Contact Committee

Comité de contact

des institutions supérieures de contrôle de l'Union européenne

Compendium d'audit

La cybersécurité dans l'UE et ses États membres

Audit de la résilience des systèmes d'information et des infrastructures numériques critiques aux cyberattaques

Rapports d'audit publiés entre 2014 et 2020

FR

Décembre 2020

Le comité de contact des institutions supérieures de contrôle (ISC) de l'Union européenne offre un espace de discussion permettant d'aborder les questions relatives à l'audit des finances publiques dans l'UE. En renforçant le dialogue et la coopération entre ses membres, il contribue à l'efficacité de l'audit externe des politiques et des programmes de l'UE. Il participe également à renforcer l'obligation de rendre compte ainsi qu'à améliorer la gestion financière et la bonne gouvernance de l'Union dans l'intérêt de tous ses citoyens.

Contact: www.contactcommittee.eu

Table des matières

Page

Table des matières

Table des matières

Avant-propos

Chères lectrices, chers lecteurs,

La transition numérique et l'utilisation croissante des technologies de l'information dans tous les aspects de notre quotidien nous ouvrent un horizon de nouvelles possibilités. En revanche, le risque que les particuliers, les entreprises et les autorités publiques soient victimes de cybercriminalité ou d'une cyberattaque a augmenté, au même titre que ses conséquences sociétales et économiques.

Au sein de l'UE, la cybersécurité relève exclusivement des États membres. L'UE a un rôle à jouer dans la création d'un cadre réglementaire commun au sein du marché unique de l'UE et dans la mise en place de conditions permettant aux États membres de collaborer dans un climat de confiance mutuelle.

La cybersécurité et notre autonomie numérique sont devenues des enjeux d'une importance stratégique pour l'UE et ses États membres. La gouvernance en matière de cybersécurité dans le secteur public et le secteur privé continue à présenter des faiblesses dans tous les États membres, bien qu'à des degrés divers. Cela compromet notre capacité à limiter les cyberattaques et, le cas échéant, à y réagir. La désinformation, souvent orchestrée hors de l'UE, gagne du terrain, comme l'a montré cette année encore la crise de la COVID-19. Elle menace la cohésion de nos sociétés et la confiance que les citoyens accordent à nos systèmes démocratiques, et nous ne pouvons l'ignorer.

En 2018, une enquête réalisée auprès des institutions supérieures de contrôle (ISC) de l'UE a révélé qu'à l'époque, la moitié d'entre elles environ n'avaient jamais réalisé d'audit de la cybersécurité. Depuis, nos ISC ont enclenché la vitesse supérieure dans le domaine de la cybersécurité, en centrant plus particulièrement leurs audits sur la protection des données, sur l'état de préparation des systèmes face aux cyberattaques ainsi que sur la protection des systèmes de services publics essentiels. Ces audits ne peuvent bien entendu pas tous être rendus publics, certains pouvant concerner des informations sensibles (liées à la sécurité nationale).

La crise de la COVID-19 de cette année a mis à l'épreuve le tissu social et économique de nos sociétés. Compte tenu de notre dépendance à l'égard des technologies de l'information, la prochaine pandémie pourrait bien prendre la forme d'une «cybercrise». Nous devons nous préparer et renforcer la résilience des systèmes d'information et des infrastructures numériques critiques aux cyberattaques.

Nous espérons que la vue d'ensemble offerte par le présent compendium stimulera l'intérêt que portent les auditeurs des finances publiques de tous les États membres de l'Union à ce domaine crucial.

Klaus-Heiner Lehne

Président de la Cour des comptes européenne
Président du comité de contact
et responsable du projet

Synthèse

I La cybersécurité et notre autonomie numériques **sont devenus des enjeux d'importance stratégique pour l'UE et ses États membres** et, à mesure que la menace s'accentue, il nous faut redoubler d'efforts pour protéger nos systèmes d'information et infrastructures numériques critiques contre les cyberattaques. La cybersécurité ne concerne pas uniquement nos systèmes de services publics, de défense ou de santé; il s'agit également de protéger nos données à caractère personnel, nos modèles commerciaux et nos droits de propriété intellectuelle. En définitive, la cybersécurité consiste à préserver nos sociétés démocratiques, notre indépendance d'Européens et la façon dont nous cohabitons.

II La première partie de ce troisième compendium du comité de contact définit **ce qui relève de la cybersécurité**. Elle décrit les défis que représente la cybersécurité pour les autorités publiques, les entreprises et les particuliers et met en lumière le nouveau phénomène de la désinformation, une menace croissante pour la cohésion de nos sociétés et de nos systèmes démocratiques. Elle présente également les acteurs et les compétences de l'UE en matière de cybersécurité, ainsi que la stratégie et la législation de l'Union et les financements qu'elle met à disposition dans ce domaine.

III La deuxième partie du compendium offre une synthèse des **résultats d'une sélection d'audits réalisés par les ISC de 12 États membres participants et par la Cour des comptes européenne**, publiés entre 2014 et 2020. Ces audits portaient sur d'importants aspects de la cybersécurité, tels que la protection des données privées, l'intégrité des centres de données nationaux, la sécurité des installations de services publics ainsi que la mise en œuvre des stratégies nationales en matière de cybersécurité au sens large du terme.

IV La troisième partie propose des **fiches d'information détaillées sur les audits sélectionnés**, ainsi qu'une vue synoptique d'autres audits en rapport avec la cybersécurité publiés par les ISC.

PREMIÈRE PARTIE – La cybersécurité dans le contexte européen

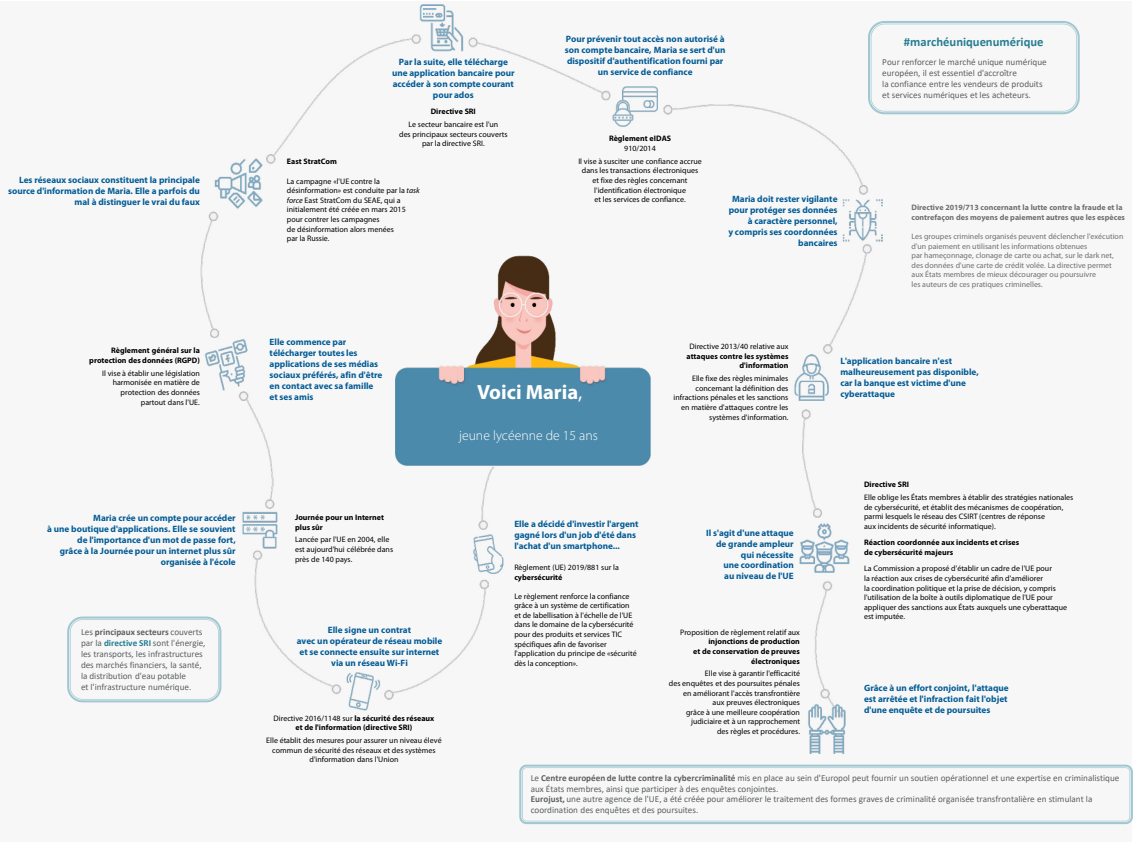
Qu'est-ce que la cybersécurité?

1 Il n'existe aucune **définition** universelle **de la cybersécurité**. Dans le présent document, la cybersécurité désigne **les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les autres personnes exposées aux cybermenaces**. Elle suppose de prévenir ou de détecter les cyberincidents, d'y répondre, puis de rétablir la situation. Ces incidents peuvent être intentionnels ou non et vont de la divulgation accidentelle d'informations à l'ingérence dans les processus démocratiques et l'organisation de campagnes de désinformation pour influencer le débat public, en passant par les attaques contre les entreprises et les infrastructures critiques et le vol de données à caractère personnel.

La cybersécurité influe sur le quotidien de tous les citoyens de l'UE

2 La cybersécurité intéresse notre quotidien de citoyens de l'UE dès lors que nous nous servons d'appareils informatiques personnels tels que les smartphones, ou que nous nous connectons à des réseaux Wi-Fi, à des médias sociaux ou à des services bancaires électroniques. En 2020 plus que jamais, il ne s'agit plus de déterminer si des cyberattaques sont susceptibles de se produire, mais plutôt quand et comment elles vont se produire. Cette menace nous concerne tous: **particuliers, entreprises et autorités publiques**. L'*image 1* illustre l'engagement de l'UE en faveur de la cybersécurité et le cadre qu'elle a créé pour protéger les activités électroniques quotidiennes de ses citoyens contre les cyberattaques. La protection des systèmes d'information et des infrastructures numériques critiques contre les cyberattaques est devenue un enjeu stratégique.

Image 1 – L'UE s'engage en faveur de la cybersécurité dans le quotidien de ses citoyens

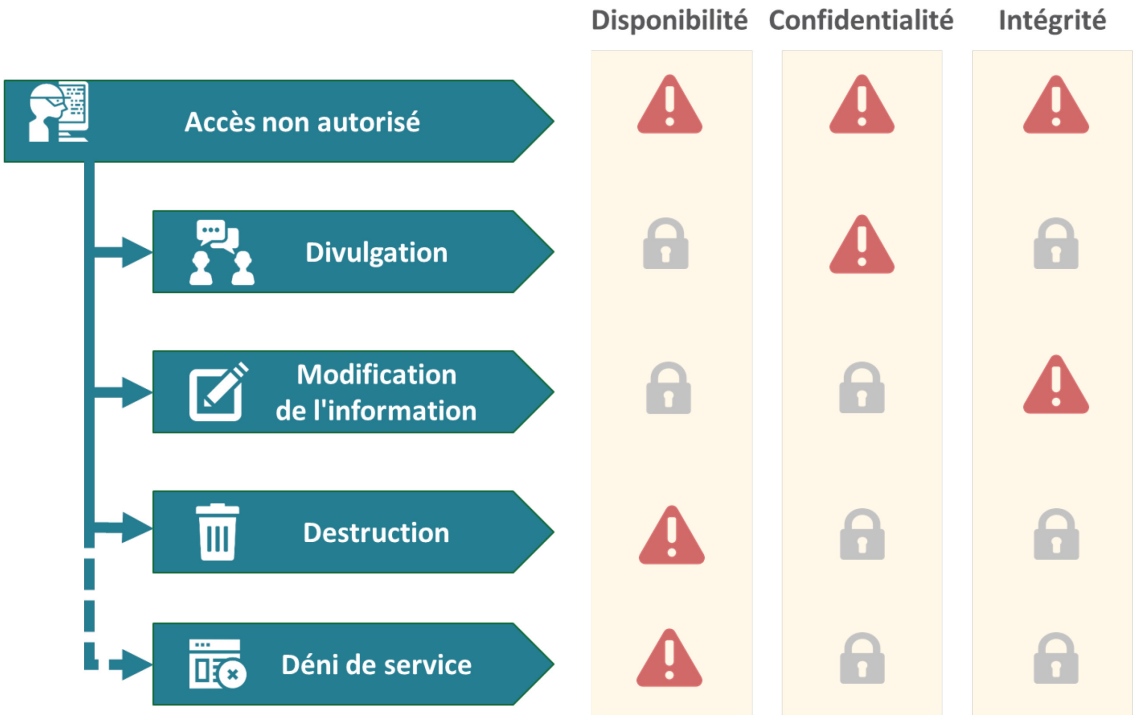


Source: Cour des comptes européenne, icônes réalisées par Pixel perfect à partir du site www.flaticon.com.

De nombreux types de menaces pèsent sur la cybersécurité

3 Dans nos sociétés, les nombreuses formes de menaces qui pèsent sur la cybersécurité peuvent être classées en fonction de **ce qu'elles font des données – divulgation, altération, destruction ou refus d'accès –** ou en fonction des principes fondamentaux relatifs à la sécurité de l'information qu'elles violent (voir ***figure 1***).

Figure 1 – Les différentes formes de menaces et les principes en matière de sécurité de l'information auxquels elles portent atteinte



Le cadenas indique que la sécurité n'est pas remise en cause; le point d'exclamation indique qu'elle est exposée à des risques.

Source: Cour des comptes européenne, sur la base d'une étude du Parlement européen[1].

4 Chaque appareil qui se connecte à l'internet ou à d'autres appareils augmente ce que l'on appelle la «surface d'attaque» en matière de cybersécurité. La croissance exponentielle de l'«internet des objets» (IdO), de l'informatique en nuage, des mégadonnées et du passage au numérique de l'industrie s'accompagne d'une vulnérabilité accrue, ce qui permet aux pirates informatiques de cibler toujours plus de victimes. Du fait de la diversité des types d'attaques et de leur sophistication croissante, il est difficile de suivre le rythme[2]. L'***encadré 1*** présente des exemples de **cyberattaques possibles**.

[1] Parlement européen, *Cybersecurity in the European Union and Beyond:Exploring the Threats and Policy Responses*, étude réalisée pour la commission LIBE, septembre 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18 janvier 2018.

Encadré 1

Types de cyberattaques

Un **maliciel** (logiciel malveillant) est conçu pour perturber le fonctionnement des appareils et des réseaux. Il peut s'agir d'un virus, d'un cheval de Troie, d'un logiciel rançonneur, d'un ver, d'un logiciel publicitaire ou d'un logiciel espion (tel que *NotPetya*).

Un **logiciel rançonneur** crypte les données, empêchant ainsi les utilisateurs d'accéder à leurs dossiers jusqu'à ce qu'ils versent une rançon, généralement en cryptomonnaie, ou qu'ils réalisent une action donnée. Selon Europol, les attaques par logiciels rançonneurs sont de loin les plus fréquentes et la variété des logiciels de ce type (par exemple *Wannacry*[3]) a explosé ces dernières années.

Les attaques par **déni de service distribué**, qui consistent à rendre des services ou des ressources indisponibles en les saturant de requêtes, connaissent également une augmentation, un tiers des organisations ayant été visées par ce type d'attaques en 2017[4].

Les **attaques sur internet** sont une méthode intéressante pour les pirates informatiques, qui peuvent utiliser les systèmes et services en ligne comme vecteurs pour tromper les utilisateurs. Ces pirates exploitent une vaste surface d'attaque, qui leur permet notamment de diffuser des adresses URL et scripts malveillants pour rediriger l'utilisateur ou la victime vers le site internet souhaité ou pour lui faire télécharger un contenu malveillant (attaque de point d'eau, attaque par téléchargement furtif (*drive-by*), et d'**insérer** un code malveillant dans un site internet légitime, mais compromis, pour voler des informations (par exemple, le piratage de formulaires ou *formjacking*) en vue d'obtenir de l'argent ou des renseignements[5].

Les utilisateurs peuvent être manipulés de sorte qu'ils effectuent une action ou divulguent des informations confidentielles de manière involontaire. Ce stratagème, qui peut être utilisé pour les vols de données ou le cyberespionnage, est appelé **piratage psychologique**. Il existe plusieurs méthodes pour ce faire, mais la plus répandue est l'**hameçonnage**, un procédé qui consiste à envoyer des courriels semblant provenir de sources fiables afin de piéger le destinataire et de l'amener ainsi à révéler des informations ou à cliquer sur des liens qui infecteront ses appareils en y installant des logiciels malveillants. Plus de la moitié des États membres ont fait état d'enquêtes sur des attaques de ce type, qui visent les réseaux[6].

Les plus néfastes sont certainement les **menaces persistantes avancées**. Causées par des attaques sophistiquées impliquant des activités à long terme de surveillance et de vols de données, elles visent parfois à semer la destruction. Leur but est d'échapper à toute détection aussi longtemps que possible. Souvent associées à un État, les menaces persistantes avancées ciblent les secteurs particulièrement sensibles comme les technologies, la défense et les infrastructures critiques. Selon certaines estimations, ce type de **cyberespionnage** représente au moins un quart de tous les cyberincidents[7].

[3] Le logiciel rançonneur *Wannacry* exploitait les failles d'un protocole Microsoft Windows permettant la prise de contrôle à distance de tout ordinateur. Microsoft a déployé un correctif après la découverte de ces failles. Toutefois, des centaines de milliers d'ordinateurs n'ont pas été mis à jour et un grand nombre ont été infectés. *Source*: A. Greenberg, *Hold North Korea Accountable for Wannacry—and the NSA, too*, WIRED, 19 décembre 2017.

[4] Europol, Évaluation de la menace que représente la criminalité organisée sur internet (*Internet Organised Crime Threat Assessment*), 2018.

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20 octobre 2020.

[6] Europol, voir supra, 2018.

[7] Centre européen de politique économique internationale (ECIPE), *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, *Occasional Paper* nº 2/18, février 2018.

L'impact économique des cyberattaques est considérable

5 Ces dernières années, la menace que font peser **les cyberattaques et la cybercriminalité** est devenue un problème majeur. En 2016 déjà, 80 % des entreprises européennes avaient connu au moins un incident de cybersécurité[8]. Lors d'une enquête de 2018, 40 % des répondants issus d'organisations ayant recours à la robotique ou à l'automatisation affirmaient que la conséquence la plus grave d'une cyberattaque de leurs systèmes serait une perturbation des opérations. Néanmoins, bien qu'elles aient conscience des risques de perturbation induits par les cyberattaques, les entreprises ne sont souvent pas dotées d'un système permettant de les gérer[9].

6 Depuis, le nombre de cyberattaques, leur gravité et leurs conséquences financières ne cessent de croître. Selon les prévisions, l'**incidence financière** de la cybercriminalité devrait représenter pour l'économie mondiale un coût annuel de **6 000 milliards de dollars des États-Unis d'ici à 2021**, une augmentation par rapport à un coût estimatif de 3 000 milliards de dollars en 2015[10], pour un PIB mondial estimé à 138 000 milliards de dollars en 2020. Les coûts de la cybercriminalité comprennent la détérioration et la destruction de données, le vol d'argent, la perte de productivité, le vol de droits de propriété intellectuelle, le vol de données personnelles et financières, la perturbation de l'activité normale à la suite d'une attaque et l'atteinte à la réputation. Le Comité européen du risque systémique (CERS) estime que le coût moyen des cyberincidents a augmenté de 72 % entre 2015 et 2020[11].

7 La cybercriminalité **a des répercussions diverses sur les différents secteurs économiques**, comme en témoigne une récente étude réalisée en 2020[12]: il s'agit de la fraude la plus déstabilisatrice pour les gouvernements et les administrations publiques, ainsi que pour les secteurs des technologies, des médias et des télécommunications ou

---

8 Europol, *Internet Organised Crime Threat Assessment*, 2017.

9 PWC, *Global State of Information Security (GSISS), Survey – Strengthening digital society against cyber shocks*, 2017.

10 Cybersecurity Ventures, *2019 Official Annual Cybercrime Report*, financé par Herjavec Group, 2019.

11 Comité européen du risque systémique (CERS), *Systemic cyber risk*, février 2020.

12 PWC, *Fighting fraud: A never-ending battle – PwC's Global Economic Crime and Fraud Survey*, 2020.

encore pour celui de la santé (voir ***encadré 2***). Elle arrive également au deuxième rang des fraudes les plus perturbatrices pour le secteur financier et pour le secteur industriel et manufacturier.

Encadré 2

Des patients finlandais de psychothérapie dont les données médicales ont été volées en 2018 et 2019 font l'objet d'un chantage

Des patients d'une importante clinique de psychothérapie finlandaise dotée de dispensaires dans tout le pays ont été contactés individuellement par un maître chanteur à la suite du vol de leurs données à caractère personnel en novembre 2018 et d'une autre violation potentielle en mars 2019. Parmi ces données figuraient, semble-t-il, les dossiers des patients et des notes sur ce qui a été dit au cours des séances de thérapie.

Le maître chanteur a demandé à la clinique et aux patients de lui verser une rançon en bitcoins pour éviter que les données soient rendues publiques. L'incident a amené le gouvernement finlandais à tenir une réunion d'urgence[13].

8 En 2019, Europol[14] a une nouvelle fois souligné la **persistance et la ténacité d'un certain nombre de menaces majeures liées à la cybercriminalité**:

- les attaques par logiciel rançonneur demeurent la principale menace; ils sont ciblés avec une précision accrue, sont plus lucratifs et causent des dommages économiques plus importants. Tant que les logiciels rançonneurs offriront des revenus relativement faciles aux cybercriminels et qu'ils continueront d'infliger des dommages et des pertes financières considérables, ils devraient rester la plus importante menace posée par la cybercriminalité;
- l'hameçonnage et l'exploitation des vulnérabilités des protocoles de bureau à distance (*remote desktop protocols* ou RDP) sont les principaux vecteurs d'infection par des maliciels;

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26 octobre 2020.

[14] Europol, *Internet organised crime threat assessment (IOCTA)*, 2019.

- les données continuent à être une cible de choix pour la cybercriminalité, mais aussi une source de revenus essentielle et un catalyseur hors pair.

9 De même, dans son **rapport de 2020 sur les principaux incidents survenus dans l'UE et dans le monde**[15], l'Agence de l'Union européenne pour la cybersécurité (ENISA) présente un certain nombre d'exemples d'incidents liés à la cybersécurité (voir ***encadré 3***).

Encadré 3

Agence de l'Union européenne pour la cybersécurité (ENISA): incidents concernant la cybersécurité survenus en 2019 et 2020

La plateforme de messagerie en ligne «verifications.io» a été victime d'une grave violation de données en raison de l'absence de protection d'une base de données MongoDB. Les données provenant de plus 800 millions de courriers électroniques ont été révélées, dont des renseignements sensibles tels que des informations à caractère personnel.

Plus de 770 millions d'adresses électroniques et 21 millions de mots de passe uniques ont été exposés sur un forum de piratage très fréquenté hébergé par le service d'informatique en nuage MEGA1. Cette collection d'identifiants personnels piratés, intitulée «collection n° 1», s'est avérée être la plus importante de l'histoire.

Le fournisseur de services en nuage et de virtualisation Citrix a été victime d'une cyberattaque ciblée. Afin d'obtenir l'accès aux systèmes de Citrix, les pirates ont exploité plusieurs vulnérabilités logicielles critiques, telles que la vulnérabilité CVE-2019-19 781, et ont employé une technique appelée «pulvérisation de mots de passe» (*password spraying*).

Le fournisseur d'hébergement en nuage iNSYNQ19 a subi une attaque par logiciel rançonneur qui a empêché ses clients d'accéder à leurs données pendant plus d'une semaine, les forçant à recourir à leurs sauvegardes locales.

[15] ENISA, *Main incidents in the EU and worldwide – From January 2019 to April 2020*, octobre 2020.

10 Selon Europol, le nombre de cyberattaques conçues pour causer des **dommages durables** a doublé au cours des six premiers mois de 2019, principalement dans le secteur de la fabrication. Contrairement aux attaques «conventionnelles» par logiciel rançonneur, ces actes de sabotage suppriment de manière permanente les données de l'entreprise ou leur causent des dommages irréversibles (voir ***encadré 4***).

Encadré 4

Logiciels rançonneurs destructifs: les attaques par *Germanwiper* de 2019

En 2019, des entreprises opérant en Allemagne ont été victimes d'une série d'attaques par logiciel rançonneur. Surnommé *Germanwiper*, ce logiciel a la capacité de remplacer les fichiers infectés par des 0 et 1, rendant ainsi impossible la restauration des fichiers. Le logiciel rançonneur s'est répandu au moyen de campagnes d'hameçonnage par courrier électronique qui ciblaient notamment le personnel des ressources humaines des plus grandes entreprises, le maliciel étant intégré dans de fausses candidatures[16].

La prise de conscience des menaces pesant sur la cybersécurité s'améliore à mesure que la fréquence des attaques augmente

11 Néanmoins, récemment encore, le public était peu conscient ou informé de l'existence de ces risques. En 2017, 69 % des entreprises de l'UE n'avaient qu'une compréhension de base, voire aucune compréhension, de leur **exposition aux cybermenaces**[17], tandis que 60 % n'avaient jamais évalué les **pertes financières potentielles**[18]. Par ailleurs, selon une étude réalisée à l'échelle mondiale en 2018, un

[16] Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany*, non daté.

[17] Commission européenne, Fiche d'information sur la cybersécurité, septembre 2017.

[18] Ces pertes peuvent comprendre: le manque à gagner, les frais de réparation des systèmes endommagés, les responsabilités potentielles à supporter pour les avoirs et les informations volés, le coût des mesures de rétention de la clientèle, des primes d'assurance plus élevées, des coûts de protection plus élevés (nouveaux systèmes, nouveaux employés, nouvelles formations), ainsi que le règlement potentiel des frais de mise en conformité ou de litige.

tiers des organisations préféreraient verser une rançon à des pirates plutôt qu'investir dans la sécurité informatique[19].

12 L'**Eurobaromètre 2020 intitulé *Europeans' attitudes towards cyber security***[20] souligne la prise de conscience et la préoccupation croissantes des citoyens de l'UE:

- les répondants qui utilisent internet sont plus susceptibles d'être préoccupés par le détournement de leurs données à caractère personnel (46 %), par la sécurité de leurs paiements en ligne (41 %), par l'impossibilité d'examiner les biens en vente ou de demander conseil à une personne en chair et en os (22 %) ou par l'éventualité de ne pas recevoir les biens ou services qu'ils ont achetés en ligne (22 %);
- plus des trois quarts (76 %) des personnes interrogées estiment que le risque d'être victime de la cybercriminalité est en augmentation. Cependant, elles sont bien moins nombreuses (52 %) à penser qu'elles sont en mesure de se protéger contre cette menace, ce qui représente une diminution de neuf points de pourcentage par rapport à 2018;
- néanmoins, un peu plus de la moitié (52 %) des répondants jugent qu'ils sont bien informés sur la cybercriminalité, mais seuls 11 % d'entre eux se déclarent très bien informées.

La cybersécurité est importante pour la cohésion sociale et la stabilité politique

Une nouvelle menace: la cybersécurité et la désinformation

13 La propagation de campagnes massives délibérées et systématiques de **désinformation constitue un défi stratégique majeur pour nos démocraties**[21]. La désinformation et la diffusion de fausses informations peuvent diviser les sociétés et

---

[19] NTT Security, *2018 Risk: Value Report*.

[20] Commission européenne, *Special Eurobarometer 499 – Europeans' attitudes towards cyber security*, janvier 2020.

[21] Selon l'étude intitulée *The Global Disinformation Order* réalisée par l'université d'Oxford (septembre 2019), le nombre de pays touchés par des campagnes de désinformation politique a plus que doublé au cours des deux dernières années, pour atteindre 70 États.

semer la méfiance, voire nuire à la cohésion sociale et à la confiance dans les processus démocratiques (voir ***encadré 5***).

Encadré 5

Désinformation

La Commission européenne définit la désinformation comme la création, la présentation et la diffusion d'informations dont on peut vérifier qu'elles sont fausses ou trompeuses, dans un but lucratif ou dans l'intention délibérée de tromper le public, et qui sont susceptibles de causer un préjudice public[22]. Par préjudice public, on entend les menaces aux processus politiques et d'élaboration des politiques démocratiques et aux biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité.

À l'inverse des contenus illicites (qui comprennent les discours de haine et les contenus terroristes ou pédopornographiques), la désinformation couvre des contenus tout à fait légitimes. Par conséquent, elle rejoint les valeurs européennes fondamentales de la liberté d'expression et des médias. Selon la définition de la Commission, la désinformation ne comprend pas la publicité mensongère, les erreurs de citation, la satire, la parodie, ni les informations et commentaires partisans clairement identifiés.

14 Les nouvelles technologies et les logiciels modernes permettent de propager la désinformation de manière simple et relativement bon marché grâce aux **réseaux sociaux et autres médias en ligne**. La désinformation porte généralement sur des sujets sensibles qui sont susceptibles de diviser l'opinion et de susciter l'émoi, et qui ont donc plus de chances d'être relayés. Ces sujets peuvent concerner la santé (par exemple, les campagnes antivaccination), la migration, le changement climatique ou la justice sociale.

[22] Commission européenne, «Lutter contre la désinformation en ligne: une approche européenne», COM(2018) 236.

Campagnes de désinformation menées par des pays tiers pour influencer les processus démocratiques

15 La désinformation vise à polariser le débat démocratique, à créer ou à exacerber les tensions dans la société ainsi qu'à ébranler les systèmes électoraux. Elle a également des conséquences plus larges sur les sociétés européennes et leur sécurité. En définitive, elle porte atteinte à la liberté d'opinion et d'expression. La désinformation est souvent **commanditée par des acteurs de pays tiers** et vise à déstabiliser nos sociétés et nos systèmes démocratiques. Dans ce contexte, les campagnes massives de désinformation peuvent également comporter des activités de piratage de réseaux. Un exemple en est la campagne de propagande russe sur le référendum britannique concernant le départ de l'UE (voir ***encadré 6***).

Encadré 6

Campagnes de désinformation russes ciblant les processus décisionnels démocratiques[23]

À la mi-2016, une campagne visant à influencer le référendum britannique de juin 2016 relatif à la sortie de l'UE a été lancée depuis la Russie. Une analyse des *tweets* montre que dans les 48 heures précédant le vote, plus de 150 000 comptes russes ont posté des *tweets* sur le *#Brexit* ainsi que plus de 45 000 messages concernant le vote. Le jour du référendum, 1 102 *tweets* contenant le hashtag *#ReasonsToLeaveEU* ont été émis par des comptes russes.

16 La lutte contre la désinformation représente un défi majeur compte tenu de la nécessité d'atteindre le juste équilibre entre sécurité et protection des droits et libertés fondamentaux tout en encourageant l'innovation et l'ouverture du marché. L'UE a pris toute une série de mesures pour **lutter contre la désinformation**:

- en 2015, la ***task force*** **East StratCom** du Service européen pour l'action extérieure (SEAE) a été mise en place pour contrer les campagnes russes de

[23] Park advisors, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr et William Gangware, 2019.

désinformation[24]. Les experts ont salué son travail de promotion des politiques de l'UE, de soutien aux médias indépendants dans les pays du voisinage européen, ainsi que de prévision et de traçage de la désinformation et de lutte contre celle-ci[25];

- en 2018, l'ENISA a publié une **communication relative à la lutte contre la désinformation en ligne**[26]. L'idée était notamment d'aider à renforcer la fiabilité des contenus et de soutenir les efforts visant à améliorer l'éducation aux médias et aux informations;
- le Centre commun de recherche de la Commission européenne a élaboré, sur la base d'instruments stratégiques existants, un **code volontaire de bonnes pratiques fondé sur l'autorégulation**, auquel ont adhéré des plateformes en ligne et le secteur de la publicité[27];
- un **réseau** européen indépendant **de vérificateurs de faits** a été créé.

La désinformation à l'heure de la COVID-19 et la réaction de l'UE

17 La désinformation pose également problème dans le contexte de la **crise sanitaire de la COVID-19**[28] (voir ***encadré 7*** pour des exemples de désinformation à ce sujet).

---

[24] Conclusions du Conseil européen, EUCO 11/15, 20 mars 2015. Deux *task forces* supplémentaires, sur les Balkans occidentaux et les pays du voisinage méridional, ont été mises en place depuis lors.

[25] Dans un rapport du groupe de réflexion Atlantic Council, il était conseillé à l'UE d'inviter tous les États membres à détacher des experts nationaux auprès de la *task force*. Voir: Fried, D., et Polyakova, A., *Democratic Offense Against Disinformation*, 5 mars 2018.

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")*, avril 2018.

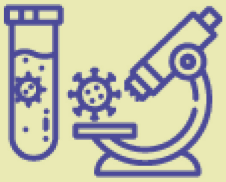
[27] Centre commun de recherche (JRC), *The digital transformation of news media and the rise of disinformation and fake news*, *JRC Technical Reports, JRC Digital Economy Working Paper 2018-02*, avril 2018.

[28] Reuters Institute et université d'Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, avril 2020.

Encadré 7

Exemples de fausses informations sur la COVID-19 signalées par la Commission[29]

Les fausses informations telles que «boire de la javel ou de l'alcool pur peut soigner les infections par le coronavirus» peuvent avoir un effet néfaste, puisque boire de la javel ou de l'alcool pur peut être très nocif. **Le centre antipoisons belge a enregistré une augmentation de 15 % du nombre d'incidents liés à la javel.**



Les **théories du complot**, telles que l'idée que le coronavirus est «une infection causée par les élites mondiales pour réduire la croissance de la population». Les preuves scientifiques sont pourtant claires: le coronavirus fait partie d'une famille de virus provenant des animaux, laquelle comte également des virus tels que ceux du syndrome respiratoire aigu sévère (SRAS) et du syndrome respiratoire du Moyen-Orient (SRMO).

Les **allégations non scientifiques** selon lesquelles les «installations 5G vont propager le virus» sont des théories sans aucun fondement qui ont donné lieu à des attaques sur des pylônes.

[29] Commission européenne, «Lutter contre la désinformation concernant la COVID-19», non daté.

18 En mars 2020, la Commission européenne, l'ENISA, la CERT-UE et Europol ont publié une **déclaration conjointe sur les menaces liées à la COVID-19**[30], signalant que des acteurs malveillants exploitaient activement les circonstances difficiles liées à la crise sanitaire pour cibler les télétravailleurs, les entreprises et les particuliers. Par ailleurs, l'ENISA a mis au point des campagnes d'information destinées aux secteurs touchés par la désinformation pendant la pandémie de COVID-19[31].

La vérification des informations est essentielle pour lutter contre la désinformation

19 L'UE a également redoublé d'efforts pour aider les vérificateurs de faits et les chercheurs qui étudient la désinformation en Europe. Elle a notamment établi un **observatoire européen des médias numériques** afin d'étudier et de mieux comprendre le phénomène de la désinformation: acteurs pertinents, vecteurs, instruments, méthodes, dynamiques de diffusion, cibles prioritaires et incidence sur la société. Les actions Provenance, SocialTruth, Eunomia et WeVerify sont d'autres exemples de projets de lutte contre la désinformation financés par l'UE.

20 En 2018, avec son **code de bonnes pratiques contre la désinformation**[32], l'UE proposait le premier ensemble mondial de normes d'autorégulation visant à lutter contre la désinformation. Ce code volontaire a été signé en octobre 2018 par des plateformes, des réseaux sociaux de premier plan, des annonceurs et le secteur de la publicité. Les signataires sont Facebook, Twitter, Mozilla, Google ainsi que des associations et membres du secteur publicitaire. Microsoft a souscrit au code de bonnes pratiques en mai 2019, et TikTok, en juin 2020.

Garantir le bon déroulement des élections au Parlement européen de 2019

21 La légitimité de nos systèmes démocratiques européens repose sur le principe qu'un corps électoral informé exprime sa volonté démocratique à travers des **élections libres et équitables**. Toute tentative malveillante et intentionnelle visant à porter atteinte à l'opinion publique et à la manipuler représente dès lors une grave menace

[30] Déclaration conjointe de la Commission européenne, de l'ENISA, de la CERT-UE et d'Europol, *Coronavirus outbreak*, 20 mars 2020.

[31] ENISA, Fiches d'information concernant la Covid-19, 2020.

[32] *EU Code of Practice on Disinformation*, septembre 2018.

pour nos sociétés. L'ingérence dans les élections et les atteintes aux infrastructures électorales peuvent avoir pour but d'influer sur le choix des électeurs, sur leur participation ou sur le processus électoral lui-même, y compris le vote proprement dit, le dépouillement des bulletins et la communication des résultats. Dans le sillage du référendum britannique, les élections européennes de 2019 ont débouché sur les premières mesures coordonnées entre les États membres destinées à **protéger l'intégrité des élections démocratiques**: celles au Parlement européen comme celles aux parlements nationaux.

22 Comme indiqué plus haut, la Commission a publié en avril 2018 une **communication intitulée «Lutter contre la désinformation en ligne: une approche européenne»**[33]. Elle a été suivie en septembre 2018 d'un **paquet électoral**[34] conçu pour protéger les élections européennes et nationales contre la désinformation et les cyberattaques. Le paquet est axé sur la protection des données, la transparence de la publicité politique et de son financement, la cybersécurité et les élections ainsi que sur les sanctions en cas de violation des règles relatives à la protection des données par les partis politiques. En outre, un **exercice conjoint** a été mené pour tester l'efficacité des mesures de réaction et des plans de crise des États membres et de l'UE lorsqu'il s'agit de protéger les élections au Parlement européen (voir ***encadré 8***).

[33] Commission européenne, «Lutter contre la désinformation en ligne: une approche européenne», COM(2018) 236 final.

[34] Commission européenne, «État de l'Union 2018», septembre 2018.

Encadré 8

EU ELEx19: protéger l'intégrité des élections au Parlement européen de 2019[35]

L'exercice EU ELEx19 sur la résilience des élections au Parlement européen avait pour objectif de trouver des moyens de prévenir, détecter et atténuer les incidents de cybersécurité susceptibles d'avoir des répercussions sur les élections européennes de 2019.

Fondé sur différents scénarios mettant en scène des menaces et des incidents facilités par l'internet, l'exercice a permis aux participants:

— d'obtenir une vue d'ensemble du niveau de résilience (en ce qui concerne les politiques adoptées ainsi que les capacités et compétences disponibles) des systèmes électoraux dans toute l'UE;

— de renforcer la coopération entre les autorités compétentes au niveau national (notamment les autorités électorales et les autres organes et agences concernés);

— de tester les plans de gestion de crise existants et les procédures conçues pour prévenir, détecter et gérer les cyberattaques et les menaces hybrides, y compris les campagnes de désinformation, et pour y réagir;

— d'améliorer la coopération transfrontière et de renforcer le lien avec les groupes de coopération concernés au niveau de l'UE (par exemple, le réseau de coopération électorale, le groupe de coopération SRI et le réseau des CSIRT);

— de recenser toutes les autres lacunes potentielles et de définir des mesures adéquates d'atténuation des risques à mettre en œuvre avant les élections du Parlement européen.

Plus de 80 représentants des États membres de l'UE, ainsi que des observateurs du Parlement européen, de la Commission européenne et de l'Agence de l'UE pour la cybersécurité, ont participé à cet exercice.

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5 avril 2019.

23 Enfin, en décembre 2018, le Conseil européen a adopté un **plan d'action contre la désinformation**[36] en vue d'apporter une réponse coordonnée et de compléter les efforts déployés au niveau national. Ce plan d'action prévoit des mesures spécifiques reposant sur quatre piliers: l'amélioration des capacités des institutions de l'UE à détecter, analyser et dénoncer les cas de désinformation; le renforcement des réponses coordonnées et conjointes à la désinformation; la mobilisation du secteur privé pour lutter contre la désinformation; la sensibilisation de la population et l'amélioration de la résilience de la société.

La cybersécurité dans l'UE: compétences, acteurs, stratégies et législation

La cybersécurité relève au premier chef de la compétence des États membres

24 Dans l'UE, la cybersécurité relève au premier chef de la **compétence des États membres**, en particulier pour ce qui est de la protection des informations sensibles liées à la sécurité nationale. Tous les États membres sont dotés d'une **stratégie nationale en matière de cybersécurité**, sur laquelle ils s'appuient pour gérer les risques qui pourraient éventuellement hypothéquer les bénéfices économiques et sociaux du cyberespace. Cependant, les capacités et l'engagement de États membres en matière de cybersécurité diffèrent toujours.

25 L'UE a un rôle à jouer dans l'établissement d'un **cadre réglementaire commun** au sein du marché unique européen, ainsi que dans la création de conditions permettant aux États membres de collaborer efficacement dans différents domaines d'action concernés par la cybersécurité: la justice et les affaires intérieures, le marché unique, les transports, la santé publique, la politique à l'égard des consommateurs ou encore la

[36] Commission européenne et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, «Plan d'action contre la désinformation», JOIN(2018) 36 final. Le plan d'action est axé sur: l'amélioration des capacités des institutions de l'UE à détecter, analyser et dénoncer les cas de désinformation; le renforcement des réponses coordonnées et conjointes; la mobilisation du secteur privé; la sensibilisation de la population et l'amélioration de la résilience de la société.

recherche. En politique extérieure, la cybersécurité intéresse la diplomatie et s'insère progressivement dans la politique de défense et de sécurité de l'UE.

26 Les principaux **acteurs** de la cybersécurité **au niveau de l'UE** sont présentés dans l'*encadré 9* ci-après.

Encadré 9

Les principaux acteurs de la cybersécurité au niveau de l'UE

La **Commission européenne** cherche à renforcer les capacités et la coopération en matière de cybersécurité, à faire de l'UE un acteur majeur dans ce domaine et à intégrer la cybersécurité dans les autres politiques de l'UE.

Un certain nombre d'agences de l'UE appuient la Commission, notamment l'**ENISA**, l'**EC3** et la **CERT-UE**. L'**Agence de l'Union européenne pour la cybersécurité** (ou **ENISA**, pour *European Network and Information Security Agency*, son ancienne appellation en anglais) joue principalement un rôle consultatif et contribue à l'élaboration des politiques, au renforcement des capacités et à la sensibilisation du public. Le **Centre européen de lutte contre la cybercriminalité (EC3)** d'Europol a été créé pour renforcer l'action répressive de l'UE à l'encontre de la cybercriminalité. L'**équipe d'intervention en cas d'urgence informatique (CERT)**, chargée d'aider l'ensemble des institutions, organes et agences de l'UE, est hébergée par la Commission.

Le **Service européen pour l'action extérieure (SEAE)** agit en qualité de chef de file dans les domaines de la cyberdéfense, de la cyberdiplomatie et de la communication stratégique et héberge des centres de renseignement et d'analyse. L'**Agence européenne de défense (ADE)** vise à développer des capacités de cyberdéfense.

À l'échelle de l'UE, les États membres agissent par l'intermédiaire du **Conseil**, qui dispose de nombreux organes de coordination et de partage d'informations (dont le groupe horizontal «Questions liées au cyberespace»). Le **Parlement européen** agit en tant que colégislateur.

Les **organisations du secteur privé**, y compris des organisations de l'industrie, des organes de gouvernance de l'internet et des universités, participent et contribuent financièrement à l'élaboration et à la mise en œuvre des politiques (par exemple, dans le cadre de partenariats public-privé contractuels (**PPPc**)).

La cybersécurité est au centre des préoccupations stratégiques de l'UE depuis 2013

27 La cybersécurité est au cœur des préoccupations politiques depuis 2013 au moins, année où la Commission a adopté sa **stratégie de cybersécurité**[37]. Cette stratégie poursuit cinq grands objectifs:

- renforcer la cyberrésilience;
- faire reculer la cybercriminalité;
- développer une politique et des moyens de cyberdéfense;
- développer les ressources industrielles et technologiques en matière de cybersécurité;
- instaurer une politique internationale en matière de cyberespace qui soit conforme aux valeurs essentielles de l'UE.

Au cours des années suivantes, d'autres stratégies de l'UE ont abordé la question de la cybersécurité (voir ***encadré 10***).

[37] Commission européenne, «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé», JOIN(2013) 1 final, 7 février 2013.

Encadré 10

Autres stratégies de l'UE abordant la question de la cybersécurité

- le **programme européen en matière de sécurité** (2015)[38], dont le but était d'améliorer l'action répressive et judiciaire à l'encontre de la cybercriminalité, principalement en actualisant les politiques et la législation existantes;
- la **stratégie pour un marché unique numérique** (2015)[39], dont l'objectif était d'améliorer l'accès aux biens et services numériques, ce qui nécessite de renforcer la sécurité, la confiance et l'inclusion de tous sur internet;
- la **stratégie globale de l'UE** (2016)[40], qui a défini un certain nombre d'initiatives destinées à renforcer le rôle international de l'UE. La cybersécurité en était un pilier central, de même que la lutte contre la désinformation.

28 Par ailleurs, en 2017, la Commission européenne et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont publié à l'intention du Parlement européen et du Conseil une **communication conjointe en faveur d'une cybersécurité pour l'UE**[41], dans laquelle elles demandent la mise en place de structures plus solides et plus efficaces pour promouvoir la cybersécurité et réagir aux cyberattaques dans les États membres, mais aussi dans les institutions, les agences et les organes de l'Union elle-même.

---

[38] Commission européenne, «Le programme européen en matière de sécurité», COM(2015) 185 final, 28 avril 2015.

[39] Commission européenne, «Stratégie pour un marché unique numérique en Europe», COM(2015) 192 final, 6 mai 2015.

[40] SEAE, «Vision partagée, action commune –Une Europe plus forte. Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne», juin 2016.

[41] Commission européenne et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, communication conjointe intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» (JOIN(2017) 450 final), 13 septembre 2017.

29 En juillet 2020, la Commission européenne a actualisé son programme 2015 et a adopté la **stratégie de l'UE pour l'union de la sécurité**[42] pour 2020-2025, qui fait de la cybersécurité une question d'importance stratégique. Dans cette stratégie, la Commission met plus particulièrement l'accent sur les menaces dites hybrides, qui allient cyberattaques et campagnes de désinformation menées de manière concertée par des acteurs étatiques et non étatiques de pays tiers dans l'intention de manipuler l'environnement de l'information et de s'en prendre aux infrastructures de base.

La législation de l'UE en matière de cybersécurité: la directive sur la sécurité des réseaux et de l'information, le RGPD, le règlement sur la cybersécurité et un nouveau mécanisme de sanctions

30 Principal pilier de la stratégie de cybersécurité de 2013, la pièce maîtresse de cette législation est la **directive sur la sécurité des réseaux et de l'information (directive SRI)**[43] de 2016, le premier acte législatif de l'UE sur la cybersécurité. Cette directive vise à parvenir à un niveau minimum de capacités harmonisées en obligeant les États membres à adopter des stratégies SRI nationales et à mettre en place des points de contact uniques et des centres de réponse aux incidents de sécurité informatique (CSIRT)[44]. Elle établit également des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels dans les secteurs critiques et pour les fournisseurs de services numériques.

---

[42] Commission européenne, Communication relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 final, 24 juillet 2020.

[43] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

[44] Ces centres sont intégrés au sein de structures de coopération instituées par la directive, à savoir le réseau des CSIRT (composé des CSIRT désignés par les États membres et de la CERT-UE, l'ENISA accueillant le secrétariat) et le groupe de coopération SRI (qui soutient et facilite la coopération stratégique et l'échange d'informations entre les États membres, la Commission accueillant le secrétariat).

31 Les États membres devaient transposer **la directive SRI en droit national** pour mai 2018. Ils devaient également désigner des «opérateurs de services essentiels» pour novembre 2018. La Commission européenne est tenue d'examiner périodiquement la mise en œuvre de la directive. Entre juillet et octobre 2020, pour atteindre son objectif stratégique clé, «adapter l'Europe à l'ère numérique», et poursuivre les objectifs de l'union de la sécurité, la Commission a organisé une consultation dont les résultats devaient servir à effectuer une première évaluation et analyse d'impact ex post de la directive SRI.

32 Par ailleurs, le **règlement général sur la protection des données**[45] (RGPD), entré en vigueur en 2016, est appliqué depuis mai 2018. Il a pour but de protéger les données à caractère personnel des citoyens européens en fixant des règles relatives à leur traitement et à leur diffusion. Il confère aux personnes concernées certains droits et impose des obligations aux responsables du traitement (les fournisseurs de services numériques) concernant l'utilisation et la transmission des informations.

33 En outre, le **règlement** européen **sur la cybersécurité**[46] introduit pour la première fois à l'échelle de l'UE un cadre de certification de cybersécurité pour les produits, services et processus des technologies de l'information et des communications (TIC). Ainsi, les entreprises qui exercent leurs activités dans l'UE ne devront plus certifier leurs produits, processus et services TIC qu'une seule fois, et leurs certificats seront reconnus sur tout le territoire de l'UE. Le règlement de l'UE sur la cybersécurité a également institué l'**Agence de l'Union européenne pour la cybersécurité** (ENISA, anciennement Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information). Il confie à l'Agence la mission de renforcer la coopération opérationnelle au niveau de l'UE en aidant les États membres qui le lui demandent à

[45] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[46] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (Texte présentant de l'intérêt pour l'EEE).

gérer certains incidents de cybersécurité et en soutenant la coordination de l'action de l'UE en cas de cyberattaques et de crises transfrontalières majeures.

34 Enfin, en mai 2019, le Conseil a établi un instrument juridique permettant à l'UE d'imposer des **mesures** restrictives ciblées **visant à décourager et contrer les cyberattaques** qui constituent une menace extérieure pour l'UE ou ses États membres[47]. En conséquence, l'UE est juridiquement habilitée à sanctionner les personnes ou entités qui:

- sont responsables de cyberattaques ou de tentatives de cyberattaques;
- apportent un soutien financier, technique ou matériel à ce type d'attaques, ou sont impliquées de toute autre manière dans celles-ci.

En juillet 2020, le Conseil a usé de ces nouvelles prérogatives pour la première fois (voir ***encadré 11***).

Encadré 11

Plus de rigueur: l'UE impose les toutes premières sanctions contre les auteurs de cyberattaques[48]

En juillet 2020, le Conseil a pris des mesures restrictives à l'encontre de six personnes physiques et de trois entités responsables de diverses cyberattaques ou y ayant participé. Parmi ces dernières figurent la tentative de cyberattaque contre l'Organisation pour l'interdiction des armes chimiques (OIAC) et celles connues sous les noms de *WannaCry*, *NotPetya* et *Operation Cloud Hopper*.

Les sanctions imposées comprennent une interdiction de pénétrer sur le territoire de l'UE et un gel des avoirs. En outre, il est interdit aux particuliers et aux entités de l'UE de mettre des fonds à la disposition des personnes physiques et des entités ou organismes inscrits sur la liste.

---

[47] Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.

[48] Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.

Cybersécurité et cyberdéfense

35 Ces dernières années, le cyberespace a fait l'objet d'une militarisation[49] et d'un armement[50] croissants. Il est aujourd'hui considéré comme le cinquième domaine d'activité militaire, après la terre, la mer, l'air et l'espace. Un **cadre stratégique de cyberdéfense de l'UE** a été adopté en 2014 et mis à jour en 2018[51]. Dans sa version actualisée en 2018, il définit des domaines prioritaires, dont le développement des capacités de cyberdéfense et la protection des réseaux de communication et d'information de la politique de sécurité et de défense commune (PSDC) de l'Union. La cyberdéfense relève également du cadre de coopération structurée permanente (CSP) et de la coopération entre l'Union européenne et l'Organisation du traité de l'Atlantique Nord (OTAN).

36 Les cas d'utilisation du cyberespace à des fins politiques ainsi que pour tester agressivement et pénétrer la cybersécurité de l'UE et des États membres sont devenus fréquents. Ces activités de cyberespionnage et de piratage informatique – qui ciblent des gouvernements nationaux, des entités politiques et des institutions de l'UE dans le but d'extraire et de collecter des informations classifiées – laissent penser que des opérations sophistiquées de cyberespionnage et de manipulation des données sont lancées contre l'UE et ses États membres. Le **cadre commun en matière de lutte contre les menaces hybrides** (2016) vise à contrer les cybermenaces pesant sur les infrastructures critiques et les utilisateurs privés et attire l'attention sur le fait que les cyberattaques peuvent également prendre la forme de campagnes de désinformation

---

[49] Centre d'études de la politique européenne, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, novembre 2018.

[50] Le logiciel malveillant utilisé pour perpétrer la cyberattaque *Wannacry*, attribuée à la Corée du Nord par les États-Unis, le Royaume-Uni et l'Australie, avait été initialement développé et stocké par l'Agence américaine de sécurité nationale pour exploiter les vulnérabilités de Windows.
Source: Greenberg, A., WIRED, 19 décembre 2017. Au lendemain des attaques, Microsoft a dénoncé le fait que des gouvernements gardent le secret sur des failles logicielles et réitéré son appel à une convention de Genève numérique.

[51] «Cadre stratégique de cyberdéfense de l'UE (dans sa version actualisée en 2018)», document n° 14413/18 du 19 novembre 2018.

sur les médias sociaux[52]. Il fait également état de la nécessité d'améliorer la connaissance de la situation et de renforcer la coopération entre l'UE et l'OTAN, à laquelle les déclarations communes UE-OTAN de 2016 et de 2018[53] ont donné corps.

Dépenses consacrées à la cybersécurité dans l'UE: des investissements épars et à la traîne

L'EU-27 investit moins dans la cybersécurité que les États-Unis d'Amérique

37 Il est difficile de fournir une estimation des dépenses publiques consacrées à la cybersécurité, en raison de la nature transversale de cette dernière et du fait qu'il est souvent impossible de distinguer les dépenses informatiques générales de celles spécifiques à la cybersécurité[54]. Cela étant dit, selon les données disponibles, il semblerait que les **dépenses publiques consacrées à la cybersécurité** dans l'UE sont comparativement faibles:

- en 2020, le budget du gouvernement fédéral des États-Unis alloué à la seule cybersécurité s'élevait à quelque **17, 4 milliards de dollars**[55];
- à titre de comparaison, la Commission a estimé que les dépenses publiques annuelles consacrées à la cybersécurité par l'ensemble des États membres de l'UE (dont la somme des produits intérieurs bruts est presque équivalente au PIB des États-Unis) oscillaient entre **un et deux milliards d'euros**[56];

---

[52] Commission européenne/Service européen pour l'action extérieure, Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne, JOIN(2016) 18 final, 6 avril 2016.

[53] Déclarations communes du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du traité de l'Atlantique Nord, 8 juillet 2016 et 10 juillet 2018.

[54] Commission européenne, COM(2018) 630 final, 12 septembre 2018.

[55] La Maison-Blanche, *Cybersecurity budget fiscal year 2020*.

[56] Document de travail des services de la Commission européenne: *Impact Assessment Accompanying the document «Proposal for a Regulation of the European Parliament and of*

- exprimées en pourcentage du PIB, les dépenses publiques consacrées à la cybersécurité sont estimées, pour de nombreux États membres, à **un dixième de celles des États-Unis**, voire moins[57].

2014-2020: les financements de l'UE en faveur de la cybersécurité sont dispersés entre plusieurs instruments différents

38 Selon la Commission[58], le budget général de l'UE compte au moins **dix instruments différents** permettant de financer des questions liées à la cybersécurité (voir l'***encadré 12*** pour une liste des principaux programmes sur le plan financier). Au total, les financements de l'UE en faveur de la cybersécurité non militaire représentaient **moins de 200 millions d'euros par an** sur la période 2014-2020. En outre, il n'existe à l'échelle de l'UE aucun instrument financier destiné à soutenir la coordination, par les États membres, de leurs activités en matière de cybersécurité.

the Council establishing the Digital Europe programme for the period 2021-2027», SWD(2018) 305 final, 6 juin 2018.

[57] Centre d'études stratégiques de La Haye, *Dutch investments in ICT and cybersecurity: putting it in perspective*, décembre 2016.

[58] Commission européenne, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final, 12 septembre 2018.

Encadré 12

Programmes de l'UE visant à soutenir les projets de cybersécurité (2014-2020)

- Pour la période 2014-2020, 600 millions d'euros environ ont été alloués aux projets liés à la cybersécurité et à la cybercriminalité au titre du **programme de recherche Horizon 2020**. Ce montant comprend 450 millions d'euros consacrés aux partenariats public-privé contractuels (PPPc) relatifs à la cybersécurité pour la période 2017-2020, le but étant d'attirer des fonds privés supplémentaires à hauteur de 1,8 milliard d'euros.

- Les **Fonds structurels et d'investissement européens (Fonds ESI)** prévoient jusqu'à la fin de l'année 2020 une contribution pouvant atteindre 400 millions d'euros pour les États membres investissant dans la cybersécurité.

- Le **mécanisme pour l'interconnexion en Europe (MIE)** a financé des investissements à hauteur d'environ 30 millions d'euros par an. De 2016 à 2018, il a notamment cofinancé les CERT nationales que les États membres sont tenus d'établir en application de la directive SRI, à hauteur de 13 millions d'euros par an environ[59].

- Le **volet «police» du Fonds pour la sécurité intérieure (FSI-Police)** finance des études, des réunions d'experts et des activités de communication, auxquelles il a consacré près de 62 millions d'euros entre 2014 et 2017. Dans le cadre de la gestion partagée, les États membres peuvent également bénéficier de subventions d'équipement, de formation, de recherche et de collecte de données. Dix-neuf États membres ont fait appel à ces subventions, pour un montant total de 42 millions d'euros.

- Le **programme «Justice»** a fourni 9 millions d'euros pour soutenir la coopération judiciaire et les traités d'entraide judiciaire, et plus particulièrement les échanges de données électroniques et d'informations financières.

[59] Article 9, paragraphe 2, de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI).

39 En outre, 500 millions d'euros provenant du budget de l'UE ont été alloués au **programme européen de développement industriel dans le domaine de la défense** en 2019 et 2020[60]. Ce programme vise à améliorer la coordination et l'efficience des dépenses des États membres en matière de défense grâce à des incitations au développement conjoint. L'objectif est de mobiliser au total, par l'intermédiaire du Fonds européen de la défense, 13 milliards d'euros d'investissements dans les capacités de défense de l'après-2020, dont une partie couvrira la cyberdéfense. Enfin, dans le cadre de l'**initiative de sécurité européenne**, la Banque européenne d'investissement fournira 6 milliards d'euros de financements à double usage (recherche et développement/cybersécurité et sécurité civile) entre 2018 et 2020[61].

2021-2027: le nouveau programme pour une Europe numérique

40 Dans ses conclusions de juillet 2020 concernant le nouveau cadre financier pluriannuel (CFP) pour la période 2021-2027, le Conseil a prévu que le **programme pour une Europe numérique**[62] investirait dans les capacités numériques stratégiques essentielles telles que le calcul à haute performance, l'intelligence artificielle et la cybersécurité de l'UE. Ce programme viendra compléter d'autres instruments, notamment Horizon Europe et le mécanisme pour l'interconnexion en Europe, afin d'appuyer la transformation numérique en Europe.

---

[60] Commission européenne, Règlement (UE) 2018/1092 du Parlement européen et du Conseil du 18 juillet 2018 établissant le programme européen de développement industriel dans le domaine de la défense visant à soutenir la compétitivité et la capacité d'innovation de l'industrie de la défense de l'Union (JO L 200, 7.8.2018, p. 30).

[61] Banque européenne d'investissement, Cadre opérationnel du Groupe BEI et Plan d'activité 2018, 12.12.2017.

[62] Commission européenne, *Europe investing in digital: the Digital Europe Programme*, septembre 2020.

41 Le Conseil a également décidé de consacrer 6,8 milliards d'euros au programme pour une Europe numérique sur la période 2021-2027, autrement dit **970 millions d'euros par an**. Il s'agit d'une augmentation considérable par rapport à la période 2014-2020, qui reste néanmoins inférieure à la proposition initiale de la Commission (8,2 milliards d'euros sur la même période, dont 2 milliards consacrés au renforcement du secteur de la cybersécurité et de la protection sociale en général, par exemple dans le cadre de la mise en œuvre de la directive SRI).

DEUXIÈME PARTIE – Vue d'ensemble des travaux des ISC

Introduction

42 La cybersécurité et notre autonomie numérique sont devenues des enjeux d'une importance stratégique pour l'UE et ses États membres. La gouvernance en matière de cybersécurité dans le secteur public et le secteur privé continue à présenter des faiblesses dans tous les États membres, bien qu'à des degrés divers. Cela compromet notre capacité à limiter les cyberattaques et, le cas échéant, à y réagir.

43 Néanmoins, en 2018, une enquête réalisée auprès des institutions supérieures de contrôle (ISC) de l'UE a révélé que la moitié d'entre elles environ n'avaient jamais réalisé d'audit de la cybersécurité. Depuis, les ISC ont enclenché la vitesse supérieure dans le domaine de la cybersécurité, en centrant plus particulièrement leurs audits sur la protection des données, sur l'état de préparation des systèmes face aux cyberattaques ainsi que sur la protection des systèmes de services publics essentiels. Elles se sont également penchées sur d'autres sujets d'importance majeure. Ces audits ne peuvent bien entendu pas tous être rendus publics, certains pouvant concerner des informations sensibles (liées à la sécurité nationale).

44 Compte tenu de l'importance que revêt la cybersécurité pour le fonctionnement de nos sociétés et de nos institutions politiques, le comité de contact a décidé de lui consacrer le compendium d'audit de cette année. Cette deuxième partie offre une synthèse des résultats d'une sélection d'audits sur la cybersécurité réalisés par les ISC de 12 États membres qui ont participé et par la Cour des comptes européenne. Chacune de ces ISC a contribué en sélectionnant un rapport d'audit, dont un résumé est présenté dans la troisième partie. De nombreux autres audits ont été réalisés sur le sujet, comme en témoignent les autres rapports mentionnés par les ISC participantes.

Méthodologie d'audit et thèmes couverts

45 En ce qui concerne les types d'audits dont il est fait la synthèse dans le présent compendium, la plupart des ISC participantes ont réalisé des audits de performance sur des sujets liés à la cybersécurité, tandis que deux d'entre elles (celles de Pologne et de Hongrie) ont effectué des audits de conformité et l'une d'elles (la Cour des comptes européenne) a procédé à une analyse des politiques.

46 Au moment de concevoir leurs audits, la plupart des ISC ont décidé que le sujet d'audit devait être examiné suivant deux approches au moins. Il pouvait s'agir d'un examen de documents stratégiques ou de politiques précises de haut niveau (national, par exemple), d'une analyse des procédures visant à évaluer leur conformité avec la méthodologie COBIT établie (voir ***encadré 13***) ou d'un examen de l'efficacité des systèmes de gestion informatique en place. Une ISC (la Cour des comptes néerlandaise) a même fait appel à des pirates éthiques pour tester l'efficacité des systèmes de cybersécurité concernant les contrôles aux frontières et les structures hydrauliques critiques. L'***encadré 14*** présente une synthèse schématique des méthodes et techniques utilisées par les différentes ISC pour réaliser leurs travaux d'audit.

Encadré 13

Qu'est-ce que COBIT?

Les objectifs de contrôle pour l'information et les technologies correspondantes (COBIT, pour *Control Objectives for Information and Related Technology*) forment un cadre de bonnes pratiques et de procédures reconnues pour la gestion et la gouvernance informatiques, lequel est défini par l'association des professionnels de l'audit et du contrôle des systèmes d'information (ISACA, pour *Information Systems Audit and Control Association*). Le cadre COBIT aide l'organisation à atteindre ses objectifs stratégiques grâce à une utilisation efficace des ressources disponibles et à la minimisation des risques informatiques. Il met en lien la gouvernance des entreprises et la gouvernance informatique. Ce lien est établi grâce à la mise en rapport des objectifs commerciaux et informatiques, à la mise en place d'indicateurs et de modèles de maturité permettant de mesurer le degré de réalisation des objectifs ainsi qu'à la définition des responsabilités des propriétaires des processus métier et des processus informatiques.

47 Les thèmes traités dans le cadre des audits de la cybersécurité étaient très variés. Certaines ISC ont axé leurs audits sur des domaines d'intérêt public bien particuliers; l'ISC néerlandaise, par exemple, a procédé à un audit de la cybersécurité de ses défenses maritimes critiques et de ses systèmes de gestion de l'eau. D'autres, telles que les ISC irlandaise et hongroise, se sont intéressées à des questions plus horizontales, telles que la mise en œuvre de la stratégie nationale en matière de cybersécurité et la protection des données à caractère personnel et des actifs de données nationaux. Elles ont cependant toutes examiné des questions susceptibles d'avoir un impact négatif sur les infrastructures ou les services publics.

48 Les ISC d'Estonie et de Lituanie ont reconnu l'importance stratégique des actifs de données nationaux, essentiels à la sécurité nationale et à la protection de leur intégrité contre les cyberattaques extérieures. L'ISC danoise a réalisé un audit visant à évaluer spécifiquement dans quelle mesure quatre organismes publics étaient capables de résister à des attaques par logiciel rançonneur. Les ISC néerlandaise, polonaise et portugaise ont effectué des audits de l'efficacité de différents systèmes informatiques servant aux contrôles aux frontières (respectivement à l'aéroport néerlandais de Schiphol, aux frontières portugaises et, en Pologne, au commandement de la garde aux frontières et au ministère de l'intérieur et de l'administration). Ces audits concernaient donc eux aussi la sécurité intérieure de l'UE.

Période couverte par l'audit

49 Les rapports d'audit sélectionnés pour figurer dans le présent compendium ont été publiés entre 2014 et 2020. La plupart d'entre eux portaient sur une période de deux ans ou plus, mais ils étaient quatre (réalisés par le Danemark, l'Estonie, la France et le Portugal) à couvrir une seule année.

Objectifs d'audit

50 Dans le cadre de leurs travaux d'audit, les différentes ISC ayant contribué au présent compendium ont analysé toute une série de risques, à savoir: les menaces pesant sur les droits des citoyens européens du fait de l'utilisation abusive de leurs données personnelles, le risque que les institutions ne soient pas à même d'assurer les services publics essentiels – ou qu'elles puissent ne les assurer que d'une manière limitée –, ou encore le risque de conséquences graves pour la sécurité publique, le bien-être public et l'économie dans les États membres ainsi que pour la cybersécurité au sein de l'UE. Quatre des ISC (l'estonienne, la hongroise, la néerlandaise et la portugaise), si pas plus, ont couvert au moins trois des thèmes mentionnés dans leurs rapports d'audit choisis pour figurer dans le présent compendium.

51 La cybersécurité continue à relever de la compétence des États membres. Néanmoins, la législation de l'UE s'est étoffée et précisée au fil du temps, et la plupart des institutions et organes audités par les ISC contribuent déjà à la réalisation des objectifs stratégiques de l'UE en matière de cybersécurité, dans des mesures différentes toutefois. Par exemple, l'ISC irlandaise, l'*Office of the Comptroller and Auditor General*, a procédé à un audit de la mise en œuvre de la directive relative à la

sécurité des réseaux et des systèmes d'information dans l'Union, qui vise à améliorer la résilience des principaux réseaux et systèmes d'information, et a formulé des recommandations à cet égard. De même, l'audit de l'ISC hongroise a porté sur la conformité avec les directives existantes de l'UE.

52 Il est également précisé, dans l'***encadré 14***, si l'audit a eu pour effet de contribuer à une amélioration de la cyberrésilience des entités auditées, à une diminution de la cybercriminalité, à l'élaboration de politiques de cyberdéfense, à un renforcement des compétences, à une amélioration au niveau du développement des technologies et à la réalisation de progrès du point de vue de la coopération internationale, c'est-à-dire aux principaux objectifs de la stratégie de l'UE en matière de cybersécurité. Dans la plupart des cas, les recommandations formulées par les ISC portaient sur plus de deux objectifs stratégiques visés par l'UE.

53 De plus, les travaux d'audit menés par les ISC ont permis de mettre en lumière certaines lacunes en matière de sécurité ou de mise en œuvre qui ont incité les institutions auditées à déployer des efforts supplémentaires. Au Danemark par exemple, alors que les travaux d'audit étaient encore en cours, quatre institutions auditées ont commencé à mettre en place plusieurs contrôles de sécurité prospectifs en vue d'accroître considérablement le niveau de protection contre les attaques par logiciel rançonneur et de renforcer les capacités de défense et la cyber-résilience, réduisant ainsi leur future exposition à la cybercriminalité.

54 Nous constatons également que les recommandations d'audit étaient adressées à différents niveaux de management et de responsabilité: l'administration centrale, les ministères et agences à un niveau opérationnel ou les propriétaires de systèmes informatiques.

Encadré 14

Aperçu des travaux d'audit des ISC figurant à titre de contribution dans le présent compendium (première partie)

Principal domaine prioritaire		Danemark	Estonie	Irlande	France	Lettonie	Lituanie	Hongrie	Pays-Bas	Pologne	Portugal	Finlande	Suède	UE (Cour des comptes
Type d'audit	Audit de la performance	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Audit de conformité							✓		✓				
	Analyse													✓
Approche d'audit	Examen des politiques	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Examen des procédures	✓	✓		✓		✓	✓		✓	✓	✓		
	Examen des systèmes	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Évaluation de la fiabilité au moyen de tests directs								✓		✓			
Menaces abordées	Impact sur les droits individuels		✓		✓			✓			✓			✓
	Impact sur les infrastructures ou services publics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Impact sur la sécurité nationale		✓	✓		✓	✓	✓	✓		✓			
	Impact sur la sécurité au sein de l'UE	✓							✓		✓			✓

Aperçu des travaux d'audit des ISC figurant à titre de contribution dans le présent compendium (deuxième partie)

Principal domaine prioritaire		Danemark	Estonie	Irlande	France	Lettonie	Lituanie	Hongrie	Pays-Bas	Pologne	Portugal	Finlande	Suède	UE (Cour des comptes
Objectifs stratégiques de cybersécurité de l'UE couverts	Renforcer la cyberrésilience	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Faire reculer la cybercriminalité	✓					✓							✓
	Développer une politique et des moyens de défense	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Développer des ressources technologiques				✓	✓			✓				✓	
	Renforcer la coopération internationale (politiques)			✓				✓						✓
Niveau du destinataire des recommandations	Administration centrale	✓	✓				✓					✓	✓	✓
	Niveau opérationnel (ministères et agences)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Propriétaires de systèmes informatiques	✓			✓			✓	✓	✓				

Principales observations d'audit

55 Les principales observations d'audit formulées par les ISC sont résumées dans les sections suivantes.

Audits de la performance

56 L'**ISC danoise, *Rigsrevisionen*,** a cherché à déterminer si les institutions gouvernementales essentielles sélectionnées bénéficiaient d'une protection satisfaisante contre les logiciels rançonneurs. Les institutions gouvernementales sont souvent la cible de cyberattaques, et les logiciels rançonneurs comptent parmi les plus importantes menaces qui pèsent actuellement sur la cybersécurité. L'audit concernait l'autorité danoise des données de santé, le ministère des affaires étrangères, le réseau ferroviaire danois (*Banedanmark*) et l'agence danoise de gestion des urgences. Ces quatre institutions ont été sélectionnées car elles assurent des services essentiels en matière de santé, d'affaires étrangères, de transport et de préparation aux situations d'urgence, des domaines dans lesquels garantir l'accès aux données peut revêtir une importance critique. L'audit a révélé que les quatre institutions ne bénéficiaient pas d'une protection satisfaisante contre les logiciels rançonneurs. Il a également montré qu'elles n'avaient pas mis en place plusieurs contrôles de sécurité courants permettant de réduire les attaques. L'audit a débouché sur la conclusion qu'il était important que les institutions envisagent de mettre en œuvre des contrôles de sécurité prospectifs pour renforcer leur résilience aux attaques par logiciel rançonneur.

57 L'**ISC estonienne, *Riigikontroll*,** a observé que la préservation de l'indépendance de l'Estonie passait non seulement par la défense physique du territoire, mais aussi par la protection des actifs numériques d'importance capitale pour l'État. Les actifs numériques ayant le plus besoin de protection sont les données relatives aux citoyens, au territoire et à la législation. Les données concernant la propriété, l'immobilier et les droits des résidents estoniens doivent également être sécurisées. L'ISC estonienne a envisagé la possibilité de cybermenaces en cas d'escalade des problèmes de sécurité. De tels scénarios de risques et une augmentation du nombre d'incidents liés à la sécurité de l'information, tels que les cyberattaques et les fuites de données, peuvent compromettre l'intégrité de données et bases de données qui revêtent la plus haute importance pour l'État. Par conséquent, les auditeurs ont cherché à savoir comment l'État déterminait quelles étaient les données et bases de données cruciales pour garantir la sécurité nationale. Ils ont conclu que malgré la mise en œuvre du système

de sécurité minimale à trois niveaux ISKE[63], obligatoire pour les organismes publics, plusieurs bases de données critiques présentaient encore d'importantes lacunes en matière de sécurité de l'information.

58 L'**ISC irlandaise, *Office of the Comptroller and Auditor General*,** a analysé les progrès accomplis en ce qui concerne les mesures de cybersécurité depuis l'établissement en 2011 du Centre national irlandais de cybersécurité, dirigé par le service des communications, de l'action pour le climat et de l'environnement. Le Centre s'attache surtout à sécuriser les réseaux publics, à aider les entreprises et les particuliers à protéger leurs propres systèmes et à garantir la sécurité des infrastructures nationales critiques. L'audit a débouché sur la conclusion que malgré la fonction cruciale exercée par le Centre national de cybersécurité, le niveau de financement au cours de ses quatre premières années de fonctionnement était considérablement inférieur à celui initialement envisagé et que le Centre avait besoin d'un plan stratégique pour définir son orientation générale. En outre, Il a été conclu que le rôle des différents organismes enquêtant sur les cybercrimes et les incidents portant atteinte à la sécurité nationale devait être clarifié et enfin, qu'il n'avait pas encore été procédé à l'élaboration de la stratégie nationale exigée dans la directive relative à la sécurité des réseaux et des systèmes d'information dans l'Union.

59 La **Cour des comptes française** a examiné «Parcoursup», une nouvelle plateforme numérique qui représente une source d'informations sur les cursus universitaires disponibles et sur les conditions d'admission. L'objectif de la plateforme est d'établir une meilleure correspondance entre les aptitudes et résultats scolaires des étudiants du secondaire et le contenu des programmes de l'enseignement supérieur. L'audit a révélé que les pouvoirs publics étaient parvenus, grâce à cette plateforme numérique, à centraliser l'accès aux études post-secondaires de manière à faire face à l'essor de l'enseignement supérieur. Cependant, le nouveau «Parcoursup» était le fruit d'un remaniement hâtif du précédent système, et aucun changement structurel important n'avait été apporté. Les faiblesses du système d'information sur le plan de la sécurité, de la performance et de la robustesse n'ont donc pas été corrigées. La plateforme présente toujours des risques importants en termes de qualité et de continuité du service public ainsi que de sécurité des données personnelles.

[63] Le système ISKE est un cadre normalisé en matière de sécurité de l'information. Conçu pour le secteur public estonien, il est obligatoire pour les organes de l'administration centrale et locale qui traitent des bases de données ou des registres.

60 L'**ISC lettone, *Valsts Kontrole*,** a réalisé un audit de la performance sur l'efficience des infrastructures publiques des technologies de l'information et de la communication (TIC). L'audit visait à vérifier si l'administration publique avait adopté une approche unifiée pour gérer de manière efficiente les infrastructures TIC et si les institutions avaient évalué les avantages de la centralisation. Il a révélé que la réticence des autorités à gérer les infrastructures TIC de manière centralisée s'était traduite par l'établissement d'un certain nombre de salles de serveurs, augmentant ainsi considérablement les frais de maintenance. La sécurité de la plupart des salles de serveurs était menacée, et les centres de données n'étaient pas suffisamment protégés contre les accès physiques et les risques environnementaux. En outre, les institutions n'avaient adopté aucune pratique consistant à évaluer à intervalles réguliers s'il était moins coûteux d'assurer la maintenance des infrastructures TIC en interne, de collaborer avec une autre institution ou de sous-traiter la maintenance des TIC. À l'issue de l'audit, il a été recommandé d'établir un système de suivi régulier qui permettrait à l'administration publique d'être évaluée dans sa globalité, en tant que système unique.

61 L'**ISC lituanienne, *Valstybės kontrolė*,** a observé l'importance des sources nationales d'informations électroniques critiques, notamment pour la gestion des finances publiques, pour l'administration fiscale ou pour le fonctionnement du système de santé. La perte d'informations critiques et l'indisponibilité des systèmes d'information correspondants pourraient avoir de graves conséquences pour la sécurité publique, le bien-être public et l'économie. L'audit visait à apprécier la gestion (le contrôle général) et la maturité des sources nationales d'informations critiques. Il a permis de détecter des problèmes systémiques en ce qui concerne l'élaboration et la mise en œuvre de la politique relative aux sources nationales d'informations publiques mais aussi le mécanisme de gestion de ces ressources. L'audit a débouché sur la conclusion que le faible niveau de maturité des sources nationales d'informations critiques indiquait la présence de faiblesses dans l'élaboration et la mise en œuvre de la politique relative aux sources nationales d'information, ce qui rend ces dernières plus vulnérables. Il a également été conclu qu'il convenait d'améliorer le mécanisme de gestion pour renforcer la sécurité des sources nationales d'informations.

62 En 2018, la **Cour des comptes néerlandaise** a décidé de réaliser des audits sur la cybersécurité dans certains secteurs essentiels pour la société. L'audit a d'abord porté sur la gestion des eaux, vitale pour une nation dont une grande partie est située sous le niveau de la mer, puis sur les contrôles automatisés aux frontières, en raison de l'importance de l'aéroport de Schiphol (Amsterdam) en tant que plateforme internationale et point d'accès vers le pays. Le ministre des infrastructures et de la gestion des eaux a qualifié d'«éléments critiques» du secteur un certain nombre de structures hydrauliques gérées par la direction générale des travaux publics et de la gestion des eaux (l'entité auditée). De nombreux systèmes informatiques servant à faire fonctionner les structures hydrauliques critiques datent des années 1980 et 1990, une époque où la cybersécurité était rarement prise en considération. Le ministre de la défense et celui de la justice et de la sécurité se partagent la responsabilité des contrôles réalisés par les gardes-frontières néerlandais à l'aéroport de Schiphol. Les deux ministères disposent de systèmes informatiques sur lesquels les gardes-frontières s'appuient. Ces systèmes sont essentiels aux opérations aéroportuaires et sont utilisés pour traiter des données très sensibles. Ainsi, ils constituent des cibles de choix pour des cyberattaques dont le but est de saboter, d'espionner ou de manipuler les contrôles aux frontières. Les auditeurs ont examiné si les entités auditées étaient prêtes à gérer les cybermenaces et si leur action était efficace. Dans le cas des structures hydrauliques, pour pouvoir atteindre ses propres objectifs en matière de cybersécurité, l'entité auditée devait encore intensifier ses efforts, tant sur le plan de la détection des menaces que sur celui de la réponse apportée. En ce qui concerne les contrôles aux frontières, les mesures de cybersécurité n'ont été jugées ni adéquates ni adaptées aux besoins futurs.

63 L'**ISC portugaise, le *Tribunal de Contas*,** a réalisé un audit des systèmes d'information qui sous-tendent la délivrance, l'émission et l'utilisation des passeports électroniques portugais (PEP), en particulier le contrôle automatisé des passagers par la lecture des données biométriques aux frontières portugaises. Les auditeurs ont vérifié la conformité avec le droit de l'UE, les législations nationales, les normes internationales et les lignes directrices régissant la délivrance, l'émission et l'utilisation des PEP, y compris le caractère approprié du cadre juridique national. Ils ont examiné l'efficacité des principaux processus associés au cycle de vie du PEP, notamment ceux qui concernent la délivrance, l'émission et l'utilisation du passeport. Ils ont également analysé certains aspects critiques de la performance des systèmes d'information, en particulier le respect des exigences de sécurité relatives aux systèmes d'information des passeports électroniques portugais (SIPEP).

64 L'**ISC finlandaise, *Valtiontalouden tarkastusvirasto*,** a cherché à déterminer si la cyberprotection au sein de l'administration centrale était aussi efficace que possible et si elle présentait un rapport coût-efficacité optimal. L'audit était centré sur la gestion de la cybersécurité dans l'administration centrale. Parmi les entités auditées figuraient les autorités chargées de la cyberprotection dans l'administration centrale (le bureau du Premier ministre, le ministère des finances ainsi que le ministère des transports et des communications) et celles responsables des activités de cyberprotection et des services informatiques centralisés dans l'administration centrale. Au sein du gouvernement finlandais, les compétences en matière de cyberprotection sont décentralisées, chaque organe étant responsable de sa propre cybersécurité. Les auditeurs ont recommandé au ministère des finances de définir et de mettre en œuvre un modèle à grande échelle pour la gestion opérationnelle des éventuels incidents de cybersécurité concernant les services TIC de l'administration centrale. Ils lui ont également recommandé de déterminer comment tenir compte de l'aspect «cybersécurité» dans le financement des services, sur tout le cycle de vie de ces derniers, et d'améliorer la connaissance de la situation opérationnelle en enjoignant aux autorités de signaler les cyberincidents au centre de cybersécurité.

65 L'**ISC suédoise, *Riksrevisionen*,** a examiné l'incidence des systèmes informatiques obsolescents dans l'administration centrale afin de déterminer si le gouvernement et les autorités avaient pris les mesures appropriées pour empêcher ces systèmes de faire obstacle à une transition numérique efficace. L'audit a révélé qu'un grand nombre d'organismes publics étaient dotés de systèmes informatiques obsolescents. Dans nombre d'organismes audités, cette obsolescence frappait un ou plusieurs systèmes informatiques essentiels à la poursuite des activités. Qui plus est, une grande partie d'entre eux n'avaient pas adopté l'approche adéquate pour le développement et la gestion du soutien informatique. Ils étaient nombreux à ne pas disposer d'une description d'ensemble de la manière dont les stratégies, les processus opérationnels et les systèmes étaient liés. De manière générale, il a été conclu que la plupart des organismes n'étaient pas encore parvenus à gérer efficacement les problèmes liés à l'obsolescence des systèmes informatiques. L'ISC suédoise estime que le problème est tellement grave et généralisé qu'il représente un obstacle à la poursuite d'une transition numérique efficace de l'administration publique.

Audits de conformité sur la cybersécurité

66 L'**ISC de Hongrie** a observé que la sécurité des actifs de données nationaux représentait pour la société un intérêt fondamental du point de vue de la préservation et de la protection des valeurs nationales. Il est essentiel de garantir l'amélioration de la sécurité des données personnelles et publiques dans les actifs de données nationaux de Hongrie afin de renforcer la confiance que les citoyens accordent à l'État et d'assurer un fonctionnement continu et fluide de l'administration publique. L'objectif de l'audit de conformité sur la protection des données était de déterminer si la Hongrie avait établi un cadre réglementaire et opérationnel pour la protection des données et si les principales organisations de gestion des données respectaient les exigences de sécurité en ce qui concerne la gestion des données et l'externalisation du traitement des données. L'audit a débouché sur la conclusion que les règlements internes relatifs aux activités de gestion des données établis par les organisations responsables en la matière garantissaient la protection des actifs de données nationaux, qui font partie intégrante des actifs nationaux, conformément aux dispositions légales en vigueur entre 2011 et 2015. Les responsables du traitement des données appliquaient les exigences de manière appropriée, et les transferts de données vers des tiers étaient correctement exécutés.

67 L'**ISC polonaise, *Najwyższa Izba Kontroli*,** a cherché à déterminer si les données collectées dans les systèmes conçus pour exécuter d'importantes missions publiques étaient sécurisées. L'audit portait sur une sélection de six institutions chargées de missions publiques importantes. Le degré de préparation et de mise en œuvre du système de sécurité de l'information ne garantissait pas un niveau de sécurité acceptable aux données collectées dans les systèmes informatiques utilisés pour réaliser d'importantes missions publiques. Les processus de sécurité de l'information étaient exécutés de manière désordonnée et – faute de procédures définies – intuitive. Sur les six institutions auditées, une seule appliquait le système de sécurité de l'information, même s'il convient de noter que son fonctionnement présentait lui aussi des défaillances considérables. Les auditeurs ont conclu qu'il importait que des recommandations et exigences générales relatives à la sécurité informatique soient élaborées et mises en œuvre au niveau central, et qu'elles s'appliquent à toutes les entités publiques.

Analyses de la cybersécurité

68 La **Cour des comptes européenne** a analysé la politique menée par l'UE dans le domaine de la cybersécurité et a recensé les principales difficultés à surmonter pour mettre en place une politique efficace. Les travaux ont porté sur la sécurité des réseaux et de l'information, la cybercriminalité, la cyberdéfense et la désinformation. Ils ont permis de relever un certain nombre de lacunes dans la législation de l'UE en matière de cybersécurité, et de noter que la législation existante n'est pas transposée uniformément par les États membres. Enfin, le document d'analyse a attiré l'attention sur le manque de données fiables concernant les cyberincidents au niveau de l'UE et sur le fait que l'UE et ses États membres ne disposaient pas d'une vue d'ensemble complète des dépenses consacrées à la cybersécurité. Il fait également état d'obstacles rencontrés par les agences de l'UE concernées par la cybersécurité pour se doter de ressources, y compris des difficultés à attirer et à retenir les talents. Le décalage entre les financements alloués à la cybersécurité et les objectifs stratégiques de l'UE était lui aussi source de difficultés.

TROISIÈME PARTIE – Synthèse des rapports des ISC

Danemark
Rigsrevisionen

Protection contre les attaques par logiciel rançonneur

Date de publication: 2017

Hyperlien vers le rapport: synthèse du rapport (en anglais)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: avril à septembre 2017

Synthèse du rapport

Sujet de l'audit

L'audit visait à déterminer si les institutions gouvernementales essentielles sélectionnées bénéficiaient d'une protection satisfaisante contre les logiciels rançonneurs.

Les institutions gouvernementales sont souvent la cible de cyberattaques, et les logiciels rançonneurs comptent parmi les plus importantes menaces qui pèsent actuellement sur la cybersécurité. Les logiciels rançonneurs sont des maliciels qui bloquent l'accès aux données. Généralement, ils cryptent les données et empêchent les institutions faisant l'objet de l'attaque de les utiliser. Les pirates exigent une rançon pour décrypter les données et permettre aux institutions d'y avoir à nouveau accès. Les logiciels rançonneurs représentent par conséquent une menace particulière pour ce qui est de l'accessibilité aux données.

Lorsqu'elles se trouvent soudainement dans l'impossibilité d'accéder à des données, les institutions peuvent rencontrer des difficultés à fournir des services importants, voire être dans l'incapacité totale de le faire. Les institutions touchées par des logiciels rançonneurs sont généralement forcées de fermer certaines parties, voir l'ensemble, de leur réseau informatique afin de mesurer l'ampleur de l'attaque. Les attaques par

logiciel rançonneur peuvent avoir une incidence économique considérable, car les institutions risquent de souffrir d'une perte de production, notamment si elles ne peuvent plus accéder à leur réseau informatique ou si les données collectées et traitées pendant une longue période sont perdues. En 2017, une attaque par logiciel rançonneur lancée sur le service de santé national britannique a entraîné l'annulation de 19 000 opérations et consultations. La direction des institutions devrait donc se concentrer sur le risque que représentent les attaques par logiciel rançonneur et mettre en place les contrôles de sécurité nécessaires pour se prémunir contre ces logiciels et réduire les incidences d'une éventuelle attaque.

L'étude a englobé l'autorité danoise des données de santé, le ministère des affaires étrangères, le réseau ferroviaire danois (*Banedanmark*) et l'agence danoise de gestion des situations d'urgence. Ces quatre institutions ont été sélectionnées car elles assurent des services essentiels en matière de santé, d'affaires étrangères, de transport et de préparation aux situations d'urgence, des domaines dans lesquels l'accès aux données peut revêtir une importance critique. L'autorité des données de santé fournit également des services informatiques centralisés à la majorité des organismes publics relevant du ministère de la santé.

L'objectif de l'étude était de déterminer si les quatre institutions étaient dotées d'une protection satisfaisante contre les attaques par logiciels rançonneurs contenus dans les courriers électroniques. Par conséquent, l'ISC a examiné 20 contrôles de sécurité courants qui offrent une protection de base contre les logiciels rançonneurs. En outre, elle a évalué cinq contrôles de sécurité que les institutions devraient envisager dans le cadre de futures évaluations des risques. Ces futurs contrôles peuvent faire appel, par exemple, à des nouvelles technologies capables de réduire le nombre de faux courriels pénétrant dans l'institution ou de détecter des activités inhabituelles sur les ordinateurs et d'envoyer des alertes. L'étude a été conduite par le *Rigsrevisionen* et repose sur les constatations de quatre audits informatiques réalisés entre avril et septembre 2017. Elle présente un instantané de la mesure dans laquelle les institutions étaient protégées contre les logiciels rançonneurs. Les institutions ont eu l'occasion de mettre en œuvre les 20 contrôles de sécurité courants à l'issue des audits informatiques. En conséquence, les résultats de l'étude concernent uniquement la protection des institutions contre les logiciels rançonneurs à l'époque où les quatre audits informatiques ont été réalisés. L'étude donne un aperçu de la performance des quatre institutions mais ne comprend pas d'analyse comparative ni de classement de leur performance.

Constatations et conclusions

L'ISC estime que les quatre institutions ne disposaient pas d'une protection satisfaisante contre les logiciels rançonneurs. Selon l'étude, elles ne réalisaient pas certains contrôles de sécurité courants permettant de réduire les attaques. L'autorité des données de santé et *Banedanmark*, en particulier, présentaient des lacunes considérables en matière de sécurité. Ainsi, les quatre institutions étaient toutes exposées à un risque accru d'attaques par logiciel rançonneur, perpétrées au moyen de courriers électroniques et susceptibles de les empêcher de fournir leurs services pendant un laps de temps indéterminé. Les quatre institutions ont toutes informé le *Rigsrevisionen* que depuis la réalisation de l'étude, elles travaillaient à la mise en place de plusieurs de ces contrôles de sécurité afin d'augmenter leur niveau de protection contre les logiciels rançonneurs.

Les mesures prises par les institutions pour prévenir les attaques par logiciel étaient inadaptées, que les menaces fussent internes ou externes. Il est particulièrement préoccupant qu'aucune des institutions n'ait assuré la mise à jour des correctifs de sécurité sur leurs logiciels et que trois d'entre elles n'aient pas établi de liste blanche pour empêcher leur personnel d'exécuter des logiciels malveillants. Cela accroît le risque que des logiciels rançonneurs infectent tout ou partie du réseau informatique avant de se répandre.

Dans trois des institutions, la direction ne s'est pas suffisamment intéressée à la menace que constituent les logiciels rançonneurs. Par ailleurs, les évaluations des risques effectuées par la direction de l'autorité des données de santé et par celle de *Banedanmark* ne couvraient pas tous les aspects pertinents. Dès lors, les institutions ne disposaient pas d'une évaluation actualisée de la menace représentée par les logiciels rançonneurs et n'étaient donc pas en bonne position pour prévenir de nouvelles attaques et réduire leur impact. La direction de l'autorité des données de santé et celle de Banedanmark n'ont pas accordé une attention suffisante à l'évaluation des risques, et par conséquent, la sécurité informatique de ces deux institutions ne reposait pas sur des priorités définies par la direction.

Trois des institutions n'étaient pas dotées de plans appropriés de réponse aux incidents qui leur auraient permis de rétablir leurs opérations après une attaque par logiciel rançonneur. Il convient tout particulièrement de noter que trois des institutions ne testaient pas régulièrement si elles seraient capables de restaurer les données et les systèmes touchés par une attaque par logiciel rançonneur. Cela majore le risque que les données détenues par ces institutions soient perdues du fait d'une

attaque par logiciel rançonneur et que les institutions soient incapables de fournir leurs services pendant une période prolongée.

Les scénarios de risque étant en évolution constante, il est essentiel que les institutions envisagent de mettre en œuvre des contrôles de sécurité prospectifs pour renforcer leur résilience aux attaques par logiciel rançonneur, c'est-à-dire des contrôles qui facilitent la vérification de l'identité des expéditeurs de courriels et permettent de détecter et de filtrer ceux qui sont potentiellement préjudiciables. Les quatre institutions travaillent actuellement sur certains contrôles de sécurité prospectifs capables de contribuer à renforcer leur protection contre les attaques par logiciel rançonneur.

Autres rapports dans le domaine

Titre du rapport:	Rapport sur la protection des données de recherche dans les universités danoises
Hyperlien vers le rapport:	synthèse du rapport (en anglais)
Date de publication:	2019

Titre du rapport:	Rapport sur la protection des systèmes informatiques et des données relatives à la santé dans trois régions danoises
Hyperlien vers le rapport:	synthèse du rapport (en anglais)
Date de publication:	2017

Titre du rapport:	Rapport sur la gestion de la sécurité informatique des systèmes sous-traités à des prestataires externes
Hyperlien vers le rapport:	synthèse du rapport (en anglais)
Date de publication:	2016

Titre du rapport:	Rapport sur l'accès aux systèmes informatiques utilisés pour fournir des services essentiels à la société danoise
Hyperlien vers le rapport:	synthèse du rapport (en anglais)
Date de publication:	2015

Estonie
Riigikontroll

Garantir la sécurité et la préservation des bases de données nationales critiques en Estonie

Date de publication: mai 2018

Hyperlien vers le rapport: synthèse du rapport (en anglais)
rapport (en estonien)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2017

Synthèse du rapport

Sujet de l'audit

Pour préserver son indépendance, l'Estonie doit non seulement défendre l'intégrité physique de son territoire, mais aussi protéger les actifs numériques, d'importance capitale pour l'État, contre les événements qui constituent la plus grande menace. Les actifs numériques ayant le plus besoin de protection sont les données relatives aux citoyens, au territoire et à la législation. Les données concernant la propriété, l'immobilier et les droits des résidents estoniens doivent également être sécurisées.

L'ISC a cherché à savoir comment l'État avait déterminé quelles étaient les données et bases de données cruciales pour garantir la sécurité nationale. La protection de la sécurité et de la continuité de ces données et bases de données a été vérifiée, y compris les outils utilisés à des fins de protection.

L'Estonie étant désormais membre de l'OTAN et de l'Union européenne, sa sécurité physique est mieux garantie qu'avant son adhésion à ces réseaux. Elle doit toutefois envisager la possibilité de cybermenaces en cas d'escalade de problèmes de sécurité. De tels scénarios de risques et une augmentation du nombre d'incidents liés à la sécurité de l'information, tels que les cyberattaques et les fuites de données,

pourraient aussi compromettre l'intégrité de données et bases de données qui sont de la plus haute importance pour l'État. Si les données d'importance capitale pour l'État étaient modifiées sans autorisation, si elles faisaient l'objet de fuites ou étaient perdues, le gouvernement ne serait plus en mesure d'assurer les fonctions nécessaires, notamment garantir la sécurité des personnes, fournir les services fondamentaux, créer l'environnement requis pour les entreprises et bien plus encore. L'Estonie prévoit initialement d'investir environ un million d'euros pour stocker les données critiques à l'étranger.

Questions d'audit

- Les ministères ont-ils recensé toutes les bases de données critiques et toutes les règles en matière de traitement?
- Les bases de données et registres critiques sont-ils sécurisés?
- La continuité à long terme des données et bases de données critiques est-elle garantie?

Constatations

L'ISC a formulé les observations suivantes concernant les bases de données critiques auditées:

- il manquait un plan d'action ou des règles applicables à la notion de bases de données critiques. Les critères permettant de sélectionner les bases de données critiques n'avaient pas été définis, et il n'était pas certain que toutes les bases de données essentielles étaient prises en considération. La protection supplémentaire des bases de données avait été organisée de manière informelle et n'était pas obligatoire pour les propriétaires de bases de données, ce qui explique que les données figurant dans les cinq bases de données critiques n'aient pas été sauvegardées à l'étranger;
- aucune règle supplémentaire n'avait été établie pour les bases de données critiques en ce qui concerne la sécurité de l'information. Ni le système de sécurité de l'information ISKE (un cadre normalisé en matière de sécurité de l'information conçu pour le secteur public estonien et obligatoire pour les organes de l'administration centrale et locale qui traitent des bases de données ou des registres) ni aucune loi ou norme ne prévoyait d'exigences supplémentaires pour les bases de données critiques, telle que l'obligation de sauvegarder les données

en dehors de l'Estonie. Des copies de sauvegarde des bases de données auditées ont été stockées à l'étranger, mais la récupération des travaux des systèmes d'information à partir de ces copies n'a pas été testée;

- la mise en œuvre d'ISKE et des contrôles y afférents posait problème en ce qui concerne les bases de données critiques. Au moment où l'ISC réalisait son audit, deux des dix bases de données n'avaient fait l'objet d'aucun contrôle dans le cadre d'ISKE, et les contrôles n'ont été organisés qu'à la fin de l'audit (30 novembre 2017). Seules deux bases de données critiques avaient été contrôlées à la fréquence prévue par la loi. En outre, dans certains cas, les problèmes relevés par le contrôleur lors d'un contrôle ISKE n'avaient pas encore été réglés au moment de la réalisation du contrôle suivant (soit deux à trois ans après);

- au cours de l'audit, l'ISC a constaté que certaines mesures importantes en matière de sécurité de l'information n'avaient pas été mises en œuvre pour certaines bases de données critiques. Par exemple, les lignes directrices relatives à la sécurité de l'information ne prévoyaient pas d'évaluation régulière des faiblesses des systèmes d'information; les journaux d'événements n'avaient pas fait l'objet d'analyses ou de contrôles réguliers; il n'existait aucun programme de formation à la sécurité de l'information, et aucune analyse des connaissances en la matière dans les secteurs de l'administration n'avait été réalisée en vue d'établir un tel programme; dans certains cas, l'intégrité des fichiers n'avait pas été vérifiée; enfin, aucun test de pénétration n'avait été réalisé.

Conclusions et recommandations

L'audit a révélé que, malgré la mise en œuvre du système de sécurité minimale à trois niveaux ISKE, dont l'utilisation est obligatoire pour les organismes publics et dans le cadre de leurs contrôles, plusieurs bases de données critiques souffraient encore d'importantes lacunes en matière de sécurité de l'information, notamment en ce qui concerne l'analyse des journaux, les tests de pénétration et la protection des appareils portables. Les exigences spécifiques à la protection des données critiques n'avaient pas encore été définies.

Le ministère des affaires économiques et des communications avait lancé les premières actions requises pour protéger les données critiques, mais le projet se trouvait dans une phase où il s'avérait nécessaire de disposer d'un ensemble de règles

légalement contraignantes. Il n'existait pas non plus d'analyse des risques détaillée ni de plan d'action pour l'avenir.

Des copies de sauvegarde de cinq bases de données critiques étaient stockées dans des ambassades situées dans des pays étrangers mais, en cas de destruction physique des centres de données installés en Estonie, la préservation des données critiques des cinq bases de données restantes ne serait pas garantie.

Deux recommandations générales ont été formulées:

- déterminer des règles visant à assurer une protection supplémentaire des bases de données critiques, notamment en ce qui concerne la sélection des bases de données critiques, le traitement des données figurant dans ces bases et la sauvegarde des données critiques pour l'État, et étudier comment allouer des financements supplémentaires à ces activités;
- analyser les différentes étapes de l'établissement des bases de données, tant du point de vue de la planification financière que de celui de la sécurité de l'information, et appliquer les bonnes pratiques en matière de gestion de projets dans la mise en œuvre de ces étapes.

Irlande
Office of the Comptroller and Auditor General

Mesures relatives à la cybersécurité nationale

Date de publication: septembre 2018

Hyperlien vers le rapport: synthèse du rapport (en anglais)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2011-2018

Synthèse du rapport

Sujet de l'audit

Le service des communications, de l'action pour le climat et de l'environnement est responsable de la politique de l'Irlande en matière de cybersécurité. Il est également chargé de coordonner, par l'intermédiaire du Centre national de cybersécurité, la réponse gouvernementale d'urgence en cas d'incident de cybersécurité survenant au niveau national.

Le Centre national de cybersécurité a été institué en 2011. Il s'attache principalement à sécuriser les réseaux publics, à aider les entreprises et les particuliers à protéger leurs propres systèmes et à garantir la sécurité des infrastructures nationales critiques.

Questions d'audit

L'audit a pour but d'évaluer les progrès accomplis en ce qui concerne les mesures de cybersécurité depuis la mise en place du Centre national de cybersécurité. Il porte plus particulièrement sur des questions concernant:

- le mandat et le financement du Centre;

- la stratégie nationale de cybersécurité (2015-2017);
- la mise en œuvre de la directive relative à la sécurité des réseaux et des systèmes d'information dans l'Union;
- les dispositions en matière de gouvernance et de surveillance.

Constatations et conclusions

Bien que, dans la décision du gouvernement instituant le Centre national de cybersécurité, un financement annuel de 800 000 euros ait été approuvé, les fonds alloués chaque année à la cybersécurité entre 2012 et 2015 représentaient en réalité moins d'un tiers de ce montant. En 2017, la dotation a été portée à 1,95 million d'euros. Les effectifs du Centre ont presque doublé au cours de l'année 2017, pour atteindre 14,5 équivalents temps plein. Le recrutement de 16 agents supplémentaires a été approuvé en 2018.

La stratégie nationale de cybersécurité (2015-2017) définissait 12 mesures à mettre en œuvre sur la période couverte par la stratégie. En mai 2018, quatre mesures étaient intégralement mises en œuvre, quatre l'étaient en partie et quatre autres n'avaient pas été mises en œuvre.

La directive la directive relative à la sécurité des réseaux et des systèmes d'information dans l'Union vise à améliorer la résilience des principaux réseaux et systèmes d'information. Une évaluation des progrès accomplis en Irlande en ce qui concerne chacun des trois piliers de la directive a donné lieu aux constatations suivantes:

- *Premier pilier: améliorer les capacités des États membres de l'UE en matière de cybersécurité.* Partiellement mis en œuvre: les exigences structurelles ont été respectées, mais des lacunes persistent dans la planification stratégique.
- *Deuxième pilier: faciliter la coopération en matière de cybersécurité entre les États membres.* Mis en œuvre.
- *Troisième pilier: instaurer des mesures de sécurité et des obligations de signalement des incidents pour les secteurs clés.* Partiellement mis en œuvre: des travaux sont encore nécessaires en ce qui concerne la définition des systèmes d'information et des réseaux critiques, la désignation formelle des entités assumant les fonctions d'opérateurs de services essentiels et la gestion des fournisseurs de services numériques.

La décision (juillet 2011) par laquelle le gouvernement a approuvé la création du Centre national de cybersécurité a également entériné la mise en place d'un comité interservices destiné à élaborer et à mettre en œuvre la politique visant à répondre aux enjeux de cybersécurité en Irlande. Bien que le comité se soit réuni à cinq reprises entre 2013 et 2015, seul le procès-verbal d'une des réunions était disponible pour examen. Le comité ne s'est pas réuni depuis 2015.

Le plan de mise en œuvre de la stratégie nationale de cybersécurité prévoit la publication d'un rapport annuel et la réalisation d'une analyse d'impact formelle des travaux du Centre à la fin de l'année 2017. La publication et l'analyse d'impact sont toujours en suspens, bien que les travaux du Centre soient exposés dans le rapport annuel du service des communications, de l'action pour le climat et de l'environnement.

Le service a officiellement demandé une évaluation de la performance du Centre. Aucun élément probant attestant qu'une telle évaluation a été réalisée n'a été fourni. Le service des communications, de l'action pour le climat et de l'environnement a indiqué que ladite évaluation faisait partie de sa pratique normale de gestion de la performance et de gouvernance d'entreprise.

Les conclusions de l'audit sont les suivantes:

- malgré la fonction cruciale exercée par le Centre national de cybersécurité, le niveau de financement au cours de ses quatre premières années de fonctionnement était considérablement inférieur à celui initialement envisagé;
- l'orientation stratégique générale du Centre n'est pas clairement définie, aucun plan n'ayant été établi;
- le rôle des différents organismes enquêtant sur les cybercrimes et les incidents portant atteinte à la sécurité nationale doit être clarifié;
- il n'a pas encore été procédé à l'élaboration de la stratégie nationale exigée dans la directive relative à la sécurité des réseaux et des systèmes d'information dans l'Union;
- Bien que des structures de gouvernance aient été prévues, la manière dont les modalités de gouvernance fonctionnent en pratique n'est pas claire.

La disponibilité et le coût des ressources affectées à la cybersécurité manquent de transparence.

France
Cour des comptes

L'accès à l'enseignement supérieur: un premier bilan de la loi relative à l'orientation et à la réussite des étudiants

Date de publication: février 2020

Hyperlien vers le rapport: Rapport

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2019-2020

Synthèse du rapport

Sujet de l'audit

La loi de 2018 relative à l'orientation et à la réussite des étudiants (ORE) visait à améliorer les trois étapes fondamentales du parcours des jeunes gens se destinant à l'enseignement supérieur: l'accompagnement à l'orientation au lycée, l'affectation dans une formation de l'enseignement supérieur et la réussite dans les premières années d'études. Elle a introduit «Parcoursup», une nouvelle plateforme numérique qui représente une source d'informations sur les cursus disponibles et sur les conditions d'admission. L'objectif de la plateforme était de parvenir à une meilleure adéquation entre le profil et les résultats scolaires du lycéen et les caractéristiques des formations du supérieur.

Les deux premières années de mise en œuvre de la loi ORE ont permis de franchir une première étape dans la transformation de l'accès à l'enseignement supérieur. Malgré de nombreuses contraintes, le déploiement de «Parcoursup» s'est très bien déroulé, même si la sécurité et la durabilité de la plateforme n'étaient pas assurées et si les données auraient pu être mieux exploitées compte tenu de leur importance.

La loi ORE a été adoptée afin de résoudre deux problèmes majeurs des politiques éducatives. D'une part, les étudiants à l'université connaissaient un taux d'échec élevé. D'autre part, l'ancienne plateforme numérique avait suscité un profond mécontentement en raison du recours au tirage au sort dans la dernière étape.

La réforme ORE a bénéficié d'un financement de 867 millions d'euros sur cinq ans. Fondée sur la notion de «continuum -3/+3», la réforme part du principe qu'une plus grande information des lycéens sur les caractéristiques des filières du supérieur permet d'améliorer leurs chances de succès aux examens, les élèves choisissant les formations qui sont le plus adaptées à leur profil et à leur projet. La loi ORE visait à répondre aux insuffisances de l'accompagnement à l'orientation dont bénéficient les lycéens et à réduire ainsi les réorientations, dont le coût a été estimé par la Cour à près de 550 millions d'euros par an pour la seule première année du supérieur.

La Cour des comptes française a réalisé un premier bilan de l'accès à l'enseignement supérieur dans le cadre de la loi ORE, en s'intéressant aux questions de sécurité informatique soulevées par la plateforme.

Le système d'information était caractérisé par une poussée des facteurs de charges (inclusion en 2020 de l'ensemble des formations relevant de l'enseignement supérieur et augmentation majeure du nombre d'usagers en quelques années), due à la transformation dans l'urgence de l'ancienne plateforme en «Parcoursup», dont l'architecture n'a pas été refondue. Cette situation crée des risques importants en termes de qualité, de continuité, d'adaptabilité et d'évolution du service public. Les faiblesses du système en matière de sécurité, de performance et de robustesse n'ont pas été rectifiées. La gestion de «Parcoursup» en mode projet autour de seulement quelques personnes particulièrement compétentes et motivées a permis sa mise en place rapide mais fragilise un dispositif aujourd'hui sans direction stratégique ni gouvernance satisfaisantes.

La Cour des comptes a examiné la qualité du système d'information et la performance de la nouvelle plateforme «Parcoursup». Créé par la loi ORE, «Parcoursup» a pour objet d'améliorer la qualité de l'affectation dans l'enseignement supérieur pour une plus grande réussite en licence.

Constatations

Même si la plateforme «Parcoursup» fonctionnait de manière satisfaisante, elle était exposée à des risques informatiques, qu'il convenait de réduire. La sécurité et la pérennité de la plateforme devaient être assurées, et les données auraient pu être mieux exploitées.

Un système d'information daté

Ayant subi peu de modifications lors de sa transformation, «Parcoursup» souffre de lourdeurs et de fragilités héritées de la précédente plateforme «Admission post-bac» (APB) et reste exposée à de nombreux risques non résolus. Le système d'information qui forme l'ossature de «Parcoursup» est l'héritier direct de celui de la plateforme précédente. Bien que présenté comme un nouveau dispositif d'affectation, le cœur du système d'information n'a été que peu modifié entre «APB» et «Parcoursup». En réalité, l'infrastructure informationnelle demeure identique à plus de 72 %, 30 % à peine du code de la plateforme APB ayant été réécrit.

Le socle informatique de la plateforme a été conçu au début des années 2000 pour traiter environ un million de candidatures pour environ 100 000 places proposées chaque année, mais le périmètre du système d'information a été étendu pour traiter un flux annuel de l'ordre de dix millions de candidatures pour environ un million de places. «Parcoursup» apparaît comme une nouvelle marque pour un outil ancien. La montée en charge a posé question sur la capacité de la plateforme à remplir pleinement ses fonctions.

Un système d'information peu documenté

En dépit des actions de mise en transparence du ministère, le code source de «Parcoursup» reste à 99 % fermé. La partie publiée demeure d'un intérêt limité pour comprendre, expertiser, et évaluer le processus d'affectation des candidats dans les formations.

Comme son prédécesseur, «Parcoursup» reste un système d'information opérationnel et peu documenté. Selon les résultats de l'audit du code source, l'application présente une qualité médiocre, avec un niveau de risque élevé et de nombreuses violations critiques recensées. Le système se situe à un niveau de qualité plus faible que d'autres logiciels d'ancienneté similaire et présente un risque élevé de rupture du fonctionnement normal.

«Parcoursup» est composé d'un code source public et d'un code source fermé. Le code ouvert présente une densité de violations critiques bien plus importante que le code fermé, ce qui signifie qu'il est exposé à un risque de rupture de service. La plateforme n'est pas non plus à l'abri d'une intrusion (audit de sécurité du code source de juillet 2018). Cependant, à la fin 2019, le ministère a annoncé qu'une démarche de certification du code «Parcoursup» avait été initiée.

La documentation du code source existante n'est ni cohérente, ni exhaustive. Le code de «Parcoursup» présente un niveau de complexité anormalement élevé. La Cour des comptes a estimé que le code source devrait être restructuré afin de réduire le nombre de ses composantes complexes.

L'architecture du système d'information de «Parcoursup» présente un risque élevé. La gestion de la base de données est manuelle, une pratique obsolète. La fragilité du système repose sur une forte dépendance à l'égard des opérateurs, qui doivent être disponibles et vigilants. Le ministère a reconnu que les risques associés à l'architecture de l'application «Parcoursup» étaient élevés et qu'ils ne pouvaient être corrigés sans un redéveloppement plus poussé de l'application.

Le système d'information «Parcoursup» est mal documenté et repose essentiellement sur la connaissance des personnes travaillant au service à compétence nationale (SCN). Une série de commentaires intégrés à la base de données qui constitue le cœur du système tiennent lieu de documentation, ce qui complique la maintenance et l'évolution du système d'information ainsi que l'exploitation des données. Les données des usagers collectées dans la plateforme peuvent difficilement être mobilisées et valorisées sans procéder à des investigations approfondies. Faute de documentation technique structurée, la capacité du SCN à assurer ses missions stratégiques repose intégralement sur le responsable du pôle informatique.

Stratégie de sécurité: des améliorations sont nécessaires

En raison de la sensibilité des données à caractère personnel collectées dans le système, la sécurité constitue un réel enjeu pour «Parcoursup». En principe, toute organisation gérant un système d'information doit se doter d'une politique de sécurité de l'information (PSSI), formalisée dans un document du même nom. Alors qu'il a été reconnu comme opérateur de service essentiel par le Premier ministre, «Parcoursup» ne dispose d'aucune PSSI. Les actions nécessaires à la mise en place d'une PSSI devraient être prises sans délai.

Chaque équipe de «Parcoursup» dispose d'un responsable de la sécurité des systèmes d'information (RSSI) rattaché au pôle informatique. Il aurait été de bonne pratique de rattacher le RSSI directement à la directrice du SCN, afin de garantir son indépendance.

Au terme du premier semestre 2019, «Parcoursup» était toujours en cours de mise en conformité avec le RGPD. Certaines actions restaient à mettre en place, notamment en ce qui concerne la formalisation des différents traitements mis en œuvre. La sécurité des données à caractère personnel reste insuffisante, et une quantité trop importante de données individuelles exhaustives est encore stockée.

Le SCN «Parcoursup» est rattaché à la fois au chef de projet «Parcoursup», chargé de mission au sein du cabinet de la ministre, et au service de la stratégie des formations et de la vie étudiante de la direction générale de l'enseignement supérieur et de l'insertion professionnelle, et relève donc d'une direction bicéphale. Les aspects pratiques du système d'information «Parcoursup» sont abordés lors de réunions hebdomadaires. Ce mode d'organisation, même s'il présente l'avantage de la réactivité dans la gestion courante des flux d'étudiants, laisse «Parcoursup» sans direction stratégique.

Enfin, le système est trop peu transparent. Il ne permet pas une pleine valorisation des données collectées dans la plateforme, et dont le potentiel est pourtant considérable. La mobilisation de ce potentiel permettrait très probablement d'obtenir des gains de performance.

Conclusions et recommandations

Face à la massification de l'enseignement supérieur, les pouvoirs publics ont cherché, avec succès, à centraliser l'accès au supérieur dans le cadre d'une plateforme numérique visant à réunir l'ensemble des formations. Le nouveau «Parcoursup» est le fruit d'un remaniement hâtif du précédent système, et aucun changement structurel important n'a été apporté. Les fragilités du système d'information en matière de sécurité, de performance et de robustesse n'ont donc pas été rectifiées, alors même que la montée en charge devait se poursuivre avec l'inclusion à terme de l'ensemble des formations du premier cycle. Le système reste également mal documenté, son processus de développement est artisanal et il souffre d'une complexité anormalement élevée qui accroît les risques d'erreurs en cas de mise en œuvre d'évolutions fonctionnelles. La plateforme présente donc des risques importants en termes de qualité et de continuité du service public ainsi que de sécurité des données personnelles.

La Cour des comptes a formulé les recommandations suivantes:

- par redéploiement des financements «ORE», renforcer les moyens humains de l'équipe informatique du SCN, ainsi que les moyens humains et matériels de la sous-direction des systèmes d'information et des études statistiques;
- pérenniser le système d'information par une correction des failles les plus urgentes, par la modernisation voire le redéveloppement de son architecture, et par la documentation systématique et structurée des bases de données primaires de l'ancien système et de «Parcoursup»;
- mettre en place une politique de sécurité du système d'information «Parcoursup»;
- structurer une fonction d'orientation commune au ministère de l'éducation nationale et de la jeunesse et au ministère de l'enseignement supérieur, de la recherche et de l'innovation supervisant la plateforme «Parcoursup» et disposant de moyens pour l'action «orientation» par redéploiement de crédits de la loi ORE.

Lettonie
Valsts Kontrole

L'administration publique a-t-elle exploité toutes les occasions de mettre en place une gestion efficiente de l'infrastructure TIC?

Date de publication: juin 2019

Hyperlien vers le rapport: synthèse du rapport (en anglais)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2017-2019

Synthèse du rapport:

Sujet de l'audit

L'ISC de Lettonie a réalisé un audit de la performance sur l'efficience des infrastructures publiques des TIC. L'audit visait à vérifier si l'administration publique avait adopté une approche unifiée pour gérer de manière efficiente les infrastructures TIC et si les institutions avaient évalué les avantages de la centralisation. Par ailleurs, la sécurité des centres de données a été considérée comme une question importante lorsqu'il s'agit de décider de ce qui pourrait faire l'objet d'une optimisation plus poussée.

La réticence des autorités à gérer les infrastructures TIC de manière centralisée, ou au moins au niveau d'un seul ministère, s'est traduite par l'établissement d'un certain nombre de salles de serveurs, augmentant ainsi considérablement les frais de maintenance. Il a été constaté que les 22 sous-entités des quatre ministères audités se servaient de 38 centres de données. Au cours de l'audit, l'ISC a observé des cas où des systèmes d'information d'importance majeure, voire nationale, étaient installés dans des locaux disposant d'un niveau de sécurité insuffisant. L'optimisation du nombre de salles de serveurs permettrait non seulement de réduire les dépenses en TIC, mais

aussi d'assurer un niveau de sécurité suffisant à un coût moindre. À l'époque, des salles de serveurs à haute sécurité étaient déjà disponibles dans les institutions mais n'étaient pas exploitées au maximum de leurs capacités.

Sujet principal de l'audit

L'audit avait pour but de vérifier que tous les prérequis pour une gestion unifiée des infrastructures TIC étaient réunis et mis en œuvre de manière à promouvoir une utilisation plus efficiente et sécurisée des ressources TIC.

Constatations et conclusions

Gouvernance et optimisation des TIC

- Il n'y avait aucune vision à long terme en matière de développement et d'optimisation des TIC, que ce soit à l'échelle nationale ou au niveau des ministères. Les ministères et leurs sous-entités ont optimisé les infrastructures TIC dans la mesure de leurs connaissances et de leurs capacités.

Entre 2011 et 2017, le coût de maintenance total des TIC des institutions auditées est passé de 17 à 20 millions d'euros par an. Les institutions n'ont adopté aucune pratique consistant à évaluer à intervalles réguliers s'il était moins coûteux d'assurer elles-mêmes la maintenance des infrastructures TIC, de collaborer avec une autre institution ou de sous-traiter la maintenance des TIC. Ni la centralisation des TIC ni leur décentralisation ne sont considérées comme des objectifs en tant que tels, mais il est nécessaire d'analyser la situation concrète et les différentes possibilités pour pouvoir déterminer clairement les coûts liés à la situation existante et les autres options possibles.

Sécurité des TIC

- Dans le cadre juridique, les exigences en matière de sécurité des infrastructures TIC n'étaient pas clairement définies selon un système logique reposant sur la pertinence des informations à traiter. Il n'existait aucune exigence technique détaillée pour la protection des centres de données TIC.

- Le manque d'exigences en matière de sécurité s'est traduit par des mesures de protection coûteuses ou, dans d'autres cas, par un défaut de protection des informations d'importance nationale. Certains systèmes d'information essentiels étaient même hébergés dans des centres de données à faible niveau de sécurité.

- La sécurité de la plupart des salles de serveurs était menacée, les centres de données ne disposant pas d'une protection suffisante contre les accès physiques et les risques environnementaux. La prévention des menaces à la sécurité exigeait un investissement d'au moins 247 000 à 765 000 euros, en fonction de l'approche choisie. Ces mesures comprenaient: 1) l'amélioration des salles de serveurs hébergeant des systèmes d'information plus importants et le stockage des ressources TIC de premier plan dans des centres de données à plus haut niveau de sécurité, ou 2) l'amélioration de toutes les salles de serveurs. Toutefois, à moins d'une diminution du nombre de centres de données, les montants à investir pour la mise en œuvre de ces mesures ne se justifieraient pas.

Le cadre juridique n'était pas complet, car il ne prévoyait pas d'exigences précises pour la sécurité des infrastructures TIC. Il existait ainsi des exigences concernant différents critères liés à la sécurité logique, mais aucune en ce qui concerne la sécurité physique et environnementale des infrastructures, qui a également une incidence sur la disponibilité des systèmes et la protection des données. Si les documents publics de planification stratégique insistaient sur l'importance de la sécurité des infrastructures TIC et sur la nécessité de la renforcer, aucune action spécifique n'était prévue à cet égard. Étant donné que les exigences de sécurité n'étaient pas différenciées de façon claire, traçable et logique, celles concernant le traitement d'informations d'importance et d'intérêt équivalents risquaient de varier au sein du pays.

La sécurité de l'espace numérique était contrôlée de manière centralisée par l'administration, et le gouvernement répondait aux incidents survenant à ce niveau, mais la responsabilité de la mise en œuvre de la sécurité des infrastructures informatiques incombait à la direction de chaque institution. Ainsi, la compréhension par les institutions des questions liées à la sécurité des TIC, l'appréciation de l'importance des informations traitées et les ressources mises à la disposition des institutions pour remédier aux problèmes de sécurité des TIC variaient fortement.

Un système de surveillance régulière de ces processus s'avère nécessaire afin d'évaluer l'ensemble de l'administration publique en tant que système unique, de manière indépendante et au moyen de critères normalisés, de recenser les différents types d'attaques et de les prévenir en déterminant les risques courants, ainsi que de planifier des actions préventives pour atténuer ces risques.

Lituanie
Valstybės Kontrolė

Gestion des sources nationales d'informations critiques

Date de publication: juin 2018

Hyperlien vers le rapport: synthèse du rapport (en anglais)
Rapport (en lituanien)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2014-2017

Synthèse du rapport

Sujet de l'audit

D'importantes fonctions gouvernementales, telles que la gestion des finances publiques, l'administration fiscale et les soins de santé, sont exercées au moyen des sources nationales d'informations critiques – les informations électroniques critiques. Toute perte d'informations critiques ou toute indisponibilité des systèmes d'information correspondants pourrait avoir de graves conséquences sur la sécurité publique, le bien-être public et l'économie. Les évaluations des contrôles informatiques généraux réalisées par l'ISC de Lituanie entre 2006 et 2016 ont révélé des problèmes récurrents dans la gestion informatique (planification, définition de l'architecture d'information, structure organisationnelle, changements, garantie de la continuité des activités, sécurité des données, suivi et évaluation de la gestion informatique). L'ISC a effectué un audit des sources nationales d'informations critiques afin d'évaluer la gestion et la sécurité de ces ressources et de proposer des mesures d'amélioration.

L'audit visait à apprécier la gestion (le contrôle général) et la maturité des sources nationales d'informations critiques ainsi qu'à mettre en évidence les problèmes systémiques.

L'ISC a évalué la maturité de la gestion informatique dans 12 organisations du secteur public[64], responsables de 44 systèmes nationaux d'information de la plus haute importance. L'audit a été réalisé conformément aux exigences concernant l'audit du secteur public et aux normes internationales des institutions supérieures de contrôle. L'évaluation a été réalisée selon la méthodologie COBIT[65] dans les domaines à haut risque suivants: planification informatique stratégique; détermination de l'architecture d'information; gestion des risques informatiques; gestion du changement; garantie de la continuité des services; gestion des données; suivi et évaluation des activités informatiques; assurance de gestion informatique. L'évaluation des processus portait à la fois sur la gestion informatique organisationnelle et nationale et sur l'interaction entre ces niveaux de gestion.

Constatations d'audit

Les tendances observées dans l'évolution des niveaux de maturité de la gestion des sources nationales d'informations critiques étaient positives. Cependant, étant donné l'augmentation des cybermenaces, les progrès observés étaient trop lents et la sécurité de ces ressources devait être renforcée. Les faiblesses ci-après en étaient la cause.

- Le système d'identification des sources nationales d'informations critiques n'était pas suffisamment efficace pour permettre la mise en œuvre de solutions de sécurité répondant aux besoins réels:
  - les évaluations visant à démontrer la nature critique des sources nationales d'informations critiques manquaient d'objectivité, les changements n'étaient pas toujours mesurés dans les réévaluations, le processus ne faisait pas l'objet d'un suivi au niveau national et les lignes directrices à appliquer pour

[64] Inspection nationale des impôts, centre national des registres, service des technologies de l'information et des communications, conseil d'administration du Fonds national d'assurance sociale, centre national d'information des entreprises et exploitations agricoles, centre d'information du système douanier, service public alimentaire et vétérinaire, bureau du Seimas de la République de Lituanie, ministère des finances, comité de développement de la société de l'information, Fonds national des patients et service national des forêts.

[65] COBIT (*Control Objectives for Information and Related Technologies*) est une norme élaborée par l'organisation internationale ISACA, qui définit les bonnes pratiques de la gestion informatique.

déterminer la nature critique ne garantissaient pas une mise en œuvre efficace;

— le système d'identification des sources nationales d'informations critiques et des infrastructures informationnelles critiques n'était pas normalisé. Par ailleurs, les sources et les infrastructures étaient définies de manière différente selon l'importance des informations et des services, ce qui compliquait l'identification desdites sources;

— aucune architecture nationale de l'information n'avait été développée pour représenter les systèmes nationaux d'information et leurs interactions, pour visualiser l'ampleur des sources nationales d'informations critiques et pour permettre de prendre des décisions éclairées concernant l'importance desdites sources.

o La gestion des sources nationales d'informations devait être mieux alignée sur les bonnes pratiques et normes en matière de gestion informatique afin de permettre une amélioration intégrée du domaine informatique qui contribuerait à progresser davantage dans la gestion des sources nationales d'informations critiques:

— la planification informatique n'était pas durable: les outils informatiques prévus étaient présentés dans différents documents et il n'existait aucune approche systématique en raison du nombre excessif de documents stratégiques. Il était dès lors difficile de définir les principales priorités et de canaliser les ressources de manière gérer les menaces les plus importantes;

— le contrôle informatique ne permettait pas de garantir que les organisations mesuraient l'efficience des opérations informatiques et que les audits réalisés par les responsables des sources nationales d'informations critiques indiquaient la maturité réelle de la gestion informatique. La gestion informatique de l'État n'a pas été évaluée au niveau national, et les problèmes y afférents n'ont pas fait l'objet d'une analyse systématique. Un système de contrôle de la conformité des sources nationales d'informations avec les exigences relatives à la sécurité des informations électroniques avait été créé dans l'unique but de faciliter le contrôle de la conformité aux exigences de sécurité, mais sa fonctionnalité n'a pas été suffisamment exploitée.

- Les mesures visant à garantir la résilience des sources d'informations critiques face aux cybermenaces n'étaient pas suffisamment efficaces. Par conséquent, ces sources risquaient toujours d'être vulnérables:

  — l'efficacité de l'évaluation des risques en matière de sécurité informatique devait être renforcée car les risques importants n'étaient pas tous mis en évidence et la méthode employée pour les évaluer n'était pas conforme aux dernières pratiques de gestion informatique. En outre, la gestion des risques inacceptables n'était pas assurée en temps utile;

  — les mesures de sécurité organisationnelle à même de réduire les cybermenaces n'ont pas été systématiquement appliquées. Des tests de sécurité insuffisants, une formation incomplète du personnel pendant le développement, la modernisation et la modification du système d'information, le défaut de gestion des configurations et des mises à niveau des logiciels de sécurité et la gestion inappropriée de la continuité des opérations informatiques et des fichiers de sauvegarde mettaient en péril la reprise des activités; les analyses de performance en matière de sécurité étaient insuffisantes et n'ont pas contribué à l'amélioration de la sécurité.

Conclusions

En moyenne, la gestion informatique des entités du secteur public auditées au cours des dix dernières années a atteint le premier des cinq[66] niveaux de maturité et se situait au niveau 1.7 au moment de la rédaction du rapport. Ce faible niveau de maturité des sources nationales d'informations critiques indiquait la présence de faiblesses dans l'élaboration et la mise en œuvre de la politique relative aux sources nationales d'information, ce qui rend ces dernières plus vulnérables. Afin de renforcer la sécurité de ces ressources, il convient d'améliorer le mécanisme de gestion des sources nationales d'informations pour l'aligner autant que possible sur les bonnes pratiques. Les auditeurs ont également constaté que les mesures visant à garantir la résistance des sources en matière d'informations critiques aux cybermenaces n'étaient pas suffisamment efficaces. Par conséquent, il importe de renforcer l'efficacité de l'évaluation des risques en matière de sécurité informatique en mettant davantage l'accent sur les tests de sécurité lors de la création et la modernisation des systèmes d'information et de la formation du personnel.

[66] Conformément à la méthodologie COBIT.

Autres rapports dans le domaine

Titre du rapport:	La lutte contre la cybercriminalité est-elle efficace?
Hyperlien vers le rapport:	synthèse du rapport (en anglais) rapport (en lituanien)
Date de publication:	2020

Titre du rapport:	L'environnement de la cybersécurité en Lituanie
Hyperlien vers le rapport:	synthèse du rapport (en anglais) Rapport (en lituanien)
Date de publication:	2015

Hongrie
Institution supérieure de contrôle

Audit de la protection des données – Audit du cadre national de protection des données et de certains enregistrements de données de base prioritaires dans le cadre de la coopération internationale

Date de publication: mars 2017

Hyperlien vers le rapport: rapport (en hongrois)

Type d'audit et période couverte

Type d'audit: audit de conformité

Période couverte par l'audit: 2011-2015

Synthèse du rapport

Sujet de l'audit

La sécurité des actifs de données nationaux représente pour la société de chaque pays un intérêt fondamental du point de vue de la préservation et de la protection des valeurs nationales. Il est dès lors essentiel de garantir l'amélioration de la sécurité des données personnelles et publiques dans les actifs de données nationaux de Hongrie afin de renforcer la confiance que les citoyens accordent à l'État et d'assurer un fonctionnement continu et fluide de l'administration publique. La protection des données et le filet de sécurité prévu par le cadre juridique pour sa mise en œuvre revêtent donc une importance primordiale pour la société.

En ce qui concerne la protection des données, l'administration publique joue un rôle essentiel dans la gestion des registres de données les plus importants et les plus sensibles parmi les actifs de données nationaux. Les responsables du traitement des données des registres collaborent étroitement afin de mener leur mission à bien. Ils transfèrent régulièrement des registres contenant un grand nombre de données et doivent tenir compte des exigences réglementaires en matière de protection des données. Il est aujourd'hui essentiel de recourir à des systèmes d'information

électroniques pour gérer et traiter les données. Des contrôles conçus et exécutés de manière appropriée doivent donc permettre de garantir le fonctionnement adéquat et fiable de ces systèmes.

Lorsqu'elle réalise ses audits, l'ISC hongroise accorde une grande attention à la protection des données. Elle a effectué des audits exhaustifs sur la protection des données entre 2011 et 2015 et a publié son rapport au premier trimestre 2017. Les travaux d'audit ont concerné également des aspects examinés lors d'audits internationaux parallèles, réalisés en coopération avec le groupe de travail de l'Eurosai sur les technologies de l'information et concernant principalement la conformité avec les directives existantes de l'Union européenne.

L'objectif de l'audit de conformité sur la protection des données en Hongrie était de déterminer si le pays avait établi un cadre réglementaire et opérationnel pour la protection des données et si les principales organisations de gestion des données respectaient les exigences en matière de sécurité concernant la gestion des données et l'externalisation de leur traitement. L'audit portait plus particulièrement sur la protection des données à caractère personnel et des actifs de données nationaux.

Dans le cadre de l'audit, l'ISC a évalué les méthodes de gestion de six organisations responsables de la gestion des données (notamment, l'administration fiscale, le trésor national, l'assurance-maladie, le versement des retraites, le bureau de l'enseignement, les données à caractère personnel et les adresses, les informations sur les véhicules et les trajets, et les agences administratives responsables de la gestion des données judiciaires), ainsi que les activités de l'autorité de protection des données et celles de l'autorité de sécurité de l'information.

Elle s'est intéressée en particulier au mandat des organisations gérant les données, notamment en cas de transferts de données à des tiers. Au cours de l'audit des contrôles internes portant sur la gestion et le traitement des données, l'ISC a cherché à déterminer s'il existait des règlements actualisés régissant les obligations, les responsabilités et les compétences, la gestion des ressources humaines et les processus.

En ce qui concerne les systèmes électroniques utilisés dans le cadre de la gestion des données, l'ISC a examiné les mesures de sécurité correspondantes, y compris la protection physique, les droits d'accès, la connexion, les procédures d'évaluation de la sécurité, la sécurité du système et des communications, ainsi que la conformité de la classification de l'organisation dans son ensemble du point de vue de la sécurité.

L'externalisation du traitement des données a été auditée sur la base des contrats conclus afin de déterminer si les organisations responsables de la gestion des données imposaient aux organisations traitant les données de respecter les exigences relatives aux activités de traitement des données, conformément à la réglementation.

Constatations et conclusions

Se fondant sur ses travaux d'audit, l'ISC hongroise a constaté que les règlements internes relatifs aux activités de gestion des données établis par les organisations responsables en la matière garantissaient la protection des actifs de données nationaux, qui font partie intégrante des actifs nationaux, conformément aux dispositions légales en vigueur entre 2011 et 2015. En pratique, les responsables du traitement des données avaient correctement appliqué les exigences en matière de sécurité concernant la gestion des données et l'externalisation de leur traitement. Le transfert de données à des tiers était mis en œuvre dans le cadre d'un mandat approprié et avec une délimitation claire des responsabilités et des compétences.

En ce qui concerne certains responsables du traitement des données, l'audit a révélé que la classification de sécurité des systèmes électroniques et de l'organisation dans son ensemble n'était pas toujours conforme aux exigences légales, mais les défaillances n'étaient pas assez importantes pour nuire substantiellement à la sécurité des données traitées. Sur la base des recommandations formulées dans le rapport d'audit, les organisations chargées de la gestion des données ont remédié aux défaillances dans le cadre de plans d'action approuvés par l'ISC.

En ce qui concerne l'audit international parallèle réalisé en coopération avec le groupe de travail de l'Eurosai sur les technologies de l'information, l'ISC a estimé que la législation hongroise relative à la protection des données était conforme à la directive de l'UE en vigueur.

En conclusion, grâce à son audit de la protection des données, l'ISC hongroise a contribué à la bonne gouvernance et à la protection des actifs de données nationaux.

Autres rapports dans le domaine

Titre du rapport:	Rapport – Audits de suivi – Audit sur la protection des données – Audit du cadre national de protection des données et de certains enregistrements essentiels de données dans le cadre de la coopération internationale
Hyperlien vers le rapport:	rapport (en hongrois)
Date de publication:	2020

Pays-Bas
Cour des comptes

Cybersécurité des structures critiques de gestion des eaux et des contrôles aux frontières aux Pays-Bas

Dates de publication: mars 2019 et avril 2020

Hyperlien vers les rapports: synthèse du rapport sur la cybersécurité et sur les structures critiques de gestion des eaux (en anglais)
synthèse du rapport sur la cybersécurité et sur les contrôles automatisés aux frontières (en anglais)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2018-2020

Synthèse du rapport

Sujet de l'audit

En 2018, la Cour des comptes néerlandaise a décidé de réaliser des audits sur la cybersécurité dans certains secteurs essentiels de la société. Forte de sa longue expérience des audits de conformité en matière de sécurité de l'information au sein de l'administration centrale, la Cour des comptes a estimé qu'auditer la *performance* des politiques et des mesures en vigueur apportait une valeur ajoutée. L'audit a d'abord porté sur la gestion des eaux, vitale pour une nation dont une grande partie est située sous le niveau de la mer, puis sur les contrôles automatisés aux frontières, en raison de l'importance de l'aéroport de Schiphol (Amsterdam) en tant que plateforme internationale et point d'accès vers le pays.

Le ministre des infrastructures et de la gestion des eaux a qualifié d'«éléments critiques» du secteur un certain nombre de structures hydrauliques gérées par la direction générale des travaux publics et de la gestion des eaux (l'entité auditée). De nombreux systèmes informatiques servant à faire fonctionner les structures

hydrauliques critiques datent des années 1980 et 1990, une époque où la cybersécurité était rarement prise en considération. Ces systèmes avaient été initialement conçus pour fonctionner de manière autonome, mais ont progressivement été reliés à d'autres réseaux informatiques plus importants, notamment dans le but de faciliter les opérations à distance. Cette tendance a rendu les systèmes plus vulnérables aux cybermenaces.

Le ministre de la défense et celui de la justice et de la sécurité se partagent la responsabilité des contrôles réalisés par les gardes-frontières néerlandais à l'aéroport de Schiphol. Les deux ministères (les entités auditées) possèdent des systèmes informatiques sur lesquels les gardes-frontières s'appuient. Ces systèmes sont essentiels aux opérations aéroportuaires et sont utilisés pour traiter des données très sensibles. Ainsi, ils constituent des cibles de choix pour des cyberattaques dont le but est de saboter, d'espionner ou de manipuler les contrôles aux frontières.

Les auditeurs ont examiné comment les entités auditées entendaient gérer les cybermenaces et ont cherché à déterminer si leur action était efficace.

- Les audits devaient permettre de répondre aux questions suivantes: Comment les entités auditées *protègent-elles* les systèmes contre les cybermenaces et *préviennent-elles* les cyberattaques?
- Comment les entités auditées *détectent-elles* les cybermenaces et les cyberattaques?
- Comment les entités auditées *réagissent-elles* en cas de cyberattaque?

Les deux audits étaient axés sur l'efficacité. En étroite coopération avec les entités auditées, des pirates éthiques ont mis à l'épreuve les structures hydrauliques critiques et l'un des systèmes de contrôle aux frontières. Il va sans dire que des mesures ont été prises, avant la publication des rapports, pour corriger toutes les défaillances détectées lors des tests et qu'aucun détail technique n'a été révélé.

La principale différence entre les deux audits était que celui concernant les structures hydrauliques était centré sur la réalisation des objectifs de l'entité auditée, tandis que celui concernant les contrôles aux frontières était fondé sur le cadre de cybersécurité du NIST.

Constatations

En premier lieu, les deux audits ont révélé que les entités auditées étaient conscientes des cybermenaces et qu'elles procédaient à la mise en place d'une approche professionnelle pour y faire face.

Dans le cas des structures hydrauliques, toutefois, pour pouvoir atteindre ses propres objectifs en matière de cybersécurité, l'entité auditée devait encore intensifier ses efforts, tant sur le plan de la détection des menaces que sur celui de la réponse apportée. L'entité auditée a établi un centre des opérations de sécurité pour détecter les cyberattaques et y répondre. Cependant, l'objectif fixé pour la fin 2017, à savoir détecter instantanément toute cyberattaque dirigée contre les structures hydrauliques critiques, n'avait pas été atteint à l'automne 2018, ce qui signifiait qu'une cyberattaque dirigée contre une structure hydraulique critique risquait de ne pas être détectée ou de l'être trop tard. En outre, le test réalisé auprès de l'une des structures hydrauliques critiques a révélé qu'il était possible d'y accéder physiquement. Des pirates sont parvenus à pénétrer dans la salle de contrôle et se sont retrouvés seuls avec des postes de travail non sécurisés. Enfin, l'entité auditée n'avait prévu aucun scénario dans lequel une cyberattaque déclenchait une crise, et les informations concernant la réponse à apporter étaient incomplètes ou obsolètes. L'existence d'informations actualisées pourrait s'avérer cruciale pour réagir de manière rapide et efficace en situation de crise.

En ce qui concerne les contrôles aux frontières, les mesures de cybersécurité n'étaient ni adéquates ni adaptées aux besoins futurs. Premièrement, les principaux systèmes de contrôle aux frontières devaient être formellement approuvés avant le lancement de l'opération afin de garantir la mise en œuvre de toutes les mesures de cybersécurité. Nous avons constaté que deux des trois systèmes étaient opérationnels sans avoir été approuvés, ce qui signifie qu'il n'y avait aucune garantie que les mesures de sécurité nécessaires étaient en place. Deuxièmement, un centre des opérations de sécurité était opérationnel, mais aucun des systèmes n'y était directement relié. Même si les infrastructures génériques étaient reliées au centre des opérations de sécurité, il existait toujours un risque que les cyberattaques ne soient pas détectées ou qu'elles le soient trop tard. Troisièmement, les tests de sécurité n'étaient pas effectués régulièrement. En fait, seul l'un des trois systèmes avait déjà été testé auparavant, et uniquement de manière limitée. Enfin, comme pour le premier audit, aucun scénario spécifique n'avait été prévu en cas de crise déclenchée par une cyberattaque.

Au cours du test de sécurité de l'un des systèmes qui n'avaient encore jamais été testés, les pirates éthiques ont décelé un certain nombre de faiblesses qui pouvaient être exploitées avec l'aide d'un complice infiltré afin de lancer une cyberattaque visant à accéder à des informations dans le système, à les copier et même à les manipuler. Ces résultats montrent à quel point il est important d'effectuer régulièrement des tests de sécurité.

Les constatations sont préoccupantes compte tenu de la procédure actuelle d'automatisation des contrôles aux frontières. Bientôt, un nombre croissant de systèmes de contrôle aux frontières traiteront de plus en plus de données en exploitant des connexions de plus en plus nombreuses, ce qui augmente le risque de cyberattaques. L'approche adoptée n'était donc pas adaptée aux besoins futurs.

Conclusions

Dans le cas des structures hydrauliques, certains éléments clés ont empêché l'entité auditée de mettre en œuvre les dernières mesures de cybersécurité. Par exemple, le niveau de menace ne pouvait être clairement évalué, et il était donc difficile de déterminer si les mesures adoptées et le budget alloué étaient suffisants ou non. Par ailleurs, le service central responsable de la cybersécurité n'était pas habilité à appliquer les mesures de cybersécurité nécessaires dans les structures hydrauliques décentralisées. L'organisation a suivi les recommandations formulées dans l'audit à cet égard, ce qui l'a aidée à progresser.

En ce qui concerne les contrôles aux frontières, aucune raison précise ne pouvait justifier le niveau insuffisant de cybersécurité. Les travaux d'audit ont révélé l'existence de politiques et de procédures complètes et détaillées en matière de cybersécurité, ainsi que celle d'un niveau d'expertise suffisant et d'un personnel compétent. Par conséquent, les recommandations formulées à l'issue de l'audit visaient principalement à garantir que toutes les mesures possibles étaient effectivement mises en œuvre.

Les deux audits ont suscité un vif intérêt de la part du parlement et des médias. Ils ont sensibilisé à l'importance de la cybersécurité dans les infrastructures vitales et ont apporté aux entités auditées des indications sur les moyens de renforcer leur sécurité numérique. Une étroite coopération avec l'entité auditée était essentielle pour appréhender pleinement la situation de cette dernière et pour gérer les risques inhérents à la réalisation d'enquêtes et de tests sur la cybersécurité.

Un troisième audit est prévu dans cette série. En outre, le niveau de sécurité de l'information au sein du gouvernement national néerlandais constitue un élément essentiel du cycle annuel des audits de conformité. Au fil des ans, l'ISC néerlandaise a constaté que les mesures adoptées par de nombreux ministères en faveur de la sécurité de l'information laissent à désirer. La Cour des comptes exploite actuellement l'expérience acquise lors de ses audits de la cybersécurité pour élargir ses perspectives en matière d'audits de la sécurité de l'information, en allant au-delà de l'analyse des documents et des politiques et en testant l'efficacité réelle des mesures.

Autres rapports dans le domaine

Titre du rapport:	*Staat van de rijksverantwoording 2019*, chapitre 3
Hyperlien vers le rapport:	rapport (en néerlandais)
Date de publication:	2020

Titre du rapport:	Le télétravail numérique au centre de l'attention
Hyperlien vers le rapport:	rapport (en néerlandais)
Date de publication:	2020

Pologne
Najwyższa Izba Kontroli

Assurer un fonctionnement sécurisé des systèmes informatiques utilisés pour l'exercice des missions publiques

Date de publication: 2016

Hyperlien vers le rapport: rapport (en polonais)

Type d'audit et période couverte

Type d'audit: audit de conformité

Période couverte par l'audit: 2014-2015

Synthèse du rapport

Sujet d'audit

L'objectif de l'audit était de déterminer si les données collectées dans les systèmes destinés à mettre en œuvre d'importantes missions publiques étaient sécurisées au sein des unités auditées. L'audit portait sur une sélection de six institutions chargées de missions publiques importantes. À l'issue de l'analyse, un système informatique essentiel a été sélectionné au sein des institutions, avant d'être examiné en détail. La version 4.1 de la méthode COBIT a été appliquée dans l'audit,

lequel a été effectué à la suite de l'évaluation, en 2015, de la performance des «organismes publics» en matière de cybersécurité en Pologne[67], dont les résultats suggéraient des problèmes systémiques. L'audit de 2016 a démontré, entre autres, que l'administration publique n'avait jusqu'alors pris aucune mesure visant à garantir la sécurité informatique du pays. Il y a été conclu que les activités des organismes publics en matière de protection du cyberespace avaient été menées de manière fragmentée et sans approche systématique. L'administration centrale n'ayant pas établi de dispositions centrales visant à assurer des conditions de sécurité concrètes

[67] https://www.nik.gov.pl/kontrole/P/14/043/

pour certains systèmes informatiques spécifiques, essentiels au fonctionnement de l'État, l'ISC s'est attachée à déterminer si les institutions responsables de l'administration des systèmes informatiques utilisés pour mener à bien d'importantes missions publiques s'assuraient que lesdites missions pouvaient être mises en œuvre de manière sécurisée.

Un autre audit des systèmes, consacré à la cybersécurité en Pologne, a été approuvé en 2019, mais les constatations qui y sont formulées sont confidentielles.

Questions d'audit

Les sous-objectifs ont été divisés en deux domaines d'évaluation, en vue de répondre à des questions spécifiques.

En ce qui concerne l'appui à la sécurité informatique, l'audit visait notamment à déterminer, au niveau de l'organisation dans son ensemble, si:

- des mesures de gestion de la sécurité informatique étaient en place;
- des plans visant à garantir la sécurité informatique étaient mis en œuvre;
- la sécurité informatique était testée, supervisée et contrôlée,
- les incidents de sécurité informatique étaient définis;
- les systèmes informatiques étaient gérés par des clés cryptographiques;
- la détection des logiciels malveillants était assurée, au même titre que la protection contre ces derniers et l'application de solutions correctives;
- la sécurité des réseaux était garantie.

En ce qui concerne l'appui à la sécurité, l'audit visait notamment à déterminer, au niveau des systèmes sélectionnés, si:

- des mesures de gestion de l'identité et des comptes des utilisateurs étaient en place;
- les technologies de sécurité et les données sensibles étaient protégées.

Constatations et conclusions

Le degré de préparation et de mise en œuvre du système de sécurité de l'information ne fournissait pas un niveau acceptable de sécurité des données collectées par les systèmes informatiques destinés à réaliser d'importantes missions publiques. Les processus de sécurité de l'information étaient réalisés de manière désordonnée et intuitive, faute de procédures définies. Sur les six institutions auditées, seule une mettait en œuvre le système de sécurité de l'information, et il convient de noter que son fonctionnement était également affecté par des défaillances considérables. Dans toutes les unités auditées, sauf une, les travaux visant à garantir les conditions appropriées pour la sécurité des informations traitées par les systèmes informatiques n'avaient pas atteint un niveau satisfaisant en raison du fait que, ayant commencé récemment, les travaux se trouvaient encore à l'étape préliminaire, et les bases officielles nécessaires n'avaient pas encore été établies. Ils étaient fondés sur des dispositions simplifiées ou informelles tirées de bonnes pratiques ou de l'expérience acquise par le personnel informatique à ce moment-là.

Conformément à la méthodologie COBIT 4.1, la maturité des processus de gestion de la sécurité de l'information dans les différentes unités auditées variait entre 1) initiale/ad hoc et 3) définie, sur une échelle de zéro à cinq, cinq étant le maximum.

Dans les unités auditées, le coordonnateur de la sécurité était chargé de garantir la sécurité informatique. Toutefois, dans la pratique, il n'était pas habilité à gérer l'ensemble de la procédure. Les tâches concernées étaient souvent réalisées par une seule personne. Bien que des équipes d'experts aient été nommées ou des accords conclus avec des prestataires externes, l'analyse requise pour déterminer si les services fournis répondaient aux besoins d'une unité en matière de sécurité n'avait pas été réalisée. Les unités auditées n'avaient qu'une compréhension fragmentée et limitée de la nécessité de garantir la sécurité informatique. La sécurité des données était principalement considérée comme relevant de la responsabilité et du domaine du service informatique, et non de celle de toutes les unités organisationnelles chargées de tâches réglementaires, ce qui a considérablement freiné le développement de systèmes de gestion de la sécurité informatique dans l'ensemble de l'institution.

Lors de la comparaison du degré de respect des obligations en matière de sécurité de l'information au niveau des organisations entières et à celui des systèmes sélectionnés, il apparaît clairement que le degré de mise en œuvre était supérieur dans le second cas. Cela peut s'expliquer par l'incidence des connaissances pratiques et de la mobilisation du personnel technique de niveau intermédiaire sur la sécurité, par l'utilisation accrue au sein de l'administration publique de systèmes informatiques

commerciaux basés sur des normes de marché ainsi que par le déploiement de solutions avancées en matière de sécurité. Grâce à de telles solutions, à l'expérience acquise et aux bonnes pratiques appliquées, il a été possible de maintenir un certain niveau de sécurité dans le fonctionnement des différents systèmes dans des conditions de ressources limitées, de défaillances organisationnelles ou de réglementation «dysfonctionnelle». Cependant, cette solution n'est pas à privilégier puisqu'en cas d'augmentation dynamique du niveau de menace, la sécurité des systèmes informatiques ne peut être assurée par des mesures gérées de manière désordonnée et équipées uniquement en vue de surmonter les difficultés immédiates.

Conclusions de l'audit

Il convient d'élaborer et de mettre en œuvre au niveau central des exigences et recommandations générales en matière de sécurité informatique qui soient applicables à tous les organismes publics. Il est par ailleurs nécessaire d'adopter une solution systémique selon laquelle les résultats des audits de la sécurité informatique seraient rendus publics afin que les citoyens puissent accéder aux informations relatives aux activités des organismes publics, tandis que l'accès aux connaissances sur les mesures et les méthodes employées pour garantir la sécurité des informations traitées serait restreint.

Autres rapports dans le domaine

Titre du rapport:	Gestion de la sécurité de l'information par les autorités régionales
Hyperlien vers le rapport:	rapport (en polonais)
Date de publication:	2019

Titre du rapport:	La cybersécurité en Pologne (informations classifiées)
Hyperlien vers le rapport:	*inaccessible au public*
Date de l'approbation:	2019

Titre du rapport:	La sécurité des systèmes informatiques garantie par les autorités régionales dans la voïvodie de Podlachie
Hyperlien vers le rapport:	rapport (en polonais)
Date de publication:	2018

Titre du rapport:	Prévenir et combattre le harcèlement en ligne chez les enfants et les jeunes
Hyperlien vers le rapport:	rapport (en polonais)
Date de publication:	2017

Titre du rapport:	Exercice des missions de cybersécurité par les organismes publics en Pologne
Hyperlien vers le rapport:	rapport (en polonais)
Date de publication:	2015

Titre du rapport:	Mise en œuvre d'une sélection d'exigences en matière de systèmes d'information, d'échange d'informations électroniques et du cadre d'interopérabilité national sur la base d'exemples issus de certains conseils municipaux et villes jouissant des droits de district.
Hyperlien vers le rapport:	rapport (en polonais)
Date de publication:	2015

Portugal
Tribunal de Contas

Audit du passeport électronique portugais

Date de publication: 2014

Hyperlien vers le rapport: rapport (en portugais)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2013

Synthèse du rapport

Sujet de l'audit

L'audit de la mise en œuvre du PEP était axé sur l'efficacité des systèmes d'information qui sous-tendent la délivrance, l'émission et l'utilisation du passeport, en particulier le contrôle automatisé des passagers par la lecture des données biométriques aux frontières portugaises[68].

L'audit visait essentiellement à:

- vérifier la conformité avec le droit de l'UE, les législations nationales, les normes internationales et les lignes directrices régissant la délivrance, l'émission et l'utilisation des PEP, y compris le caractère approprié du cadre juridique national;
- examiner l'efficacité des principaux processus associés au cycle de vie du PEP, notamment ceux qui concernent la délivrance, l'émission et l'utilisation du passeport;

[68] Nous faisons référence ici aux systèmes de contrôle automatisé aux frontières au sein de Frontex (l'Agence européenne de garde-frontières et de garde-côtes).

- analyser certains aspects critiques de la performance des systèmes d'information, en particulier le respect des exigences de sécurité relatives aux systèmes d'information des passeports électroniques portugais (SIPEP).

Les principaux domaines à risque étaient les suivants:

- la perte/le vol de biens physiques et/ou d'informations électroniques;
- l'utilisation abusive d'informations confidentielles;
- le risque de non-conformité (non-respect des exigences légales et réglementaires).

Période couverte par l'audit: 1er janvier 2013 – 31 décembre 2013 (le cas échéant, la couverture a été étendue aux années précédentes ou suivantes).

Constatations et conclusions

Il existe trois catégories de PEP: le passeport traditionnel[69], le passeport diplomatique et le passeport spécial. S'y ajoute un passeport destiné aux ressortissants étrangers, qui confère des privilèges restreints.

Le système d'établissement des PEP compte plusieurs formulaires de demande et différents organismes assurant la collecte des données et la délivrance du passeport, mais un seul organe d'émission (chargé de la production, de la personnalisation et de la livraison).

Plusieurs entités (les «entités PEP») interviennent dans la procédure. Celles qui collectent les données et délivrent des passeports sont:

- Portugal continental: *Serviço de Estrangeiros e Fronteiras* (SEF)[70] et *Instituto dos Registos e do Notariado* (IRN)[71];

[69] Environ 99 % de l'ensemble des passeports.

[70] Service de l'immigration et des frontières.

[71] Service des greffes et du notariat (collecte uniquement).

- régions autonomes des Açores[72] et de Madère: services relevant de la *Vice-Presidência do Governo Regional*[73] compétente; à l'étranger: les consulats du Portugal;
- l'Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] émet et délivre les passeports.

Les principaux processus reposent en grande partie sur le SIPEP (système central de gestion des demandes pour l'émission des passeports portugais). Le SIPEP permet d'enregistrer, de stocker, de traiter, de valider et de fournir les informations requises pour la délivrance du PEP. En outre, il déclenche la procédure de personnalisation menée par l'INCM et garantit l'interconnexion avec les autres demandes dans le système, en coordonnant toutes les entités PEP qui participent à l'enregistrement physique et logistique des données collectées.

Les entités PEP ont une structure organisationnelle qui leur permet d'atteindre les objectifs juridiques en la matière. Le système est toujours fortement dépendant des ressources humaines disponibles aux niveaux de la demande et de la collecte. Cependant, le SIPEP prévoit plusieurs fonctions de traitement et contrôles de validation automatiques.

Puisque les procédures garantissent les fonctions de contrôle et de traitement des données, dont certaines peuvent être menées de manière indépendante, sans intervention humaine, le SIPEP a une incidence considérable sur l'organisation et le système d'information, notamment en ce qui concerne: i) la compréhension et la définition des normes, des processus et des données requises; ii) la définition d'exigences propres au système d'information.

---

[72] Ainsi que les points de service de l'*Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – Agence pour la modernisation et la qualité du service aux citoyens, institut public (collecte uniquement).

[73] Vice-présidence des autorités régionales.

[74] L'Imprimerie nationale et la Monnaie, entreprise publique.

L'efficience et l'efficacité du processus de collecte des données sont garanties par l'interaction du SIPEP avec d'autres systèmes d'information[75], conformément à la réglementation.

Un cadre de contrôle général des activités informatiques (gouvernance, développement et acquisition, opérations informatiques, continuité des activités et rétablissement après sinistre, sécurité de l'information) a été établi, bien qu'il ne soit pas très documenté. Il garantit le développement, le fonctionnement, la gestion et la maintenance du SIPEP.

Indicateurs d'activité (2013):

- le Portugal a délivré quelque 500 000 PEP, dont environ 63 % remis par le SEF, 33 % par les consulats portugais et 4 % par les autorités régionales;
- les recettes générées par l'émission des PEP représentaient un total d'environ 37 millions d'euros, provenant principalement de l'INCM (43 %), du SEF (32 %) et du *Ministério dos Negócios Estrangeiros* (MNE)[76] (17 %).

Pour l'année 2013, les tests effectués au niveau du SIPEP n'ont pas permis de confirmer le respect du délai de livraison maximal établi par la législation (de la date de la demande jusqu'à la mise à disposition du PEP au point de retrait), car la date effective de livraison au point de retrait n'était pas toujours enregistrée en temps voulu.

Le SEF, le MNE, la RIAC et l'INCM ont réalisé des investissements liés à l'acquisition d'équipements pour la collecte des signatures et données biométriques (guichets), d'équipements pour les systèmes de contrôle automatisé aux frontières, ainsi qu'à l'achat et à la maintenance de systèmes informatiques, de services et d'une assistance technique, pour un montant de 11 millions d'euros, le SEF ayant investi le montant le plus élevé.

Avant l'apparition du PEP, le prix du passeport (non biométrique) de la République portugaise s'élevait à 22,24 euros. En 2006, le PEP (biométrique) traditionnel coûtait 60 euros, et il est passé à 65 euros en 2011.

---

[75] À savoir: le système d'information intégré du SEF (SIISEF); la partie nationale du système d'information Schengen (NSIS); la base de données d'identification civile; la base de données relative aux casiers judiciaires).

[76] Ministère des affaires étrangères.

Les demandes de PEP

Les demandes de PEP sont traitées par des agents des services compétents, qui reçoivent les dossiers de demande, collectent les données biographiques et biométriques des demandeurs, perçoivent les redevances, puis délivrent le passeport électronique.

Le système sous-jacent (SIPEP) valide l'exactitude et la qualité des données au moyen de contrôles virtuels et de recoupements avec d'autres systèmes d'information, notamment la base de données d'identification civile, ce qui permet de garantir que la demande est conforme et que le PEP peut être émis et délivré.

Les modifications de statut connexes sont enregistrées dans des fichiers journaux, garantissant le caractère vérifiable, l'intégrité et la non-répudiation des opérations.

La transmission de données entre les organismes de collecte des données (au Portugal et à l'étranger) et le SEF se fait par RPV (réseau privé virtuel) grâce à un système de gestion des accès reposant sur un contrôle des identifiants par le SEF[77].

Le traitement des demandes de PEP traditionnel diffère lorsqu'elles sont déposées par des citoyens dont les droits sont limités ou restreints, notamment: i) ceux qui ne peuvent exercer leurs droits (les mineurs, les personnes frappées d'incapacité ou d'interdiction); ii) les personnes exclues par voie judiciaire ou par la police (en raison d'un casier judiciaire, ou encore d'une poursuite judiciaire ou d'une saisie de documents en cours); iii) les personnes soumettant une demande pour un deuxième PEP, lorsqu'elles invoquent un intérêt national ou légitime.

Délivrance du PEP

La décision de délivrance d'un PEP traditionnel peut être:

- automatique – approbation automatique par le SIPEP après validation de l'identité du demandeur et confirmation de l'absence de casier judiciaire (par recoupement avec les bases de données d'identification civile et de casiers judiciaires de l'IRN) et de l'absence de poursuites en cours. Uniquement lorsque

[77] Le SIPEP est accessible (sur internet), aux niveau national/régional et international, pour les services situés sur le continent, dans les régions autonomes des Açores et de Madère ainsi qu'à l'étranger (consulats portugais).

l'autorité délivrant le passeport est le SEF, pour les demandes de PEP sur le continent[78];

- soumise à l'acceptation/approbation, au cas par cas, d'autres entités (autorités régionales et représentations consulaires) ou, lorsqu'il s'agit du SEF, à des exigences ne relevant pas de la procédure de délivrance automatique[79].

Émission du PEP

L'émission du PEP, qui comprend la production, la personnalisation et la livraison, relève de la compétence de l'INCM. Lorsque la livraison d'un PEP est enregistrée dans le SIPEP, le statut du passeport est modifié et celui-ci devient «valide».

Le prix varie en fonction du niveau de service requis. Pour mesurer le niveau de service, le SIPEP doit prendre en considération la date de livraison effective du passeport,

une livraison assurée par un service de transport externe.

Résiliation des PEP

Lorsqu'un demandeur remet un PEP antérieur toujours valide, ce dernier doit être invalidé pour empêcher toute réutilisation ce qui correspond au statut «inutilisable» dans le système de demande du SIPEP.

---

[78] Il s'agit d'une fonctionnalité automatisée du SIPEP permettant de valider (ou, selon le jargon interne, d'«autoriser») une demande (sauf pour un deuxième PEP) émanant d'un citoyen en âge légal, muni d'une carte d'identité valide, ne faisant pas l'objet de poursuites judiciaires et n'étant ni exclu ni déchu de ses droits. Les PEP traditionnels délivrés par le SEF, soit 60 % environ de l'ensemble des passeports, relevaient de procédures de validation et de décisions d'octroi automatiques, tandis que les passeports restants étaient soumis pour examen et approbation à la *Direção Central de Imigração e Documentação* (DCID).

[79] Notamment dans le cas de demandeurs incapables d'exercer leurs droits (les mineurs, les personnes frappées d'incapacité ou d'interdiction), de personnes exclues par voie judiciaire ou par la police, ou encore lorsqu'il s'agit d'un deuxième PEP, les demandes étant examinées au cas par cas par la DCID.

Finlande
Valtiontalouden tarkastusvirasto

Dispositions en matière de cyberprotection

Date de publication: 2017

Hyperlien vers le rapport: rapport (en finlandais)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2016-2017

Synthèse du rapport

Sujet de l'audit

L'objectif de l'audit était de déterminer si la cyberprotection au sein de l'administration centrale avait été mise en place de manière aussi efficace que possible et selon un rapport coût-efficacité optimal. L'audit était centré sur l'organisation et la gestion de la cybersécurité au sein de l'administration centrale. Les résultats de l'audit ont pu être utilisés pour renforcer l'efficience et l'efficacité de la cybersécurité dans l'administration centrale. L'audit s'est déroulé du 22 septembre 2016 au 4 septembre 2017. Un suivi a été assuré à l'automne 2019. Au cours du suivi, l'ISC a examiné les mesures prises pour donner suite aux constatations et recommandations de l'audit.

Parmi les entités auditées figuraient les autorités chargées de la cyberprotection au sein de l'administration centrale (le bureau du Premier ministre, le ministère des finances ainsi que le ministère des transports et des communications) et celles responsables des activités de cyberprotection et des services informatiques centralisés au sein de l'administration centrale (le centre national de cybersécurité de l'agence finlandaise des transports et des communications, le centre national Valtori pour les technologies de l'information et de la communication, l'agence des services numériques démographiques). L'efficacité des orientations fournies a également été

évaluée. Pour ce faire, il a été procédé à un examen des entités de l'administration centrale responsables des services électroniques (l'agence des services numériques et démographiques, l'agence finlandaise des transports et des communications (Traficom), le bureau administratif national chargé de l'exécution ainsi que le ministère de la justice, dont il relève, et enfin le centre de services TIC dudit ministère).

Questions d'audit

Les questions d'audit suivantes ont été posées afin d'évaluer l'organisation de la cybersécurité:

- L'entité auditée a-t-elle suffisamment tenu compte de l'aspect économique lorsqu'elle a organisé la cybersécurité?
- La cybersécurité des systèmes bénéficie-t-elle des connaissances de l'entité auditée en la matière?
- La capacité de l'entité auditée à réagir aux cyberattaques est-elle suffisante?

L'audit des dispositions en matière de cyberprotection relevait du thème «Garantir la fiabilité opérationnelle de la société de l'information» inscrit au programme d'audit 2016-2020 de l'ISC de Finlande. Du point de vue de son importance financière pour l'administration centrale, le sujet d'audit se justifie, étant donné les préjudices causés par les interruptions de service et les violations de données, ainsi que les effets néfastes produits sur les activités commerciales par une cybersécurité insuffisante. L'audit a été réalisé en parallèle avec un autre, intitulé «Guider la fiabilité opérationnelle des services électroniques», qui relève du même thème. Il s'est appuyé essentiellement sur de documents et sur des entretiens menés avec les autorités responsables de l'activité en question.

Constatations et conclusions

La stratégie de la Finlande en matière de cybersécurité définit les principaux objectifs et politiques visant à faire face aux défis auxquels est confronté le cyberenvironnement, ainsi qu'à garantir le fonctionnement de ce dernier. Des efforts ont été consentis pour mettre en œuvre la stratégie de cybersécurité sur la base d'un programme dont l'exécution est évaluée chaque année. Le comité de sécurité est un organisme de coopération au sein du ministère de la défense qui contrôle et coordonne la mise en œuvre de la stratégie en matière de cybersécurité.

Une organisation efficace de la cybersécurité exige une bonne gestion du risque qui, à son tour, requiert des structures et modalités de gestion efficaces permettant d'intégrer la gestion du risque dans les opérations à tous les niveaux de l'organisation. À l'instar de nombreux autres pays, la Finlande (c'est-à-dire son administration centrale) ne dispose pas de ressources propres suffisantes pour assurer sa cyberprotection. La législation de l'Union européenne s'est développée au fil du temps et est devenue plus contraignante. Au sein du gouvernement finlandais, les compétences en matière de cyberprotection sont décentralisées, chaque organe étant responsable de sa propre cybersécurité. Dans l'administration centrale, la répartition des responsabilités en ce qui concerne la nature, l'étendue et la mise en œuvre des réponses apportées aux éventuelles cyberattaques est complexe.

Du fait de cette complexité, la réponse à un incident peut être excessivement lente, et le financement limité a freiné la mise en œuvre de la stratégie de la Finlande en matière de cybersécurité. Sur la base des constatations d'audit, l'ISC a formulé les conclusions et recommandations ci-après en ce qui concerne l'organisation de la cybersécurité dans l'administration centrale:

La gestion opérationnelle des atteintes majeures à la cybersécurité n'était pas définie

La planification de la gestion opérationnelle des atteintes majeures à la cybersécurité ainsi que le partage des responsabilités à cet égard permettraient des réactions plus rapides, une coordination appropriée et l'affectation de ressources à la mise en place de contre-mesures. Dans le modèle de fonctionnement actuel, chaque agence est responsable de sa propre cyberprotection. Elles ne disposent toutefois pas d'une expertise suffisante en la matière, ce qui les empêche de mettre en place une cyberprotection en interne ou en externalisant.

Certains des objectifs en matière de cybersécurité n'ont pas été atteints

Le programme de mise en œuvre de la stratégie de la Finlande en matière de cybersécurité a permis de renforcer la cyberprotection. Certains des objectifs du premier programme de mise en œuvre n'avaient pas été atteints, car les mesures suscitaient un intérêt variable qui n'a pu être stimulé de manière centralisée. Le nouveau programme de mise en œuvre prévoyait uniquement des mesures qui avaient recueilli l'adhésion des autorités compétentes et des autres acteurs. L'adhésion dépendait des ressources disponibles et vice-versa.

La pertinence des solutions de financement de la cyberprotection n'était pas claire

Les différences dans le développement de la cyberprotection étaient dues en partie à des inégalités au niveau des ressources de développement dont disposaient les organisations. Aucune procédure visant à garantir que les fonds étaient affectés aux objectifs les plus importants en matière de cyberprotection n'a été mise en évidence dans les règlements concernant l'élaboration du budget de l'État ou au moment de l'établissement de celui-ci. Les agences et institutions ont imputé les crédits alloués à la cybersécurité au budget des dépenses de fonctionnement de l'agence ou de l'institution, sans définir de poste spécifique. Les mesures décrites dans la stratégie de la Finlande en matière de cybersécurité n'ont été mises en œuvre que dans la limite des crédits disponibles.

La cyberprotection devrait également être prise en considération dans les modifications apportées à l'organisation des TIC

Les modifications apportées à l'organisation des TIC au sein de l'administration centrale ont influencé les dispositions en matière de cyberprotection. La mise en place d'une cybersécurité centralisée par le centre Valtori s'est révélée difficile. L'évaluation de la pertinence des procédures concrètes en matière de cyberprotection et la mise en œuvre des nouvelles dispositions présentaient des déficiences.

Il convient d'améliorer la connaissance de la situation concernant les opérations de cybersécurité

Le centre de cybersécurité a veillé à ce que la situation en matière de cybersécurité soit connue à l'échelle nationale. Au moment de l'audit, il n'existait aucune obligation de signaler les atteintes à la sécurité informatique au centre de cybersécurité. Exiger des organisations publiques qu'elles signalent les incidents améliorerait la situation, de même qu'étendre la couverture des procédures centralisées de détection des cyberattaques.

Se fondant sur les constatations susmentionnées, l'ISC recommande au ministère des finances de définir et de mettre en œuvre un modèle à grande échelle pour la gestion opérationnelle des éventuels incidents de cybersécurité concernant les services TIC de l'administration centrale. Le ministère des finances devrait également déterminer comment tenir compte de l'aspect «cybersécurité» dans le financement des services, et ce sur tout le cycle de vie de ces derniers, et améliorer la connaissance de la situation opérationnelle en enjoignant aux autorités de signaler les cyberincidents au centre de cybersécurité. Il a été recommandé au centre Valtori d'améliorer la mise en

œuvre, l'évaluation et l'élaboration des procédures de cybersécurité et de détection des cyberincidents.

L'audit de suivi a consisté à examiner comment les recommandations formulées pendant l'audit initial avaient été mises en œuvre. L'ISC a considéré que le ministère des finances, en sa qualité d'autorité compétente pour la mise en œuvre des recommandations, n'avait pas pris de mesures suffisantes en réponse aux recommandations formulées. Cependant, la cybersécurité en Finlande avait également été renforcée par des mesures prises par d'autres autorités que le ministère des finances. On observait un basculement de la gestion stratégique de la cybersécurité vers un modèle directeur en la matière. Dans la proposition de budget pour 2020, le gouvernement a augmenté les crédits destinés aux autorités de l'administration centrale qui jouent un rôle essentiel dans le renforcement de la cybersécurité. En outre, le centre Valtori prenait des mesures conformes aux recommandations de lISC. Cette dernière a déclaré, en conclusion, qu'un audit de suivi s'avérait nécessaire étant donné que certaines recommandations n'avaient pas été mises en œuvre, et que la réalisation d'un nouvel audit totalement distinct dans le domaine était justifiée par l'évolution des dispositions en matière de cybersécurité, de l'environnement opérationnel numérique et des risques connexes, ainsi que par l'importance de la cybersécurité pour les finances de l'administration centrale et la société.

Suède
Riksrevisionen

L'obsolescence des systèmes informatiques: un obstacle à une transition numérique efficace

Date de publication: 2019

Hyperlien vers le rapport: synthèse du rapport (en anglais)
rapport (en suédois)

Type d'audit et période couverte

Type d'audit: audit de la performance

Période couverte par l'audit: 2018-2019

Synthèse du rapport

Sujet de l'audit

Les systèmes informatiques critiques obsolescents induisent un risque majeur du point de vue de l'efficience, car les organisations sont tenues de mobiliser proportionnellement davantage de ressources pour assurer ne fût-ce que la maintenance du système. L'on peut dès lors raisonnablement penser que les systèmes informatiques obsolescents font courir un risque élevé de mauvaise gestion des fonds publics. Ils supposent également un certain détournement des capacités d'innovation d'un organisme pour ce qui est de développer de nouveaux systèmes informatiques. Cependant, l'obsolescence des systèmes informatiques n'induit pas seulement des risques pour l'organisme concerné: les problèmes de ce dernier peuvent avoir de lourdes conséquences sur sa capacité à coordonner les opérations avec un autre organisme ou avec une partie prenante du secteur privé. Les systèmes informatiques obsolescents sont également porteurs de risques pour la sécurité de l'information.

Définition du principal sujet d'audit, des questions d'audit et du contexte

L'objectif de l'audit était d'examiner l'incidence des systèmes informatiques obsolescents dans l'administration centrale et de déterminer si le gouvernement et les autorités avaient pris les mesures appropriées pour empêcher ces systèmes de faire obstacle à une transition numérique efficace. Les questions d'audit étaient les suivantes:

- Les autorités ont-elles pris les mesures appropriées pour gérer les problèmes associés à l'obsolescence des systèmes informatiques?
- Le gouvernement a-t-il pris les mesures appropriées pour gérer les problèmes associés à l'obsolescence des systèmes informatiques?

Constatations et conclusions

- L'audit a révélé qu'un grand nombre d'organismes publics étaient dotés de systèmes informatiques obsolescents. Qui plus est, dans de nombreux organismes, cette obsolescence frappait un ou plusieurs systèmes informatiques essentiels à la poursuite des activités. À la connaissance de l'ISC suédoise, il s'agit là d'une information nouvelle, et personne n'était jusqu'alors conscient de l'étendue du problème au sein de l'administration centrale. Environ 80 % des organismes ont déclaré avoir du mal à maintenir un niveau de sécurité de l'information satisfaisant dans un ou plusieurs de leurs systèmes critiques. Plus d'une autorité sur dix a indiqué que le phénomène touchait la majorité, voire l'intégralité, de ses systèmes.
- Une grande partie des organismes audités n'avaient pas adopté l'approche adéquate pour le développement et la gestion du soutien informatique. Ils n'utilisaient pas les outils de développement opérationnel existants pour déterminer comment le soutien informatique pouvait contribuer au mieux à la réalisation des objectifs des opérations essentielles. Ils étaient donc nombreux à ne pas disposer d'une description d'ensemble de la manière dont les stratégies, les processus opérationnels et les systèmes étaient liés. Ainsi, ils ont rencontré des difficultés à analyser et à comprendre dans quelle mesure les changements influaient sur les objectifs de l'organisation, et il leur a été par conséquent d'autant plus difficile de définir une situation souhaitable pour l'avenir.

- Plus de la moitié des autorités ont déclaré qu'elles ne disposaient d'aucun modèle accepté sur lequel s'appuyer pour gérer leurs systèmes informatiques depuis la phase de développement jusqu'à la mise hors service (autrement dit, pour assurer la gestion du cycle de vie), ou pour prendre des décisions à cet égard. Selon l'ISC suédoise, cela montrait que la gestion du cycle de vie n'était pas assurée de manière structurée et méthodique. Des faiblesses ont également été observées dans les travaux d'analyse des risques et dans la capacité à ventiler les coûts informatiques selon un niveau de détail qui permette de prendre des décisions éclairées.

- Près de 60 % des autorités n'avaient pas établi de plan concernant le cycle de vie du développement des systèmes, sauf pour un ou deux systèmes critiques. Faute de documents de planification concernant, entre autres, le cycle de vie dans de nombreux organismes, et en raison de défaillances dans la mise en œuvre concrète de la gestion du cycle de vie, il n'a pu être considéré que les organismes, de manière générale, avaient adopté une position consciente et explicite sur leurs systèmes informatiques.

- L'ISC suédoise a estimé que les ministères concernés et, partant, le gouvernement, ne disposaient pas de connaissances suffisantes en ce qui concerne l'incidence et les conséquences de l'obsolescence des systèmes informatiques.

De manière générale, il a été conclu qu'au moment de l'audit, la plupart des organismes n'étaient pas vraiment parvenus à gérer efficacement les problèmes liés à l'obsolescence des systèmes informatiques. L'ISC suédoise a estimé que le problème était tellement grave et généralisé qu'il constituait un obstacle à la poursuite d'une transition numérique efficace de l'administration publique. L'audit a également révélé que le gouvernement n'était pas suffisamment informé de l'existence et des conséquences des problèmes liés à l'obsolescence des systèmes informatiques et qu'en outre, il n'avait pris aucune mesure pour remédier de manière plus directe au problème de l'obsolescence des systèmes informatiques. L'ISC suédoise a dès lors conclu qu'il n'était pas possible de considérer que le gouvernement avait pris les mesures suffisantes pour garantir une atténuation, voire la résolution, des problèmes.

Autres rapports publiés dans ce domaine

Titre du rapport:	Faciliter le lancement d'une entreprise: les efforts du gouvernement pour promouvoir le passage au numérique (RiR 2019:14)
Hyperlien vers le rapport:	synthèse du rapport (en anglais) rapport (en suédois)
Date de publication:	2019
Titre du rapport:	La transition numérique de l'administration publique: une administration simplifiée, plus transparente et plus efficace (RiR 2016:14)
Hyperlien vers le rapport:	synthèse du rapport (en anglais) rapport (en suédois)
Date de publication:	2016
Titre du rapport:	Les travaux liés à la sécurité de l'information dans neuf organismes (RiR 2016:8)
Hyperlien vers le rapport:	synthèse du rapport (en anglais) rapport (en suédois)
Date de publication:	2016
Titre du rapport:	Cybercriminalité – La police et le ministère public pourraient faire preuve d'une plus grande efficience (RiR 2015:21)
Hyperlien vers le rapport:	synthèse du rapport (en anglais) rapport (en suédois)
Date de publication:	2015

Union européenne
Cour des comptes européenne

Document d'information: Défis à relever pour une politique efficace dans le domaine de la cybersécurité

Date de publication: 2018

Hyperlien vers le rapport: rapport (disponible en 23 langues)

Type d'audit et période couverte

Type d'audit: analyse des politiques

Période couverte par l'audit: avril à septembre 2018

Synthèse du rapport

Objet de l'analyse

Ce document d'information, qui ne constitue pas un rapport d'audit, visait à donner une vue d'ensemble du paysage complexe de la politique de l'UE dans le domaine de la cybersécurité et à recenser les principales difficultés à surmonter pour mettre en place une politique efficace. Il porte sur la sécurité des réseaux et de l'information, la cybercriminalité, la cyberdéfense et la désinformation.

La Cour des comptes européenne a fondé son analyse sur un examen des documents officiels accessibles au public, des documents de prise de position et des études réalisées par des tiers. Les travaux sur le terrain ont été menés entre avril et septembre 2018, et les développements intervenus jusqu'à décembre 2018 ont été pris en considération. Ces travaux ont été complétés par une enquête auprès des ISC des États membres, ainsi que par des entretiens avec des acteurs clés des institutions de l'UE et des représentants du secteur privé.

Il n'existe aucune définition normalisée de la cybersécurité. Au sens large, le terme désigne toutes les garanties et mesures adoptées pour défendre les systèmes informatiques et leurs utilisateurs contre les accès non autorisés, les attaques et les dommages, de manière à assurer la confidentialité, l'intégrité et la disponibilité des données. La cybersécurité suppose de prévenir ou de détecter les cyberincidents, d'y répondre puis de rétablir la situation. Ces incidents peuvent être provoqués volontairement ou pas, et aller, par exemple, de la divulgation accidentelle d'informations à l'ingérence dans les processus démocratiques, en passant par les attaques contre les entreprises et les infrastructures critiques et le vol de données à caractère personnel.

La pierre angulaire de la politique de l'UE dans ce domaine est la stratégie de cybersécurité de 2013, qui vise à offrir à l'UE l'environnement numérique le plus sûr du monde, sans compromettre les valeurs et les libertés fondamentales. Elle poursuit les cinq grands objectifs suivants: i) renforcer la cyberrésilience; ii) faire reculer la cybercriminalité; iii) développer une politique et des moyens de cyberdéfense; iv) développer les ressources industrielles et technologiques en matière de cybersécurité; v) instaurer une politique internationale en matière de cyberespace qui soit conforme aux valeurs essentielles de l'UE.

Constatations

Compte tenu du manque de données fiables, il était difficile de mesurer l'incidence d'une préparation insuffisante aux cyberattaques. L'impact économique de la cybercriminalité a été multiplié par cinq entre 2013 et 2017, frappant de plein fouet les administrations publiques et les entreprises de toutes tailles. La croissance escomptée des primes de cyberassurance de 3 milliards d'euros en 2018 à 8,9 milliards d'euros en 2020 reflète cette tendance. Même si 80 % des entreprises de l'UE ont subi au moins un incident lié à la cybersécurité en 2016, la prise de conscience des risques reste d'une faiblesse alarmante. Dans l'UE, 69 % des entreprises n'ont qu'une compréhension de base, voire aucune compréhension, de leur exposition aux cybermenaces, tandis que 60 % n'ont jamais évalué les pertes financières potentielles. Selon une étude réalisée à l'échelle mondiale, un tiers des organisations préféreraient verser une rançon à des pirates plutôt qu'investir dans la sécurité informatique.

Les constatations de la Cour des comptes européenne sont les suivantes:

- Complexe et comportant plusieurs niveaux, le cyberécosystème de l'UE fait intervenir de nombreuses parties prenantes. Rassembler tous les éléments disparates qui le composent constitue un véritable défi.
- L'UE aspire à avoir l'environnement en ligne le plus sûr du monde. La réalisation de cette ambition requiert des efforts considérables de la part de toutes les parties prenantes, ainsi qu'une assise financière solide et bien gérée. Les chiffres sont difficiles à obtenir, mais selon certaines estimations, les dépenses publiques consacrées à la cybersécurité dans l'UE se situent entre un et deux milliards d'euros par an. À titre de comparaison, les dépenses inscrites au budget du gouvernement fédéral des États-Unis pour 2019 représentaient quelque 21 milliards d'euros.
- La gouvernance en matière de sécurité de l'information consiste à mettre en place des structures et des politiques permettant d'assurer la confidentialité, l'intégrité et la disponibilité des données. Plus qu'une simple question technique, elle requiert une direction efficace, des processus fiables et des stratégies conformes aux objectifs de l'organisation.
- Au sein des modèles de gouvernance de la cybersécurité, qui varient d'un État membre à l'autre, les responsabilités en matière de cybersécurité sont souvent réparties entre différentes entités. Ces différences pourraient entraver la coopération nécessaire pour réagir aux incidents transfrontières à grande échelle, ainsi que l'échange de renseignements sur les menaces au niveau national et, a fortiori, à l'échelle de l'UE.
- Il est essentiel d'élaborer une réponse efficace aux cyberattaques pour les arrêter le plus en amont possible. Il importe en particulier que les secteurs critiques, les États membres et les institutions de l'UE soient en mesure de réagir de manière rapide et coordonnée. Pour ce faire, une détection précoce est essentielle.

Recommandations

L'examen de la Cour des comptes européenne montre qu'il est nécessaire de passer à une culture de la performance qui intègre des pratiques d'évaluation si l'on veut garantir une réelle obligation de rendre compte et une véritable évaluation. Certains vides juridiques subsistent, et la législation existante n'est pas transposée

uniformément par les États membres. Cette situation pourrait empêcher la législation d'atteindre son plein potentiel.

Un autre défi recensé concerne l'alignement des niveaux d'investissement sur les objectifs stratégiques, qui suppose d'accroître l'investissement global et d'en amplifier l'impact. La tâche est d'autant plus ardue que l'UE et ses États membres ne disposent pas d'une vue claire des dépenses de l'UE en matière de cybersécurité. Il a également été fait état d'obstacles rencontrés par les agences de l'UE concernées par la cybersécurité pour se doter de ressources adéquates, y compris des difficultés à attirer et à retenir les talents.

Acronymes et abréviations

AED: Agence européenne de défense

Cadre CSP: cadre de coopération structurée permanente

CERS: Comité européen du risque systémique

CERT-UE: équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne

CFP: cadre financier pluriannuel

COBIT: objectifs de contrôle pour l'information et les technologies correspondantes (*Control objectives for Information and related Technology*)

COVID-19: maladie à coronavirus 2019

CSIRT: centre de réponse aux incidents de sécurité informatique (*Computer Security Incident Response Team*)

Directive SRI: directive sur la sécurité des réseaux et de l'information

EC3: Centre européen de lutte contre la cybercriminalité (Europol)

ENISA: Agence de l'Union européenne pour la cybersécurité

Europol: Agence de l'Union européenne pour la coopération des services répressifs

Fonds ESI: Fonds structurels et d'investissement européens

FSI-Police: Volet «police» du Fonds pour la sécurité intérieure

IdO: internet des objets

ISACA: association des professionnels de l'audit et du contrôle des systèmes d'information (*Information Systems Audit and Control Association*)(

ISC: institution supérieure de contrôle

MIE: mécanisme pour l'interconnexion en Europe

OTAN: Organisation du traité de l'Atlantique Nord

PIB: produit intérieur brut

PPPc: partenariat public-privé contractuel

PSDC: politique de sécurité et de défense commune

RDP: protocole de prise de contrôle à distance (*Remote Desktop Protocol*)

RGPD: règlement général sur la protection des données

SEAE: Service européen pour l'action extérieure

SRAS: syndrome respiratoire aigu sévère

SRMO: syndrome respiratoire du Moyen-Orient

TIC: technologies de l'information et des communications

UE: Union européenne

Glossaire

5G: norme technologique de cinquième génération destinée aux réseaux cellulaires à large bande, que les sociétés de téléphonie mobile ont commencé à déployer en 2019. Il est prévu qu'elle succède aux réseaux 4G, qui assurent la connectivité de la plupart des téléphones mobiles actuels. La 5G atteint une vitesse supérieure en partie grâce à l'utilisation d'ondes radio de fréquence plus élevée que celle des réseaux cellulaires précédents.

Actif numérique: tout ce qui existe dans un format numérique, est détenu par un particulier ou une entreprise, et est assorti d'un droit d'utilisation (par exemple, des images, photos, vidéos, fichiers contenant du texte, etc.).

Attaques sur l'internet: stratégies qui poussent l'utilisateur à penser que la confidentialité et la sécurité des informations personnelles sensibles qu'il divulgue sur le site internet seront assurées. Du fait d'une (attaque par) intrusion, une carte de crédit, un numéro de sécurité sociale ou des informations médicales sont susceptibles d'être rendus publics, ce qui peut avoir de graves conséquences.

Bitcoin: monnaie numérique ou virtuelle créée en 2009 qui s'appuie sur la technologie pair-à-pair pour faciliter les paiements instantanés.

Calcul à haute performance: capacité à traiter des données et à effectuer des calculs complexes à des vitesses élevées.

Cheval de Troie: type de code ou de logiciel malveillant qui semble légitime, mais qui peut prendre le contrôle d'un ordinateur. Un cheval de Troie est conçu pour endommager, perturber, voler ou, de manière générale, exercer une action dommageable sur des données ou des réseaux.

Confidentialité: protection des informations, des données et des avoirs contre tout accès non autorisé.

Contenu numérique: toute donnée (telle que texte, son, image ou vidéo) stockée dans un format numérique.

Cryptage: transformation d'informations lisibles en code indéchiffrable en vue de les protéger. Pour déchiffrer l'information, l'utilisateur doit avoir accès à une clé secrète ou à un mot de passe.

Cryptomonnaie: actif numérique qui est émis et échangé au moyen de techniques de cryptage, indépendamment de toute banque centrale. Il est accepté comme moyen de paiement parmi les membres d'une communauté virtuelle.

Cyberattaques: tentative de limiter ou de compromettre la confidentialité, l'intégrité et la disponibilité de données ou d'un système informatique via le cyberespace.

Cybercriminalité: activités criminelles diverses impliquant des ordinateurs et des systèmes informatiques, en tant qu'outils ou cibles principaux. Il peut s'agir d'infractions classiques (fraude, établissement de faux, usurpation d'identité, etc.), d'infractions liées au contenu (comme la diffusion en ligne de matériel pédopornographique ou l'incitation à la haine raciale) et d'infractions spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service, logiciel malveillant ou logiciel rançonneur).

Cyberdéfense: volet de la cybersécurité visant à défendre le cyberespace par des moyens appropriés, militaires et autres, en vue d'atteindre des objectifs militaro-stratégiques.

Cyberdiplomatie: utilisation de ressources diplomatiques et exercice de fonctions diplomatiques en vue de sécuriser les intérêts nationaux en matière de cyberespace. Elle est appliquée, en tout ou en partie, par des diplomates lors de réunions bilatérales (telles que le dialogue États-Unis-Chine) ou multilatérales (au sein des Nations unies, par exemple). Au-delà de leur mandat diplomatique traditionnel, les diplomates interagissent avec divers acteurs non étatiques, tels que des dirigeants d'entreprises de l'internet (comme Facebook ou Google), des entrepreneurs dans le secteur des technologies ou des organisations de la société civile. La diplomatie peut aussi consister à faire entendre la voix des opprimés dans d'autres pays au moyen de la technologie.

Cyberécosystème: désigne un ensemble complexe d'appareils, de données, de réseaux, de personnes, de processus et d'organisations qui interagissent, ainsi que l'environnement des processus et des technologies qui influent sur ces interactions et les rendent possibles.

Cyberespace: environnement immatériel mondial dans lequel a lieu la communication en ligne entre les personnes, les logiciels et les services, par l'intermédiaire de réseaux informatiques et de dispositifs technologiques.

Cyberespionnage: acte ou pratique consistant à obtenir des secrets et des informations sans l'autorisation ou à l'insu du propriétaire, auprès de particuliers, de concurrents, de rivaux, de groupes, de gouvernements et d'ennemis, pour en tirer un avantage personnel, économique, politique ou militaire par l'intermédiaire d'internet, de réseaux ou d'ordinateurs personnels.

Cyberincident: événement qui compromet, ou menace de compromettre, directement ou indirectement, la résilience et la sécurité d'un système informatique et celles des données que ce système sert à traiter, à stocker ou à transmettre.

Cybermenace: acte malveillant visant à endommager des données, à les voler ou à perturber la vie numérique en général.

Cyberrésilience: capacité à prévenir les cyberattaques et les cyberincidents, à s'y préparer, à y résister et à rétablir la situation.

Cybersécurité (ou cyberprotection): toutes les garanties et mesures adoptées pour défendre les systèmes informatiques et leurs données contre les accès non autorisés, les attaques et les dommages, de manière à assurer la confidentialité, l'intégrité et la disponibilité de ces dernières.

Déni de service distribué: cyberattaque qui consiste à saturer de requêtes un service ou une ressource en ligne pour empêcher ses utilisateurs légitimes d'y accéder.

Désinformation: informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public.

Disponibilité: principe consistant à garantir que les informations sont accessibles et utilisables en temps utile et de manière fiable.

Données à caractère personnel: toute information concernant une personne physique identifiable.

Données biométriques (biométrie): mesures physiologiques (comme les empreintes digitales ou oculaires) ou comportementales concernant des caractéristiques humaines. L'authentification est utilisée en sciences informatiques comme moyen d'identification et de contrôle d'accès.

Données d'accès: informations sur les connexions et les déconnexions d'un utilisateur à un service, telles que l'heure, la date et l'adresse IP.

Fournisseur de services numériques: toute personne morale qui fournit un ou plusieurs des trois types de services numériques suivants: places de marché en ligne, moteurs de recherche en ligne et services d'informatique en nuage.

Hameçonnage: pratique consistant à envoyer des courriers électroniques supposés provenir d'une source fiable afin de tromper les destinataires pour qu'ils cliquent sur des liens malveillants ou qu'ils partagent des données à caractère personnel.

Informatique en nuage: fourniture de ressources informatiques à la demande (par exemple stockage, puissance de calcul ou capacité de partage des données) sur internet, grâce à l'hébergement sur des serveurs distants.

Infrastructure critique: ressources physiques, services et installations dont l'arrêt ou la destruction aurait un impact grave sur le fonctionnement de l'économie et de la société.

Infrastructure électorale: il s'agit notamment des systèmes informatiques et des bases de données servant aux campagnes électorales, ainsi que des informations sensibles concernant les candidats, l'inscription des électeurs et les systèmes de gestion.

Installation de correctifs: introduction d'un ensemble de modifications dans un logiciel pour le mettre à jour, le réparer ou en améliorer le fonctionnement, y compris pour remédier aux failles de sécurité.

Installations de services publics: tout poteau, tour, conduit suspendu ou souterrain, toute autre structure de support ou de soutien et toute tranchée, y compris les accessoires, susceptibles d'être utilisés pour fournir ou distribuer l'électricité, le téléphone, le télégraphe, la diffusion par câble, un service de signalisation ou tout autre service similaire.

Intégrité: principe consistant à prévenir la modification ou la destruction abusives de l'information et à en garantir l'authenticité.

Intelligence artificielle: simulation de l'intelligence humaine par des machines qui sont programmées pour réfléchir comme des humains et imiter leurs actions; toute machine qui présente des caractéristiques associées à l'esprit humain, telles que l'apprentissage et la résolution de problèmes.

Internet des objets (IdO): réseau constitué d'objets de la vie quotidienne équipés de dispositifs électroniques, de logiciels et de capteurs qui leur permettent de communiquer et d'échanger des données via l'internet.

Logiciel espion: logiciel au comportement malveillant destiné à rassembler des informations sur une personne ou une organisation, puis à envoyer de telles

informations à une autre entité de manière à nuire à l'utilisateur, par exemple, en violant son droit à la vie privée ou en mettant en péril la sécurité de son appareil.

Logiciel publicitaire: logiciel malveillant qui affiche des bandeaux publicitaires ou des fenêtres contextuelles (*pop-ups*) comprenant des codes qui permettent de surveiller le comportement en ligne des victimes.

Logiciel rançonneur: logiciel malveillant qui empêche les victimes d'accéder à un système informatique ou rend les fichiers illisibles, généralement par un procédé de cryptage. La plupart du temps, l'auteur fait ensuite chanter la victime en refusant de rétablir l'accès jusqu'à ce qu'une rançon soit versée.

Maliciel: logiciel malveillant. Programme informatique conçu pour porter atteinte à un ordinateur, à un serveur ou à un réseau.

Menace hybride: acte hostile commis par des adversaires au moyen d'une combinaison de techniques de guerre conventionnelles et non conventionnelles (à savoir des méthodes militaires, politiques, économiques et techniques), dans la poursuite acharnée de leurs objectifs.

Menace persistante avancée: attaque permettant à un utilisateur non autorisé d'accéder à un système ou à un réseau et d'y rester pendant un laps de temps considérable sans être détecté. Cette menace est particulièrement dangereuse pour les entreprises, car les pirates ont un accès continu à leurs données sensibles, mais elle ne cause généralement pas de dommages aux réseaux ou aux appareils en local. L'objectif est de voler des données.

Numérisation: processus qui consiste à transformer les informations dans un format numérique, où elles sont organisées sous la forme d'octets. Cela permet de représenter un objet, une image, un son, un document ou un signal en générant une suite de nombres qui décrivent un ensemble distinct de points ou d'échantillons.

Opérateur de services essentiels: entité publique ou privée qui fournit un service essentiel au maintien d'activités sociétales et économiques critiques.

Piratage psychologique: dans le domaine de la sécurité de l'information, manipulation psychologique visant à tromper une personne pour l'amener à effectuer une action ou à divulguer des informations confidentielles.

Pirate éthique: personne (experte en sécurité informatique) qui pénètre un réseau informatique afin de mettre à l'épreuve et d'évaluer sa sécurité, sans intention malveillante ou criminelle.

Pirate: individu qui se sert d'ordinateurs, de réseaux et d'autres compétences pour obtenir un accès non autorisé à des données, des systèmes informatiques ou des réseaux.

Plateforme numérique: environnement d'interaction entre au moins deux groupes différents, l'un étant généralement constitué de fournisseurs, et l'autre, de consommateurs ou utilisateurs. Il peut s'agir du matériel ou du système d'exploitation, voire d'un navigateur internet et des interfaces de programmation des applications connexes, ou d'autres logiciels sous-jacents, à condition que le code du programme soit exécuté conjointement.

Protocole de prise de contrôle à distance (ou protocole RDP): norme technique (établie par Microsoft) permettant d'utiliser un ordinateur à distance. Ceux qui se servent de ce protocole peuvent accéder à leur ordinateur, ouvrir et modifier des fichiers et utiliser des applications comme s'ils étaient réellement assis devant leur ordinateur.

Sabotage: action délibérée visant à détruire, à endommager ou à perturber des activités, notamment en vue d'en tirer un avantage politique ou militaire.

Sécurité de l'information: ensemble des processus et outils de protection des données physiques et numériques contre tout accès, toute utilisation, toute divulgation, toute perturbation, toute altération, tout enregistrement ou toute destruction non autorisés.

Sécurité des réseaux: volet de la cybersécurité consistant à protéger les données transmises au moyen d'appareils connectés à un même réseau, afin de garantir que les informations ne sont ni interceptées ni modifiées.

Système d'information critique: tout système d'information, existant ou envisagé, qui est considéré comme essentiel au fonctionnement efficient et efficace de l'organisation.

Traitement des données: réalisation d'opérations sur des données, notamment au moyen d'un ordinateur, pour récupérer, transformer ou classer des informations.

Vectorisation de texte: procédé consistant à convertir des mots, des phrases ou des documents entiers en vecteurs numériques pouvant être utilisés par des algorithmes d'apprentissage automatique.

Ver informatique: maliciel autonome qui se réplique afin d'infecter d'autres ordinateurs. Il utilise souvent les réseaux informatiques pour se répandre et exploite les failles de sécurité de l'ordinateur cible pour y accéder.

Violation de données: divulgation, volontaire ou accidentelle, d'informations sécurisées, privées ou confidentielles dans un environnement non fiable.

Comment prendre contact avec l'Union européenne?

En personne
Dans toute l'Union européenne, des centaines de centres d'information Europe Direct sont à votre disposition. Pour connaître l'adresse du centre le plus proche, visitez la page suivante: https://europa.eu/european-union/contact_fr

Par téléphone ou courrier électronique
Europe Direct est un service qui répond à vos questions sur l'Union européenne. Vous pouvez prendre contact avec ce service:
- par téléphone:
  - via un numéro gratuit: 00 800 6 7 8 9 10 11 (certains opérateurs facturent cependant ces appels),
  - au numéro de standard suivant: +32 22999696
- par courrier électronique via la page https://europa.eu/european-union/contact_fr

Comment trouver des informations sur l'Union européenne?

En ligne
Des informations sur l'Union européenne sont disponibles, dans toutes les langues officielles de l'UE, sur le site internet Europa à l'adresse https://europa.eu/european-union/index_fr

Publications de l'Union européenne
Vous pouvez télécharger ou commander des publications gratuites et payantes à l'adresse https://publications.europa.eu/fr/publications.
Vous pouvez obtenir plusieurs exemplaires de publications gratuites en contactant Europe Direct ou votre centre d'information local (https://europa.eu/european-union/contact_fr).

Droit de l'Union européenne et documents connexes
Pour accéder aux informations juridiques de l'Union, y compris à l'ensemble du droit de l'UE depuis 1952 dans toutes les versions linguistiques officielles, consultez EUR-Lex à l'adresse suivante: https://eur-lex.europa.eu/

Données ouvertes de l'Union européenne
Le portail des données ouvertes de l'Union européenne (http://data.europa.eu/euodp/fr/home) donne accès à des ensembles de données provenant de l'UE. Les données peuvent être téléchargées et réutilisées gratuitement, à des fins commerciales ou non commerciales.

Contact Committee

Comité de contact

des institutions supérieures de contrôle de l'Union européenne