9 TRENDS CYBER INNOCHERCHE 2020

Le Think Tank Cybersécurité de l'association de veille pour dirigeants INNOCHERCHE identifie, décrypte et vulgarise les trends en matière de cybersécurité pour aider les dirigeant à décoder, pour anticiper et pour passer à l'action.

Le Trophée INNOCHERCHE de Cybersécurité vise à mettre en avant des startups en capacité de relever les défis posés par ces 9 trends identifiés au cours de l'année 2019 par le Think Tank Cyber et de proposer des solutions efficaces pour 2020.

Voici les 9 trends en matière de cybersécurité observés en 2019. Pour chacun, le concept est expliqué, des exemples sont donnés avec les résultats observés et dans les enseignements que l'on en tire, on se réfère à notre fiche des 8 principes que l'on maintient à jour dans notre référentiel de veille InnoCherche :

On a classé ces 9 trends en :

- trois trends généraux pour tous
    - toujours plus de fuites sur les données les plus sensibles
    - … et de demande de rançons
    - une nouvelle menace Deepfake
- quatre trends sectoriels
    - tous infrastructures sont vulnérable
    - notamment à cause développement de l'IOT
    - dont il faut maîtriser le risque Cyber
    - avec la Supply Chain très visée étant donné son pouvoir de contamination
- … et deux trends Management
    - travailler la résilience digitale
    - avec une politique RH au centre de votre Cyber sécurité

Trend 1 : toujours plus de fuite des données les plus sensibles

L'affaire des Panama papers est la plus importante fuite mondiale de données confidentielles privées censées être très protégées.

Au sein du cabinet panaméen Mossack Fonseca, spécialisé dans la création et la domiciliation de sociétés offshore, un informaticien interne a exporté 2,6 téraoctets de données portant sur 214 000 sociétés offshore, majoritairement liées d'une façon ou d'une autre à des personnalités publiques.
Cette fuite constitue la plus grande révélation de documents exploités par les médias (2,6 To (équivaut à 2600 films d'une heure en HD) et dépasse de loin le total des données des

câbles de WikiLeaks de 2010 (1,7 Go), des Offshore Leaks de 2013 (260 Go), des Luxleaks de 2014 (4 Go) et des Swissleaks de 2015 (3,3 Go).

Les volumes sont impressionnants :

- 4,8 millions d'emails
- 3 millions de bases de données
- 2 millions de fichiers PDF
- 1,1 million d'images (notamment les photocopies des passeports des actionnaires et des scans de contrats signés)
- 320 000 fichiers texte
- 2 000 fichiers d'autres formats

Ces documents ont été adressés dès 2015 au quotidien allemand Süddeutsche Zeitung.Ce dernier a rapidement partagé les informations avec l'International Consortium of Investigative Journalists (Consortium international pour le journalisme d'investigation) pour partager le travail d'investigation journalistique de façon secrète puis diffuser en masse quand ils sont prêts et que le scandale explose en avril 2016.

Résultats :

- Une vaste enquête portant sur 40 ans (1977-2015) et 70 pays, menée par 370 journalistes, a révélé que 140 responsables politiques ou personnalités auraient des avoirs dans des paradis fiscaux.
- Une base de données en ligne encore aujourd'hui avec moteur de recherche permet d'obtenir des informations sur les 214 000 sociétés offshores créées par Mossack Fonseca et, quand les données le permettent, les noms de leurs vrais propriétaires. Les internautes peuvent éplucher ces données et visualiser les réseaux autour d'une centaine de ces entités.

Enseignements trend 1 "fuite données sensibles" :

- Principe 5 Innocherche : la Cybersécurité est un processus récurrent qui devient stratégique
- Principe 2 Innocherche : Travailler en amont sur la classification des données
- Principe 4 Innocherche : Toujours partir de l'analyse du risque
- Principe 7 Innocherche : La Cybersécurité est une affaire d'Homme avant d'être une affaire de Technologie

Trend 2 : toujours plus de Ransomware (demande de rançon)

Il s'agit d'attaques où l'objectif est de demander une rançon en promettant de récupérer son bien ou d'arrêter le chantage.

En 2017, la première plus importante attaque mondiale de ransomware a eu lieu
Le 14 avril 2017, le groupe de hackers The Shadow Brokers publie EternalBlue, un exploit développé et utilisé par la NSA, qui utilise une faille de sécurité de Windows. (Le 14 mars 2017, Microsoft avait publié une mise à jour de sécurité pour les versions maintenues de Windows pour colmater cette faille)

Le vendredi 12 mai 2017, un ransomware, « WannaCry » utilise cette faille de sécurité pour se propager sur des milliers de vieux PC non mis à jour, y aller chiffrer les fichiers et demander une rançon pour les déchiffrer. WannaCry cible le protocole SMB (Server Message Block) pour infiltrer ses victimes (spécifiquement par une connexion TCP au port 445). Créé dans les années 1980, ce protocole a été utilisé sous plusieurs formes jusqu'à Windows 8. Elle y installe ensuite le ransomware WannaCry, qui rend les fichiers inutilisables et demande une rançon en Bitcoin d'environ 300 dollars (qui double après 3 jours). Si la rançon n'est pas payée au bout d'une semaine, les fichiers sont effacés.
Ce vendredi 12 mai 2017, WannaCry s'est propagé à une vitesse folle dans le monde au point de toucher une centaine de pays : Grande-Bretagne, Espagne, Portugal, Mexique, Australie, Russie mais aussi… la France. Au total, ce sont au 300 000 PC qui ont été affectés.

Résultats :

- Une maigre recette de 110.000 euros car les recommandations des autorités de ne pas payer ont bien été suivies (si vous payez, vous êtes mis sur une liste de gogo dans le dark web augmentant votre chance d'être à nouveau attaqué)
- Un arrêt de la production : Par prévention, Renault a décidé de mettre à l'arrêt ses sites industriels. L'arrêt de la production « fait partie des mesures de protection qui ont été prises pour éviter la propagation du virus », a déclaré à une porte-parole, sans préciser le nom des sites concernés.
- Une faiblesse inacceptable … transformée en opportunité par Microsoft : en raison de la gravité de l'attaque de WannaCry le 13 mai 2017, Microsoft prend la mesure inhabituelle de publier une mise à jour de sécurité pour les systèmes d'exploitation qu'il ne maintient plus, comme Windows XP, Windows 8 et Windows Server 20037,8.
- Un arrêt de la production un mois après la fin de l'épidémie : le 21 juin 217, Honda a dû arrêter la production un jour à son usine de Sayama : les machines Windows n'avaient pas été mises à jour.

En 2019, la plus importante attaque mondiale industrielle de ransomware a eu lieu

En mars 2019, le ransomware LockerGoga cible le fabricant norvégien d'aluminium Norsk Hydro. Il crypte les données, déconnecte les utilisateurs et les réseaux. Son originalité réside dans le fait de ne pas avoir la capacité de se diffuser seul sur le réseau de l'organisation visée : il est déployé via Cobalt Strike (un outil d'entraînement des équipes de défense et de protection des systèmes d'information) couplé à des serveurs de commande et de contrôle. Plus d'un mois plus tard, la plupart de ses 160 sites de fabrication fonctionnaient toujours en opérations manuelles (non informatiques).
Deux entreprises américaines du monde de la chimie, Hexion et Momentive, ont été également ciblées.

Enseignements trend 2 "Ransomware" :

- Principe 7 Innocherche : La Cybersécurité est une affaire d'Homme avant d'être une affaire de Technologie
- Principe 8 Innocherche : Prêt à communiquer

Pour anticiper et préparer, vous devez mettre en place :

- un plan de continuité des activités
- un plan de restauration des données
- un plan de communication de crise
- un plan de mise à jour automatique des correctifs de sécurité

Trend 3 : nouvelle menace Deepfake après FakeNews (en français, attaque informationnelle)

Ce sont des fausses nouvelles ou fausses vidéos, de plus en plus réalistes visant à manipuler l'opinion en vue d'un gain électoral ou financier.

En jouant sur le phénomène de bulles FaceBook - qui isolent des audiences qui ne reçoivent que l'information allant dans un sens - la propagande russe a réussi à complètement polariser la vie politique américaine. Avec un débat devenu parfois haineux, sans aucun argument rationnel et objectif, basé uniquement sur des peurs et des craintes, les Russes ont ainsi facilité l'élection de Trump comme démontré dans le rapport MUELLER.

D'après les calculs approximatifs de Roger McNamee (...dans son remarquable livre ZUCKED), pour monter une telle opération, il faut pendant 4 ans, mobiliser 80 à 100 hackers professionnels, pour un coût global estimé autour de 100 millions de dollars. C'est le coût d'un chasseur militaire F35... ce qui est peu de chose aux vues des enjeux géopolitiques de la Russie. (Concept asymétrique warfare)

Dans ce coût total, la part de la publicité payée à Facebook est minime. FaceBook a admis devant le congrès avoir reçus 100K $ de compte d'agents Russes **en rouble** pour financer 3000 annonces relayés par 470 fake accounts et de nombreux BoT. Etant donné le patient travail de terrain fait en amont dans les différentes communautés, ces Fakenews qui rebondissent sur de l'actualité déformée, ont été vues 340 millions de fois. Cela vous montre l'aspect viral de ces fake news, qui bien orchestrées, avec des relais de groupes similaires en groupes similaires, touche un auditoire très large. Dans un autre témoignage et utilisant une autre métrique, Facebook a reconnu que 126 millions de personnes ont été touchées par ces publicités et ces fake news russes lors des élections. Ce chiffre est à rapporter aux 137 millions de votants des dernières élections de 2016.

In fine, cette entreprise construite pour décourager les démocrates d'aller voter a bien fonctionné puisqu'entre l'élection de Obama en 2012 et la défaite de Hillary Clinton en 2016, 4 millions d'électeurs démocrates sont restés chez eux le jour du scrutin pour Hillary Clinton.
Du point de vue de Poutine, il s'agit d'un succès extraordinaire de asymmetric warfare parce que, pour un tout petit budget de 100 millions de dollars, il a complètement réduit à néant le "soft power" que la démocratie américaine avait créé depuis la fin de la seconde guerre mondiale.

Voici les vidéos relatives à ce sujet :
https://www.youtube.com/watch?v=DIrlZRwtRl0
https://www.youtube.com/watch?v=__3ouxlHskk
https://www.youtube.com/watch?v=Z5shuMkducs
Depuis 2019, la menace s'alourdit avec les Deepfakes.

Enseignements trend 3 "Fakenews et DeepFake" :

- Principe 1 Innocherche : la Cybersécurité ne tolère pas la médiocrité et l'amateurisme ("soit tu joues en premier league, … soit tu ne joues pas") : l'ambition doit être portée par une capacité réelle d'exécution, d'innovation et d'adaptation.
- Principe 5 Innocherche : la Cybersécurité est un processus récurrent qui devient stratégique
- Principe 2 Innocherche : Travailler en amont sur la classification des données
- Principe 4 Innocherche : Toujours partir de l'analyse du risque … et mettre en place des plans d'actions pour être capable de contrer la propagande si possible en moins d'une heure pour les Deepfakes… contre 24h pour les FakeNews.

Trend 4 : infrastructures physiques (Web, IOT) toutes vulnérables.

Jusqu'à présent, en faisant du dommage dans le monde digital, on viser de l'information u de l'argent. Avec ces nouvelles attaques, on met à terre vos serveurs physiques

Le déni de service (DDoS) est une attaque qui consiste à saturer les capacités de traitement d'un fournisseur d'accès internet. Concrètement par analogie, si nous considérons qu'un bus peut transporter 75 clients, le fait que 1200 faux clients se présentent à la porte de ce bus vont empêcher les clients légitimes de monter dedans et donc de les transporter ; le service est interrompu.

L'attaque d'OVH est la plus importante attaque mondiale de déni de service.
Au mois de septembre 2016, le géant français de l'hébergement internet OVH qui gère plus de 260.000 serveurs dans le monde a été victime de la plus puissante attaque de déni de service à l'échelle mondiale : 145.607 dispositifs d'émission de messages automatiques introduits dans des logiciels de caméras de surveillance elles-mêmes connectées à internet, ont déversé plus de 1,5 Tb par seconde de données sur les serveurs OVH pendant une semaine.

Résultats :

- Après ce déni de service, une **communication transparente** par tweet du fondateur de l'entreprise, Octave Klaba sur l'évolution de la situation : On a l'infrastructure qui tient (expliquer qu'il a réussi à maintenir un service dégradé ?!!). Cette communication transparente a été relayée dans les médias.
- **Un travail de Pro chez OVH :** L'infrastructure a en effet pu encaisser l'attaque grâce à une anticipation des volumes de données à recevoir et grâce à une innovation interne le « VAC » (diminutif de « vacuum »). Contrer une attaque DDoS consiste essentiellement à détecter dans le flux des requêtes celles qui sont malveillantes et à les supprimer. Mais pour cela, l'hébergeur doit déjà être en mesure d'accueillir la totalité des requêtes sur son réseau. En plus d'une grande capacité d'interconnexion, OVH a mis en place une grande capacité de filtrage de paquets : le VAC est un système matériel, développé maison en anticipation d'une telle attaque, basé sur des circuits logiques programmables de type FPGA (Field-programmable gate array), sur lesquels les ingénieurs de l'hébergeur implémentent des algorithmes de filtrage qu'ils ont développés eux-mêmes. « *Au début, nous avons utilisé des produits du marché. Mais ils ne sont pas assez flexibles. Les pirates sont malins et trouvent toujours un moyen pour contourner un système de filtrage. Il faut donc constamment pouvoir s'adapter, ce qui n'était pas possible avec ces produits-là. Nous avons donc commencé à créer nos propres solutions qui elles ne sont pas connues du marché : Il n'est pas question, d'ailleurs, de les revendre*", explique Stéphane Lesimple, Responsable SOC OVH.

- … mais travail **d'amateur chez le fabricant de caméra vidéo** avec toutes ses caméras livrées sur le marché avec le même mot de passe de type "00000" et pas de possibilité de mettre à jour le SW à distance après détection d'une faille (cf Principe 6 : Mon espace est un espace à défendre") … ce qui va devenir un problème majeur pour tous les IOT.
- Un projet pour l'avenir : en février 2018, l'hébergeur veut créer une « digue numérique » capable de résister à un flot de 7 terabits/s. L'objectif est d'avoir une douzaine de VAC, chacun avec une capacité de traitement de 600 Gbits/s, soit un total de 7,2 terabits/s. En février 2017, OVH dispose de trois VAC, répartis à travers le monde. Chacun est capable de traiter un débit de 160 Gbits/s, ce qui représente une capacité de filtrage totale de 480 Gbits/s.

Enseignements trend 4 "infra Physique" :

- Principe 1 Innocherche : **La Cybersécurité ne tolère pas la médiocrité et l'amateurisme ("soit tu joues en premier league, … soit tu ne joues pas")** : l'ambition doit être portée par une capacité réelle d'exécution, d'innovation et d'adaptation.
- Principe 8 Innocherche : Prêt à communiquer
  - La Cybersécurité est une opportunité réelle de transformer une menace en une opportunité Business alignée sur son Business Model (cf réaction d'OVH)
  - La Cybersécurité est un formidable vecteur de communication
  - Anticiper et gérer une communication de crise
  - Les objets connectés diffusé par milliards, comme ces caméras vidéo, vont démultiplier la force des attaques reçues

Trend 5 : attention aux risques cyber en IOT

Jusqu'à présent, en faisant du dommage dans le monde digital, on viser de l'information ou de l'argent. Avec ces nouvelles attaques, on met à terre vos serveurs physiques… Mais aussi tous les objets physiques aujourd'hui connectés à l'internet pour les contrôler à distance et les détourner de leur mission.

l'IOT est une opportunité Business uniquement si la Cybersécurité est prise en compte.
L'IOT a été l'objet de nombreuses restitutions au sein du Think Tank Cybersécurité.
Voici les vidéos relatives à ce sujet :
https://youtu.be/E6l4wPTmJ-Q
https://youtu.be/z0PnVljQWJM
https://youtu.be/1KvSJDALkzQ
https://youtu.be/CIzNrGHoSlU

Enseignements Trend 5 "IOT" :

- Principe 5 Innocherche : la Cybersécurité est un processus récurrent qui devient stratégique
- Principe 2 Innocherche : Travailler en amont sur la classification des données
- Principe 4 Innocherche : Toujours partir de l'analyse du risque
    - Chaque objet IOT doit être considéré en termes de vulnérabilité comme un élément de votre périmètre informatique. Il devrait pouvoir être patché à distance.

Trend 6 : Utilisation croissante d'armes de destruction physique

Jusqu'à présent, en faisant du dommage dans le monde digital, on viser de l'information ou de l'argent. Avec ces nouvelles attaques, on met à terre vos serveurs physiques…. Mais aussi tous les objets physiques aujourd'hui connectés à l'internet pour les contrôler à distance et les détourner de leur mission pour les détruire.

Stuxnet de la CIA en 2010 détruit les centrifugeuses Iranienne. Les Hackers se saisissent de ce genre de malware et les développent.

La plus importante attaque mondiale de wiper (en français, virus destructeur) a eu lieu en 2017. Le 27 juin 2017, NotPetya (une variante du malware Petya découvert en 2015) s'est diffusée à très grande vitesse : 2000 entreprises ont été touchées.
Le vecteur d'infection initiale est un logiciel de comptabilité et de fiscalité ukrainien, M.E.Doc. C'est une mise à jour de ce dernier, modifiée par les attaquants, qui a servi de rampe de lancement au malware. Pour se propager, le virus de type Wiper utilise EternalBlue, un exploit développé et utilisé par la NSA, qui utilise une faille de sécurité de Windows. Ce ransomware NotPetya lui s'affiche à chaque démarrage de l'ordinateur à la place de Windows. Ainsi, on voit, sur un écran noir ce texte écrit en rouge et en anglais, le message suivant : "*Ooops, vos fichiers ont été cryptés. Si vous voyez ce message, vos fichiers ne sont plus accessibles, car ils ont été cryptés. Peut-être que vous recherchez un moyen de récupérer vos fichiers, mais ne perdez pas votre temps. Personne ne peut récupérer vos fichiers sans notre service de décryptage.*"

Ainsi, ce dernier demande une rançon, payable en Bitcoin, monnaie informatique intraçable, de 300 Dollars et de l'envoyer à une adresse e-mail au hasard, pour pouvoir récupérer l'accès à ses fichiers. Mais l'adresse renvoyée a été désactivée par le fournisseur de messagerie allemand Posteo, ce qui fera qu'aucun fichier ne sera récupéré après le paiement de la rançon ; les données sont alors détruites !

Par ailleurs, NotPetya chiffre les données des utilisateurs en utilisant une clé de chiffrement aléatoire, ce qui rend impossible la récupération de la clé de déchiffrement. Par conséquent, il s'agit d'un wiper qui utilise le mode opératoire d'un ransomware comme façade.

Résultats :

- Une maigre recette de 8.600 euros de rançon, payés par 46 victimes
- Un arrêt de la production : Les usines Saint-Gobain de Toul, Foug et Pont à Mousson ont été arrêtées pendant 5 jours. La filiale ukrainienne de Auchan a été arrêtée.
- Une faiblesse transformée en opportunité par la SNCF : "*Comme d'autres entreprises, la SNCF subit l'attaque en cours (…) nous ne sommes pas victimes",* a insisté un porte-parole, soulignant que *"les opérations de l'entreprise ferroviaire n'étaient pas affectées. Nos équipes sont sur le pont, elles (les attaques) sont contenues* », a-t-il ajouté.

Enseignements trend 6 " armes destruction" :

- Principe 6 InnoCherche: D'abord humain
- Principe 7 InnoCherche : Repenser l'organisation
- Principe 8 InnoCherche: soyez prêt à communiquer

Pour anticiper et préparer, vous devez mettre en place :

- un plan de continuité des activités
- un plan de restauration des données
- un plan de communication de crise
- un plan de mise à jour automatique des correctifs de sécurité

Trend 7 : La Supply Chain de + en + visée

L'attaque Supply Chain consiste à infiltrer les serveurs de référence et à utiliser ses produits pour infecter ses clients directs. Plus le fournisseur est global, plus la contamination est importante.

En mars 2019, il a été révélé que le constructeur Asus (top 5 des fournisseurs PC) a été victime d'une attaque informatique ayant permis d'utiliser son infrastructure pour diffuser des logiciels malveillants via mécanisme de mise à jour installé sur les machines, Asus LiveUpdate. Cette attaque ciblait un groupe spécifique et limité de 600 machines.
Le groupe de hackers Barium avait déjà réalisé une attaque similaire en 2017 sur un logiciel très populaire CCleaner.

En avril 2019, il a été annoncé que le logiciel de développement Visual Tool (édité par Microsoft) a été infiltré par le même groupe de hackers pour contaminer les logiciels codés avec cet outil.

Enseignements Trend 7 "supply chain" :

- Principe 5 Innocherche : la Cybersécurité est un processus récurrent qui devient stratégique
- Principe 2 Innocherche : Travailler en amont sur la classification des données
- Principe 4 Innocherche : Toujours partir de l'analyse du risque

Trend 8 : la résilience digitale est devenue vitale

Des petits états en situation de guerre latente avec de grands pays voisins ont développé une résilience importante en cas d'attaques.
Israel est devenue la Cybersecurity startup nation à l'échelle internationale. Chaque année, de nombreux grands groupes américains achètent soit la structure soit les compétences soit les services de ces startups.
L'Estonie a développé un système de sauvegarde et de restauration de ces données à l'échelle internationale. Elle a monté un réseau de tous les RSSI du pays pour se regrouper sur les cibles critiques en cas d'attaque généralisée. Ce système est très efficace comme démontré par les attaque NoPetya et Wanna Cry où l'Estonie a été un des rares pays non affectés.

Voici les vidéos relatives à ce sujet :
https://youtu.be/m_kYYqJAhMs
https://youtu.be/Yvaqty4-G30

Enseignements trend 8 "Résilience" :

- Principe 1 Innocherche : la Cybersécurité ne tolère pas la médiocrité et l'amateurisme ("soit tu joues en premier league, … soit tu ne joues pas") : l'ambition doit être portée par une capacité réelle d'exécution, d'innovation et d'adaptation.
- Principe 5 Innocherche : la Cybersécurité est un processus récurrent qui devient stratégique La chaîne n'est pas plus forte que son maillon faible. La cybersécurité prend une dimension nationale et stratégique où l'entraide devient un must.

Trend 9 : la politique RH est au centre de la cybersécurité

Les attaques sont de plus en plus conçues et designer avec minutie pour tromper les collaborateurs, à partir notamment de toutes les données disponibles sur votre organisation et les habitudes personnelles étalées sur des réseaux comme Linkedin.

Le Think Tank Cybersécurité prépare une enquête autour de la place stratégique de la politique RH dans la cybersécurité. Voici la vidéo relative à la présentation de ce projet : https://youtu.be/BoTtQCnU8zQ

Enseignement trend 9 "RH" :

- Principe 6 Innocherche : La Cybersécurité est une affaire d'Homme avant d'être une affaire de Technologie