Cyberdéfense et détection du hacking

École Polytechnique - Palaiseau

Jeudi 1er décembre 2016

Coordination Scientifique

Patrick Legand (Xirius Informatique)

Partenaire

Editorial Board

Cyberdéfense et détection du hacking

Séminaire Aristote, 01/12/2016 à l'École Polytechnique

Coordination scientifique

Patrick Legand (Xirius)

Table des matières

Compte-rendu des interventions

Introduction

Patrick Legand, de Xirius Informatique, est l'organisateur du séminaire qu'il introduit. Il souhaite la bienvenue à la soixantaine de personnes présentes. Il propose le séminaire en plusieurs parties. Comme on constate un nombre accru d'attaques, il a fait venir des personnes qui présentent l'état de la vulnérabilité afin qu'on ait une vision pratique du risque qui pèse sur les entreprises et les services étatiques. Puis d'autres présentations traiteront des ATP, des malwares et des ransomwares. Il y aura aussi des retours d'expériences en France et en Europe.

1. Retour sur un cas historique : Enigma, 2ème guerre mondiale

Patrick Legand (Xirius)

C'est lui qui commence le séminaire par, dit-il, un moment de récréation.

Durant la seconde Guerre mondiale, la sécurité a été poussée très loin avec la machine Enigma. Auparavant il n'y avait pas de chiffrement, hormis de la substitution alphabétique, ce que faisait déjà César. C'était simple. À partir du Xème siècle, on s'est rendu compte que ce système était sensible aux fréquences (en français, le « e » apparait beaucoup souvent que les autres lettres). Une analyse des fréquences permet de trouver quelle lettre remplace les lettres les plus utilisées, en premier lieu le « e ». Dans « le Scarabée d'or », Edgar Poe montre comment on déchiffre ce genre de code. Au lendemain de la 1ère Guerre mondiale, le chiffrage de Vigenere n'utilise pas une clef, mais plusieurs. Patrick Legand en fait une démonstration. Chaque lettre du message clair est chiffrée suivant le code de la lettre précédente. Ce chiffrage a été un peu utilisé pour les machines de chiffrement. C'est sur ce principe, qu'en Allemagne, une machine qui allait devenir Enigma a fonctionné. L'idée est de partir d'un clavier dont les lettres passent dans un rotor qui relie chaque point d'entrée à un point de sortie. Avec Enigma, il y avait 3 rotors de 26 lettres et un réflecteur qui réinjecte le signal dans le circuit afin de retrouver le message en clair. Avec 3 rotors, il y avait ainsi 26x26x26= 17578 possibilités, qui pouvaient s'inverser. Il y avait en tout 10 millions de milliards de chiffres possibles.

Les Français ont tenté d'en savoir plus. Ils avaient ciblé une personne de l'équipe Enigma, l'ont rencontré et ont récupéré les plans. Mais c'était trop compliqué. Ils ont abandonné. En Pologne, on a décidé de « casser » la machine. Ils en ont construit une

réplique avec les plans récupérés par les Français et ont engagé des cryptanalystes doués comme Marian Rejewski pour analyser les failles possibles du protocole. Patrick Legand entre alors dans la technique de chiffrement de la machine. Les Allemands avaient compris qu'une clef ne devait pas être utilisée trop longtemps. Ils diffusaient des carnets de codes quotidiens avec tableau des connections, réglage et orientation des brouilleurs. Mais il y avait tellement de messages que même une durée d'une journée était trop longue. Le chiffrement de la nouvelle orientation était répété deux fois. Ce qui était une faille dont Marian Rejewski a profité. Il a trouvé les différents chainages possibles, ce qui donnait une signature de la position de rotors. Au lieu de 100 millions de chainages possibles, il n'y en avait que 105 000 qu'il a établi un par un en 9 mois.

Il a donc fallu une toute petite erreur (le doublement de l'écriture de la clef) pour casser le code Enigma. Cela donne une leçon pour les techniques de chiffrement actuelles.

2. La détection en temps réel des menaces persistantes avancées.

Philippe Baumard (Akheros)

Philippe Baumard est le fondateur de la start-up Akheros, créée en décembre 2012. Le premier contrat était avec Airbus. Son métier est la détection des comportements à très haut risque échappant aux contrôles normatifs. Après l'aéronautique, avec son équipe qu'il présente, il s'intéresse aux applications bancaires.

Par l'apprentissage machine, ils détectent des comportements atypiques sans avoir recours à une qualification préalable des « interdits » et des « autorisés ». Cet apprentissage, unique, fournit une évaluation constante et automatique de toute déviation incohérente avec « l'ADN comportemental ». Chaque point du grid a un modèle comportemental.

Il revient sur les problématiques liées aux APT. Ce sont des campagnes d'attaque, asynchrones, dormantes, sur déclencheurs IA. Les détections par signatures sont souvent inefficaces, car elles arrivent trop tard. Les attaquants sont expérimentés. L'élévation de privilège n'est pas systématiquement suivie d'une attaque immédiate. Du coup, la détection doit être téléologique. Il faut établir l'existence d'une coordination qui ne suit pas forcément l'archétype du cycle de l'APT.

Il y a des obstacles à la détection. Il y a une logique de compromission grise. Avec l'élévation de privilège, on glisse en zone noire. Les approches usuelles sont les détecteurs d'abus (liste noire), d'anomalie (déviation de la ligne nominale) avec des excès de faux positifs et qui ne détectent pas le comportement des super-administrateurs. Autre approche usuelle, le renseignement humain sur les groupes actifs et la détection des mégasignatures comportementales.

Philippe Baumard prend un exemple concret : Snowden, un agent technique autorisé et légitime mais sortant de son rôle à la NSA, l'agence de renseignement électromagnétique américaine. Il a réparé le back-up du département de déchiffrement. Bine noté par ses supérieurs, on lui a offert un emploi dans le Tailored Access Operations, le top du top à la NSA. Mais il a décliné. C'est lui qui concevait le front end pour l'accès aux bases de données de l'intranet. Il n'a brisé aucune protection chiffrée, jamais convaincu ses collègues de lui remettre leurs logins et leurs mots de passe. Il est dans la zone verte. Akheros essaie de modéliser les habitudes (fichiers déplacés, clés USB utilisées, géographie, interactions). Le tout sans a priori et sans règles préétablies. La comparaison du modèle comportemental avec l'action réelle mesure l'écart en termes de singularité, de surprise, de nouveauté, d'incongruités.

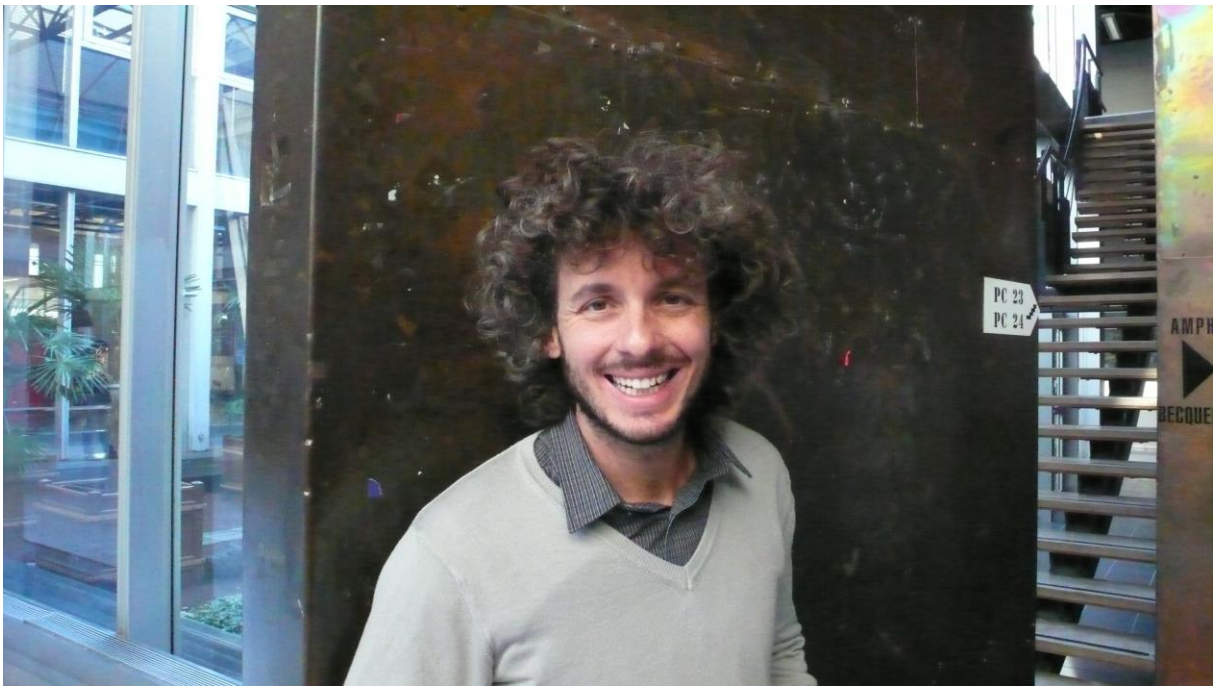
Dans le secteur bancaire, un client d'Akheros a donné 127 000 entrées de logs sur une journée. La société de Philippe Baumard a identifié 5 profils comportementaux déviants en 1 minute. En qualifiant bien un problème, on peut d'autant mieux mesurer l'atypisme d'une action.

Aujourd'hui, Akheros développe ses prototypes (Airbus, banques) et s'active sur le projet de mesure de gestion des clés de chiffrement. Ils ont été contactés en septembre par l'industriel américain ICT et par une société spécialisée dans les levers de fonds.

3. Is traditional AV Dead? Real-time Machine-learning Detection of Modern Malware Downloads

Marco Balduzzi (Trend Micro)

Marco Balduzzi décrit comment peut-on utiliser le *machine learning* pour détecter des chargements de malwares. Il a eu son PHD à Télécom ParisTech et possède son site Madlab (www.madlab.it).



Il commence sa présentation par une comparaison des détections par signatures plutôt que statistiques. Il juge la détection par signatures inefficace à cause du polymorphisme, de l'obfuscation (assombrissement), du packing. L'analyse prend du temps tellement il y a de données à regarder. Les URL backlists sont très vite obsolètes. Il vaut mieux une conscience globale que locale. Il faut regarder les relations entre les fichiers et les machines.

Il détaille son approche X-Gen : l'analyse du contenu n'est pas nécessaire. Il faut regarder les relations entre des formes et trouver « Who-What-Where ». C'est basé sur une approche statistique globale par une combinaison d'approche conjointe au niveau du système et du réseau. Ce qui est bénéfique pour détecter des chargements malicieux, efficace pour détecter en temps réel des menaces inconnues. Marco Balduzzi explique son système : des serveurs chargent des fichiers exécutables qui font des demandes de classification. Marco Balduzzi construit alors des graphes qui représentent l'ensemble des chargements et donnent une situation globale (URL, fichiers, machines). On peut déterminer ce qui est normal ou ce qui est malicieux. En analysant sur les 10 jours précédents les relations dans le système, il arrive à déterminer quel fichier issu de quel

url est suspect. Il conclut en présentant des cas d'études comme Somoto Adware ou TTAWinCDM Spyware.

4. Analyse dynamique de malware Android

Valérie Viet Triem Tong (Centrale Supelec)

Valérie Viet triem Tong, est enseignant chercheur à Centrale Supelec à Rennes et chercheur à l'Inria de Rennes.

Sur les tablettes qui tournent sur Android on peut télécharger des applications. Il y a donc beaucoup de téléchargements (entre 50 et 100 millions pour une application). Il y a eu 1 400 000 applications proposées sur Googleplay en 2014. Certaines sont malveillantes : elles s'évertuent à envoyer des messages vers des numéros surtaxés, prendre le contrôle d'un téléphone, espionner un utilisateur ou le rançonner en chiffrant ses données. Un malware Android provenant des téléchargements est un ensemble de codes malveillants cachés dans un code existant correct. C'est souvent très peu de lignes de codes. Pour s'en débarrasser, il y a deux approches : statique ou dynamique (observation du code pendant son exécution). Un auteur de malwares obfusque le code ou l'occulte. L'analyse statique a des difficultés pour détecter ce malware surtout si elle n'a pas de code à analyser. Pour échapper à l'analyse dynamique, il suffit que le code ne soit pas exécuté. Les auteurs de malwares attendent donc un événement, un temps donné ou par exemple, que le code est exécuté si on est sur une plate-forme spécifique. L'analyse dynamique marche si on force l'exécution d'un code, qu'on capture le comportement du malware. Pour déclencher le code suspect écrit dans une application écrite en java, il faut voir la forme du malware. Et savoir s'il envoie un SMS ou un appel. Avec l'application écrite en Java, on va calculer un score de risque. L'équipe de Valérie Viet Triem Tong a construit un outil (GroddDroid) qui singe un utilisateur et peut forcer l'utilisation du code malveillant en bypassant toutes les actions conditionnelles inclues dans le code.

Comment capturer ce que fait le malware ? Il faut entrer dans le système d'exploitation. Par exemple, un fichier sensible et marqué de façon claire sera copié et écrit dans un autre fichier. Les appels au système vont modifier le flux d'informations du noyau. C'est fait par l'outil (Andro)Blare, qui génère de quantités de logs. Pour savoir quelles IP externes le malware a utilisé, quels fichiers ont été modifiés, qui l'a écrit, la connaissance des logs est très utile. C'est fait suivant un graphe, ce qui est plus lisible que 10 000 ou 100 000 lignes de logs. On y voit l'application qui crée des fichiers et demande des services à l'aide du processus système-serveurs qui regarde si l'application a le droit de la faire. Cela crée deux sous-ensembles de graphes qu'on peut isoler. Le reste inexpliqué du graphe représente le malware. Ce n'est donc pas très compliqué. Sur beaucoup de malwares à la fois, il faut savoir que sous Android les applications se ressemblent au niveau comportemental. Cela réduit le travail de l'analyste.

Valérie Viet Triem Tong termine en disant que ce qu'elle a présenté fait partie du projet CominLabs Kharon (2015-2018) dont la plate-forme est située au LSH de Rennes.

5. Cas avérés d'attaques, conséquences sur les intérêts économiques, commerciaux et stratégiques d'une entreprise ou d'un pays

Hervé Hosy (Oppida)

Hervé Hosy est directeur d'Oppida, un cabinet de conseil et expertise en sécurité des systèmes d'information.

Il commence son propos par une revue des attaques passées. En septembre 2011, Areva a subi une attaque de grande ampleur. Les pirates, probablement asiatiques, se sont introduits pendant 2 ans dans le système informatique. Ils sont passés par des stagiaires qui ont pris connaissance du système et ont eu le temps de se l'approprier. En février 2016, le réseau interbancaire Swift a été hacké. Les hackers voulaient transférer 800 millions de dollars. Mais ils ont été bloqués grâce à une erreur d'orthographe sur le mot anglais foundation. Cependant 4 virements (81 millions de dollars) ont été honorés. Les enquêteurs ont retrouvé les dernières traces (après une dizaine de banques) dans des casinos philippins.

En avril 2016, TV5 Monde a subi une attaque par phishing (email signé par un confrère). Résultat : arrêt de la diffusion des programmes, publication de messages de propagandes de l'état islamique sur le site internet et les réseaux sociaux. Le phishing est une menace facile à mettre en œuvre et sans grand risque pour l'expéditeur.
La semaine dernière (26 novembre 2016), les transports de San Francisco ont eu un ransomware qui a provoqué une panne des distributeurs de billets, le vol des données personnelles des usagers, et une rançon a été demandée (100 bitcoins). Le pirate a été… piraté. Il avait une dizaine d'attaques à son actif, en ciblant des utilisateurs d'Oracle. Il

n'a pas encore été pris. Enfin, hier, 30 novembre, la Deutsche Telekom a subi une panne de son réseau internet.

Hervé Hosy parle alors des conséquences de ces attaques : une image de marque écornée, des pertes financières, une interruption de service, une responsabilité juridique en cas de vol des données personnelles. Les cibles des cyber-attaques sont larges : réseaux et utilisateurs, locaux informatiques, les PC nomades, les smartphones et les tablettes.

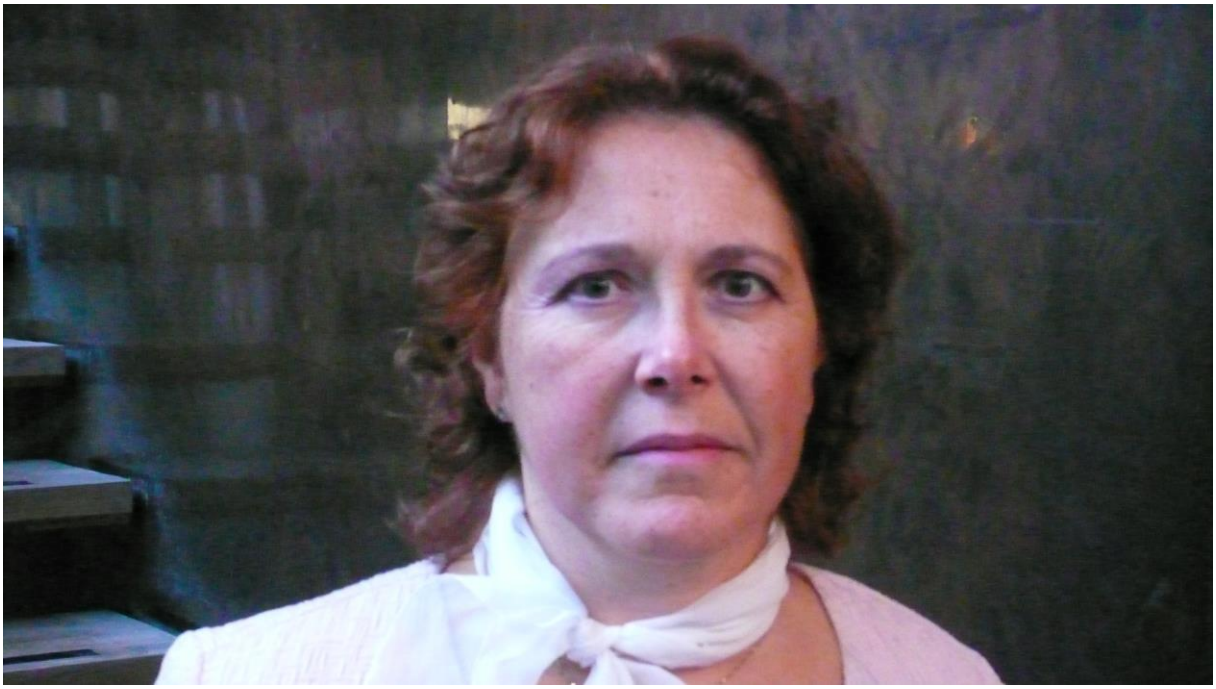
Les cyber-attaques se font par intrusion de réseau en exploitant une vulnérabilité, un phishing permettant d'ouvrir une porte d'entrée, un virus ou un ransomware envoyé par email ou par une clé USB piégée. Il peut s'agir aussi d'un piégeage physique en accédant physiquement à l'entreprise. Elles sont souvent ignorées, car trop style « James Bond », mais elles existent. Ce sont des intrusions ou des attaques « Evil maid ». Dans les data centers, les serrures peuvent être volées, photographiées ou moulées. Les gâches électriques contrôlées par badge sont aussi sensibles (cache-penne inefficace, radiographie). Il est aussi possible de contourner les dispositifs de contrôles (ventouses magnétiques avec contre-aimant, issues de secours, accès aux clés, pression sur le personnel). On peut aussi activer des interfaces externes sur des PC ou des serveurs par l'ajout d'une clé USB ou en utilisant un smartphone comme partage de connexion internet. On peut aussi ajouter des relais convertisseurs Ethernet vers WIFI ou 3G/4G dans des baies informatiques.

L'accès à l'ordinateur ciblé peut être évité si le PC est éteint. Mais on peut démarrer le PC sur un support amovible, introduire un outil physique dans le disque dur. On peut alors casser le mot de passe et le modifier. Avec la sécurité LM, on réussit en moins d'une journée. Avec la sécurité NTLM, c'est beaucoup plus long. Si la session est verrouillée, on arrête l'ordinateur et on récupère les clés de chiffrement en mémoire RAM. Avec un périphérique matériel, on peut commander l'accès direct à la mémoire (DMA) via le contrôleur PCI dédié. Ou écrire un patch mémoire pour contourner l'authentification. Donc la menace est bien réelle. Il y a des solutions pour les éviter. Hervé Hosy termine par une alerte : le piratage touche toutes les entreprises, les grandes comme les PME. Le maillon faible, c'est l'homme.

6. Focus sur le “ransomware”, monétisation du crime. Finalités, fonctionnement et risques. Moyens pour s'en prémunir

Martine Giralt (Thales/Cert IST)

Martine Giralt, de Thalès, est responsable du CERT-IST, créé en France en 1999. Ils offrent aux entreprises un suivi des menaces et des rapports sur les incidents.



Un ransonware (ou ransongiciel) est un logiciel qui bloque des systèmes et demande une rançon souvent en cryptomonnaies (bitcoins). Il peut aussi être utilisé pour détruire un système, le saboter. Il y en a plusieurs types : les *encryptions ransonware* qui chiffrent les données comme Locky ou Crypto-locker ; les *lock screen ransonware* qui bloquent l’utilisation comme Reveton ; des *master boot record* comme Petya ou Satane qui modifient le processus de boot ; les *ransonware encrypting web server* ciblent les serveurs web comme Rex ; les *mobile device ransonware* comme Small ou Fusob visent les mobiles. Les techniques utilisées visent les mails avec des fichiers piégés, des pages web avec des kits d’exploitation, des campagnes de publicité malveillantes. Au début, les particuliers étaient visés. Aujourd’hui ce sont les entreprises, les services publics comme les hôpitaux, les administrations. Cela rapporte bien plus. Les campagnes de ransomwares ciblent davantage certains pays que d’autres. L’ancêtre est apparu en 1989 : disquette AIDS. La disquette envoyée contenait un programme sur les dangers du Sida mais aussi un logiciel malveillant demandant une rançon qui devait être envoyée au Panama. Aujourd’hui certains changent leur signature toutes les 15 secondes pour éviter les outils de détection. Ils sont fabriqués par des gens de moins en moins qualifiés qui les créent avec des logiciels dédiés. Les ransomwares peuvent aussi être loués. En 2016, on en a détecté 4 fois plus qu’en 2015. Pour une prévision de plus de 1 milliard de dollars (50 millions en 2015). Les impacts sont évidemment financiers, un arrêt de l’activité,

une atteinte à l'e-réputation et des impacts juridiques si les données personnelles ou celles d'une entreprise ont été perdues.

Pour s'en protéger, Martine Giralt vante des mesures d'hygiène informatique classique : politique de sécurité ; sensibilisation des utilisateurs tout en sachant qu'il y aura toujours un utilisateur qui ouvrira une pièce jointe ; faire des sauvegardes et les tester ; patcher, patcher et encore patcher. Il faut aussi s'informer sur l'évolution des menaces, mettre à jour les outils de sécurité, mettre en place un système de supervision avec des IOC qualifiés et bloquer certaines pièces jointes.

Comment réagir si on est victime d'un ransomware ? Il faut immédiatement déconnecter le poste du réseau, ne pas payer la rançon (qui ne garantit rien), utiliser l'initiative « No more Ransom » (a été lancée en juillet 2016 par la police des Pays-Bas et Europol) ou « ID ransomware » qui aident les entreprises à se prémunir et donnent des clés pour déterminer le ransomware. Il faut aussi garder les données chiffrées et ne pas oublier de porter plainte.

Deux prévisions des menaces sont contradictoires. Mc Afee labs prévoit qu'au 2ème semestre 2017 il y en aura moins. Alors que Keasperky prévoit l'émergence de « ransomwares sales et menteurs » et une non-diminution des attaques. Celles-ci vont changer : attaques DDOS utilisant les objets connectés, attaques vers les smartphones, vols de données, destruction de données et désinformations comme Vinci en novembre 2016.

7. Comment enclencher réellement la mise en mouvement des organisations au niveau Sécurité Opérationnelle ?

Gérard Gaudin (G2C)

Gérard Gaudin est consultant international indépendant. Il préside le club R2GS France et Europe

En 25 ans, que s'est-il passé en sécurité ? La technologie a évolué, mais la menace a avancé plus vite. Au niveau des entreprises, le chemin vers la sécurité est encore long. C'est le mythe de Sisyphe. Il faut toujours avancer pour survivre. Malgré la mobilisation globale, il y a du travail. 70% des incidents exploitent des défaillances de bases. Ils peuvent être évités. Or, certaines entreprises remettent en cause les firewalls. La protection de sécurité faiblit. Quand il faut répondre aux agressions, il y a de grands manques surtout au niveau communication. Gérard Gaudin présente deux axes majeurs pour débloquer la mise en mouvement des organisations en GOS. Le premier est quantitatif : il faut des indicateurs et des chiffres. Le deuxième est un meilleur dialogue entre le SSI et le Comex. Les deux axes peuvent être déverrouillants. Il faut parler au Comex des risques. Il faut aussi créer un lien avec le management. Les points de repère de référentiel généraux sont appréciés des commissaires aux comptes. Les entreprises peuvent se *benchmarker* avec le référentiel qui sont des chiffres moyens. Elles ont beaucoup d'outils mais les utilisent très mal. Il faut aussi les mobiliser pour concerner l'ensemble du Comex et du management et même « l'ensemble de l'entreprise » comme disait John Chambers, l'ancien patron de Cisco. Le phishing est dangereux pour tous. L'approche quantitative fait avancer la résolution de ces problèmes. Or 70% des défaillances impliquent l'humain. SI tout le monde est impliqué, le taux diminue. Il faut davantage systématiser les tests, car 6 mois sont encore nécessaires entre la détection et

la résolution d'une défaillance. L'idée est d'automatiser les processus afin de rendre la réponse plus efficace. Il y a 10 types d'outils de détection. Il faut comprendre leurs efficacités respectives et conjointes. Des travaux de standardisation sont en cours pour 98 indicateurs. Le réseau de club R2GS a lancé Information security indicators (ISI), un ensemble de standards accessibles gratuitement en ligne. L'incident subi par une entreprise peut être ainsi comparé aux statistiques. Cela permet de partager l'expérience et facilite la notification aux autorités.

Le standard a commencé à être créé en 2009 en France, puis en Europe en 2012. Il faut accélérer son adoption par tous.

8. Cyberdéfense et détection : plateforme et exercice

Philippe Delaunay (DCI)

Philippe Delaunay, responsable de l'offre cyberdéfense chez DCI, aborde les moyens de détection utilisés pas la Défense.

Il faut évaluer la gouvernance et l'opérationnel. En défense, la sécurité concerne le renseignement, la planification, les opérations. La fonction J3 est la conduite des opérations. La planification la plus importante est celle qui est dite chaude. Il faut proposer des solutions à la chaine de commandement dans un temps très court. La formation comprend un scénario, une architecture, des documents, une animation (peut-être avec des gens externes comme un DSI…). Des pen testers peuvent intervenir. Philippe Delaunay revient sur des exercices réalisés. En crise Cyber dans une chaine de commandement, la cellule de crise intervient directement avec les acteurs locaux. Avec un élément Slunk, les participants devaient retrouver l'origine d'un malware et évaluer les impacts sur une mission. La question était : que fait le participant vis-à-vis de la chaine de commandement ? Le tout se faisait sur une journée.

Un autre exercice s'est fait avec d'autres pays européens. Deux jours de détections d'attaques. Que sont-elles et d'où viennent-elles ? La difficulté était encore une fois la planification. Troisième type d'exercice, un bâtiment de la marine avec un malware qui agit sur un automate. Sur l'écran de visualisation, l'utilisateur ne sait plus si la température indiquée est la bonne, ce qui risque de rompre le matériel. Pour l'aider, il a des sondes avec les nœuds qui interagissent. Cet exercice servait à se poser la question des mesures d'urgence à prendre.

9. Processus de mise en conformité LPM chez un Opérateur d'Importance Vitale (OIV)

Guillaume Kaddouch (Grand Port Maritime de Rouen)

Guillaume Kaddouch travaille au Grand Port maritime de Rouen. La Loi de Programmation Militaire (LPM) s'applique désormais sur les Opérateurs d'Importance Vitale (OIV), dont le Port fait partie.

Il présente comment le port a appliqué cette mise en conformité. Le premier axe est l'organisation de la sécurité. La Loi n'est pas une simple liste. Il faut une gouvernance de sécurité. Or le port n'avait pas de RSSI. Le seul était un responsable de sécurité incendie, qui lui aussi installe des pare-feux. C'est autour de la chaine de commandement que s'est construit l'organisation de la sécurité. Le service informatique du Port est petit (7 personnes dont 4 développeurs). Il fallait donc tout faire à trois. Or la LPM demande d'ajouter des règles obligatoires et des mesures récurrentes, ce qui demande du temps de travail supplémentaire. La priorité donnée à la sécurité par la LPM implique aussi moins de temps pour les autres taches. Il a donc fallu embaucher. Comme il faut avoir les bons outils, il faut aussi une augmentation de budget.

Guillaume Kaddouch l'a estimé entre 200 et 300 000 euros sur les premières années, juste pour le démarrage de la nouvelle activité de sécurité, mais d'autres OIV ont investi plus d'un million d'euros. Il n'est pas question de s'y soustraire car si on a des manquements sur une des 20 règles, il y a des amendes dissuasives. Ce n'est donc pas une solution. Le Grand Port maritime de Rouen a du aussi demander plusieurs audits de vulnérabilité et de compromission à des prestataires qualifiés. Cela a permis de découvrir plusieurs failles, surtout organisationnelles, et de passer des certifications de sécurité offensive. C'est une méthode de pensée plutôt que des connaissances. L'examen est pratique et non théorique. À titre individuel, cela éclaire sur les portes d'entrée du

système et, pour le Port, de trouver des failles de sécurité non répertoriées qui ont depuis été corrigées par les éditeurs.

Cette année, les consciences changent entre autre par les campagnes répétées de ransomware qui ont alerté tous les OIV.

10. L'approche « Security by design » : Conception d'architectures sécurisées

Gwenn Feunteun (ACCEIS)

Gwenn Feunteun, de la société Acceis, décrit l'approche « security by design ».

L'architecture est l'art de concevoir par des techniques, des matériaux, des volumes. Cet art est destiné à protéger l'homme contre des contraintes extérieures. Une architecture sécurisée est donc un pléonasme. Dans l'architecture de sécurité des systèmes d'information, c'est la même chose. On fortifie d'abord la ceinture extérieure (pare-feux), mais la grande majorité des failles se situe au niveau applicatif. Il faut donc une défense en profondeur. Comme Vauban l'a fait pour les forts français, il faut appliquer ces méthodes au SI : on empile les couches de sécurité afin que la tentative d'intrusion soit trop couteuse. La défense passive met en place des mesures intrinsèques (séparation fonctionnelle, chiffrement des communications, segmentation en sous-réseaux, cloisonnement par réseaux virtuels (VLAN)). Ce sont comme des issues de secours d'un bâtiment. La défense active utilise quant à elle des composants de sécurité dédiés (filtrage applicatif, pare-feux, ACL, contrôle d'accès). Il y a de plus une approche temporelle. Il faut prévenir (filtrage), protéger puis y remédier (sauvegarde).
Bref une architecture de sécurité demande une séparation, un cloisonnement, un filtrage. Les seules limitations sont l'imagination et le budget.

Gwenn Feunteun donne un exemple autour d'un service web, actionné depuis internet, avec un pare-feu. Si le serveur est compromis, tout tombe. Pour être plus robuste, il faut séparer le frontal web qui dialogue avec les clients, le serveur applicatif et la base de données. Mais les trois sont dans la même DMZ. C'est dangereux. On peut aller plus loin. Des liens logiques du pare-feu permettent à un possible hacker de ne suivre que ces liens sans voir les autres protocoles. Mais si le pare-feu est compromis, il vaut mieux en

utiliser deux avec des technologies différentes, sans qu'ils se voient. Le flux est alors rompu naturellement.

Ce sont des exemples de défense passive. Pour la défense active, il faut un filtrage des flux applicatifs. Mais rien n'empêche une intrusion par le poste d'administration. Il suffit alors de lui mettre un pare-feu spécifique. Ce qui permet de séparer les flux de production et d'administration. En plaçant des sondes à différents endroits de cette architecture robuste et complexe, on peut déterminer rapidement où sont les intrusions. Mais cela coûte cher. En souriant, Gwenn Feunteun espère que c'est cette architecture qu'utilise sa banque.

11. La détection et la réponse aux incidents de sécurité

Nicolas Prigent (LSTI)

Nicolas Prigent, travaille à LSTI, une société qui qualifie les prestataires de confiance.

La défense en profondeur c'est bien, mais il faut aussi surveiller le système. Sur les documents de l'ANSSI on voit qu'il y a plein de bonnes pratiques. Or aucun plan ne se déroule sans accroc. Le SI est amené à évoluer. Or un changement, tel l'installation d'un serveur web en plus, fait évoluer la sécurité. De nouvelles vulnérabilités apparaissent tous les jours. Le groupe Shadow brokers aurait récupérer des données de la NSA et les a mis sur le net. Cette vulnérabilité était connue. Cela peut arriver à tout le monde. Nicolas Prigent reconnaît que la technique de Vauban dont parlait Gwenn Feunteun est bien mais surtout parce qu'on voit l'ennemi avancer quand une barrière est franchie. Sans surveillance active, la défense en profondeur ne marche pas.

Pour lui, la sécurité est un processus. Il faut une analyse de risque donnant une politique de sécurité qui sera appliquée opérationnellement. L'appel à des prestataires extérieurs pour des audits de sécurité est un plus, mais pas suffisant. Il faut détecter les défaillances de sécurité quand ce sont de vrais hackers qui tentent d'entrer. Les guides de l'ANSSI permettent de déployer les mesures de sécurité. Les audits font appel à des PASSI. La détection d'incidents est faite avec des PDIS. Et la réponse à des incidents doit suivre le référentiel PRIS de l'ANSSI.

Nicolas Prigent revient sur la détection des incidents de sécurité. Il reconnaît que tout le monde a acheté son IDS. Mais il y a plein de faux positifs. Il faut des moyens humains et de l'organisation. Il faut gérer les événements de sécurité, identifier ceux qui sont pertinents et peuvent révéler une attaque. De même, il faut identifier les événements à

collecter en fonction des menaces. Donc bien choisir les sources de collectes (IDS réseau, IDS hôte, IDS applicatif, journaux divers) et les points de collectes. Tout est expliqué dans le référentiel de l'ANSSI. L'analyse de ces événements en temps réel permet de repérer les attaques en cours. C'est un problème de big data.

Passer de l'événement à l'incident. Les règles de détection permettent de générer des alertes. Elles prennent en compte les événements redoutés de l'analyse du risque, le contexte, les informations collectées. Cette gestion des règles de détection est une partie particulièrement sensible de l'activité de sécurité.

En cas d'incident, il faut réagir vite. Les interlocuteurs doivent avoir été identifiés selon leurs besoins. Les canaux de communications ont été déjà mis en place. Ils doivent être sécurisés et séparés du SI compromis. Comment réagir ? C'est indiqué dans le référentiel PRIS. On définit le cadre du système d'information qui doit être à jour. L'analyste est un détective qui va chercher le mode opératoire et les objectifs de l'attaquant. Mais aussi qualifier l'étendue de la compromission et évaluer les risques et impacts associés. Puis préconiser les mesures de remédiation.

Le processus se passe en 6 étapes itératives (compréhension, collecte, analyse, synthèse et capitalisation des IdC, révision des mesures de remédiation, mise à jour de la compréhension). L'itération s'arrête quand il n'y a plus de mise à jour envisagée.

12. La Threat Intelligence piquée au sérum de vérité

Jérôme Robert (Orange Cyberdefense)

Jérome Robert fait partie des mille personnes qui travaillent sur la cybersécurité chez Orange. C'est un fournisseur de service de sécurité informatique.

Le cybercrime est aujourd'hui un vrai business avec des acteurs spécialisés et des échanges sur des marchés undergrounds et une forte innovation. Les meilleures techniques sont largement réutilisées.

Pour Jérome Robert, ce sont de bonnes nouvelles. Comme l'organisation est bonne, les hackers sont identifiables et identifiés. Ils ont des habitudes, s'échangent des données. On peut infiltrer cet écosystème. Le renseignement intervient pour l'aide à la décision. Cela réduit les temps de détection et de réponses aux incidents de sécurité. Mais ne pas confondre information (brute, non filtrée, non évaluée) et le renseignement (contextualisé, pertinent, vérifié). Pour passer de l'information à l'intelligence (le renseignement), on recueille des données de partout même sur des sites cybercriminels en toutes langues. L'ensemble passe dans une infrastructure big data, puis une analyse humaine est lancée pour qualifier les informations (souvent par contact avec le cybercriminel qui cherche à vendre ses produits).

Il y a 3 types de renseignements. Le premier est opérationnel. Ce sont des données techniques à effet immédiat. C'est réactif. On obtient le résultat d'observations passées. Un autre est le renseignement tactique. Après avoir observé le comportement d'un groupe cybercriminel, vous êtes capables de prévoir sur 6 mois le type d'attaque qu'il va conduire. Vous pouvez dire quelle est la méthode utilisée et dans quel secteur elle est appliquée. C'est quand même assez rare, même chez les spécialistes de la CTI. Et doit

être interprété par l'utilisateur final pour action. Enfin il y a aussi des renseignements stratégiques qu'Orange ne fait pas. Cela permet des prévisions d'impacts business à 2 ans.

13. Recherche et Innovation en cyber sécurité

Florent Kirchner (CEA)

Au CEA, Florent Kirchner fait de la recherche en cybersécutité. Il détaille certains résultats parus durant les six derniers mois.

Côté utilisateur, un utilisateur peut installer un plug-in qui réagit quand le site qu'il visite peut être compromis. Ce travail a reçu le Prix de l'innovation par la Commission européenne. Au niveau du réseau, un travail a cherché une méthode de détection d'intrusion et fait que le réseau se reconfigure. Au niveau du code et de son évaluation, il s'agit de faire des audits exhaustifs. Sans avoir accès au code source, certains regardent comment les malwares sont construits. Avec la DGA, les nouveaux outils développés par le CEA ne peuvent pas être trompés par les hackers. Pour les données, le chiffrement avance. Le serveur peut maintenant faire des calculs sur des données chiffrées. Dernier point, la séparation devient « construite par essence ».

Florent Kirchner continue en décrivant le partenariat public-privé en cybersécurité avec la commission européenne, des institutions, des Etats, des industriels. Cela permet un agenda entre 2018 et 2020 qui coûte un peu moins de 300 millions d'euros. Il comporte quatre axes. Le premier est sur l'écosystème, le second est formé des démonstrateurs sur des secteurs types comme l'énergie ou les transports. Troisième axe, des travaux d'innovations plus fondamentaux qui peuvent être appliqués à tous les secteurs : gestion du risque, prévention et protection, détection et réponse. Enfin, le dernier axe vise les composants de base comme le traitement de données de sécurité et de vie privée.

Patrick Legand conclut la journée en remerciant tous les intervenants et Régine Lombard, de l'association Aristote, sans qui rien ne se fait.

Il note une professionnalisation dans la défense grâce à la Loi de Programmation Militaire et une complexité croissante des menaces en cybercriminalité. La difficulté de gestion de ces nouvelles menaces force à définir des stratégies intelligentes sur les cybercriminels ou la protection des réseaux. Les systèmes futurs seront-ils sécurisés ? On n'en sait rien, mais la prise de conscience est aujourd'hui réelle.

Il a une pensée pour Roland Sénéor qui a disparu en avril dernier.