LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

Recommandations de cybersécurité en matière de rançongiciel (« ransomware »)

Novembre 2022

Table des Matières

1 Préambule

Suivant la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, celui-ci a, dans sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI), pour mission : « […] d'émettre des recommandations d'implémentation des politiques et lignes directrices de sécurité de l'information et d'assister les administrations et services de l'État au niveau de l'implémentation des mesures proposées » et «[…] de conseiller, à leur demande, les établissements publics et les infrastructures critiques en matière de sécurité des réseaux et systèmes d'information et des risques y liés […]. »

L'ENISA a rapporté une augmentation de 234% du nombre d'attaques par rançongiciels en 2021. En raison de cette évolution significative, l'Agence nationale de la sécurité de systèmes d'information (ANSSI) a élaboré des recommandations en matière de cybersécurité en matière de rançongiciel.

Ces recommandations ont pour but la prévention, la protection et la réaction aux attaques par rançongiciels.

Il est recommandé à toute entité publique ou privée de définir les priorités d'implémentation des recommandations en fonction de sa posture actuelle, des coûts et des risques adressés.

2 Recours aux services du CERT gouvernemental

Il est rappelé que le CERT gouvernemental peut assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et systèmes d'information des opérateurs d'infrastructures critiques.

Il est fortement recommandé aux opérateurs d'infrastructures critiques d'avoir recours aux services du CERT gouvernemental. Les modalités de leur collaboration pourront être définies dans le cadre d'un mémorandum d'entente (en anglais « Memorandum of Understanding »).

3 Le rançongiciel (« ransomware »)

3.1 Définition

L'Agence européenne pour la cybersécurité (ENISA) définit un rançongiciel[1] comme : « Le rançongiciel est un type d'attaque où les acteurs de la menace prennent le contrôle des actifs d'une cible et exigent une rançon en échange du retour de la disponibilité et de la confidentialité de l'actif. »

[1] ENISA Threat Landscape for Ransomware Attacks - July 2022

3.2 Schéma d'une attaque

3.2.1 Accès initial

L'accès initial est souvent obtenu en utilisant un ou plusieurs vecteurs d'attaque :

- L'utilisation d'identifiants et de mots de passe volés préalablement ;
- L'ouverture volontaire par un utilisateur d'une pièce jointe ou d'un lien contenu dans un e-mail (attaque de type « phishing »). L'attaquant peut également utiliser des mécanismes d'ingénierie sociale afin de favoriser la réalisation de ces actions par l'utilisateur ;
- L'exploitation de vulnérabilités (p.ex. « zero-day ») et d'erreurs de configuration des systèmes.

L'accès initial peut également être obtenu par l'exploitation de tiers et fournisseurs de services de confiance. Les attaquants ciblent alors un tiers ou un fournisseur de service connecté à distance.

Les scénarios d'attaques suivants sont les plus souvent rencontrés[1] :

1. Utilisation d'identifiants et de mots de passe volés sur des solutions d'accès à distance (40% des attaques par rançongiciels impliquent des accès à distance) ;
2. L'hameçonnage (« phishing ») par e-mail (35% des attaques par rançongiciels impliquent des e-mails) ;
3. Exploitation de vulnérabilités sur une application ou infrastructure exposées à Internet (15% des attaques par rançongiciels impliquent des applications web).

3.2.2 Persistance

Après l'accès initial, les attaquants réalisent les actions nécessaires pour que cet accès soit pérenne. Il doit en effet résister à des actions utilisateurs telles que le redémarrage du système ou le changement de mots de passe.

Afin d'atteindre cet objectif, les attaquants peuvent notamment :

- Installer un ou plusieurs logiciels malveillants, qui cherchent généralement à se cacher des antivirus et autres mécanismes de détection ;
- Activer des protocoles d'accès à distance (p.ex. Remote Desktop Protocol), s'ils sont désactivés ;
- Modifier des mots de passe de comptes utilisateurs ;
- Créer des comptes malicieux ;
- Créer des tâches systèmes planifiées.

3.2.3 Élévation de privilèges

L'accès initial pérennisé, les attaquants cherchent à obtenir des droits d'accès de plus en plus élevés. Pour les environnements Windows, l'accès aux droits « Domain Administrators » est recherché.

[1] « 2022 Data Breach Investigation Report (DBIR) » de Verizon

Afin d'atteindre cet objectif, les attaquants cherchent généralement à identifier des vulnérabilités non corrigées et/ou voler des identifiants et des mots de passe.

3.2.4 Reconnaissance et mouvements latéraux

Les attaquants cherchent à comprendre l'architecture des systèmes d'information de l'organisation ciblée. Afin d'atteindre cet objectif, les attaquants peuvent notamment réaliser les actions suivantes :

- Utiliser des outils ou des commandes telles que ADFind, nltest, Bloodhound, etc. ;
- Utiliser des outils de contrôle à distance tels que Remote Desktop Protocol (RDP) ou PsExec (un outil légitime de la suite SysInternals de Microsoft) ;
- Utiliser des logiciels malveillants spécifiquement développés pour réaliser leurs attaques ;
- Utiliser des méthodes d'ingénierie sociale (p.ex. collecte d'informations confidentielles auprès des collaborateurs en les contactant par téléphone).

3.2.5 Exfiltration

En utilisant les privilèges frauduleusement instaurés, les attaquants déploient des logiciels malveillants dans le but d'exfiltrer des données. Les données volées peuvent être fractionnées en lots afin de faciliter leur exfiltration.

Pour les environnements Windows, ces logiciels peuvent être déployés par le biais d'une utilisation frauduleuse des « Group Policies Object (GPO) » de l'Active Directory.

3.2.6 Chiffrement

Les attaquants procèdent au chiffrement des données accessibles avec une clé qu'eux seuls possèdent.

Ils cherchent également à détruire les sauvegardes pour empêcher le recouvrement des données et ainsi maximiser les chances de paiement de la rançon.

3.2.7 Extorsion

Après le chiffrement des données, les attaquants procèdent à de multiples tentatives d'extorsion, le plus souvent en même temps :

- Menace de supprimer définitivement les fichiers, sans possibilité pour l'organisation de les récupérer ultérieurement;
- Menace de publier publiquement ou de façon privée les données volées de l'organisation sur le « dark web ». Les attaquants peuvent également menacer de les vendre à des tiers ;
- Menace de procéder à une attaque par déni de service distribuée (« DDoS ») sur l'organisation.

Les attaquants demandent généralement à obtenir le paiement de la rançon en cryptomonnaie (p.ex. Bitcoin) car cette forme de paiement permet d'échapper à toute identification par les autorités.

3.3 Professionnalisation des attaquants

Depuis leurs premières apparitions en 1989, la fréquence et la complexité des attaques par rançongiciels sont en constante augmentation.

Au départ, ces attaques étaient l'œuvre d'attaquants isolés. Ces attaquants agissaient seuls ou en petits groupes. Les attaques étaient généralement peu complexes et utilisaient des outils chiffrant automatiquement les données accessibles.

Actuellement, ces attaques sont généralement[1] réalisées par des groupes hautement spécialisés. Il s'agit de groupes criminels très organisés, se répartissant les tâches pour réaliser l'attaque et agissant de façon très coordonnée.

De plus en plus d'attaques sont également réalisées à l'aide d'infrastructures « Ransomware-as-a-Service (RaaS) ». Il s'agit de plateformes permettant aux groupes affiliés de disposer de solutions « clés en main » pour réaliser des attaques par rançongiciels.

4 Prévention : recommandations prioritaires

4.1 Sauvegarde des données

R1	Sauvegarder régulièrement les données.

R2	Mettre en place une stratégie de rétention des sauvegardes couvrant plusieurs mois.

Etant donné que des attaquants peuvent se propager dans les réseaux durant plusieurs mois sans être détectés, des sauvegardes de plusieurs mois devraient être conservés.

R3	Réaliser des tests réguliers de restauration des sauvegardes.

R4	Conserver hors ligne (c.-à-d. déconnectée des réseaux internes) au moins une sauvegarde saine des données, afin qu'elle ne puisse pas être chiffrée, corrompue ou supprimée.

4.2 Correctifs de sécurité

R5	Se tenir informé des vulnérabilités identifiées pour les logiciels, systèmes et applications utilisés.

Des vulnérabilités de sécurité sont régulièrement découvertes et publiés par les éditeurs de logiciels et de systèmes, des organisations à but non lucratif[2], etc.

[1] ENISA Threat Landscape for Ransomware Attacks - July 2022

[2] p.ex. CVE - CVE (mitre.org)

R6	Installer dans les meilleurs délais les correctifs de sécurité, en priorisant les plateformes exposées sur Internet (p.ex. applications web, site web ou de messagerie) et les plateformes critiques pour la continuité des activités (p.ex. « Domain Controller Active Directory »).

R7	Réaliser régulièrement des scans de vulnérabilités et/ou des tests de pénétration sur les plateformes exposées sur Internet et les plateformes critiques pour la continuité des activités.

4.3 Authentification multi-facteurs pour les accès à distance

R8	Implémenter une authentification multi-facteurs pour les accès à distance (p.ex. VPN).

L'authentification à multi-facteurs nécessite une combinaison d'au moins deux composantes d'authentification avant de donner l'accès à un compte : quelque chose qu'un utilisateur connait (p.ex. un mot de passe), quelque chose qu'un utilisateur possède (p.ex. une « SmartCard » ou une clé USB) ou quelque chose qui identifie l'utilisateur (p.ex. empreinte digitale).

4.4 Gestion des accès à distance

R9	Limiter le plus possible l'attribution des accès à distance, selon le principe du « moindre privilège ».

R10	Désactiver sans attendre les accès à distance d'utilisateurs à la fin de leur date de travail effectif. Planifier périodiquement une revue des accès afin de s'assurer que seuls les utilisateurs sous contrat disposent de comptes actifs.

R11	Mettre en place des mécanismes de prévention ou, à défaut, de détection d'usage non autorisé de l'accès à distance.

Par exemple, un accès ou tentative d'accès à distance devrait être investigué s'il est réalisé en dehors des heures habituelles de travail (p.ex. le week-end), par le biais de machines inconnues, ou provenant d'un pays où aucun utilisateur n'est localisé.

4.5 Sensibilisation des utilisateurs

R12	Mettre en place un programme de sensibilisation des utilisateurs. Ce programme doit comporter une sensibilisation initiale des nouveaux utilisateurs et une sensibilisation continue et périodique de ceux déjà en fonction.

Les attaquants profitent très souvent d'un manque de vigilance d'un utilisateur (p.ex. ouverture d'une pièce jointe) pour s'introduire dans le réseau interne.

Il est donc crucial de s'assurer d'une sensibilisation régulière des utilisateurs, notamment en matière de comportements à adopter vis-à-vis des attaques de type « Phishing »[1] : comment les reconnaitre et comment réagir. Il devrait être également clair pour les utilisateurs comment et à qui rapporter tout incident de sécurité.

R13	Tester la vigilance des utilisateurs vis-à-vis des tentatives de « phishing ».

Des simulations d'attaque de type « Phishing », comprenant l'envoi d'un faux message « Phishing » aux utilisateurs, peuvent être réalisées afin de mesurer la vigilance des utilisateurs et promouvoir l'importance du respect des règles de sécurité.

4.6 Détection des comportements anormaux

R14	Mettre en place des mécanismes techniques et organisationnels de détection des comportements anormaux, sur base notamment de sondes IDS et/ou un SIEM.

Les équipements couverts par cette surveillance devraient notamment comprendre les équipements exposés sur Internet, les serveurs et applications critiques pour les activités ainsi que les serveurs de fichiers.

Les activités pouvant faire l'objet d'une surveillance particulière comprennent la création de nouveaux comptes utilisateurs, la modification de mots de passe utilisateurs ou de comptes systèmes et applicatifs, la création ou la modification de tâches planifiées, modification des droits d'accès, l'utilisation de comptes ou d'outils d'administration, en particulier en dehors des heures de travail habituelles.

R15	Recourir à un Centre des Opérations de Sécurité (ou « Security Operation Center ») externe, afin de s'assurer une surveillance en continue des événements de sécurité par du personnel qualifié.

4.7 Plan de réponse « rançongiciel »

R16	Préparer un plan de réponse « rançongiciel » et le tester régulièrement.

Ce plan comprendra notamment la réaction immédiate à adopter face à une attaque par rançongiciel, son confinement ainsi que le recouvrement des activités affectées.

Il devra comprendre également une description claire du processus de décision, l'utilisation possible de moyens de communication alternatifs (les postes de travails ou les e-mails pourraient ne plus fonctionner correctement) et les détails de contact des personnes clés.

Lorsqu'une attaque survient, des heures précieuses peuvent être perdues pour déterminer et obtenir les assistances dont l'organisation a besoin pour gérer cette attaque. Il peut s'agir d'assistance dans le domaine de la cybersécurité ou juridique. En dehors de toute attaque, il est donc recommandé d'identifier les entités en mesure de fournir ces assistances et de définir avec elles les modalités pratiques de leurs interventions ainsi que les procédures à appliquer.

[1] Des supports de sensibilisation et des recommandations de sécurité relatives au phishing/rançongiciels peuvent être fournis par l'ANSSI.

4.8 Plan de communication de crise

R17	Préparer un plan de communication de crise, couvrant la communication interne (p.ex. la direction, les employés et contractants) et externe (p.ex. autorités de régulation, actionnaires ou clients).

En général, il s'agit de déterminer les acteurs devant être informés ainsi que d'identifier les modalités pratiques de communication (notamment les délais et médias utilisés) par acteur identifié. Les réseaux sociaux ne devraient pas être oubliés.

Dans le cadre des attaques par rançongiciel, une attention particulière devrait être portée aux obligations en matière du Règlement Général sur la Protection des Données (concernant l'information des personnes concernées par une violation de données) et aux obligations vis-à-vis des autorités (p.ex. Haut-Commissariat à la protection nationale ou Institut Luxembourgeois de Régulation).

5 Prévention : recommandations complémentaires

5.1 Gestion des accès utilisateurs et d'administration

R18	Appliquer le principe du « Moindre privilège » dans la gestion des accès utilisateurs et d'administration.

R19	Ne pas attribuer les droits d'administrateur local aux utilisateurs.

R20	Limiter l'attribution et l'usage des comptes d'administrateur.

Les comptes d'administrateurs sont des cibles de choix pour les attaquants. Leur attribution devrait donc être limitée. De la même façon, les droits d'administrateur ne devraient pas être utilisés pour réaliser des actions qu'un compte utilisateur simple permet de faire (p.ex. consulter les e-mails ou surfer sur Internet).

R21	Réaliser des revues régulières des accès, afin de s'assurer que seulement les comptes utilisateurs du personnel sous contrat sont actifs, et que les comptes disposent des droits d'accès minimum requis pour accomplir leur mission.

5.1 Sécurité des équipements utilisateurs

R22	Installer des logiciels de sécurité des équipements utilisateurs (« Endpoint security ») pouvant comprendre un pare-feu, un antivirus et/ou des mécanismes techniques garantissant que seules des applications autorisées peuvent être téléchargées et/ou exécutées.

5.2 Sécurisation des e-mails

R23	Implémenter une solution technique performante permettant d'identifier et de bloquer les spams et tentatives de phishing.

R24	Alerter les utilisateurs lorsqu'un e-mail provient d'une source extérieure.

5.3 Cloisonnement des réseaux

R25	Mettre en place un cloisonnement adéquat du réseau en fonction de l'utilisation, de la criticité ou des risques.

Un réseau peut ainsi comprendre une zone ou sous-réseau pour les équipements utilisateurs, pour les postes de travail des administrateurs, pour les serveurs applicatifs ou pour les équipements exposés directement sur Internet. Un cloisonnement adapté pourra ainsi limiter la capacité des attaquants de se déplacer au sein du réseau interne.

Dans le cadre de la gestion de ces sous-réseaux, les segments internes devraient être considérés comme n'étant pas dignes de confiance. Des règles strictes de filtrage devraient être implémentées entre ces sous-réseaux.

R26	Mettre en place la séparation la plus hermétique possible entre le réseau de production, comprenant l'infrastructure critique permettant de fournir les services essentiels, et le reste du réseau. Les règles de maintenance du réseau de production devraient être plus strictes.

5.4 Filtrage des flux Internet

R27	Bloquer les flux à provenance ou à destination de sites de rançongiciels, à mauvaise réputation ou connus pour être malicieux.

R28	Mettre en place des mécanismes techniques et organisationnelles de détection d'exfiltration de données.

5.5 Journaux d'activités (« logs »)

R29	S'assurer que les équipements clés disposent de journaux d'activités activés et correctement configurés. Déterminer la durée de conservation de ces journaux d'activité sur base d'une analyse de « coût-bénéfices » et des réglementations en vigueur.

5.6 Protection des données sensibles

R30	En ligne avec les principes du règlement général sur la protection des données, appliquer le principe de minimisation dans le cadre de la gestion des données personnelles. Appliquer l'anonymisation ou la pseudonymisation des données lorsque cela est possible.

5.7 Relations avec les tiers et fournisseurs de services de confiance

R31	Renforcer la coopération en matière de sécurité de l'information avec les tiers et fournisseurs de services de confiance.

Des obligations contractuelles en matière de cybersécurité (p.ex. règles de sécurité à respecter, réaction à adopter en cas d'incident de sécurité, protection des données ou continuité des activités) peuvent ainsi être définies avec les tiers et fournisseurs de services de confiance. Leur niveau de maturité peut être aussi évalué (p.ex. en consultant leurs politiques de sécurité), des audits de sécurité peuvent être réalisés périodiquement ou des rapports indépendants d'évaluation de leur niveau de sécurité peuvent être obtenus.

6 Plan de réponse en cas d'attaque

6.1 Isolation des réseaux et équipements infectés

L'équipement infecté devrait être déconnecté en débranchant le câble réseau ou en désactivant l'interface wifi. Si plusieurs équipements d'un même réseau sont infectés, il faudra peut-être alors débrancher le réseau affecté. S'il est impossible de les isoler, il faudra alors éteindre les équipements infectés.

Les systèmes de sauvegarde des données devraient être déconnectés du système d'information (ou bloquer leur accès) afin de garantir au maximum leur intégrité. Les disques partagés contenant des données sensibles devraient être déconnectés ou désactivés afin de s'assurer que les données contenues ne soient pas corrompues.

6.2 Développement d'une compréhension de l'attaque

Des spécialistes de cyber sécurité internes et/ou externes qualifiés devraient intervenir afin de comprendre le plus rapidement possible l'attaque, et en particulier :

- Confirmer la réalité de l'attaque par un rançongiciel ;
- Identifier le type et le nombre d'équipements infectés ;
- Déterminer le type et la version du rançongiciel. Sur base de ces informations, des sites[1] peuvent fournir des explications sur le fonctionnement du rançongiciel, la façon de limiter ses impacts et même des outils permettant de déchiffrer les données affectées ;

[1] p.ex. le site « The No More Ransom Project »

- Comprendre quels supports de données sont visés par le rançongiciel. Il peut s'agir de disques partagés, de stockage réseau, de stockage en ligne et/ou « cloud », de stockages externes ou USB, etc. ;
- Comprendre si des données ont été exfiltrées. Une consultation des journaux d'activité (« logs ») peut permettre de déterminer si des scripts ont été exécutés pour copier, compresser ou transférer des données. Une analyse du volume de données transférées peut permettre, par comparaison avec une journée habituelle, de déterminer si un volume particulièrement massif de transfert a été réalisé ;
- Identifier le vecteur d'attaque utilisé ;
- Identifier et corriger les vulnérabilités exploitées.

6.3 Communication et partage d'information

Dans les meilleurs délais, et avec les moyens de communications disponibles, la direction, les supérieurs hiérarchiques et les utilisateurs devraient être alertés qu'une attaque est en cours. Le comportement attendu des utilisateurs devrait être également clairement communiqué.

Le plan de communication de crise devrait être exécuté.

Les indicateurs de compromission découverts ainsi que le *modus operandi* succinct de l'attaque devraient être partagés avec les partenaires (p.ex. GOVCERT.LU).

6.4 Réponse

Le paiement de la rançon ne devrait jamais être effectué. Il n'y a en effet aucune garantie que les données chiffrées puissent être restaurées sans être corrompues ou que les données exfiltrées ne soient utilisées ultérieurement pour réaliser d'autres actions criminelles. Payer la rançon encourage également la cybercriminalité et la recrudescence de ces attaques.

Il est important de porter plainte, si possible avec l'aide d'une assistance juridique. Dans tous les cas, les journaux d'activité des équipements clés, des images de systèmes infectés et des captures d'écrans des logiciels malveillants devraient être collectés et conservés.

6.5 Recouvrement

Si les sauvegardes n'ont pas été affectées et que l'intrusion est éradiquée, la restauration des informations supprimées ou corrompues peut être réalisée.

Les systèmes infectés devraient être reconstruits totalement, en effaçant les disques et dispositifs de stockage de tous les équipements connectés puis en procédant à une réinstallation complète sur base de sauvegardes saines.

Les systèmes devraient être rétablis en fonction des résultats des analyses d'impacts métiers (« Business Impact Analysis »).