A N D S I

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

Sécuriser sa vie numérique

Compte rendu rédigé par ANDSI & Pierre Delort

En bref…

Pierre-Guillaume GOURIO-JEWELL abordera la thématique de la sécurisation de la vie numérique, professionnelle et personnelle. Après avoir identifié diverses menaces, il présentera des solutions permettant de faire face aux risques qui peuvent mettre en danger les organisations.

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.

Le contexte

Pierre-Guillaume GOURIO-JEWELL souligne qu'il convient en premier lieu de définir les menaces. Six catégories d'attaques peuvent être identifiées : lucrative, politique, militaire, ludique, technique et pathologique. La probabilité d'être confronté à une attaque miliaire apparaît relativement faible.

De manière générale, les objectifs recherchés par les attaquants sont classiques. Ils renvoient à l'espionnage, l'invasion, la propagande, le sabotage, la fraude massive et la saturation. Les attaques de saturation ne sont pas évidentes à définir, leur intérêt n'étant pas toujours identifié.

Les menaces les plus courantes se déclinent comme suit :

- chantage économique : ciblage d'entreprises spécialisées, cryptolocker ;
- pression stratégique : vote dans un Conseil d'administration ;
- espionnage : Pegasus.

Par ailleurs, deux types de sources d'attaques doivent être distingués, à savoir celles opérées par les particuliers et celles réalisées par États/entreprises, ces dernières étant plus dangereuses.

Face à ces menaces, les moyens de protection sont toujours identiques et renvoient notamment aux bons outils, aux bonnes pratiques, à la séparation des activités et des moyens. Le risque résiduel existe toujours. En conséquence, il apparaît nécessaire de jouer « franc-jeu ». Autrement dit, les acteurs en mesure d'intervenir afin d'apporter leur aide doivent être correctement informés à propos de la situation, ce qui suppose d'avoir confiance.

Il est également indispensable d'utiliser les bons outils. A titre d'illustration et concernant les mots de passe, le recours à KeePass s'avère très utile. Dans les Directions, les mots de passe sont encore trop souvent partagés. La question du chiffrement est également très importante. L'absence d'automatisme en la matière est regrettable, car le chiffrement représente une réelle solution.

Int : Les clés de chiffrement sont-elles passées de 128 à 256 caractères ?

PGGJ : Je relève plusieurs solutions en matière de chiffrement. La première consiste à augmenter la taille. *A priori*, il n'existe plus de limite maximum. Il n'y en a d'ailleurs jamais eu dans le domaine stratégique. De nouvelles techniques de chiffrement reposant sur des courbes elliptiques permettent d'atteindre un niveau de complexité de chiffrement plus important.

Par ailleurs, il est important de disposer de plusieurs téléphones et ordinateurs et de ne pas utiliser à l'étranger son ordinateur professionnel. Il convient de se méfier des voyages à l'étranger. En outre, il semble opportun de prendre en compte les « faiblesses » de son entourage personnel et professionnel.

Int : Quelle longueur de mot de passe conseillez-vous dans ce cas ?
PGGJ : La longueur du mot de passe ne représente pas forcément un élément important. Il est essentiel que le mot de passe soit auto généré, ce qui permet de ne pas le mémoriser. Un mot de passe comprenant entre 20 et 25 caractères peut suffire dans la plupart des cas. Un mot de passe plus long (typiquement 60 caractères) peut être utilisé pour des applications critiques (banques, administration d'hyperviseurs, …) . Il est aussi recommandé de ne pas utiliser un mot de passe identiques sur deux sites différents.

Les différents acteurs institutionnels

Plusieurs entités sont en mesure d'apporter une aide. Il convient tout d'abord de mentionner les acteurs étatiques à l'instar du COMCYBER, mais également l'ANSSI et le C3N de la Gendarmerie Nationale. Les gendarmes ont la particularité de correctement mailler le territoire et de disposer d'experts cyber. D'autres acteurs institutionnels correspondent à des acteurs profonds : la DGSI/DGSE ainsi que le Ministère des Affaires Étrangères qui est un relai important hors de France.

Exemples de risques

Une famille de risques renvoie à l'ingénierie sociale. Dans ce cadre, HBGary qui était une société de sécurité en est un exemple pertinent. Cette entreprise qui avait affirmé qu'elle comptait détruire les *anonymous* alors qu'elle n'était pas prête techniquement a finalement été attaquée de manière profonde. Cet exemple correspond à un réel cas d'école intéressant à étudier.

Un autre risque lié à l'ingénierie sociale renvoie à la fraude au Président. Le *phishing* représente également un risque qui permet de récupérer des données ou des identifiants. Certaines tentatives s'avèrent extrêmement réalistes.

Les menaces logicielles renvoient à une autre catégorie de menace : il s'agit de composants logiciels qui existent « sur étagère ». Ces derniers peuvent utiliser des *exploits* qui n'ont jamais été référencés, ce qui rend toute protection difficile. L'ingénierie sociale constitue un point d'entrée privilégié pour rentrer dans une entreprise. A titre d'illustration, une simple photographie permet de récupérer une empreinte. Une personne qui dispose de connaissances techniques peut exploiter cette faille.

En outre, la plupart des applications de *chat* stockent énormément des données. Les plus saines en la matière sont Signal et Telegram. A l'opposé, il convient de mentionner WhatsApp et Facebook.

Le hacking par des composantes physiques

Certains outils discrets permettent une intrusion. Dans ce cadre, une simple clé USB trouvée par terre ou distribuée dans un salon peut s'avérer suffisante. Le *USB rubber key* qui ressemble à une clé USB correspond à un type d'appareil beaucoup plus dangereux. A noter également l'existence du keylogger.

Int : Ce type de matériel peut-il être détecté ?
PGGJ : Non. Ces appareils relativement peu onéreux se retrouvent désormais aisément sur Internet.
Int : La sécurisation des IoT permet-elle de les détecter ?
PGGJ : Non.

Pour ce qui est des techniques complexes, le backdoor correspond à un exemple pertinent. Il s'agit d'un composant directement assemblé sur la carte de l'ordinateur et qui permet d'accéder au système. Il s'avère extrêmement délicat à détecter. Peu de personnes démontent leur ordinateur afin de rechercher une puce.

Int : Ces puces sont-elles implantées sur l'ensemble des produits ?
PGGJ : Non, certains ordinateurs sont ciblés.

D'autres outils existent, et les Israéliens sont très avancés dans ces domaines et sont des producteurs de source de hacking (matériel ou non) réputés, pour des prix généralement abordables vis-à-vis des cibles visées
Autre exemple, un processus d'attaque original se rapporte à la reconstitution vocale à partir de sources vidéo (sans l'audio). C'est d'ailleurs pour cela qu'il est déconseillé de tenir une réunion stratégique dans une pièce équipée de fenêtres donnant sur la rue.

Le Crime as a Service (CaaS)

Le CaaS ne se trouve pas aisément sur Internet, mais plutôt sur le darknet. Le darknet correspond généralement à un *overlay network*. Un réseau superposé ou réseau *overlay* se définit comme un réseau informatique bâti sur un autre réseau. Les nœuds du réseau superposé sont interconnectés par des liens logiques du réseau sous-jacent. La complexité du réseau sous-jacent n'est pas visible par le réseau superposé. Ce type de réseau est généralement très résistant, voir indestructible, à moins qu'une erreur humaine ne soit commise. Ces *overlay networks* représentent un véritable problème. Pour autant, il s'agit parfois d'un moyen pour des opposants politiques de mener leur lutte.

Quelques solutions peuvent être envisagées afin de réduire les risques et tout d'abord le VPN. Cet outil protège les utilisateurs dans le train, l'avion, etc. Pour des activités personnelles dans certains pays, il est fortement conseillé de recourir à un VPN. Le fait de séparer ses activités en fonction des téléphones et des tablettes permet également de réduire les risques en cas de piratage.

Un autre sujet important se rapporte à la destruction du matériel. Un matériel ayant détenu des données sensibles, même si elles ont été chiffrées, ne doit pas être donné. Les éléments sensibles doivent être détruits physiquement.

En termes de bonnes pratiques, il apparaît nécessaire de se préparer, de n'allumer ses appareils qu'au moment de l'usage, de ne pas se connecter aux réseaux (Wifi, Bluetooth, 4G, etc.) ou à des comptes existants. Il est également impératif de s'adapter en fonction des pays et des législations. En Europe, les lois cyber sont peu nombreuses, et assez permissives, ce qui n'est pas le cas dans d'autres pays.

Enfin, les trois références suivantes, bien que différentes, s'avèrent intéressantes : l'Art de la guerre de Sun Tzu, la série TV Mr Robot ainsi que le livre intitulé Habemus Piratam.

Débat

Int : Que pensez-vous du niveau d'efficacité du VPN natif de Microsoft ?

PGGJ : Le problème majeur des produits Microsoft est qu'ils sont… des produits Microsoft. La probabilité qu'ils présentent un risque de sécurité est importante. Les personnes qui cherchent des failles se tourneront vers ces produits. A ce jour, le meilleur standard correspond à WireGuard.

Int : Auriez-vous un conseil à prodiguer concernant le stockage des mots de passe ?
PGGJ : Je vous conseille d'utiliser KeePass qui correspond à une référence pour les mots de passe sensibles. Dans le cadre des connexions régulières, l'utilisation de 1Password ou du gestionnaire de mots de passe de Firefox semble suffisante. En effet, le risque n'est pas identique.
Int : KeePass correspond à l'un des rares outils approuvés par l'ANSSI.
PGGJ : En effet. Pour autant, la nouvelle version n'a pas fait l'objet d'une réévaluation.

Int : L'authentification à facteurs multiples qui renvoie à une parade intéressante est insuffisamment utilisée dans les entreprises.
PGGJ : Vous avez raison. Toutefois, tous les acteurs dans une entreprise ne sont pas sensibilisés à l'informatique et aux risques cyber. Il convient de fournir des systèmes simples aux salariés. Il s'agit d'un sujet humain plus que technique.

Int : Quels sont les outils de visioconférence les plus sécurisés et quels sont les risques ?
PGGJ : Je recherche toujours l'outil parfait qui offrirait une réelle résistance. Les différentes solutions qui existent sur le marché sont équivalentes en termes de sécurité. Au début de la pandémie, des problèmes de sécurité avaient été constatés avec Zoom et les difficultés ont globalement été corrigées depuis. Quelques applications à l'instar de Signal ou de Telegram permettent de faire des visioconférences. Elles sont plus sécurisées que Teams ou Zoom. Néanmoins, je ne vous conseille pas de les utiliser dans un cadre professionnel.

Int : La faiblesse des anti-spams en termes de détection me semble surprenante.
PGGJ : Le spam provient désormais de boîtes mails valides qu'il s'avère délicat de neutraliser. De surcroît et dans leur stratégie de communication, des entreprises comme Amazon confient le démarchage à des entreprises tierces.

Présentation des orateurs

Pierre-Guillaume GOURIO-JEWELL est expert Cybersecurity & Privacy, et participe à de nombreuses interventions sur le sujet (Institut des Hautes Études de la Défense Nationale, Clusif, IRIS…). Il est Docteur Ingénieur en Mathématiques appliquées.