ÉLÉMENTS FONDAMENTAUX DU G7 POUR LA RÉSILIENCE AUX RANÇONGICIELS DANS LE SECTEUR FINANCIER

Octobre 2022

La croissance et la prolifération des rançongiciels constituent l'un des défis majeurs auxquels sont actuellement confrontées les entités financières. Les rançongiciels exploitent un système d'information compromis à des fins d'extorsion, si bien que la victime ne peut pas utiliser entièrement le système ou les données qui y sont stockées jusqu'à ce qu'une demande de rançon soit satisfaite[1]. Par sa nature, le rançongiciel a un impact sur la capacité des victimes à poursuivre leurs activités. Dans le secteur financier, les rançongiciels peuvent constituer un risque inacceptable.

Les attaques par rançongiciels pourraient ne s'arrêter que lorsque leur utilisation ne sera plus rentable. Il est important que les entités financières prennent les mesures nécessaires pour devenir résilientes aux rançongiciels avant qu'une attaque ne se produise. Ce faisant, elles devraient également prendre en compte les risques encourus par les tiers prestataires critiques, qui sont susceptibles de créer des risques directs ou indirects liés aux rançongiciels pour les entités financières. Remédier à ces problèmes permettra aux entités financières de préserver leurs activités commerciales et d'éviter de payer des rançons qui pourraient inciter les auteurs d'attaques à poursuivre leur quête de profits grâce aux rançongiciels.

Ce document fournit aux entités financières des blocs constitutifs de haut niveau pour faire face à la menace des rançongiciels. Il est non normatif et non contraignant, et vise à intégrer les approches politiques, les orientations sectorielles et les meilleures pratiques actuellement en vigueur dans les pays membres du G7. Bien qu'il soit principalement axé sur les entités financières du secteur privé et leurs tiers prestataires critiques, ce document peut également être utilisé par les autorités financières pour leurs propres activités internes de lutte contre les rançongiciels ainsi que pour leurs efforts visant à promouvoir la résilience du secteur financier.

Dans de nombreux cas, les étapes visant à créer une résilience aux rançongiciels devraient se rapprocher de ce que les entités ont déjà mis en œuvre pour se préparer aux incidents de cybersécurité. Le document *éléments fondamentaux du G7 pour la résilience aux rançongiciels dans le secteur financier* s'aligne sur le document *groupe des sept – éléments fondamentaux pour la cybersécurité* publié en 2016. Pour chaque élément présenté dans le document original, ce document décrit les considérations qui sont essentielles pour faire face à la menace des rançongiciels.

[1]Pour les besoins de ce document, les définitions des termes clés font référence au Cyber Lexicon (lexique de la Cybersécurité) du Conseil de stabilité financière (CSF), sauf indication contraire. Une mise à jour du Lexique de la Cybersécurité du CSF (2018) est en cours et une version révisée devrait être publiée en 2023. La version révisée devrait inclure une définition reconnue des rançongiciels, qui ne disposaient pas de définition distincte dans le Lexique de 2018.

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.

Élément 1 : Stratégie et cadre de cybersécurité
Intégrer la résilience aux rançongiciels dans la stratégie globale et le cadre général de cybersécurité de l'entité.

Une stratégie globale et un cadre général de cybersécurité sont des composantes nécessaires de tout programme de cybersécurité dans toute organisation. Avec les autres menaces prises en compte par une entité financière, le meilleur moyen de traiter le risque d'attaque par rançongiciel est de recourir à une approche intégrée et globale.

La plupart des attaques par rançongiciel réussies résultent d'une violation rendue possible par des mesures d'hygiène informatique inadéquates au sein d'une organisation. Ceci peut comprendre l'absence de pratiques d'authentification fortes, une formation insuffisante des utilisateurs finaux en matière de cybersécurité et de protection contre l'hameçonnage, une gestion insuffisante des actifs informatiques, l'absence de segmentation efficace du réseau ou le déploiement lent ou incomplet de correctifs de sécurité sur les actifs critiques. Ces vulnérabilités sont généralement traitées dans la stratégie globale et le cadre général de cybersécurité de l'entité financière.

Élément 2 : Gouvernance
Assurer une coordination efficace face aux impacts des rançongiciels sur l'ensemble de l'organisation grâce à des structures de gouvernance efficaces.

Les incidents de rançongiciels sont rarement circonscrits aux fonctions de technologies de l'information d'une organisation, mais ont en revanche des répercussions importantes sur les activités commerciales, la conformité juridique et réglementaire, le marketing et les affaires publiques. Il est important de développer une gouvernance forte de la cybersécurité de l'entreprise, qui intègre la planification de lutte contre les rançongiciels dans les processus décisionnels globaux. Cette préparation comprend une surveillance au niveau du Conseil d'administration et un haut niveau de coordination entre les unités opérationnelles. Les discussions sur la gouvernance pourront couvrir des questions telles que le suivi des ressources (*asset tracking*), la classification des données et les stratégies de sauvegarde, les exercices, la détection des vulnérabilités et la formation des utilisateurs finaux à la cybersécurité, questions qui ont toutes leur importance pour la protection contre les rançongiciels et les autres cyber-menaces. D'autres sujets importants de discussion au niveau de gouvernance des instances dirigeantes liés aux rançongiciels sont :

Prévoir les réponses aux demandes de rançon – Les pays du G7 déconseillent généralement le paiement de rançons, qui peut contribuer au financement d'entreprises criminelles et encourager involontairement la persistance de comportements malveillants. Le paiement d'une rançon ne garantit pas le rétablissement de l'accès aux données, puisqu'il est possible que la clé privée ne puisse être obtenue ou que la restauration des données à l'aide de cette clé soit beaucoup trop lente ou incomplète. Les attaquants peuvent également conserver des copies des données sensibles saisies

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.

lors d'une attaque par rançongiciel, qui pourraient leur permettre de conserver des moyens de pression sur une victime.

Des politiques nationales ou des normes sectorielles peuvent avoir un effet dissuasif sur le paiement des rançons. Dans certains cas, les paiements de rançon peuvent être interdits par la loi, par exemple lorsqu'ils impliquent des versements à une entité soumise à des sanctions économiques. Les entités devraient consulter préventivement les lois en vigueur dans leur juridiction s'agissant des incidents de rançongiciel. Les entités doivent également prendre en compte les éventuelles difficultés d'identification de l'attaquant ou du destinataire d'un paiement lié à un rançongiciel afin d'évaluer les éventuels risques de sanctions.

Planification de la continuité d'activité – Les incidents de rançongiciels peuvent interrompre le fonctionnement de systèmes d'information critiques sur des périodes prolongées, pouvant exercer un impact significatif sur des activités opérationnelles critiques. Les professionnels de la cybersécurité au sein de l'organisation gagneront à collaborer étroitement avec d'autres composantes opérationnelles sur les questions de planification de la continuité opérationnelle. Ils devraient envisager d'inclure des scénarios impliquant des rançongiciels dans leurs plans de continuité d'activité.

Planification des communications – Les plans de communication interne et externe sont des éléments supplémentaires qui doivent de préférence être gérés au niveau des instances dirigeantes. Les entités financières reposent fortement sur la confiance, qui est au cœur de leurs activités. Les entités financières souhaiteront anticiper les intérêts et les préoccupations des principaux groupes de parties prenantes afin de pouvoir y répondre au moyen d'une communication rapide et efficace. Cela peut inclure des clients, des partenaires commerciaux, des employés, des autorités de surveillance et le grand public.

Ces groupes pourraient s'inquiéter de l'impact d'un incident de rançongiciel sur la capacité de l'entité financière affectée à continuer à fournir ses services, ainsi que sur la sécurité des comptes bancaires, des données personnelles et des données de l'entreprise. Ils pourraient également avoir des questions sur la manière dont l'entité réagit aux demandes de rançon.

Planification interorganisationnelle – En plus de leur fort impact sur une entité individuelle, les incidents de rançongiciels au sein du secteur financier pourraient avoir des répercussions importantes sur de nombreuses autres entités du secteur financier et sur leurs clients. Les entités financières, les organisations du secteur et les autorités financières jouent un rôle important dans la mise en place de structures solides permettant de faire face aux risques liés aux rançongiciels. Une planification interorganisationnelle efficace définira clairement les rôles, les responsabilités et les mécanismes de coordination des différents niveaux de prise de décision. Il peut s'agir d'un large éventail de parties prenantes, dont les autorités de régulation, les organismes chargés de faire respecter la loi et les agences de cybersécurité, les compagnies d'assurance, les équipes

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.

d'intervention d'urgence, et même de nouvelles parties prenantes telles que les prestataires de services liés aux actifs virtuels.

Élément 3 : Évaluation des risques et des contrôles
Assurer la mise en œuvre de contrôles pour faire face au risque liés aux rançongiciels.

Les entités financières ont tout intérêt à évaluer les risques liés aux rançongiciels et les mesures de contrôle compensatoires prévues par leur dispositif de cybersécurité existant, ainsi qu'à identifier les tiers prestataires (y compris les services du *cloud* tels que le stockage et la messagerie électronique) qui peuvent constituer des points d'entrée pour les cyber-menaces. Les entités financières bénéficient d'une sensibilisation aux pratiques de cybersécurité des tiers prestataires et aux incidents qu'ils peuvent rencontrer.

Les entités pourraient tenter de faire face au risque lié aux rançongiciels notamment en souscrivant des polices d'assurance. Les polices d'assurance peuvent protéger les métiers de certaines pertes dues aux rançongiciels, en particulier les pertes relatives au rétablissement d'activités. De nombreuses polices donnent également accès à un large éventail de ressources d'intervention, notamment l'intervention d'un gestionnaire d'incident (*breach coaching*), le traitement des communications de l'attaquant, les relations publiques et l'enquête judiciaire. Les polices d'assurance ne peuvent pas se substituer à une bonne hygiène informatique et à une planification efficace de lutte contre les rançongiciels et, en fait, de nombreux assureurs exigent des preuves de ces pratiques dans le cadre de leur processus de souscription. Les polices sont accompagnées de limitations, de franchises, de sous-limites et d'exclusions, et ne couvrent généralement pas la totalité des pertes financières. Par exemple, il est extrêmement difficile de s'assurer contre les conséquences négatives graves d'un rançongiciel, comme les impacts sur la réputation et la conformité.

Élément 4 : Surveillance
Surveiller les systèmes pour détecter les signaux d'une éventuelle activité de rançongiciel.

Ce sont les systèmes de détection d'intrusion et les systèmes connexes mis en place par une entité financière afin de détecter les activités malveillantes ou anormales sur ses systèmes d'information qui permettent le mieux d'identifier les signes d'une activité de rançongiciel. Les organisations peuvent utiliser toute une variété de sources d'information pour détecter les menaces externes de rançongiciels et tenter d'identifier les tendances. Ces sources d'information comprennent les rapports sur les menaces et les flux de renseignements publiés par les organismes chargés de faire respecter la loi et d'assurer la cybersécurité, les organismes du secteur et les tiers prestataires de sécurité, entre autres.

Élément 5 : Réponse
Appliquer les plans élaborés en réponse aux incidents de rançongiciels.

Les entités seront particulièrement efficaces dans leur réponse aux rançongiciels si elles interviennent à plusieurs niveaux de manière coordonnée. Il est important que les entités déploient

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.

des efforts continus pour renforcer leurs réponses systématiques par le biais de formations couvrant plusieurs scénarios qui reflètent différents aspects des impacts des rançongiciels.

Les incidents de rançongiciels peuvent constituer des crimes et nécessiter une coordination avec les autorités compétentes appropriées. Les entités financières ont tout intérêt à établir des relations avec les autorités compétentes chargées de l'application de la loi, de la sécurité nationale et de la réglementation avant la survenue d'un incident de rançongiciel, afin de faciliter la communication pendant l'incident. Selon la juridiction, une entité financière peut être en mesure ou tenue de signaler aux autorités compétentes toute activité suspecte pouvant indiquer un incident de rançongiciel.

De nombreuses organisations font appel à des tiers pour les assister dans leurs activités de réponse aux rançongiciels. Le recours à des tiers permet aux organisations d'augmenter rapidement leur capacité d'intervention grâce au soutien d'un personnel qualifié et expérimenté dans la réponse aux rançongiciels. Les entités financières doivent toutefois être informées que, dans le cas d'incidents de grande ampleur, ces services peuvent faire l'objet d'une forte demande de la part de plusieurs organisations en même temps. Les entités peuvent donc envisager de répertorier d'autres prestataires potentiels dans le cadre de leur plan d'intervention.

Il peut être demandé aux entités financières de jouer un rôle dans la réponse aux incidents qui n'ont pas d'impact sur leurs propres systèmes. Les paiements liés aux rançongiciels sont souvent effectués par l'intermédiaire d'entités financières, notamment par le biais d'échanges de monnaie virtuelle. Les entités financières jouent un rôle important dans la protection du système financier face aux menaces des rançongiciels en respectant leurs obligations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, ce qui inclut le signalement des activités suspectes liées aux rançongiciels. En outre, les pays devraient se conformer aux normes du *Financial Action Task Force*, notamment en terme d'actifs virtuels, afin de réduire la possibilité pour les criminels d'accéder aux services financiers et de les exploiter.

Élément 6 : Rétablissement

Prendre des dispositions pour restaurer les capacités qui ont pu être compromises par un incident de rançongiciel.

La sauvegarde et le rétablissement des systèmes et des données constituent un élément essentiel de la reprise après un incident de rançongiciel. Lors de l'élaboration d'une stratégie de sauvegarde des données, les entités devraient considérer les capacités des acteurs des rançongiciels à contourner ou à compromettre les procédures de sauvegarde courantes. Elles doivent prendre en compte le fait que les acteurs des rançongiciels peuvent chercher à infecter les données de sauvegarde et amorcer ce processus bien avant que l'attaque par rançongiciel ne soit visible. Cela peut rendre difficile la restauration des données sans réinfecter les systèmes de l'entité. En outre, même si les données sont correctement sauvegardées et restaurées, les attaquants peuvent conserver les données exfiltrées à des fins d'extorsion avec la menace de les exposer publiquement.

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.

Les entités financières devraient envisager des stratégies de sauvegarde possédant des caractéristiques qui les rendraient résilientes aux rançongiciels. Ces solutions peuvent inclure des systèmes qui empêchent la modification, la suppression ou le cryptage des données stockées[2]. Elles peuvent également inclure des pratiques telles que des sauvegardes plus fréquentes, des délais de conservation des sauvegardes plus longs, des sauvegardes hors ligne et la duplication des solutions de stockage des données sur différents systèmes sur site et hors site.

Comme c'est le cas pour les mesures d'intervention, ce sont les entités qui auront testé au préalable leurs sauvegardes, pratiqué et confirmé la restauration de leurs données et la réinstallation des comptes utilisateurs et des logiciels critiques dans les délais impartis qui se rétabliront le mieux après des attaques par rançongiciel. La restauration des données est notoirement difficile, surtout pour les volumes importants de données, et les entités risquent de rencontrer des difficultés inattendues lors de la restauration à partir de leurs sauvegardes.

Il est important qu'une entité documente soigneusement son processus de rétablissement, car les enquêteurs peuvent en avoir besoin. Il est également essentiel d'identifier et de documenter les enseignements tirés afin que l'entité puisse les appliquer à de futurs incidents.

Élément 7 : Échange de renseignements
Échanger des données, des informations et/ou des connaissances sur les incidents et les tendances en matière de rançongiciels avec des partenaires internes et externes.

Une activité de rançongiciel suit souvent des schémas basés sur les acteurs malveillants, le secteur ciblé, les tactiques employées et d'autres facteurs. Les entités doivent s'efforcer de comprendre ces schémas afin d'améliorer la compréhension de la situation et de surveiller en permanence les vulnérabilités communes pour y remédier et identifier les nouveaux signes de compromission.

Selon la juridiction, il peut exister des régimes de déclaration obligatoire concernant les attaques par rançongiciel. Les entités doivent également envisager de transmettre des rapports à des services compétents tels que les réseaux de renseignement et de partage de l'information (par exemple, les équipes de réponse aux incidents de cybersécurité financière et les centres d'analyse et de partage de l'information).

Élément 8 : Formation continue
Renforcer la résilience aux rançongiciels en tirant les enseignements des incidents passés

Comme pour tous les aspects de la cybersécurité, le traitement efficace des rançongiciels nécessite l'adoption d'une approche d'apprentissage continu. Les attaques par rançongiciel étant souvent associées à un manque d'hygiène informatique globale face aux attaques complexes, les entités devraient envisager de consacrer des ressources supplémentaires à la formation des utilisateurs finaux, qui peuvent être exposés à l'hameçonnage, à l'ingénierie sociale et à d'autres attaques qui

[2]Les technologies de sauvegarde présentant tout ou partie de ces qualités sont parfois qualifiées « d'immuables ».

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.

entraînent une intrusion dans les systèmes d'une entité et créent des faiblesses que les rançongiciels peuvent exploiter. En outre, les menaces liées aux rançongiciels évoluent constamment, tout comme les technologies permettant de s'en protéger. Les entités financières peuvent conserver leur capacité de résistance aux rançongiciels en suivant les évolutions de l'environnement des menaces, en examinant fréquemment les journaux des systèmes pour s'assurer de leur conformité aux bonnes pratiques, et en améliorant les processus et les configurations lorsque des défaillances sont identifiées.

TLP WHITE : Soumis aux règles standards relatives au droit d'auteur, ce document peut être distribué librement, sans aucune restriction.