Matière à Cyber-réflexion

Auteur : Corinne France
General Secretary EFCSE

BE SECURE

BE CURIOUS

EUROPEAN CYBER SECURITY MONTH

Cyberattaque, importance d'une collaboration internationale

En préambule, rappelons qu'au niveau de l'Union Européenne, la cybersécurité dispose de règles strictes et d'une protection accrue.

Quelques jalons en 2019 [source : Conseil de l'UE] :

- 17 mai : le Conseil est en mesure d'imposer des sanctions en cas de cyberattaques, y compris en cas de cyberattaques dirigées contre des États tiers ou des organisations internationales / politique étrangère et de sécurité commune (PESC).
- 9 avril : le Conseil adopte le Security Act
- 13 mars : le Conseil négocie avec le Parlement européen pour la mise en commun de l'expertise en matière de cybersécurité.

Une cyberattaque se situant par définition dans le cyber espace, le risque ne se cantonne donc pas aux frontières géographiques d'un pays, la collaboration entre les états européens et au-delà, reste essentielle et représente un facteur de réussite pour contrer des cyber pirates.

Pour exemple, rappelons l'action de niveau mondial de la gendarmerie française sur la neutralisation du botnet géant « Retadup » (actualité de fin août 2019).

Ci-après à titre indicatif, un tableau (figure 1) affichant les axes d'attaques, les tendances et les impacts majeurs liés aux cyberattaques. [Source / présentation GEN19 - conférence Cédric Richy[1] et Éric Wies[2]].

En France, lorsqu'une entreprise est victime d'une cyber-attaque, Gendarmerie Nationale ou Police Nationale sont les relais indispensables vers des équipes spécialisées en cyber criminalité.

Pour information, la gendarmerie française affiche à elle seule 5700 plaintes de cyber-attaques par mois.

[1] Cédric Richy : chef du groupe cyber-investigations créé au sein de la région de gendarmerie de Lorraine le 1er septembre 2017, spécialement dédié à la lutte contre la cybercriminalité.

[2] Éric Wies : après 15 ans au service de l'Université de Lorraine en tant que responsable de service informatique et de formateur en master sécurité (sécurité des systèmes), il a intégré la réserve citoyenne (bénévole) d'une part et l'INSEE en tant qu'ingénieur réseau d'autre part. Son implication dans la réserve couvre essentiellement deux axes : la prévention (avant l'incident), et l'explication et les moyens de protections (après l'incident).

ESCROQUERIES	EXTORSIONS DE FONDS	PIRATAGES INFORMATIQUES	ATTEINTES AUX PERSONNES	ATTEINTES A LA SECURITE NATIONALE	SERVICES ILLEGAUX EN LIGNE
FRAUDE A LA REPARATION INFORMATIQUE E	RANÇONGICIELS I E	CHEVAUX DE TROIE (RAT) E	USURPATION D'IDENTITE E H	ACTIVISME EN LIGNE I	MARCHES NOIRS EN LIGNE E
FAUX INVESTISSEMENTS BOURSIERS E	EXTORSIONS CIBLEES I E	BOTNETS / DDOS E	VIOLENCE MORALE H	INCITATION A L'EMEUTE I	CYBERCRIME EN TANT QUE SERVICE E
FAUX INVESTISSEMENTS EN CRYPTOMONNAIES E	SEXTORSIONS H	VOL DE CRYPTOMONNAIE E	CYBERHARCELEMENT H	APPELS A LA VIOLENCE CONTRE LES FORCES DE L'ORDRE I H	FRAUDE DOCUMENTAIRE E H
FAUX INVESTISSEMENTS EN "ICO" E		CRYPROJACKING E	DEFIS / CHALLENGES H	CYBERTERRORISME I H	TRAFICS DE STUPEFIANTS E H
FAUX INVESTISSEMENTS EN MATIERES PRECIEUSES E		FUITES DE DONNEES I E	PROXENETISME EN LIGNE H	ATTEINTE A LA DEMOCRATIE I	PRODUITS PHARMACEUTIQUES ET DERIVES E H
VENTES PYRAMIDALES DE CRYPTOMONNAIES E		DEFACEMENT E	ABUS SEXUELS SUR MINEURS I H		TRAFIC D'ARMES E
ESCROQUERIE AU RGPD E		PIRATAGE DE LA CARTE BANCAIRE E			
SIM SWAPPING E		PARTAGE DE LIGNE TELEPHONIQUE E			
ESCROQUERIE A LA CARTE BANCAIRE E		OBJETS CONNECTES E			
CLOUDMINING E		TRANSPORTS INTELLIGENTS E			
TYPOSQUATTAGE I E					

Figure 1 - source / présentation GEN19 conférence Cédric Richy et Éric Wies.

LEGENDE	
TENDANCE A LA HAUSSE	⇧
IMPACT ECONOMIQUE	E
IMPACT INSTITUTIONNEL	I
IMPACT HUMAIN	H

Zoom sur les objets connectés

Des plus grandes organisations au plus petites entreprises, dans de nombreux secteurs d'activité et corps de métier, les objets connectés sont une opportunité de croissance économique. Que ce soit pour sécuriser des personnes, optimiser services clients ou process de production, faire des économies, corriger des postures de travail, faire de la maintenance prédictive, etc. La combinaison capteur / collecte d'informations est source d'un volume énorme (voire plus) de data. Pour exploiter cette opportunité supplémentaire de business, l'entreprise doit « tout simplement » faire en sorte que ses applications, programmes et autres « mécaniques informatiques » internes, soient capables de communiquer avec tous ces objets connectés. Mais, c'est derrière ce « tout simplement » que sont embusquées des difficultés, auxquelles s'ajoute la question de la finalité de la récolte et de l'analyse de ce volume massif de données.

Pour une PME cela peut prendre des allures de casse-tête, où le risque de surcoût peut réduire à peau de chagrin toutes formes de bénéfices (financier en 1er), pourtant, c'est un marché très prometteur, liés à de réels besoins en face desquels produits et services se doivent d'être adaptés.

En même temps que les choix technologiques, se pose la question de la cybersécurité car à ce jour, les failles de sécurité dans l'univers IoT[3] ne sont pas une légende, d'autant que les cybercriminels ont une appétence particulière pour tous ces points d'entrée potentiels dans un système.

Pour toute dirigeant / patron de PME, ETI ou autre TPE, faire preuve de curiosité pour comprendre les enjeux de ces mutations / révolutions, est sans conteste un atout dans la démarche d'évolution numérique de son entreprise.

> 75 MILLIARDS D'OBJETS CONNECTES A INTERNET D'ICI 2025 [SOURCE IHS MARKIT]
>
> HORIZON 2022 LE MARCHE DE L'IOT DEPASSERAIT 1 000 MILLIARDS DE DOLLARS [SOURCE IDC]

En allant plus loin dans la réflexion, quid des problématiques d'éthiques lorsque l'IoT s'allie aux ressources humaines dans une organisation, ou encore de son introduction directement dans le corps humain ?

[3] IoT : Internet of Things

En Europe, dans un cadre d'expérience de réalité augmentée, dans un environnement professionnel pour déverrouiller portes, ou imprimantes, il y déjà des personnes porteuses de puces électroniques dans leur corps.

Nous avions abordé le sujet en compte rendu de l'événement Grand Est Numérique de septembre dernier, Olivier Buchheit[4] y animait une conférence intitulée « Transhumanisme, Société, Business : Rats, Cyborgs, Iot dans la chair ».

Un dossier dédié à ce thème est en préparation pour une publication prévue pendant ce mois européen de la cybersécurité.

Be secure,

Be curious

[4] Olivier Buchheit : ingénieur généraliste en mécanique et matériaux, docteur en physique du solide, actuellement médiateur technologique et scientifique dans l'enseignement secondaire et supérieur, ainsi qu'auprès d'instituts privés, publics, et du grand public, dans le domaine du digital (4.0, Intelligence Artificielle, Blockchain, Interaction Homme-Machine…).