Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'AGRICULTURE ET DE L'ALIMENTATION

Références :

1. Note n° NP/151/SHFDS du 21 octobre 2019 relative à la posture VIGIPIRATE « AUTOMNE HIVER 2019 – PRINTEMPS 2020 » ;
2. Note n°10083/SGDSN/PSE/PSN/CD du 16 octobre 2019 relative à l'adaptation de posture VIGIPIRATE « AUTOMNE HIVER 2019 – PRINTEMPS 2020 » ;
3. Plan gouvernemental VIGIPIRATE n° 10200/SGDSN/PSE/PSN/CD du 1er décembre 2016 (édition octobre 2018) – partie publique « Faire face ensemble » (décembre 2016) https://www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd.pdf.

Objet : Fiche SECNUM « *Sécurité numérique* »

Destinataires : Responsables Sécurité des Systèmes d'Information (RSSI)

Posture VIGIPIRATE « AUTOMNE HIVER 2019 – PRINTEMPS 2020 »[1] :

La posture VIGIPIRATE « AUTOMNE HIVER 2019 – PRINTEMPS 2020 » est active à compter du 18 octobre 2019.

Elle s'applique, sauf événement particulier, jusqu'au 14 mai 2020.

L'ensemble du territoire national est maintenu au niveau « *Sécurité renforcée – Risque attentat* ».

Sur le territoire national, la menace terroriste se maintient à un niveau élevé et émane essentiellement de ressortissants nationaux. Bien qu'affaiblie, la propagande djihadiste reste soutenue dans la sphère numérique et est toujours susceptible de provoquer des passages à l'acte individuels.

La présente posture adapte le dispositif de sécurité nationale pour cette période marquée par :

- les fêtes de fin d'année qui seront ponctuées par les célébrations religieuses et l'organisation sur l'ensemble du territoire national de marchés de Noël de plus ou moins grande ampleur ;
- les flux importants de voyageurs dans les transports collectifs de personnes lors des vacances scolaires et universitaires et leur présence sur les sites touristiques ;
- les grands évènements qui se dérouleront sur le territoire national qu'ils soient sportifs, culturels ou commémoratifs ;
- les élections municipales des 15 et 20 mars 2020.

[1] Différents supports sont disponibles sur le https://www.gouvernement.fr/reagir-attaque-terroriste :
- Affiches de sensibilisation à destination du grand public : « *Réagir en cas d'attaque terroriste* », « *Les gestes d'urgence* », « *Que faire en cas d'exposition à un gaz toxique* » ;
- Fiches « réflexes » informant les citoyens et les professionnels de différents secteurs d'activité sur les bonnes pratiques à adopter face à la menace terroriste ;
- Guides de bonnes pratiques, à destination des professionnels et des particuliers.

Domaine « Sécurité numérique » :

Les menaces visant les administrations et les entreprises privées restent élevées et variées. Les événements majeurs de la période feront l'objet d'une attention particulière face aux principaux modes d'action malveillants actuellement observés (attaques par rançongiciels, attaques indirectes et vulnérabilités critiques).

Les entreprises privées opérant dans des domaines d'activités du ministère de l'agriculture et de l'alimentation ne sont pas épargnées par les cyberattaques ou les tentatives d'attaque : signalons notamment les sociétés FLEURY MICHON et EUROFINS dont les attaques, survenues respectivement en avril et en juin 2019, ont fait l'objet de communication.

Les éléments relatifs à l'évaluation des principaux risques cyber sur la période couverte sont précisés en annexe 1 (annexe à « Diffusion restreinte »).

Les objectifs de sécurité recherchés et les mesures associées, qui sont détaillées en annexe 2, sont les suivants :

- Concernant les vulnérabilités critiques, les opérateurs et administrations **doivent appliquer les correctifs de sécurité** signalés dans les bulletins d'alerte du CERT-FR[2].
- La fin de la maintenance, en janvier 2020, des systèmes d'exploitation ***Windows 7, Windows Server 2008, Windows Server 2008 R2*** doit être anticipée et la migration, vers un système supporté et offrant la durée de support adéquate, planifiée.
- Afin de prévenir les attaques touchant l'*Active Directory*, l'ANSSI **recommande la réalisation d'audit des annuaires** et le renforcement, si nécessaire, de leur niveau de sécurité. Une fiche pratique dédiée à l'utilisation du service ADS (*Active Directory Security*) est jointe en annexe 4.
- Face à la **menace persistante d'attaques par rançongiciel** (fiche pratique en annexe 3), les mesures visant à prévenir leur survenue et à limiter leurs impacts doivent être poursuivies par les opérateurs et les administrations, en particulier la vérification régulière, au moyen notamment d'exercices, du caractère opérationnel du plan de continuité d'activité (PCA).

L'implication de l'ensemble du personnel ainsi que l'application des règles élémentaires d'hygiène informatique constituent des éléments essentiels au renforcement de la sécurité des systèmes d'information.

A ce titre, les recommandations de posture permanente de sécurité[3] doivent être rappelées régulièrement aux agents, personnels et apprenants. Des réflexes simples peuvent être appliqués, au quotidien par chacun :

- les douze règles essentielles définies, à destination des non-spécialistes, dans le guide des bonnes pratiques de l'ANSSI[4] pour la sécurité des systèmes d'information des petites et moyennes entreprises ;
- les dix règles, à destination des agents du ministère de l'agriculture et de l'alimentation, pour sécuriser les équipements numériques professionnels[5] ;
- les neufs bonnes pratiques de sécurité numérique à observer, par les professionnels, lors de déplacements[6].

[2] *Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques* de l'*agence nationale de sécurité des systèmes d'information* (ANSSI).
[3] https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/
[4] https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
[5] Infographie (http://intranet.national.agri/IMG/pdf/missdef_secuinfo_aff_cle0dffa3.pdf).
[6] Guide de l'ANSSI mise à jour en 2019 (https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/).

Annexe 1 : Evaluation des principaux risques cyber sur la période couverte

Annexe 1 à diffusion restreinte

Annexe 2 : Posture Vigipirate « AUTOMNE HIVER 2019 – PRINTEMPS 2020 »

Liste des mesures applicables au domaine « sécurité du numérique »

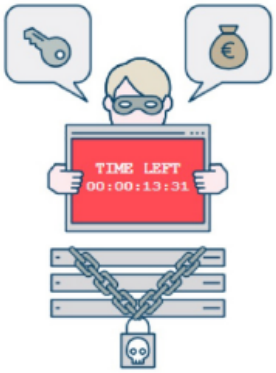
Annexe 2 à diffusion restreinte

Annexe 3 : Rançongiciel : vos données prises en otage

SÉCURITÉ DU NUMÉRIQUE
RANÇONGICIEL : VOS DONNÉES PRISES EN OTAGE

Cible : tous publics

- Un rançongiciel (*ransomware* en anglais) est un programme malveillant dont le but est de chiffrer partiellement ou entièrement les données d'un système, bloquant ainsi leur accès.
- La machine peut être infectée après l'ouverture d'une pièce-jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en navigant sur des sites compromis, ou encore suite à une intrusion dans le système.
- Le principal but recherché est d'extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Si l'intention de ce type d'attaque est cybercriminelle, le mode opératoire de ces attaques peut être lourd de conséquences pour les victimes qui peuvent par exemple voir leur activité paralysée.
- Particulièrement répandues, ces attaques sont de plus en plus sophistiquées et peuvent toucher l'ensemble des acteurs de la société, qu'il s'agisse de citoyens ou d'organisations publiques ou privées.



1 Comment réagir ?

1- N'éteignez pas la machine concernée

L'interruption du processus de chiffrement empêche toute tentative ultérieure de récupération des données.
Mettez la machine en veille prolongée si possible.

2- Déconnectez immédiatement du réseau les machines concernées

L'objectif est de limiter la propagation de l'attaque en bloquant la poursuite du chiffrement des documents sur le réseau.
Ne connectez pas non plus d'appareil supplémentaire sur le réseau.

3- Contactez immédiatement votre service informatique ou un expert

Vous êtes un ministère, un opérateur d'importance vitale (OIV), un opérateur de service essentiel (OSE) ou un fournisseur de service numérique (FSN) ?

→ Prévenez l'ANSSI :
www.ssi.gouv.fr/en-cas-dincident/

Vous êtes une collectivité territoriale, une entreprise privée (non OIV, non OSE), une association ?

→ Contactez si besoin cybermalveillance :
www.cybermalveillance.gouv.fr

4- Ne payez pas la rançon réclamée

Le paiement ne garantit pas le déchiffrement des données et compromettra le moyen de paiement utilisé.

SÉCURITÉ DU NUMÉRIQUE
RANÇONGICIEL : VOS DONNÉES PRISES EN OTAGE

5- Portez plainte auprès des services compétents

Pensez à réunir toutes les traces et indices qui pourraient servir comme éléments de preuve (ex : copies physiques de disques durs des postes compromis).

6- Identifiez la source de l'infection

Prenez les mesures nécessaire pour que la source de l'infection ne puisse pas être utilisée à nouveau (par l'application d'un correctif de sécurité par exemple).

2 Comment se protéger ?

Effectuez des sauvegardes régulières de vos données critiques

Ces sauvegardes vous permettent de limiter le préjudice de l'incident et de reprendre vos activités rapidement. Les supports de ces sauvegardent doivent être déconnectées physiquement du réseau afin d'éviter toute compromission en cas d'incident. Faites également des tests de restauration de sauvegarde réguliers afin de vérifier votre capacité à restaurer vos données en cas d'incident.

Mettez à jour régulièrement vos logiciels

Les rançongiciels utilisent les vulnérabilités des programmes pour se propager, appliquez-donc de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur vos systèmes.

Privilégiez un compte utilisateur pour vos usages courants

N'utilisez pas un compte avec des droits « administrateurs » pour consulter vos messages ou naviguer sur Internet.

Méfiez-vous des messages douteux

Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semble douteuse et méfiez-vous des pièces-jointes et des liens suspects. Il convient en effet de ne pas cliquer sans vérification sur les liens ni d'ouvrir les pièces jointes présentes ; une attention toute particulière devant être apportée aux messages de provenance inconnue, d'apparence inhabituelle ou frauduleuse.

3 En savoir plus

Les bonnes pratiques de l'informatique :
www.ssi.gouv.fr/precautions-elementaires/

Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

En cas d'incident : https://www.ssi.gouv.fr/en-cas-dincident/

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrication, image – DSAF/DPGS – Avril 2019.

Annexe 4 : Sécurité du numérique : retrouvez de la visibilité sur votre annuaire

SÉCURITÉ DU NUMÉRIQUE RETROUVEZ DE LA VISIBILITÉ SUR VOTRE ANNUAIRE

Cible : Administrateurs AD, CHAINE SSI

- L'ANSSI met à disposition des opérateurs stratégiques de l'État une capacité d'audit des annuaires Active Directory (et Samba) au travers du service ADS (Active Directory Security).
- Cette capacité vise à redonner de la visibilité aux opérateurs stratégiques de l'État (ministères, OIV, OSE, etc.) sur le niveau de sécurité de leur annuaire et à les accompagner dans son durcissement par l'application progressive de mesures adéquates. Cette prestation est basée sur l'expérience et l'expertise du bureau audits sur les sujets d'Active Directory (AD), et enrichie par les différentes opérations de cyberdéfense auxquelles le bureau participe.
- Le service ADS permet ainsi à la fois d'objectiver le niveau de sécurité et d'accompagner progressivement les opérateurs vers un niveau de sécurité à l'état de l'art. Cette capacité est pensée à la fois pour les chaînes SSI et pour les chaînes exploitation. Pour les unes, l'application présente les tableaux de bord avec les indicateurs ; pour les autres, elle présente les recommandations détaillées à appliquer et accompagne les bénéficiaires dans le pilotage de leurs prestataires.

1 Bénéficier du service ADS ?

Pour bénéficier du service, la procédure à suivre est particulièrement simple.

1. Télécharger la dernière version de l'outil de collecte ORADAD (Outil de récupération automatique de données de l'*Active Directory*) sur GitHub [**https://github.com/ANSSI-FR/ORADAD/releases**].
2. Extraire les fichiers exécutables (exécutable ORADAD.exe et fichier de configuration).
3. Ouvrir un terminal et exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine. Le fichier de configuration doit être positionné dans le dossier contenant l'exécutable ORADAD.exe [commande à lancer : ORADAD.exe <outputDirectory>].
4. Envoyer l'archive tar contenant les résultats de la collecte (et présent dans le répertoire outputDirectory) à l'adresse club@ssi.gouv.fr. Si la taille du fichier est supérieure à 10 Mo, l'ANSSI met à disposition un serveur d'*upload* sur lequel déposer le fichier. L'URL et les comptes permettant d'accéder au serveur sont fournis à la demande (email à adresser à l'adresse **club@ssi.gouv.fr**)

Dès réception du fichier de collecte, l'ANSSI lancera les analyses et en partagera les résultats dans un délai de 15 jours, sous forme d'un rapport détaillé présentant les différents points de contrôle qui ont révélé des défauts de configuration pouvant entrainer des risques de sécurité.

2 ADS pour les nuls

L'annuaire AD, centre névralgique de la sécurité des systèmes d'information Microsoft

L'annuaire Active Directory est l'élément qui permet de gérer de manière centralisée l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI.

SÉCURITÉ DU NUMÉRIQUE
RETROUVEZ DE LA VISIBILITÉ SUR VOTRE ANNUAIRE

Le faible niveau de sécurité des annuaires met en danger les systèmes d'information

Les prestations d'audit effectuées par l'ANSSI auprès de ses bénéficiaires font apparaître un manque de maturité critique récurrent sur la sécurité des annuaires Active Directory. Ce défaut de sécurité affaiblit significativement le niveau global de sécurité de ces SI. Cette observation est confortée par la connaissance acquise au contact des différents réseaux compromis sur lesquels l'agence est intervenue lors d'opérations de cyberdéfense. Au-delà du manque de maturité, le bureau Audits constate par ailleurs que le niveau de sécurité des annuaires Active Directory décroît en fonction du temps et du cycle de vie du SI.

Développement d'une capacité spécifique et ouverture d'un service

Au sein de l'agence, les prestations d'audit sur un système d'information donnent habituellement lieu à la rédaction d'un rapport détaillé, répertoriant à un temps t les vulnérabilités qui touchent le système d'information, les recommandations correspondantes et la priorité de leur déploiement. Ces rapports, souvent volumineux, ne permettent pas toujours de prioriser avec aisance les actions à mener. Par ailleurs, si un audit donne une idée du niveau de sécurité à un instant donné, il ne mesure pas durablement l'évolution du niveau de sécurité.

Face à ce constat, le bureau Audits a développé une nouvelle capacité dont l'objectif est d'auditer, à la demande du bénéficiaire et de manière autonome, le niveau de sécurité des Active Directories des ministères.

Une approche ludique et personnalisée

Les résultats sont rendus disponibles depuis une interface web qui répertorie et ordonne les vulnérabilités et recommandations afférentes. Lors de chaque audit, le niveau de sécurité de la configuration de l'Active Directory est traduit par un niveau sur une échelle de 1 à 5. Le niveau obtenu découle immédiatement de la gravité des vulnérabilités trouvées le niveau 1 étant synonyme de défauts critiques et le niveau 5 d'un niveau à l'état de l'art.

Un niveau donne ainsi accès à un lot de recommandations adaptées. Une fois ces dernières mises en œuvre, des scripts de contrôle sont aussitôt référencés dans l'interface pour permettre à l'administrateur de contrôler de manière autonome et indépendante la bonne application des recommandations.

L'évolution relative à chaque niveau est objectivée par un score et représentée sur l'interface graphique par une barre de progression. Même si elle ne permet pas toujours d'accéder aux vulnérabilités et recommandations du niveau suivant, la correction progressive des vulnérabilités à un niveau donné, se traduit néanmoins par l'obtention de points. L'administrateur peut ainsi justifier de manière objective que ses actions améliorent significativement le niveau de sécurité de l'AD et donc du SI.

Considérant l'enjeu majeur pour un réseau qu'est la bonne sécurisation de son AD (et son maintien), l'idée de l'ANSSI est d'accompagner progressivement vers un niveau de sécurité à l'état de l'art grâce à l'application de recommandations adéquates et dans un contexte plus ludique (*gamification*).

3 En savoir plus

Envoyer un email à club@ssi.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle Graphisme, Fabrication, Image – DSNR/DPSG – Octobre 2019.