Conférence sur les attaques informatiques du Mercredi 19 décembre 2018

Artema était présent à la table ronde sur les attaques informatiques organisée à la préfecture des Hauts-de-Seine en collaboration avec Cap'Tronic (programme public d'aide à l'innovation par l'électronique et le logiciel embarqué), l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et la DGSI (ex-DST + ex-RG). Le public visé : des dirigeants de PME franciliennes et de start-up, des responsables informatiques de grandes entreprises ou de laboratoires et des associations professionnelles.

Parmi les sujets abordés : le bilan 2018 des attaques informatiques, les enjeux de la sécurité des systèmes d'information, l'e-réputation des entreprises, les différentes attaques cyber et les solutions et recommandations face à ce risque. Dans le cadre d'une industrie de plus en plus connectée, la cybersécurité est un enjeu vital.

Pour aller plus loin : un portail est à la disposition des PME incluant une sélection de prestataires sélectionnés par l'ANSSI : www.cybermalveillance.gouv.fr et le MOOC de l'ANSSI : www.secunumaacademie.gouv.fr

1. Bilan 2018

Les attaques continuent et touchent même les organismes les plus sécurisés. **Elles passent régulièrement par la chaine logistique client/fournisseur** :

- Le Pentagone en novembre 2018 : fuite d'informations sur 33 000 personnels via l'agence de voyage interne,
- Le Ministère de La Défense australien : attaque sur leur système de marchés publics par des hackers chinois,
- La chaîne de grande distribution américaine Target : attaquée à travers son fournisseur de climatisation : 400 millions de $ de dégâts,
- Les serveurs téléphoniques de Moscou ont été piratés en décembre 2018.

Conseil : les entreprises doivent veiller à ce que leurs communications avec leurs fournisseurs soient bien sécurisées. **Les hackers « rebondissent » par les entités les moins sécurisées qui sont en contact avec leur cible.**

A noter : baisse forte en 2018 des attaques de rançongiciels à la différence de 2017 avec notamment WannaCry (300 000 ordinateurs infectés en mai 2017) qui a nuit chèrement à Renault, à Saint-Gobain, à Veolia et même à un hôpital, privé de son informatique. Croissance des tentatives d'attaques sur les crypto-monnaies autres que Bitcoin. La presse ne relate que le haut de l'iceberg car les attaqués restent souvent discrets (cyber-réputation). La cybercriminalité a rapporté 400 millions de dollars en 2015, 2000 en 2018.

Un label sécurité ANSSI va voir le jour en 2019 à destination des hébergeurs informatiques car ceux-ci hébergent des serveurs d'OIV (opérateur d'importance vitale pour le pays). L'ANSSI travaillent sur une dizaine de grosses affaires de piratage par an.

. . . / . . .

✉ Artema - 39, rue Louis Blanc – CS 30080 – 92038 La Défense Cedex
Tél : + 33 1 47 17 63 69 - Fax : + 33 1 47 17 63 70
www.artema-france.org - info@artema-france.org
Association 1884 – SIRET 353 550 817 00020 – APE 9411Z

2. Les enjeux de la sécurité des systèmes d'information

La chaine de sécurité informatique = SSI + Loi + Organisation interne + Processus métier.
80 % de la sécurité est atteinte à travers l'aspect humain.

a. *Les attaques par portes dérobées*

Une mise à jour de logiciel d'un fournisseur de logiciel a été piégée par des hackers chinois. Le fournisseur a mis un mois pour le voir (pas toujours évident à repérer) et la mise à jour a été téléchargée 2,2 millions de fois.

Il est recommandé de mettre à jour ses logiciels type Acrobat, Windows, Outlook, car les mises contiennent des protections contre les failles de sécurité. Pas à jour = failles possibles.

b. Attaques via de faux supports informatiques

80 % des attaques se font via l'ingénierie sociale (« bluff », imposture, pratiques de manipulation psychologique à des fins d'escroquerie).

c. Fraude au président : toujours vivace

- Pathé : 19,2 millions d'euros (record) en mars via la holding des Pays-Bas. Mise en œuvre digne d'un service secret étranger.
- Un Conseil Général : 800 000 euros.

Conseil : l'entreprise attaquée doit déposer plainte. Il faut sensibiliser les comptables à ce type d'attaque.

d. le phishing ou hameçonnage

L'ANSSI constate qu'il y a toujours 5 % des destinataires de messages de type phishing (des spams) qui cliqueront sur le lien suspect. **Conseil : la formation des salariés couplée à des mesures de bon sens.** La sensibilisation doit être personnalisée avec des cas d'usage sur le métier des salariés.

e. les malveillances internes

16 % des attaques sont le fait d'employés ou ex-employés. Motivations : financière, vengeance (30 à 50 % des attaques de ce type en France), concurrence.
Conseil : quand un salarié s'en va de l'entreprise, il faut veiller à lui couper ses accès informatiques (VPN, mail, etc.). Il faut compartimenter les droits informatiques des utilisateurs. Avoir une charte informatique et un règlement intérieur sur le sujet de la confidentialité.

f. IOT

L'attaque d'un IOT est souvent en vue de sabotage par des hacktivistes type Anonymous, éco-terroristes : c'est le **cyber-sabotage**. Cibles régulières : banque, énergie, transport.

Les attaques sur des systèmes industriels vont croître (chantage, rançon). En mars 2016, une hydrolienne au large d'Ouessant a été piratée (Sabella).

. . . / . . .

✉ Artema - 39, rue Louis Blanc – CS 30080 – 92038 La Défense Cedex
Tél : + 33 1 47 17 63 69 - Fax : + 33 1 47 17 63 70
www.artema-france.org - info@artema-france.org
Association 1884 – SIRET 353 550 817 00020 – APE 9411Z

Le Wifi doit être protégé correctement et bien géré ; en effet, il permet de contourner la sécurité informatique d'une entité s'il est ouvert et piraté. Attention aux boitiers ADSL non-autorisé au sein de l'entreprise qui créé des failles de sécurité dans le système.

A l'heure actuelle les voitures connectées seraient bien mieux sécurisées que par le passé. Enjeu : la voiture autonome dont un malveillant prendrait le contrôle.

g. Typologie des attaquants

Quelques nouveautés :

- Industrialisation de la pratique : professionnalisation, découpage des tâches telle une taylorisation, des spécialisations, des filiales,
- Location de hackers et de compétences, marché noir sur le dark web,
- Des vendeurs de faux antivirus qui permettent à des hackers de pénétrer les systèmes protégés par ces deniers.

3. L'e-réputation

Warren Buffet : « *il faut des années pour construire une réputation et quelques secondes pour la détruire.* »

Des entreprises forment à la communication de crise cyber, avec des mises en situation afin que l'entreprise soit préparée et exercée. Le plan de crise doit être géré avant la crise. Qui doit dire quoi ? Quels sont les éléments de langage.

Il est bien pour une entreprise de faire réaliser un audit de son e-réputation (sites, Google Image, réseaux sociaux, etc.) afin d'effacer éventuellement des informations nuisibles, repérer des parasitismes (faux comptes au nom de l'entreprises, faux employés, problème des « caches » qui ne sont pas effacés). Un back-up des serveurs, externalisé et déconnecté, est important.

✉ Artema - 39, rue Louis Blanc – CS 30080 – 92038 La Défense Cedex
Tél : + 33 1 47 17 63 69 - Fax : + 33 1 47 17 63 70
www.artema-france.org - info@artema-france.org
Association 1884 – SIRET 353 550 817 00020 – APE 9411Z