ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Criminalité économique et cyber-risques : ma PME passe à l'action

Et si vous misiez sur vos employés ?

25 juin 2020

Isabelle Augsburger-Bucheli, Sébastien Jaquier

Hes·so

ilce - institut de lutte contre
la criminalité économique
heg - haute école de gestion

Au menu

- L'ILCE de la HEG Arc en bref
- Criminalité économique: les faits sont têtus !
- Criminalité économique et cybercriminalité
- Phénomènes cybercriminels touchant les entreprises
- La responsabilité du dirigeant en matière cyber
- La digitalisation n'est plus une option,
  penser sécurité de l'information non plus !
- Pourquoi miser sur l'Humain et donc sur vos employés ?
- Exemples de mesures élémentaires au niveau de l'entreprise, « Bonne hygiène cyber » au travail à l'usage du dirigeant et de l'employé

Hes·so

Structure de l'ILCE (chiffres 2019)

ILCE
2000
I. Augsburger-Bucheli

+ 130
intervenants

+ 600
personnes ont suivi un cours ou un colloque

131
personnes en formation PG

ERMP
2007
R. Weber

ERAJ
2010
R. Weber

CINC
2010
R. Roubaty

MAS LCE: 30
CAS IF: 4
CAS CEP: 53

CAS MAP: 24

CAS AJP: 10

5 CAS IN: 10
CAS CY: NEW !

\+ Colloques et Conférences
Cours spécialisés
Mandats et Ra&D

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Mandats 2018-2020

- Analyses et expertises effectuées par le CINC
- Avis de droit – expertises
- Mandats en finance et fiscalité
- Concept de formation Cyber pour policiers réalisé par l'ILCE
  - Collaboration à la réalisation d'un eLearning pour 18'000 policiers
  - Participation à un pilote de formation cyber pour enquêteurs
- eCyAd: projet de formation en ligne en matière de cybersécurité pour administrations cantonales et communales

- Formations spécifiques sur mandat : par ex.,
  - Formation du personnel en entreprise (cybersécurité)
  - Stratégie de sécurité de l'information à l'attention du Conseil d'administration
  - Bonnes pratiques en matière informatique à l'usage du magistrat
  - La face cachée du Net pour membres de la poursuite pénale

Institut suisse de police
Istituto svizzero di polizia
Swiss police institute
Schweizerisches Polizei-Institut

Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Ra&D 2018-2020

- Projet: www.coronafraud.ch
- L'arnaque aux sentiments à l'ère du Covid-19
- Valorisation du projet « Abus financiers contre les seniors »
- Projet RCSO: « Prévenir et lutter contre les abus financiers envers les seniors en Suisse »
- Projet RCSO: « Redflags d'avoirs illicites de potentats »
- Valorisation du projet « The future of blockchain – synergy between the legal and technical challenges» (ILCE + HE-ARC Ingénierie) (bootstrap HE-ARC)
- « Fraude médicale en Suisse: étude exploratoire » (ILCE + HE Arc Santé) (bootstrap HE-ARC)

Criminalité économique et cybercriminalité
Un vecteur d'infection foudroyant

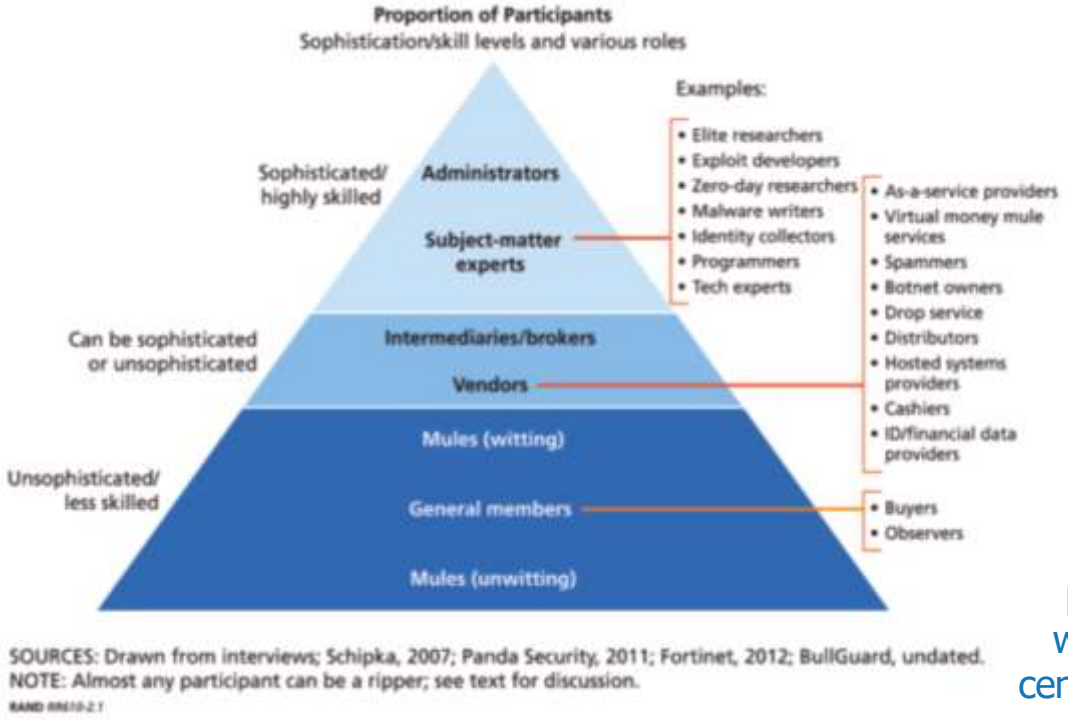
	2020	2018	2016	2014	2011
Détournement d'actifs	31%	45%	64%	69%	79%
Fraude de la part des clients	35%	29%			
Cybercriminalité	34%	31%	32%	24%	23%
Corruption et pots de vin	30%	25%	24%	27%	24%
Fraude liée à l'approvisionnement *(procurement fraud)*	19%	22%	23%	29%	
Fraude comptable	28%	20%	18%	22%	24%
Blanchiment d'argent	11%	9%	11%	11%	9%
Atteintes à la propriété intellectuelle, contrefaçon	11%	7%	7%	8%	8%
Fraude fiscale	8%	5%	6%	6%	4%
Concurrence déloyale *(competition law/antitrust law)*	13%	7%	4%	5%	7%

Sources:
http://www.pwc.ch/publications/2016/pwc_global_economic_crime_survey_14_e.pdf
https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf
https://www.pwc.ch/en/publications/2018/Global-economic-crime-survey-2018_en_web-double.pdf
https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

L'économie cybercriminelle

«Chaque année, l'économie mondiale perd **600 milliards de dollars** en termes de croissance, d'innovation ou de compétitivité»

Source: CSIS, Center for Strategic and International Studies, communiqué de presse, 21.02.2018



SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.
NOTE: Almost any participant can be a ripper; see text for discussion.


JUNIPER RESEARCH

CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019

Mark Hughes, CEO, BT Security:
"The industry is now in an arms race with professional criminal gangs and state entities with sophisticated tradecraft. The twenty-first century cyber criminal is a ruthless and efficient entrepreneur, supported by a highly developed and rapidly evolving black market.

L'économie cybercriminelle

Les impacts de la cybercriminalité sur les entreprises

- Continuité des opérations remise en question
- Pertes financières
- Divulgation d'informations confidentielles (internes, clients, tiers et partenaires)
- Dommages réputationnels
- Atteintes à la propriété intellectuelle
- etc.

- Plus de **40%** des attaques ayant réussi ont un impact sur la continuité des opérations et engendrent des pertes financières !
- Dans **un tiers** des cas, des informations confidentielles sont divulguées

Sources: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf

L'arnaque au président

Quel est le maillon faible ?

10.02.2017, 12:40

Suite à une grosse arnaque à La Chaux-de-Fonds, la police lance une mise en garde

PAR RON

Réagir à cet article

ESCROQUERIE - La police neuchâteloise vient de lancer une alerte à l'escroquerie informatique dite "du président". Elle le fait après un cas chaux-de-fonnier où une entreprise a perdu un bon million.

Une entreprise chaux-de-fonnière s'est fait escroquer récemment d'un bon million de francs, suite à une arnaque informatique sophistiquée.

A la suite de ce cas, et de plusieurs autres tentatives dans le canton, la police neuchâteloise lance un avertissement contre ce qu'elle appelle une "escroquerie au président", en recrudescence ces temps-ci en Suisse romande en tout cas.

Sources: https://www.arcinfo.ch/sortir-articles/suite-a-une-grosse-arnaque-a-la-chaux-de-fonds-la-police-lance-une-mise-en-garde-634928

Infrastructures d'entreprises sensibles
amateurs s'abstenir !

Deloitte, l'un des Big 4 reconnaît que les eMails de certains de ses clients stockés sur Azure ont pu être compomis. Certains craignent que des identifiants, adresses IP, diagrammes architecturaux et données de santé le soient également.

Un compte administrateur sans restriction d'accès et non muni d'une identification à deux facteurs aurait servi de porte d'entrée…

Sources: http://www.lemondeinformatique.fr/actualites/lire-deloitte-pirate-des-documents-confidentiels-clients-derobes-69479.html
https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails#img-1

Vol de données, rançon

Et ses coulisses

22 NOVEMBRE 2017 / DONNÉES PERSONNELLES

Vol massif de données chez Uber : 57 millions de comptes piratés

La compagnie de transports Uber a annoncé qu'elle avait été victime d'un vol massif de données en 2016. Des informations sur les clients et les chauffeurs ont été aspirées

Uber a payé une rançon pour étouffer le hack de 57 millions de données d'utilisateurs

Les hackers sont parvenus à récupérer des identifiants utilisés par des ingénieurs logiciels d'Uber puis à les utiliser pour accéder aux données stockées sur le compte Amazon Web Services utilisé par la firme. Ils auraient ainsi mis la main sur une archive contenant les informations faisant l'objet de la rançon.

Sources: Clearswift Insider Threat Index (CITI) - 2015
https://www.lebigdata.fr/uber-fuite-donnees-personnelles

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Cyberattaque ou ingénierie sociale ?

...ou les les deux

Mai 2016

LEMONDE INFORMATIQUE

Après les institutions financières canadiennes et américaines, auxquelles il a réussi à extirper la coquette somme de 4 millions de dollars le mois dernier, le Trojan hybride GozNym s'intéresse désormais aux banques européennes.

De faux sites bancaires pour tromper les clients

Attention aux pièces jointes !

Mai 2019

datanews

Grâce à une opération à l'échelle mondiale, la police a mis hors d'état de nuire une bande de cybercriminels, qui proposaient ses services en ligne. Le gang 'GozNym' a utilisé un malware pour dérober quelque nonante millions d'euros chez plus de 40.000 victimes.

Cybercrime-as-a-Service

GozNym était diffusé par des mails de hameçonnage (phishing) et essayait, une fois installé, de dérober les noms d'utilisateur et mots de passe pour des opérations de banking en ligne. De l'argent était ensuite retiré des comptes, puis blanchi.

Hes·so

Sources: https://www.lemondeinformatique.fr/actualites/lire-dossier-l-ia-moteur-de-la-transformation-numerique-des-entreprises-75275.html
https://datanews.levif.be/ict/actualite/demantelement-d-un-gang-international-a-l-initiative-d-un-maliciel-bancaire/article-news-1139557.html?cookie_check=1558170918

Cyberattaque ou ingénierie sociale ?

…ou les les deux

Blick

Hacker knacken Zahlungs-Software

Bei Berner Firma verschwanden 1,2 Millionen Franken

BERN - Hacker haben über Nacht 1,2 Millionen Franken von den Konten der Berner Küng Holding abgezweigt. Firma, Banken und Software-Vertreiberin streiten darum, wer schuld ist.

Nicole Bruhin

Es war mysteriös: Mitte Februar stellten Buchhalter der Berner Küng Holding AG fest, dass 1,2 Millionen Franken über Nacht von den Firmenkonten verschwunden waren. Schnell war klar: Da waren Hacker am Werk. Diese waren ins Firmennetzwerk eingedrungen und hatten über die interne Zahlungssoftware drei Banken beauftragt, Geld ins Ausland zu transferieren, wie die «Berner Zeitung» berichtet.

So überwies die Berner Kantonalbank 785'000 Franken an eine Einzelperson in Kirgistan. Die UBS tätigte Zahlungen von 309'000 Franken, und die Credit Suisse transferierte 121'000 Franken. Alle drei Banken hatten die Transaktionen ohne Rücksprache mit der Küng Holding veranlasst.

L'attaque provient de l'extérieur, mais les failles sont bien souvent internes:

- Pas de double authentification / mots de passe faibles
- Inattention du personnel (mails de phishing)
- Parc informatique insuffisamment entretenu

Hes·so

Sources: https://www.blick.ch/news/schweiz/groesster-tankstellenraub-der-schweiz-bei-avia-verschwanden-1-2-millionen-franken-id6308208.html

Des doutes sur le potentiel impact opérationnel d'une cyberattaque ?

Systèmes et processus touchés:

SAP;
Gestion des entrepôts;
Téléphonie fixe;
Site web;
Toutes les adresses mail.

Méthode utilisée:

probablement un Cryptotrojan

Vecteur d'infection:

non communiqué (Phishing ?)

PIRATAGE

Meier Tobler paralysée par une cyberattaque

ABONNÉ

2 minutes de lecture

Economie suisse

Florian Delafoi

Publié lundi 29 juillet 2019 à

L'entreprise zurichoise est la cible d'un piratage qui neutralise l'intégralité de son système informatique depuis mercredi dernier. Un plan d'urgence est activé

Sources: https://www.rts.ch/info/economie/10641218-lombre-des-ransomwares-plane-sur-leconomie-suisse.html
Le Temps: https://www.letemps.ch/economie/meier-tobler-paralysee-une-cyberattaque
ICTjournal: https://www.ictjournal.ch/news/2019-08-07/les-zurichois-de-meier-tobler-toujours-paralyses-par-

Dirigeants: passez à l'action !

- Conseil d'administration (CA)
- Direction

Pourquoi ?

- Bases légales:
  - Attributions du CA (art. 716 et 716 a CO)
  - Devoir de diligence (art. 717 al. 1 CO)
  - Responsabilité (art. 754 CO)

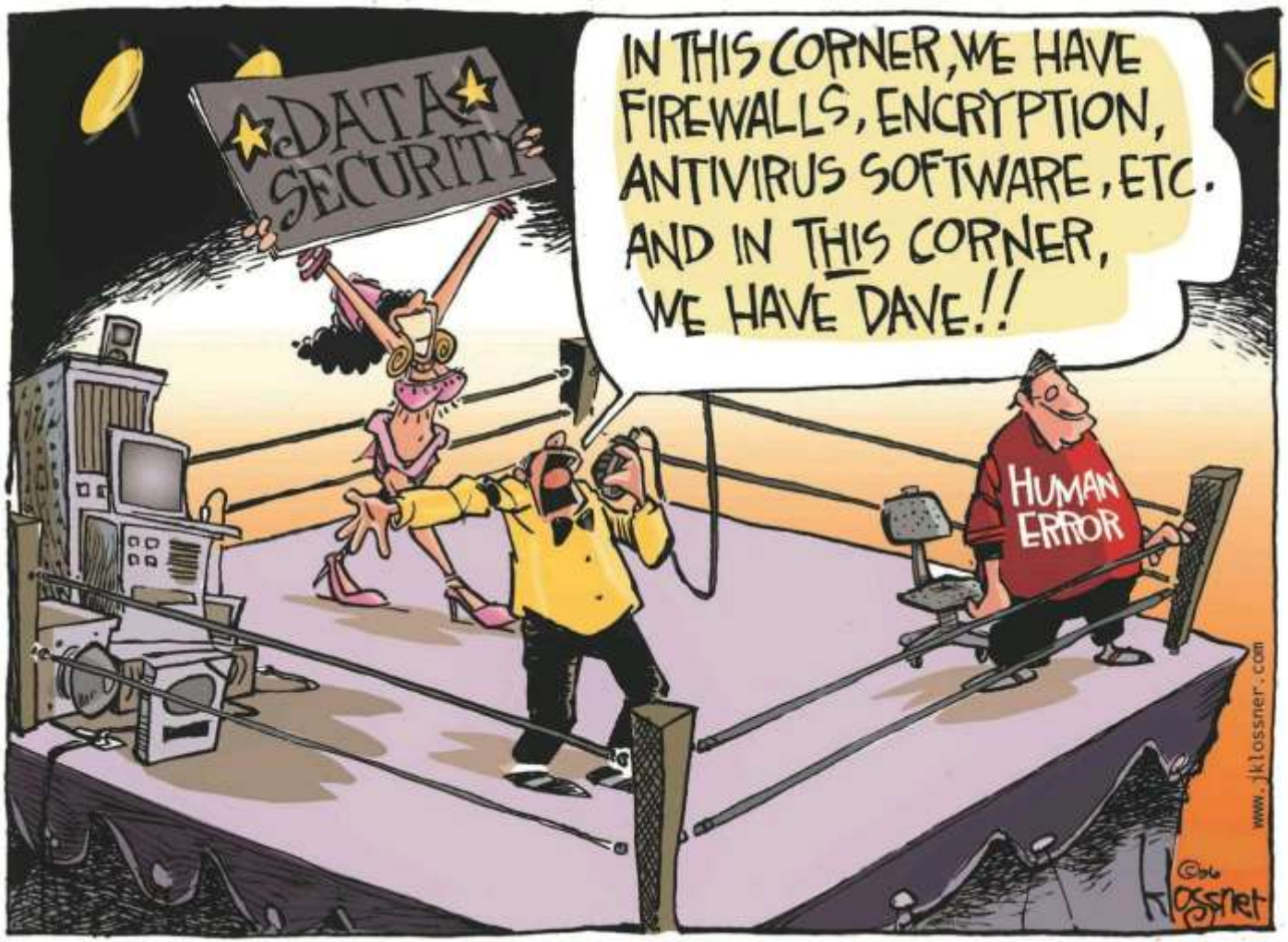
5 Principes clés formulés par la NACD

(National Association of Corporate Directors)

- cybersécurité = partie intégrante du management des risques de l'entreprise
- implications juridiques des risques cyber spécifiques au domaine d'activité
- gestion et prévention des risques cyber avec ressources humaines et financières adéquates
- un expert cyber dans un CA
- cartographie des risques cyber (identification risques majeurs vs risques acceptables et priorisation des investissements nécessaires)

Sources: https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687

Un point commun à la plupart des attaques…



La sécurité informatique en question

Le développement fulgurant des systèmes connectés

2020:
~50 mia.

2015:
~5 mia

5G

X 35

2012

2014

2016

2018

2020

Source: Ericsson Mobility Report, June 2020

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

La sécurité informatique en question

L'impact de la digitalisation sur les comportements

de Office Work à Anytime, Anywhere, Any device

de JE à NOUS

plusieurs activités

de Work-life balance à Work-life integration

Employé
BYOB

d'employé à son propre chef

Hes·so

Sources: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

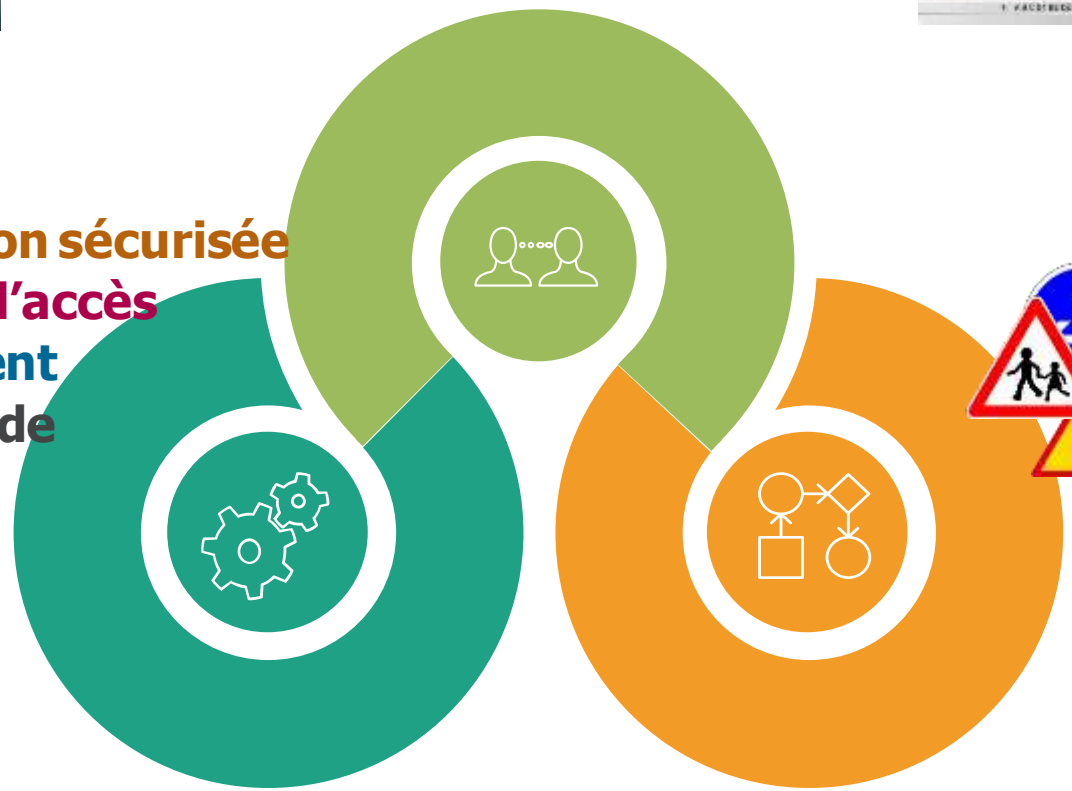
Les clés d'une sécurité de l'information efficace

Les individus: Security by Design n'est pas dans leurs gènes !

*57%
L'Humain au centre

Clients
Personnel
Prestataires
Partenaires
Fournisseurs

Antispam
Antivirus
Pare-feu
Destruction sécurisée
Contrôle d'accès
Chiffrement
Sauvegarde



Flux d'information
Flux logistiques
Flux financiers

Mesures techniques
Processus ajustés

*Source: PWC, Fighting fraud: A never-ending battle, PwC's Global Economic Crime and Fraud Survey, 2020 (https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html)

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

« Si tu veux la paix, prépare la guerre »

Toujours prêts !

Les **menaces cybercriminelles**

exploitent les **vulnérabilités** de l'organisation et

ciblent vos **actifs**, votre **valeur** !

Comment se prémunir ?

- En ciblant d'abord **ce qui a de la valeur**
- En identifiant les **vulnérabilités**, si possible les **menaces potentielles**, ainsi que **les conséquences** pour l'organisation
- Afin de **classifier les risques** et **déterminer les mesures** à prendre
- Les **mettre en œuvre**
- Mesurer leur **efficacité** et
- Déterminer les mesures correctives

… puis recommencer !!!

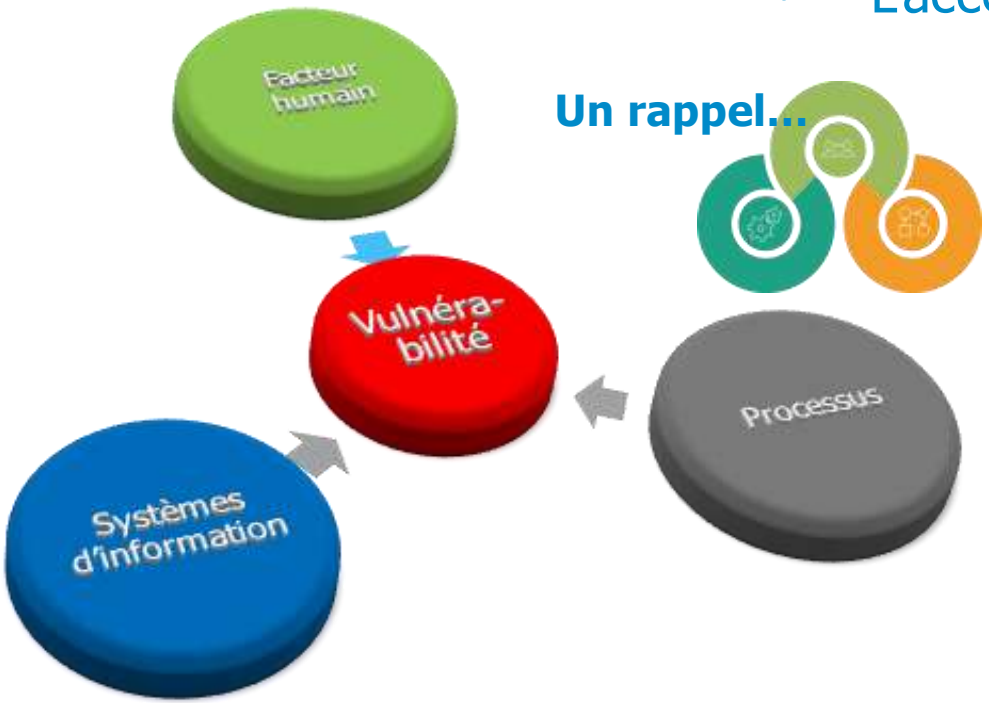
Hes·so

« Si tu veux la paix, prépare la guerre »

Toujours prêts !

Face à chaque risque, identifiez la bonne réponse à donner:

- L'éviter
- Le réduire
- L'accepter
- Le transférer



Un rappel…

En parlant d'assurances

- Une tendance en développement
- Ce n'est pas une panacée !
- Il s'agit d'un outil de plus

« Si tu veux la paix, prépare la guerre »

L'objectif fondamental: assurer la continuité des opérations !

Pour les risques impactant les opérations:

- Déterminer le mode de fonctionnement dégradé
- Attribuer les responsabilités
- Tester le plan dégradé
- Connaître les actions à entreprendre pour rétablir la situation

« Si tu veux la paix, prépare la guerre »

Besoin d'outils ?

Melani : Sécurité de l'information: aide-mémoire pour les PME

OFAE « Norme minimale pour les TIC et outil d'évaluation :

ICT Swizterland : Cybersecurity-Schnelltest für KMU

Etc.

Remarques:

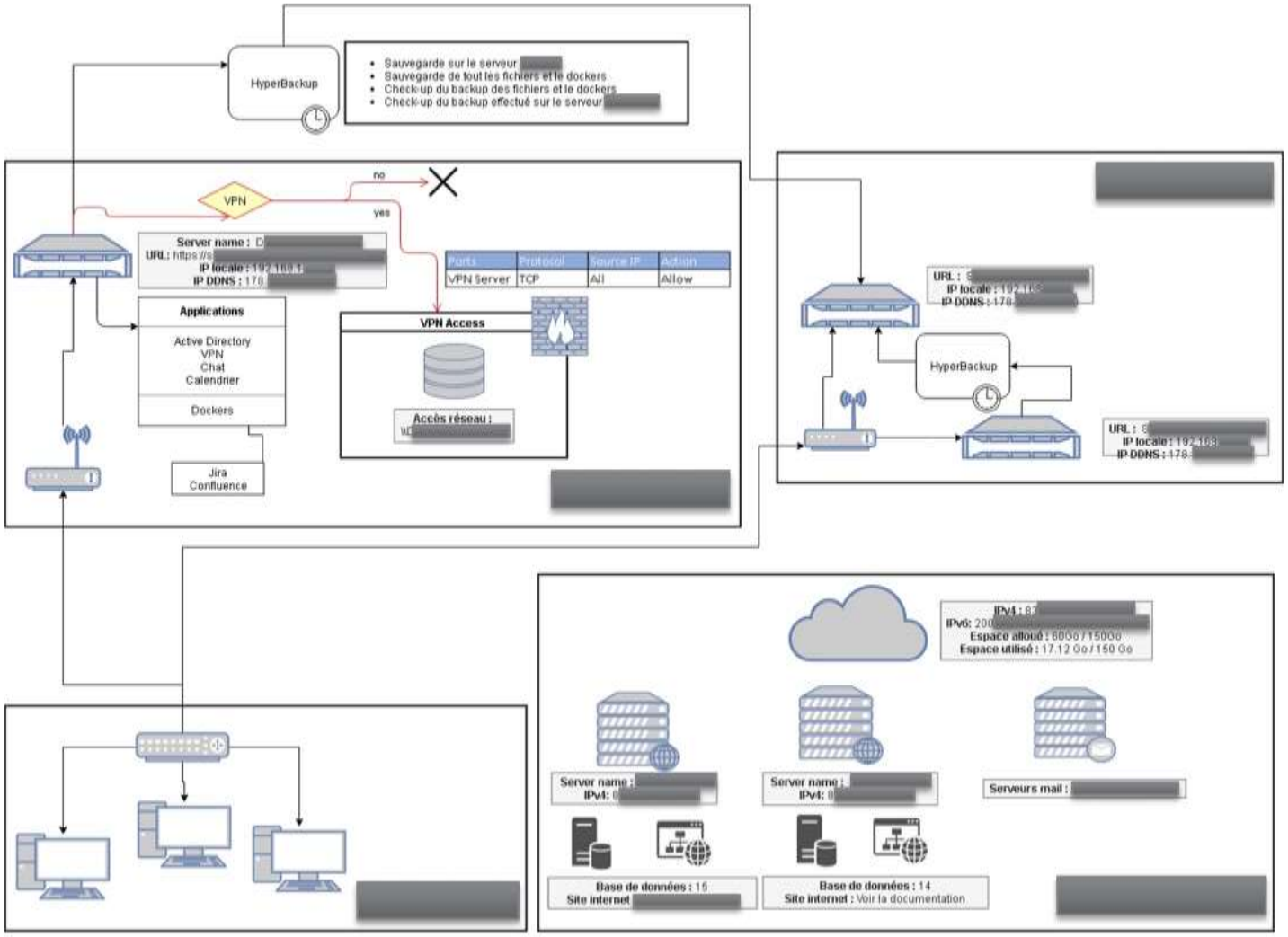
- Ces questionnaires sont par définition génériques
- La réponse aux questions est question d'appréciation
- Un non informaticien sera rapidement dépassé
- La checklist doit s'inscrire dans un cycle

Le dilemme du responsable de la sécurité de l'information

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

Connaître son environnement informatique. Mission accomplie ?



ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

Protégez particulièrement les données qui ont de la valeur pour VOUS !

☺ **Les données** qui sont **importantes** pour vous **devraient être chiffrées**;
☺ Cela **protège** votre **vie privée**
☺ Cela vous protège également **en cas de détérioration ou de vol** de votre ordinateur.

- Conserver une **copie de sauvegarde** de ses données, c'est une **assurance**, par exemple:
  - En cas d'erreur de manipulation
  - En cas d'attaque par Ransomware

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

Protégez particulièrement les données qui ont de la valeur pour VOUS !

Cloud public

- Cercle des utilisateurs potentiels indéterminé
- Ressources publiques partagées
- Accessible directement par internet

Cloud privé

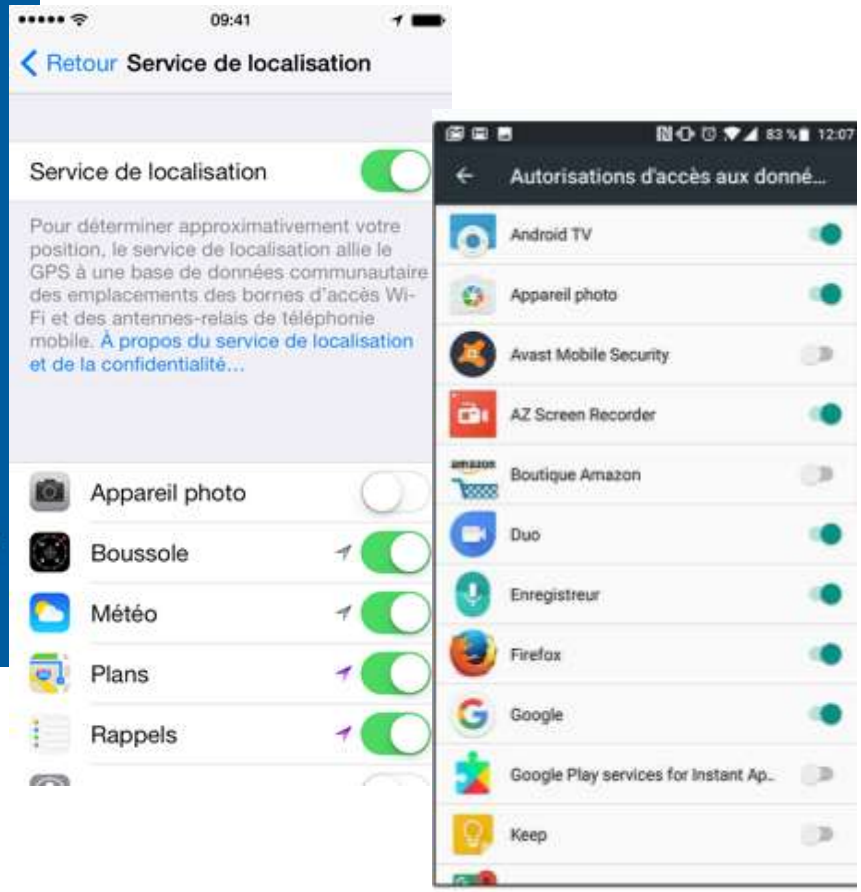
- Cercle des utilisateurs potentiels déterminé
- Ressources dédiées partagées
- Accessible en interne ou par VPN

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

Veillez à la configuration de vos appareils personnels

Exemple avec Microsoft Windows 10



Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

RIEN ne ressemble plus à un vrai eMail qu'un faux eMail !

PayPal

Transaktionscode: O-7A286334J4405335B

Guten Tag, Sébastien Jaquier!

Sie haben eine Bestellung über an Microsoft Payments gesendet

Vielen Dank für Ihre Bestellung bei Microsoft Payments. Das Geld wird erst dann von Ihrem Konto abgebucht, wenn die Bestellung von Microsoft Payments verarbeitet wurde. Ihr PayPal-Guthaben wird hierfür immer vorrangig vor anderen Zahlungsquellen wie Bankkonto oder Kreditkarte verwendet.

Loggen Sie sich in Ihr PayPal-Konto ein, um alle Transaktionsdetails anzuzeigen. Es kann einige Minuten dauern, bis die Transaktion in Ihrem Konto angezeigt wird.

https://www.paypal.com/ch/cgi-bin/webscr?cmd=_view-a-trans&id=o-7a286334j4405335b

Cliquez ou appuyez pour suivre le lien.

PayPal

Ihr PayPal Konto hat ein neues Entgerät

Guten Tag
Ihr letzter Einkauf in Höhe von **299,64 ?** zzgl. Versandkosten bei dem Online-Anbieter **ebay.com** wurde zu Ihrer Sicherheit zunächst nicht ausgeführt. Hier gelangen Sie zum jeweiligen Produkt.

Scheinbar wurde Ihr Zugang von einem dritten Endgerät genutzt, welches uns nicht bekannt ist.

Wenn Sie diesen Einkauf **nicht** durchgeführt haben, bitten wir Sie über den unten aufgeführten Button Ihre Daten zu bestätigen und anschließend die Bestellung zu stornieren.

Für die Stornierung der Bestellung haben Sie eine Frist von **12 Werktagen**. Läuft diese ab und Sie beantragen keine Stornierung, wird die Transaktion automatisch genehmigt.

Stornieren Sie hier (zum Widerruf)

Vielen Dank für Ihre Zeit.

http://paypal.re-signup.account-personalaccountsignup.nulidadesfl.com/signlimithl/mt_personal_cm/

Cliquez ou appuyez pour suivre le lien

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

Vos mots de passe… l'équivalent de la clé de votre domicile !

1. 123456
2. Password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. Sunshine
9. Qwerty
10. Iloveyou
11. Princess
12. Admin
13. Welcome
14. 666666
15. abc123

Quel sont vos mots de passe ?

Sources: https://www.lesnumeriques.com/vie-du-net/mots-passe-plus-utilises-en-2018-toujours-meme-rengaine-n81693.html
https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Quelques bonnes pratiques en matière de cybersécurité

Vos mots de passe… l'équivalent de la clé de votre domicile !

Optez pour un mot de passe sûr

- ☺ **Au MINIMUM 8 caractères** (12 à 18 c'est mieux !)
- ☺ Des **chiffres** et des **lettres**… et des **caractères spéciaux** !
  + « » * ç % & / ( ) = ? @ # $ £ ! < > \ -
- ☺ Ne mettez pas tous les œufs dans le même panier !
- ☺ Changez régulièrement vos mots de passe !

Et pourquoi faire ?

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

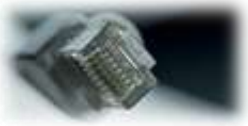
Quelques bonnes pratiques en matière de cybersécurité

Que faire si un problème survient ?

- Vous pensez avoir ouvert un lien vers un site malveillant ?
- Vous craignez d'avoir ouvert un fichier infecté ?
- Vous avez un doute ?

Une réaction en trois temps:

1. Débranchez votre câble réseau (le cas échéant)



2. Mettez votre appareil en mode avion

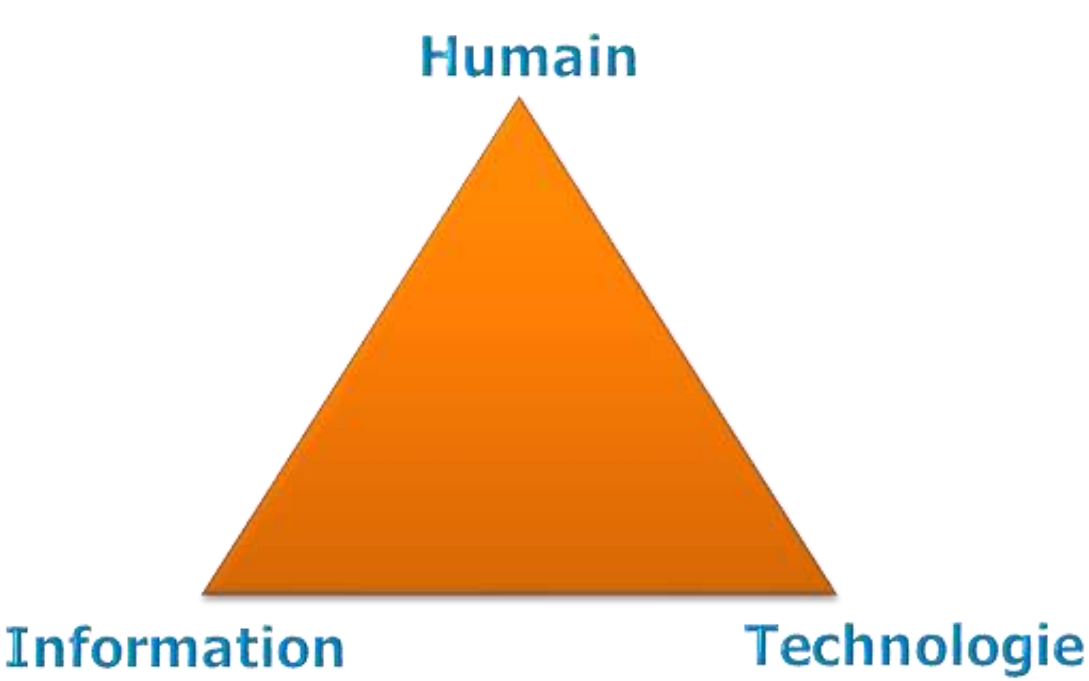
3. Prenez contact avec votre service informatique

…et de 4… après nettoyage, vous récupérez les documents importants que vous aviez archivé !

Hes·so

Information – Humain – Technologie

Un trio infernal ?



Un cercle vertueux !

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

L'ILCE propose des solutions

Formations

- Management de la sécurité de l'information dans les PME
- Stratégie de sécurité de l'information à l'attention du Conseil d'administration

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

L'ILCE propose des solutions

Formations sur mandat

Formations sur mandat = le luxe du sur mesure :

- Sensibilisation du management ou / et du personnel
- Formations ciblées du personnel, des spécialistes ou des cadres

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

L'ILCE propose encore d'autres solutions:
analyses, expertises, coaching

Prévention

- Méthodologie pour la réalisation d'une analyse de risques
- Etablissement d'une cartographie «personnalisée» des risques
- Mise en œuvre de mesures préventives et dissuasives

Détection - Investigation

- Expertise juridique, économique et informatique
- Analyses et expertises effectuées par le CINC: Centre d'investigation numérique et de cryptologie

www.ilce.ch

Hes·so

ilce - institut de lutte contre la criminalité économique
heg - haute école de gestion

Merci, à votre disposition

Dr Isabelle Augsburger-Bucheli, Prof.
Doyenne de l'ILCE
Tél. direct: + 41 (0)32 930 20 10
e-mail: isabelle.augsburger@he-arc.ch

Sébastien Jaquier
Responsable adjoint de l'ILCE
Dirigeant d'entreprise / Administrateur
Tél. direct: +41 79 380 222 7
E-mail: sebastien.jaquier@he-arc.ch

Hes·so