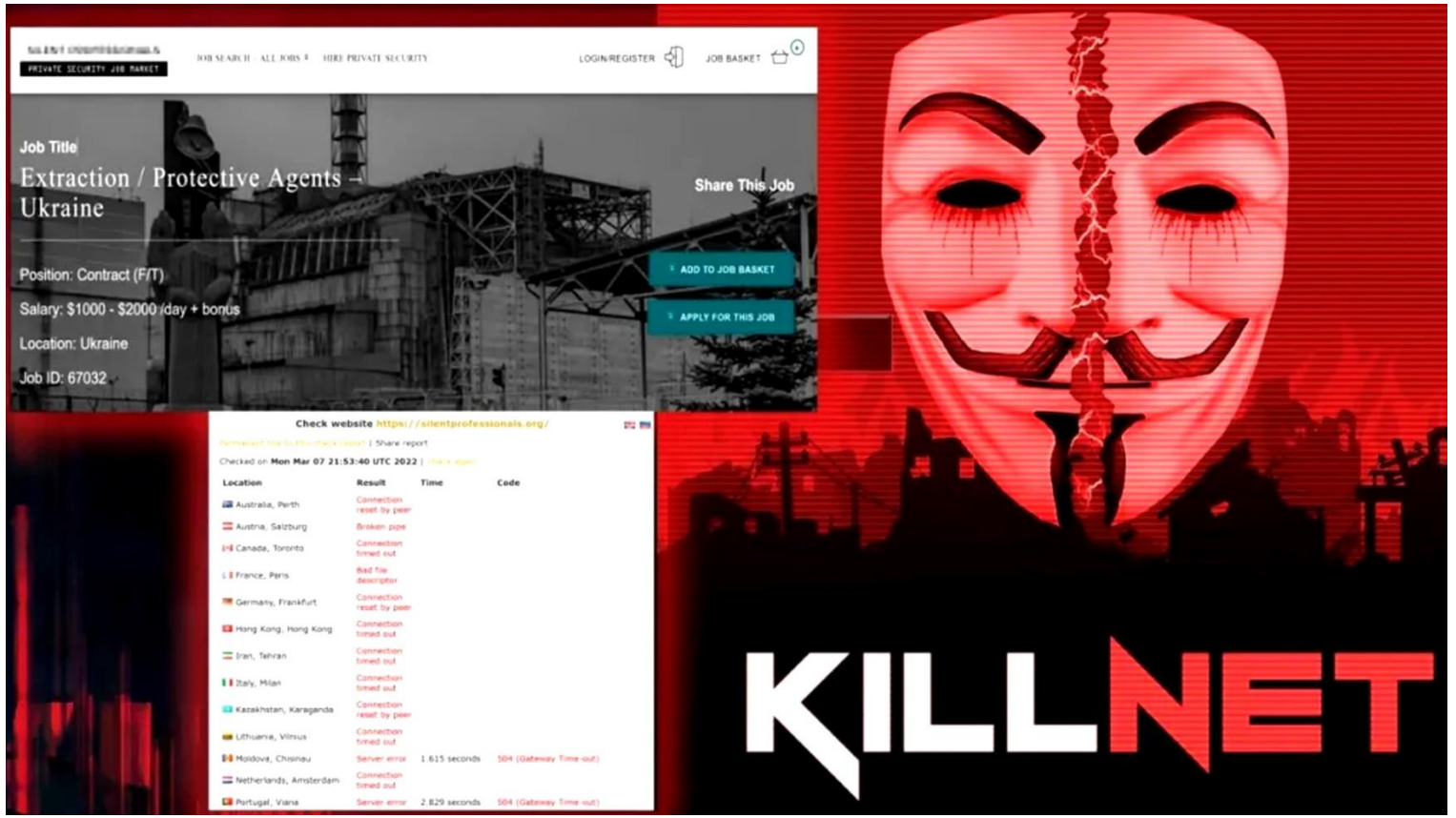
Das Logo des Militärbündnisses Nato

Am Sonntag sind die Webseiten des Militärbündnisses Nato Cyberangriffen ausgesetzt gewesen. Das bestätigte eine Sprecherin des Militärbündnisses der Deutschen Presse-Agentur (dpa). Cyberexperten des Verteidigungsbündnisses befassten sich aktiv mit dem Vorkommnis, erklärte die Sprecherin.

art, Stuttgart
ist (m/w/d)
sbaden, Berlin,

Twitter-Nutzer berichteten laut dpa, dass pro-russische Aktivisten unter anderem die Internetseite des Nato-Hauptquartiers für Spezialoperationen (NSHQ) attackierten. Die Webseite war zeitweise nicht zu erreichen. Wahrscheinlich handelt es sich um einen DDoS-Angriff (Distributed Denial of Service), bei dem die Server mit Anfragen überflutet werden, bis sie unter der Last zusammenbrechen.

Hinter dem Angriff wird die pro-russische Hacktivistengruppe Killnet vermutet, die immer wieder mit DDoS-Angriffen auf Webseiten und Infrastruktur auffällt. Sie wurde zuletzt unter anderem mit Angriffen auf die Internetpräsenzen des Bundestags, der Polizei und kritischer Infrastruktur in Deutschland in Verbindung gebracht.



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
ıes 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

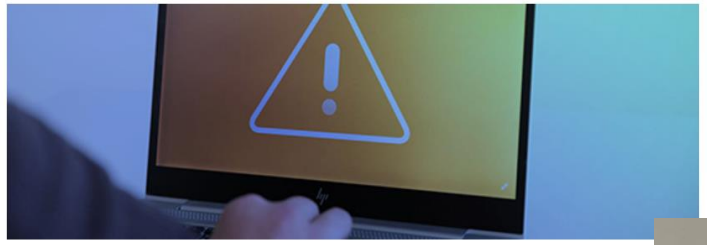
HEUTE, 07:49 GESUNDHEIT, SCHWEIZ
Relief-Übernahmeziel APR hat Studie mit Covid-Nasenspray gestartet

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

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.



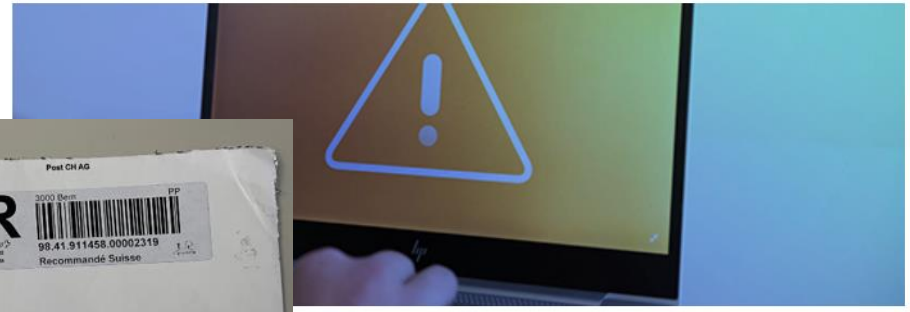
Die Sicherheitslücken bei Microsoft Exchange-Servern sind schon seit üb
einem Jahr bekannt und Patches sind längst verfügbar. Dennoch gibt es
immer noch zahlreiche Systeme, die verwundbar sind.

Warnung mittels eingeschriebenem Brief

Aus diesem Grund hat das NCSC am Wochenende erneut über 200
Unternehmen und einzelne Gemeinden mit einem eingeschriebenen Bri
informiert und vor der Sicherheitslücke gewarnt. An wen die Briefe verse
wurden, wird vom NCSC aus Sicherheitsgründen nicht bekannt gegeben
Einige der Unternehmen haben die seit Langem bekannte Sicherheitslüc
immer noch nicht gepatcht. Es sind aber auch Unternehmen darunter, di
bereits vor einiger Zeit durch das NCSC informiert worden sind, reagiert
haben, und die Sicherheits-Updates damals eingespielt haben. Jedoch ha
sie seither keine Patches mehr installiert. Da in der Zwischenzeit neue
Sicherheitslücken aufgetaucht sind, sind ihre Systeme wieder verwundba
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.

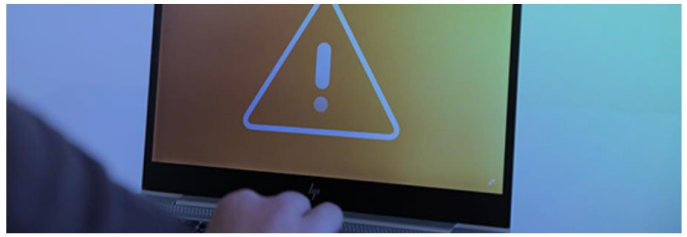


d warnt regelmässig öffentlich zu aktuellen
seinen Kanälen, wie Twitter, LinkedIn oder auf der
ssteil der Warnungen betrifft jedoch nicht die ganze
estimmte Unternehmen. In diesem Fall informiert
Unternehmen direkt per E-Mail, per Telefon und
hriebenen Brief. In vielen Fällen konnten so Lücken
und eine Verschlüsselung und ein Datenabfluss

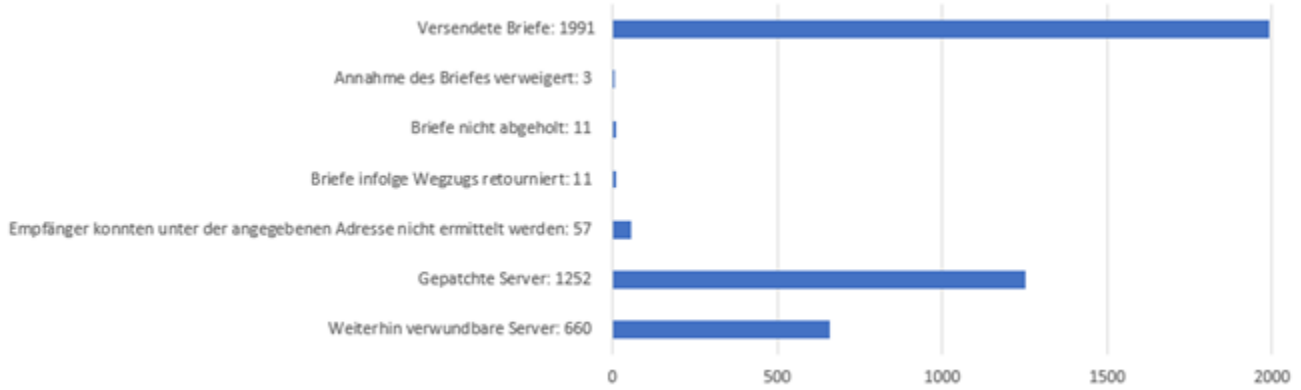
Warnungen

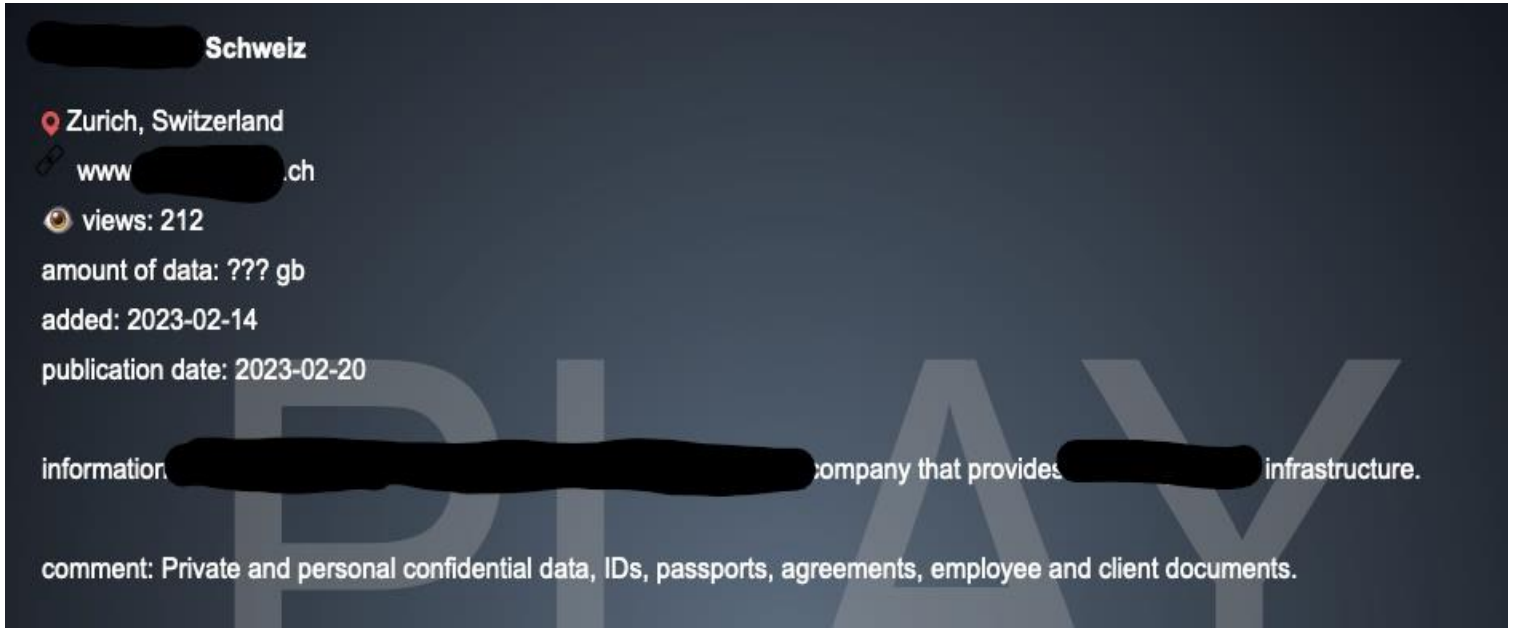
Weiterhin verwundbare Microsoft Exchange Server in der Schweiz («ProxyNotShell») trotz Warnung des NCSC

02.02.2023 - Das NCSC hat bereits im November 2022 darüber informiert, dass über 2'800 Microsoft-Exchange-Server in der Schweiz verwundbar sind, da sie die kritische Verwundbarkeit namens «ProxyNotShell» aufweisen. Einen Monat später wurden rund 2000 Betreiber vom NCSC mittels eingeschriebenen Briefs aufgefordert, die Sicherheitslücke zu schliessen. Dennoch ist die Botschaft noch immer nicht überall angekommen. Über 600 Server in der Schweiz weisen das Einfallstor für Cyberkriminelle immer noch auf.



Microsoft hat im September 2022 informiert, dass es in ihren Exchange-Servern eine kritische Verwundbarkeit namens «ProxyNotShell» gibt und mit Verspätung im November 2022 ein Sicherheits-Update zur Verfügung gestellt. Die Lücke wird bereits seit längerer Zeit aktiv von Cyberkriminellen ausgenutzt («0day exploit»). Aus diesem Grund ist eine rasche Behebung des Problems sehr wichtig. Obwohl der Patch von Microsoft seit mehreren Monaten zur Verfügung steht, sind aktuell in der Schweiz immer noch 660 Server verwundbar.





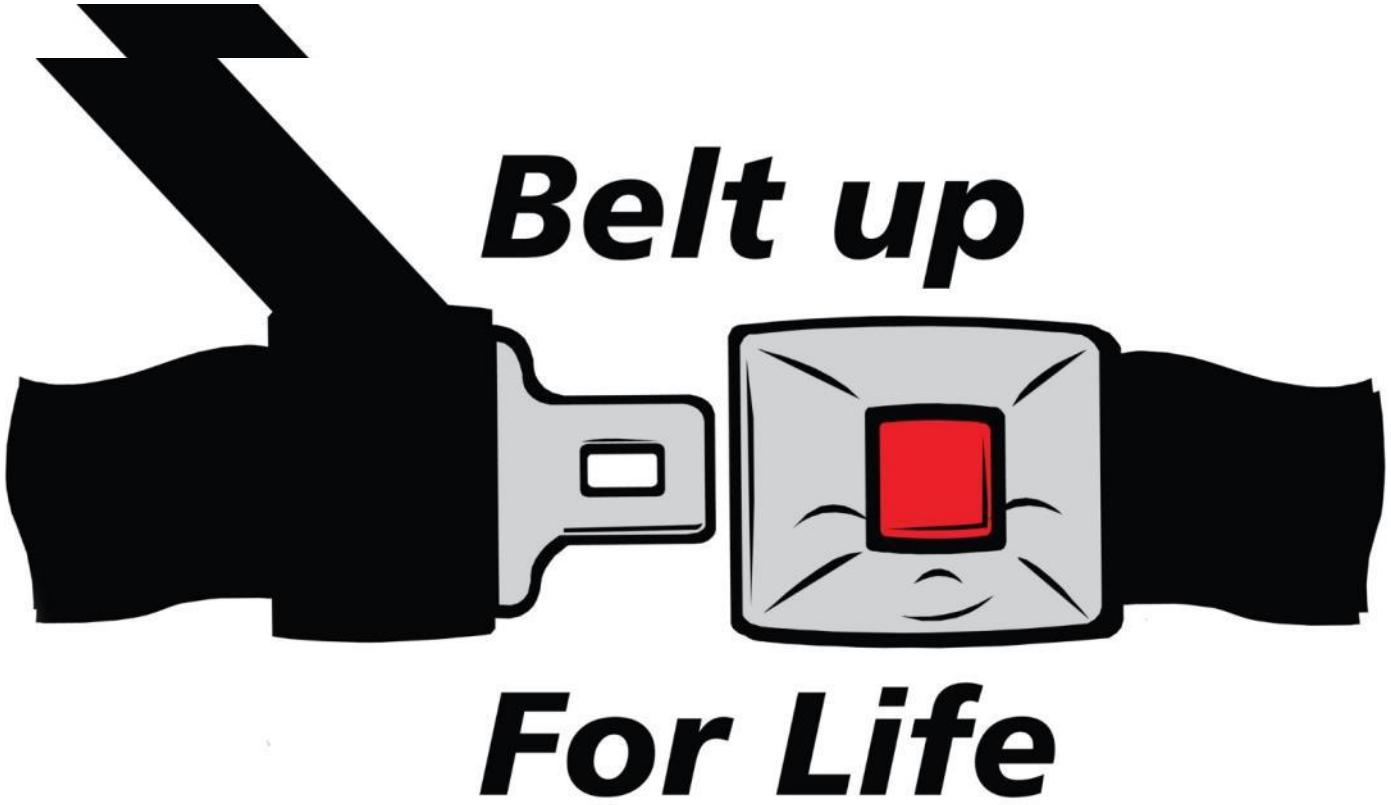
Und was braucht es denn ?

«Es braucht eine Sicherheitskultur»

Mit einem neuen Ansatz beherrschen Organisationen die zunehmenden Bedrohungen aus dem Cyberraum. Es braucht eine konstante Erneuerung der technologischen Basis und eine Sicherheitskultur, die auf Zusammenarbeit und Achtsamkeit beruht.

Moderne Sicherheitskultur ist ein Mix aus Technik, einer klar kommunizierten Strategie und einer guten Zusammenarbeit von IT, Security und dem Business

Sicherheit vs. Risiko



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

Besten Dank für Ihre Aufmerksamkeit

Pascal Lamia
Stv. des Delegierten des Bundes für Cybersicherheit
Leiter der operativen Cybersicherheit im NCSC

Schwarztorstrasse 59
3003 Bern
pascal.lamia@gs-efd.admin.ch
www.ncsc.admin.ch