RANSOMWARE TASK FORCE

Plan directeur de défense contre les rançongiciels

Plan de mesures d'atténuation, d'intervention et de récupération destinées aux PME victimes d'un rançongiciel

IST Institute for SECURITY + TECHNOLOGY

Auteurs principaux

Aaron McIntosh, directeur de la commercialisation des produits, ActZero
Valecia Stocchetti, ingénieure principale en cybersécurité, CIS

Collaborateurs

ActZero

Aaron McIntosh, directeur de la commercialisation des produits, ActZero

CIS Center for Internet Security®

Curt Dukes, premier vice-président, division des pratiques exemplaires en matière de sécurité, CIS
Phyllis Lee, directrice principale des contrôles, CIS
Valecia Stocchetti, ingénieure principale en cybersécurité, CIS
Brian de Vallance, conseiller principal, CIS

CYBER THREAT ALLIANCE

Michael Daniel, président de la Cyber Threat Alliance

GLOBAL CYBER ALLIANCE

Brian Cute, directeur, Programme de capacité et de résilience, Global Cyber Alliance
Leslie Daigle, directrice technique principale et directrice du programme d'intégrité de l'Internet, Global Cyber Alliance
Renee McLaughlin, responsable des produits, Programme des boîtes à outils, de la capacité et de la résilience, Global Cyber Alliance

Traduction fournie par le gouvernement du Canada
Translation provided by the Government of Canada
Canada

IST Institute for SECURITY + TECHNOLOGY

Megan Stifel, directrice principale de la stratégie, Institute for Security and Technology

resilience

Davis Hake, co-fondateur, Résilience

SecurityScorecard

Sachin Bansal, chef de la direction des opérations et des affaires juridiques, SecurityScorecard
Charlie Moskowitz, vice-président, Politique et affaires gouvernementales, SecurityScorecard

VENABLE LLP

John Banghart, directeur principal des services de cybersécurité, Venable LLP

Table des matières

Résumé

Selon la U.S. Small Business Administration, les États-Unis comptent 32 540 953 millions de petites entreprises, soit 99,9 p. cent de l'ensemble des entreprises de ce pays.[1] À l'heure actuelle, la plupart d'entre elles ne sont toujours pas suffisamment préparées pour faire face à une cyberattaque. Par exemple, l'étude d'Accenture en 2019 sur le coût de la cybercriminalité révèle que « 43 p. cent des cyberattaques visent les petites entreprises, mais que ces dernières ne sont que 14 p. cent à pouvoir s'en protéger »[2]. Pour contrer un tel risque, un nombre croissant de petites et moyennes entreprises (PME) souscrivent une cyberassurance. Cependant, les assureurs exigent de plus en plus qu'elles comprennent bien les pratiques de gestion des risques en matière de cybersécurité et qu'elles les appliquent pour être admissibles.

C'est dans ce contexte que nous recommandons aux PME d'adopter un cadre de cybersécurité qui inclut des pratiques exemplaires spécifiques pour se protéger des rançongiciels. L'adoption et l'application rigoureuse d'un tel cadre peuvent les aider à renforcer leurs mécanismes de défense. En revanche, il leur est difficile de savoir par où commencer, et la façon d'établir l'ordre de priorité des efforts en matière de cybersécurité échappe à bon nombre d'entre elles. C'est pourquoi nous devions rédiger le présent cadre en termes clairs, avec des conseils pratiques et faciles à assimiler. Malheureusement, certaines PME s'estiment incapables de mettre en œuvre certains cadres de cybersécurité et d'en atteindre les objectifs, les forçant à abandonner des occasions d'affaires pour des questions de conformité. Cette pratique les enferme dans un cycle perpétuel de préparation inefficace en matière de cybersécurité.

En réponse à la mesure 3.1.1 du rapport du Groupe de travail sur la lutte contre les rançongiciels (GTLR), qui recommande à la communauté de la cybersécurité d'« élaborer un cadre clair de mesures exécutables d'atténuation, d'intervention et de récupération relatives aux rançongiciels », le Groupe de travail sur le Plan directeur de défense contre les rançongiciels a intégré au présent document un sous-ensemble structuré de mesures de protection essentielles en matière de cyberhygiène[3], puisées dans le site Web Contrôles de sécurité essentiels du Center for Internet Security® (contrôles du CIS®) v8. Ces mesures de protection forment une norme minimale de sécurité de l'information que doivent appliquer toutes les entreprises pour se défendre contre les attaques les plus courantes. Le présent Plan directeur de défense contre les rançongiciels constitue un ensemble de mesures de protection fondamentales et exécutables destiné aux petites et moyennes entreprises[4] (PME).

Par conséquent, le présent plan directeur reprend les contrôles du CIS, un ensemble prescriptif de mesures classées par ordre de priorité et élaborées par une communauté mondiale d'experts du domaine de la cybersécurité. Les quarante (40) mesures de protection recommandées dans le plan directeur ont été retenues parce qu'elles sont faciles à mettre en œuvre et s'avèrent efficaces pour se défendre des attaques par rançongiciel. L'analyse du Modèle de défense de la communauté (MDC) 2.0 du CIS le confirme : l'application des mesures de protection présentées ici permet de se protéger contre plus de 70 p cent[5] des techniques d'attaque associées aux rançongiciels. Il faut souligner que le plan ne doit pas servir de guide de mise en œuvre, mais plutôt être vu comme une source de mesures défensives recommandées à prendre pour se protéger contre les rançongiciels et d'autres cyberattaques courantes et savoir comment intervenir dans de telles situations. L'annexe C du présent document et celui-ci proposent plusieurs outils et ressources pour faciliter la mise en œuvre de ces mesures de protection.

1 FAQ à l'intention des PME, U.S. Small Business Advisory Office of Advocacy, décembre 2021. https://cdn.advocacy.sba.gov/wp-content/uploads/2021/12/06095731/Small-Business-FAQ-Revised-December-2021.pdf.

2 Accenture, Ninth Annual Cost of Cybersecurity, mars 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.

3 Une cyberhygiène essentielle repose sur des mesures de protection du groupe de mise en œuvre 1 (IG-1) des contrôles de sécurité critiques (CSC) du Center for Internet Security (CIS).

4 Les entreprises comprennent à la fois les commerces et les organisations gouvernementales.

5 Tel que présenté dans le Modèle de défense de la communauté (MDC) 2.0 du CIS.

Public cible

Le GTLR a conçu le présent plan directeur dans le but exprès d'éliminer un obstacle majeur qui empêche les PME de se protéger des rançongiciels en raison de leur expertise limitée en matière de cybersécurité. Il est rédigé en termes simples et décrit le fonctionnement des mesures de protection recommandées pour atténuer les risques associés aux rançongiciels. Il contient de l'information utile destinée aux chefs d'entreprise et à leur personnel technique qui doivent chercher ensemble à comprendre ces risques et à établir l'ordre de priorité des mesures.

Introduction

Le GTLR a sollicité la communauté de la cybersécurité pour qu'elle « élabore un cadre clair de mesures exécutables d'atténuation, d'intervention et de récupération relatives aux rançongiciels ». Le présent plan directeur s'appuie sur les contrôles du CIS, un ensemble de pratiques exemplaires très répandues qui aident les entreprises à concentrer leurs ressources sur les mesures critiques nécessaires pour se défendre contre les attaques cybernétiques les plus courantes. Le plan comprend un sous-ensemble de ces pratiques exemplaires, ou mesures de protection, les plus pertinentes pour lutter contre les rançongiciels.[6]

Le CIS a conçu les mesures de protection choisies pour les PME dont le service de la technologie de l'information (TI) emploie une petite équipe sans grande expérience de la cybersécurité et dont le travail se limite habituellement à protéger l'organisation contre des cyberattaques générales, c'est-à-dire qui ne ciblent pas celle-ci en particulier. Ces mesures de protection assurent une cyberhygiène essentielle sous la forme de contrôles et de capacités fondamentales de protection nécessaires à la mise en œuvre de capacités plus avancées. Une lutte efficace contre les rançongiciels requiert une planification et des préparatifs. À l'instar d'un édifice ou d'un exercice d'incendie, plus les assises et le plan sont solides, plus l'entreprise a de chances de résister à une attaque de cybersécurité fulgurante et imprévue qui peut interrompre brutalement les activités d'une organisation mal préparée.

Pour aider les entreprises à mieux établir l'ordre de priorité de ses préparatifs, le présent plan directeur définit deux types de mesures de protection : fondamentales et exécutables. Les mesures fondamentales forment l'ensemble de pratiques en matière de cybersécurité qu'une entreprise doit appliquer avant d'intervenir de quelque manière que ce soit. Les mesures exécutables viennent compléter ces mesures fondamentales pour renforcer sa posture de cybersécurité.

Nous encourageons les PME à prendre le plus grand nombre de mesures de protection possible, en sachant très bien que certaines ne pourront toutes les appliquer. Bien que le GTLR recommande la mise en œuvre intégrale des mesures de protection indiquées dans son plan directeur, l'application d'une seule mesure constitue un important pas dans la bonne direction pour améliorer la cybersécurité. En effet, le but n'est pas d'atteindre la perfection. Si la plupart des PME mettent en œuvre ces contrôles, notre communauté d'entreprises sera plus résiliente et plus sûre sur le plan cybernétique.

Comment utiliser le plan directeur

Le présent plan directeur doit servir de point de départ de l'entreprise pour établir l'ordre de priorité de ses mécanismes de défense en matière de cybersécurité. L'annexe A dresse la liste exhaustive des mesures de protection contre les rançongiciels. Plusieurs outils et ressources figurant à l'annexe C , ainsi que le cahier de scénarios qui s'y rapporte, sont disponibles pour faciliter la mise en œuvre de ces mesures. Le Groupe de travail sur le Plan directeur de lutte contre les rançongiciels n'endosse d'aucune façon les outils ou les solutions qu'il a choisi d'inclure dans le document d'accompagnement, et ne garantit pas non plus qu'ils amélioreront la protection contre les rançongiciels parce qu'il en fait mention.

6 Ces pratiques sont tirées du groupe de mise en œuvre 1 (IG-1) de la version 8 des contrôles du CIS.

Reconnaissance du risque

Le présent plan directeur met fortement l'accent sur la mise en œuvre de mesures de protection et sur le renforcement de la capacité à mettre en œuvre des moyens plus avancés. Après analyse, une cyberhygiène essentielle protège contre plus de 70 p. cent[7] des techniques d'attaque associées aux rançongiciels, mais son efficacité dépend en fin compte de la rigueur avec laquelle elle est pratiquée et du niveau de détermination des attaquants.

Comme nous le verrons plus loin, la pratique d'une cyberhygiène essentielle est la norme minimale que doivent appliquer les entreprises pour assurer la sécurité de leur information et sert de tremplin vers la mise en œuvre d'autres contrôles du CIS. Le présent plan directeur est ce que toute entreprise doit suivre pour se défendre contre les attaques les plus courantes. Les PME peuvent juger nécessaire de mettre en œuvre d'autres mesures de protection pour se défendre contre des attaques plus sophistiquées.

Plan d'action

Pour se défendre contre les rançongiciels, les PME doivent adopter une approche par couches qui protège leurs biens les plus essentiels. Cela nécessite la mise en œuvre de contrôles dans divers domaines, comme la gestion des stocks d'équipements informatiques et de logiciels, la gestion des vulnérabilités, la défense contre les logiciels malveillants, la formation du personnel, la récupération des données et les interventions en cas d'incident. Les rançongiciels évoluant sans cesse, les cybercriminels conçoivent de nouveaux stratagèmes, comme l'extorsion où l'attaquant exfiltre les données avant de les chiffrer, et exigent ensuite de l'argent à la victime pour que ses données ne soient pas rendues publiques. En mettant en œuvre les mesures de protection du présent plan directeur, les PME sont en meilleure posture pour se défendre contre les rançongiciels et d'autres types d'attaques.

Les paragraphes suivants décrivent les mesures de protection fondamentales et exécutables pour se protéger des rançongiciels, tout en montrant leur importance. Les utilisateurs du plan directeur doivent se concentrer d'abord sur la mise en œuvre des mesures de protection fondamentales, puis porter leur attention sur les mesures exécutables (c'est-à-dire plus techniques).

Harmonisation avec les fonctions définies par le Cadre de cybersécurité du NIST

Puisqu'il est largement accepté au sein des administrations publiques, des entreprises et des communautés de la cybersécurité, le Groupe de travail sur le Plan directeur de défense contre les rançongiciels a harmonisé le sous-ensemble de mesures de protection avec les cinq fonctions du cadre de cybersécurité (CCS) du National Institute of Standards and Technology (NIST), soit l'identification, la protection, la détection, l'intervention et la récupération. Ces fonctions facilitent la mise en place de programmes de cybersécurité efficaces. Regrouper les mesures de protection selon ces fonctions aide les PME à mieux comprendre les risques auxquels elles sont exposées, les mesures à prendre pour s'en protéger, les outils à leur disposition pour les détecter, et les solutions disponibles pour contenir les menaces et y remédier le plus rapidement possible.

En raison de leur nature technique complexe, les mesures de protection associées à la détection ont été exclues du présent plan directeur. Toutefois, le GTLR recommande vivement aux PME qui appliquent le plan directeur de recourir au besoin à un prestataire de services de cybersécurité pour mettre en œuvre des contrôles de détection ou tout autre contrôle pour lequel elles ont besoin d'une assistance.

7 Tel que présenté dans le Modèle de défense de la communauté (MDC) 2.0 du CIS.

Vue d'ensemble des mesures de protection

Le plan directeur comporte 40 mesures de protection en tout, soit 14 fondamentales et 26 exécutables. Il regroupe d'abord ces mesures selon les fonctions du CCS du NIST. Pour chaque fonction, il présente les mesures par ordre de priorité selon leur efficacité à combattre les rançongiciels et la posture générale de défense de la cybersécurité qu'elles procurent.[8]

MESURES DE PROTECTION FONDAMENTALES

Les mesures de protection fondamentales sont autant de pierre d'assise sur lesquelles repose l'établissement d'un programme de cybersécurité au sein d'une entreprise. Elles permettent également la mise en œuvre de mesures de protection exécutables. 14 mesures fondamentales ont été sélectionnées et classées par ordre de priorité dans le plan directeur, comme il est décrit ci-après.

Identification

Pour assurer la défense du réseau, il faut d'abord savoir ce qui s'y trouve, c'est-à-dire les technologies employées et la nature de l'information stockée ou communiquée. Les mesures de protection fondamentales relatives à l'identification requièrent des PME qu'elles établissent et tiennent à jour un inventaire de leurs équipements informatiques et de leurs logiciels pour mieux gérer tous les appareils connectés, et qu'elles instaurent des processus de gestion des données qui décrivent clairement la façon de recueillir, d'utiliser et de conserver les données. Les activités d'identification incluent également l'établissement et la tenue à jour d'un inventaire des comptes d'utilisateur, ordinaires ou assortis de privilèges élevés.

Ces mesures de protection s'avèrent indispensables pour se protéger d'un rançongiciel et y réagir. L'entreprise peut difficilement se défendre si elle ne sait pas quels équipements informatiques, logiciels ou comptes d'utilisateur sont présents sur son réseau. Par exemple, il est plus facile pour un pirate informatique de compromettre et d'exploiter un appareil qui n'est pas ainsi répertorié. L'entreprise fait alors face à un risque plus élevé et peut subir d'autres attaques ou voir se prolonger l'attaque en cours. Une bonne connaissance de son environnement informatique est propice à la pratique d'une cyberhygiène essentielle au niveau de chaque appareil.

Mesures de protection

- Mettre en place et tenir à jour un inventaire détaillé des équipements informatiques de l'entreprise.
- Mettre en place et tenir à jour un inventaire des logiciels.
- Mettre en place et maintenir un processus de gestion des données.
- Mettre en place et tenir à jour un inventaire des comptes d'utilisateur.

Bien que la gestion de ces mesures de protection s'avère complexe en raison des nouveaux équipements informatiques et logiciels qui s'ajoutent sans cesse au réseau, elles sont fondamentales pour assurer une défense efficace et jouent un rôle essentiel dans d'autres activités défensives, comme la sauvegarde de l'information et l'intervention en cas d'incident. De plus, les données ne sont plus confinées à l'intérieur des murs de l'entreprise. En effet, les appareils mobiles et portatifs se connectent aux ressources de cette dernière, ce qui complique la gestion des données en l'absence de mesures de protection appropriées.

Protection

Une fois qu'une PME sait ce qui se trouve sur son réseau, l'étape suivante consiste à mettre en œuvre des mesures pour protéger ses biens, ses données et ses utilisateurs contre des acteurs malveillants qui cherchent à leur nuire.

Configurations sécurisées

8 Le GTLR s'est appuyé sur l'analyse du cadre Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) de la société MITRE, réalisée par le CIS et présentée dans le Modèle de défense de la communauté 2.0 du CIS pour établir cet ordre de priorité.

Les processus de gestion de la configuration sont importants pour assurer la sécurité et la maintenir au fil du temps. Les présentes mesures de protection sont axées sur la disposition des appareils connectés au réseau et de celui-ci dans son ensemble, et s'arriment également à des règles de fonctionnement qui leur sont appliquées. L'ensemble de ces règles forme ce qu'on appelle une configuration. Les mesures axées sur la protection de la configuration comprennent la mise en œuvre de processus de configuration sécurisés des équipements informatiques de l'entreprise, comme les ordinateurs portatifs et de bureau, les serveurs et les appareils mobiles, pour ne nommer que ceux-là. Un processus pour configurer l'infrastructure du réseau, y compris divers dispositifs comme les pare-feu, les routeurs et les commutateurs, est également important. L'ajout d'équipements informatiques, de logiciels, de comptes d'utilisateur, etc., peut accroître les risques s'il n'y a pas de processus rigoureux en place pour assurer l'application répétée des contrôles de sécurité appropriés. Par exemple, une mise à jour logicielle peut modifier un paramètre de configuration et le rendre moins sûr. L'entreprise doit avoir en place un processus de configuration sécurisé pour remédier à une « dérive » progressive de la sécurité, c'est-à-dire vérifier que ses biens sont conformes aux configurations et aux politiques établies et, dans le cas contraire, rétablir leur conformité.

Gestion des comptes et de l'accès

S'ils sont assortis de privilèges élevés, les comptes d'utilisateur donnent accès à un large éventail de fonctions de base, comme le courrier électronique, ou encore à presque tout dans l'entreprise. Les mesures de protection fondamentales requièrent de l'entreprise qu'elle établisse un processus d'autorisation et de révocation de l'accès à ses systèmes. Autre point crucial : elle doit également appliquer le principe du moindre privilège, c'est-à-dire n'accorder à chaque utilisateur que les seuls accès dont il a besoin pour accomplir une tâche. Cette obligation demeure lorsqu'un membre du personnel change de rôle ou a besoin d'une autorisation, permanente ou temporaire, pour participer à un projet, ou encore lorsqu'il se joint à l'entreprise ou qu'il la quitte.

Processus de gestion des vulnérabilités

Les chercheurs et d'autres intervenants en sécurité relèvent et publient annuellement plus de 18 000 vulnérabilités logicielles. Bien qu'il y en aura toujours d'autres qui échapperont à la vigilance de cette communauté, les acteurs malveillants exploitent habituellement les vulnérabilités connues en premier. La gestion des vulnérabilités joue donc un rôle essentiel dans la protection de l'infrastructure de l'entreprise. Le présent plan directeur recommande deux mesures de protection à prendre au moment de mettre en œuvre des processus de gestion des vulnérabilités et d'atténuation des risques. Ces mesures incluent le déploiement de correctifs au niveau des systèmes d'exploitation et des applications. Cela concerne autant les équipements informatiques et les logiciels que les dispositifs de réseau qui permettent de les gérer et de les surveiller.

Sensibilisation à la sécurité et formation

Il est important d'investir dans la technologie, mais le personnel constitue une ressource essentielle pour bien se protéger des rançongiciels et d'autres attaques informatiques. Selon le rapport Verizon Data Breach Investigations Report (DBIR) de 2021[9], 85 p. cent des atteintes à la protection des données comportent un élément humain. Le plan directeur stipule que les PME doivent mettre en place et maintenir un programme de sensibilisation à la sécurité à l'intention de tout leur personnel, de leurs partenaires et des utilisateurs tiers. Un tel programme a non seulement pour but de former les membres du personnel à employer le réseau et les systèmes de l'entreprise en toute sécurité, mais également de s'assurer qu'ils comprennent l'importance d'agir ainsi et le rôle qu'ils jouent dans sa protection.

Mesures de protection

- Mettre en place et maintenir un processus de configuration sécurisé.
- Mettre en place et maintenir un processus de configuration sécurisé de l'infrastructure du réseau.
- Mettre en place un processus d'autorisation de l'accès.
- Mettre en place un processus de révocation de l'accès.

9 *Verizon Data Breach Investigations Report*, 2021. https://www.verizon.com/business/resources/reports/dbir/.

» Mettre en place et maintenir un processus de gestion des vulnérabilités.

» Mettre en place et maintenir un processus d'atténuation des risques.

» Mettre en place et maintenir un programme de sensibilisation à la sécurité.

Intervention

Une bonne préparation est essentielle pour faire face aux incidents. L'entreprise saura ce qu'elle doit faire si elle dispose déjà d'un plan avant même qu'une attaque informatique ne survienne. Les mesures d'intervention permettent d'accélérer la reprise des activités interrompues parce qu'un attaquant a réussi à les perturber et que les contrôles en place n'ont pu l'en empêcher.

Ces mesures stipulent que l'entreprise doit mettre en place des processus de signalement des incidents et de gestion des journaux de sécurité. Les PME doivent au moins disposer d'un processus que le personnel suit pour rendre compte d'un incident de sécurité. Ce processus précise les délais à respecter, le nom de la personne à qui signaler l'incident, la façon de le signaler et les renseignements à fournir dans le signalement. Une entreprise qui a mis en place de telles mesures peut reprendre rapidement ses activités et limiter la durée de leur interruption, la perte de revenus et les dommages à sa réputation. Elle doit tenir périodiquement des exercices impromptus, prévus dans le plan d'intervention en cas d'incident, pour obtenir les meilleurs résultats en situation réelle.

La journalisation est également essentielle pour que l'entreprise puisse réagir adéquatement à un incident. La première étape de la gestion des journaux consiste à établir un processus. Celui-ci permet à l'organisation de savoir quels journaux recueillir en premier, la fréquence à laquelle les examiner et la durée de leur conservation. Une entreprise compromise aura besoin de ces journaux pour intervenir, déterminer la source de l'attaque ou fournir des preuves à des fins judiciaires.

Mesures de protection

» Mettre en place et maintenir un processus intégré de signalement des incidents.

» Mettre en place et maintenir un processus de gestion des journaux de vérification.

Récupération

La perte de données essentielles au fonctionnement des PME est l'un des préjudices les plus graves causés par les rançongiciels. Le présent plan directeur comporte une mesure de protection fondamentale que les PME doivent prendre pour mettre en place et maintenir un processus de récupération des données dans le cadre de la planification des interventions et du rétablissement des activités. Les nouvelles techniques utilisées dans le domaine des rançongiciels (par exemple, l'extorsion) créent des difficultés à l'entreprise dont les contrôles récupèrent efficacement les données, mais qui s'avèrent déficientes pour les protéger. Elle doit pouvoir compter sur des contrôles pareillement efficaces pour reprendre normalement ses activités si elle est victime d'un rançongiciel.

Mesure de protection

» Mettre en place et maintenir un processus de récupération des données.

MESURES DE PROTECTION EXÉCUTABLES

Les mesures de protection fondamentales pour profiter d'une sécurité efficace à long terme ne suffisent pas. Il faut aussi adopter d'autres mesures. Les 26 mesures de protection exécutables sélectionnées et priorisées dans le plan directeur permettent à l'entreprise d'améliorer sa sécurité et de se défendre contre les rançongiciels et d'autres formes génériques d'attaques qui ne ciblent aucune victime en particulier. Elles complètent les mesures fondamentales et consistent à appliquer les contrôles techniques nécessaires pour protéger l'environnement de l'entreprise.

Identification

Outre les mesures de protection fondamentales relatives à l'identification qui permettent aux PME de répertorier les appareils et de déterminer la nature des données dans leur environnement, le plan directeur fait état de mesures d'identification exécutables à prendre pour s'assurer que l'entreprise emploie toujours les logiciels autorisés les plus récents avec l'ensemble de ses biens. Les cybercriminels parcourent sans arrêt les réseaux pour exploiter les versions vulnérables des logiciels. Ces vulnérabilités logicielles demeurent l'un des principaux vecteurs d'attaque des rançongiciels. Pour réduire le risque qu'elles soient exploitées, il faut donc tenir les logiciels à jour et vérifier fréquemment leur inventaire.

Mesure de protection

» S'assurer que les logiciels autorisés sont actuellement pris en charge.

Protection

Près de 70 p. cent des mesures exécutables du plan directeur ont trait à la protection. Celle-ci est essentielle, puisqu'elle a pour but de limiter ou de contenir les répercussions d'un possible incident lié à la cybersécurité. Les mesures de protection recommandées sont techniques et comportent un volet de formation. Les mesures techniques comprennent notamment la mise en œuvre et la gestion de pare-feu au niveau des serveurs de l'organisation, la gestion de la sécurité de ses supports amovibles, ainsi que le déploiement et la gestion de logiciels antimaliciels. Les mesures liées à la formation portent sur les moyens de reconnaître et de signaler une attaque lorsqu'elle survient.

Configurations sécurisées

Les rançongiciels exploitent divers vecteurs d'infection initiaux, mais trois d'entre eux appuient leurs tentatives de s'introduire dans un réseau ou un système : le protocole RDP (Remote Desktop Protocol) employé dans la gestion des appareils Windows à distance, l'hameçonnage, c'est-à-dire l'envoi de courriels malveillants dont l'origine semble fiable, mais qui en réalité ont pour but de voler des identifiants ou des données sensibles, et enfin l'exploitation des vulnérabilités logicielles. Le renforcement de la sécurité des équipements informatiques, des logiciels et des composants de réseau permet de se défendre contre ces principaux vecteurs d'attaque et de combler les lacunes en matière de sécurité qui peuvent résulter de configurations par défaut non sécurisées. Les comptes créés par défaut qui ne sont pas désactivés ou fermés, les mots de passe par défaut qui ne sont pas changés et tout autre paramètre vulnérable laissé tel quel concourent tous à faciliter l'exploitation des vulnérabilités. Les mesures exécutables ayant trait à la protection consistent à installer et à gérer un pare-feu sur chaque serveur et à gérer les comptes par défaut sur les réseaux et systèmes de l'entreprise.

Il est également recommandé d'employer des pratiques exemplaires (p. ex., celles des guides CIS Benchmarks™, Defense Information Systems Agency Security Technical Implementation Guides [DISA STIGs]) pour sécuriser un système au moment de le configurer.

Gestion des comptes et des accès

Dès qu'un pirate obtient les identifiants associés à un compte d'utilisateur, surtout s'il est assorti de privilèges élevés, les dommages qu'il peut causer s'aggravent considérablement. Non seulement a-t-il réussi à pénétrer dans le réseau de l'entreprise, mais il peut également s'y déplacer pour compromettre les comptes et les systèmes à proximité. Le plan directeur recommande diverses mesures pour réduire le risque de compromission d'un compte, notamment l'évaluation périodique des droits d'accès privilégiés, la fermeture des comptes inactifs, une gestion efficace des mots de passe pour éviter qu'ils ne soient réutilisés et la mise en place de l'authentification multifactorielle (AMF) dans tous les systèmes de l'entreprise. L'activation de l'AMF est particulièrement importante puisqu'elle ajoute une couche de sécurité en cas de compromission des mots de passe. La gestion des comptes et des accès s'applique également aux plateformes infonuagiques, en particulier aux services de courrier électronique dans le nuage qui peuvent se connecter à d'autres ressources de l'entreprise.

Planification de la gestion des vulnérabilités

Les rançongiciels continuent de s'attaquer aux entreprises dont la direction n'applique pas en temps opportun les correctifs de vulnérabilités connues. Plusieurs rapports publics montrent que les attaquants exploitent à la fois les vulnérabilités récemment découvertes et celles qui remontent à plusieurs années. Le plan directeur recommande plusieurs mesures de protection contre les vulnérabilités, notamment mieux gérer les correctifs et s'assurer que les réseaux et les dispositifs utilisent les versions les plus récentes de leur système. La gestion des vulnérabilités s'avère particulièrement importante avec les systèmes en place qui pourraient exécuter des logiciels désuets dont le fournisseur n'assure plus le soutien technique, les rendant ainsi vulnérables aux attaques. Si un tel système ne peut être mis à jour, il faut mettre en œuvre d'autres contrôles pour le protéger adéquatement, ou encore trouver une solution de rechange.

Les entreprises doivent envisager d'automatiser l'application des correctifs des systèmes d'exploitation comme Microsoft® Windows® et Apple® MacOS®. Sans un tel mécanisme, les entreprises elles-mêmes, ou leurs partenaires spécialisés dans la sécurité, doivent porter une attention particulière aux vulnérabilités critiques ou du jour zéro dont font état les notifications et les mises à jour de sécurité des différents fournisseurs, pour ensuite appliquer à la hâte ces correctifs.

Défenses contre les logiciels malveillants

Les rançongiciels peuvent s'introduire de différentes manières dans les systèmes, notamment par l'intermédiaire d'un lien ou d'une pièce jointe dans un courriel, d'un navigateur Web ou d'un support de données amovible. Le plan directeur prévoit diverses mesures de protection contre les logiciels malveillants, dont le déploiement de programmes antimaliciels pour bloquer les attaques ciblant les biens, tenir ces programmes à jour et en télécharger les signatures. Il est tout aussi important d'utiliser les versions les plus récentes des navigateurs et des systèmes de messagerie client pour les empêcher de servir de porte d'entrée à du code d'exploitation. Les supports amovibles, les clés USB par exemple, présentent également un risque à ce titre. Ces supports sont parfois dotés d'une fonction d'exécution ou de lecture automatique du contenu lorsqu'ils sont connectés à un système, directement ou non. S'ils contiennent un maliciel, ils infectent ce système et ceux qui se trouvent à proximité. La désactivation de cette fonction réduit le risque de compromission.

Les adresses URL (Uniform Resource Locator) malveillantes constituent un autre vecteur d'attaque par rançongiciel très répandu. Elles se transmettent par courriel ou directement au moyen d'un navigateur Web. Quelle que soit l'origine des URL, l'application de contrôles comme le filtrage par DNS (système de noms de domaine) peut bloquer le téléchargement de maliciels dans le système d'une victime ou empêcher un utilisateur de voir une page d'hameçonnage conçue pour l'inciter à transmettre ses identifiants à un pirate ou à télécharger un fichier malveillant. De nombreux services de filtrage par DNS sont gratuits et constituent un moyen rapide et facile de réduire les risques de compromission de l'entreprise.

Sensibilisation à la sécurité et formation

Il est essentiel de combler les lacunes au sein de l'organisation, dont l'absence de formation en matière de cybersécurité. La prolifération de l'hameçonnage par courriel ou par texto, c'est-à-dire l'envoi de messages texte incitant le destinataire à divulguer ses informations personnelles ou à télécharger des applications malveillantes, ne montrant aucun signe d'essoufflement, le présent plan directeur recommande aux PME de former leur personnel à reconnaître le piratage psychologique et à signaler les incidents de sécurité.

La sensibilisation du personnel au piratage psychologique est essentielle à l'établissement des défenses d'un réseau. Les outils technologiques ou autres mis en place pour contrer l'hameçonnage ne pouvant protéger parfaitement l'entreprise, la défense de première ligne du réseau incombe donc au personnel.

La formation sur le signalement des incidents de sécurité est tout aussi importante. Quel que soit le type d'attaque, il est crucial de réagir dans les meilleurs délais. Le signalement rapide d'un tel événement, suivi d'une mesure prise tout aussi rapidement, peut y mettre fin, stopper les dommages ou en limiter l'étendue. La formation est essentielle pour s'assurer que le personnel comprend ce qu'il doit faire et comment le faire.

Mesures de protection

- Gérer les comptes par défaut liés aux équipements informatiques et aux logiciels de l'entreprise.
- Utiliser des mots de passe uniques.
- Fermer les comptes inactifs.
- Restreindre les privilèges d'administrateur aux seuls comptes réservés à cette fonction.
- Imposer l'AMF avec les applications accessibles de l'extérieur.
- Imposer l'AMF avec l'accès au réseau à distance.
- Imposer l'AMF avec l'accès d'administrateur.
- Automatiser la gestion des correctifs des systèmes d'exploitation.
- Automatiser la gestion des correctifs des applications.
- N'autoriser que les navigateurs et les clients de messagerie entièrement pris en charge.
- Utiliser des services de filtrage par DNS.
- Maintenir systématiquement à jour l'infrastructure du réseau.
- Déployer des programmes antimaliciels et en assurer la maintenance.
- Configurer le téléchargement automatisé des signatures antimaliciels.
- Désactiver la fonction d'exécution et de lecture automatique des supports amovibles.
- Former les membres du personnel à reconnaître le piratage psychologique.
- Former les membres du personnel à reconnaître et à signaler les incidents de sécurité.

Intervention

Malheureusement, même les meilleures protections ne parviennent pas toujours à arrêter un adversaire bien décidé à investir le temps et les efforts nécessaires pour perturber les opérations d'une entreprise. Les mesures d'intervention exécutables incluent signaler les incidents, établir une liste de personnes-ressources principales, déterminer la façon et le moment de les solliciter, ainsi que suivre la procédure et employer les outils nécessaires pour recueillir et conserver adéquatement les divers journaux d'événements.

Il est plus facile de coordonner les interventions dans la foulée d'un incident si l'on désigne au moins une personne pour en gérer le traitement. Il peut s'agir d'un membre du personnel ou d'un fournisseur, ou encore d'une équipe formée des deux. Créer une liste de personnes-ressources à mettre au courant lorsque survient un incident s'avère utile pour que l'entreprise soit déjà prête à intervenir. Elle peut désigner ces personnes au sein de son personnel, ou encore s'adresser à un service de police, à son assureur, à un organisme gouvernemental, à un cabinet d'avocats ou à d'autres intervenants. La communication est essentielle lorsqu'un incident se produit, puisqu'il y a beaucoup de choses à gérer.

La collecte des journaux de vérification avant un incident est également importante. On les retrouve notamment au niveau du système d'exploitation, de l'application ou d'un périphérique de réseau. Lorsqu'un incident se produit, les journaux s'avèrent souvent très utiles pour l'analyser et reconstituer ce qui s'est passé. Plus important encore, cette analyse peut servir à mettre en place des mesures d'atténuation pour éviter que le scénario ne se répète. Il faut aussi veiller à ce que le stockage des journaux soit adéquat, puisque ces fichiers peuvent encombrer rapidement cet espace dans un système et rendre ce dernier moins performant.

Mesures de protection

- Désigner le personnel chargé de gérer le traitement des incidents.
- Dresser et tenir à jour une liste de personnes-ressources auxquelles signaler les incidents de sécurité.
- Recueillir les journaux de vérification.
- Prévoir un espace de stockage adéquat pour les journaux de vérification.

Récupération

La sauvegarde des données essentielles constitue l'une des stratégies les plus efficaces pour les récupérer à la suite d'une attaque par rançongiciel. Le plan directeur précise différentes mesures de protection exécutables à prendre pour ce faire, dont la sauvegarde et la restauration. Automatiser la sauvegarde des données, les protéger et veiller à ce qu'elles ne soient pas accessibles régulièrement sur le réseau sont toutes des mesures essentielles qui permettent à l'organisation victime d'un rançongiciel de récupérer son information. La dernière mesure est particulièrement importante. En effet, il ne sert à rien de mettre en œuvre tous les contrôles nécessaires pour protéger les données de sauvegarde si elles sont stockées directement dans le système ou sur le réseau ciblé par une demande de rançon, puisqu'elles sont chiffrées elles aussi par l'attaquant.

Mesures de protection

- Automatiser la sauvegarde des données.
- Protéger les données de récupération.
- Créer et maintenir une instance isolée des données de récupération.

Plan directeur pour une meilleure cyberassurance

Le Groupe de travail sur la lutte contre les rançongiciels (GTLR) estime qu'en 2021, les victimes de rançongiciels se sont fait extorquer 602 millions de dollars, soit une augmentation de 70 p. cent par rapport à l'année précédente. Les incidents liés aux rançongiciels ont représenté 79 p. cent des demandes d'indemnisation liées aux interruptions des activités[10], entraînant une hausse des primes d'assurance de plus de 90 p cent d'une année à l'autre.[11] Cette situation est intenable pour les assurés et le marché, et c'est en partie la raison pour laquelle de nombreux fournisseurs de cyberassurances se sont empressés d'appuyer le travail du GTLR.

Lancée voilà 20 ans pour couvrir les risques d'atteintes à la protection des données des entreprises, la cyberassurance a évolué de manière spectaculaire au cours de la dernière décennie, pour devenir un outil essentiel pour assurer la gestion de tels risques à l'interne. Des mesures de protection qualifiées de fondamentales ou d'exécutables sont décrites dans le présent plan directeur. Les PME peuvent s'adresser à leur cyberassureur pour obtenir de l'aide et des conseils sur l'application de bon nombre de ces mesures. La plupart des cyberassureurs proposent des primes proactives à faible taux qui réduisent substantiellement le coût et la complexité de la mise en œuvre d'un grand nombre des mesures présentées ici. Toutefois, le bond spectaculaire observé au niveau de l'efficacité et de l'étendue des attaques par rançongiciel complique le travail des assureurs et d'autres intervenants qui quantifient la responsabilité légale en s'appuyant sur des atteintes à la protection des données à grande échelle.

Le Plan directeur de défense contre les rançongiciels fournit deux éléments essentiels de la lutte du secteur de la cyberassurance contre la multiplication des attaques criminelles par rançongiciel.

- Il constitue avant tout un guide pratique, fondé sur des données et conçu spécifiquement pour les PME qui ont souvent le plus de mal à défendre leurs systèmes. S'i l'on commence avec les mesures de protection du groupe de mise en œuvre 1 (IG-1) des contrôles de sécurité critiques (CSC) du Center for Internet Security (CIS), le Groupe de travail sur le Plan directeur de défense contre les rançongiciels les a placées en tête de liste des défenses essentielles pour se protéger des rançongiciels. Des professionnels de l'assurance ont également examiné ces mesures IG-1 pour s'assurer qu'elles s'appliquent à ce que l'on constate concrètement dans les demandes d'indemnisation et qu'elles peuvent réduire les risques d'attaque.
- Ensuite, le plan directeur aide le secteur de l'assurance à mieux cerner les signaux qu'il doit rechercher au moment de la souscription des comptes. Dans d'autres branches d'assurance, les données sur les pertes de nature technique orientent les efforts de souscription et de réduction des risques des assureurs et

10 https://netdiligence.com/wp-content/uploads/2021/09/NetD_2021_Claims_Study_1.0_PUBLIC.pdf

11 https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html

des réassureurs. En raison de sa dimension humaine et de sa nature hautement technique, l'assurance cybernétique s'est souvent appuyée sur les données des litiges relatifs aux atteintes à la protection des données pour déterminer les prix actuariels et les lignes directrices en matière de souscription. La multiplication des attaques par rançongiciel illustre de façon spectaculaire la nécessité de mettre davantage l'accent sur les contrôles de sécurité capables à la fois de stopper les attaques et d'accélérer la récupération de l'information afin que les assurés ne soient pas contraints de payer une rançon pour retrouver le plein contrôle de leurs systèmes essentiels.

Conformément à de nombreuses recommandations du présent plan directeur, voici une liste de contrôles de sécurité spécifiques que l'industrie de la cyberassurance a vu faire diminuer les coûts des incidents et qu'il examine activement au cours du processus de souscription :

- Mise en place de procédures de sauvegarde rigoureuses.
- Sensibilisation à la sécurité et formation sur l'intervention en cas d'incident.
- Déploiement de mécanismes de protection du courrier électronique à l'échelle de l'entreprise.
- Protection avancée contre les logiciels malveillants aux points d'extrémité
- Visibilité et sécurité du réseau.

Nous avons également intégré au document plusieurs ressources d'intervention en cas d'incident, afin que les entreprises dépourvues de politiques de sécurité solides puissent utiliser une telle base reconnue dans l'industrie pour amener leur cybersécurité à un niveau supérieur.

Conclusion

Les quarante (40) mesures de protection recommandées dans le Plan directeur de protection contre les rançongiciels ont été soigneusement sélectionnées en tenant compte de leur facilité de mise en œuvre et de leur efficacité dans la défense contre les attaques par rançongiciel. Une cyberhygiène essentielle a pour but de donner aux PME la capacité d'atténuer les répercussions d'une attaque par rançongiciel, de réagir à celle-ci et de récupérer leurs données. La mise en œuvre du plus grand nombre possible de ces mesures de protection doit faire partie d'un programme itératif de gestion des risques dans chaque entreprise. Les PME qui pratiquent une cyberhygiène essentielle sont aptes à bien se défendre contre les rançongiciels en raison du niveau élevé de protection qu'elle leur procure. Elles peuvent également gérer plus efficacement leur risque cybernétique et mettre en œuvre au besoin d'autres contrôles pour faire face à des menaces spécifiques.

Enfin, le groupe de travail chargé d'élaborer ce plan directeur cherche à éliminer autant que possible les obstacles à l'adoption des mesures de protection qu'il recommande dans ce document, et à cette fin, il a inclus des outils et des ressources utiles pour mettre en œuvre chacune de ces mesures. Si ces ressources ne semblent pas suffisantes, posez des questions et demandez conseil aux fournisseurs de services de cybersécurité. Bien qu'une cybersécurité parfaite soit impossible, vous pouvez rendre votre entreprise plus résistante aux cybermenaces.

Vos premiers pas

Comme nous l'avons dit, de nombreuses PME peuvent se sentir dépassées par la mise en œuvre d'un cadre de sécurité. Elles doivent donc commencer modestement et développer leurs défenses au bon rythme. Pour commencer, elles peuvent télécharger le Plan directeur de défense contre les rançongiciels pour évaluer les mesures de protection dont la mise en œuvre est recommandée. On y décrit chacune de ces mesures et les fonctions du cadre de cybersécurité du National Institute of Standards and Technology qui s'y rattachent, ainsi que plusieurs outils et ressources susceptibles de faciliter leur mise en œuvre.

Toute entreprise a également accès à un large éventail d'autres outils et ressources pour acquérir une cyberhygiène essentielle. Par exemple, certaines d'entre elles ont un autre cadre de sécurité en place et hésitent à le remplacer ou à le compléter par un autre. Heureusement, le Center for Internet Security (CIS) renvoie à plusieurs autres cadres de sécurité – p. ex., la certification du modèle de maturité de la cybersécurité du National Institute of Standards and Technology (CMMC NIST) – mis gratuitement à la disposition de toute entreprise via ses pages Web Navigateur des contrôles du CIS et Plan de travail du CIS. Les entreprises qui veulent en savoir plus sur les contrôles CIS et sur la manière de mettre en œuvre le présent plan directeur peuvent compter sur plusieurs ressources, dont les suivantes :

- Spécifications et évaluation des contrôles du CIS – Pour comprendre ce qui doit être mesuré afin de vérifier que les mesures de protection du CIS sont correctement mises en œuvre.
- Outil d'auto-évaluation des contrôles (OAEC) du CIS – Pour évaluer et suivre la mise en œuvre des contrôles du CIS.
- Méthode d'évaluation des risques (MER) du CIS, v2.1 – Pour mettre en œuvre et évaluer la posture de sécurité de l'information de l'entreprise par rapport aux contrôles du CIS.

L'annexe C du présent document contient également plusieurs autres ressources réputées. Comme on l'a mentionné, l'objectif du plan directeur n'est pas d'atteindre la perfection. Chaque mesure de protection adoptée est un pas dans la bonne direction vers une cyberhygiène essentielle. En règle générale, la défense contre les rançongiciels et les cybermenaces n'est pas une mince affaire, mais elle est indispensable pour renforcer la posture de cybersécurité des entreprises du monde entier. Notre groupe de travail est convaincu que les mesures de protection qu'il a sélectionnées contribueront à la défense contre les rançongiciels et d'autres cyberattaques, ainsi qu'à constituer une cyberdéfense efficace sur des bases solides.

Annexe A : Plan directeur de défense contre les rançongiciels

Catégorie	Mesures de protection du CIS	Fonction de sécurité du NIST	Nom de la mesure de protection	Type
Identification				
Connaître son environnement	1.1	Identification	Établir et tenir à jour un inventaire détaillé des équipements informatiques de l'entreprise.	Fondamentale
	2.1	Identification	Établir et tenir à jour un inventaire des logiciels.	Fondamentale
	2.2	Identification	S'assurer que les logiciels autorisés sont actuellement pris en charge.	Exécutable
	3.1	Identification	Établir et maintenir un processus de gestion des données.	Fondamentale
	5.1	Identification	Établir et tenir à jour un inventaire des comptes d'utilisateur.	Fondamentale
Protection				
Configurations sécurisées	4.1	Protection	Établir et maintenir un processus de configuration sécurisé.	Fondamentale
	4.2	Protection	Établir et maintenir un processus de configuration sécurisé de l'infrastructure du réseau.	Fondamentale
	4.4	Protection	Mettre en œuvre et gérer un pare-feu sur les serveurs.	Exécutable
	4.7	Protection	Gérer les comptes par défaut liés aux équipements informatiques et aux logiciels de l'entreprise.	Exécutable
Gestion des comptes et des accès	5.2	Protection	Utiliser des mots de passe uniques.	Exécutable
	5.3	Protection	Fermer les comptes inactifs.	Exécutable
	5.4	Protection	Restreindre les privilèges d'administrateur aux seuls comptes réservés à cette fonction.	Exécutable
	6.1	Protection	Établir un processus d'autorisation de l'accès.	Fondamentale
	6.2	Protection	Mettre en place une procédure de révocation de l'accès.	Fondamentale
	6.3	Protection	Imposer l'AMF avec les applications accessibles de l'extérieur.	Exécutable
	6.4	Protection	Imposer l'AMF avec l'accès au réseau à distance.	Exécutable
	6.5	Protection	Imposer l'AMF avec l'accès d'administrateur.	Exécutable
Planification de la gestion des vulnérabilités	7.1	Protection	Établir et maintenir un processus de gestion des vulnérabilités.	Fondamentale
	7.2	Protection	Établir et maintenir un processus d'atténuation.	Fondamentale
	7.3	Protection	Automatiser la gestion des correctifs des systèmes d'exploitation.	Exécutable
	7.4	Protection	Automatiser la gestion des correctifs des applications.	Exécutable
	12.1	Protection	Maintenir systématiquement à jour l'infrastructure du réseau.	Exécutable
Défense contre les logiciels malveillants	9.1	Protection	N'autoriser que les navigateurs et les clients de messagerie entièrement pris en charge.	Exécutable
	9.2	Protection	Utiliser des services de filtrage par DNS.	Exécutable
	10.1	Protection	Déployer des antimaliciels et en assurer la maintenance.	Exécutable
	10.2	Protection	Configurer le téléchargement automatisé des signatures antimaliciels.	Exécutable
	10.3	Protection	Désactiver la fonction d'exécution et de lecture automatique des supports amovibles.	Exécutable
Sensibilisation à la sécurité et formation	14.1	Protection	Établir et maintenir un programme de sensibilisation à la sécurité.	Fondamentale
	14.2	Protection	Former les membres du personnel à reconnaître le piratage psychologique.	Exécutable
	14.6	Protection	Former les membres du personnel à reconnaître et à signaler les incidents de sécurité.	Exécutable
Détection				

Intervention				
Récupération de données et intervention en cas d'incident	17.1	**Intervention**	Désigner le personnel chargé de gérer le traitement des incidents.	Exécutable
	17.2	**Intervention**	Établir et tenir à jour une liste de personnes-ressources auxquelles signaler les incidents de sécurité.	Exécutable
	17.3	**Intervention**	Établir et maintenir un processus intégré de signalement des incidents.	Fondamentale
	8.1	**Intervention**	Établir et maintenir un processus de gestion des journaux de vérification.	Fondamentale
	8.2	**Intervention**	Recueillir les journaux de vérification.	Exécutable
	8.3	**Intervention**	Prévoir un espace de stockage adéquat pour les journaux de vérification.	Exécutable
Récupération				
Récupération de données et intervention en cas d'incident	11.1	**Récupération**	Établir et maintenir un processus de récupération des données.	Fondamentale
	11.2	**Récupération**	Automatiser la sauvegarde des données.	Exécutable
	11.3	**Récupération**	Protéger les données de récupération.	Exécutable
	11.4	**Récupération**	Établir et maintenir une instance isolée des données de récupération.	Exécutable

Annexe B : Abréviations, sigles et acronymes

AMF	Authentification multifactorielle
CCS	Cadre de cybersécurité
CIS	Center for Internet Security (Centre pour la sécurité de l'Internet)
CISA	Cybersecurity and Infrastructure Security Agency (Agence pour la cybersécurité et la sécurité des infrastructures)
CMMC	Certification du modèle de maturité de la cybersécurité
Contrôles du CIS	Contrôles de sécurité essentiels du CIS
DBIR	Verizon Data Breach Investigations Report (rapport d'enquête de Verizon sur les fuites de données)
DISA STIGs	Defense Information Systems Agency Security Technical Implementation Guides (guides de mise en œuvre technique de la sécurité de l'Agence des systèmes d'information de la Défense
DNS	Système de noms de domaine
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center (centre d'analyse et d'échange d'informations sur les infrastructures électorales)
FBI	Federal Bureau of Investigation (Bureau d'enquête fédéral)
GCA	Global Cyber Alliance (Alliance mondiale pour la cybernétique)
GTLR	Groupe de travail sur la lutte contre les rançongiciels
IG	Implementation Group (groupe de mise en œuvre)
IG-1	Implementation Group 1 (groupe de mise en œuvre 1)
II	Intervention en cas d'incident
ISO	Organisation internationale de normalisation
MDC du CIS	Modèle de défense de la communauté du Center for Internet Security
MER du CIS	Méthode d'évaluation des risques du CIS
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge (tactiques, techniques et connaissances communes adverses de MITRE)
MS-ISAC	Multi-State Information Sharing and Analysis Center (Centre d'analyse et de partage de l'information multiétatique)
NIST	National Institute of Standards and Technology (Institut national des normes et de la technologie)
OAEC du CIS	Outil d'auto-évaluation des contrôles du CIS
PME	Petites et moyennes entreprises
RDP	Remote Desktop Protocol (protocole de bureau à distance)
SLTT	State, Local, Tribal, and Territorial governments (gouvernements des États, des collectivités locales, des tribus et des territoires)
TI	Technologie de l'information
TSI	Institute for Security and Technology (Institut pour la sécurité et la technologie)
URL	Uniform Resource Locator (localisateur de ressources uniforme)
USB	Universal Serial Bus (bus série universel)

Annexe C : Autres ressources

Contrôles de sécurité essentiels du CIS, v8 – Apprenez-en plus sur les contrôles du Center for Internet Security : comment les mettre en place, pourquoi chaque contrôle est essentiel, quelles procédures et quels outils utiliser pendant la mise en œuvre et quelles mesures de protection sont associées à chaque contrôle.

Spécifications et évaluation des contrôles du CIS – Pour comprendre ce qui doit être mesuré et confirmer que les mesures de protection du CIS sont correctement mises en œuvre.

Navigateur des contrôles du CIS – Apprenez comment les contrôles et les mesures de protection s'articulent avec d'autres normes de sécurité (la CMMC, la publication spéciale SP 800-53 Rev. 5 du NIST, la base de connaissances ATT&CK de MITRE, etc.).

Outil d'auto-évaluation des contrôles (OAEC) du CIS – Pour évaluer et suivre la mise en œuvre des contrôles du CIS.

Modèle de défense de la communauté (MDC) 2.0 du CIS – Guide publié par le CIS et qui reprend les comptes rendus gratuits et complets d'attaques et d'incidents de sécurité, en plus de s'appuyer sur la base de connaissance ATT&CK de MITRE, reconnue par l'industrie.

Méthode d'évaluation des risques (MER) du CIS, v2.1 – Pour mettre en œuvre et évaluer la posture de sécurité de l'information de l'entreprise par rapport aux contrôles du CIS.

Abonnement à la suite d'outils SecureSuite du CIS – CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, et d'autres outils de sécurisation. Gratuit pour les gouvernements des États, des collectivités locales, des tribus et des territoires.

CIS Benchmarks℠ – Directives de configuration sécurisée de plus de 100 technologies, y compris les systèmes d'exploitation, les applications et les périphériques de réseau.

Cybersecurity and Infrastructure Security Agency (CISA) et Multi-State Information Sharing and Analysis Center (MS-ISAC®) – Guide collectif sur les rançongiciels – Ces pratiques exemplaires et ces recommandations incontournables en matière de rançongiciels sont fondées sur les connaissances opérationnelles de la CISA et du MS-ISAC.

CISA | Stop Ransomware – Guichet unique du gouvernement américain pour stopper la prolifération des rançongiciels.

Cyber Readiness Institute | Guide sur les rançongiciels – Comment se préparer à une attaque par rançongiciel, y réagir lorsqu'elle survient et récupérer ses données.

Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) – Normes de configuration élaborées par la Defense Information Systems Agency.

Abonnement au Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC®) – Gratuit pour tout gouvernement SLTT qui soutient les fonctionnaires électoraux des É.-U. et leurs associations.

Federal Bureau of Investigation (FBI) | Fiche d'information sur les rançongiciels – Apprenez-en plus les rançongiciels et la manière d'y réagir.

Global Cyber Alliance (GCA) | Boîte à outils de cybersécurité pour les petites entreprises - Outils gratuits et efficaces que vous pouvez utiliser dès aujourd'hui pour prendre des mesures immédiates qui réduisent votre vulnérabilité cybernétique.

Institute for Security and Technology (IST) | RTF Report: Combating Ransomware – Cadre de mesures fondé sur les principales recommandations du Groupe de travail sur les rançongiciels.

Abonnement à MS-ISAC – Gratuit pour les 50 États américains, le district de Columbia, les territoires américains, les gouvernements locaux et des tribus, les établissements d'enseignement public du primaire

et du secondaire, les établissements publics d'enseignement supérieur, les autorités et toute autre entité publique non fédérale aux États-Unis.

National Institute of Standards and Technology (NIST) – Cadre de cybersécurité du National Institute of Standards and Technology (NIST)

NIST Small Business Cybersecurity Corner – Page Web de ressources en cybersécurité et d'informations sur les rançongiciels du NIST

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org
info@securityandtechnology.org