

Zwei Jahre Anlaufstelle im NCSC – Erfahrungen und Entwicklungen

**43. Informationstagung der Schweizerischen Kriminalprävention in Basel
26. November 2021**



Anlaufstelle NCSC

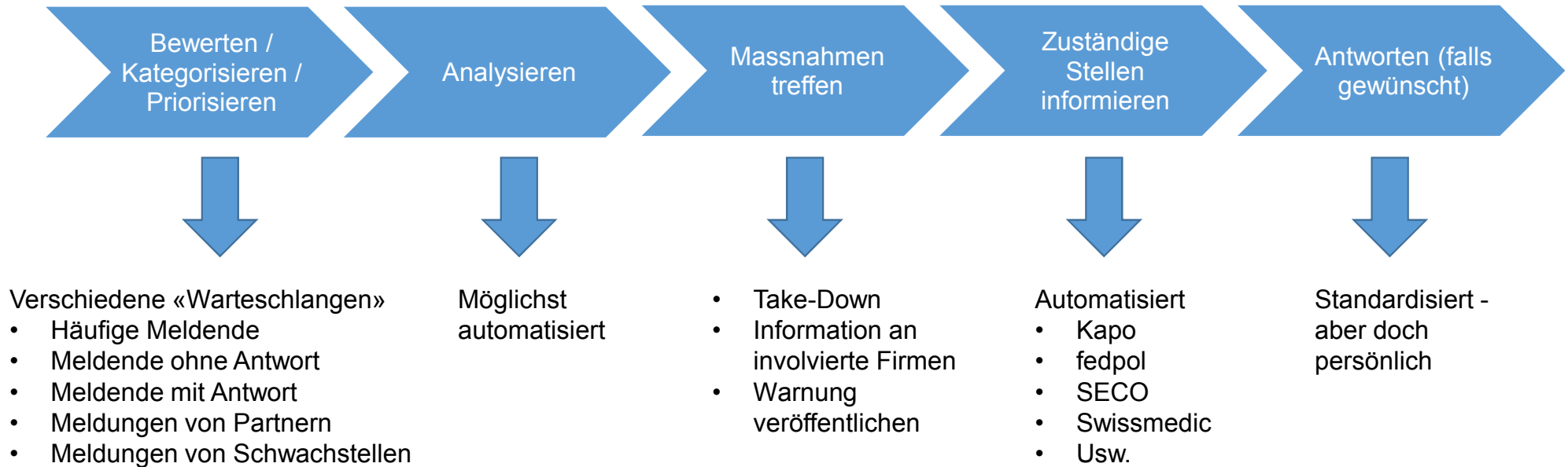
Die Anlaufstelle Cyber existiert seit dem **1. September 2019** und bearbeitet seit dem **1. Januar 2020** Anfragen und Meldungen von Unternehmen und aus der Bevölkerung.

Single Point of Contact	Meldungen	Vorfalls-meldungen	Statistik	Erste Hilfe (zur Selbsthilfe) *
<p>Kontaktpflege mit Bundesstellen, Kantonen, Branchenverbänden, KMU, ...</p> <p>→ Enge Zusammenarbeit mit anderen Stellen im Cyberbereich / Strafverfolgungsbehörden</p>	<p>Entgegennahme und Bearbeitung von Meldungen aus der Bevölkerung, sowie von KMUs und Partnern</p> <p>Bewerten und konsequente Kategorisierung der Phänomene</p>	<p>Warnungen zu aktuellen Vorfällen</p>	<p>Erhebung von Fallzahlen als Unterstützung für eine effektive Beurteilung der nationalen Bedrohungslage</p>	<p>Tipps und Vorgehensweise bei Vorfällen</p>

* Folie von der SKP-Informationstagung 2019



Meldeprozess - effizient und automatisiert





Cyber Incident Workflow and Response Management (CIWORM)

Vorgefertigte Standardsätze und Antworten in 4 Sprachen für zahlreiche Situationen erlauben eine effiziente Bearbeitung

Konkrete Massnahmen

- * Ignorieren Sie Fake Sextortion E-Mails und lassen Sie sich nicht einschüchtern! Bisher sind der Nationalen Anlaufstelle Cyber keine Fälle bekannt, in denen kompromittierendes Bildmaterial vorhanden gewesen wäre.
- * In diesen Fällen ist der Computer der Betroffenen weder infiziert, noch wurden die angegebenen Konten wirklich geknackt.
- * Wenn das erwähnte Passwort von Ihnen verwendet wird, sollten Sie es dennoch dringend ändern.
- * Die in den E-Mails vorhandenen Bitcoin Adressen können Hinweise auf die unbekannte Täterschaft liefern. Mit der Weiterleitung solcher Erpressungs-Mails an reports[at]stop-sextortion.ch helfen Sie mit, die Ermittlungen zu unterstützen.

You can insert report and queue details in your message. For more information, see the [context help page](#).

Internal show comment only in internal reports

Comment

Report Tags

Betrug Fake-Sextortion

Other Tags

Grundschutz | Kein-Telefon-support | Keine-Aktion | Phishing-Vorgehen | Rueckfrage | Take-Down | Take-Down SEO
Zusatzinfos-Anhang | Zusatzinfos-Header | Zusatzinfos-Mailinhalt | CMS-Informationen | Danke | DDoS-Nachbereitung
EDOB-Melden | Empfehlung-externe-Cyber-Beratung | Filetransfer | Gründe-für-Anzeige | Hohes-Phishing-Aufkommen
ID-angeben | Informationen aus E-Mailkonto | Kein-individueller-Support | Keine-Evaluation-Firmen | Keine-Evaluation-Software
Keine-Mailadresse-publizieren | Meldung-Seco-Unlauterer-Wettbewerb | Newsletter-Registrierung | Passwort-Sicherheit

Jede Meldung wird noch zusätzlich manuell überprüft und falls nötig korrigiert.

Submitter Type

Undefined Public SME / KMU KI / Kritische Infra.
Verwaltung Politische Partei Verein NGO / NPO
Medien

Submitter Type

Main category

Awareness-Kampagne False-Positive
Nicht-kategorisierbar Betrug Cybermobbing
Cybersquatting Datenabfluss DDoS Finanzagenten
Generelle-Anfrage Generelle-Information Grooming
Hacking Hoax Insider-Threat Phishing Rufschädigung
Schadsoftware Schwachstelle SEO Sextortion Spam
Spoofing Undefined Verbotene-Pornographie

Kategorisierung der Phänomene gemäss Vorgaben

Tagged To

Betrug Abofalle Betruegerische-Gewinnspiele
Business-E-Mail-Compromise CEO-Fraud Domainfraud
Ersuchen-um-finanzielle-Hilfe-bei-Kontakten Fake-Credit
Fake-DDoS-Erpressung Fake-Extortion Fake-Gebühr
Fake-Sextortion Fake-Spende Fake-Support Fake-Verkauf
Fake-Webshop Identity-Theft Immobilienanzeigebetrug
Investment-Fraud Kleinanzeigenbetrug
nicht-gewollte-Bestellung Payservices-Betrug
Romance-Scam Skimming Ueberzahlbetrug
Vorschussbetrug Werbung-für-Investmentfraud Wire-Fraud

Individuelle Unterkategorien zur Verfeinerung des Lagebildes



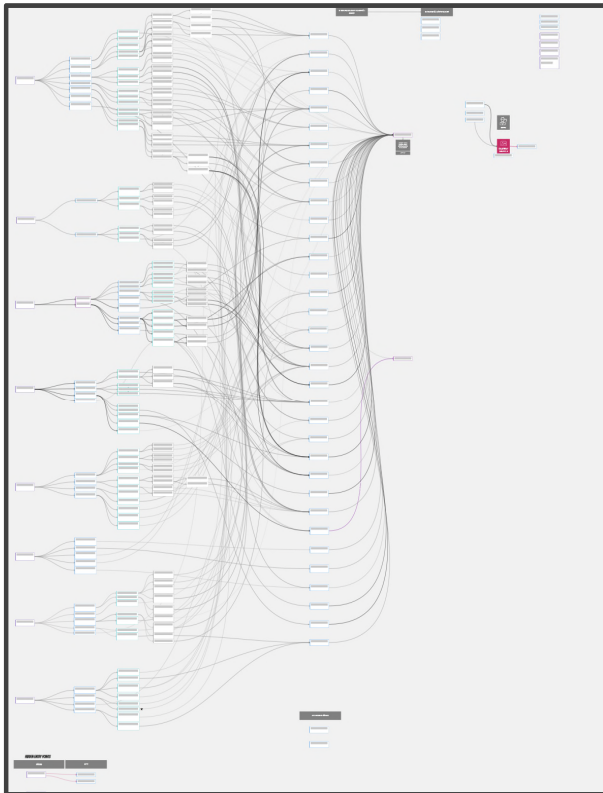
Herausforderung Kategorisierung

Für aussagekräftige Statistiken ist eine konsistente Kategorisierung zentral!

- Ausgangspunkt: Phänomenblätter von fedpol
- Mittlerweile 38 Hauptphänomene und diverse Unterphänomene
- Entwicklung neuer Phänomene ist sehr dynamisch
- Das Bedürfnis für detailliertere Statistiken steigt
- Unterscheidung «Neues Phänomen» oder «Variante eines Phänomens» ist anspruchsvoll
 - ➔ Definition Detaillierungsgrad
- Zunehmende Kombination zweier Phänomene
 - z. B. Kleinanzeigen Phishing
 - z. B. Fake Support Phishing



Interaktives Meldeformular (1)



- Mit möglichst wenigen Schritten ans Ziel
- Mehr als 300 Fragen in 4 Sprachen
- 38 Zielphänomene mit konkreten und präventiven Tipps
- 8 Eingangspunkte mit verschiedenen Perspektiven (Technisch oder Schaden)
- Tipps werden eingeblendet, nachdem gemeldet wurde
- Die Angabe von allen persönlichen Angaben ist freiwillig



Interaktives Meldeformular (2)

Wenige kurze Fragen führen rasch zur Lösung

ich

✉ Eine E-Mail / eine SMS / eine WhatsApp-Nachricht

Ich möchte einen anderen Fall melden

Ich werde erpresst / bedroht

Jemand behauptet, mein Computer sei gehackt worden und man habe peinliche Aufnahmen von mir gemacht

zurück ↩

Über 90% Trefferquote

Wir danken Ihnen für Ihre Unterstützung.

Sie leisten damit einen wichtigen Beitrag, damit wir Trends zu aktuellen Gefahren im Internet zeitnah erkennen und dagegen aktiv werden können.

Nachfolgend finden Sie unsere Empfehlungen für den Umgang mit der Situation.

Fake-Sextortion

Fake-Sextortion

Erpresser drohen mit der Veröffentlichung kompromittierender Bilder. Die Erpressungen kommen unerwartet. Erpresser und Opfer hatten im Vorfeld nie Kontakt.

[mehr erfahren ...](#)

Schaden oder nur Meldung?

NCSC

Bitte wählen Sie die zutreffenden Aussagen:

Ich habe Geld überwiesen

Ich habe kein Geld überwiesen

Soforthilfe und präventive Massnahmen

Konkrete Massnahmen

- Ignorieren Sie Fake Sextortion E-Mails und lassen Sie sich nicht einschüchtern! Bisher sind der Nationalen Anlaufstelle Cyber keine Fälle bekannt, in denen kompromittierendes Bildmaterial vorhanden gewesen wäre.
- In diesen Fällen ist der Computer der Betroffenen weder infiziert, noch wurden die angegebenen Konten wirklich geknackt.
- Wenn das erwähnte Passwort von Ihnen verwendet wird, sollten Sie es dennoch dringend ändern.
- Die in den E-Mails vorhandenen Bitcoin Adressen können Hinweise auf die unbekannte Täterschaft liefern. Mit der Weiterleitung solcher Erpressungs-Mails an [reports\[at\]stop-sextortion.ch](mailto:reports[at]stop-sextortion.ch) helfen Sie mit, die Ermittlungen zu unterstützen.

[schliessen](#) ^



Interaktives Meldeformular - Erkenntnisse

- Unterschiedliche Bedürfnisse von Expertinnen/Experten und Madame oder Monsieur Tout-le-Monde
- Einige wollen sich nicht durch einen Fragekatalog klicken, sondern einfach nur melden
- Es ist schwierig einzuschätzen, ob der Meldende noch weitere Informationen benötigt oder die gewünschten Informationen durch das Formular bekommen hat
- Unstrukturierte Übermittlung von Findings (URLs, Telefonnummern, BitCoin-Adressen) ergibt zusätzlichen Aufwand
- Das Übermitteln von Daten - insbesondere von E-Mails - über ein Formular ist für Meldende nicht einfach und führt zu erweitertem Aufwand auf unserer Seite



Meldeformular Version 2.0 (seit August 21 online)



Direkt Melden

Möglichkeit direkt eine Meldung zu verfassen.
Meldende können das Phänomen direkt wählen.

Möchten Sie eine zusätzliche Antwort per E-Mail erhalten? (Bitte wählen)

- Zusätzliche Antwort erwünscht
- Ich benötige keine zusätzliche Antwort

Meldende können wählen, ob Sie eine Antwort möchten oder ob sie «nur» melden möchten.

Art der Cyberbedrohung

Fake-Sextortion

Krypto Adresse

βFZbgi29cpjq2GjdwV8eyHuJnkLtkZc5

Abhängig von bestimmten Phänomenen, wird gezielt nach Indikatoren gefragt. Beispielsweise wird im Fall von Fake Sextortion nach der Bitcoin-Adressen gefragt.



Informationen

The screenshot shows the homepage of the National Cyber Security Centre (NCSC) of Switzerland. At the top, there is a navigation bar with the logo and the text 'Nationales Zentrum für Cybersicherheit NCSC'. Below this is a search bar and a menu with categories like 'Aktuell', 'Cyberbedrohungen', 'Informationen für', 'NCS Strategie', 'Dokumentation', and 'Über NCSC'. A large blue banner with the text 'Herzlich Willkommen im Nationalen Zentrum für Cybersicherheit NCSC' is prominent. Below the banner, there are two main sections: 'Informationen für' (with icons for Privatpersonen, Unternehmen, and IT-Spezialisten) and 'Melden Sie uns' (with icons for Melden Cybervorfall and eine Schwachstelle). The bottom section features 'Aktuelle Vorfälle', a 'Statistik' chart titled 'NCSC.ch: Meldeeingang', and 'Im Fokus' with a news item about 'Die Woche 39 im Rückblick'.

Generelle Informationen / Trends

Vorfall? Was nun?

Warnungen zu laufenden Angriffen

Aktuelle Statistik

Regelmässige Information zu aktuellen Vorfällen



End of Week

Intern

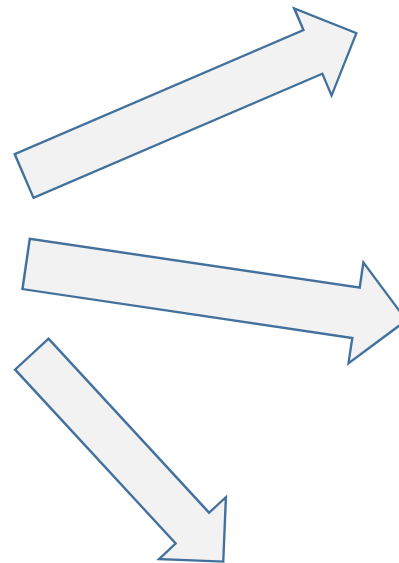
Regelmässige Information

mit den aktuellen Zahlen und den wichtigsten Fällen

End-of-Week - Zusammenfassung

Zusammenfassung der Meldungen von 2. Januar 2021 bis 8. Januar 2021

Anzahl Meldungen pro Hauptkategorie		
Hauptkategorie	Meldungen	davon Schadenfälle
Betrug	203	1
Phishing	85	2
Schadssoftware	14	2
Nicht-kategorisierbar	7	0
Sexortion	4	3
False-Positive	4	0
Spam	4	0
Verbotene-Pornographie	3	0
Hacking	2	0
Cybersquatting	2	0
Finanzagenten	1	0
Datenabfluss	1	0
Undefinierte und allgemeine Meldungen resp. Informationen	20	0
Total	350	8



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Aktuelle Zahlen mit Schadensmeldungen
Stichwortartige Zusammenfassung der
wichtigsten Fälle (ca. 10 – 15 pro Woche)

SKPPSC



Wochenrückblick

Öffentlich

Regelmässige Information

Ein oder zwei interessante Fälle der vergangenen Woche möglichst einfach erklärt!

Wochenrückblicke NCSC

Ergebnisse 1 - 15 von 30 | 1 2 | Eine Seite vor



Die Woche 39 im Rückblick

05.10.2021 - Anlässlich der einsetzenden Herbstferien verzeichnete das NCSC in der letzten Woche einen tieferen Meldeeingang. Das NCSC hat beobachtet, dass die Betrüger bei «Fake Support» Anrufen neuerdings versuchen, auf andere Weise an ihre Opfer zu gelangen. Ergaunertes Geld muss irgendwann eingewaschen werden. Wie für diese Tätigkeit Personen gesucht werden, wird im zweiten Fall beschrieben.



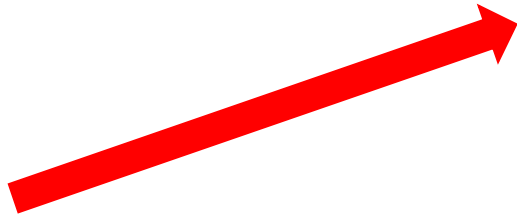
Die Woche 38 im Rückblick

28.09.2021 - In der letzten Woche verzeichnete das NCSC wieder einen erhöhten Meldeeingang. Im Fokus standen betrügerische Gewinnspiele, die angeblich zum 50. Geburtstag von Coop versendet werden. Und bei Kleinanzeigenbetrug vom Typ, dass man trotz eines Verkaufes bezahlen soll, wird ein erheblicher Aufwand betrieben, um das Opfer zur Angabe von Kreditkartendaten zu bewegen.



Die Woche 37 im Rückblick

21.09.2021 - In der letzten Woche verzeichnete das NCSC einen erhöhten Meldeeingang. Aufgefallen sind diverse Varianten von angeblichen Drohungen unter anderem im Namen der Polizei. In der E-Mail wird gedroht, ein Strafverfahren gegen die Empfängerin oder den Empfänger einzuleiten, wenn nicht innerhalb von 72 Stunden geantwortet werde. Und wieder einmal verspricht eine Website Opfern von Investmentbetrug, die verlorenen Gelder zurückzuholen.



- Ignorieren Sie solche Drohmails und lassen Sie sich nicht einschüchtern
- Wenden Sie sich an die Polizei, wenn Sie sich unsicher sind.

service: [redacted]@express [redacted]@express@gmail.com
AVERTISSEMENT POUR SUITE AJOURD'HUI

GENDARMERIE

Bonjour : [redacted]

Nous vous informons qu'en vue de la Charte [redacted] portant sur les fraudes et escroqueries sur internet, des poursuites judiciaires seront prises contre vous et vous risquez une peine de 5 ans d'emprisonnement ferme pour abus de confiance et tentative d'escroquerie via internet, et achetez votre Courrier Express [redacted] en charge DU COURRIER MANDAT [redacted]. Si nous ne recevons pas les coupons [redacted] de 2 coupons 200.00 CHF au plus tard aujourd'hui avant [redacted] des poursuites judiciaires engagées auprès des différentes autorités compétentes.

Nous vous informons aussi que nous disposons de toutes les informations sur vous et l'acheteur (e). Par conséquent, nous vous prions de bien vouloir procéder à l'achat du coupon et nous remettre le code de recharge dans les plus brefs délais

- Vu la Loi n° 92-1341 du 04 mai 2014, Portant supervision des activités financières et réglementaires sur internet,
- Vu la Loi n° 56-7127 du 16/08/2021, Portant Vérification de transfert des fonds par Mandat Fedex via internet

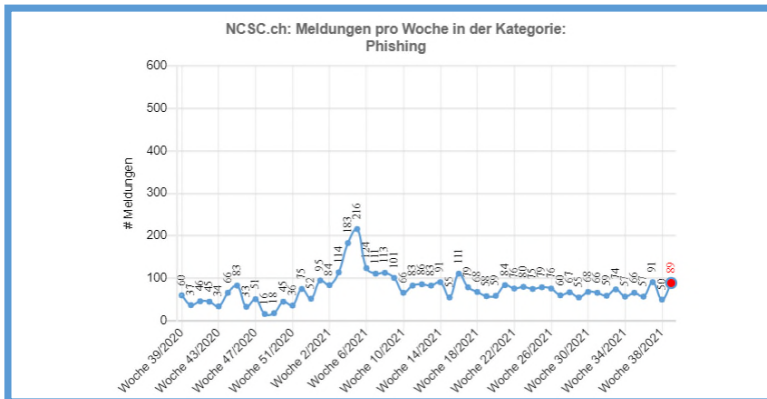
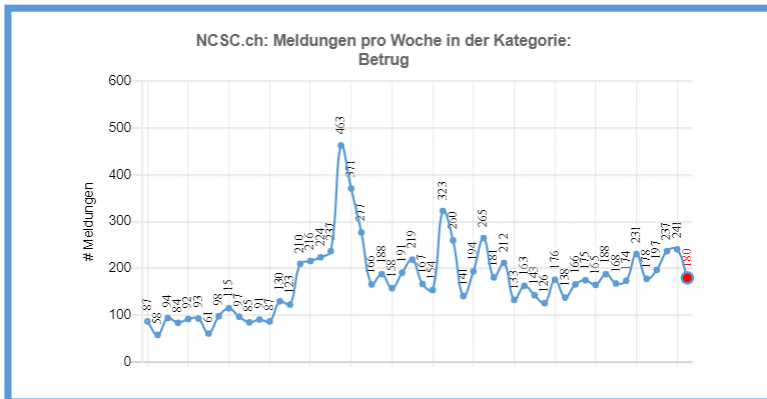
Dans les 24 Heures à venir des poursuites et publications en partenariat avec suisse 24 et RFI seront engagés auprès des différents autorités compétentes en effet vous percevez vos fonds



Was wird gemeldet? Neue interaktive Statistik

Öffentlich

Regelmässige
Information



Erstes Halbjahr 2021

10234 Meldungen

davon

2439 Phishing

1351 Fake Sextortion

1284 Vorschussbetrug

640 gefälschte Zollgebühren

307 Kleinanzeigenbetrug

252 Investment Betrug

239 CEO Betrug

91 Ransomware (vor allem Qlocker)



Vorfallsmeldungen

Öffentlich

Warnung


Aktuelle Vorfallsmeldungen bei erhöhtem Meldeeingang direkt im Meldeformular oder auf der Startseite von www.ncsc.admin.ch

Ich

Eine E-Mail / eine SMS / eine WhatsApp-Nachricht

NCSC


Ist Ihr Fall identisch mit:



Gefälschte Erpressungsmails
Aktuell versenden Betrüger in grosser Menge gefälschte Erpressungsmails, in denen sie vorgeben, den Computer gehackt und Zugang zu Kamera und Mikrofon zu haben. Sie drohen mit der Veröffentlichung von kompromittierenden Filmen und Bildern, wenn man kein Lösegeld in Bitcoin bezahle. Es handelt sich dabei um einen Bluff. Lassen Sie sich nicht einschüchtern und ignorieren Sie diese Fake-Sextortion E-Mails.

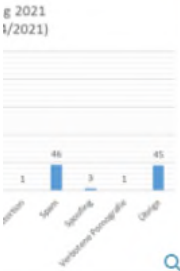
Aktuelle Vorfälle

121 (pro Woche)



Gefälschte Erpressungsmails
Aktuell versenden Betrüger in grosser Menge gefälschte Erpressungsmails, in denen sie vorgeben, den Computer gehackt und Zugang zu Kamera und Mikrofon zu haben. Sie drohen mit der Veröffentlichung von kompromittierenden Filmen und Bildern, wenn man kein Lösegeld in Bitcoin bezahle. Es handelt sich dabei um einen Bluff. Lassen Sie sich nicht einschüchtern und ignorieren Sie diese Fake-Sextortion E-Mails.
03.02.2021 01:00

Betrugsversuche im Namen der Zollverwaltung
In den letzten Tagen werden wieder vermehrt E-Mails gemeldet, welche Bezug auf eine angebliche Paketlieferung nehmen und Gebühren verlangen. Man solle eine Paysafecard kaufen und den Bezahlcode an eine E-Mail Adresse senden. Die E-Mail Adresse der Betrüger ist dabei hinter der offiziell erscheinenden Adresse z.B von der Zollverwaltung versteckt. Ignorieren Sie solche E-Mails.





Generell: Informationen und Trends

Öffentlich

Generelle Information

Aktuell Cyberbedrohungen Informationen für NCS Strategie Dokumentation Über NCSC

Schliessen X

Top Cyberbedrohungen des aktuellen Monats



Phishing



Fake Sextortion



Ransomware



CEO-Betrug

Weitere Cyberbedrohungen (in alphabetischer Reihenfolge)

Abofallen

Betrügerische Gewinnspiele

Checkbetrug

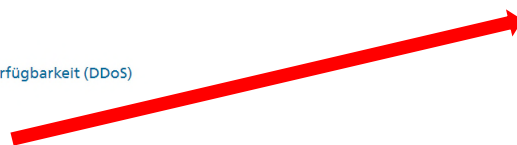
Cybersquatting

Angriff auf die Verfügbarkeit (DDoS)

CEO-Betrug

Cybermobbing

Datenabfluss



92% finden die Informationen und Massnahmen hilfreich!

CEO-Betrug

Angeblich dringende Zahlungsaufforderung vom Chef oder Präsidenten. Typischerweise ist der Chef oder Präsident für Rückfragen telefonisch nicht erreichbar.

Die Angreifer beschaffen sich im Vorfeld Informationen über eine Firma oder einen Verein aus unterschiedlichen öffentlichen Quellen. Mit diesen Informationen wird dann ein Szenario ausgearbeitet und ein massgeschneiderter Angriff durchgeführt. Der eigentliche Betrug findet häufig mit einer E-Mail des angeblichen CEO an die Finanzabteilung oder einer E-Mail vom angeblichen Vereinspräsidenten an den Kassier statt. Durch eine glaubwürdige Geschichte soll die angeschriebene Person dazu bewegt werden, angeblich dringende Zahlungen auszulösen.

Konkrete Massnahmen

- Sollten Sie eine Zahlung getätigt haben, wenden Sie sich bitte umgehend an die Bank, über welche Sie die Zahlung getätigt haben. Allenfalls hat diese noch die Möglichkeit, die Zahlung zu stoppen. Zusätzlich empfehlen wir Ihnen, sich an die für Ihren Geschäftssitz verantwortliche Kantonspolizei zu wenden und Strafanzeige zu erstatten.
- Verifizieren Sie die Richtigkeit des Auftrages bei ungewöhnlichen Aufforderungen innerhalb der Firma / beim Vereinspräsidenten durch telefonische Rücksprache.

- > Vorbeugende Massnahmen
- > Auswirkungen und Gefahren



Vorfall - Was nun?

Die wichtigsten Massnahmen bei Vorfällen mit grossem Schadenspotential. Kurz erklärt, damit der Schaden nicht noch grösser wird.

Öffentlich

Generelle Information

Erfolgreiche Ransomware-Angriffe auf Schweizer Unternehmen

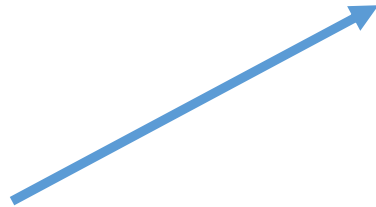
18.08.2021 - Das NCSC hat in den letzten Monaten mehrere erfolgreiche Cyberangriffe gegen Schweizer Unternehmen beobachtet. Bei diesen haben Cyberkriminelle die Unternehmensnetzwerke mittels eines Verschlüsselungstrojaners (sogenannter «Ransomware») verschlüsselt und erfolgreich Lösegeld eingefordert.



In den vergangenen Jahren hat das NCSC immer wieder eindringlich vor Cyberangriffen durch Ransomware gewarnt. Während es sich bei solchen Angriffen in der Regel um komplexe Attacken handelt, lassen sich die meisten davon relativ einfach verhindern. Häufigstes Einfallstor für erfolgreiche Angriffe mit Ransomware sind nicht gepatchte Systeme sowie Fernzugänge wie VPN (Virtual Private Network) und RDP (Remote Desktop Protocol), welche nicht mittels Zwei-Faktor-Authentisierung (2FA) abgesichert sind. Auch Warnmeldungen von installierter Sicherheitssoftware wie Virenschutz werden leider immer wieder auf kritischen Systemen wie Windows Domain-Controllern ignoriert.

Bereits im Februar 2020 hat das NCSC auf die Problematik aufmerksam gemacht:

Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs



Ransomware - Was nun?



Datenabfluss - Was nun?



Webseite gehackt - Was nun?



Cyberattacke – was tun? Checkliste für CISOs



DDoS-Angriff - Was nun?



Wer macht was?

Polizei

- Gibt Ihnen Tipps zur Prävention
- Strafverfolgung. Nimmt Ihre Anzeige auf, sichert Spuren und ermittelt.
- Berät und Unterstützt Sie bezüglich weiteres Vorgehen und Täterkommunikation.
- Kontakt: Grundsätzlich jederzeit möglich. Auf jeden Fall bei einem akuten Angriff, z.B. Erpressung oder Schaden, z.B. Diebstahl.

Nationales Zentrum für Cybersicherheit NCSC

- Gibt Ihnen Tipps zur Prävention
- Keine Strafverfolgung. Nimmt Ihre freiwillige Meldung auf und beantwortet Ihre Fragen.
- Unterstützt Sie und die Polizei bei der Identifizierung der Schadsoftware und Analyse.
- Kontakt: Freiwillige Meldung. Auch bei Ereignissen, die keinen Schaden verursacht haben oder im Versuchsstadium entdeckt wurden, z.B. Phishingmails

IKT-Support

- Bespricht und setzt Präventionsmassnahmen mit Ihnen um.
- Evaluiert das Problem und liefert bei einem Angriff Informationen an die Polizei.
- Stellt Ihre Netzwerke wieder her und behebt Ihre Sicherheitsprobleme.



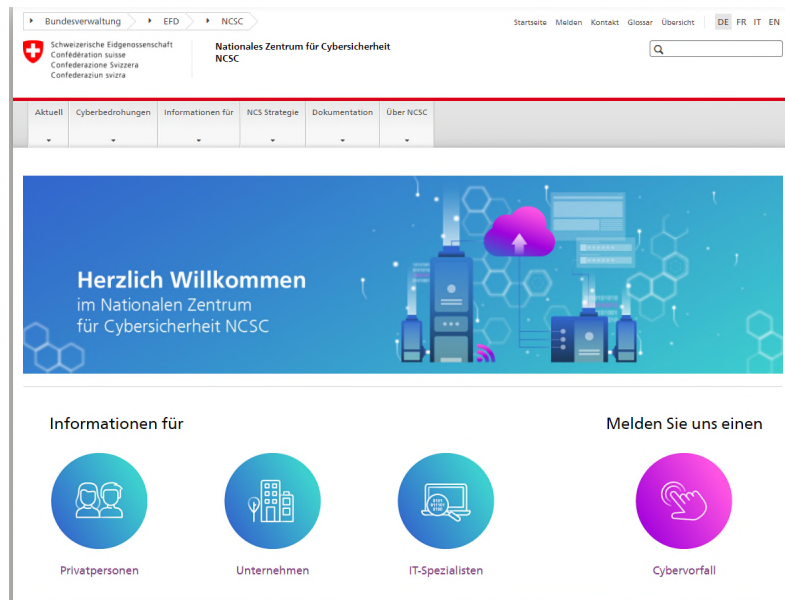
Ausblick

- Alarmierung (Newsletter, Twitter usw.)
- Automatisierte Schnittstelle NCSC - Polizei
- Anbindung Meldeformular an die Möglichkeit einer elektronischen Anzeigeerstattung
- Systematische Erhebung von Daten nach einem Vorfall zwecks statistischer Auswertung
- Systematische Verwertung (auch für die Strafverfolgung) von Daten
 - Betrugsseiten
 - Telefonnummern
 - Bitcoin-Adressen
 - IBAN-Nummern
 -





Vielen Dank für Ihre Aufmerksamkeit!



National Cyber Security Centre NCSC

Web: <https://www.ncsc.admin.ch>

E-Mail: outreach@ncsc.ch