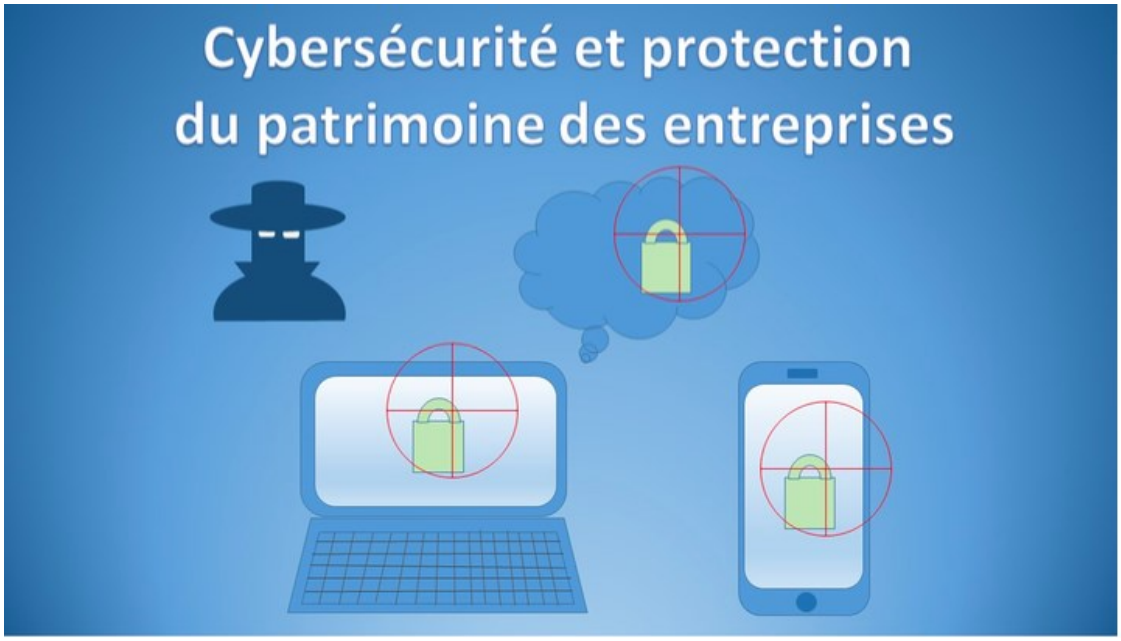
Cyber sécurité et protection du patrimoine des entreprises

Nano-INNOV - Palaiseau

Lundi 1 octobre 2018



Coordination Scientifique

Samuel Evain (CAP'TRONIC), Patrick Legand (Xirius Informatique)

Editorial Board

Dr. Christophe Calvin (CEA)

Mr. Laurent Duplouy (BnF)

Mr. Philippe Wlodyka (Polytechnique)

Mr. Pascal Pavel (CEA)

Dr. Thiên-Hiêp Lê (ONERA)

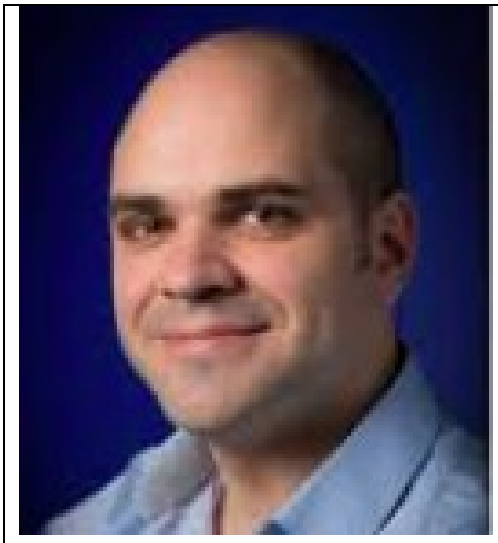
Ms. Katia Castor (Association Aristote)

Cyber sécurité et protection du patrimoine des entreprises

Séminaire Aristote, 01/10/2018 à Nano INNOV

Coordination scientifique

Samuel Evain (CAP'TRONIC), Patrick Legand (Xirius Informatique)



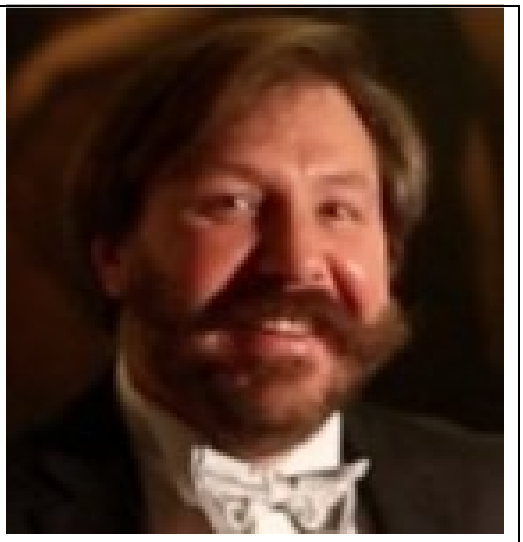


Table des matières

Compte-rendu des interventions

Introduction

Samuel Evain (Cap'tronic), qui a préparé ce séminaire avec Patrick Legand (Xirius Informatique), introduit la journée.

Il invite Christophe Calvin, le président d'Aristote à dire quelques mots. Celui-ci annonce les prochains séminaires, le 6 décembre à EDF-Lab (Réinventer l'informatique. Au-delà des architectures von Neumann). Il sera précédé le 15 novembre par un autre séminaire, celui-là sur l'intelligence artificielle. Il présente aussi Katia Castor qui remplace Régine Lombard au secrétariat de l'association.

Christophe Calvin

Katia Castor

Samuel Evain reprend la parole pour introduire le thème du séminaire. Les entreprises sont en effet sujettes à des vols de prototypes et se posent des questions. Hélas, aucune aujourd'hui n'ose dire comment elle a été victime, car personne ne s'en vante. Pour faire le tour de la question, la journée commencera par l'état de la menace, puis les préconisations, le rôle de l'homme et la façon de survivre à une attaque.

1. Etat de la menace

Orateur DGSI (Ministère de l'Intérieur)

2. Présentation du CLUSIF et panorama des incidents de cyber sécurité

Thierry Matusiak (IBM & CLUSIF)

Thierry Matusiak présente Panocrim, le panorama de la cybercriminalité de l'année 2017. Il est un membre actif du Clusif, une association de 700 professionnels de la sécurité de l'information en France qui publie sur cette thématique, organise des conférences, des ateliers et réalise chaque année ce Panocrim.

Thierry Matusiak décrit pour 2017, ce qui s'est passé concernant les attaques destructives, les attaques via des tierces parties, le Cloud et l'IoT et enfin les bitcoins.

Parmi les attaques destructives, il cite Petya qui a commencé à œuvrer en 2016. Il y a maintenant 4 versions. Les shadow brokers, un groupe de pirates, se sont attaqués à Equation group, de la NSA. Ils ont mis à disposition de tous le 14 avril 2017 les outils dérobés à la NSA. Cela a donné Wannacry, qui est très virulent, et se propage très rapidement (230 000 postes infectés dans 150 pays en une journée). Les conséquences ont été moindres que ce qu'on pouvait craindre (une dizaine d'entreprises en France, pas de particuliers, inefficace sur Windows XP) grâce à la réaction rapide due à une forte mobilisation et à la création de killwitch par un chercheur pour stopper Wannacry.

Puis est arrivé NotPetya, un wiper qui détruit sans restaurer. Le 4 juillet 2017, les pirates ont demandé une rançon pour fournir la clé de chiffrement. NotPetya est moins virulent que Wannacry, mais plus dangereux. Il a fait moins de dégâts. En bilan, la sensibilisation du grand public s'est améliorée comme la prise de consciences de certains dirigeants et le développement d'outils de contremesure. Mais il y a eu des pertes financières et un climat de méfiance entre les Etats.

La deuxième thématique de Panocrim est l'attaque via des fournisseurs comme Apple. Si vous êtes bien protégé, c'est une porte d'entrée des pirates. En cause, des bourdes

d'éditeurs de confiance (Apple, HP, Microsoft), mais aussi des problèmes de fond plus graves, comme Krack qui permet d'insérer une nouvelle clé de sécurité dans les connexions wifi. Ou chez Intel, une faille au niveau des cartes mères. En début d'année 2018, Meltdown et Spectre sont apparus. Ils concernent plusieurs milliards de processeurs, mais permettent uniquement d'accéder à des données en mémoire. Intel a averti de ne pas télécharger Spectre. Une version corrompue de Ccleaner a touché 2 270 000 ordinateurs dont ceux de 18 grands groupes.

Une menace moins visible mais présente est le piégeage des infrastructures. Par exemple, CloudHopper a ciblé les infogérants. Cela a commencé en 2014 (15 pays ciblés, plus de 70 variantes de backdoor et de trojans utilisés.) La problématique commune de ce type d'attaques est l'effet de masse. Il faut donc anticiper ce risque systémique en observant les comportements des ressources autorisées et être capable d'isoler les machines infectées.
En ce qui concerne le Cloud, un cas intéressant concerne la NSA et l'armée américaine. Des documents top secret ont été exposés sur les serveurs sur AWS S3 via l'entrée INSCOM. À travers Amazon Web Services, le Pentagone a laissé l'accès public à des milliards de données collectées en ligne pendant plusieurs mois voire plusieurs années. Accenture a aussi été victime d'une fuite de données suite à l'exposition de plusieurs espaces de stockage AWS S3. En 2016, Uber a subi une attaque de deux pirates qui ont dérobé plus de 50 millions de comptes clients. Uber a payé la rançon pour tenir l'attaque secrète, mais les données ont quand même été revendues. Deloitte a aussi subi un vol des données. Pour toutes ces attaques, il aurait fallu gérer les niveaux de privilège de façon différenciée, changer régulièrement les mots de passe, avoir plusieurs facteurs d'authentification et restreindre les privilèges ou droits d'accès au strict nécessaire. Car comme le volume de données dans le Cloud ne cesse de grossir, les surfaces d'attaques augmentent avec des risques potentiellement plus importants.

Autre point du panorama 2017, les vecteurs d'attaques des objets connectés. Fin 2016, Mirai utilisait les images des caméras des objets et on prédisait que les voitures allaient être volés. Mirai a été réutilisé en 2017 et amélioré. Mais depuis avril 2017 il y a des attaquants « gentils » qui prennent le contrôle de votre machine pour nettoyer le net. Plusieurs démonstrations ont été faites qu'on pouvait utiliser les objets connectés pour passer une commande à votre place. En décembre 2017, la CNIL a mis en demeure Genesis Industries limited de détruire la poupée My friend Cayla et le robot I-QUE. Il n'y a pas que des jouets. Un aspirateur autonome comporte un gyroscope, un capteur de distance, une mémoire des milieux nettoyés, ce qui permet de cartographier la maison.

Dernier point du panorama, les bitcoins, sujet majeur en 2017 et 2018. L'explosion du cours en 2017 a attisé la convoitise des hackers. Et cela sur toute la chaine des bitcoins. Cela commence sur le minage (NiceHash a perdu près de 64 millions de dollars). La couche d'échange (ICO) est aussi attaquée de même que l'utilisateur.

3. Les préconisations de l'ANSSI

Patrice Bigeard (ANSSI)

Patrick Bigeard, de l'ANSSI, commence par dire que la meilleure défense, c'est … la défense. Aujourd'hui, les attaquants vont plus vite à réaliser de nouveaux codes d'exploitation que les défenseurs à mettre à jour les systèmes d'information. Le nombre de sites web non légitimes augmente beaucoup.

L'ANSSI, créée le 7 juillet 2009, qui dépend du Secrétariat général de la défense et de la sécurité nationale (Premier Ministre), propose des règlements et est un opérateur de sécurité. Elle essaie de comprendre et détecter les menaces. Ses deux principaux domaines de compétences sont d'être une autorité de sécurité (la prévention) et une autorité de défense (la réaction) et non le renseignement ou l'action offensive. L'ANSSI qualifie les produits et les services de confiance et contribue au développement de produits gouvernementaux ou commerciaux. Dans le cas d'une attaque majeure, c'est elle qui décide des mesures de protection à appliquer. Comme les autres intervenants, Patrice Bigeard conseille de sensibiliser, former, éduquer les utilisateurs et effectuer des sauvegardes. Il note que les attaques réussissent à cause de sensibilisation insuffisante, de systèmes non mis à jour, d'une mauvaise gestion des mots de passe et du manque de séparation des usages (utilisateur/administrateur). Il faut ajouter le laxisme des droits d'accès, l'absence de surveillance des SI, l'absence de restrictions (périphériques) ainsi que le nomadisme et le télétravail incontrôlés. Les tendances sont à l'augmentation du nombre d'attaques, de la sophistication des codes malveillants, au développement des attaques par point d'eau et des DDoS, et des surfaces d'attaques, sans compter que l'IoT complique les choses.

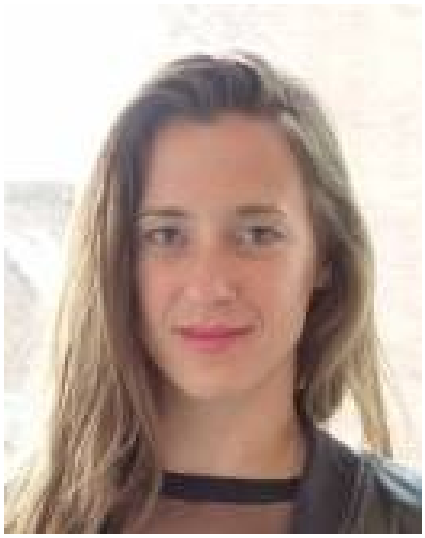
Patrick Bigeard insiste pour que les dirigeants d'entreprise se forment régulièrement à la cyber sécurité, se demandent si leur entreprise est une cible potentielle, s'ils ont pris toutes les précautions concernant les informations et les échanges et qu'ils mettent l'argent nécessaire au suivi de sécurité. L'analyse du risque est fondamentale. L'ANSSI édite les 42 règles de sécurité dans son guide d'hygiène informatique et le guide des

bonnes pratiques informatiques. Pour aller plus loin, il conseille le MOOC de l'ANSSI à suivre sur https://secnumacademie.gouv.fr.

4. La sécurité oui ! Mais jusqu'où ? Faut-il avoir peur ?

Judith Nicossian (Anthropobiologiste)

Judith Nicogossian, en tant qu'anthropobiologiste, travaille sur l'adaptabilité du cerveau.



La relation au monde est changée avec le digital. On sombre dans les données. De nombreux dispositifs existent pour relier des sites très distants. La réalité augmentée avec avatars nous emmène dans des mondes virtuels… la cryptographie maintient la confidentialité et la non-répudiation avec le https. Les problèmes viennent de l'utilisation qui en est fait. On se retrouve face à un double digital qui circule sans qu'on en soit lucide. L'attaque peut être algorithmique (mathématique) ou les solutions, par la faute des entreprises ou le business des failles. Nos données sont habituellement anonymes mais il est possible de ré-identifier car nos données sont reliées à d'autres données géolocalisées. Or, comme le dit Reporters Sans Frontières, chiffrement et anonymat sont indispensables à la liberté numérique. Il faut savoir chiffrer. La plupart des risques sont extérieurs mais il en existe à l'intérieur des machines via les poubelles, les post-its ou l'historique Word. L'IoT nous rhabille. Le facteur humain est instable au vu de l'expérience Sophie Perso : une clé USB était posé par terre dans un parking avec écrit dessus « Sophie perso ». Tous les passants l'ont branchée sur leur ordinateur. Il faut échanger sur VPN, ne pas laisser trainer ses données, choisir ses mots de passe. Mais si on fait une erreur, on apprend et on évite que cela se reproduise.

Souvent on donne ses données par consentement. C'est plus simple de ne pas lire les conditions d'utilisation. Car on est prêt à tout donner pour avoir un service gratuit. Mais quel prix donne-t-on à la vie privée ?

Données et sécurité génèrent des questions, car elles heurtent nos sens. L'authentification par empreinte digitale ou l'iris ne fonctionne pas. La seule est la relation directe et le retour au réel. En attendant, il faut systématiser l'utilisation des

VPN, arrêter ses comptes Google et être conscient que les données sont « données » pour toujours.

5. L'obligation de sécurisation des systèmes d'information

Marc-Antoine Ledieu (Bardehle-Pagenberg)

Les problématiques de Marc-Antoine Ledieu sont le machine Learning et les contrats à rédiger.

En tant qu'avocat, l'image qu'il a de la sécurité informatique est quelque chose de très verrouillée. Mais c'est une porte blindée qu'on croit bien sécurisé, mais qui est en fait ouverte. Il faut donc sécuriser. C'est même obligatoire selon le RGPD. Il faut des conditions a minima de protection de toutes les data du SI (personnelles et autres). Les mesures appropriées sont le chiffrement et la pseudonymisation. Les responsables des data comme les prestataires sont astreints aux mêmes obligations sous peine de sanctions pécuniaires (2% du CA). Il y a violation de données par accès non autorisé ou pire. Par négligence, on peut être sanctionné. Le chiffrement doit concerner les back-up. En France, la législation crypto commence à dater (2004). Il faut pourtant garantir un niveau de sécurité adapté aux risques, compte tenu de l'état des connaissances, des couts, de la nature, de la portée, du contexte… Mais concrètement, la jurisprudence a débuté en 2014. Il y a eu 9 délibérations. Souvent avec condamnations. 35 000 ID exposés chez Hertz : sanction 40 000 €. 912 000 ID exposées chez Darty : sanction 200 000 € car Darty aurait dû procéder aux vérifications du logiciel de son prestataire. 350 000 ID exposés chez Optical Center : sanction 250 000€. Chez Daily motion (juillet 2018) qui a subi une attaque coordonnée pendant plusieurs mois, un mot de passe était inscrit en clair dans le code source. Sanction 50 000€ malgré l'audit trimestriel de la société.

La Cnil contrôle le fonctionnement des mesures de sécurité et les contrats qui doivent être complets en ce qui concerne la sécurisation des données.

La loi SRSI (sécurité des réseaux et systèmes d'information) du 26 février 2018 (arrêt du 13 juin 2018) oblige de manière contraignante de sécuriser tout ce qui concerne le SI (logiciel, données, serveur, backup) c'est-à-dire être capable de résister à des incidents

(attaques). Cela concerne les opérateurs de service essentiel (comme les opérateurs d'importance vitale) et les fournisseurs de service numérique (place de marché en ligne, moteur de recherche en ligne, services d'informatique Cloud) de + de 50 employés et de + de 10 M€.

C'est l'ANSSI qui contrôle et qui peut mettre en demeure les dirigeants de se conformer aux obligations dans un délai qu'elle fixe.

6. Aspects réglementaires (OIV, LPM, RGS, ISO). L'effet boule de neige !

Patrick Legand (Xirius Informatique)

Patrick Legand accompagne les entreprises dans la sécurité informatique et la défense.

Selon lui, on vient de loin. Avant 2005, personne ne parlait de sécurité hormis les hackers. Pourtant en 2000, à l'étranger, on fabriquait déjà du malware à des fins militaires. Il y avait des exigences contractuelles mais pas de réglementation. Ce qui a changé, c'est le livre blanc sur la défense et la sécurité nationale en 2008, suivi de la création de l'ANSII en 2009. Le référentiel général de sécurité date de 2010. Il concerne les administrations et comporte l'obligation d'homologuer les systèmes. En 2013, un deuxième livre blanc a commencé à parler des OIV (opérateurs d'importance vitale). Plus les années passent, plus la sécurité informatique est prise en compte. Les services de renseignements, la défense, les banques, les administrations en faisaient déjà. Cela a fait effet boule de neige. La dématérialisation a amené des services de confiance. L'avantage concurrentiel partagé est devenue une obligation pour être certifié. Les clauses de sécurité dans les contrats, et la formation maintenant normale, ont fait que la sécurité est rentrée dans les mœurs. Les prestataires de détection d'incidents ou de réponses aux incidents se créent. Cependant, on remarque que les protocoles impénétrables sont abandonnés, que les administrations font de la résistance, que les budgets ne suivent pas, qu'il y a des produits farceurs, des erreurs qui tuent et que les attaques sont bien ficelées.

Dans 10 ans, il y aura du plus et du moins. Côté plus, la maturité, la maîtrise de la sécurité dans les systèmes industriels et les objets connectés et davantage de dématérialisation. Côté moins, une sophistication des attaques, des objets connectés incontrôlables, la fin de la confidentialité et l'IA au service du hacking. Vers quel côté cela penchera-t-il ? Tout dépendra des jeunes qui vont prendre le pouvoir.

7. L'audit de sécurité, pour quels objectifs et par quels procédés ? Retour d'expérience

Damien Cauquil (Digital.Security)

Damien Cauquil fait un tour des différents audits des SI.

Ils servent d'abord à connaître la situation réelle et à la comparer à celle supposée, mais aussi à éprouver les capacités de détection et de réaction face à une attaque. Rappelons-nous les reportages après l'attaque de TV5 Monde où les journalistes filmaient la salle de crise dans laquelle les mots de passe étaient visibles accrochés au mur. Les audits servent aussi à calculer la probabilité de réalisation des pires scénarios et ce qu'on peut perdre. Il existe une grande variété de types d'audit : analyse et cartographie des risques, audit de configuration, test d'intrusion, points de présence sur internet, tests de réseaux wifi, des systèmes connectés, des campagnes de hameçonnage, des test Red Team.

Les audits varient aussi par les contextes de réalisation (niveaux de connaissances de la cible par l'attaquant, type d'attaquants, types d'actions autorisées). Mais que souhaite-t-on vérifier ? Savoir ce qui peut arriver de pire ? Alors il faut faire une analyse de risque par cartographie et avoir une connaissance complète du contexte. Cela apporte beaucoup mais est long et coûte cher. Pour savoir ce qu'un pirate peut faire de pire, il faut un test d'intrusion dans un contexte externe. Les audits PASSI concernent les OIV. Ils sont faits par des prestataires certifiés et doivent se dérouler dans des conditions strictes.

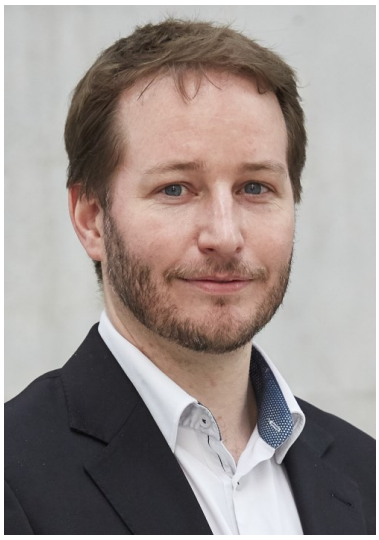
Il faut donc savoir si on veut un résultat exhaustif. Si oui, il faut une boîte banche mais cela prend du temps. La boîte grise est un compromis permettant d'optimiser les tests. En ce qui concerne l'IoT, les cibles sont variées (plateforme Cloud, serveurs applicatifs, appli mobiles, matériels, protocoles de communication variées). Il faut avoir au moins deux exemplaires pour le matériel, cela prend encore plus de temps et il faut envisager les attaques physiques. L'ensemble demande des compétences variées.

Damien Cauquil conclut par le top 10 des erreurs qu'il a rencontrées. Il montre une serrure connectée qui donne les informations d'ouvertures et fermetures quand l'appli demande une authentification. Il poursuit par un cadenas connecté facilement ouvrable, ce qui ne sert à rien. À noter aussi des erreurs cryptographiques, des mots de passe par défaut, des mises à jour non sécurisées, des mauvaises conceptions électroniques, des mauvaises utilisations des protocoles de communication et des interfaces de débogages non interdites.

8. Lokly : Solution de transport d'informations sensibles dans un contexte de mobilité multi-support

Benoît Berthe (Vandelay)

Benoit Berthe reconnaît que les clés USB sont le maillon faible de la sécurité informatique.



Si on va à l'étranger et qu'on doit transmettre des données, la clé USB est fondamentale. Elle sert aussi dans l'industrie pour mettre à jour les automates et autres machines. Il s'en vend 500 millions par an dans le monde pour un marché d'un milliard d'euros. Vandelay a été créée en 2015 pour sécuriser ces clés. Car la clé USB a des limites : l'authentification par code à 4 ou 6 chiffres reste simple, l'empreinte digitale aussi. Elle offre une faible protection en cas de perte. Et les solutions de sécurité sont complexes. De plus, c'est le grand vecteur d'attaque informatique. Une badUSB peut être comme une clé USB normale, mais peut aussi se présenter comme un port mural ou autre. Ces badUSB se vendent sur internet, se programment facilement et peuvent enregistrer des scénarios d'attaque. Le principe est de faire croire à un ordinateur qu'il est autre chose, comme un clavier comme si il y avait un homme qui tapait des commandes. Il y a aussi les USB killer qui détruisent le smartphone ou l'ordinateur en le grillant.

Pour tous ces risques, Vandelay a développé Lokly qui comporte une clé USB connecté en buetooth 4.2 sécurisé à votre smartphone. Il n'y a pas de pilote ou de logiciel. Le bluetooth fonctionne à moins de 10 mètres. Si on s'en éloigne, le smartphone avertit qu'on a oublié la clé et la bloque automatiquement. Lokly comporte aussi un port USB femelle qui sert de filtre pour les badUSB et USB killer. Ainsi au pire, c'est Lokly qui grille et non l'ordinateur. La batterie intégrée permet de transférer des données par le smartphone sans toucher à l'ordinateur. L'appli est simple et cloisonne les données que la clé contient. Les concurrents n'offrent pas tous ces services pour un prix comparable.

Vandelay pense à faire de même pour des badges d'entrée, des démarrages de véhicules ou de machines industrielles.

9. Cyber attaques : retour d'expérience sur la remédiation de systèmes compromis ou hors services

Didier Pilon et Mohammed Bakkali (Zyroc)

Didier Pilon et Mohammed Bakkali dirigent la PME Zyroc, une spin-off de l'ANSSI.

Que fait-on une fois que l'on a été attaqué ? On distingue 3 types de compromission : 1/un système down comme chez Saint-Gobain. 2/Un attaquant actif et présent. 3/Un système compromis dont l'action est ancienne.

Les 5 phases de la remédiation sont les mêmes quel que soit le type d'attaque. Il faut d'abord initialiser, c'est-à-dire prendre contact avec le système compromis et son contexte afin d'identifier les mesures d'urgence. Chez Saint-Gobain (seul exemple dont il peut parler), Didier Pilon a demandé de couper le réseau tout de suite. Cela a évité le chiffrement des machines à l'étranger. Il faut aussi savoir s'il y a des contraintes pour garder les preuves au niveau juridique et savoir quels métiers sont impactés. Sans oublier la communication de crise et l'identification du responsable. Il faut aussi faire comprendre la situation pour que le responsable l'accepte. Il faut être meilleur que l'attaquant sur la connaissance du SI, ce qui n'est pas facile car le hacker a eu le temps de comprendre le Si avant d'attaquer. Le travail de remédiation est aussi psychologique. L'attaqué passera forcément par différentes phases : de la sidération puis du déni, de la colère, du marchandage, de la dépression puis de l'acceptation pour enfin s'investir. La collecte d'information durant cette phase d'initialisation concerne les acteurs victimes (mêmes collatérales), le côté juridique, technique… Et le prise des mesures d'urgence en impliquant le top management (Saint-Gobain a perdu 250 M€ de CA en 14 jours), en vérifiant les obligations légales, en caractérisant la compromission, en créant une équipe dédiée à la résolution de l'incident.

Seconde phase, l'investigation qui consiste à cartographier le SI et à collecter les informations sur les processus. Il faut aussi faire une analyse du MOA et vérifier le respect des bonnes pratiques de sécurité comme la détermination des machines compromises. Après cette phase, on est capable de proposer des scénarios pour rétablir le service informatique.

La préparation, qui dure environ trois mois suivant la complexité du SI, va définir la gouvernance de la remédiation, choisir le scénario, définir les paramètres de durcissement du SI tout en administrant ses composants sensibles. Plus la préparation est bien faite, plus la remédiation sera efficace. Plusieurs chantiers sont à traiter : en premier la brique « identité », puis le réseau, les données, les serveurs, les postes de travail et le système de sauvegardes et de stockages. Comme on ne peut être juge et partie, une autre équipe vérifie que l'équipe dédiée fait bien son travail. Il s'agira soit de contenir la compromission et protéger les assets, soit d'effectuer la remédiation en ligne si on ne peut pas arrêter le service, ou offline pour remédier les services d'authentification et des systèmes compromis. Autre solution, créer un nouveau Si en parallèle qui permet de recréer les parties applicatives les plus sensibles. On se rend compte que l'authentification centralisée est plus sûre qu'une authentification locale.

Les phases suivantes sont le rétablissement sécurisé, puis enfin la stabilisation du SI. Mais en conclusion, il ne faut pas se retrouver en mode crise.

10. Le transfert du risque cyber à l'assurance

Christophe DELCAMP (FFA)

Christophe Delcamp commence par montrer la courbe empirique de Farmer qui présente la fréquence décroissante des risques acceptables, inacceptables ou majeurs.

La Fédération Française de l'Assurance (FFA) considère que le risque c'est l'alea multiplié par la vulnérabilité des enjeux. Il faut donc connaître les deux paramètres. La FFA commence à développer des connaissances sur le risque de sécurité informatique, mais n'y connaît hélas pas grand chose, ce que les assureurs n'aiment pas. Surtout que le temps et l'espace n'existent pas en sécurité informatique contrairement aux autres domaines de l'assurance. Le point le plus important est de maîtriser le cumul des engagements. Si Wannacry demande 5 m€ par site et qu'il touche un million de sites, le système explose. Depuis cette année, il est obligatoire de notifier les incidents. Une question reste en débat : faut-il assurer les amendes administratives et les rançons ? La FFA a rédigé un document pour les TPE et PME sur le risque cyber. Les garanties existantes concerne les erreurs humaines (incendie, altération des données) ou la malveillance (idem + fraude). Les contrats mutli-risques DAB classiques couvrent tout sauf ce qui est typiquement cyber (la gestion de crise, frais de notification. Les contrats cyber peuvent prendre en charge les dommages directs, les frais dus à une cyber extorsion, mais pas le risque juridique pénal. Il y a aussi des parties cyber assurées dans les contrats Responsabilité Civile et Dommages aux biens. Mais il faut un dialogue entre l'assurance et l'assuré tout en respectant la confidentialité des échanges et des données transmises.

Christophe Delcamp termine en signalant que, pour savoir ce qui est assuré, il faut cartographier les risques. C'est une habitude chez les assureurs. Un dernier point concerne le RGPD. Il introduit une culture du risque au sein de toutes les entreprises et instaure un dialogue entre les entreprises et la Cnil. Christophe Delcamp trouve cela plutôt rassurant.

En conclusion de la journée, Samuel Evain (Cap'Tronic) remercie les participants et donne la parole à Patrick Legand (Xirius Informatique). Celui-ci fait un tour d'horizon des interventions. Il a noté qu'il existe des outils pas chers. Et qu'on devient de plus en plus sous la coupe de nos données. Malgré les années qui passent, il y a toujours des failles dans les logiciels, ce qui laisse la place aux attaques surtout avec l'émergence des objets connectés. Il note aussi que les humains sont facteurs d'erreurs et qu'il y a encore beaucoup de sujets ouverts et de débats sur le sujet.