CYBER RISK : LA NÉCESSAIRE PRÉVENTION

Benoît Lonay

Account Manager

Municipalia, Marche en Famenne, 30 septembre 2021

Ethias MEMBERS' ACADEMY

LE PROGRAMME :

1. **Le contexte**
2. **Quels niveaux de protection mettre en place ?**
    1. Classique et classique … amélioré
    2. Innovant
3. **Quelle sensibilisation / formation envisager ?**
4. **La CCU et son rôle**
5. **Un retour du marché de l'assurance face à une augmentation du risque**
6. **Quelles initiatives la Région Wallonne peut-elle proposer ?**
7. **Conclusions**

Ethias MEMBERS' ACADEMY

1. CONTEXTE : LES CYBER ATTAQUES

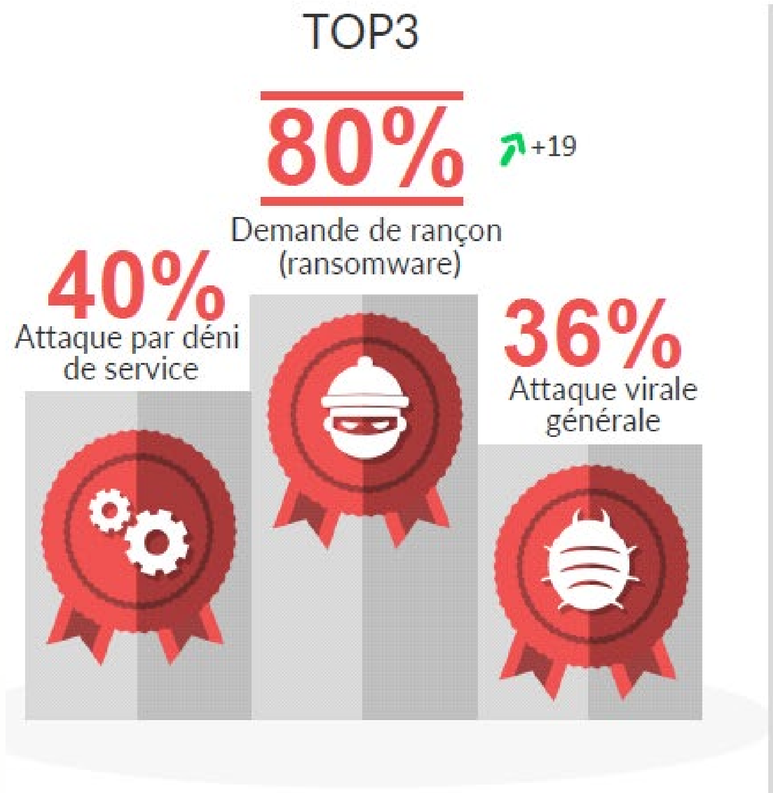
- **Pour l'année 2020, le Centre belge pour la cybercriminalité (CCB) a reçu 7.433 signalements de cyber incidents (contre 4.484 en 2019): en cause le télétravail.**
- **2/3/2020 : l'ULB victime d'une cyberattaque**
- **25/1/2020 : La commune de Willebroeck est victime d'un ransomware**
- **Dimanche 17/1/21 : CHU Ambroise…**
- **12/02/2021 : Ville de Seraing, à l'arrêt plusieurs jours**
- **14/3/21 : piratage via la messagerie « Exchange Microsoft »** des PME, des zones de police, des conseils communaux et même un de nos parlements concernés.
- **Floreffe** en 2021
- **Ville de Liège** le 21 juin dernier …

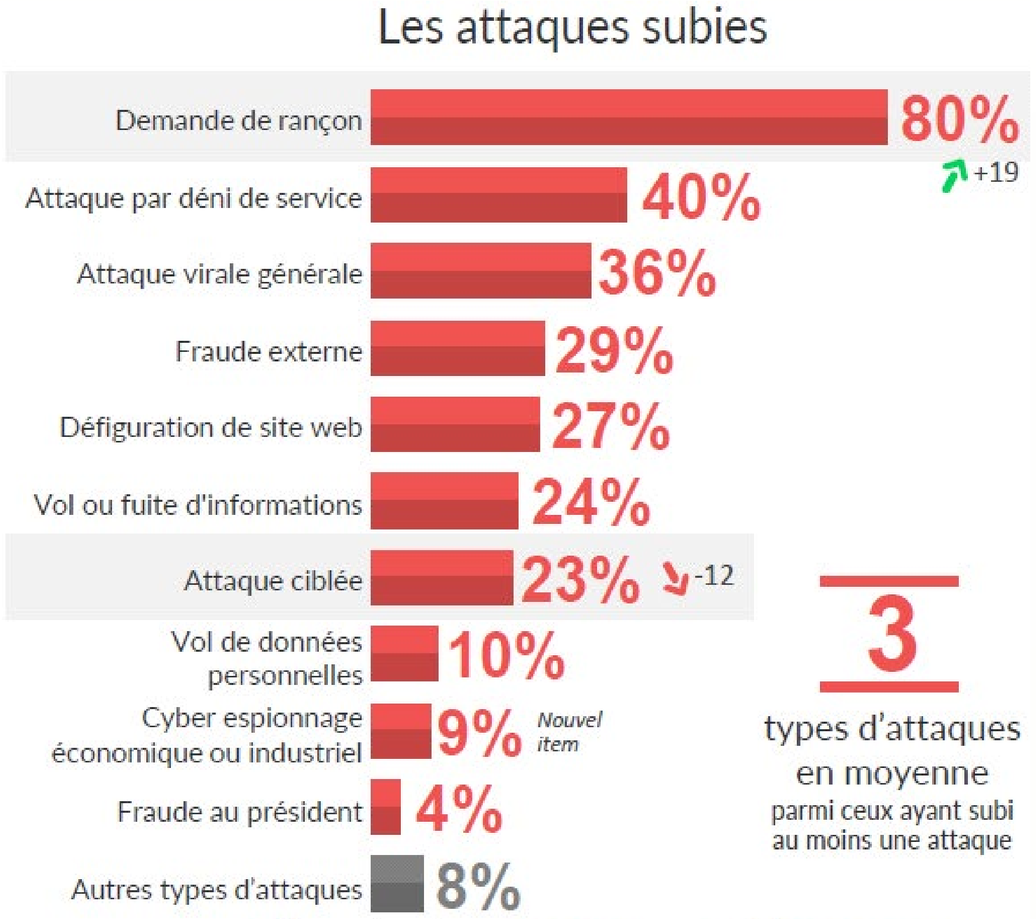
4 mai 2021 : Parlement fédéral, universités, hôpitaux, centres de recherches… Le réseau Belnet victime d'une cyberattaque (DDoS) de grande ampleur

Ethias MEMBERS' ACADEMY

1. CONTEXTE - LES TYPES DE CYBERATTAQUES

Les attaques les plus courantes :





Source : Curtispc.fr

Ethias MEMBERS' ACADEMY

QUESTION BREAK

Réactions ?

Avez-vous été victime d’une attaque ?

Ethias MEMBERS’ ACADEMY

1. CONTEXTE : LES LÉGISLATIONS

Directive SRI (9/2017) : garantir un niveau de sécurité élevé dans l'ensemble de l'UE. Notamment par une meilleure gestion des risques et par la notification des incidents.

RGPD (25/5/2018) :

- Renforce les anciennes dispositions « Vie Privée »
- Impact très important sur l'organisation interne
- Une foule d'exigences à mettre en place mais diverses formes de sanction…
- … Toutefois secteur public belge exonéré d'amendes (décision contestée)

⇨ 2 principes : Sécurité / maturité « IT » et responsabilité

Ethias MEMBERS' ACADEMY

QUESTION BREAK

Pensez-vous que les législations tels que le RGPD entraînent des risques financiers et des contraintes administratives ?

Ethias MEMBERS' ACADEMY

2. QUELS NIVEAUX DE PROTECTION METTRE EN PLACE ?

3.1. Protection classique

Idée :

Assurer un risque marginal le plus faible possible grâce à des éléments techniques « IT » de protection.

Processus classique :

Questionnaire ⇨ Analyse questionn. ⇨ Projet si analyse fav. ⇨ Décision client

2. QUELS NIVEAUX DE PROTECTION METTRE EN PLACE ?

2.1 Classique mais avec assessment poussé et suivi des mesures

Pour les risques plus importants, une analyse du risque plus poussée est requise. Ceci passe généralement par :

- **Questionnaire discuté lors d'interview(s)**
- **Visites sur place**
- **Testing (« white hacker »)**

  → Rapport avec recommandations
- **Le tout revu régulièrement**

Ethias MEMBERS' ACADEMY

2. QUELS NIVEAUX DE PROTECTION METTRE EN PLACE ?

2.2 Innovant

Solution innovante mise en place à l'intérieur du groupe Ethias dont font partie NRB/Civadis.

Civadis propose deux formules spécifiques de gestion des risques de cyber sécurité :

- Le « carnet d'entretien étendu »

- La solution cloud : « CivaCloud »

Si le client a souscrit à l'une de ces deux solutions, il peut recevoir une offre « Ethias Cyber Protection » sans qu'il lui soit nécessaire de compléter le questionnaire.

Par ailleurs, il bénéficiera d'une réduction de la prime d'assurance.

~~Questionnaire~~ ⇨ ~~Analyse questionn.~~ ⇨ Projet ~~si analyse fav~~. Et -10% ⇨ Décision client

Ethias MEMBERS' ACADEMY

A titre d'exemple : contenu du Carnet d'entretien étendu

	Garantie constructeur	Maint. Civadis	Carnet entret. étendu
Civadis - Rôle d'intermédiaire avec constructeur	👍		
Remplacement pièces défectueuses (main d'œuvre et déplacements)	👍		
ServiceDesk pour incidents Hardware	✗	👍	
Prêt de matériel en cas de crash majeur (Serveur, NAS, Firewall, Switch)	✗	👍	
Restauration des données à partir des sauvegardes en cas de panne Hardware	✗	👍	
Sensibilisation risques sécurité	✗	✗	👍
Inventaire des éléments du « Datacentre » + statut contrats maintenances	✗	✗	👍
Révision des utilisateurs et de la sécurité des accès aux données	✗	✗	👍
Mises à jour des logiciels systèmes : VMWare, Windows, Veeam, Antivirus	✗	✗	👍
Validation du fonctionnement des UPS des serveurs	✗	✗	👍
Mises à jour des éléments critiques : NAS (backups), Serveurs, SAN, …	✗	✗	👍
Test annuel de reprise d'activité (restauration des serveurs « Civadis »)	✗	✗	👍
Monitoring temps réel des serveurs et éléments critiques	✗	✗	👍

CIVADIS
SOLUTIONS IT POUR LES AUTORITÉS LOCALES

Ethias MEMBERS' ACADEMY

3. FORMATION ET SENSIBILISATION

Nous avons plusieurs expériences dans ce domaine.

Partenaire 1 - objectifs :

Sensibiliser et susciter la curiosité

<u>Exemples :</u>

- **Les menaces / type d’attaque & conséquences**
- **Focus sur l’Internet des objets (facilitent les tâches mais la sécurité est faible)**
- **Trucs & astuces**

Ethias MEMBERS’ ACADEMY

Les principales catégories de risques

Solutions

Risques humains

- Effacement des données, piratage…
- Vol, vandalisme…
- Crypto-virus…

> **Sensibilisation des utilisateurs**
> **Solutions techniques**
> **Cyber-Assurances**

Risques environnementaux

- Incendies, foudre…
- Inondations
- Explosion de gaz

> **Solutions techniques**
> **Tests de reprise d'activité**
> **Assurances**

Dysfonctionnements matériels

- Panne disque dur
- Panne du système de refroidissement de la salle…

> **Solutions techniques**
> **Contrats de maintenance**
> **Entretien préventif des infrastructures**

Ethias MEMBERS' ACADEMY

4. FORMATION ET SENSIBILISATION - SUITE

Partenaire 2 - mémento « Les 10 bonnes pratiques en Cyber sécurité »

Recueil de 10 pratiques de base :

1. **Mot de passe**
2. **E-mails et phishing**
3. **Sécurité physique de vos appareils**

Etc

Cf. livrets à disposition.

Citons aussi les formations données par UVCW en cette matière (articles, webinaires, formations, etc.)

Ethias MEMBERS' ACADEMY

5. LA COMPUTER CRIME UNIT (CCU) ET SON RÔLE

Federal Computer Crime Unit (CCU)

1. Les **RCCU (Regional Computer Crime Unit**) soutiennent à la fois la Police Fédérale et la Police Locale dans l'analyse du matériel informatique saisi dans le cadre de dossiers judiciaires. Elles enquêtent également sur la cybercriminalité au sein de leur arrondissement judiciaire.

2. Federal Computer Crime Unit (FCCU) mène des enquêtes et fournit un appui aux divisions d'enquête des services centraux.

Les *« geeks »* de la FCCU ont notamment pour tâches :
- ✓ d'entretenir un réseau de partenaires / contacts
- ✓ cartographier les cyber menaces
- ✓ de mener des enquêtes judiciaires complexes visant des organisations cybercriminelles et d'identifier les hackers responsables des attaques

D'autres missions sont tournées vers l'avenir comme la connaissance de l'IoT (*Internet of things* ou l'internet des objets), le développement d'AI (*artificial intelligence* ou IA pour intelligence artificielle) notamment

https://www.police.be/villagepolicier/fr/police-federale/federal-computer-crime-unit

5. LA CCU ET SON RÔLE

Signaler un incident de cyber sécurité

1. Déclaration à la police locale qui vous orientera et fera appel éventuellement à RCCU ou FCCU

2. Le CERT

https://www.cert.be/fr/signaler-un-incident

Qu'est-ce que la CERT.be ?

La Computer Emergency Response Team fédérale, ou CERT.be, est le service opérationnel du Centre pour la Cyber sécurité Belgique (CCB). CERT.be est chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne ainsi que d'informer en permanence à ce sujet.

CERT.be fournit des services réactifs, proactifs et de gestion de la qualité de la sécurité dans le domaine de la cyber sécurité.

3. Fuite de données à caractère personnel : déclaration à faire auprès APD

https://www.autoriteprotectiondonnees.be/notifier-une-fuite-de-donnees

QUESTION BREAK

Retour de la salle : avez-vous mis en place d'autres moyens de prévention ?

Des questions sur les moyens présentés ?

Avez-vous suivi une formation / sensibilisation ?

Qui a déjà fait appel à la CCU ?

<u>Remarque :</u> Obligation de porter plainte dans le produit Ethias en matière de Ransomware

Ethias MEMBERS' ACADEMY

ethias |

6. UN RETOUR DU MARCHÉ DE L'ASSURANCE

Devant la fréquence accrue des attaques, la réaction des compagnies :

- **Majoration des franchises**
- **Limitation des capacités (c.à.d. des limites d'intervention)**
- **Suppression de la garantie Ransomware**
- **Plus grande exigence en matière d'analyse préalable (assessment, suivi…)**
- **Majoration des primes ?**
- **La réassurance épingle le Cyber Risk, avec les changements climatiques, comme un grand défi et estime que le marché a besoin de plus de résilience (LLB 14/9/21)**

Vers quelle(s) évolution(s) ?

Ethias MEMBERS' ACADEMY

7. QUELLES INITIATIVES DE LA RÉGION WALLONNE ?

Dans le cadre de « Get Up Wallonia ! », la Région a mis à disposition :

- **Budget de 10M€ entre 09/2020 et 09/2021 pour équiper les commues et CPAS en matériel IT (Up Grade, dont cyber sécurité) : hardware et software + mise en conformité des sites internet + formation au télétravail notamment.**
- **Collaboration UVCW et RW : formations annuelles pour les agents et les élus (cyber, RGPD, gestion des données etc.)**
- **Idée générale : des budgets annuels pour améliorer l'IT mais aussi mettre en place des projets de plus grande ampleur « Digital Wallonia »**

2 Ministères traitent de ce sujet :
Ministère de l'Economie, du Comm. Ext, Innovation et Numérique (W. Borsus) et
Ministère du Logement et des Pouvoirs Locaux & Ville (Ch. Collignon)

7. QUELLES INITIATIVES DE LA RÉGION WALLONNE ?

A l'avenir :

- **Accord TOP (taxes on pylones) entre les opérateurs de télécoms et la RW visant à améliorer la couverture digitale et mobile en Wallonie mais aussi à soutenir la transition numérique des pouvoirs locaux. Y compris amélioration de l'architecture IT. Le tout via appel à projet. 10M€**
- **Projets plus structurants en vue de se diriger vers « Smartcities », « connectivité avancée », « Portail régional Digital Wallonia Connect », « wi-fi urbain », etc.**
- **Restez attentifs aux déclarations futures du Ministre des Pouvoirs Locaux… nouveaux budgets, projets à remettre, baromètre de maturité « cyber »…**

8. CONCLUSIONS

Le risque « Cyber » est aujourd'hui tel qu'il n'est plus possible de le transférer à l'assureur de façon classique.

Nous avons vu, à travers les différents acteurs repris dans cette présentation, qu'une prise en charge par l'assuré / collectivité locale publique est désormais nécessaire.

Ceci doit notamment prendre la forme d'une maturité organisationnelle et technique plus poussée.

Dans ce cadre la prévention devient une nécessité incontournable.

Des aides et solutions existent !

Ethias MEMBERS' ACADEMY

ETHIAS CYBER PROTECTION

ethias

Question break

EXPERTISE & PROXIMITÉ

www.ethias.be/**membersacademy-fr**

ethias

EXPERTISE & PROXIMITÉ

www.ethias.be/**membersacademy-fr**

ethias