Cnam Ile-de-France – Formation Ouverte à Distance
Année 2022/2023 – 1er semestre

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Examen SEC101 – FOAD IDF

Session 1
Le jeudi 19 janvier 2023

Durée 3 heures
Document (s) autorisé(s) : tout document papier
Calculatrice : **Interdit**
Téléphone portable : Interdit
Le sujet comporte X pages (dont celle-ci).
Barème d'évaluation : voir ci-dessous

L'étude de cas comporte **4** questions pour **8 pts**

Les **3** questions à développement court représentent **5 pts**

1pt : pour la présentation et l'orthographe **si et seulement si** toutes les questions sont traitées.

Au total 14pts, auxquels il faut rajouter :

1 pt pour participation durant le semestre
5 pts pour la restitution réalisée en fin de cursus en groupe.

Votre note sur 20.

Sans participation et sans devoir rendu, il reste possible de réussir.

Courage

"N'acceptez jamais la défaite, vous êtes peut-être à un pas de la réussite."
Jack E. Addington

Enseignant : Pierre LENOIR

ÉTUDE DE CAS :

Le piratage de TV5 Monde vu de l'intérieur

Extrait du site lemonde.fr 08/12/2022
Par Martin Untersinger (Rennes, envoyé spécial)

(…)Pour la première fois, les agents envoyés à la rescousse de la chaîne de télévision en 2015 racontent comment ils ont paré cette cyberattaque inédite.

Mercredi 8 avril 2015, vers 3 heures du matin. Dans la « tour Mercure », les locaux parisiens ultra-sécurisés de l'Agence nationale de sécurité des systèmes d'information (ANSSI), un téléphone sonne. Au bout du fil, TV5 Monde. Les techniciens de la chaîne de télévision francophone se battent depuis une poignée d'heures contre une attaque informatique sans précédent : son site Internet et ses comptes sur les réseaux sociaux diffusent de la propagande djihadiste, son système de production d'images est inutilisable et sa diffusion est interrompue. La chaîne, qui émet dans 200 pays pour 50 millions de téléspectateurs, affiche un écran noir.

À l'aube, une réunion est organisée. Autour de la table, les équipes de TV5 Monde, l'unité de la police nationale spécialisée en cybercriminalité, les services de renseignement intérieur et l'ANSSI. Cette agence, chargée de la défense des systèmes informatiques critiques de l'Etat et des entreprises les plus sensibles, n'est théoriquement pas concernée par une attaque contre une chaîne de télévision. Mais l'épisode est inédit, déjà public et touche une des « voix de la France » dans le monde : décision est prise de dépêcher les « pompiers informatiques » de l'ANSSI en urgence dans les locaux de la chaîne.

Une transparence inédite

Ces interventions sont communes pour ces agents, qui mènent des opérations similaires une vingtaine de fois par an. En temps normal, ces manœuvres – dans des entreprises critiques ou des systèmes fondamentaux de l'Etat – se font dans le plus grand secret. TV5 Monde est un cas particulier : les dégâts sont immédiats et très visibles. C'est la première fois que le travail des agents de l'ANSSI prend autant la lumière. Deux ans après cet incident, ils ont présenté dans le détail cette intervention, lors du symposium sur la sécurité des systèmes d'information (SSTIC), à Rennes, vendredi 9 juin. C'est la première fois que l'ANSSI se prête en public à un tel exercice.
(…)
Pendant les quarante-huit premières heures, les agents – entre 9 et 15, qui seront mobilisés pendant plusieurs semaines – recherchent les indices les plus évidents laissés par les attaquants. À l'instar des démineurs quadrillant les rues après le départ d'une armée ennemie, ils craignent également la présence de « bombes logiques », des lignes de code laissées par les attaquants, conçues pour s'activer au redémarrage des systèmes infectés et destinées à paralyser un peu plus le réseau. Cette crainte ne se matérialisera finalement pas.

Dès les premières heures de l'enquête, l'attention des agents est attirée par un compte dont l'intitulé est en anglais sur le réseau informatique de TV5 Monde, qui est configuré en français,

et disposant de très larges pouvoirs. Problème : il n'appartient pas aux équipes techniques de TV5 Monde, mais aux pirates. Les enquêteurs parviennent à reconstituer ses dernières actions et se rendent compte qu'il s'est connecté à un serveur inconnu sur Internet, hors du réseau de TV5 Monde. Ils mettent la main sur l'adresse IP, l'identifiant de ce serveur sur Internet. Une première pièce d'un immense puzzle pour tenter de comprendre qui est derrière cette attaque.

Au fil de leurs investigations, les agents de l'ANSSI recueillent de grandes quantités de données à analyser, et notamment le déroulé de toutes les actions réalisées par les pirates sur le réseau. Il leur faudra plusieurs semaines pour comprendre en détail comment les attaquants ont pu pénétrer dans les réseaux de TV5 Monde et quasiment tout détruire sur leur passage.

Le déroulé de l'attaque

L'offensive débute le 23 janvier. Les attaquants observent, de loin, l'infrastructure du réseau de TV5 Monde. Ils découvrent qu'il est possible de se connecter au réseau interne de la chaîne depuis l'extérieur, au moyen d'un réseau privé virtuel (VPN). Ce qu'ils font, au moyen de l'identifiant et d'un mot de passe appartenant à un sous-traitant de la chaîne. Comment se sont-ils procurés cette information ? C'est l'une des rares inconnues de l'enquête. Toujours est-il que les attaquants sont désormais à l'intérieur du réseau de TV5 Monde, qu'ils auscultent avec soin.

Ce repérage leur permet de localiser deux serveurs bien particuliers, qui pilotent les caméras sur les plateaux de télévision. Les pirates utilisent l'un de ces deux serveurs pour se connecter au système qui a la responsabilité de déterminer ce qu'est autorisé à faire ou non chaque ordinateur sur le réseau. Le Graal : une fois à l'intérieur, il leur est possible de s'octroyer les pleins pouvoirs.

Ensuite, les pirates fouinent. Ils se plongent dans la documentation interne des services informatiques de TV5 Monde et dans leur messagerie et partent à la recherche de toute information leur permettant de poursuivre leur infiltration. Les mots-clés qu'ils saisissent sont précis : ils veulent savoir comment est organisé et paramétré le réseau, et plus spécifiquement celui qui gère les flux vidéo diffusées par la chaîne. Dès le début, c'est le système de diffusion des images de la chaîne francophone qui les intéresse.

Cette moisson est fructueuse, et les pirates récupèrent de nombreuses informations, notamment des identifiants et des mots de passe de diverses machines. Pendant plusieurs semaines, les pirates se font très discrets. Aucune activité n'est enregistrée dans cet intervalle. Les agents de l'ANSSI suspectent que cette période a été passée à analyser, à comprendre, voire à traduire les éléments récoltés. Ce n'est que pour mieux revenir, d'abord pour vérifier que les éléments qu'ils ont récupérés sont valides. Les assaillants vérifient ainsi que les mots de passe pour accéder aux réseaux sociaux fonctionnent bien. Nous sommes alors le 6 avril, deux jours avant l'attaque proprement dite.

Le 8 avril, à 15 h 40, les pirates s'assurent une dernière fois de leur contrôle du réseau de TV5 Monde. Ils y déposent, bien en évidence, un logiciel espion standard. Étrangement, ce dernier n'a jamais été activé. Selon les agents de l'ANSSI, il est possible que ce « malware », largement accessible à n'importe qui en ligne, ait été laissé pour servir de leurre et égarer les enquêteurs.

Le début de l'offensive

À 19 h 57, l'assaillant commence son entreprise de démolition. Il modifie les paramètres des multiplexeurs – les ordinateurs qui gèrent et orientent les lourds flux vidéo de la chaîne – afin de rendre leur redémarrage impossible. Cette modification est invisible tant que ces derniers ne sont pas éteints, et la chaîne continue d'émettre. La première action visible intervient à 20 h 58, quand les comptes sur les réseaux sociaux prennent les couleurs d'un mystérieux « cybercalifat » et affichent leur soutien à l'organisation État islamique.

À 21 h 48, nouveau coup de boutoir. Les attaquants se connectent à plusieurs pièces critiques du réseau de TV5 Monde et détruisent le logiciel qui les fait fonctionner. Tous les flux vidéo de TV5 Monde s'interrompent, les écrans deviennent noirs.

Dans son malheur, TV5 Monde a de la chance : une nouvelle chaîne thématique vient d'être lancée, et de nombreux techniciens sont encore dans les locaux à cette heure tardive pour en fêter l'arrivée. Ils réagissent immédiatement. Leur tâche est compliquée par une nouvelle offensive des pirates, qui suppriment à 22 h 40 la messagerie interne de l'entreprise. À ce stade, les équipes de TV5 Monde ont complètement perdu le contrôle de leur réseau. Peu avant minuit, elles prennent la seule décision possible pour stopper l'attaque : elles l'isolent complètement du reste du monde.

Les pirates ont perdu la main, mais c'est dans un champ de ruines numérique qu'arrivent, au petit matin, les agents de l'ANSSI. Ils viennent aider des équipes techniques désemparées, mais compétentes et très coopératives. Jamais les experts de l'ANSSI, dont la discrétion est proverbiale, n'ont eu à affronter une telle pression médiatique. Les caméras de télévision campent devant l'entrée de la chaîne de télévision. Les journalistes de TV5 Monde, dont le lieu de travail fait la « une » de l'actualité, tentent de leur extorquer des informations, au détriment de l'extrême sensibilité de ces premières heures d'enquête. Les agents doivent calfeutrer les portes vitrées de leur salle de crise, mise en place pour l'occasion, afin de ne pas être vus, fuir les caméras dans les couloirs, et même se réfugier sous leur bureau pour cacher leurs écrans lorsqu'elles font irruption dans la salle. Les agents de l'ANSSI et les équipes de TV5 Monde à l'ouvrage pour récupérer le contrôle de leur réseau.

Leur tâche est également techniquement complexe. Pour comprendre le mode opératoire des attaquants, ils doivent se familiariser à très grande vitesse avec des matériels spécifiques au secteur de l'audiovisuel. Si les attaquants ont, pour ce faire, disposé de plusieurs semaines, les délais qui s'imposent aux agents de l'ANSSI se comptent en heures. L'objectif est fixé dès leur arrivée : il faut reprendre au plus tôt la diffusion et offrir aux salariés une solution temporaire mais sécurisée pour travailler. Et surtout, tout faire pour que les pirates ne remettent pas les pieds dans le réseau de la chaîne. La pression est énorme : chaque minute qui passe sans diffusion satellitaire coûte des milliers d'euros à la chaîne de télévision.

Dès le soir, à 20 heures, TV5 Monde émet de nouveau, mais seulement avec des contenus préenregistrés. En attendant, le ménage commence : les machines infectées sont jetées et remplacées par du matériel neuf. Les agents mettent en place une petite salle pour que les journalistes puissent reprendre leur travail : (…)

Au fil des jours, des postes de travail sont ajoutés et forment bientôt la nouvelle salle de rédaction pour les journalistes. Pendant des semaines, les salariés de la chaîne seront traumatisés par cet épisode : un vent de panique souffle sur l'entreprise lorsque l'ANSSI annule

les mots de passe trop vieux et donc vulnérables. Ils deviennent alors inutilisables et de nombreux journalistes ont alors cru que les pirates étaient de retour.

Une bascule à haut risque

Pendant un mois, les agents de l'ANSSI, les équipes de TV5 Monde et leurs sous-traitants travaillent à cartographier le réseau et à préparer la bascule vers un système sécurisé et débarrassé des traces de l'attaque. Cette dernière intervient le 11 mai, soit un mois après l'attaque. De 17 heures à 5 heures du matin, ils réalisent cette opération extrêmement délicate sans pouvoir débrancher le réseau, car TV5 Monde ne peut pas – à nouveau – cesser d'émettre. Les experts doivent même s'interrompre toutes les 4 heures leurs opérations techniques pour ne pas risquer de perturber la diffusion des journaux télévisés.

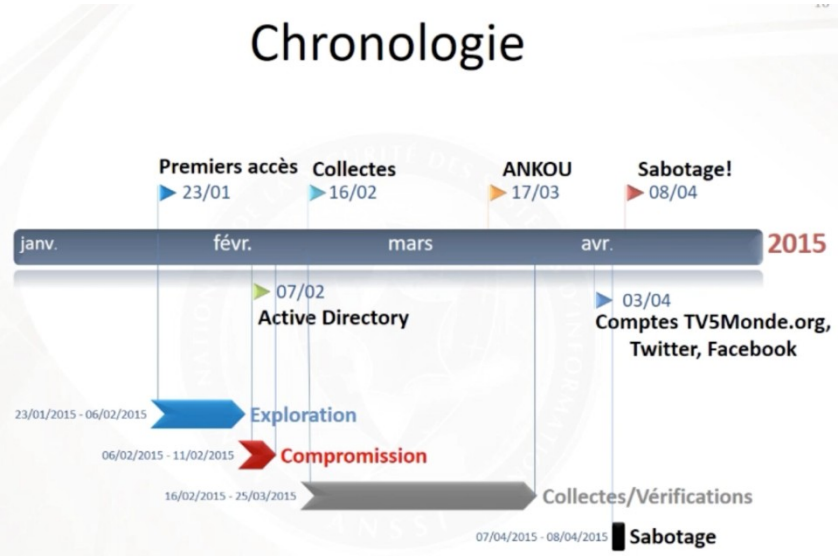
Les deux années écoulées depuis cet épisode mouvementé sont riches d'enseignement. Les pirates ont profité de manquements en termes de sécurité : TV5 Monde avait confié de larges parties de son réseau à des sous-traitants, diluant d'autant les connaissances sur ce réseau, et certaines bonnes pratiques de base n'étaient pas respectées. Mais ces défauts se retrouvent à l'identique dans la plupart des grandes entreprises françaises, soulignent les agents de l'ANSSI, bien placés pour le savoir.

L'attaque contre TV5 Monde a également nourri les inquiétudes de ces experts de l'Etat. *« Il y a une réelle prise de conscience de l'importance de l'informatique dans nos sociétés modernes »* explique l'un des agents de l'ANSSI sur scène au SSTIC :

« Il y a eu plusieurs coups de semonce, TV5 Monde en faisait partie. Aujourd'hui, aucun attaquant n'a réellement voulu faire des morts en France, mais gardez à l'esprit qu'un jour, ça pourra faire très mal. »

Au total, cette attaque aura coûté environ 20 millions d'euros sur cinq ans à la chaîne de télévision. Qui est derrière cette attaque ? Comme à son habitude, l'ANSSI ne s'est pas prononcée sur cette question éminemment politique, laissant à l'enquête judiciaire, ouverte par le parquet antiterroriste dès le soir de l'attaque, le soin de remonter vers d'éventuels responsables ou commanditaires.

Cette dernière, malgré les revendications postées sur le site et les réseaux sociaux de la chaîne, s'est orientée vers le groupe de pirates APT28, avait appris *Le Monde* de source judiciaire en juin 2015. Celui-ci est soupçonné d'être le bras armé du Kremlin sur Internet.



Questions sur l'étude de cas :

A la lecture de cette étude de cas, vous vous placerez en tant que **RSSI de TV5 MONDE** :

1. Si l'attaque avait lieu à une date postérieure au RGPD : quelles seraient les obligations légales à la suite de cette attaque informatique (1,5 pts)
   - Déclaration dans les 96h à la CNIL et l'ANSSI
   - Contacter les personnes dont l'entreprise possède des données personnelles, on peut imaginer
   - Démontrer une sécurité suffisante
   - Porter plainte

Les autres éléments du RGPD sur les responsabilités

2. Quelles sont les solutions techniques à mettre en place afin de **détecter** ce type d'attaque ? (2 pts)
   - Firewall nextgen
   - Zero trust avec ségrégation des flux d'administration et d'exploitation
   - Waf
   - Supervision de l'AD
   - EDR/NDR
   - Corrélateur de log et conservation des traces
   - Equipe de réponse à incident
   - SIEM/SOAR si SOC… (possibilité de prendre un prestataire)

3. Quelles sont les objectifs des attaquants de cette attaque ? comment communiqueriez-vous en interne, vers les médias, avec les forces de l'ordre ? (1,5pts)
   - En effet les éléments djihadiste cache une manouvre du groupe APT 28 proche du pouvoir russe : leur objectif est de couper le service de diffusion de la chaine afin de démontrer leur force de frappe en dehors de leur pays sur un media international. Il n'y a pas de but lucratif à leur action. Donc un but politique est recherché
   - Communication interne : rassurer, faire taire les rumeurs, expliquer aux collaborateurs que leur paroles, texte ou gestes seront interprétés par les médias (en même temps c'est un copain qui est tombé). Donc rappeler que la communication officielle est de la cellule de gestion de crise et que toute interview d'un collaborateur l'engage à titre personnel. Donc on déconseille voire interdire suivant le mode de management et le milieu. Enfin rappeler que la crise sera longue
   - Communication vers les médias : belle mise en abime n'est-ce pas ? comment un media parle aux autres médias. Comme les autres, factualité, secret de l'enquête, sans émotion avec une maitrise de mots pour éviter les interprétations
   - Communication avec les forces de l'ordre… l'ANSSI n'est pas une force de l'ordre mais participe à la sécurité nationale. C'est bien la préfecture de police de paris et le parquet de la PP qui sont compétent dans le domaine.

4. Comment organisiez-vous la réponse à incident ?(1,5 pts)
   - Couper les accès aux réseaux de l'entreprise
   - Utiliser des ordinateurs propres et séparer ceux de l'investigation de ceux de la communication.
   - Rappeler que la crise sera longue

- Rassembler les traces et preuves de l'attaque
- Circonscrire l'attaque
- Reconstruire le SI en ayant patché les vulnérabilités
- Tracer les actions menées
- Rédiger un retex de l'incident et mettre en place les propositions par un plan d'action

Se réferer à la norme ISO27032/35

Questions à court développement :

5. Pascal est **l'urbaniste** SI de votre organisation : comment peut-il vous aider pour initier votre démarche d'analyse de risque ? (1pt)
   en tant qu'urbaniste, Pascal devrait posséder l'architecture des SI de l'entreprise, la CMDB, la liste des biens essentiels et les processus de l'entreprise concourant à la création de valeur ainsi que la liste RACI des biens. Finalement tout ce qu'il faut pour initier une analyse de risque. Par la suite, Pascal sera mis au courant des résultats de l'analyse de risque afin qu'il suive la liste des services possédant une mesure de sécurité et les responsables des mesures le cas échéant.

6. **La mise en place** d'un système de management de la sécurité de l'information (SMSI) présente un travail important, quels sont ses étapes principales ? (2pts)

   - Étude d'opportunité (pas obligatoire vis-à-vis de la norme)
   - Choix du périmètre du **SMSI**. ...
   - Déclaration d'intention. ...
   - Démarche d'analyse de risques. ...
   - Objectifs de sécurité ...
   - Exploitation du **SMSI**. ...
   - Surveillance du **SMSI**. ...
   - Certification (**étape** optionnelle)

   Il n'était pas pertinent de réexpliquer le PDCA sans évoquer les taches décrites ici

7. Un centre opérationnel de la sécurité répond à de nombreux problèmes de la sécurité : décrivez **l'environnement de travail** et les outils qu'utilisent un analyste ? vous compléterez avec les sources de données auxquelles il a accès. (2pts)

L'analyste travaille au sein d'un SOC. Son environnement de travail peut etre sur site suivant le niveau de sensibilité des informations traitées ou à distance en cas de téléactivité. Idéalement, il travaille avec les résultats d'une REDTEAM ciblant les vulnérabilités des SI supervisés. Une PURPLETEAM fournissant le CTI. Lui-même fournit des informations aux autres équipes. A cet effet, plusieurs outils lui sont nécessaires afin de mener à bien ses investigations :

- Un SIEM pour interroger les sources de logs collectées (FW, EDR, SYSMON, surveillance AD, etc…)
- SOAR : pour automatiser la source de données, suivre les tickets crées des alertes et poursuivre les investigations en partageant les enquetes voire participer à du hunting.

- BdC : sous forme d'une GED, sa base de connaissance évolue aux contacts des expériences cumulées du SOC
- CMdB : Une base de données de gestion de configuration comporte tous les composants d'un système IT de manière à avoir une vue d'ensemble sur l'organisation de ces composants et d'en modifier leur configuration si nécessaire. L'analyste en a besoin afin d'enrichire son SOAR et en cas d'investigation