Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Berne, le 13 novembre 2024

# Mesures contre les attaques par rançongiciel

## Rapport du Conseil fédéral en réponse au postulat 21.4512 Graf-Litscher du 16 décembre 2021

# Table des matières

# 1 Introduction

## 1.1 Généralités

Les cyberattaques sont des menaces que les entreprises et les autorités ne doivent pas prendre à la légère. En effet, elles peuvent avoir des incidences majeures sur le plan opérationnel, entraîner d'importants préjudices financiers et porter atteinte à la réputation des victimes. L'évolution de la cybercriminalité au cours des dernières années a montré que toute entreprise ou organisation constitue par principe une cible potentielle pour des attaques par rançongiciel. Dans la quasi-totalité des incidents de ce type suivis par l'Office fédéral de la cybersécurité (OFCS), les cybercriminels ont agi de manière opportuniste, attaquant là où ils pouvaient obtenir un retour sur investissement optimal dans des délais les plus courts possible et en déployant un minimum d'efforts. Contrairement aux idées reçues, le choix des victimes en cas d'attaques par rançongiciel n'est la plupart du temps pas ciblé. Les cybercriminels exploitent souvent des failles résultant du fait que les organisations n'ont pas mis en œuvre l'ensemble des mesures de sécurité de base dans le domaine de la cybersécurité. Ces lacunes en matière de défense numérique font de nombreuses entreprises et institutions des cibles faciles, bien qu'aléatoires, pour de telles attaques[1].

L'extorsion sous la forme d'attaques par rançongiciel[2] constitue un modèle économique particulièrement lucratif pour les cybercriminels, lesquels s'introduisent dans des systèmes informatiques afin de subtiliser ou de chiffrer des données personnelles ou commerciales, puis exigent une rançon en contrepartie de leur restitution ou de leur déchiffrement. Les rançons sont presque toujours payées en cryptomonnaie, ce qui rend l'identification des cybercriminels particulièrement difficile, voire impossible dans de nombreux cas[3].

Considérées comme financièrement solides, les entreprises et les autorités suisses, constituent une cible attrayante pour les cybercriminels en comparaison internationale. Les petites et moyennes entreprises (PME) disposent souvent de moins de connaissances et de ressources dans le domaine de la cybersécurité et sont donc elles aussi toujours plus visées par les pirates. En 2023, une centaine d'attaques par rançongiciel contre des entreprises, des autorités et des particuliers ont été signalées à l'OFCS[4]. Comme il n'existe aucune obligation de signaler ces cyberattaques, on peut supposer que ce chiffre est loin d'inclure toutes les attaques par rançongiciel abouties l'année dernière en Suisse. Affichant un degré élevé de professionnalisme, les cybercriminels ont mis en place des structures extrêmement complexes basées sur la répartition du travail qui, à l'instar d'une entreprise, regroupent différents spécialistes au sein d'un groupe avec des missions précises (p. ex. programmeurs des logiciels malveillants, pirates, experts en communication avec les victimes ou en blanchiment d'argent). Ils peuvent ainsi mener des attaques élaborées de grande envergure, ce qui complique sensiblement la lutte pour les autorités chargées de la sécurité. De plus, de nouveaux groupes voient le jour en permanence, généralement dans des États où aucune poursuite pénale efficace n'est garantie. Les tensions géopolitiques accentuent ce phénomène et compliquent la coopération internationale en la matière. La poursuite pénale des malfaiteurs se révèle donc particulièrement

---

1 Cf. OFCS (alors NCSC), Attaques au rançongiciel réussies contre des entreprises suisses, publié le 18 août 2024 (site internet : https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/ransomware-8.html ; consulté pour la dernière fois le 20 octobre 2024).

2 Les rançongiciels sont un type de programme malveillant conçu pour chiffrer les données d'une organisation dans le but d'exiger le paiement d'une rançon afin d'en rétablir l'accès. Ils peuvent également être utilisés pour subtiliser les informations d'une organisation et exiger un paiement supplémentaire en échange de la non-divulgation de ces informations aux autorités, à des concurrents ou au public (cf. NISTIR 8374, *Cybersecurity Framework Profile for Ransomware Risk Management* ; site internet : https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf ; consulté pour la dernière fois le 20 octobre 2024).

3 Si les pirates demandent uniquement une rançon pour le déchiffrement des données, on parle alors d'extorsion simple. Dans le cas d'une double extorsion, les malfaiteurs vont encore plus loin en menaçant aussi de publier des données sensibles. Dans le cas d'une triple extorsion, des menaces sont également proférées à l'encontre de tiers, p. ex. des clients ou des partenaires commerciaux de la victime.

4 Cf. OFCS, Sécurité de l'information, La situation en Suisse et sur le plan international, Rapport semestriel 2023/II (juillet – décembre), publié le 6 mai 2024, p. 15 (site internet : https://www.newsd.admin.ch/newsd/message/attachments/87435.pdf ; consulté pour la dernière fois le 20 octobre 2024 et OFCS, Sécurité de l'information, La situation en Suisse et sur le plan international, Rapport semestriel 2023/I (janvier – juin), publié le 2 novembre 2023, p. 4 et 20 ss (site internet : https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/lageberichte/NCSC_2023-1_HJB_FR.pdf.download.pdf/NCSC_2023-1_HJB_FR.pdf ; consulté pour la dernière fois le 20 octobre 2024).

complexe, mobilisant énormément de ressources et ne portant que rarement ses fruits. Par conséquent, des mesures préventives adéquates en matière de cybersécurité s'avèrent indispensables.

En raison du modèle commercial bien rodé des cybercriminels, une recrudescence des attaques est à craindre. Les experts en cybersécurité estiment que les attaques par rançongiciel génèrent chaque année plusieurs milliards de dollars pour les différents groupes criminels[5]. Les cybercriminels fixent le montant de leurs demandes de rançon de manière à ce qu'il soit inférieur aux coûts de réparation des dommages causés par les attaques, notamment en ce qui concerne la récupération des données. D'un point de vue économique, il est donc souvent plus avantageux pour les organisations de répondre aux exigences des criminels afin de remédier le cas échéant à la perte de leurs données et à une interruption de leur activité. Cependant, les organisations qui décident de payer la rançon demandée contribuent au succès et à la poursuite du développement du modèle économique des cybercriminels. En conséquence, les capacités économiques de ces derniers augmentent, ce qui accroît également la menace constituée par la cyber-extorsion.

En Suisse, la hausse du nombre d'attaques par rançongiciel a un impact sur la sécurité publique ainsi que sur la compétitivité de l'économie. Les institutions et administrations publiques sont particulièrement vulnérables à de telles attaques. La perte de données et l'interruption de l'exploitation peuvent fortement perturber leur activité, mettant en péril à la fois la sécurité et la fiabilité des services publics. Les entreprises sont également confrontées à des charges financières considérables liées aux paiements de rançons, aux coûts de remise en état et à l'atteinte à leur réputation. En plus de déstabiliser les institutions publiques, les autorités et les entreprises concernées, ces attaques amoindrissent également la confiance à l'égard des infrastructures numériques.

La protection contre les rançongiciels présente des enjeux non seulement techniques, mais aussi économiques et sociaux.

- *Enjeux techniques* : l'évolution constante des rançongiciels présente des enjeux techniques, les autorités et les entreprises devant investir en permanence dans des solutions de sécurité de pointe et adapter leurs infrastructures informatiques de manière à faire face aux nouvelles menaces.
- *Enjeux économiques* : la mise en œuvre de mesures de sécurité globales peut engendrer des coûts considérables, en particulier pour les PME.
- *Enjeux sociaux* : l'importance de la cybersécurité est souvent insuffisamment prise en considération. Les initiatives en matière de sensibilisation et d'information sont essentielles pour renforcer la prise de conscience par rapport au problème et promouvoir une culture de la sécurité. La coopération entre les autorités et les entreprises est importante pour élargir les connaissances et les ressources en matière de cybersécurité, et les utiliser efficacement.

## 1.2 Mandat d'examen

Le Conseil fédéral a été chargé d'examiner les questions suivantes en lien avec le postulat 21.4512 Graf-Litscher « Améliorer la protection contre les rançongiciels », déposé le 16 décembre 2021 :

[5] Les attaques graves impliquant vol et chiffrement de données peuvent coûter entre 50 et 150 millions de francs selon la branche et la taille. En cas de défaillance générale de l'informatique lors d'une telle attaque, la reprise (du moins provisoire) de l'exploitation nécessite parfois 5 à 7 jours. Le nombre de préjudices non signalés est élevé, de nombreuses entreprises et autorités craignant que rendre l'affaire publique ne ternisse leur réputation (cf. KÜDERLI URS/DOHREN JOHANNES, PWC, « Gros plan sur : cybersécurité Celui qui paie reste vulnérable », date inconnue ; site internet : https://www.pwc.ch/fr/insights/disclose/33/cyberattaques-celui-qui-paie-reste-vulnerable.html ; consulté pour la dernière fois le 20 octobre 2024 ; voir aussi RASCH MICHAEL, *Firmen scheuen die Anzeige von Cyberangriffen*, dans : NZZ n° 133, 12 juin 2017, p. 20). On estime qu'à l'échelle mondiale les préjudices économiques causés chaque année par la cybercriminalité s'élèvent à plus de 900 milliards de dollars (GEIGER MICHAELA, « *Hackerangriffe werden immer massiver, Cyberattacken : Banken und Versicherungen zahlen am häufigsten Lösegeld* », publié le 7 avril 2023 ; site internet : https://www.handelszeitung.ch/insurance/neue-studie-zu-cyberattacken-banken-und-versicherer-zahlen-am-haufigsten-losegeld-589550 ; consulté pour la dernière fois le 20 octobre 2024). L'Union européenne estime même que les coûts annuels liés à la cybercriminalité s'élèvent à 5,5 billions d'euros (cf. site internet : https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act ; consulté pour la dernière fois le 20 octobre 2024).

> « Les cyberattaques utilisant des rançongiciels (chiffrement de données grâce à un cheval de Troie) sont devenues l'une des principales cybermenaces pour notre économie et notre administration. De telles attaques sont très attrayantes pour les criminels car elles demandent relativement peu de moyens pour chiffrer les systèmes des victimes et que certaines entreprises et organisations payent de grosses sommes pour récupérer leurs données.
>
> Pour la sécurité de la population et de la place économique suisse, il est très important de renforcer la protection contre les rançongiciels. Le Conseil fédéral est donc chargé de présenter un rapport sur la manière d'atteindre cette protection. Il examinera notamment les possibilités suivantes :
>
> 1. introduction de directives contraignantes pour les organisations chargées d'une mission de service public en matière de protection de base contre les rançongiciels ;
> 2. introduction d'une obligation de déclaration en cas de paiement de rançons et d'une obligation d'impliquer les autorités dans les négociations avec les criminels ;
> 3. échange d'informations renforcé en cas d'attaque par rançongiciel, aboutie ou non, entre la Confédération, les autorités cantonales de poursuite pénale, les entreprises privées de réponse aux incidents de sécurité et les assurances. »

À la suite de la proposition du Conseil fédéral du 16 février 2022, le postulat a été adopté par le Conseil national le 8 juin 2022.

Le présent rapport décrit les mesures de protection existantes et les domaines dans lesquels elles sont déjà obligatoires. Il évalue ensuite s'il est nécessaire d'édicter des directives contraignantes supplémentaires pour les organisations chargées d'une mission de service public. Le chapitre suivant examine l'introduction d'une obligation de signaler en cas de paiement de rançon. Il présente les prescriptions légales en vigueur en Suisse en matière d'obligation de signaler dans le contexte des cyberattaques et montre, dans le cadre d'une comparaison juridique, comment la question est abordée dans d'autres pays. Sur cette base, les options de la Suisse sont exposées en ce qui concerne l'obligation de signaler tout paiement de rançon. Le dernier chapitre aborde quant à lui la question de l'échange d'informations, montrant comment il intervient aujourd'hui et comment il pourrait être renforcé à l'avenir. Les considérations finales servent à l'évaluation des résultats de l'examen et à l'indication des prochaines étapes.

# 2 Mesures de protection contre les attaques par rançongiciel

Aujourd'hui, la cybersécurité n'est plus un sujet technique marginal. Depuis un certain nombre d'années, il est indéniable que les cybermenaces représentent un risque économique et social important. En conséquence, différentes mesures techniques et organisationnelles ont été développées afin de renforcer la protection contre les cyberattaques. Décrites dans des instructions et des directives, ces mesures de protection doivent en principe être mises en œuvre par les entreprises et les autorités de manière à rendre le risque de cyberattaques acceptable pour elles.
Toutefois, les cyberattaques contre des organisations entraînent souvent des préjudices pour des tiers (p. ex. services partiellement indisponibles ou risque de publication de données personnelles ou commerciales volées). Les entreprises et les autorités doivent donc se prémunir contre les cyberattaques non seulement afin de défendre leurs propres intérêts, mais aussi en raison de la responsabilité plus large qu'elles assument en ce qui concerne la cybersécurité de leurs clients, de leurs collaborateurs et de leurs partenaires. Cet aspect est particulièrement important dans le cas d'organisations chargées d'une mission de service public. Dans le présent rapport, cela concerne les organisations qui reçoivent un financement public pour s'acquitter de tâches d'intérêt public. Elles

peuvent relever aussi bien du secteur public que du secteur privé. Les catégories ci-dessous sont notamment concernées.

- *Administrations publiques* : administrations fédérales, cantonales et communales qui assument des tâches publiques et fournissent des services publics.
- *Institutions publiques* : écoles, universités, hôpitaux et autres établissements d'enseignement ou prestataires de soins de santé qui sont financés par des fonds publics ou qui accomplissent des tâches publiques.
- *Entreprises de services publics* : entreprises qui fournissent au public des services d'infrastructure de base comme la gestion des eaux, de l'énergie ou des déchets, les services de télécommunications et les transports publics.

Cette délimitation est particulièrement importante pour la compréhension du cadre juridique, car l'applicabilité des lois pertinentes, notamment la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[6] et la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[7], varie en fonction de la mission et de la forme d'organisation.

Le présent chapitre sert à la description des mesures de protection qui sont déjà prévues par la Confédération en matière de cybersécurité au moyen d'instructions et de directives ou qui seront imposées par la législation. Il permet aussi la précision des prescriptions en vigueur concernant la mise en œuvre de mesures de protection pour les organisations chargées d'une mission de service public. Cette base permettra de déterminer s'il convient d'imposer des prescriptions contraignantes supplémentaires à ces organisations pour la protection fondamentale contre les attaques par rançongiciel.

## 2.1 Instructions et directives de la Confédération

Lors de cyberattaques, les pirates exploitent des failles dans la protection technique des systèmes ou des erreurs humaines. La plupart de ces attaques sont menées à des fins criminelles. Dans ce cas, les malfaiteurs agissent généralement de manière opportuniste, attaquant là où ils peuvent obtenir un retour sur investissement optimal en déployant un minimum d'efforts. Ils ne choisissent donc pas leurs victimes de manière ciblée : ils ont souvent recours à des méthodes relativement simples et attaquent là où une occasion favorable se présente. Il s'agit là d'une différence majeure par rapport aux pirates qui attaquent des organisations spécifiques à des fins d'espionnage, voire de sabotage, et qui utilisent pour cela des méthodes très sophistiquées.

Lorsque les attaques par rançongiciel reposent sur des motivations financières, l'objectif est de se protéger contre les actes opportunistes. Des mesures de protection relativement simples fonctionnent déjà à cet égard. Le moyen le plus efficace d'empêcher les cyber-extorsions à la suite d'attaques par rançongiciel est de se protéger de manière proactive contre ces attaques en mettant en œuvre d'autres mesures organisationnelles et techniques.

L'OFCS et d'autres services de l'administration fédérale comme l'Office fédéral pour l'approvisionnement économique du pays (OFAE) mettent à disposition sur leurs sites internet des informations, des instructions et des directives concernant les mesures fondamentales en matière de protection informatique (p. ex. mesures contre les attaques par rançongiciel) afin que les organisations chargées d'une mission de service public puissent également s'y référer.

6 RS **128**
7 RS **235.1**

### 2.1.1 Informations de l'OFCS

En vertu de l'art. 15*a*, al. 2, let. d et e, de l'ordonnance sur l'organisation du DDPS (Org-DDPS)[8], le Conseil fédéral a chargé l'OFCS de publier des informations relatives aux cyberincidents dès lors que cela est utile à la protection contre les cybermenaces, et d'alerter les entreprises, les autorités et les personnes concernées en cas de cybermenace immédiate ou de cyberattaque en cours. Une grande partie de ce mandat consiste à publier des alertes concernant les vulnérabilités actuelles ou les nouvelles méthodes d'attaque. L'OFCS fournit des informations à ce sujet sur son site internet ainsi que sur la plateforme d'échange d'informations pour les exploitants d'infrastructures critiques, le Cyber Security Hub (CSH). Il informe également les organisations au sein desquelles des failles critiques ont été découvertes et représentent une menace immédiate pour elles. En 2022, par exemple, l'OFCS a ainsi attiré l'attention de plus de 2000 entreprises suisses sur des failles critiques qui ont manifestement déjà été activement exploitées par plusieurs groupes criminels pour faire chanter des sociétés sises en Suisse par l'utilisation de rançongiciels[9].

Toutefois, il est important de disposer non seulement d'alertes à jour sur les vulnérabilités et les méthodes d'attaque actuelles, mais aussi de recommandations et d'instructions concernant les mesures de protection. Sur son site internet, l'OFCS énumère entre autres les principales mesures préventives de protection contre les rançongiciels[10]. Il décrit des mesures tant organisationnelles que techniques et souligne qu'une combinaison de ces mesures permet à l'ensemble des entités de renforcer de manière significative leurs défenses contre les attaques par rançongiciel. Les mesures-clés que les organisations chargées d'une mission de service public devraient aussi prendre en considération figurent ci-dessous[11].

Les mesures de protection organisationnelles minimales sont les suivantes.

- *Sensibilisation et formation des collaborateurs* : une mesure essentielle pour se prémunir contre les attaques par rançongiciel réside dans la sensibilisation et la formation continues du personnel. Des programmes de formation devraient être organisés régulièrement afin d'encourager la prise de conscience et l'utilisation en toute sécurité des moyens numériques comme les courriels. Cette mesure devrait par exemple aider les collaborateurs à faire preuve de prudence face aux pièces jointes et aux liens hypertexte dans des courriels suspects, à ne pas les ouvrir ni cliquer dessus, et à examiner attentivement les expéditeurs afin de s'assurer qu'ils sont connus et dignes de confiance[12]. La sensibilisation et la formation peuvent notamment être assurées au moyen de plateformes d'apprentissage en ligne, d'ateliers et de simulations d'attaques par hameçonnage.
- *Mise en œuvre des directives de sécurité* : les organisations devraient développer et mettre en œuvre des directives et des procédures en matière de cybersécurité dans le cadre de leur gouvernance informatique. Il s'agit notamment de processus permettant de réagir rapidement à des incidents ayant trait à la sécurité, d'effectuer des sauvegardes et de les vérifier régulièrement.

Les mesures de protection techniques minimales sont les suivantes.

- *Copies de sauvegarde régulières* : la sauvegarde régulière des données fait partie des mesures les plus efficaces contre les attaques par rançongiciel. Un concept de sauvegarde et de restauration détaillé aide à définir la fréquence des copies de sauvegarde, les mesures de test pour les restaurations et les procédures spécifiques pour les contrôles réguliers et garantit une restauration fiable et rapide des données en cas d'incident de sécurité ou de panne du

---

8 RS **172.214.1**

9 OFCS (alors NCSC), Update : À l'heure actuelle, plus de 2000 serveurs Microsoft Exchange ne sont toujours pas sécurisés en Suisse, publié le 1er décembre 2022 (site internet : https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2022/schwachstelle-proxynotshell-2.html ; consulté pour la dernière fois le 20 octobre 2024).

10 Cf. https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ransomware.html ; consulté pour la dernière fois le 20 octobre 2024.

11 Cf. https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ransomware.html ; consulté pour la dernière fois le 20 octobre 2024.

12 Cf. page internet détaillée https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-private/aktuelle-themen/umgang-mit-e-mails.html ; consulté pour la dernière fois le 20 octobre 2024.

système. Le principe de sauvegarde GFS[13] devrait être utilisé pour la création des copies de sauvegarde. Par ailleurs, il faut s'assurer, après le processus de sauvegarde, que le support sur lequel la copie est enregistrée est physiquement distinct de l'ordinateur ou du réseau et qu'il est conservé en toute sécurité afin de le protéger de tout chiffrement par les rançongiciels.

- *Mise à jour des logiciels et des systèmes d'exploitation* : les logiciels et les systèmes d'exploitation devraient être régulièrement mis à jour afin de corriger les failles de sécurité connues. Il convient de procéder aux mises à jour de sécurité de manière systématique et rapide pour l'ensemble des systèmes. Pour les systèmes accessibles par internet, les mises à jour corrigeant des failles de sécurité critiques devraient être effectuées dans les 24 heures. Les logiciels ou systèmes qui ne sont plus pris en charge par le fabricant devraient être désactivés ou déplacés dans une zone de réseau distincte et isolée.
- *Sécurisation des accès à distance* : le réseau privé virtuel (VPN), le protocole RDP (bureau à distance) et Citrix sont des technologies fréquemment utilisées pour accéder à distance à des systèmes informatiques et à des réseaux. Tous ces accès à distance, ainsi que tous les autres accès à des ressources internes (p. ex. messagerie web, SharePoint, etc.), devraient être sécurisés par des authentifications multifacteur (MFA)[14]. Cela vaut aussi par exemple pour les accès de prestataires informatiques et de partenaires contractuels.
- *Utilisation d'applockers* : la protection d'une infrastructure informatique contre les logiciels malveillants comme les rançongiciels peut être renforcée par l'utilisation de programmes informatiques spécifiques, également appelés *applockers* (p. ex. Windows AppLocker, Gatekeeper, SELinux ou des solutions tierces appropriées). Ces solutions permettent de contrôler et de définir quels programmes peuvent être exécutés sur l'ordinateur dans l'environnement de l'organisation.
- *Blocage des pièces jointes dangereuses dans les courriels* : les organisations doivent bloquer les pièces jointes dangereuses (types de fichiers souvent utilisés pour la diffusion de logiciels malveillants) sur la passerelle de messagerie ou à l'aide du filtre anti-spam, ou du moins les mettre en quarantaine. Pour ce faire, il est possible de recourir à des listes officielles de types de fichiers bloqués. Les pièces jointes dangereuses doivent également être bloquées dans le cas de fichiers d'archive comme ZIP et RAR. Il convient en outre de bloquer toutes les pièces jointes contenant des macros (p. ex. Word, Excel ou PowerPoint).

En collaboration avec des partenaires, des entreprises, des organisations et des particuliers, l'OFCS sensibilise au sujet des attaques par rançongiciel, s'efforçant ainsi de renforcer la prise de conscience en matière de cybersécurité. Ainsi, il organise régulièrement des campagnes de sensibilisation en collaboration avec les corps de police cantonaux et d'autres partenaires[15]. D'autres initiatives soutenues par l'OFCS englobent la plateforme de sécurité internet *iBarry.ch*[16] et les labels *Cyber-safe.ch*[17] et *Swiss Cyber Seal*[18] ainsi que l'auto-test de cybersécurité *Cybero*[19]. À cet égard, il convient de mentionner qu'il existe également en Suisse des initiatives régionales visant à améliorer

---

13 Le principe de sauvegarde GFS (*Grandfather-Father-Son backup*) est un principe de triple sauvegarde qui consiste à stocker plusieurs versions des données sur une certaine période. Des copies sont ainsi régulièrement créées et conservées à différents niveaux hiérarchiques ou « générations », des sauvegardes étant généralement planifiées à une fréquence quotidienne, hebdomadaire et mensuelle. La dernière copie en date est la « jeune génération » (*son*), tandis que les copies qui remontent le plus loin sont les « anciennes générations » (*grandfather*). Ce système permet non seulement d'accéder aux données les plus récentes, mais aussi de revenir aux versions antérieures si des données ont été supprimées ou modifiées par inadvertance. Il est p. ex. possible de récupérer un fichier qui a été supprimé la semaine précédente ou de restaurer l'état d'un système tel qu'il était un mois auparavant. Le principe de sauvegarde GFS assure donc une protection complète contre la perte de données et offre davantage de souplesse lors de la restauration de données.

14 L'authentification multifacteur est une procédure de sécurité qui nécessite l'utilisation d'au moins deux éléments distincts pour vérifier l'identité d'un utilisateur souhaitant accéder à un compte ou à un système : généralement quelque chose qu'il connaît (p. ex. mot de passe), qu'il possède (p. ex. smartphone pour recevoir un code de confirmation) ou une caractéristique biométrique propre (p. ex. empreinte digitale). Cette méthode renforce considérablement la sécurité, un pirate potentiel ayant alors plusieurs obstacles à franchir pour obtenir un accès non autorisé.

15 Exemple : la campagne S-U-P-E-R, cf. site internet : https://www.s-u-p-e-r.ch/fr/ ; consulté pour la dernière fois le 20 octobre 2024.

16 Cf. https://www.ibarry.ch/ ; consulté pour la dernière fois le 20 octobre 2024.

17 Cf. https://www.cyber-safe.ch/ ; consulté pour la dernière fois le 20 octobre 2024.

18 Cf. https://www.digitalsecurityswitzerland.ch/fr/cyberseal ; consulté pour la dernière fois le 20 octobre 2024.

19 Cf. https://cybero.ch/ ; consulté pour la dernière fois le 20 octobre 2024.

la cybersécurité dans les PME, comme *trust4sme*[20] dans le canton de Vaud et *ITSec4KMU*[21] dans le canton de Zoug.

### 2.1.2 Norme minimale pour les TIC

La cyberstratégie nationale (CSN)[22] soutient la mise en œuvre de la norme minimale élaborée par l'OFAE pour améliorer la résilience des technologies de l'information et de la communication (norme minimale pour les TIC) afin d'accroître la protection générale contre les cyberattaques.

La norme minimale pour les TIC repose sur le *Cybersecurity Framework* du *National Institute of Standards and Technology* (NIST) américain[23]. Elle comporte 108 mesures réparties en 23 catégories, une structure permettant d'évaluer le degré d'avancement et d'efficacité de la cybersécurité d'une organisation tout en offrant un cadre en vue d'une amélioration systématique de la cybersécurité. Les mesures de base de la norme sont en grande partie invariables, mais leur mise en œuvre requiert une certaine flexibilité, une adaptation aux menaces et aux dangers émergeants ou spécifiques à l'entreprise, des outils techniques et une expertise appropriée[24]. Elles ne prescrivent pas de solutions techniques, car les entités doivent les élaborer de manière autonome. À cette fin, ces dernières peuvent également se regrouper dans le cadre des structures associatives existantes afin d'élaborer une norme spécifique à leur branche.

## 2.2 Dispositions légales en matière de cybersécurité

Il existe d'ores et déjà des directives juridiquement contraignantes en matière de cybersécurité, qui figurent dans des directives de sécurité sectorielles. Le Conseil fédéral et les autorités administratives ont édicté des directives spécifiques dans ce domaine, notamment par voie d'ordonnance, pour les entreprises d'approvisionnement en énergie, les installations de transport par conduites, le secteur financier et l'administration fédérale. En outre, la LPD et la LSI jouent également un rôle important dans le domaine de la cybersécurité.

### 2.2.1 Entreprises d'approvisionnement en énergie

Les révisions de la loi fédérale sur l'approvisionnement en électricité (LApEl)[25] et de l'ordonnance sur l'approvisionnement en électricité (OApEl)[26] sont entrées en vigueur le 1er juillet 2024[27]. Des exigences contraignantes ont ainsi été édictées en matière de sécurité de l'information pour l'informatique et la technologie opérationnelle des producteurs d'électricité, des gestionnaires de réseau, des exploitants de stockage et des prestataires suisses. Le niveau de protection à atteindre dépend de la performance des systèmes. Les mesures permettant de l'atteindre sont déterminées sur la base de la norme minimale pour les TIC de l'OFAE, mentionnée plus haut.

---

20 Cf. https://trustvalley.swiss/trust4smes/ ; consulté pour la dernière fois le 20 octobre 2024.
21 Cf. https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/zuger-regierungsrat-lanciert-cybersecurity-offensive ; consulté pour la dernière fois le 20 octobre 2024.
22 Cf. cyberstratégie nationale (CSN), (site internet : https://www.ncsc.admin.ch/ncsc/fr/home/strategie/cyberstrategie-ncs.html ; consulté pour la dernière fois le 20 octobre 2024).
23 Cf. https://www.nist.gov/cyberframework ; consulté pour la dernière fois le 20 octobre 2024.
24 Chaque entreprise peut déterminer elle-même, par une analyse des risques, si les mesures minimales imposées sont suffisantes ou si des mesures supplémentaires s'avèrent nécessaires. Le guide pour la protection des infrastructures critiques (PIC), publié par l'Office fédéral de la protection de la population, peut aider les entreprises dans cette tâche (cf. https://www.babs.admin.ch/fr/guide-pour-la-protection-des-infrastructures-critiques ; consulté pour la dernière fois le 20 octobre 2024).
25 RS **734.7**
26 RS **734.71**
27 Cf. le Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité (protection contre les cybermenaces) (site internet : https://pubdb.bfe.admin.ch/fr/publication/download/11501 ; consulté pour la dernière fois le 20 octobre 2024).

### 2.2.2 Installations de transport par conduites

Le 29 novembre 2023, le Conseil fédéral a adopté l'art. 39*a* de l'ordonnance sur la sécurité des installations de transport par conduites (OSITC)[28], qui oblige les exploitants de ce type d'installations à améliorer leur cybersécurité et qui prévoit l'élaboration conjointe de directives dans ce domaine. Par la suite, l'industrie gazière a révisé sa recommandation G1008 f *Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en gaz*[29], qui se fonde sur la norme minimale pour les TIC susmentionnée. En raison de l'augmentation des menaces et compte tenu des différences significatives en ce qui concerne la mise en œuvre de la cybersécurité, le Conseil fédéral estime que cette nouvelle norme sectorielle doit impérativement être déclarée contraignante (cf. art. 39*a*, al. 2 et 4, OSITC)[30]. C'est pourquoi le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) a ouvert le 18 septembre 2024 la procédure de consultation relative à cette modification de l'ordonnance.

### 2.2.3 Marchés financiers

Ent ant qu'autorité de surveillance indépendante des marchés financiers suisses, l'Autorité fédérale de surveillance des marchés financiers (FINMA) est dotée de prérogatives de puissance publique à l'égard des banques, des entreprises d'assurances, des bourses, des établissements financiers, des placements collectifs de capitaux, de leurs gestionnaires et directions de fonds, ainsi que des intermédiaires d'assurance. La FINMA s'engage pour la protection des créanciers, des investisseurs et des assurés, et veille au bon fonctionnement des marchés financiers. Dans le cadre de la révision de la circulaire 2008/21 de 2019 (qui est une ordonnance administrative), la FINMA a intégré différents ajouts dans le domaine des cyberrisques. Conformément à ces règles, la procédure en matière de protection contre les cyberrisques doit faire l'objet d'une documentation couvrant au moins les aspects suivants[31] :

- identification des risques potentiels de cyberattaques ;
- protection des processus opérationnels et de l'infrastructure technologique contre les cyberattaques ;
- identification et désignation rapides de cyberattaques ;
- réaction aux cyberattaques par des mesures rapides et ciblées ;
- garantie d'un rétablissement rapide de la marche normale des affaires à la suite d'une cyberattaque.

Les prestataires de services financiers sont en outre tenus d'effectuer régulièrement des analyses de vulnérabilité ainsi que des tests d'intrusion.

---

28 RS **746.12**

29 Norme minimale pour garantir la sécurité des TIC pour l'approvisionnement en gaz (site internet : https://www.bwl.admin.ch/bwl/fr/home/bereiche/ikt/ikt_minimalstandard/ikt_branchenstandards/gasversorgung.html ; consulté pour la dernière fois le 20 octobre 2024).

30 Cf. le communiqué de presse du 19 septembre 2024 Le DETEC ouvre une procédure de consultation sur la révision d'ordonnances dans le domaine de l'énergie (site internet : https://www.uvek.admin.ch/uvek/fr/home/detec/medias/communiques-de-presse.msg-id-102488.html ; consulté pour la dernière fois le 20 octobre 2024), le projet d'ordonnance (site internet : https://pubdb.bfe.admin.ch/fr/publication/download/11856 ; consulté pour la dernière fois le 20 octobre 2024) et le rapport explicatif (site internet : https://pubdb.bfe.admin.ch/fr/publication/download/11857 ; consulté pour la dernière fois le 20 octobre 2024).

31 Circulaire FINMA 2008/21 (cf. https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=fr ; consulté pour la dernière fois le 19 juin 2024), ROLF H. WEBER/OKAN YILDIZ, *Cybersicherheit und Cyber-Resilienz in den Finanzmärkten*, 9e volume du recueil du Centre pour les technologies de l'information, de la société et du droit (ITSL), p. 33 (cf. https://eizpublishing.ch/wp-content/uploads/2022/04/Cybersicherheit-und-Cyber-Resilienz-in-den-Finanzmaerkten-Digital-V1_01-20220404.pdf ; consulté pour la dernière fois le 20 octobre 2024).

### 2.2.4 Protection informatique de base dans l'administration fédérale

Rattaché au Secrétariat d'État à la politique de sécurité, le service spécialisé de la Confédération pour la sécurité de l'information[32] peut, en vertu de l'art. 29, al. 1, de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI)[33], édicter des ordonnances administratives pour l'ensemble de l'administration fédérale concernant la protection de base des moyens informatiques (« protection informatique de base » ou « protection de base ») et fixer des directives en matière de sécurité des réseaux dans l'administration fédérale. C'est ce qui a été fait avec la directive du 5 juillet 2024 *Si001 – Protection informatique de base dans l'administration fédérale*[34]. La protection informatique de base définit de manière contraignante les prescriptions de sécurité minimales sur les plans de l'organisation, du personnel et de la technique dans le domaine de la sécurité informatique. La protection informatique de base doit être mise en œuvre dans l'administration fédérale pour chaque objet informatique à protéger. La mise en œuvre des directives et des mesures de sécurité doit être documentée et contrôlée par les unités administratives concernées[35].

### 2.2.5 Dispositions légales relatives à la protection des données qui touchent la cybersécurité

La loi sur la protection des données (LPD)[36] et l'ordonnance sur la protection des données (OPDo)[37] jouent un rôle-clé dans la cybersécurité des autorités fédérales et des entreprises. En vertu de l'art. 8, al. 1 et 2, LPD, les entités qui traient des données personnelles doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate de ces données par rapport au risque encouru afin d'éviter toute violation de la sécurité des données. Conformément à l'art. 8, al. 3, LPD, le Conseil fédéral a édicté des dispositions sur les exigences minimales en matière de sécurité des données (art. 3 ss, OPDo).

- *Mesures techniques* : la protection des données personnelles doit souvent être assurée par un chiffrement des données afin d'éviter tout accès non autorisé. Des mécanismes de contrôle d'accès doivent être mis en place afin de garantir que seules les personnes dûment autorisées peuvent accéder aux données sensibles. Par ailleurs, il convient de tenir compte des aspects liés à la sécurité du réseau afin d'empêcher toute personne non autorisée d'accéder à ces données (protection de l'infrastructure informatique par des pare-feu, systèmes de détection d'intrusions, exécution de mises à jour afin de garantir la sécurité du système, etc.).
- *Mesures organisationnelles* : des directives et des procédures de sécurité doivent être développées et mises en œuvre pour garantir la sécurité des données, et des formations régulières doivent être organisées pour les collaborateurs sur les thèmes de la protection des données et de la cybersécurité afin de les sensibiliser et d'améliorer leurs compétences dans ces domaines.
- *Analyses des risques et analyses d'impact relatives à la protection des données* : dans la mesure où des organisations chargées d'une mission de service public traitent des données personnelles, elles sont tenues d'effectuer régulièrement des analyses des risques afin d'identifier les vulnérabilités potentielles de leurs systèmes et de prendre les mesures qui s'imposent. Lors de l'introduction de nouveaux systèmes ou processus qui concernent des données personnelles, des analyses d'impact relatives à la protection des données doivent

---

32 L'art. 51, al. 6, OSI prévoit que l'OFCS assume jusqu'au 30 juin 2025 les tâches et les compétences du service spécialisé de la Confédération pour la sécurité de l'information. Par la suite, cette tâche incombera au Secrétariat d'État à la politique de sécurité (SEPOS).

33 RS **128.1**

34 L'art. 51, al. 1 de l'OSI, qui est entrée en vigueur le 1er janvier 2024, prévoit que les directives en matière de sécurité informatique émises par le Centre national pour la cybersécurité (NCSC), devenu l'OFCS depuis le 1er janvier 2024, et les exceptions qu'il a autorisées avant l'entrée en vigueur de l'ordonnance conservent leur validité durant trois ans au plus après l'entrée en vigueur de ladite ordonnance.

35 Cf. Directive du 5 juillet 2024 « Si001 – Protection informatique de base dans l'administration fédérale » (site internet : https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-IT-Grundschutz-V5-1-f.pdf.download.pdf/Si001-IT-Grundschutz-V5-1-f.pdf ; consulté pour la dernière fois le 20 octobre 2024).

36 RS **235.1**

37 RS **235.11**

être réalisées s'il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée afin d'évaluer les conséquences sur la protection des données et de prendre des mesures pour réduire les risques.

Au vu des mesures susmentionnées, il est possible d'affirmer que la LPD et l'OPDo ont contribué de manière significative à l'amélioration de la cybersécurité au sein des organisations chargées d'une mission de service public en imposant un niveau élevé de protection des données personnelles et en garantissant ainsi la protection de ces données contre tout accès non autorisé et tout usage abusif au profit de l'ensemble de l'infrastructure informatique.

Cependant, les entreprises privées qui assument un mandat public (p. ex. écoles privées, maisons de retraite) ne sont pas soumises à la LPD ni à l'OPDo, mais à la législation de leur canton sur la protection des données. Le contenu des lois cantonales s'inspire fortement de la loi fédérale sur la protection des données, afin de réglementer le traitement des données à caractère personnel au niveau cantonal, en particulier dans le secteur public. Ces actes législatifs cantonaux contiennent des principes et des exigences en matière de protection des données qui sont en grande partie similaires à ceux de la LPD et de l'OPDo et l'on peut donc se référer par analogie aux explications ci-dessus en ce qui concerne la cybersécurité.

### 2.2.6 Dispositions légales liées à la sécurité de l'information qui s'appliquent à la cybersécurité

Entrées en vigueur le 1er janvier 2024, la LSI et ses ordonnances d'exécution visent à renforcer la protection des informations et la cybersécurité de la Confédération. Il n'est pas question ici uniquement de l'infrastructure informatique fédérale : la protection des informations et des données de la Confédération doit être garantie aussi auprès des tiers, des cantons et des partenaires internationaux. Ainsi, les entreprises privées et les organisations publiques qui assument un mandat public au sens des art. 2, al. 3, et 5 LSI sont soumises non seulement à la LPD, mais aussi à la LSI. Bien que les lois cantonales sur la protection des données soient applicables, les organes publics cantonaux sont également soumis à la LSI lorsqu'ils ont accès aux moyens informatiques de la Confédération, à condition qu'ils ne garantissent pas une sécurité au moins équivalente de l'information (art. 3 LSI). Si les autorités et organisations soumises à la LSI collaborent avec des tiers, elles veillent à ce que les exigences et mesures prévues par la loi soient reprises dans les accords et contrats qu'elles concluent à cet effet (art. 9 LSI).

La LSI et l'OSI proposent des directives efficaces et modernes en matière de cybersécurité, car plusieurs dispositions (art. 6 à 23 LSI) indiquent comment mettre en place un système de management de la sécurité de l'information (SMSI).

- Les autorités et organisations concernées doivent évaluer le besoin de protection (art. 6 LSI) des informations qu'elles traitent et classifier ces dernières (art. 11 à 15 LSI).
- Pour protéger ces informations, il faut veiller à prendre des mesures appropriées contre les accès non autorisés, les pertes, les perturbations et les utilisations abusives (art. 6 à 10 LSI).
- Les autorités et organisations soumises à la LSI doivent veiller à ce que les risques en matière de sécurité de l'information soient constamment évalués (art. 8 LSI).
- Si des moyens informatiques sont utilisés (p. ex., selon l'art. 5 LSI, les applications, les systèmes d'information, les fichiers ainsi que les installations, les produits et les services servant au traitement électronique des informations), une procédure de sécurité doit être mise en place afin de garantir la sécurité des informations. Une catégorie de sécurité définissant les exigences minimales et les mesures de sécurité (« protection de base », « protection élevée », « protection très élevée ») doit être attribuée aux moyens informatiques (art. 16 à 19 LSI).
- Il faut veiller à ce que les personnes qui accèdent à des informations, à des moyens informatiques, à des locaux et à d'autres infrastructures de la Confédérations soient choisies avec soin et qu'elles soient identifiées en fonction de la sensibilité de l'activité concernée (art. 20

LSI). Le personnel doit recevoir une formation et une formation continue adaptées à son niveau de responsabilité et, le cas échéant, être tenu au maintien du secret.
- Les autorités et organisations soumises à la LSI doivent veiller à assurer une protection physique adéquate des informations et moyens informatiques. Les locaux et les espaces peuvent être classés en zones de sécurité, lesquelles impliquent des contrôles prenant par exemple la forme de fouilles (art. 22 et 23 LSI).

Le 29 septembre 2023, le Parlement a adopté une modification de la LSI introduisant une obligation de signaler les cyberattaques contre les infrastructures critiques. Ce projet crée les bases légales pour soumettre les exploitants d'infrastructures critiques à une obligation de signalement et définit les tâches de l'OFCS en la matière, lequel doit servir de centre de signalement pour cyberattaques. Cette obligation n'est pas encore en vigueur, car des dispositions d'exécution doivent être édictées pour sa mise en œuvre. Le Conseil fédéral n'a pas encore fixé leur date d'entrée en vigueur.

## 2.3 Résultat de l'examen

Au vu des informations, instructions et directives des autorités, des directives en matière de cybersécurité basées sur des ordonnances et des dispositions légales relatives à la protection des données et des informations présentées dans le présent rapport, il existe aujourd'hui en Suisse de nombreuses mesures de protection informatique proposées par les autorités ou juridiquement contraignantes. Les organisations chargées d'une mission de service public peuvent ou doivent y recourir afin d'améliorer la cybersécurité et de garantir une protection contre les attaques par rançongiciel.

En raison de la répartition constitutionnelle des compétences entre la Confédération et les cantons, la Confédération n'a en principe pas la possibilité, compte tenu de l'autonomie des cantons et des communes, d'édicter des mesures de cybersécurité juridiquement contraignantes à des organisations qui sont chargées d'une mission de service public en vertu du droit cantonal ou communal et qui ne sont soumises ni à la LPD ni à la LSI. En d'autres termes, l'autonomie des cantons et des communes signifie que, faute de base constitutionnelle dans le domaine cyber, la Confédération ne peut ni édicter de prescriptions légales ni exercer une surveillance sur la mise en œuvre de mesures de protection, et que la responsabilité quant à la mise en œuvre des mesures de protection correspondantes incombe aux autorités cantonales ou communales. Par conséquent, les cantons et les communes doivent en principe définir et mettre en œuvre de manière autonome des règles et des mesures pour protéger leurs infrastructures informatiques. C'est pourquoi la plupart des cantons disposent de leurs propres stratégies ou concepts de cybersécurité, qui s'inspirent parfois de la CSN et fixent des directives pour la mise en œuvre de mesures de cyberprotection. Par ailleurs, les autorités ou les législateurs cantonaux et communaux peuvent également s'inspirer du contenu des informations, des instructions et des directives susmentionnées de la Confédération.

Le Conseil fédéral estime qu'il n'est pas judicieux d'introduire des directives juridiquement contraignantes à l'échelle nationale pour les organisations chargées d'une mission de service public en ce qui concerne la protection de base contre les attaques par rançongiciel, la Confédération faisant déjà beaucoup pour garantir une résilience face aux cyberattaques et, par conséquent, aux attaques par rançongiciel. Il apporte son soutien dans ce domaine, informe en toute transparence, met en place des mesures incitatives ou intervient dans des questions de réglementation dans le cadre de la répartition des compétences fixée dans la Constitution et les bases légales fédérales, comme il l'a fait récemment pour les infrastructures d'approvisionnement en électricité et de conduites en raison de leur importance économique. Dans ce contexte, des échanges intensifs sont systématiquement recherchés avec les acteurs concernés en vue d'une étroite collaboration.

# 3 Introduction d'une obligation de signaler en cas de paiement de rançons et d'une obligation d'impliquer les autorités dans les négociations avec les criminels

Le renforcement de la protection contre les cyberattaques est le principal moyen de prévenir les attaques par rançongiciel. Toutefois, des attaques abouties ne peuvent être exclues, même avec des mesures de protection. Par conséquent, il convient d'élaborer la réaction aux attaques par rançongiciel de manière à éviter autant que possible les dommages et à compliquer les agissements des malfaiteurs. La question essentielle est de savoir comment limiter au maximum les paiements de rançons en cas d'attaques par rançongiciel[38]. Si le versement d'une rançon peut permettre aux organisations visées par l'attaque de résoudre leur problème, cela contribue en revanche au succès et à la poursuite du développement du modèle économique des cybercriminels. Cette réponse a pour conséquence d'accroître non seulement les capacités des cybercriminels, mais aussi l'attrait de la Suisse comme cible potentielle et donc, en fin de compte, la menace de cyber-extorsion.

Le postulat 21.4512 Graf-Litscher demande à cet égard au Conseil fédéral de déterminer s'il est possible de contrer de telles fausses incitations en introduisant une obligation de déclaration en cas de paiement de rançons ainsi qu'une obligation d'impliquer les autorités dans les négociations avec les criminels.

Le présent chapitre examine tout d'abord les bases légales existantes en matière de paiement de rançons lors d'attaques par rançongiciel, puis dresse un état des lieux dans d'autres États dans le cadre d'une brève comparaison juridique, avant de décrire et d'évaluer les options dont dispose la Suisse.

## 3.1 Bases légales existantes

Afin de déterminer si les mesures à examiner doivent être introduites, il convient de clarifier les bases légales actuelles qui doivent être respectées lors du paiement de rançons en cas d'attaques par rançongiciel. L'accent est mis sur les conséquences pénales potentielles en cas de paiement de rançon ainsi que sur les éventuelles obligations de signaler.

### 3.1.1 Conséquences pénales potentielles en cas de paiement de rançon

En Suisse, il n'existe aucune interdiction générale de verser une rançon en cas d'attaque par rançongiciel ; de tels agissements ne donnent donc en principe lieu à aucune sanction[39]. Il convient

[38] Cf. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html ; consulté pour la dernière fois le 20 octobre 2024. Le taux de réussite de la récupération des données après le paiement d'une rançon n'est apparemment pas aussi élevé que le souhaiteraient les entreprises concernées. Les statistiques montrent que la récupération des données n'est en aucun cas garantie. Selon le rapport de Sophos intitulé L'état des ransomwares 2023, seuls 58 % des organisations ont pu récupérer leurs données après le paiement d'une rançon. Parmi celles qui ont payé une rançon, 21 % seulement ont pu récupérer l'intégralité de leurs données, tandis que 37 % n'en ont récupéré qu'une partie. Cela montre que même en répondant aux demandes de rançon, les organisations ne sont en aucun cas assurées de récupérer l'ensemble de leurs données. De plus, le paiement d'une rançon peut également augmenter la probabilité d'être à nouveau la cible d'une attaque. Selon le même rapport de Sophos, 80 % des organisations qui ont payé une rançon ont subi une autre attaque par rançongiciel, souvent par le même groupe (site internet : https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/ ; consulté pour la dernière fois le 20 octobre 2024).

[39] Cf. FABIAN TEICHMANN/LÉONARD GERBER, Les cyberattaques par spyware – Poursuite et qualification en droit pénal suisse, dans : Sécurité & Droit 3/2021 ; OLIVER M. BRUPBACHER/CLAUDIA GÖRTZ STAEHELIN, Herausforderungen durch Cybersecurity in der modernen Unternehmensrealität, dans : RSJ 118/2022, p. 518 ; YANIV BENHAMOU/LOUISE WANG, Cyberattaque et ransomware : risques juridiques à payer et assurabilité des rançons, dans : RSDA 2023, p. 83 : « En droit suisse, aucun texte ne sanctionne expressément le paiement de la rançon par la victime » ; DELPHINE SARASIN/SARA PANGRAZZI/PAULINE MEYER, The Legal Risks of Ransomware Payments, dans : PJA 2023, p. 1080.

toutefois de noter que le paiement d'une rançon peut entraîner les conséquences pénales ci-dessous pour la victime[40].

- *(Complicité de) blanchiment d'argent (art. 305bis CP[41])* : les auteurs d'attaques par rançongiciel exigent souvent des paiements en cryptomonnaie, qui sont généralement effectués sous un pseudonyme. La question qui se pose est donc de savoir si un tel paiement de rançon ne peut pas être considéré comme du blanchiment d'argent – ou de la complicité de blanchiment d'argent – (art. 305bis CP). Ce d'autant que l'entreprise[42] voire, le cas échéant, les banques mandatées savent ou peuvent partir du principe que les sommes versées serviront à des activités illégales et qu'il sera donc probablement question de blanchiment d'argent. Cette problématique n'a pas encore été clarifiée par la jurisprudence fédérale. Par ailleurs, il faudrait examiner au cas par cas dans quelle mesure la partie qui paie la rançon peut invoquer comme justificatif un état de nécessité licite (art. 17 CP) ou un état de nécessité excusable (art. 18 CP)[43].
- *Soutien à une organisation criminelle (art. 260ter CP) et financement du terrorisme (art. 260quinquies CP)* : si des organisations criminelles ou des groupes terroristes génèrent de l'argent en ayant recours à la cyber-extorsion de fonds, il convient également d'examiner les éléments constitutifs du soutien à une organisation criminelle (art. 260ter CP) et du financement du terrorisme (art. 260quinquies CP). Contrairement au financement du terrorisme, il suffit, dans le cas du soutien à une organisation criminelle, que l'entreprise s'attende, au moins par dol éventuel, à ce que le paiement de la rançon serve l'objectif criminel de l'organisation. Pour les personnes contraintes à des actes de soutien comme le paiement de rançons, l'état de nécessité licite (art. 17 CP) ou l'état de nécessité excusable (art. 18 CP) entrent en ligne de compte comme justificatifs[44]. Cette question n'a pas non plus été clarifiée à ce jour par la jurisprudence fédérale. Il convient de mentionner à cet égard que le paiement d'une rançon pourrait enfreindre des sanctions et des mesures internationales de lutte contre le financement du terrorisme ou des embargos imposés[45].

### 3.1.2 Absence d'obligation de signaler le paiement d'une rançon en cas d'attaque par rançongiciel ou d'impliquer les autorités dans les négociations

En Suisse, il n'est pas obligatoire de signaler aux autorités le paiement d'une rançon en cas d'attaque par rançongiciel, et aucune disposition légale n'oblige les entreprises ou les particuliers à impliquer les autorités dans les négociations avec les auteurs de telles attaques. Autrement dit, la décision de consulter ou d'informer les pouvoirs publics, et sous quelle forme, est laissée à la discrétion de l'entreprise touchée ou de l'individu concerné.

---

40 La question de la punissabilité des auteurs d'attaques par rançongiciel ne faisant pas l'objet des présents éclaircissements juridiques, nous nous contentons d'énumérer ci-dessous la liste des délits qu'ils pourraient éventuellement avoir commis en demandant une rançon : art. 143 (Soustraction de données), art. 143bis (Accès indu à un système informatique), art. 144bis, ch. 1 (Détérioration de données), art. 144bis, ch. 2 (Fabrication de logiciels dans le but de détériorer des données), art. 147 (Utilisation frauduleuse d'un ordinateur), art. 156 (Extorsion et chantage), art. 179novies (Soustraction de données personnelles) et art. 260ter (Organisations criminelles) CP ; voir aussi SANDRO GERMANN/DAVID WICKI-BIRCHLER, Hacking und Hacker im Schweizer Recht, dans : PJA 2020, p. 87 ss ; TEICHMANN/GERBER, loc. cit., p. 124, ss et BENHAMOU/WANG, loc. cit., p. 81, ss).

41 RS **311.0**

42 Selon l'art. 102, al. 1, CP, une entreprise (cf. définition légale à l'art. 102, al. 4, let. a à d, CP) peut également s'exposer à des sanctions pénales dans la mesure où un crime ou un délit qui est commis au sein d'une entreprise dans l'exercice d'activités commerciales conformes à ses buts est imputé à l'entreprise s'il ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise. L'art. 102, al. 2, CP précise qu'en cas d'infraction prévue notamment aux art. 260ter, 260quinquies et 305bis CP, l'entreprise est punie indépendamment de la punissabilité des personnes physiques s'il doit lui être reproché de ne pas avoir pris toutes les mesures d'organisation raisonnables et nécessaires pour empêcher une telle infraction (voir aussi SARASIN/PANGRAZZI/MEYER, loc. cit., p. 1084).

43 BRUPBACHER/GÖRTZ STAEHELIN, loc. cit., p. 518 ss ; BENHAMOU/WANG, loc. cit., p. 83 ; SARASIN/PANGRAZZI/MEYER, loc. cit., p. 1082 ss.

44 Voir aussi BRUPBACHER/GÖRTZ STAEHELIN, loc. cit., p. 519 ss ; BENHAMOU/WANG, loc. cit., p. 83 ss ; ainsi que SARASIN/PANGRAZZI/MEYER, loc. cit., p. 1080 ss.

45 Ainsi, une autorité étrangère pourrait p. ex. considérer le paiement d'une rançon par une personne relevant d'une juridiction étrangère comme une infraction à des sanctions et imposer des poursuites civiles sur la base d'une responsabilité objective. Les entreprises pourraient ainsi s'exposer à des contrôles de la part des autorités ou à des poursuites judiciaires, ce qui pourrait nuire à leurs activités futures dans des pays soumis à de telles réglementations.

Mesures **contre les attaques par rançongiciel**

Les cyberattaques doivent être signalées aux autorités comme suit.

- *Signalements en cas de violation de la sécurité de données conformément à la législation en matière de protection des données* : la révision de la loi sur la protection des données (LPD) et l'ordonnance sur la protection des données (OPDo) prévoient les exigences susmentionnées relatives aux mesures techniques et organisationnelles de cybersécurité[46]. Les cas de violations de la sécurité des données (*data breach*) qui entraînent vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, lesquels se produisent généralement aussi en cas d'attaque par rançongiciel, doivent être signalés au Préposé fédéral à la protection des données et à la transparence (PFPDT) conformément à l'art. 24, al. 1, LPD. Ainsi, les violations de la sécurité des données entraînant la perte, la suppression, la destruction ou la modification involontaire ou illicite de données personnelles, leur divulgation ou leur mise à disposition à des personnes non autorisées et qui sont susceptibles d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées doivent être signalées au PFPDT. Ce dernier a créé un formulaire d'annonce électronique[47] pour indiquer le contenu énuméré à l'art. 24, al. 2, LPD, et à l'art. 15, al. 1, let. a à g, OPDo. En particulier, l'art. 15, al. 1, let. a, OPDo prévoit l'annonce de la nature de la violation, et l'art. 15, al. 1, let. f, OPDo, celle des mesures prises ou prévues pour remédier à cette défaillance et atténuer les conséquences, y compris les risques éventuels. Conformément à l'art. 24, al. 4, LPD, le responsable du traitement informe la personne concernée lorsque cela est nécessaire à sa protection ou que le PFPDT l'exige.
- *Obligation de signaler les cyberattaques pour les entreprises soumises à la surveillance de la FINMA* : les entreprises soumises à la surveillance de la FINMA sont légalement tenues de lui signaler toute cyberattaque. Cette réglementation vise à garantir l'intégrité et la stabilité du marché financier suisse. L'obligation de signaler inclut différents types de cyberattaques, y compris les celles par rançongiciel. Lors du signalement d'une attaque, les entreprises concernées sont tenues de fournir des informations détaillées afin de permettre à la FINMA de procéder à une évaluation globale de la situation, à savoir le type d'attaque, la date de l'incident, les systèmes et les données concernés ainsi que les conséquences probables sur l'activité commerciale. La description des mesures prises pour endiguer et remédier à l'attaque est tout aussi importante. Ces informations aident la FINMA à évaluer le risque pour l'ensemble du système financier et, le cas échéant, à proposer des mesures supplémentaires de soutien ou de réglementation. Par ailleurs, les entreprises doivent expliquer quelles mesures préventives ont été mises en œuvre pour éviter des incidents similaires à l'avenir. Cette transparence est essentielle pour renforcer la confiance à l'égard des marchés financiers et favoriser la résilience face aux cybermenaces. La FINMA surveille étroitement le respect de ces règles et peut imposer des sanctions en cas de non-respect, ce qui souligne l'importance de l'obligation de signaler[48].
- *Obligation de signaler les cyberattaques contre des infrastructures critiques* : les dispositions des art. 74*a* ss LSI[49], qui entreront vraisemblablement en vigueur en 2025, prévoient une obligation de signaler pour les exploitants d'infrastructures critiques en cas de cyberattaque. L'art. 74*e*, al. 2, LSI précise le contenu du signalement, à savoir les informations-clés

---

46 Cf. ch. 2.2.5 ci-dessus, p. 11.

47 Cf. https://databreach.edoeb.admin.ch/report ; consulté pour la dernière fois le 20 octobre 2024.

48 Cf. Communication FINMA sur la surveillance 05/2020 du 7 mai 2020 – Obligation de signaler les cyberattaques selon l'art. 29, al. 2, LFINMA (cf. site internet : https://www.finma.ch/fr/documentation/dossier/dossier-cyberrisiken/~/media/a2e26e3b011c4c02a297ff3ac322313f.ashx ; consulté pour la dernière fois le 20 octobre 2024), qui se fonde sur l'art. 29, al. 2, de la loi sur la surveillance des marchés financiers (LFINMA ; RS **956.1**) et a été précisée par la FINMA dans la Circulaire 2023/1 – Risques et résilience opérationnels – banques (cf. site internet : https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=fr&hash=3DA82629BEBD5388845AB8FD93121801 ; consulté pour la dernière fois le 20 octobre 2024) ainsi que dans la Communication FINMA sur la surveillance 3/2024 – Enseignements tirés de l'activité de surveillance des cyberrisques, précisions sur la communication FINMA sur la surveillance 05/2020 et sur les cyberexercices fondés sur des scénarios (cf. site internet : https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=fr&hash=666EEE255C04FB42F01BFD0BC6C80191 ; consulté pour la dernière fois le 20 octobre 2024).

49 La date d'entrée en vigueur n'a pas encore été déterminée par le Conseil fédéral au moment de la rédaction du présent rapport.

nécessaires pour remplir l'obligation de signaler. L'étendue concrète et le contenu des informations à signaler seront précisés dans la future ordonnance sur la cybersécurité et repris par l'OFCS dans un formulaire sur sa plateforme d'échange d'informations (Cyber Security Hub). Ce formulaire décrira par ailleurs en détail ce qu'il faut entendre par *informations à signaler*. L'art. 19, al. 1, let. c, d et e, du projet d'ordonnance sur la cybersécurité exige le signalement du type et des méthodes d'attaque ainsi que des données sur l'attaquant. L'accès non autorisé et l'utilisation de logiciels malveillants sont cités en exemple dans les explications. Par ailleurs, l'art. 19, al. 2, du projet d'ordonnance sur la cybersécurité[50] précise que le signalement doit aussi contenir des informations sur l'éventualité d'un chantage en lien avec la cyberattaque. La divulgation de tentatives d'extorsion ou de menaces liées à une cyberattaque peut contribuer à alerter d'autres victimes potentielles et à la mise en œuvre de mesures dans le but de prévenir des incidents similaires. Il ne sera pas demandé d'indiquer si le versement d'une rançon a été effectué ou est prévu[51].

Même si une attaque par rançongiciel est signalée aux autorités susmentionnées et que des entreprises ou des particuliers demandent de l'aide pour négocier avec les attaquants, il convient de respecter le principe de la légalité. Autrement dit, le PFPDT, la FINMA ou l'OFCS n'ont aucune obligation d'assistance à cet égard.

## 3.2 Analyse de droit comparé

Les conditions-cadres juridiques régissant la gestion de paiements de rançons en cas d'attaques par rançongiciel et l'obligation d'impliquer les autorités dans les négociations avec les attaquants ne varient guère d'un pays à l'autre. Il existe de nombreux points communs dans les réglementations respectives en ce qui concerne l'obligation de signaler tout paiement de rançon et l'obligation d'impliquer les autorités dans les négociations avec les attaquants. Dans le cadre d'une comparaison internationale, les obligations de signaler les paiements de rançons ou d'impliquer les autorités sont brièvement expliquées ci-après pour les États-Unis, qui jouent un rôle de pionnier dans la lutte contre les attaques par rançongiciel, ainsi que pour deux de nos pays voisins, la France et l'Allemagne. Cette analyse des conditions-cadres juridiques dans ces trois pays offre une vue d'ensemble des approches adoptées dans les principaux pays industrialisés et permet d'identifier les meilleures pratiques ainsi que d'en déduire des améliorations potentielles pour notre propre législation.

### 3.2.1 Absence d'obligation de signaler le paiement d'une rançon en cas d'attaque par rançongiciel

À l'instar de la Suisse, de nombreux pays ont déjà mis en place – ou du moins prévu – des obligations de signaler les cyberattaques. Il n'existe en revanche aucune obligation de signaler les paiements de rançons. Les réglementations relatives à l'obligation de signaler se présentent comme suit dans les pays susmentionnés.

- *États-Unis* : comme en Suisse, le paiement d'une rançon après une attaque par rançongiciel n'est ni interdit ni soumis à une obligation de signaler, mais il est punissable dans certaines situations s'il est destiné à des personnes faisant l'objet de blocus ou de sanctions en vertu du droit américain, ou en cas d'infraction à l'interdiction du blanchiment d'argent. Le non-respect de ces règles peut entraîner des sanctions civiles fondées sur une responsabilité stricte, indépendamment de la prise de conscience du fait de s'engager dans une transaction avec

[50] Cf. site internet : https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2024/35/cons_1/doc_1/fr/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2024-35-cons_1-doc_1-fr-pdf-a.pdf ; consulté pour la dernière fois le 20 octobre 2024.

[51] Rapport explicatif concernant le projet d'ordonnance sur la cybersécurité, p. 29 ss (site internet : https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2024/35/cons_1/doc_2/fr/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2024-35-cons_1-doc_2-fr-pdf-a.pdf ; consulté pour la dernière fois le 20 octobre 2024).

une personne faisant l'objet de sanctions américaines. C'est pourquoi l'Office américain de contrôle des actifs étrangers (*Office of Foreign Assets Control*, OFAC) encourage les victimes et les personnes impliquées dans la gestion d'attaques par rançongiciel à prendre immédiatement contact avec l'OFAC si elles soupçonnent une demande de paiement en cas d'attaque par rançongiciel d'avoir un quelconque lien avec des sanctions. Les victimes devraient également contacter l'Agence de cybersécurité et de sécurité des infrastructures (*Cybersecurity and Infrastructure Security Agency*, CISA) si une attaque devait toucher une institution financière américaine ou pourrait avoir un impact significatif sur la capacité d'une entreprise à fournir des services financiers critiques[52].

- *Allemagne* : selon l'Office fédéral de la police judiciaire (*Bundeskriminalamt*, BKA), il n'existe en Allemagne aucune interdiction de payer une rançon en cas d'attaque par rançongiciel ; les autorités conseillent toutefois de ne pas répondre aux demandes de rançon[53]. Depuis le 15 septembre 2017, l'Autorité allemande de supervision financière (*Bundesanstalt für Finanzdienstleistungsaufsicht*, BaFin) autorise expressément les compagnies d'assurance à couvrir les paiements de rançons sous certaines conditions[54]. Par ailleurs, il n'existe aucune obligation légale spécifique de signaler le paiement d'une rançon après une attaque par rançongiciel ; les entreprises sont toutefois encouragées à signaler les incidents en lien avec la sécurité informatique[55].
- *France* : la situation est similaire à celle de la Suisse. Le paiement d'une rançon après une attaque par rançongiciel n'est pas interdit en soi. Les autorités le déconseillent toutefois, car cela peut encourager davantage les activités criminelles. Dans certaines situations, le paiement d'une rançon peut constituer une infraction de financement du terrorisme si la victime sait que les fonds seront utilisés pour un acte terroriste. Le Haut comité juridique de la place financière de Paris (HCJP) a notamment retenu à cet égard, dans un rapport du 28 janvier 2022, que les entreprises du secteur financier doivent être soumises à des règles particulières dans le cadre de leurs activités et déclarer ou s'abstenir de toute transaction impliquant des fonds dont elles soupçonnent ou ont de bonnes raisons de penser qu'ils proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou qu'ils sont liés au financement du terrorisme[56].

### 3.2.2 Obligation d'impliquer les autorités dans les négociations avec les auteurs d'attaques par rançongiciel

Une comparaison juridique concernant l'obligation d'impliquer les autorités publiques dans les négociations avec les auteurs d'attaques par rançongiciel montre ce qui suit.

- *États-Unis* : il n'existe aucune obligation d'impliquer les autorités dans les négociations avec les auteurs d'attaques par rançongiciel. L'OFAC, le *Federal Bureau of Investigation* (FBI), la CISA, le *Secret Service* et d'autres autorités (de poursuite pénale) recommandent toutefois de coopérer avec eux dans les affaires d'attaques par rançongiciel. En effet, cela peut constituer

---

52 Cf. BENHAMOU/WANG, loc. cit., p. 86 ; OFAC, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, 1er octobre 2020 (site internet : https://ofac.treasury.gov/media/48301/download?inline ; consulté pour la dernière fois le 20 octobre 2024) et OFAC, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, 21 septembre 2021 (site internet : https://ofac.treasury.gov/media/912981/download?inline ; consulté pour la dernière fois le 20 octobre 2024) ainsi que SARASIN/PANGRAZZI/MEYER, LOC. CIT., p. 1089.

53 Cf. site internet : https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/DigitaleErpressung/digitaleErpressung_node.html ; consulté pour la dernière fois le 20 octobre 2024.

54 Cf. site internet : https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html ; consulté pour la dernière fois le 20 octobre 2024, avec renvoi à la circulaire 3/1998 (VA) – Hinweise des BAV zum Betrieb von Lösegeldversicherungen ci-dessus (site internet : https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_9803_va_loesegeldversicherung.html;jsessionid=0AA1AC030FE93BF2BB27BE3F90E9BCA8.internet972?nn=19659504 ; consulté pour la dernière fois le 20 octobre 2024).

55 Cf. site internet de l'Office fédéral de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) : https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?nn=133680&cms_pos=4 ; consulté pour la dernière fois le 20 octobre 2024.

56 Cf. HCJP, Rapport sur l'assurabilité des risques cyber, 28 janvier 2022 (site internet : https://www.banque-france.fr/system/files/2023-10/rapport_45_f.pdf ; consulté pour la dernière fois le 20 octobre 2024).

une circonstance atténuante eu égard à la peine si le paiement de la rançon est considéré comme un acte de blanchiment d'argent[57]. Les autorités encouragent les victimes d'attaques par rançongiciel à signaler ces dernières. L'incident ne doit être signalé qu'une seule fois, car des interfaces permettent d'informer les autorités susmentionnées[58].

- *Allemagne* : les autorités de poursuite pénale allemandes, en particulier les offices régionaux de la police judiciaire (*Landeskriminalämter*, LKA) et le BKA, conseillent aux victimes de coopérer avec les autorités en cas d'attaque par rançongiciel. Il n'existe aucune obligation légale, mais il est précisé que coopérer peut augmenter les chances de succès des poursuites[59].
- *France* : aucune obligation n'impose d'impliquer les autorités dans les négociations avec les auteurs d'attaques par rançongiciel. Les autorités de poursuite pénale françaises, y compris la Police nationale et la Gendarmerie nationale, recommandent vivement de coopérer avec elles en cas d'attaque par rançongiciel afin d'accroître l'efficacité des poursuites et de la prévention[60].

### 3.2.3 Résultat de l'analyse de droit comparé

La comparaison juridique ci-dessus montre que les pays sélectionnés ne prévoient aucune interdiction du paiement de rançons en cas d'attaque par rançongiciel, ni aucune obligation spécifique de signalement aux autorités. Ces dernières ne sont pas tenues de participer aux négociations en cas d'attaque par rançongiciel, mais il est recommandé de leur signaler de telles attaques et de coopérer avec elles. De nombreux États discutent certes d'une réglementation plus stricte des paiements de rançons en cas d'attaques par rançongiciel[61], mais aucun pays comparable à la Suisse n'a introduit de telles mesures.

## 3.3 Possibilités législatives en Suisse

En Suisse, il n'existe actuellement aucune interdiction de payer une rançon en cas d'attaque par rançongiciel, ni aucune obligation légale spécifique de signaler de tels paiements en cas d'attaque par rançongiciel ou dans d'autres cas de cyber-extorsion. Il n'est par ailleurs pas légalement obligatoire d'impliquer les autorités dans les négociations avec les criminels et, par conséquent, il n'existe aucun droit à une quelconque assistance à cet égard de la part des autorités. Les avantages et les inconvénients liés au maintien du statu quo ainsi qu'à la création de nouvelles bases légales en vue de l'introduction de l'obligation de signaler et de l'obligation d'impliquer les autorités dans les négociations relatives à une rançon sont examinés ci-après. En dernier lieu, la possibilité d'instaurer une interdiction légale de paiement de rançons en cas d'attaques par rançongiciel est également abordée.

---

57 Cf. OFAC, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, 1er octobre 2020 (site internet : https://ofac.treasury.gov/media/48301/download?inline ; consulté pour la dernière fois le 20 octobre 2024) et OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (site internet : https://ofac.treasury.gov/media/912981/download?inline ; consulté pour la dernière fois le 20 octobre 2024).

58 L'Internet Crime Complaint Center (IC3) fournit p. ex. au public un mécanisme de signalement fiable et pratique pour transmettre des informations sur des activités criminelles présumées sur internet. Le site internet suivant permet aussi d'envoyer un rapport directement au FBI : https://ransomware.ic3.gov/default ; consulté pour la dernière fois le 3 juillet 2024. Il est également possible de signaler une attaque par rançongiciel directement à la CISA sur le site internet suivant : https://www.cisa.gov/forms/report ; consulté pour la dernière fois le 20 octobre 2024.

59 Cf. site internet : https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/DigitaleErpressung/digitaleErpressung_node.html ; consulté pour la dernière fois le 20 octobre 2024.

60 Cf. site internet : https://www.internet-signalement.gouv.fr/PharosS1/ ; consulté pour la dernière fois le 20 octobre 2024, et le site internet : https://www.service-public.fr/particuliers/vosdroits/N31138 ; consulté pour la dernière fois le 20 octobre 2024.

61 Cf. discussions au Royaume-Uni (U.K. Government To Consider Licensing Ransomware Payments | Lawfare (lawfaremedia.org)), en Australie (Australia : New Law in Australia will require mandatory reporting of ransomware payments (therecord.media)) ou aux États-Unis (Proposed Legislation Would Add Ransomware Reporting and Compliance Obligations for Covered U.S. Financial Institutions, Brock Dahl, David Sewell, Nathaniel Balk, David Benger (freshfields.us)).

### 3.3.1 Maintien des réglementations actuelles (absence de mesures spécifiques)

Le maintien des réglementations actuelles repose sur une évaluation minutieuse des avantages et des moyens à mettre en œuvre. Un aspect-clé réside dans l'efficacité des obligations de signaler supplémentaires par rapport à la charge administrative correspondante pour les entreprises et les autorités. Une cyberattaque aboutie peut se révéler extrêmement éprouvante pour les personnes concernées. Dans une telle situation, une action rapide et flexible s'avère souvent décisive. Des contraintes supplémentaires pourraient compliquer la gestion de cette phase critique sans nécessairement garantir de meilleurs résultats. Du côté des autorités, des ressources considérables seraient nécessaires pour traiter efficacement les signalements et y réagir en temps utile. Il n'est pas certain que les efforts requis soient proportionnels aux avantages potentiels, notamment au vu des obligations déjà en vigueur de signaler les cyberincidents. Le cadre juridique actuel permet par ailleurs de développer des solutions adaptées au marché, par exemple en collaboration avec des compagnies d'assurance, sans toutefois les restreindre par des réglementations supplémentaires. Si une obligation de signaler les paiements de rançons s'avérait nécessaire à l'avenir, il faudrait d'abord créer une base légale appropriée. La décision de ne pas imposer une telle obligation à ce stade repose sur l'avis selon lequel les mesures existantes sont actuellement les plus efficaces pour relever les défis liés aux attaques par rançongiciel.

Le statut quo inclut toutefois le problème fondamental de la mauvaise incitation au paiement de rançons. Cette pratique reste dans de nombreux cas une solution bon marché et rapide pour les personnes concernées, mais aggrave en même temps le problème pour toutes les autres, les cybercriminels étant ainsi encouragés à lancer d'autres attaques par rançongiciel. Cette dynamique affecte l'ensemble de la société, le nombre accru d'attaques affaiblissant la sécurité générale et la résistance à la cybercriminalité. De plus, les paiements de rançons ne sont pas divulgués. Ce manque de transparence quant à l'ampleur des attaques par rançongiciel complique la mise en place de stratégies globales par les autorités chargées de la poursuite pénale et de la cybersécurité pour lutter contre ces menaces. Même en cas de maintien du statu quo, des mesures doivent donc être mises en œuvre afin de permettre une meilleure évaluation de l'impact de telles attaques.

### 3.3.2 Introduction d'obligations de signaler les attaques par rançongiciel et les paiements de rançons, soutien de l'État lors de négociations

Compte tenu de la fréquence des attaques par rançongiciel, il est possible d'affirmer que des mesures législatives s'imposent dans l'optique d'empêcher le paiement de rançons, par exemple l'introduction d'obligations de signaler ou d'impliquer les autorités dans les négociations. Les avantages d'une telle solution résident en premier lieu dans l'effet dissuasif escompté. Si les entreprises étaient obligées de déclarer les paiements de rançons, elles devraient faire preuve de transparence. Il ne serait plus possible de gérer l'incident de sécurité en payant secrètement les criminels. Le paiement de rançons perdrait ainsi de son attrait pour les victimes. Par ailleurs, le recours obligatoire aux autorités a un effet dissuasif sur les malfaiteurs, ces derniers souhaitant généralement éviter de traiter directement avec la police. Si les criminels savent que les autorités de poursuite pénale sont automatiquement impliquées à chaque attaque, cela pourrait avoir pour conséquence que les entreprises suisses soient perçues comme des cibles moins attrayantes en raison de l'augmentation du risque pour les attaquants d'être identifiés.

Outre ces effets dissuasifs, une obligation de signaler crée une plus grande transparence en ce qui concerne les cyberattaques en donnant aux autorités un aperçu détaillé de l'ampleur, des dimensions financières et des tactiques utilisées par les pirates. Cela permettrait de développer des mesures

préventives plus ciblées et d'identifier les vulnérabilités de l'infrastructure numérique afin d'empêcher de futures attaques.

L'introduction de charges administratives supplémentaires pourrait toutefois soumettre les entreprises à une pression excessive, notamment les plus petites, et nuire à l'efficacité de la gestion des incidents. Dans l'ensemble, les mesures entraînent également un certain stress pour les victimes. Outre les préjudices directs occasionnés par les attaques, les mesures devraient également satisfaire à des exigences légales, ce qui nécessiterait des ressources supplémentaires. Par ailleurs, une telle réglementation rendrait le rôle de l'État plus difficile. D'une part, les autorités recommanderaient de ne pas verser de rançon afin de ne pas encourager davantage les criminels. D'autre part, ces mêmes autorités agiraient comme centre de compétences pour les négociations avec les criminels, créant en quelque sorte un conflit d'intérêts. Ce double rôle pourrait non seulement engendrer confusion et incertitude pour les entreprises concernées, mais aussi saper l'efficacité des recommandations de l'État.

Une autre solution que l'introduction d'obligations de signaler les paiements de rançons serait une obligation simplifiée pour les entités qui paient des rançons pour le compte de tiers en cas d'attaques par rançongiciel ou qui les font couvrir par une assurance. Cette variante présenterait les avantages suivants : premièrement, cette obligation de signaler simplifiée éviterait de pénaliser les victimes d'attaques par rançongiciel ou de leur imposer un stress supplémentaire, la responsabilité du signalement étant alors transférée aux prestataires ou aux assureurs versant la rançon. Cela éviterait de soumettre les entreprises et les particuliers ayant déjà à endurer l'attaque à des contraintes bureaucratiques supplémentaires. Deuxièmement, une telle obligation de signaler permettrait d'avoir une meilleure vue d'ensemble des rançons versées. Les autorités pourraient tenir des statistiques détaillées sur la fréquence et le montant des paiements, ce qui permettrait de recueillir de précieuses données pour la lutte contre la cybercriminalité. Cette transparence pourrait contribuer à améliorer les mesures préventives sur la base de données fiables et permettre de développer des stratégies ciblées dans le but de réduire les attaques par rançongiciel.

Toutefois, cette variante d'obligation simplifiée présente également des inconvénients : l'introduction d'une telle obligation de signaler entraînerait des contraintes bureaucratiques supplémentaires, tant pour les entreprises d'assurance que pour les prestataires versant la rançon (p. ex. intermédiaires financiers). Ces derniers devraient mettre en place de nouveaux processus et systèmes pour garantir la déclaration en bonne et due forme de l'ensemble des paiements de rançons. Un autre inconvénient résiderait dans la possibilité de contourner cette réglementation en ayant recours à des assurances et à des prestataires étrangers qui ne sont pas soumis à l'obligation de signaler en Suisse. Cela pourrait avoir pour conséquence qu'une partie des paiements de rançons ne soit pas divulguée et que la transparence souhaitée ne soit pas totalement atteinte. En outre, une telle réglementation créerait des désavantages concurrentiels pour les assureurs suisses, les autres pays ne connaissant pas une telle obligation de signaler.

### 3.3.3 Interdiction du paiement de rançons

L'interdiction du paiement de rançons lors d'attaques par rançongiciel est une mesure de grande ampleur visant à empêcher le financement d'activités criminelles et à réduire les incitations pour les criminels. La mise en œuvre d'une telle interdiction en Suisse impliquerait la création d'une base légale. Pour ce faire, il faudrait soit prévoir une disposition pénale correspondante dans le Code pénal (CP) avec des sanctions (p. ex. amende), soit discuter de l'introduction d'une loi spéciale de lutte contre la cybercriminalité définissant le cadre juridique d'une telle interdiction. Dans ce contexte, il faudrait définir précisément la notion de paiement de rançon, y compris la distinction entre paiements directs et indirects. Il conviendrait également de déterminer si l'interdiction s'applique uniquement aux attaques par rançongiciel ou également aux enlèvements et aux autres formes d'extorsion en général. Par ailleurs, les responsabilités et compétences des autorités pour faire respecter l'interdiction

devraient être discutées. Il faudrait notamment penser et développer des systèmes et des technologies permettant de surveiller les transactions suspectes et d'identifier les paiements de rançons. À cette fin, les banques et les institutions financières pourraient par exemple être tenues de signaler toute activité suspecte. En parallèle, il faudrait renforcer la capacité des autorités de poursuite pénale à enquêter et à poursuivre les violations de l'interdiction, organiser des formations, voire créer des unités spécialisées pour pouvoir assumer cette tâche.

L'introduction d'une interdiction du paiement de rançons en cas d'attaque par rançongiciel présente des avantages potentiels visant à réduire l'efficacité et la rentabilité de ces activités criminelles. Une telle interdiction aurait un effet dissuasif en réduisant l'incitation financière à lancer de telles attaques. Le signal envoyé par cette position légale claire souligne la tolérance zéro vis-à-vis de l'extorsion et de la cybercriminalité. À long terme, cela pourrait contribuer à réduire la fréquence et la gravité des attaques par rançongiciel et à endiguer la cybercriminalité.

Il y a cependant des inconvénients majeurs à prendre en compte : l'applicabilité pratique d'une telle interdiction implique des charges administratives considérables, tant pour les entreprises lors de la mise en œuvre de mesures de conformité que pour les autorités publiques lors de la surveillance et de la mise en application. Cela pourrait nuire à l'efficience et à la flexibilité tant de l'économie que de l'administration publique. Il existe en outre un risque de pénalisation des victimes d'attaques par rançongiciel, qui pourraient subir des pressions pour contourner l'interdiction afin de récupérer leurs données. Un autre inconvénient réside dans la réorientation potentielle de la menace vers d'autres activités criminelles moins réglementées, ce qui pourrait compromettre davantage la sécurité globale. Et surtout, une telle interdiction augmente le risque pour les victimes qui, sans l'option de paiement d'une rançon, pourraient être contraintes de subir des pertes d'exploitation et des préjudices financiers graves, voire de mettre en péril leur survie.

## 3.4 Résultat de l'examen

En Suisse, il n'existe certes aucune obligation générale de signaler le paiement d'une rançon, mais il existe des obligations de signaler toute cyberattaque relevant de la protection des données et du droit des marchés financiers, qui seront complétées à l'avenir par l'obligation de signaler au sens de la LSI pour les exploitants d'infrastructures critiques. Ces obligations de signaler servent à évaluer la menace et à renforcer l'alerte précoce, mais n'ont eu aucun effet dissuasif vis-à-vis des auteurs d'attaques par rançongiciel. L'introduction d'une obligation de signaler supplémentaire ou d'une interdiction du paiement de rançons afin de modifier le comportement des entreprises concernées a été examinée ci-dessus. Différents aspects ont été pris en compte, comme l'efficacité discutable de telles mesures pour dissuader durablement les attaquants, les conséquences involontaires éventuelles comme la dissimulation d'incidents, la nécessité d'une certaine flexibilité dans la gestion des crises et l'accent mis sur des mesures préventives plutôt que sur des obligations supplémentaires après une attaque. L'obligation de signaler tout paiement de rançon par des tiers comme des assurances, des intermédiaires financiers ou des prestataires de services de sécurité a également été envisagée. À défaut, des efforts sont toutefois déployés pour renforcer l'échange volontaire d'informations entre les autorités et ces acteurs afin d'obtenir une plus grande transparence, sans créer d'obstacles réglementaires supplémentaires[62].

Après un examen minutieux des avantages et des inconvénients, le maintien et l'optimisation des réglementations actuelles sont considérés comme l'approche la plus judicieuse. Cela garantit un équilibre entre une défense efficace contre les menaces, une réaction flexible aux attaques et la promotion de mesures de sécurité proactives. En même temps, la Suisse reste en phase avec les approches d'autres acteurs importants comme les États-Unis, l'Allemagne et la France.

[62] Cf. ch. 4, p. 23.

Cette stratégie est évaluée en permanence et adaptée si nécessaire afin de pouvoir réagir à l'évolution constante de la menace. L'objectif est d'adopter une approche globale mettant l'accent sur la prévention, la réactivité et la coopération internationale, sans restreindre inutilement la capacité d'action des entreprises concernées en situation de crise.

# 4 Échange accru d'informations

En matière de cybersécurité, l'échange d'informations sur les menaces, les vulnérabilités et les méthodes d'attaque est considéré comme un moyen de prévention décisif pour renforcer la protection contre les attaques. Il s'agit de l'outil le plus efficace d'améliorer la protection des personnes concernées, car les pirates peuvent utiliser le même procédé pour s'attaquer à un très grand nombre de victimes. Partager des informations permet d'identifier plus rapidement les méthodes et les tendances des attaques par rançongiciel. Si les entreprises et les institutions échangent des informations sur les attaques qui ont eu lieu, les méthodes utilisées et les vulnérabilités identifiées, d'autres victimes potentielles peuvent prendre des mesures proactives pour se prémunir contre des attaques similaires. La détection précoce et la prévention sont essentielles pour minimiser l'impact des attaques par rançongiciel.

Outre le renforcement de l'alerte précoce, l'échange d'informations favorise également la transparence. Si suffisamment d'organisations y participent, il est possible d'obtenir des informations plus détaillées sur la menace, même sans instaurer d'obligations de signaler.

Nous présentons ci-après les formes d'échange d'informations qui sont d'ores et déjà pratiquées ainsi que celles qui pourraient être développées spécifiquement pour les attaques par rançongiciel.

## 4.1 Échange d'informations pour améliorer la prévention et la réaction

En Suisse, l'OFCS coordonne l'échange d'informations entre les autorités et les personnes concernées par les cybermenaces. Il met à la disposition des entreprises et des autorités un service de signalement volontaire des cyberattaques et des cybermenaces ainsi qu'une plateforme permettant d'échanger des informations sur les menaces, les vulnérabilités et les méthodes d'attaque. Cela contribue à identifier plus rapidement les menaces et à y réagir de manière appropriée. De plus, cela permet d'améliorer en permanence les mesures de sécurité existantes et de développer de nouvelles technologies et procédures destinées à renforcer la protection contre les attaques par rançongiciel. Enfin, cela contribue à la résilience globale de l'infrastructure numérique de la Suisse et aide à renforcer la confiance dans les services et produits numériques.

La collaboration de l'OFCS avec des organismes internationaux est un autre aspect important. L'office fédéral travaille en étroite collaboration avec des partenaires et des réseaux internationaux afin d'échanger des informations sur les cybermenaces et les attaques à l'échelle mondiale. Depuis 2021, l'OFCS participe, avec d'autres services de la Confédération, à la *Counter Ransomware Initiative*[63]. Cette initiative internationale, à laquelle participent l'UE et plus de 30 autres États, coordonne les efforts dans la lutte contre la cybercriminalité au niveau politique et stratégique. Ce point s'avère particulièrement important, car la cybercriminalité est généralement transfrontalière et nécessite une lutte efficace fondée sur une coopération internationale. L'échange d'informations et de bonnes pratiques avec des partenaires internationaux permet à la Suisse de profiter de connaissances mondiales et d'adapter ses propres stratégies en conséquence. Par ailleurs, les instruments de droit

[63] Cf. site internet : https://counter-ransomware.org/ ; consulté pour la dernière fois le 20 octobre 2024.

international comme la Convention de Budapest[64] et la Convention des Nations Unies sur la cybercriminalité[65] jouent un rôle majeur dans la promotion de l'échange transfrontalier d'informations. Ces formats internationaux permettent d'avoir une vision plus large des tendances et tactiques des cybercriminels à l'échelle mondiale et renforcent la réponse coordonnée aux attaques par rançongiciel.

Au niveau national, l'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques, déjà décidée, et la poursuite du développement de la plateforme d'échange d'informations de l'OFCS amélioreront encore la capacité de détection et de défense contre les menaces. Cette combinaison d'initiatives nationales et de coopération internationale crée un vaste réseau d'échange d'informations qui contribue de manière décisive à la lutte contre les attaques par rançongiciel.

Par ailleurs, il est essentiel d'organiser régulièrement des rencontres et des ateliers entre la Confédération, les autorités cantonales de poursuite pénale, les entreprises de sécurité privées et les assurances. De tels événements offrent une base pour échanger des expériences, discuter des menaces actuelles et élaborer ensemble les meilleures pratiques. Des ateliers réguliers permettent aux participants d'élargir et d'adapter en permanence leurs connaissances et leurs compétences. Ces événements favorisent la compréhension des défis auxquels les différents acteurs sont confrontés et contribuent à l'élaboration de solutions communes. Ils renforcent en outre le réseau et la confiance entre les parties concernées, ce qui facilite la coopération en cas d'urgence. L'OFCS encourage cette forme de coopération en organisant des événements sectoriels et en mettant en place des organisations sectorielles pour l'échange d'informations. Ainsi, il a contribué à la mise en place du *Swiss Financial Sector Cyber Security Centre* (FS-CSC)[66]. L'échange d'informations au sein d'un secteur de l'industrie permet aux participants de se focaliser sur les menaces et les méthodes d'attaque pertinentes pour leur secteur. Des projets sont en cours en vue de la mise en place d'organisations similaires dans d'autres secteurs.

## 4.2 Partage d'informations pour améliorer l'action pénale

Le rapport du Conseil fédéral *Poursuites pénales en matière de cybercriminalité. Efficacité des cantons*, publié le 19 juin 2024 et donnant suite aux postulats 22.3145 d'Andri Silberschmidt du 16 mars 2022 et 22.3017 de la Commission de la politique de sécurité du Conseil national du 15 février 2022, souligne la nécessité de renforcer la coordination et la coopération dans le domaine des poursuites pénales en matière de cybercriminalité au niveau national et international. Il montre que le nombre et la gravité des infractions ainsi que l'ampleur des préjudices ne cessent d'augmenter. De plus, il met en évidence l'importance des réseaux et des groupes de travail spécialisés ainsi que la nécessité pour les cantons de procéder à des ajustements sur le plan de l'organisation et du personnel afin de lutter plus efficacement contre la cybercriminalité. Malgré les progrès réalisés, des défis subsistent, notamment le manque de ressources et les obstacles réglementaires à l'échange

---

64 La Convention de Budapest, officiellement connue sous le nom de Convention sur la cybercriminalité (RS **0.311.43**), est un accord international adopté par le Conseil de l'Europe le 23 novembre 2001. Il s'agit du premier instrument de droit international contraignant spécifiquement élaboré pour lutter contre la cybercriminalité. La convention vise à harmoniser les législations nationales, à améliorer les techniques d'enquête et à promouvoir la coopération internationale dans la lutte contre les délits informatiques. Elle couvre des domaines comme l'accès non autorisé à des systèmes informatiques, la fraude informatique et la diffusion de pédopornographie sur internet. La Suisse est partie à la Convention de Budapest depuis le 1er janvier 2012 et a ainsi réaffirmé son engagement en faveur de la coopération internationale dans la lutte contre la cybercriminalité. En ratifiant cette convention, la Suisse s'est engagée à adapter sa législation nationale aux exigences de la convention et à participer, dans le cadre du droit pénal, aux enquêtes transfrontalières ainsi qu'à l'échange d'informations.

65 La Convention des Nations Unies sur la cybercriminalité se propose de créer un cadre juridique pour la pénalisation des cyberdélits, y compris les attaques par rançongiciel, et de promouvoir la coopération internationale en matière de poursuites pénales. La convention vise à permettre une réponse coordonnée à la menace transnationale que constituent les rançongiciels. Le Département fédéral des affaires étrangères et l'Office fédéral de la justice coordonnent la position suisse sur la convention. L'efficacité de la convention dépend de sa ratification à grande échelle et de sa mise en œuvre cohérente par les États membres. Ce processus prend habituellement du temps, souvent plusieurs années. La Suisse examinera la convention en vue d'une éventuelle signature et d'une ratification ultérieure selon sa procédure nationale.

66 Cf. site internet : www.fscsc.ch ; consulté pour la dernière fois le 20 octobre 2024.

d'informations. Le rapport appelle donc à intensifier les mesures de prévention et de répression et à renforcer la collaboration entre la Confédération, les cantons et les partenaires internationaux[67].

Ce rapport confirme que le renforcement de l'échange d'informations dont il est question ici peut favoriser la collaboration et la confiance entre la Confédération, les autorités cantonales de poursuite pénale, les entreprises de sécurité privées et les assurances. Le partage systématique et régulier d'informations par l'ensemble des parties concernées créera une transparence qui favorisera la confiance mutuelle. Cet aspect est essentiel pour développer et mettre en œuvre conjointement des solutions efficaces afin de lutter contre les attaques par rançongiciel. La population, les entreprises et les institutions se sentent plus en sécurité lorsqu'elles savent qu'elles peuvent compter sur le soutien et les connaissances d'une large communauté. Une approche coordonnée entre la Confédération, les autorités cantonales de poursuite pénale, les entreprises de sécurité privées et les assurances renforce la défense globale contre les attaques par rançongiciel. Conjointement, des stratégies de défense plus efficaces et plus complètes peuvent être développées, ce qui permet également une meilleure allocation des ressources pour lutter contre la cybercriminalité.

L'échange d'informations aide les autorités de poursuite pénale à identifier et à poursuivre les cybercriminels. En partageant des données sur les attaques, les techniques et les profils des pirates, les autorités de poursuite pénale peuvent mettre au jour les méthodes employées et mener des enquêtes ciblées, ce qui augmente les chances d'identifier et de condamner les responsables des attaques. Des poursuites pénales efficaces ont un effet dissuasif sur les auteurs potentiels.

## 4.3 Résultat de l'examen : possibilité de mise en œuvre d'un échange accru d'informations

L'échange d'informations actuel se concentre principalement sur la détection et l'alerte précoces en cas de menaces. Il est essentiel d'aller au-delà des détails techniques des attaques et d'acquérir une compréhension globale de leur impact à large échelle. Cela implique de recenser le nombre de systèmes touchés, la durée des interruptions d'exploitation, les préjudices financiers et la quantité de données compromises. En ce qui concerne les attaques par rançongiciel, de telles informations permettraient de se prononcer sur la problématique du paiement des rançons.

Pour recueillir de telles informations de manière plus systématique, l'échange d'informations existant doit être étendu à d'autres acteurs. Les assurances, les autres intermédiaires financiers et les prestataires de services de sécurité, en particulier, disposent d'informations précieuses sur les répercussions de cyberattaques. Renforcer cet échange d'informations permettrait d'améliorer la transparence quant aux préjudices causés par les attaques par rançongiciel. Dans un premier temps, il serait possible de miser sur un échange d'informations volontaire plutôt que d'introduire une obligation légale de signalement pour les assurances, les autres intermédiaires financiers et les prestataires de services de sécurité. Cette décision repose sur plusieurs considérations : une obligation de signaler entraînerait des charges administratives et financières considérables pour les assurances et les autorités, qui pourraient ne pas être proportionnelles aux avantages escomptés. Un échange volontaire permet d'adapter continuellement le système aux nouvelles connaissances et aux nouveaux besoins, sans nécessiter de modifications législatives fastidieuses. Par ailleurs, les informations partagées volontairement sont souvent plus détaillées et plus contextuelles que celles qui sont communiquées en vertu d'une obligation légale. Une approche coopérative favorise la confiance entre les parties prenantes et peut encourager une culture de la communication plus ouverte. Pour favoriser cet échange d'informations, la Confédération pourrait mettre à disposition une plateforme de partage d'informations dépassant le cadre de la détection et de l'alerte précoces et permettant des analyses approfondies des causes et des conséquences de cyberattaques. Il convient d'impliquer

[67] Communiqué de presse Le Conseil fédéral publie un rapport sur la lutte contre la cybercriminalité en Suisse (site internet : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-101469.html ; consulté pour la dernière fois le 20 octobre 2024).

notamment les assurances et les prestataires de services de sécurité dans cet échange d'informations. L'efficacité de cette approche pourrait ensuite faire l'objet d'une évaluation périodique. S'il s'avère que l'échange volontaire d'informations ne donne pas les résultats escomptés, des mesures plus contraignantes pourraient être envisagées. Il pourrait s'agir par exemple d'une obligation de signaler anonyme pour les assureurs, les autres intermédiaires financiers et les prestataires de services de sécurité. Cette approche échelonnée et un examen régulier fourniraient un état des lieux plus complet et plus nuancé de la cybersécurité que ne le ferait une obligation de signaler immédiate. Cela permettrait en outre d'élaborer et de mettre en œuvre des stratégies plus efficaces de prévention et de lutte contre les cyberattaques. La possibilité de recourir aux plateformes existantes de l'OFCS pour un tel échange d'informations sera examinée afin d'exploiter les synergies et de minimiser la charge de travail pour l'ensemble des parties prenantes. Cette approche constitue un instrument concret permettant de suivre l'évolution et l'efficacité de l'échange d'informations et, si nécessaire, de réagir en temps utile.

# 5 Considérations finales

En ce qui concerne la protection contre les attaques par rançongiciel, il existe d'ores et déjà en Suisse de nombreuses informations, instructions et directives officielles concernant les mesures de protection informatique de base ainsi que des prescriptions juridiques relatives à la cybersécurité. Le Conseil fédéral estime qu'en cas de besoin, il faudrait développer les directives générales existantes en matière de cybersécurité afin de permettre une stratégie de défense plus large et plus flexible plutôt que d'édicter de nouvelles directives spécifiques aux rançongiciels.

La répartition des compétences entre la Confédération et les cantons ainsi que le principe de subsidiarité inscrit dans la Constitution signifient que la Confédération ne peut pas imposer des mesures de cyberprotection contraignantes et généralisées aux organisations cantonales ou communales chargées d'une mission de service public. Les cantons et les communes doivent donc développer de manière autonome des directives pour protéger leurs infrastructures informatiques en s'inspirant de la cyberstratégie nationale ainsi que des ordonnances légales et administratives, des informations, des instructions et des directives de la Confédération en matière de cybersécurité.

L'examen d'une éventuelle obligation de signaler tout paiement de rançon en cas d'attaque par rançongiciel a montré que les objectifs d'une transparence accrue et d'une meilleure vue d'ensemble des préjudices résultant d'attaques par rançongiciel peuvent être atteints en encourageant l'échange d'informations plutôt qu'en introduisant une obligation supplémentaire.

L'amélioration de l'échange d'informations existant sur une base volontaire permettrait de prendre des mesures techniques et organisationnelles qui augmenteraient la résilience face aux attaques par rançongiciel et renforceraient l'infrastructure numérique à long terme. Une collaboration accrue et un échange d'informations plus approfondi entre la Confédération, les autorités cantonales de poursuite pénale, les entreprises de sécurité privées, les assurances et les autres intermédiaires financiers sont essentiels pour lutter efficacement contre la menace de la cybercriminalité et garantir durablement la sécurité de l'infrastructure numérique.

La Confédération soutient l'échange d'informations et peut jouer un rôle de coordination afin de renforcer la défense commune contre les attaques par rançongiciel. Si l'efficacité de l'échange d'informations volontaire ne produit pas les résultats escomptés, des mesures plus contraignantes pourraient être envisagées, comme une obligation anonyme de signaler pour les entreprises d'assurance, les autres intermédiaires financiers et les prestataires de services de sécurité. Le Conseil fédéral estime que cette approche s'avère plus efficace que de nouvelles directives spécifiques aux attaques par rançongiciel.

# Glossaire

| | |
|---|---|
| AppLocker | Logiciel permettant de contrôler quelles applications les utilisateurs sont autorisés à exécuter. |
| Apprentissage en ligne | Apprentissage assisté par voie électronique, souvent au moyen d'internet. |
| Ateliers | Événements interactifs au cours desquels les participants acquièrent une expérience pratique et échangent des connaissances. |
| Citrix | Plateforme de virtualisation permettant d'accéder à distance à des applications et à des postes de travail. |
| Courriel | Courrier électronique ; système de messagerie numérique pour l'échange de messages et de fichiers via des réseaux informatiques. |
| Cyberstratégie nationale (CSN) | Plan global à l'échelle nationale visant à améliorer la cybersécurité et à protéger les infrastructures critiques contre les cybermenaces. |
| Excel | Tableur édité par Microsoft, utilisé pour créer et modifier des tableaux et des graphiques et pour effectuer des calculs. |
| Filtre anti-spam | Programme ou appareil qui détecte et bloque les courriels non sollicités (spam). |
| Gatekeeper | Mécanisme de sécurité de macOS qui contrôle l'installation et l'exécution de logiciels. |
| Gouvernance | Principes, procédures et mesures de gestion et de contrôle d'une entreprise. |
| Identification multifacteur (MFA) | Système de sécurité nécessitant plusieurs preuves d'identité (facteurs) pour l'authentification. |
| Informatique | Technologies de l'information ; englobe tous les moyens techniques de traitement d'informations. |
| Infrastructure informatique | Ensemble du matériel, des logiciels, des réseaux et des installations nécessaires au fonctionnement et à la gestion de l'environnement informatique d'une organisation. |
| Macro | Séquence de commandes ou d'instructions pouvant être exécutées de manière automatisée dans un programme afin de simplifier des tâches répétitives. |
| Meilleures pratiques | Méthodes ou procédures éprouvées et reconnues comme étant les meilleures. |
| Messagerie web | Service de messagerie électronique accessible au moyen d'un navigateur internet. |

| | |
|---|---|
| PowerPoint | Logiciel de présentation édité par Microsoft permettant de créer et de faire des présentations visuelles. |
| Protocole RDP (bureau à distance) | Protocole permettant aux utilisateurs de se connecter à un autre ordinateur via un réseau. |
| Rançongiciel | Type de logiciel malveillant qui chiffre des données et exige une rançon en contrepartie de leur restitution. |
| RAR | Format de fichier pour des archives compressées. |
| Réseau privé virtuel (VPN) | Connexion réseau chiffrée permettant de communiquer en toute sécurité via des réseaux publics. |
| Sauvegarde | Copie des données pouvant être utilisée à des fins de restauration si les données originales sont perdues ou endommagées. |
| SELinux | *Security-Enhanced Linux* ; module de sécurité pour le noyau Linux offrant des mécanismes de contrôle d'accès supplémentaires. |
| SharePoint | Plateforme internet de Microsoft pour la collaboration et la gestion de documents. |
| Système informatique | Combinaison de matériel, de logiciels et de ressources réseau fonctionnant ensemble pour traiter et stocker des informations. |
| Système de management de la sécurité de l'information (SMSI) | Système structuré de directives, de processus et de mesures qui aide les entreprises à assurer la sécurité de leurs informations. Souvent fondé sur des normes internationales comme ISO/IEC 27001, il inclut la définition de directives de sécurité, une gestion des risques ainsi que la mise en œuvre de mesures techniques et organisationnelles. L'objectif est de protéger les informations contre les menaces et de répondre aux exigences légales tout en garantissant un contrôle et une amélioration continus du système. |
| Technologie opérationnelle (TO) | Matériel et logiciels qui surveillent et contrôlent les équipements physiques, les processus et les événements dans les entreprises. |
| Technologies de l'information et de la communication (TIC) | Englobe tous les moyens techniques de traitement et de transmission d'informations. |
| Word | Logiciel de traitement de texte édité par Microsoft servant à créer et à modifier des documents. |
| ZIP | Format de fichier très répandu pour les archives compressées. |
| Zone de réseau | Zone délimitée au sein d'un réseau avec des directives de sécurité spécifiques. |