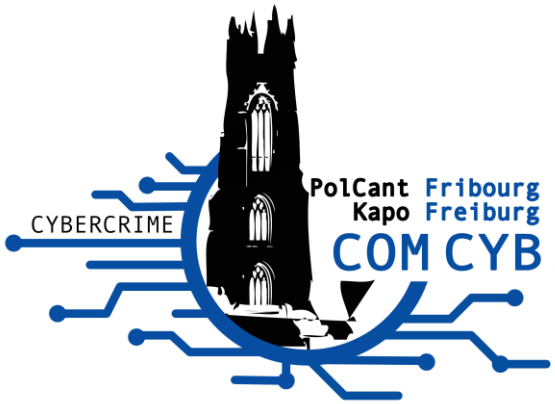
Präsentation für

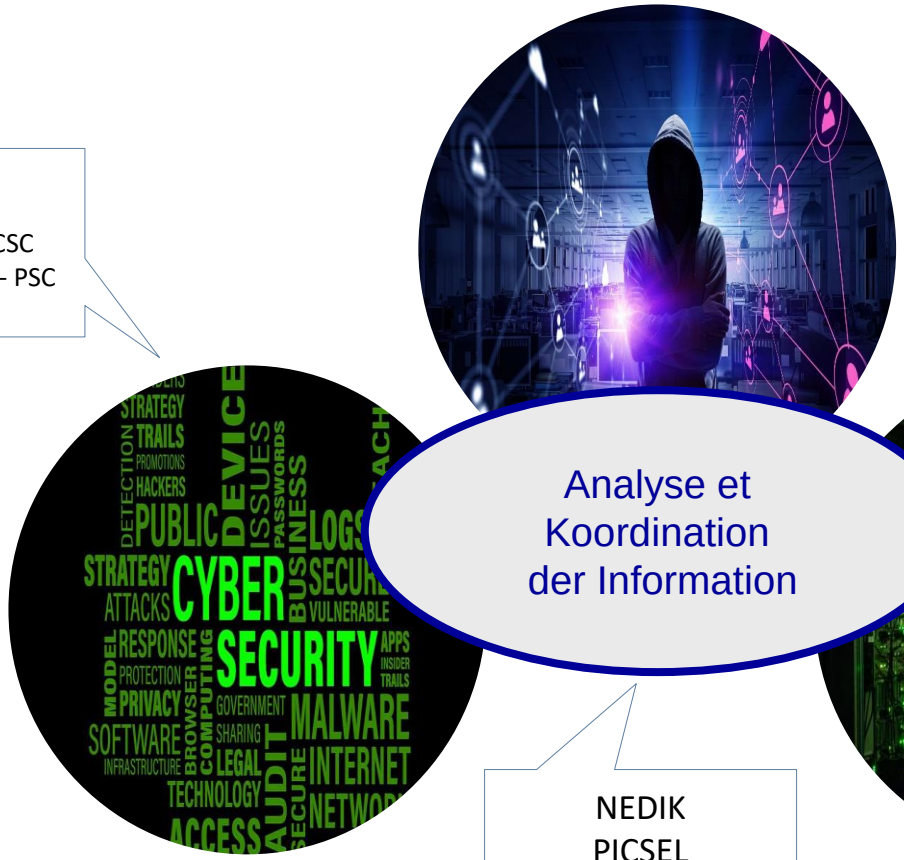
die INFRI-Direktionen

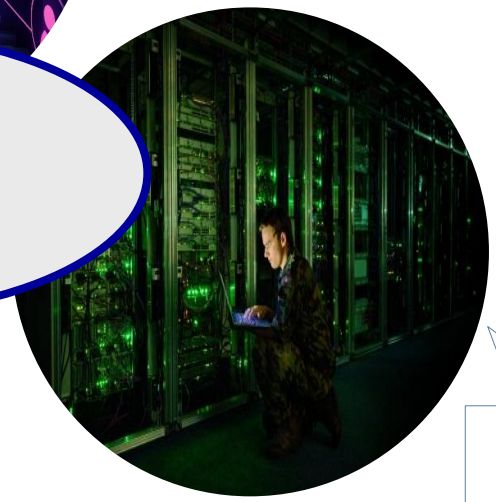
16.12.2022, Freiburg



Tables des matières

Umsetzung der Strategie





Analyse et
Koordination
der Information

NCSC
SKP - PSC

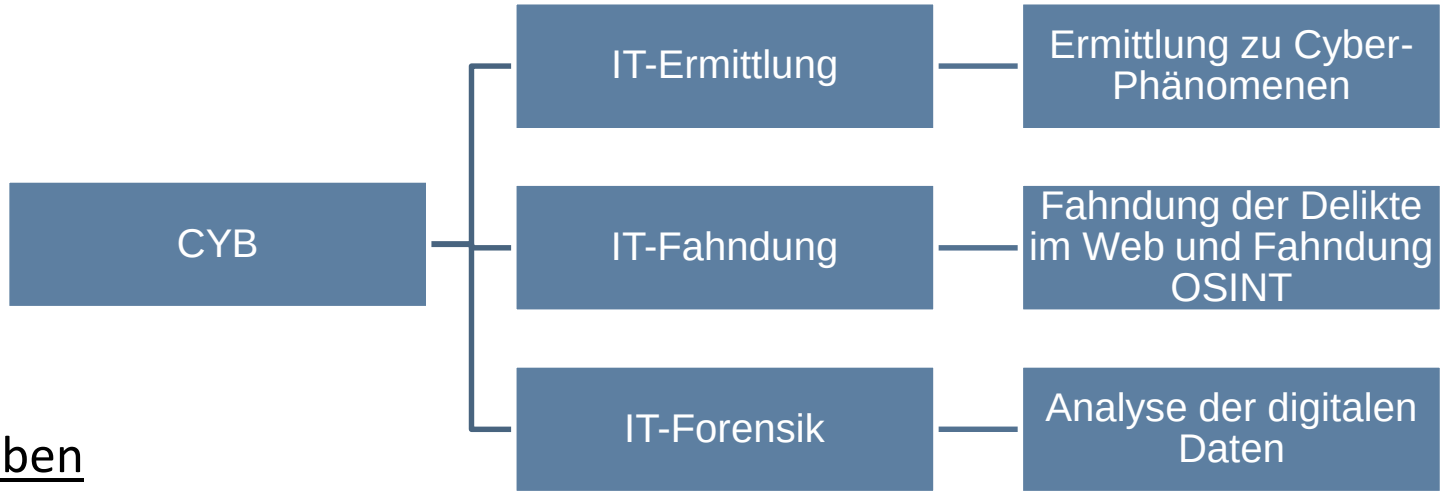
Kantonspolizeien
Kompetenzzentren
Fedpol
Cybercase / Cyberboard

NEDIK
PICSEL

VBS - FUB –
Führungsunter-
stützungsbasis

Bekämpfung der Cyberkriminalität in Freiburg

Kommissariat Cyberkriminalität (CYB)



Aufgaben

1. Prävention
2. Ermittlung
3. Analyse
4. Fahndung
5. Zusammenarbeit

Bekämpfung der Cyberkriminalität in Freiburg

Jeder Freiburger Polizist muss sich mit Cyberkriminalität befassen

Er verfügt über:
- Grundausbildung
- Dokument «Cyber-Strafanzeige»
- Die Unterstützung durch das Kommissariat Cyber bei komplexen Fällen
- Gesetzliche Grundlagen, die eine Anzeige ermöglichen

Cybercrime im Kanton Freiburg

2019 | **529** Cyber-Anzeigen | ~ CHF 2’940’000.00
2020 | **570** Cyber-Anzeigen | ~ CHF 2'510‘000.00
2021 | **804** Cyber-Anzeigen | ~ CHF 7’190’000.00
…
581 Cyber-Anzeigen zwischen Januar und August 2022

Ransomeware

Phase 1

- Der Hacker schickt eine Malware-E-Mail
- Die E-Mail überwindet die Spam-Filter des Opfers
- Das Opfer öffnet die E-Mail

Phase 2

- Das Opfer lädt den Anhang herunter
- Der Antivirus erkennt die Gefahr nicht
- Die Ransomware kontaktiert den Server, um den Entschlüsselungscode zu erhalten
- Die Daten des Opfers werden verschlüsselt
- Der Verschlüsselungscode auf dem Computer des Opfers wird zerstört

Phase 3

- Auf dem Computer des Opfers erscheint eine Nachricht, in der ein Lösegeld für die Wiederherstellung der Daten gefordert wird
- Wenn bezahlt wird, kann der Verschlüsselungscode, mit dem die Daten entschlüsselt werden können, normalerweise wieder erlangt werden
- Wenn nicht bezahlt wird, bleiben die Daten verschlüsselt und gelangen in das dark-deepweb

https://youtu.be/v-ITcpD1KcQ

Ransomeware

1. Wenn vertrauliche Daten unserer Mitarbeiter oder Bewohner offengelegt werden oder Cyberangriffe festgestellt werden, was sind die ersten Reflexe, die in einer solchen Situation zu beachten sind? Ist die Polizei dafür zuständig, uns zu helfen, oder ist dies die Aufgabe eines privaten Akteurs? Wir haben einen Drittanbieter: Ist es in diesem Fall seine Aufgabe, die Schritte zu unternehmen? Wie sind die Kompetenzen und Verantwortlichkeiten verteilt?

   - Die Polizei alarmieren
   - Stoppen / Abschalten
   - Polizei: berät, sammelt Spuren und unterstützt bei der Verwaltung der Ransomware
   - Den Datenbeauftragten informieren
   - Keine Wiederherstellung der Infra durch die Polizei, sondern durch einen privaten Anbieter

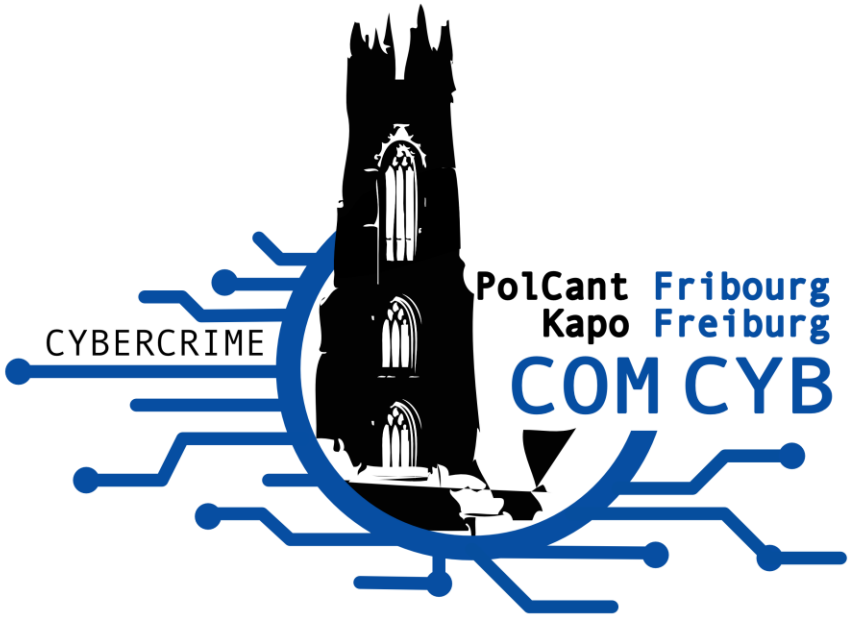
2. Welches sind die Erwartungen in Sachen Krisenmanagement?

Die Polizei rufen, die richtigen Personen im Unternehmen/in der Institution vor Ort haben, bereit sein, zu informieren. Uns vertrauen uns zuhören.

3. Ist es besser, das Lösegeld zu zahlen?

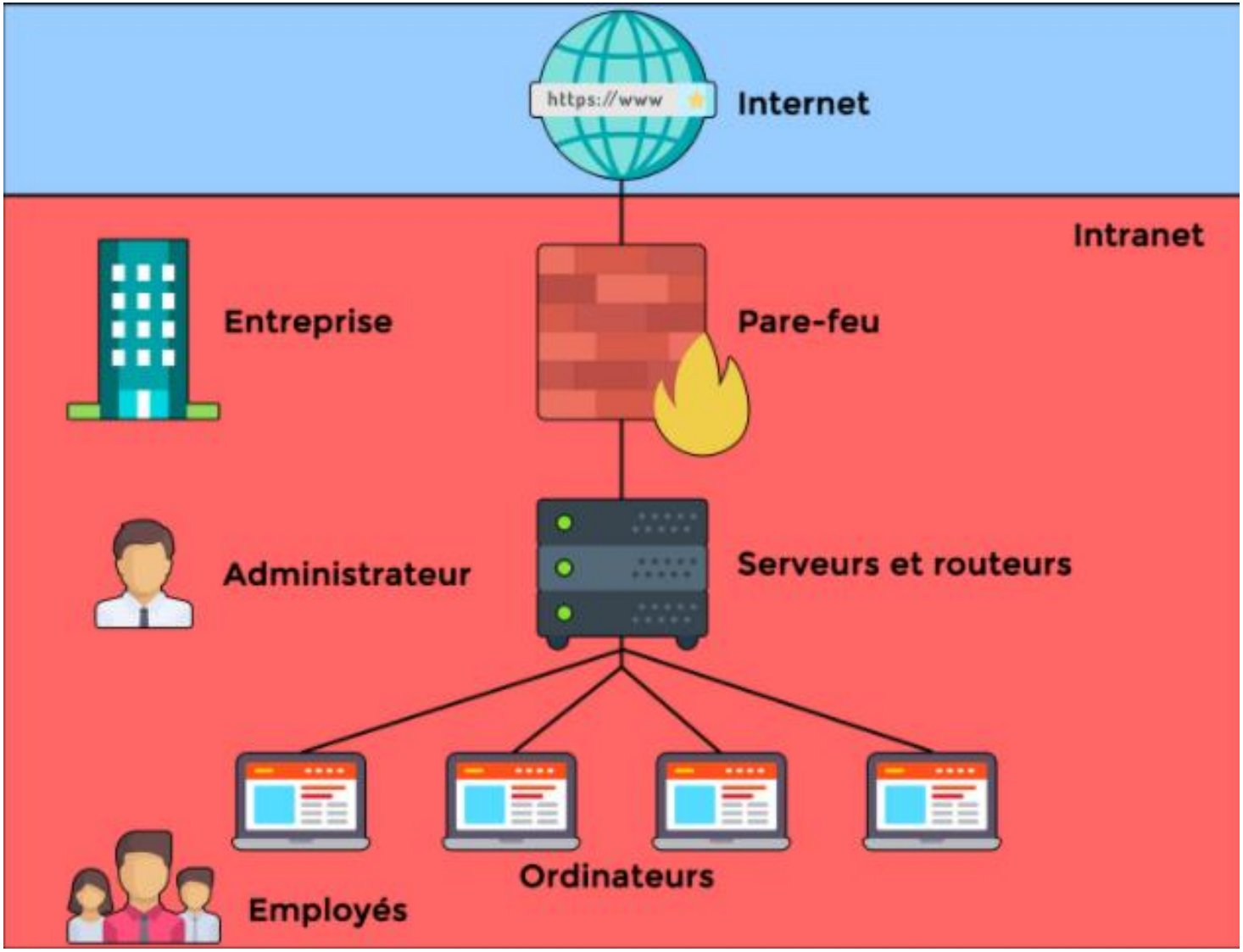
Nein, es ist nie empfehlenswert, es sei denn, es gibt eine andere keine andere Wahl. Laut US-Regierung als Unterstützung des organisierten Verbrechens eingestuft, daher ist es nicht mehr möglich, in den USA Deals zu machen….

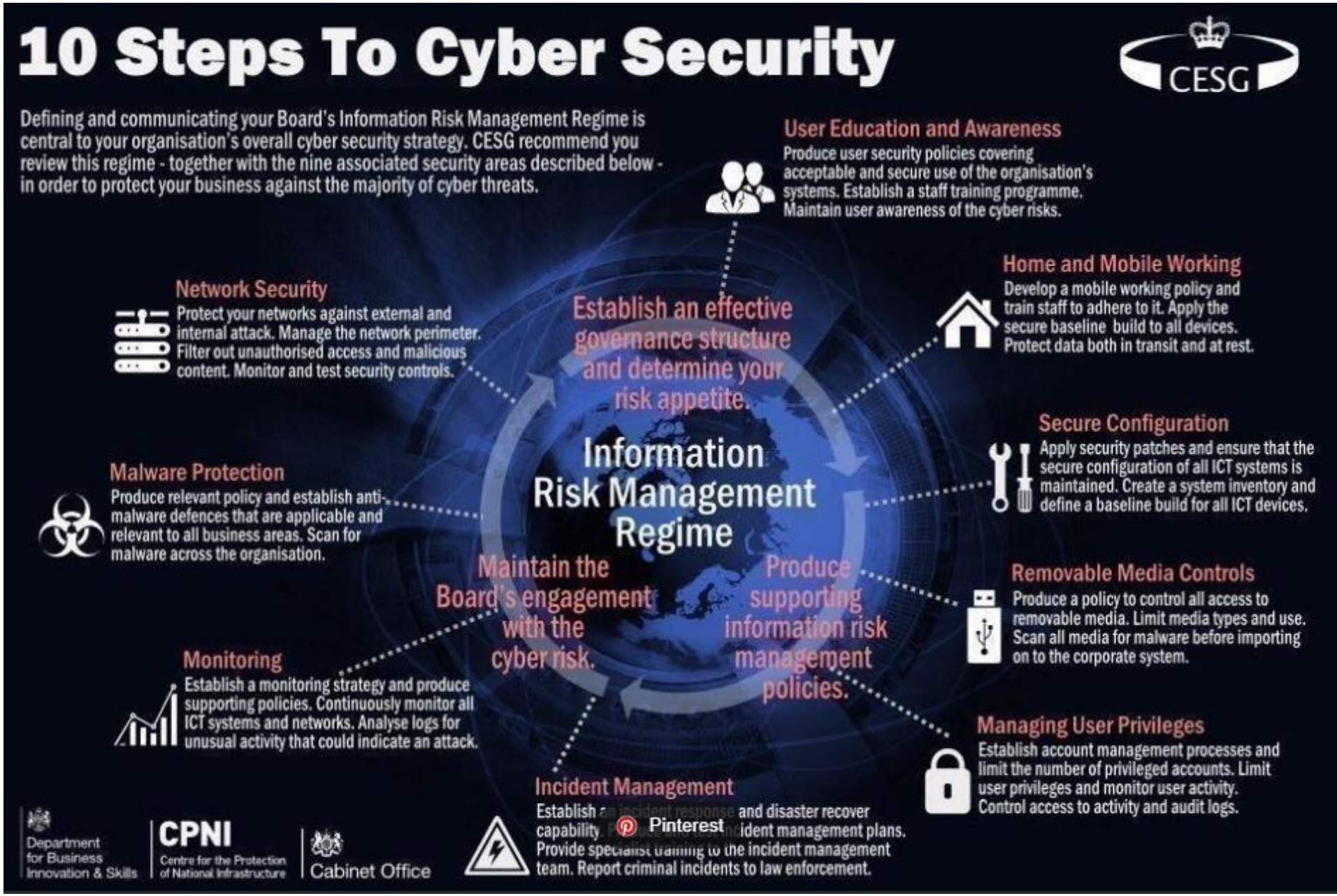
Cybersicherheit



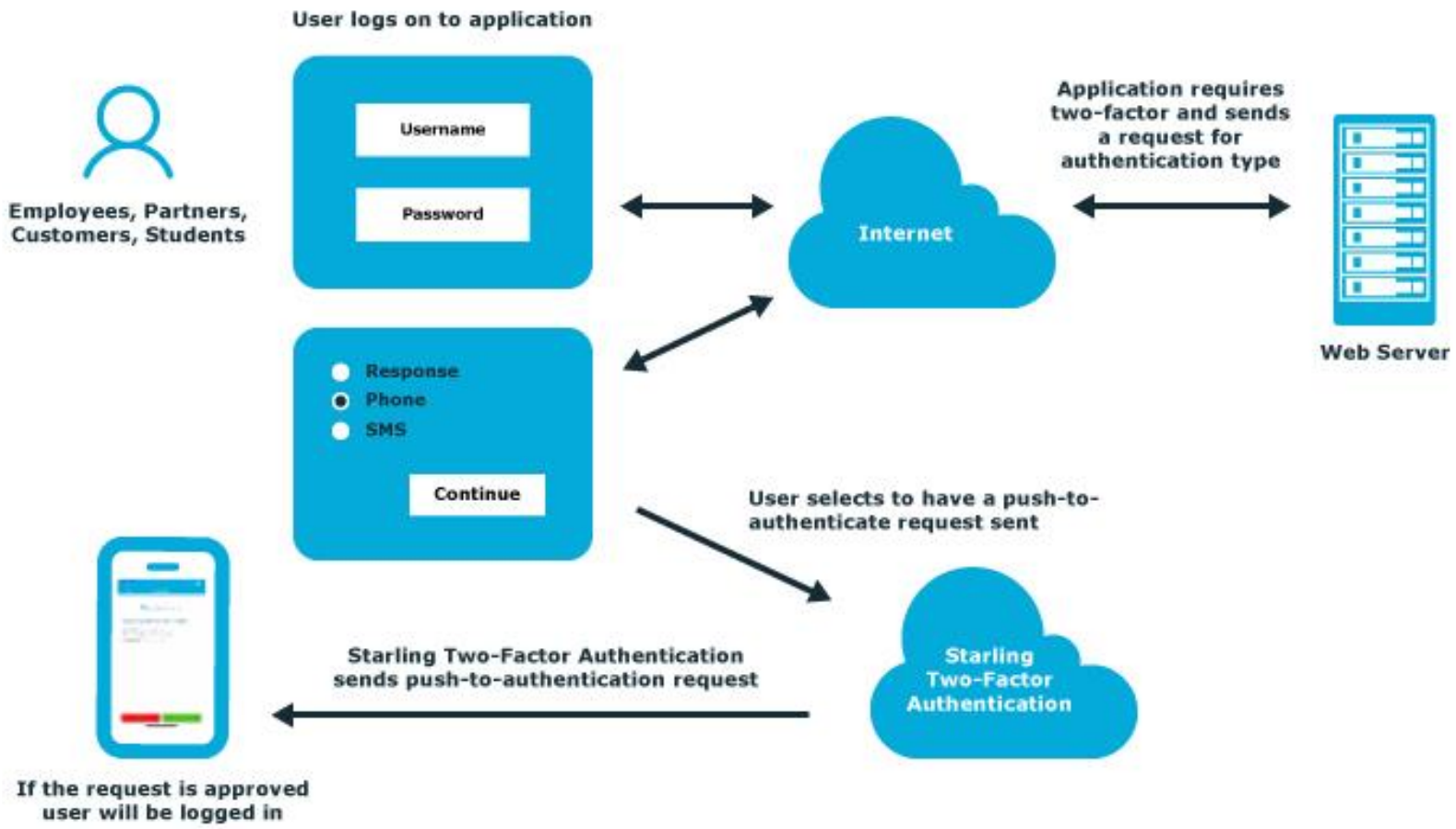
https://www.fr.ch/police-et-securite/prevention/cybercriminalite

Sicherheit


https://www
Internet
Intranet
Entreprise
Pare-feu
Administrateur
Serveurs et routeurs
Ordinateurs
Employés


10 Steps To Cyber Security
CESG
Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.
User Education and Awareness
Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.
Home and Mobile Working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.
Network Security
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.
Establish an effective governance structure and determine your risk appetite.
Information Risk Management Regime
Secure Configuration
Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.
Malware Protection
Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.
Maintain the Board's engagement with the cyber risk.
Produce supporting information risk management policies.
Removable Media Controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.
Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.
Managing User Privileges
Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
Incident Management
Establish an incident response and disaster recover capability. Test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.
Pinterest
Department for Business Innovation & Skills
CPNI
Centre for the Protection of National Infrastructure
Cabinet Office

Doppelte Authentifizierung



Smartphone und Sicherheit

1. Sperren des Telefons
2. Keine Passwörter auf den Datenträgern
3. Nicht das gleiche Passwort für mehrere Verwendungszwecke
4. Kein automatisches Speichern von Passwörtern
5. Aktualisierungen durchführen
6. Keine Links oder Dokumente öffnen

Das Passwort wählen und verwalten

1. Starkes Passwort mit Zeichen, Sonderzeichen, Grossbuchstaben und mind. 9 Zeichen
2. Speichern von Passwörtern nur auf sicheren Tools
3. Kein kostenloses automatisches Erstellen von Passwörtern
4. Regelmässiges Ändern des Passwortes
5. Die Passwörter nicht in Ihrer Suchmaschine speichern
6. Die doppelte Authentifizierung / Bestätigung verwenden

Betrügerischer falscher technischer Support

1. Adresse und Absender überprüfen
2. Kontrollfragen stellen
3. Sie brauchen Hilfe, nicht umgekehrt
4. Keine dringende Aktion oder Aktion unter Druck
5. Nichts installieren
6. Vorsicht: Was kostenlos ist, ist gesponsert oder gehackt

Schutz

1. Gibt es ausser Antivirenprogrammen auch andere Lösungen, um Computer zu schützen?

Ich würde ein EDR hinzufügen.

2. Was wäre die derzeitige ideale Konfiguration, um ein Höchstmass an Sicherheit zu gewährleisten? 2 Grundregeln.

Die beste Sicherheit ohne die beste Ausbildung hat keine Chance. Wenn man wirklich will, kommt man auch rein.

3. Muss auf dem Server die Firewall regelmässig ausgetauscht werden?

Aktualisieren aber nicht austauschen.

4. Ist es besser, die Daten auf einem lokalen Server oder in der Cloud zu hosten oder eine spezialisierte Firma zu beauftragen?

Für den Schutz von Daten auf einem Server hängt das Mandat von der internen Fähigkeit ab, das System zu aktualisieren und zu warten.

Schutz

4. Ansonsten haben wir unsererseits einen regelmässigen Wechsel der Passwörter und eine verstärkte Authentifizierung eingeführt. Welche anderen Wege könnten erforscht werden?

Doppelte Authentifizierung/Validierung, Datenspeicherung, Identifizierung durch Geolokalisierung. Passwort alle 60-90 Tage ändern. Die beste Sicherheit hat keine Change ohne die bestmögliche Ausbildung. Wenn man wirklich will, kommt man rein.

5. Sind die Risiken für Mitarbeiter, die sich vor ihrem Computer oder Mobiltelefon aus in das Firmennetzwerk einloggen, grösser? Was ist zu tun?

Nein, wenn das Material von der Firma bereitgestellt und von der Firma auf dem neuesten Stand gehalten wird. Wess es sich um privates Material handelt, dann ja, die Risiken sind sehr hoch. Aktualisieren, aber nicht ändern.

6. Was kann konkret umgesetzt werden, um Cyberkriminalität wirksam zu bekämpfen?

Ausbildung, System auf dem neuesten Stand, Backup korrekt und praktikabel. Der Sicherungsserver aktiviert sich selbst, holt die Daten und schaltet sich von selbst wieder ab. Nicht der Hauptserver, der die Daten ablegt.

Schutz

7. Können in der IT-Infrastruktur Massnahmen ergriffen werden, damit ein möglicher Hackerangriff nicht alle Bereiche der Einrichtung betrifft?

Die Abschottung der Dienste…

8. Definition von sensiblen oder nicht sensiblen Daten? (wenn ich z.B. an eine Begünstigten-Akte denke)

Zum Beispiel für die Polizei: persönliche Daten sind sensibel, der Rest nicht.

9. Wie hoch ist der Anteil von Social Engineering, menschlichem Versagen bei der Cyberkriminalität? Was sind die besten Präventionsinstrumente in einem Unternehmen?

80% menschlich, 20% Aktualisierung der Systeme, aber man erkennt keine physischen Angriffe.

10. Sichere und computergestützte Übermittlung von Bilanzen, Berichten, zwischen Institutionen: Welche Vorkehrungen?

Wenn per E-Mail, dann Verschlüsselung der E-Mail und des Anhangs. Ansonsten SharePoint mit doppelter Authentifizierung.

Telearbeit ohne Risiko

1. Sicheres Wifi
2. Geändertes Passwort
3. Empfehlungen der Firma
4. PC sperren
5. Arbeitsdokumente wegräumen

Sicherheit

1. Was wären die «Warnzeichen» oder «Vorboten»?

Die Systeme werden immer intelligenter und stehlen nach und nach Informationen, um von der Systemüberwachung nicht entdeckt zu werden.

2. Was sind die Vor- und Nachteile der Datenspeicherung auf physischen Servern oder in einer Cloud? Wird ein Weg bevorzugt?

Physische Server erfordern mehr Investitonen und Wartung, während die Cloud dies bereits in ihren Pauschalen anbietet. Auch Backups werden oft automatisiert. Der Datenschutz muss überprüft werden.

3. Auf der Seite der E-Mails, die Viren enthalten, welche Mittel gibt es, um diese zu erkennen, wenn sie vorhanden sind?

Office 365 bietet eine Sandbox, die eine Art Analyse der Datei durchführt, aber grundsätzlich ermöglicht nur das Misstrauen des Benutzers die Erkennung.

Versicherung

CYBERCRIME
PolCant Fribourg
Kapo Freiburg
COM CYB

Versicherung

1. Sollte man sich gegen solche Risiken versichern?

Vorzugsweise ja. Eine Versicherung geht von 2000-10000 pro Jahr und deckt die Instandsetzung und bei manchen auch einen kleinen Betrag der Ransomeware ab.

Versicherung

2. Existieren klare Verantwortlichkeiten für die IT-Sicherheit in einer Sozialinstitution? Im Moment interessiert mich vor allem die Frage, inwiefern eine Direktion für mögliche Unterlassungen (z.B. keine Cyber-Versicherung, ungenügendes Backup) haftbar gemacht werden kann.

Unter dem Gesichtspunkt des Schweizer Strafgesetzbuches gibt es meiner Meinung nach keine Bestimmung, die einen solchen Fall unter Strafe stellen würde.

Die Prüfung muss somit unter dem Blickwinkel des Datenschutzgesetzes (DSG) erfolgen.

Auch die in Art. 34 und 35 DSG enthaltenen Strafbestimmungen in ihrer derzeitigen Fassung sind nicht geeignet, eine solche Situation zu ahnden (siehe SR 235.1 - Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) (admin.ch)

Dies wird ab dem 1. September 2023, dem Datum des Inkrafttretens des neuen DSG, anders sein (nachstehend: nDSG - BBl 2020 7639 - Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) (admin.ch)

Denn Art. 61, insbesondere sein Buchstabe c, wird es ermöglichen, Privatpersonen zu bestrafen, die vorsätzlich die vom Bundesrat erlassenen Mindestanforderungen an die Datensicherheit nicht einhalten. Zu diesem Zweck ist auf Art. 8a Abs. 3 nDSG zu verweisen, der wiederum auf Art. 3 ff. der neuen Datenschutzverordnung vom 31.08.2022 verweist.

Weitere Informationen finden Sie unter folgendem Link:
https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-90134.html#:~:text=Berne%2C%2031.08.2022%20%2D%20La,septembre%202023%2C%20conform%C3%A9ment%20%C3%A0%20la

Cybersecurity Phishing – Ausbildung

CYBERCRIME
PolCant Fribourg
Kapo Freiburg
COM CYB

Phishing

1. Adresse und Absender überprüfen
2. Den Inhalt der E-Mail überprüfen, aber keine Anhänge öffnen
3. Keine URL- oder Internet-Links öffnen
4. Die Firma oder den üblichen Lieferanten anrufen, um die Echtheit zu prüfen

Ausbildung

1. Wir erwägen, unsere Mitarbeiter zu testen, indem wir eine Pseudo-Hacker-E-Mail versenden, um zu sehen, wie viel Prozent der Leute den Anhang öffnen? Ist das legal?

Meines Wissens ist dies nicht illegal. Ich würde nur darauf achten, dass die Datei später nicht zur Überwachung von Mitarbeitern verwendet wird.

2. Wäre es denkbar, gemeinsam Ausbildungen oder E-Learnings für Mitarbeiter hinsichtlich des Verhaltens im Umgang mit Cyberkriminalität zu organisieren?

Es ist alles möglich.

3. Wir haben die Prävention gegen Cyberangriffe bei den Mitarbeitern unserer Unternehmen in unserem Unternehmen auf drei Schwerpunkte ausgerichtet: 1. Doppelte Authentifizierung auf unseren Systemen / 2. Prävention-Informationen über Malware wie Anhänge / 3. Information über Techniken des Social Engineering (z. B. betrügerische Telefonanrufe). Steht dies im Einklang mit dem aktuellen Kontext?

Perfekt. Passwörter und Authentifizierung durch Geolokalisierung hinzufügen. Präsenzschulungen wären ideal, E-Mails bringen oft nicht viel.

Phishing du 13.12.22

Répondre Répondre à tous Transférer

mar. 13.12.2022 13:29

Protection des donnees <fdataprotection1234@gmail.com>

Notification de plainte pénale (LPD)

À Landert Matthieu

Madame, Monsieur

Cette notification vous a été automatiquement envoyée car nous avons reçu une plainte pénale d'un client alléguant que votre entreprise viole la loi fédérale sur la protection des données (Art. 61 LPD - Violation des devoirs de diligence).

Vous pouvez télécharger le dossier constitué contenant la plainte et les coordonnées du plaignant à partir du lien ci-dessous:

http://bit.ly/3PqX4Lk

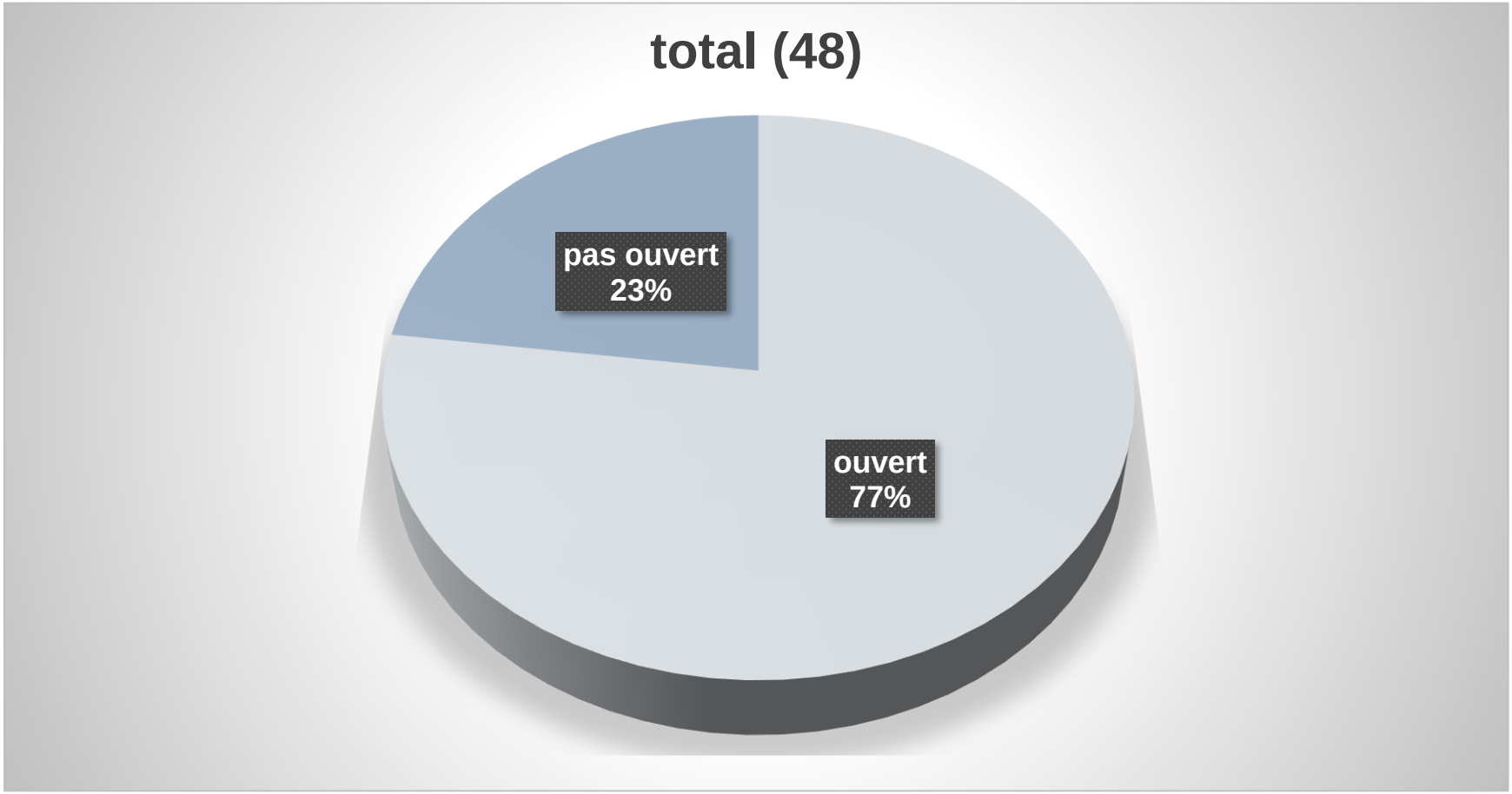
Veuillez prendre un moment pour examiner la section en gras de la plainte, concernant le respects des exigences minimales en matière de sécurité des données édictées par le Conseil fédéral selon l'art. 8, al. 3.

Cordialement,

Préposé fédéral à la protection des données

Phishing du 13.12.22

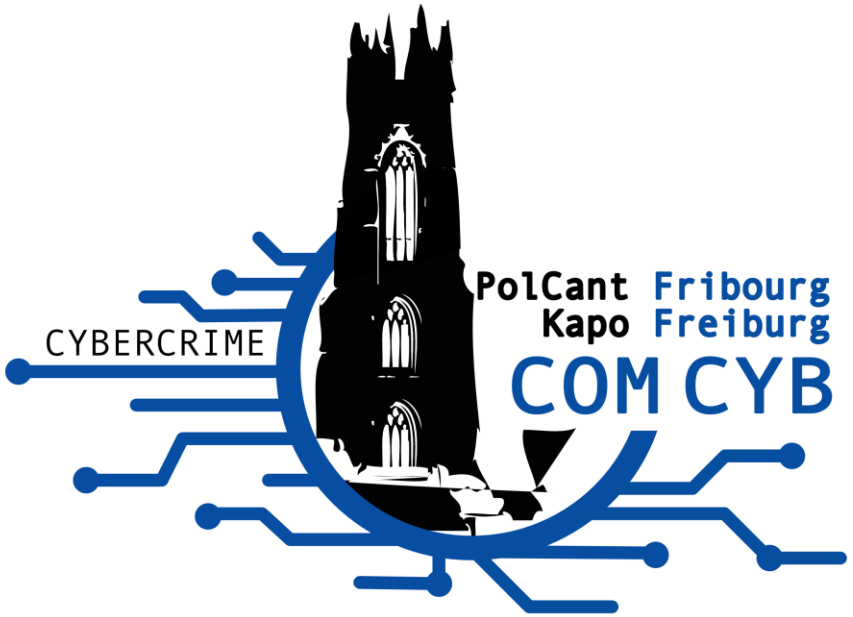
Phishing du 13.12.22



Phishing du 13.12.22

```
2022-12-13 - 13:28:57 -  52.11.247.9 : 38020 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
2022-12-13 - 13:29:31 -  40.94.105.4 : 56230 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
2022-12-13 - 13:39:33 -  104.47.22.126 : 43798 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 13:39:34 -  164.128.184.170 : 13262 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/
2022-12-13 - 13:39:56 -  51.107.43.35 : 13176 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
2022-12-13 - 13:40:16 -  104.47.22.126 : 13954 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 13:40:16 -  164.128.184.170 : 65264 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/
2022-12-13 - 13:40:19 -  104.47.22.62 : 15630 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 13:40:20 -  195.65.152.146 : 22052 | Mac OS X | Mozila | Come from site :direct connection | user agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0
2022-12-13 - 13:40:40 -  104.47.22.62 : 23602 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 13:40:40 -  195.65.152.146 : 30848 | Mac OS X | Mozila | Come from site :direct connection | user agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0
2022-12-13 - 13:41:16 -  104.47.22.62 : 31382 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 13:41:16 -  195.65.152.146 : 21400 | Mac OS X | Mozila | Come from site :direct connection | user agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:107.0) Gecko/20100101 Firefox/107.0
2022-12-13 - 13:41:18 -  104.47.22.126 : 16798 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 13:41:19 -  164.128.184.170 : 14066 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
2022-12-13 - 13:43:39 -  178.197.238.95 : 55370 | Android | Handheld Browser | Come from site :direct connection | user agent:Mozilla/5.0 (Android 11; Mobile; rv:107.0) Gecko/107.0 Firefox/107.0
2022-12-13 - 13:46:08 -  35.165.36.118 : 39942 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
2022-12-13 - 13:47:34 -  109.202.219.87 : 42576 | Mac OS X | Safari | Come from site :direct connection | user agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.1 Safari/605.1.15
2022-12-13 - 13:50:34 -  109.202.219.87 : 41018 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:Wget/1.21.3
2022-12-13 - 13:54:06 -  109.202.219.87 : 35816 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:Wget/1.21.3
2022-12-13 - 13:55:22 -  40.94.34.17 : 28876 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
2022-12-13 - 14:56:54 -  104.47.22.62 : 18902 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 14:56:56 -  103.217.239.61 : 56836 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/1
2022-12-13 - 14:57:10 -  104.47.22.62 : 46368 | Unknown OS Platform | Unknown Browser | Come from site :direct connection | user agent:
2022-12-13 - 14:57:10 -  103.217.239.61 : 63786 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/1
2022-12-13 - 14:57:35 -  51.107.43.35 : 30946 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
2022-12-13 - 14:57:55 -  13.64.151.60 : 19484 | Windows 8.1 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36
2022-12-13 - 14:57:57 -  103.217.239.61 : 42216 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/1
2022-12-13 - 14:58:01 -  13.64.151.60 : 47946 | Windows 8 | Safari | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
2022-12-13 - 15:24:17 -  40.77.167.80 : 62464 | Unknown OS Platform | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; MicrosoftPreview/2.0; +https://aka.ms/Microsoft
2022-12-13 - 16:21:49 -  51.107.43.35 : 43340 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
2022-12-13 - 22:46:08 -  194.230.147.29 : 61552 | iPhone | Handheld Browser | Come from site :direct connection | user agent:Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/108.0.535
2022-12-13 - 22:52:18 -  194.230.147.29 : 39980 | iPhone | Handheld Browser | Come from site :direct connection | user agent:Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/108.0.535
2022-12-14 - 07:52:45 - US 40.94.25.136 : 36490 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
2022-12-14 - 19:25:22 -  205.169.39.76 : 39618 | Windows 7 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
2022-12-14 - 19:25:28 -  205.169.39.76 : 53344 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.79 Safari/537.36
2022-12-15 - 09:55:54 -  51.107.101.195 : 54502 | Windows 10 | Chrome | Come from site :direct connection | user agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
```

Die Herausforderungen



Die aufgetretenen Schwierigkeiten

- Alles ist Cyber, aber fast nichts ist wirklich Cyber
- Ständige Veränderung der Cyberangriffe und der verwendeten Tools
- Mangelendes Wissen und Verständnis der Geschädigten und zukünftigen Geschädigten
- Die notwendige Schnelligkeit, um zu versuchen, Transaktionen zu verhindern

Die aufgetretenen Schwierigkeiten

Auf Schweizer Ebene

- Partielle Datenbank (Identifizierung von Serien)
- Beschlagnahmung von Kryptowährungen
- Monitoring – Zusammenarbeit mit den Behörden und privaten Partnern
- Prävention – nicht gezielt genug

Die aufgetretenen Schwierigkeiten

Auf Schweizer Ebene

- Blockieren von betrügerischen Anzeigen im Internet
- Kontrolle von Geldflüssen
- Fristen für die Aufbewahrung
- Internationale Rechtshilfe und Dauer bis zur Rechtshilfe

Fragen?

Kom Matthieu Landert
Police de sûreté-*Kriminalpolizei*
Kommissariat Cyberkriminalität
Place Notre-Dame 2, 1701 Fribourg
T +41 26 305 16 61, www.policefr.ch|
cybercrime@fr.ch|—