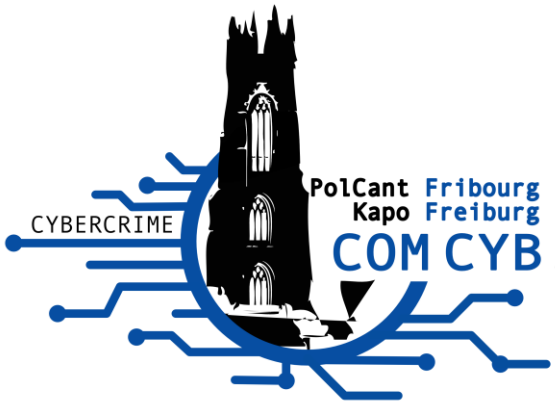
Présentation à l'intention

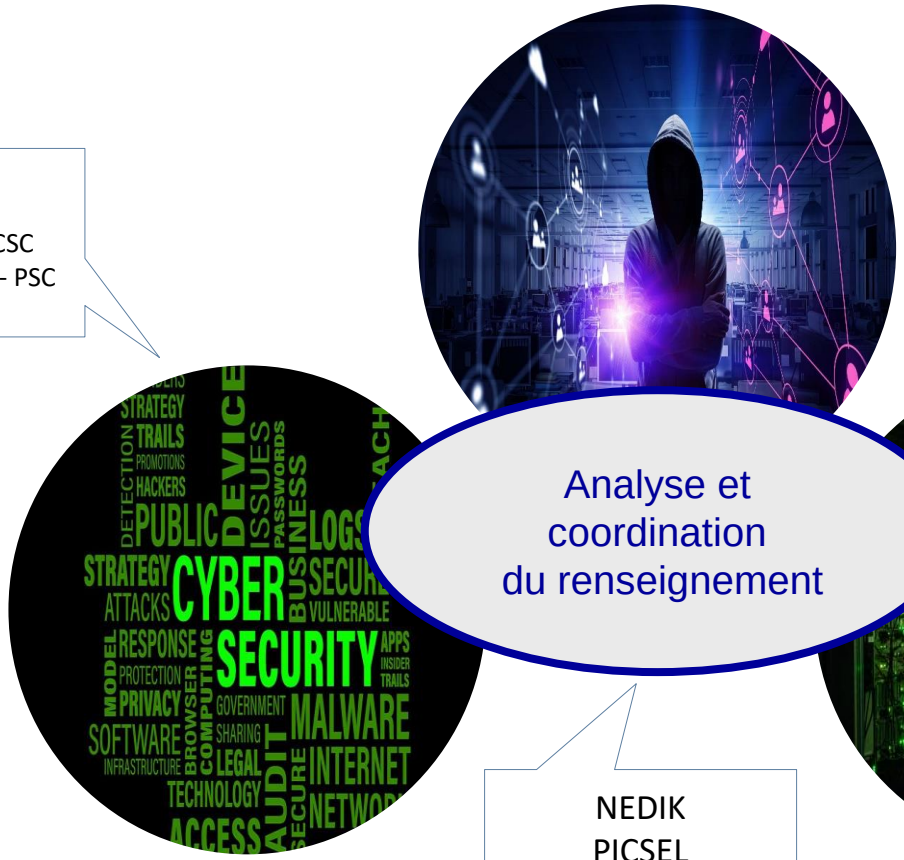
des directions INFRI

16.12.2022, Fribourg



Tables des matières

Mise en application de la stratégie



NCSC
SKP - PSC

Polices cantonales
Centres de compétences régionaux
Fedpol
Cybercase / Cyberboard

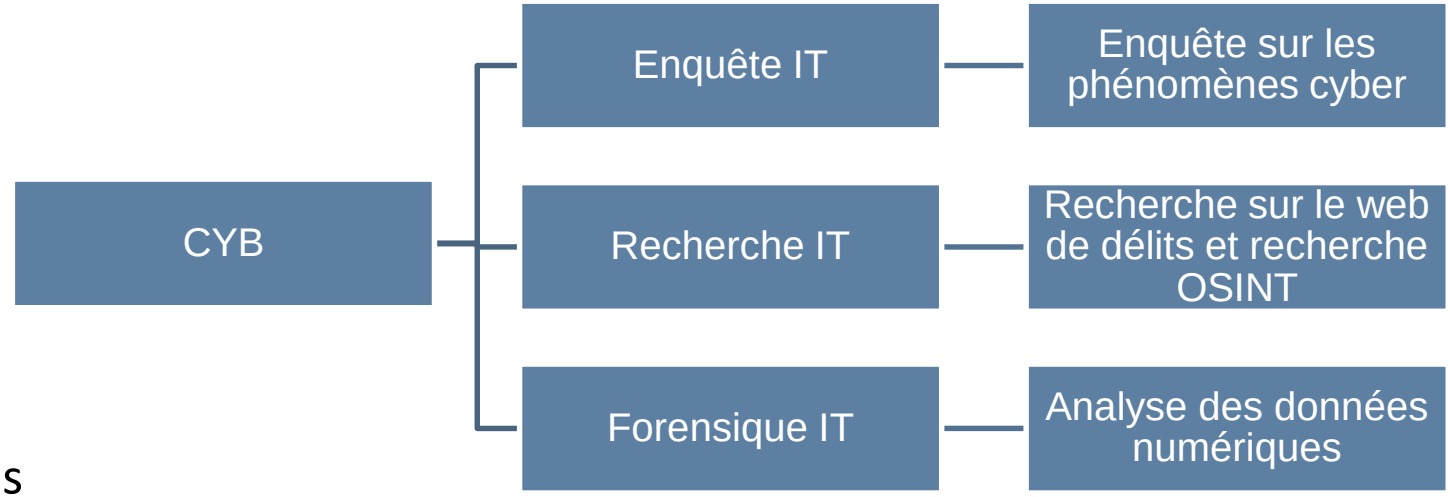
Analyse et coordination du renseignement

NEDIK
PICSEL

DDPS - BAC - Base aide au commandement

Lutte contre la cybercriminalité à Fribourg

Commissariat Cybercriminalité (CYB)



Tâches

1. Prévenir
2. Enquêter
3. Analyser
4. Rechercher
5. Collaborer

Lutte contre la cybercriminalité à Fribourg

Chaque policier fribourgeois est amené à traiter de la cybercriminalité

Il dispose de:
- Formation de base
- Document « plainte pénale cyber »
- Le soutien du Commissariat Cyber pour les cas complexes
- De bases légales permettant la dénonciation

Cybercrime dans le canton de Fribourg

2019 | **529** Plaintes Cyber | ~ CHF 2’940’000.00
2020 | **570** Plaintes Cyber | ~ CHF 2'510‘000.00
2021 | **804** Plaintes Cyber | ~ CHF 7’190’000.00
…
581 plaintes cyber entre janvier et août 2022

Ransomeware

Phase 1

- Le hackeur envoie un email malveillant
- L'email passe les filtres de spam de la victime
- La victime ouvre l'email

Phase 2

- La victime télécharge la pièce jointe
- L'antivirus ne repère pas le danger
- Le ransomware contacte le serveur pour avoir la clé de chiffrement
- Les données de la victime sont chiffrées
- La clé de chiffrement sur l'ordinateur de la victime est détruite

Phase 3

- Un message s'affiche sur l'ordinateur de la victime qui demande une rançon pour récupérer ses données
- Si on paie, normalement on récupère la clé de chiffrement qui permet de déchiffrer nos données
- Si on ne paie pas, nos données resterons chiffrées et mise sur le dark-deepweb

https://youtu.be/v-ITcpD1KcQ

Ransomeware

1. En cas de divulgation de données confidentielles de nos collaborateurs ou résidents ou d'un constat de cyber-attaques, quels sont les premiers réflexes à avoir dans une telle situation ? Est-ce que la police est compétente pour nous aider ou est-ce le fait d'un acteur privé ? Nous avons un fournisseur de service tiers, est-ce à lui de faire les démarches dans ce cas ? Comment sont réparties les compétences et responsabilités ?
    - Alarmer la Police
    - Stopper / éteindre
    - Police: conseille, récolte de traces et aide à la gestion du ransomeware
    - Informer la préposée aux données
    - Pas de remise en place de l'infra par Police mais par prestataire privé

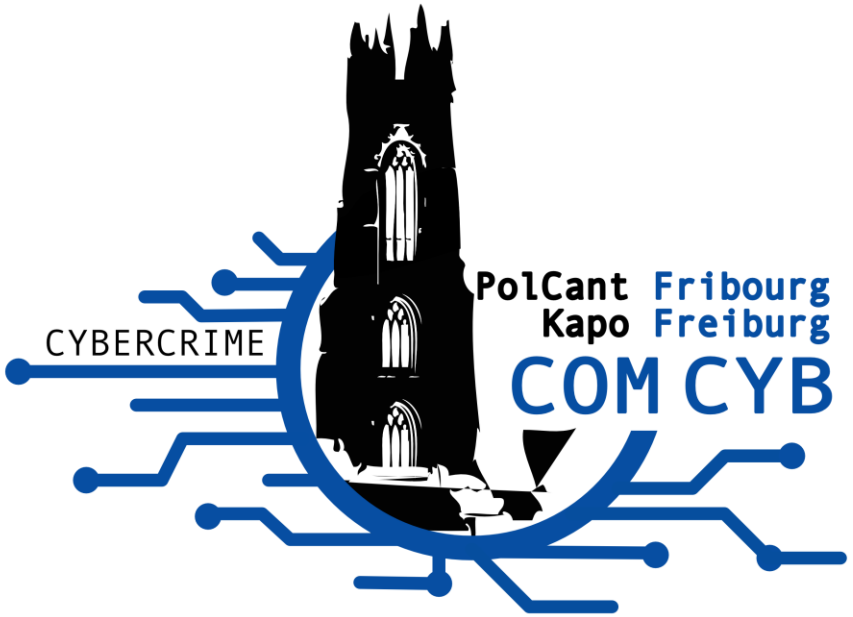
2. Quelles sont les attentes en matière de gestion de crise ?

Appeler la police, avoir les bonnes personnes présentent de l'entreprise / l'institution, être prêt à informer. Nous faire confiance, nous écouter.

3. Vaut-il mieux payer la rançon ou pas ?

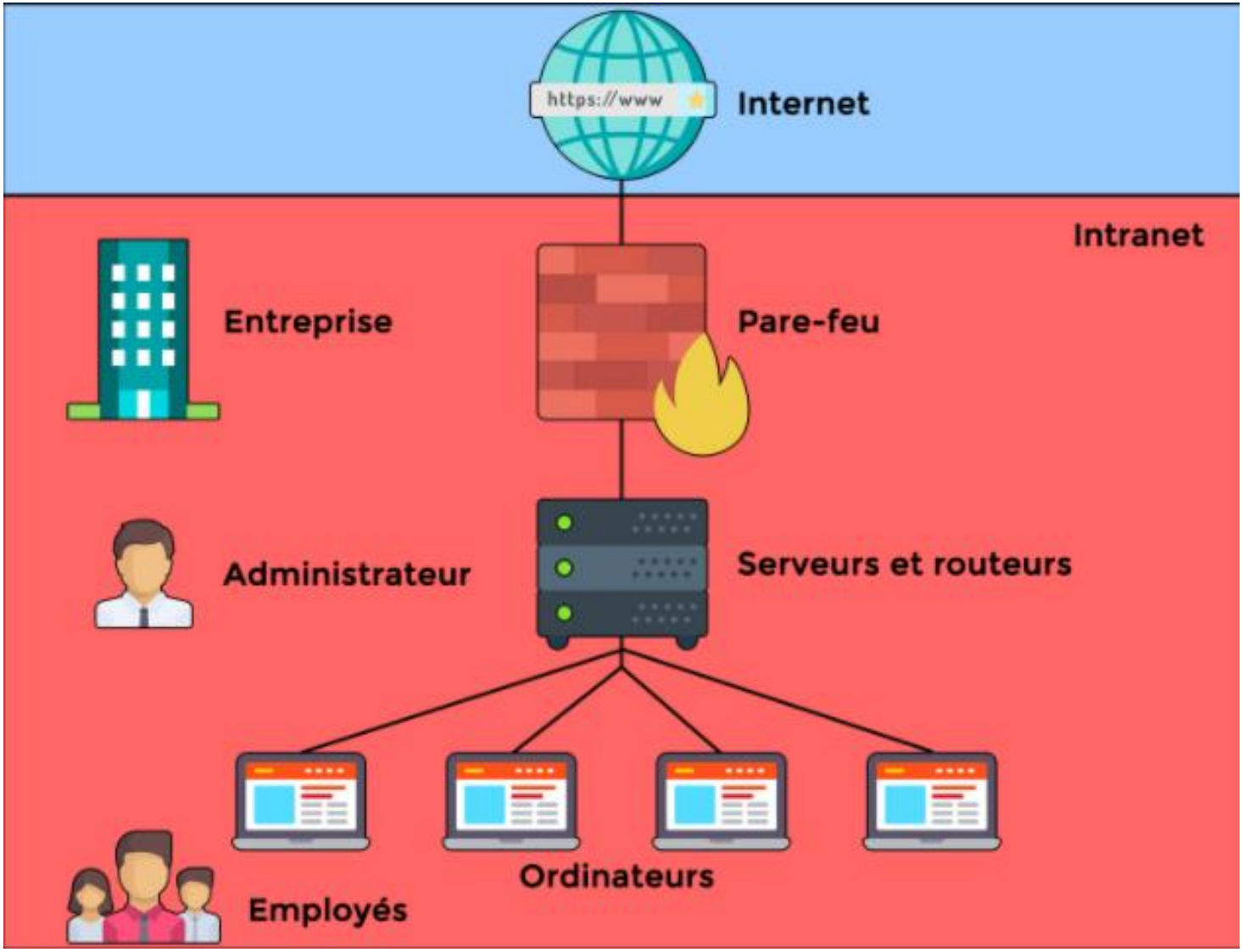
Non, il est jamais conseillé, sauf si pas le choix. Selon gouv US qualifié de soutien aux crimes organisés, donc plus possible de faire des deals au US….

Cybersécurité



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

Sécurité


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

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

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.

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

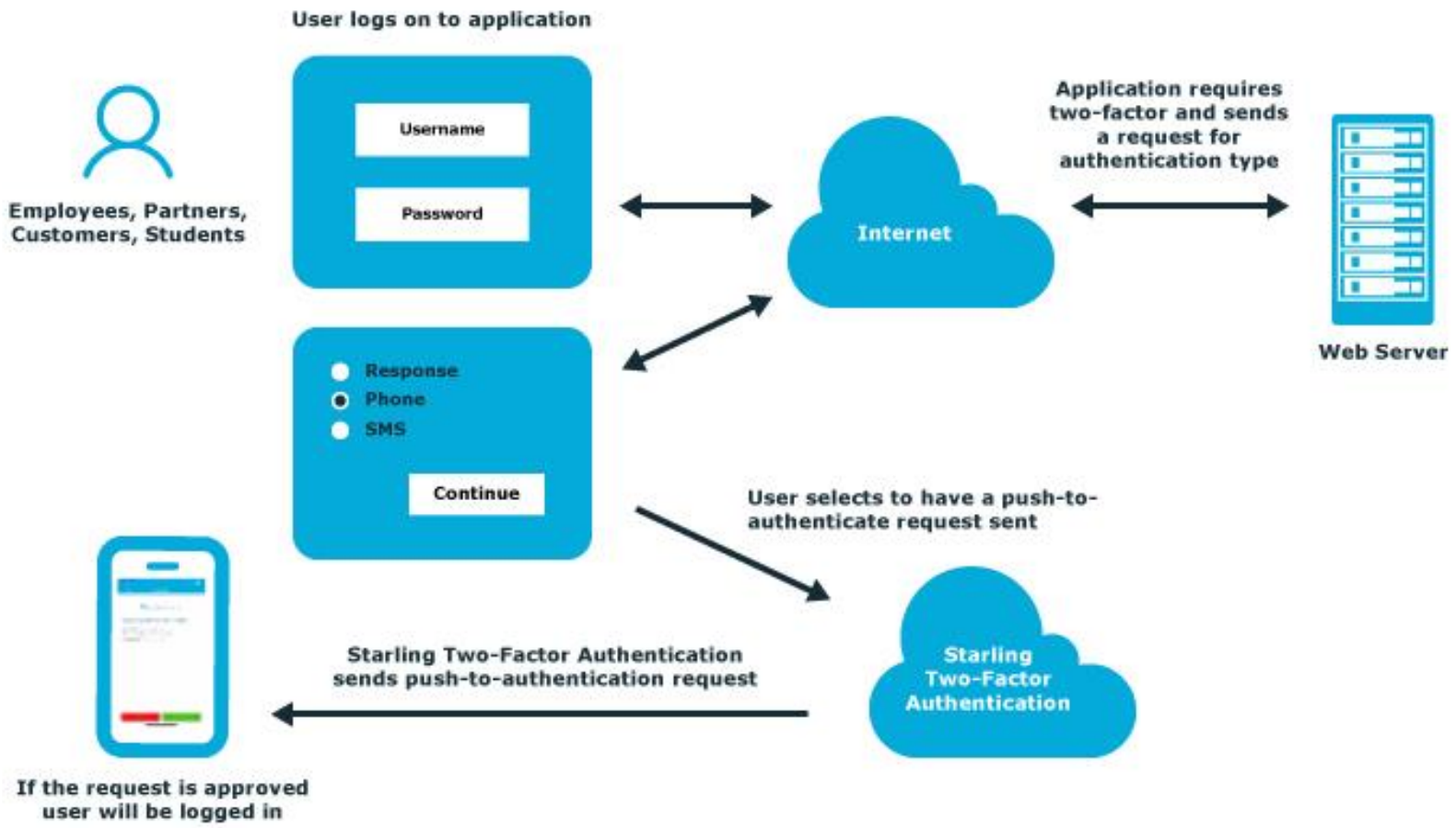
Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

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.

Department for Business Innovation & Skills | CPNI Centre for the Protection of National Infrastructure | Cabinet Office

Double authentification



Smartphone et sécurité

1. Verrouillage du téléphone
2. Pas de mots de passe sur les supports
3. Pas le même mot de passe pour plusieurs utilisations
4. Pas d’enregistrement automatique de mots de passe
5. Effectuer les mise à jour
6. Pas d’ouverture de lien ou de document

Choisir et gérer ses mots de passe

1. Mot de passe fort avec caractères, signes, majuscule, et au min 9
2. L’enregistrement de mot de passe uniquement sur des outils sécurisés
3. Pas de création de mot de passe automatique gratuit
4. Changement régulier de mots de passe
5. Ne pas enregistrer vos mots de passe sur votre moteur de recherche
6. Utiliser la double authentification / validation

Arnaque aux faux supports techniques

1. Vérifier l’adresse et l’expéditeur
2. Effectuer des questions de contrôle
3. Vous avez besoin d’aide, pas l’inverse
4. Pas d’action urgente ou sous pression
5. Ne rien installer
6. Attention : ce qui est gratuit est sponsorisé ou piégé

Protection

1. A part les anti-virus, existe-t-il des solutions pour protéger les ordinateurs ?

J'ajouterais un EDR.

2. Quelle serait la configuration idéale actuelle pour garantir un maximum de sécurité ? 2 règles de base.

La meilleure sécurité sans la meilleure formation n'a pas de chance. Si l'on veut vraiment, on arrivera à entrer.

3. Sur le serveur, faut-il changer régulièrement le firewall ?

Mettre à jour mais pas changer.

4. Est-il préférable d'héberger les données sur un serveur en local ou sur le cloud ou mandater une entreprise spécialisée ?

Pour la protection des données sur un serveur, le mandat dépend de la capacité interne de mettre à jour et effectuer la maintenance du système.

Protection

4. Sinon de notre côté nous avons mis en place un changement périodique des mots de passe et une authentification renforcée, quels autres moyens pourraient être explorés ?

Double authentification / validation, enregistrement des données, identification par géolocalisation. Mot de passe à changer tout les 60-90 jours. La meilleure sécurité sans la meilleure formation n'a pas de chance. Si l'on veut vraiment on arrivera à entrer.

5. Pour les collaborateurs qui se connectent sur le réseau de l'entreprise depuis leur ordinateur ou téléphone portable, les risques sont-ils plus grands ? Que faire ?

Non, si le matériel est fourni par la société et maintenu à jours par la société. Si c'est du matériel privé alors oui, les risques sont très élevés. Mettre à jour mais pas changer.

6. Que mettre en place de concret pour lutter efficacement contre la cybercriminalité ?

Formation, système à jour, sauvegarde correct et viable. Le serveur de sauvegarde s'active lui-même, va chercher les données et s'éteint de nouveau de lui-même. Pas le serveur principal qui va poser les données.

Protection

7. Peut-on prendre des mesures dans l'infrastructure informatique pour qu'un piratage éventuel ne touche pas tous les secteurs de l'institution ?

Le cloisonnement des services…

8. Définition des données sensibles ou non ? (lorsque je pense à un dossier bénéficiaire par exemple)

Par exemple pour Police : données personnelles sont sensibles, le reste pas.

9. Quelle est la part d'ingénieurerie sociale, d'erreur humaine dans la cybercriminalité ? Quelles sont les meilleurs outils de prévention au sein d'une entreprise ?

80% humaine, 20% mise à jour des systèmes mais nous ne voyons pas d'attaques physiques.

10. Transmission sécurisée et informatisée des bilans, rapports, entre institutions : quels dispositifs ?

Si par mail, alors chiffrement du mail et de la pièce jointe. Sinon sharepoint avec double authentification.

Télétravail sans risque

1. Wifi sécurisé
2. Mot de passe changé
3. Recommandation de l’entreprise
4. Verrouiller le PC
5. Ranger les documents de travail

Sécurité

1. Quels seraient les « signes » d'alerte ou « avant-coureurs » ?

Les systèmes sont de plus en plus intelligents et volent petit à petit les informations pour ne pas être détectés par le monitoring du système.

2. Quels sont les avantages / inconvénients d'un stockage de données sur des serveurs physiques ou dans un cloud ? Un moyen est-il préconisé ?

Serveurs physiques demande plus d'investissement et de maintenance alors que le cloud propose déjà dans leurs forfaits. Les sauvegardes sont souvent également automatisées. La protection des données doit être vérifiées.

3. Du côté des mails contenant des virus, quels moyens pour les détecter s'il y en a ?

Office 365 propose un Sandbox qui effectue une sorte d'analyse du fichier mais de base, uniquement la méfiance de l'utilisateur permet la détection.

Assurance

CYBERCRIME
PolCant Fribourg
Kapo Freiburg
COM CYB

Assurance

1. Doit-on s’assurer contre ce genre de risques ?

C’est préférable. Une assurance va de 2000-10000 par an et couvre la remise en état et pour certaines un petit montant du Ransomeware.

Assurance

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.

Sous l'angle du Code pénal suisse, il n'y a, à mon sens, pas de disposition qui permettrait de réprimer un tel cas de figure.

L'examen doit ainsi se faire sous l'angle de la loi sur la protection des données (LPD).

Dans sa version actuelle, les dispositions pénales qu'elle contient, figurant aux art. 34 et 35 LPD, ne permettent pas non plus de réprimer une telle situation
(cf. https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/fr)

Il en ira autrement à partir du 1er septembre 2023, date d'entrée en vigueur de la nouvelle LPD (ci-après : nLPD - https://www.fedlex.admin.ch/eli/fga/2020/1998/fr

En effet, l'art. 61, plus particulièrement sa lettre c, permettra de réprimer les personnes privées qui, intentionnellement, ne respectent pas les exigences minimales de sécurité des données édictées par le Conseil fédéral. A cet effet, il convient de se référer à l'art. 8a l. 3 de la nLPD qui lui-même renvoie aux art. 3ss de la nouvelle Ordonnance sur la protection des données du 31.08.2022.

Pour de plus amples informations, je vous invite à consulter le liens suivant :
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 – Formation

CYBERCRIME
PolCant Fribourg
Kapo Freiburg
COM CYB

Phishing

1. Vérifier l’adresse et l’expéditeur
2. Vérifier le contenu du mail mais ne pas ouvrir de pièces jointes
3. Ne pas ouvrir de lien URL ou internet
4. Appeler l’entreprise ou le fournisseur normal pour vérifier de l’autanticité

Formation

1. Nous envisageons de tester nos collaborateurs en envoyant un mail pseudo pirate afin de voir quel pourcentage de personnes ouvriront la pièce jointe ? Est-ce légal ?

A ma connaissance ceci n'est pas illégal. Je regarderai juste que le fichier ne serve par la suite pas à surveiller les collaborateurs.

2. Serait-il envisageable d'organiser, en commun, des formations ou e-learnings pour les collaborateurs quant aux comportements à adopter face à la cybercriminalité ?

Tout est possible.

3. Nous avons axé la prévention contre les cyber-attaques auprès des collaborateurs de notre entreprises dans notre entreprise sur 3 axes : 1. Double authentification sur nos systèmes / 2. Prévention-information au sujet des logiciels malveillants tels que pièces jointes / 3. Information sur les techniques d'ingénieurerie sociale (p.ex. appels téléphoniques frauduleux). Est-ce cohérent avec le contexte actuel ?

Parfait. Ajouter les mots de passe et authentification par géolocalisation. Formation en présentiel serait idéal, les mails ne servent souvent pas assez.

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

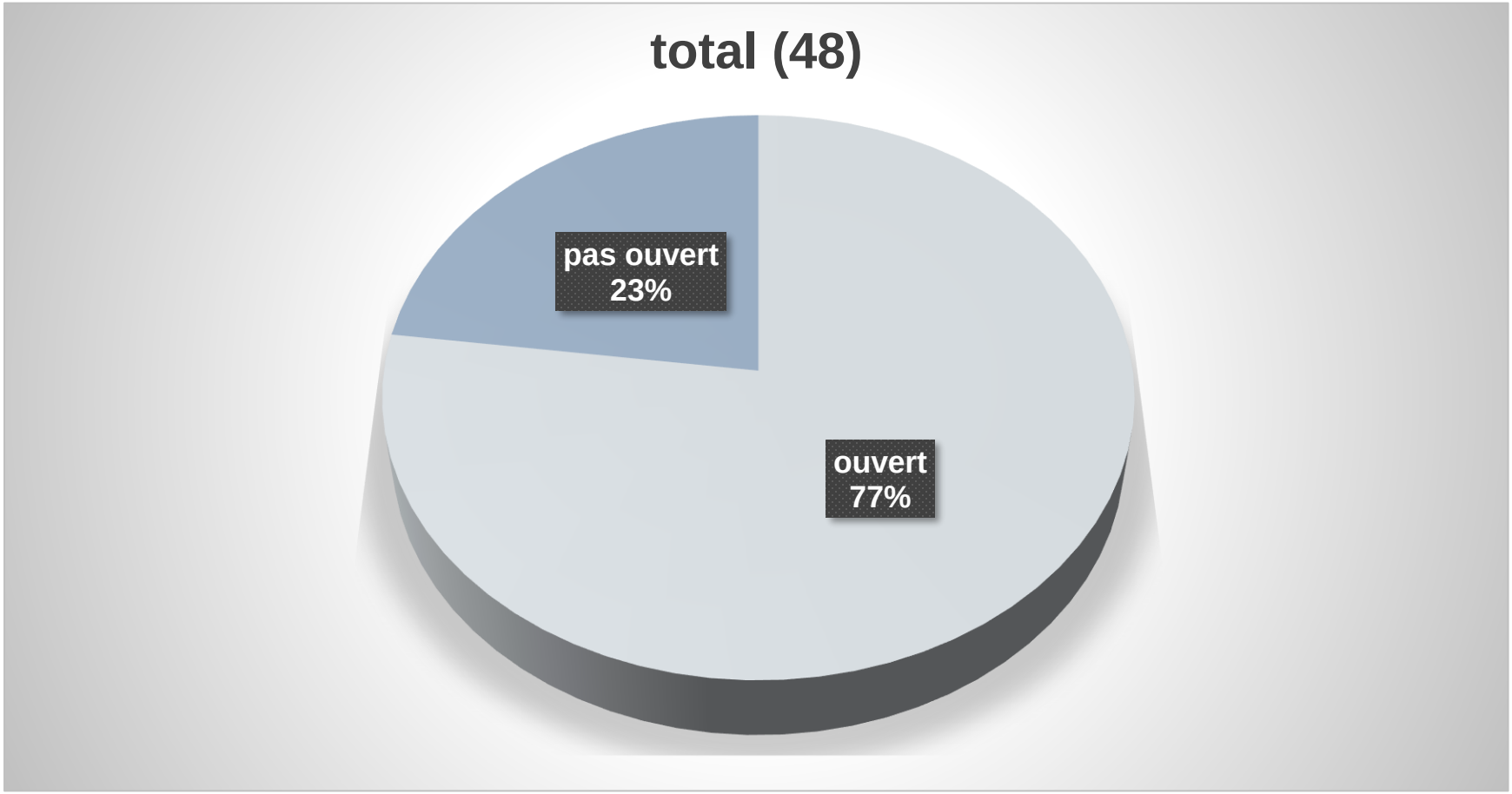
Veuillez prendre un moment pour examiner la section en gras de la plainte, concernant le respects des exigences minimales en matière de sécurité des données édictées par le Conseil fédéral selon l'art. 8, al. 3.

Cordialement,

Préposé fédéral à la protection des données

Phishing du 13.12.22

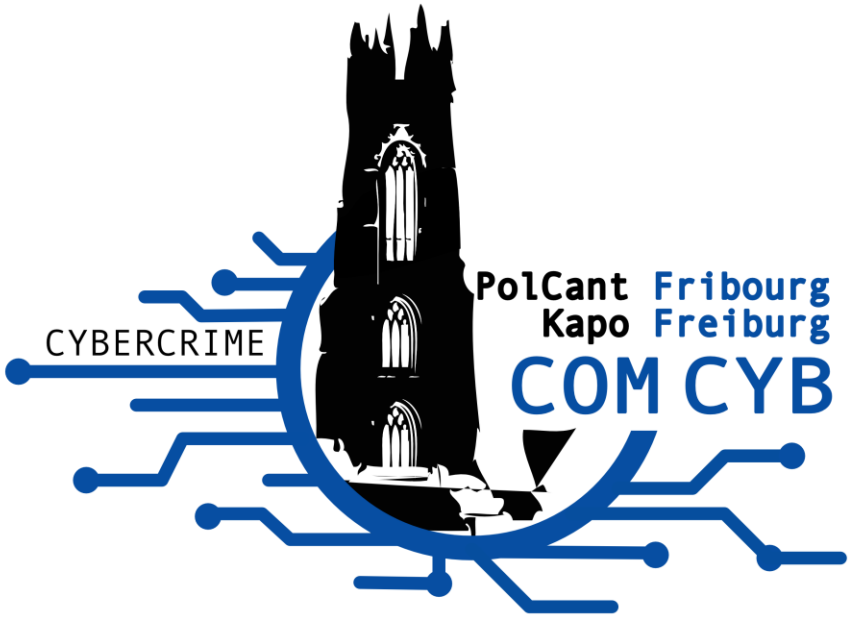
Phishing du 13.12.22



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
```

Les défis



Les difficultés rencontrées

- Tous est cyber mais presque rien n’est vraiment cyber
- Modification constante des attaques cyber et outils utilisés
- Manque de connaissances et de compréhensions des lésés et futurs lésés
- La rapidité nécessaire pour tenter d’empêcher des transactions

Les difficultés rencontrées

Au niveau national

- Base de données partielle (identification de séries)
- Séquestre des cryptomonnaies
- Monitoring - Collaboration avec les autorités et les partenaires privés
- Prévention – pas assez ciblée

Les difficultés rencontrées

Au niveau international

- Blocage d’annonces frauduleuses sur internet
- Contrôle des flux financiers
- Délais de conservation
- Entraide internationale et durée jusqu’à l’entraide

Questions?

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