A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Bernard Barbier sur le Cyber, entre gouvernance et après 16 mois d'agression Russe....

Compte rendu rédigé par ANDSI

En bref…

Bernard BARBIER proposera un exposé dédié à la thématique de la cybersécurité. Après avoir abordé la situation ukrainienne et plus précisément la résistance à la cyber agression de la Fédération de Russie, il évoquera les questions du risque numérique et de la stratégie cybersécurité de l'entreprise.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Eléments d'introduction

Bernard BARBIER indique qu'il est physicien de formation et qu'il a travaillé au CEA, ce qui lui a permis de devenir l'un des experts français des supercalculateurs. Il précise avoir été sollicité par la DGSE en 1989 et être devenu Directeur technique. Il explique également avoir dirigé le LETI à Grenoble puis avoir occupé le poste de DSI du CEA. Enfin, il a de nouveau rejoint la DGSE en 2006, ce qui lui a permis de présenter de grands projets techniques au Président Sarkozy. Dans ce cadre, il a embauché des centaines d'ingénieurs et d'analystes. Il précise également avoir participé à la création de la cyber armée française en 2008. Enfin, il indique avoir occupé la fonction de CISO mondial de Capgemini et CTO de l'équipe business.

La situation ukrainienne

Le 27 juin 2017, *NotPetya* a représenté une réelle surprise stratégique, peu de temps après *WannaCry*. Ce *malware* a été installé par les Russes dans un logiciel qui avait vocation à gérer les taxes que devaient payer les entreprises qui travaillaient en Ukraine. L'idée pour les Russes était de bloquer les capacités informatiques de l'Ukraine, mais le virus s'est propagé. En France, Saint-Gobain a été touché ainsi que Maersk ou TNT Express. A l'origine, ce virus correspondait à une arme numérique de la NSA qui a été dérobée. Les services secrets russes ont récupéré la souche du *malware*.

Une autre étape renvoie au sabotage, toujours par les Russes, du Ka-Sat/Viasat. Le terminal terrestre a été bloqué à la suite de l'envoi d'un *malware* qui a détruit le *firmware*. La difficulté se rapportait au fait qu'il était nécessaire de se rendre sur chaque terminal afin de recharge le *firmware*. Les Ukrainiens utilisaient ce satellite pour piloter leurs drones. Les Américains ont réagi rapidement tandis que des centaines de terminaux Starlink ont été données aux Ukrainiens. Il est apparu que les services secrets russes étaient à la manœuvre. Grâce aux réseaux sociaux, il s'est avéré possible d'identifier les cadres qui menaient ces cyberattaques.

De son côté, le FBI disposait d'une grande équipe dédiée à la cybersécurité, mais celle-ci a été dissoute par le Président Trump. Dès 2020, les Américains ont lancé un grand programme de modernisation de la cybersécurité ukrainienne. Notamment, le Département de l'énergie a renforcé les systèmes de distribution électrique. En effet en 2015, un tiers du système électrique ukrainien avait été détruit à la suite d'une cyberattaque.

A compter de janvier 2023, Microsoft a apporté son aide à l'Ukraine. Amazon a sauvegardé les data center qui étaient bombardés par les Russes et donc les données de l'Etat. En matière cyber, les Russes ont été surpris de l'aisance avec laquelle les Ukrainiens ont infiltré leurs systèmes. A titre d'illustration, les services ukrainiens ont été en mesure de dérober la base de données RH de Wagner.

De leur côté, les Russes ont accepté la présence de cyber mercenaires : ils sont utilisés par l'Etat lorsque ce dernier a besoin d'eux. Le reste du temps, ils se servent par l'intermédiaire de *ransomwares*.

Menace cyber dans le monde

L'Iran a créé des cyber mercenaires à l'université de Téhéran. Leur objectif est de voler de l'argent au profit de l'Etat iranien. Dans ce cadre, ces corsaires se sont spécialisés dans le *ransomware as a service*. Une fois le *malware* installé dans une entreprise, la clé est vendue très cher.

De son côté, la Chine dispose de réels moyens étatiques sur le sujet. La notion de mercenaire commence à apparaître. Un sujet peu évoqué se rapporte à l'espionnage. L'ANSSI a commencé à mettre en exergue la menace que représente l'espionnage chinois. En 2022, cet organisme a mené douze opérations majeures de cyberdéfense.

Pour les entreprises, la concurrence chinoise constitue une réalité, mais l'espionnage également. Récemment, Microsoft a publié des documents en lien avec la NSA (National Security Agency, Agence US de renseignement par moyens électroniques) et le CISA (Cybersecurity & Infrastructure Security Agency, cf. ci-après). En effet, les Chinois ont récupéré des vulnérabilités dans les systèmes Microsoft et ont mené des opérations essentiellement contre les Etats-Unis. Leur objectif est d'attaquer les infrastructures.

En 2008 et dans le cadre de la loi de programmation militaire française, des opérateurs d'importance vitale ont été définis. Un débat avait porté sur la nécessité pour l'Etat de réguler ou non les entreprises privées. Il apparaît que les entreprises n'investissent jamais vraiment en matière de cybersécurité avant de subir une attaque. De leur côté, les entreprises américaines privées qui fournissent des services essentiels ont désormais l'obligation de déployer des règles de cybersécurité contraignantes. Dans ce cadre, les Américains ont créé le CISA ou *Cyber Infrastructure Security Agency*. Cette agence est chargée de vérifier que ces entreprises mettent bien en œuvre ces règles.

Le rapport du CERT-ANSSI

Chaque année, une conférence technique est organisée à propos de la sécurité de l'information, à savoir le SSTIC. A l'occasion de la conférence 2023, un exposé a été réalisé par le responsable du CERT.

Dans les années 2010, les attaques ciblaient les secteurs stratégiques à l'instar d'Airbus. Ces entreprises ont ensuite renforcé leur système d'information, ce qui a conduit à un basculement sur les sous-traitants. Il est apparu que de nombreuses tentatives d'attaques provenaient de Chine. Au lieu d'attaquer Airbus qui est très bien protégé, les pirates préféraient s'en prendre à Capgemini qui s'occupe des serveurs d'Airbus.

Un basculement est ensuite intervenu sur les équipements embarqués. De nombreuses attaques ont été conduites sur les systèmes télécom. L'idée est de récupérer des informations dans les usines et de les bloquer. Il convient ensuite de mentionner de nouvelles formes d'espionnage. L'exemple de Pegasus est intéressant. Il s'agit d'un *malware* qui permet de rentrer dans un smartphone et d'en prendre le contrôle. Cet espionnage

ciblé à travers les téléphones portables constitue une réalité. A titre d'illustration, une vingtaine de téléphones portables d'autorités publiques françaises ont été piratés.

Int : Comment l'installation intervient-elle ?
BB : Par exemple et avec l'iPhone, il convient de mentionner une faille dans iMessage. Toute réponse à un message caché infecte le téléphone. Il n'y a pas besoin de *phishing*. Enfin, l'espionnage ne concerne pas uniquement les autorités chinoises, il est également pratiqué par les concurrents.

Apprendre à gérer le risque numérique

Le problème du risque numérique est qu'il ne peut pas être éliminé, ce qui suppose de vivre avec. Les entreprises doivent le comprendre et déployer des outils techniques et d'organisation afin de le maîtriser. Or, de nombreuses sociétés n'ont pas encore engagé de réflexion en la matière. Dans les années 1990, l'informatique était cloisonnée. Désormais, le système est complètement ouvert : les données doivent circuler. Leur maîtrise correspond à un changement culturel.

Le *National Institute of Standards and Technology* (NIST) a défini un *framework*, à savoir le *Zero Trust Model* dont la stratégie repose sur cinq éléments :

- *identify ;*
- *protect ;*
- *detect ;*
- *respond ;*
- *recover.*

La stratégie cybersécurité de l'entreprise

Les failles sont souvent le fait des personnes et des équipes. La stratégie cybersécurité de l'entreprise doit reposer sur un certain nombre de fondamentaux :

- séparer clairement les fonctions d'exploitant du numérique (DSI) et de contrôleur du numérique (CISO – Chief Information Security Officer) ;
- créer une tour de contrôle du numérique rattachée au PDG ;
- déployer de nouveaux métiers : identifier (*Cyber Threat Intelligence*), créer un CERT (Computer Emergency Response Team), détecter et réagir (SOC CSIRT - Security Operations Center & Computer Security Incident Response Team), apprendre à gérer la crise cyber, préparer et tester un plan de reprise d'activité PRA ;
- contrôler en temps réel la bonne garantie des règles techniques des exigences de sécurité : ANSSI, NIST, ISO27000).

Le contrôle permanent de *l'active directory* est primordial. Afin de gérer le risque numérique, quatre instances s'avèrent fondamentales :

- la cyber *design authority* qui est responsable de la qualification de toutes les applications de l'entreprise ;
- SOC CSIRT: détecter, réagir ;
- le CERT : identifier les risques (internes) et les menaces (externes) ;
- le maintien en conditions de sécurité : AD, Firewall, Patch, DMZ, etc.

Int : Un compromis consiste à avoir un RSSI dans la DSI, mais qui se comporte de manière indépendante.
BB : Je ne suis pas certain.

Bernard BARBIER relève ensuite la nécessité de disposer d'une capacité opérationnelle de défense, expérimentée et entraînée. Deux éléments clés de réussite se rapportent au fait de comprendre, de réagir très vite, mais également de rester discret. La plupart des entreprises ne disposent pas de ressources pour créer une capacité opérationnelle de défense efficace, elles externalisent. Il convient impérativement de disposer d'un cyber arsenal défensif souverain, mais également de créer et d'entraîner une cyber armée prête à se projeter immédiatement pour conduire la guerre défensive au sein des entreprises.

Enfin, il importe de retenir les éléments clés suivants :

- segmenter les réseaux, *Zero Trust Network* ;
- mettre en place des bastions durcis : tier0 et comptes à privilèges, MFA (Mail Filtering Agent), IAM (Identity & Acess Management) ;
- système de détection et réaction avancée : EDR (Endpoint Detection and Response) et SOAR (Security Orchestration & Automated Response) ;
- chiffrement des données, maîtriser les données dans le *Cloud.*

En France, 1,06 milliard d'euros de chiffre d'affaires a été perdu entre le 1er janvier et le 31 août 2022 à la suite d'attaques de type *ransomware*. Les attaques revendiquées envers le secteur public en Europe ont enregistré une croissance de 14 % entre mai et août 2022. Les attaques sont aujourd'hui quasiment automatisées et pénalisent fortement le secteur public. Les grandes entreprises ont renforcé leur SI et peuvent se protéger, ce qui n'est pas le cas des PME, des collectivités ou des hôpitaux.

Il explique ensuite s'être associé à plusieurs start-up, dont Tehtris qui regroupe 300 personnes à Pessac et au cyber campus de la Défense. Cette entreprise œuvre dans le domaine de la cybersécurité et propose un outil EDR-XDR (Extended Detection and Response). Pour les grandes entreprises, il presque obligatoire d'avoir un EDR afin d'être cyber assuré. L'EDR est efficace dans la mesure où il détecte des évènements anormaux grâce à un effet d'apprentissage. En outre, il bloque tout process qui pose une difficulté et empêche le *malware* de se propager. Pour autant, il peut être problématique de bloquer un système sur certaines fonctions métiers.

Int : A quel endroit les data sont-elles stockées avec Tehtris ?
BB : Elles sont chez OVH.

Un autre outil intéressant se rapporte à Anozr Way. Le constat est que 80 % des attaques cyber passent par les personnes. Cet outil permet de détecter et de remédier aux vulnérabilités des dirigeants au sein de l'entreprise. Anozr Way a obtenu le prix de la start-up FIC 2023.

Int : Cette entreprise dispose-t-elle d'une équipe afin de convaincre les dirigeants ?
BB : Tout à fait. Je travaille avec eux afin de convaincre les dirigeants.
Int : Il peut s'avérer délicat de les convaincre.

Présentation des orateurs

Bernard Barbier, Centralien, a travaillé au CEA sur les supercalculateurs avant d'en devenir le DSI. Il a poursuivi sa carrière comme Directeur Technique de la DGSE, puis RSSI du groupe Cap Gemini, et maintenant consultant.