Annexe 8

Posture de cybersécurité (ANSSI)

1. Évaluation de la menace

La période couverte par la présente posture est caractérisée par les trois tendances suivantes.

1.1. Exploitation de vulnérabilités critiques

La divulgation en sources ouvertes de vulnérabilités, dont certaines sont dites « exfiltrées » des agences américaines du renseignement, la NSA et la CIA, est régulièrement observée. L'exploitation par des codes malveillants de ces vulnérabilités peu de temps après leur divulgation tend à se répéter de façon inquiétante.

Ainsi, le rançongiciel WannaCry s'est répandu dans 150 pays, en mai 2017. Nombre des organismes concernés ont éprouvé des difficultés à mettre en œuvre une politique de mise à jour de leurs logiciels et de leurs systèmes d'exploitation. Les correctifs publiés par les éditeurs de logiciels ne sont pas appliqués assez rapidement, rendant les systèmes d'information d'autant plus vulnérables. Cette campagne d'attaque a perturbé le fonctionnement d'entreprises françaises, notamment le constructeur automobile RENAULT, qui a dû fermer temporairement plusieurs sites de production.

1.2. Attaques par rançongiciel

L'ANSSI observe une augmentation des attaques par rançongiciel, dont certaines à des fins de sabotage. Les rançongiciels sont majoritairement diffusés par un courriel piégé et/ou un site Internet piégé. L'ANSSI constate une variété de rançongiciels, de virulence variable, tels que Cryptolocker, Locky, Cryptowall ou Wannacry, qui séquestrent les données des machines infectées jusqu'à ce que la victime paie la rançon généralement avec une cryptomonnaie notamment de type Bitcoin.

1.3. Attaques indirectes par l'intermédiaire des systèmes de distribution de logiciels

Certains attaquants compromettent des systèmes de mise à jour de logiciels légitimes afin d'atteindre leurs cibles finales, passant outre les mesures de protection numérique mis en place par ces dernières. Ce mode opératoire d'attaque a été observé par l'ANSSI à plusieurs reprises ces derniers mois. Ainsi, le code malveillant NotPetya, initialement identifié sous l'apparence d'un rançongiciel, a été diffusé, fin juin 2017, par des sites populaires préalablement compromis et par une mise à jour d'un logiciel de gestion ukrainien. La compromission du système de mise à jour du logiciel de gestion ukrainien a été la piste la plus étudiée. La propagation de NotPetya s'est appuyé en partie sur l'exploitation des mêmes vulnérabilités critiques identifiées lors de la compromission par le rançongiciel WannaCry. Il ne fait aucun doute que ce code malveillant a perturbé le fonctionnement d'entités françaises, jusqu'à rendre inopérant le système d'information victime.

Plus récemment, il a été rapporté la compromission du système de mise à jour du logiciel grand public CCleaner qui opère plus de cinq millions de téléchargements par semaine. Ce type d'attaque permet de maximiser le nombre de machines infectées pour mener des actions ultérieures à des fins d'espionnage ou de sabotage.

1.4. Sécurité des connections Wi-Fi

Le 16 octobre 2017, des chercheurs belges en sécurité informatique ont révélé l'existence d'une vulnérabilité majeure mettant en cause la sécurité de l'ensemble des connexions Wi-Fi. Cette faille permettrait à un attaquant de déchiffrer les données transmises sur un réseau Wi-Fi, même lorsque ce dernier est protégé par un protocole de chiffrement. Cette vulnérabilité affecte les protocoles de sécurité WPA et WPA 2 (Wi-Fi Protected Access), qui permettaient jusqu'alors, d'assurer la sécurité des communications sans fil.

1.5. Sensibilité liée à la période de la fin d'année et aux périodes de congés

La période des fêtes devrait accroître ces tendances. Traditionnellement, cette période est propice à l'échange massif de courriels (vœux, offres promotionnelle, etc.) et à une baisse de la vigilance, tant des utilisateurs que des équipes de sécurité informatique.

En raison des congés du personnel dans les entreprises et dans les administrations, il peut être plus difficile pour les responsables informatiques de détecter les tentatives et les signes d'attaque en cours, de réduire les impacts d'une attaque sur l'organisation et de réagir de manière adaptée lors d'un incident.

En outre, le retour de congés peut, en lui-même, représenter un moment particulièrement critique. En effet, le système d'information peut être plus vulnérable lors du redémarrage des stations de travail, éteintes pendant la période des congés, et qui nécessitent l'application des mises à jour du système d'exploitation et des logiciels. La baisse de vigilance des utilisateurs de l'outil informatique peut engendrer des incidents de sécurité des systèmes d'information. Le risque de compromission voire de sabotage, notamment par la réception d'un courriel d'hameçonnage, est ainsi accru durant cette période car la consultation de la messagerie professionnelle est souvent la première action des agents revenant de congés (cf. annexe 6).

2. Les mesures de protection cyber

Les mesures cyber actuellement en vigueur sont maintenues.

Afin de faire face aux risques induits par la période de référence, il convient de rappeler l'importance des mesures socle aux ministères et aux opérateurs. Il leur appartient de surveiller leurs propres sites et de s'assurer de l'application des mesures proposées dans la PSSIE et la loi de programmation militaire ou dans le guide d'hygiène informatique pour les opérateurs non-OIV.

En outre, il importe de mettre en œuvre les mesures prescrites dans les fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR, notamment la fiche CERTFR-2017-ALE-012 sur la campagne de maliciels prenant l'apparence d'un

rançongiciel à multiples capacités de propagation (Petya/Not Petya). Ces recommandations sont listées en pièce jointe.

Concernant la sécurité des connexions Wi-Fi, l'ANSSI préconise d'appliquer les mises à jour de sécurité dès leur publication et de limiter l'utilisation du Wi-Fi à des communications non sensibles. Une fiche de recommandations sur ce sujet est accessible sur le site https://www.cert.ssi.gouv.fr/alerte/actives .

Les mesures cyber du plan VIGIPIRATE proposées pour renforcer la vigilance, la protection et la prévention pendant la période de validité de la posture concernent :

- les capacités à assurer une continuité des activités en cas d'incident (limitation des effets d'un sabotage éventuel ou d'une intrusion) ;

- la journalisation et la capacité à détecter des incidents (identification des événements suspects et investigation) ;

- la mise en place d'un filtrage réseau adéquat (prévention des intrusions) ;

- la sauvegarde effective des données sensibles et la capacité de restauration (mise en œuvre des plans de continuité d'activité et de reprise d'activité) ;

- la robustesse face à une élévation du volume des flux réseau (dispositif de prévention d'attaque en déni de service) ;

- l'application exhaustive des mises à jour de sécurité sur les composants exposés sur Internet (prévention des attaques) ;

- pour les opérateurs d'importance vitale, la transmission, sans délai, à l'ANSSI de déclarations d'incidents sur les systèmes d'information exposés (veille globale et réactivité d'intervention du COSSI) ; pour les particuliers, entreprises et collectivités territoriales (hors OIV) victimes d'une attaque, il est recommandé de se rendre sur la plateforme numérique www.cybermalveillance.gouv.fr, afin d'être mis en relation avec des prestataires de proximité susceptibles de les assister techniquement.