Paris, le 10/08/2021

SYSTÈME D'INFORMATION HYBRIDE ET SÉCURITÉ : UN RETOUR À LA RÉALITÉ.

NOTE BLANCHE

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Table des matières

Résumé / Abstract

La conception des architectures sécurisées des systèmes d'information a beaucoup évolué au cours des dernières décennies, suivant le rythme de besoins d'interconnexions toujours plus nombreux et de menaces toujours plus dangereuses pour la continuité d'activité des entités publiques et privées. L'article montre que, si de nouveaux concepts de défense sont apparus (*Zero Trust Network*) et peuvent parfois prétendre remplacer les modèles historiques (tel que le « modèle forteresse »), ils revisitent des principes de sécurité éprouvés (principe de moindre privilège) en les plaçant dans des contextes nouveaux (SI hybrides) et viennent compléter une défense en profondeur robuste du SI. De nouveaux moyens techniques mis à disposition de ces entités (*cloud*, automatisation des déploiements d'infrastructures, accroissement des capacités de détection, etc.) ainsi que l'évolution des exigences réglementaires en matière de cybersécurité, accompagnent cette mutation et sont la réponse à des attaques de plus en plus sophistiquées, en provenance d'un écosystème de plus en plus complexe.

The design of secured information system architectures evolved a lot over the past decades, following the ever increasing need for system interconnections and the multiplication of always more dangerous threats that are likely to wreak havoc business continuity of both public and private sectors. This article shows that, while some new security concepts emerged (*Zero Trust Network*) and sometimes claimed to replace legacy but proven security models (such as « fortress model »), they eventually revisit recognized security principles (least privilege) in new contexts (hybrid information systems) and though complement strong defence in depth concept. The new technical means offered to entities (*cloud*, infrastructure as code, improvement of security incident capabilities…), as well as new cybersecurity regulations are the community responses to more and more sophisticated IT attacks coming from an always more complex ecosystem.

Introduction

Cléopâtre — Et c'est toi, Numérobis, qui en sera l'architecte.
Numérobis — D'accord…Euh c'est moi, c'est moi qui en serai l'architecte…c'est-à, c'est-à-dire ? C'est moi qui vais architecter tout le…

Astérix et Obélix Mission Cléôpatre

Chacun se représente le métier d'architecte, concepteur d'un bâtiment ou d'un ouvrage d'art. Par analogie, l'architecte d'un système d'information (SI) doit prendre en compte toutes les contraintes d'environnement pour bâtir un SI fonctionnel et résilient, avec des coûts raisonnables d'investissement et d'entretien. Son rôle est d'agencer judicieusement les briques qui permettent de rendre *in fine* des services numériques à des utilisateurs. Pour mener à bien sa mission, il définit des exigences ou des recommandations de nature technique ou organisationnelle.

Dans un contexte de menaces grandissantes et protéiformes, l'architecte SI doit aussi intégrer des exigences de sécurité de sorte que l'architecture qu'il conçoit soit celle d'un système d'information *sécurisé*. Un de ses objectifs est de concevoir des architectures non seulement pour prévenir les intrusions mais aussi les détecter au cas où les protections mises en œuvre seraient défaillantes, compromises ou inefficaces face à un type d'attaque. Ces protections doivent couvrir aussi bien les interconnexions que les échanges internes. Sécuriser un SI ne consiste pas à poser un boîtier tout-en-un mais à identifier les risques avec les métiers et définir une stratégie pour les traiter. Pour cela, des compétences spécifiques en sécurité des systèmes d'information (SSI) sont indispensables.

Alors que des modèles historiques de sécurité ont permis de sécuriser les premiers SI dans un périmètre maîtrisé et dans un environnement numérique où les menaces étaient rares et opportunistes, cet écosystème des SI a beaucoup évolué à mesure que le numérique façonnait nos modes de travail. Ainsi de nouveaux termes occupent régulièrement l'actualité technologique (p. ex. *Zero Trust Network*, *X as a Service*), sans qu'il soit évident de discerner un changement profond, réellement structurant, d'une démarche uniquement *marketing*. Cet article vise à donner quelques clés de compréhension. Entre autres, les sujets désormais structurants de l'automatisation et de la détection sont abordés plus en détails.

Hormis pour des jeunes pousses (*start-up*) qui peuvent choisir de déployer un SI entièrement dans le *cloud*, il est aujourd'hui fréquent de rencontrer des SI composés d'une partie historique hébergée *in situ* (tout du moins dans un périmètre connu et maîtrisé) et d'une partie plus récente, externalisée dans le *cloud*. Ces SI sont qualifiés ici de *SI hybrides*.

Cet article vise *in fine* à expliquer comment appréhender une architecture de SI hybride du point de vue de sa sécurité, c'est-à-dire une architecture où les concepts de sécurité hérités des modèles historiques sont adaptés à des capacités technologiques et à des réalités contemporaines.

1
Le système d'information et sa sécurité, des modèles à l'épreuve du temps

1.1 Système d'information hybride, de quoi s'agit-il ?

Concrètement, la notion de SI hybride est un ensemble de topologies intermédiaires entre, d'une part le SI « traditionnel » où tous les moyens informatiques sont hébergés et maîtrisés directement par l'entité, et d'autre part le SI où l'hébergement et les traitements sont totalement déportés dans le *cloud* et les moyens informatiques gérés par l'entité sont très réduits (p. ex. la simple remise d'un équipement terminal aux utilisateurs).

Le choix des topologies dépend de la stratégie de l'entité, des contraintes pesant sur son écosystème et de nombreux critères dont :

- **La taille de l'entité** Seules 26 % des entreprises françaises sont des grandes entreprises [12]. Ainsi, une part très importante des entreprises (TPE, PME, ETI, etc.) sont dans l'incapacité de mettre en œuvre un SI interne en respectant les mesures d'hygiène SSI les plus élémentaires car elles n'ont tout simplement pas les moyens ou les compétences pour cela.
- **L'ancienneté de l'entité** Une entreprise qui a un historique doit souvent composer avec des systèmes vieillissants et parfois irremplaçables ; elle a forcément plus de contraintes qu'une *start-up* dont les ressources informatiques sont souvent réduites et qui peut faire des choix techniques plus novateurs.
- **Les besoins en confidentialité et en intégrité** La divulgation ou la modification d'informations (brevet, secrets de fabrication, etc.) peuvent avoir des conséquences très dommageables ; des contre-mesures doivent être anticipées dès la conception du SI.
- **Les besoins en disponibilité** Une entreprise qui développe une solution de commerce exclusivement en ligne recherchera un SI présentant un haut niveau de disponibilité.
- **L'exposition aux menaces** Les domaines d'activités stratégiques ou dont le modèle commercial implique une présence forte sur Internet seront plus exposés aux menaces.
- **Le domaine d'activité de l'entité** Certaines activités économiques, en particulier celles orientées Web vont trouver dans le *cloud* un réceptacle plus naturel que les SI traditionnels pour bénéficier de l'élasticité qu'apporte ce type de SI, en cas de montée en charge brutale par exemple.
- **Les réglementations applicables à l'entité** Dans des secteurs d'activité réglementés, l'imposition d'exigences de sécurité va conditionner l'étendue des choix en matière de SI.
- **L'organisation géographique** Certaines entités peuvent être concentrées sur un ou quelques sites alors que d'autres peuvent être réparties sur plusieurs dizaines de sites, potentiellement sur plusieurs continents.
- **Autres critères** : la stratégie de développement de l'entité, son écosystème et les interactions avec ses partenaires, des considérations d'ordres politique et stratégique (souveraineté), l'impact environnemental, la maintenabilité, etc.

Chaque entité a des objectifs qui lui sont propres et évolue dans un écosystème spécifique à son domaine d'activité. À ce titre, il semble illusoire de donner des règles universelles pour savoir sur quel SI héberger et traiter telle ou telle information. Néanmoins il est possible de dégager quelques tendances de fond qui devraient dessiner les architectures des SI de demain.

1.2 Les modèles d'architecture de sécurité historiques

> *Il n'existe pas de forteresse imprenable. Il n'y a que des attaques mal menées.*
>
> Vauban

La citation de Vauban est certes datée mais elle est révélatrice de l'utilisation de principes issus du monde militaire lors de la mise en place des premiers systèmes d'information dans les grandes entités.

Le modèle dit « forteresse », ou évoqué également sous la fine appellation de château-fort, a répondu à des besoins de sécurisation des systèmes d'information dès les années 80 et 90, lorsque les premières attaques informatiques ont commencé à voir le jour.

Ce modèle fait une double hypothèse :

- la menace est principalement externe et la défense doit se focaliser sur les interconnexions (défense dite *périmétrique*) ;
- le système d'information interne est considéré de confiance.

Ce modèle a été adapté en fonction de la taille et des besoins des entreprises, mais il répondait plutôt bien à l'écosystème informatique jusqu'à la fin du XX^{e} siècle :

- au cours des années 70-80, avec l'apparition des premiers programmes de type virus ou vers [10], la menace informatique, opportuniste, ne concernait qu'une population réduite, notamment dans un but de recherche universitaire [7, 2, 9]. La sécurité informatique a commencé à prendre un premier tournant dans les années 90 avec l'industrialisation des logiciels antivirus visant à se protéger des programmes malveillants et également avec l'apparition d'une doctrine « cyber » dans les milieux militaires [17]. Mais les attaques n'étaient que très rarement le fait de groupes organisés et les motivations des attaquants n'étaient pas toujours clairement établies. À titre d'exemple, le virus *I Love You*, apparu en 2000, est emblématique de cette période [14] ;
- les utilisateurs de l'entreprise n'avaient généralement qu'un seul moyen de se connecter au SI : le poste de travail de l'entreprise. Les postes domestiques n'étaient pas encore très répandus et il n'existait que peu de moyens de connexion à distance pour accéder au SI de l'entreprise ;
- les interconnexions du SI avec d'autres SI étaient limitées et toutes les entreprises n'avaient pas nécessairement un accès à Internet, ni même de ressources accessibles depuis Internet (p. ex. un site Web).

Ce contexte a permis au modèle de forteresse d'être efficace pendant plusieurs années. Il suffisait bien souvent de construire une barrière de protection unique, constituée dans un premier temps de pare-feux [13], puis d'équipements « intermédiaires » comme des relais de messagerie, des serveurs mandataires (*proxy*) afin d'assurer la sécurité du système d'information.

La figure 1 représente un exemple d'architecture de type forteresse.

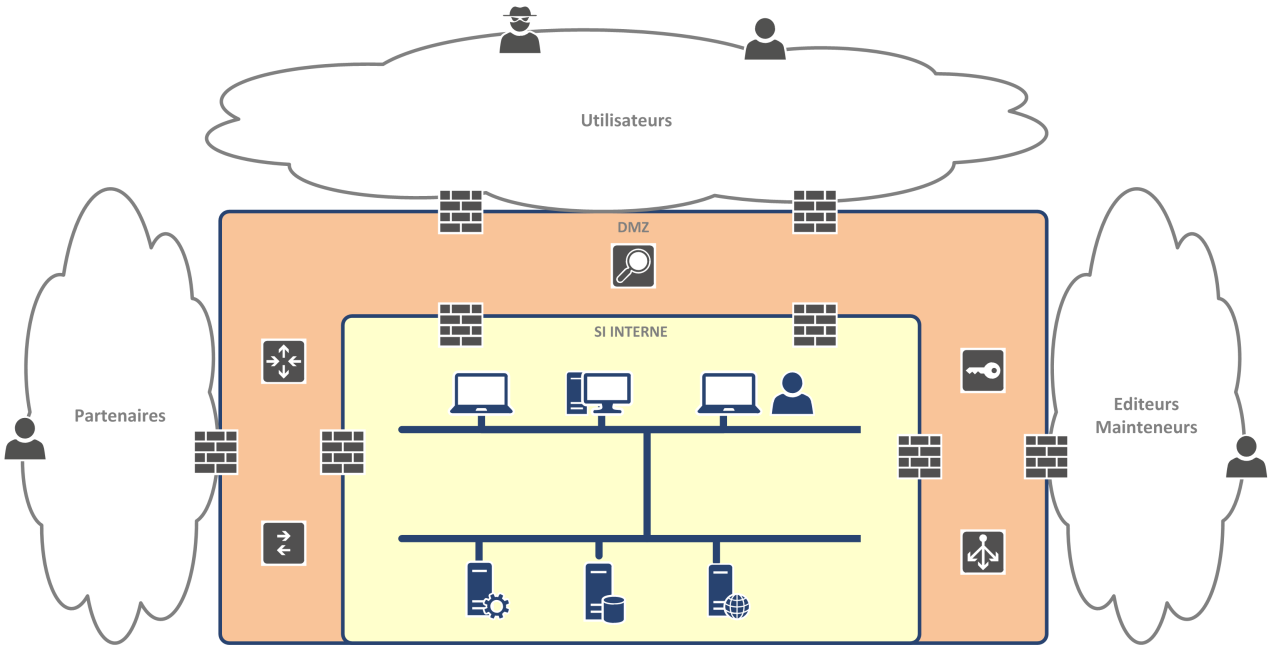

Figure 1.1 – Représentation d'un modèle d'architecture de type forteresse

Le modèle d'aéroport [20] est une évolution plus récente du modèle de forteresse. Ce modèle s'appuie également sur la défense périmétrique, mais à la différence du modèle de type forteresse, définit plusieurs périmètres appelés zones de confiance, à l'instar d'un aéroport qui dispose de plusieurs zones de sécurité et de différents niveaux de contrôle en fonction des personnes devant accéder à ces zones.

Ce modèle implique de mener une analyse fine de ce qui fait la valeur de l'entreprise et d'adapter la stratégie de sécurisation en fonction des besoins de sécurité exprimés par le métier. Les zones de confiance se définissent généralement en prenant en compte les critères suivants :

- les besoins de sécurité liées aux applications et aux données, c'est-à-dire classiquement la disponibilité, l'intégrité, la confidentialité, la traçabilité ;
- la criticité métier des applications, ou des processus métier en lien avec les applications, ce qui rejoint généralement les besoins de sécurité évoqués plus haut ;
- le niveau d'exposition des ressources (Internet, intranet, etc.) ;
- les besoins opérationnels des utilisateurs.

Une politique de sécurité est associée à chaque zone de confiance et définit les moyens de protections adaptés (sécurité physique des locaux, filtrage réseau, cloisonnement, mode d'authentification, granularité de la journalisation, supervision, etc.).

La figure 2 représente un exemple d'architecture de type aéroport.

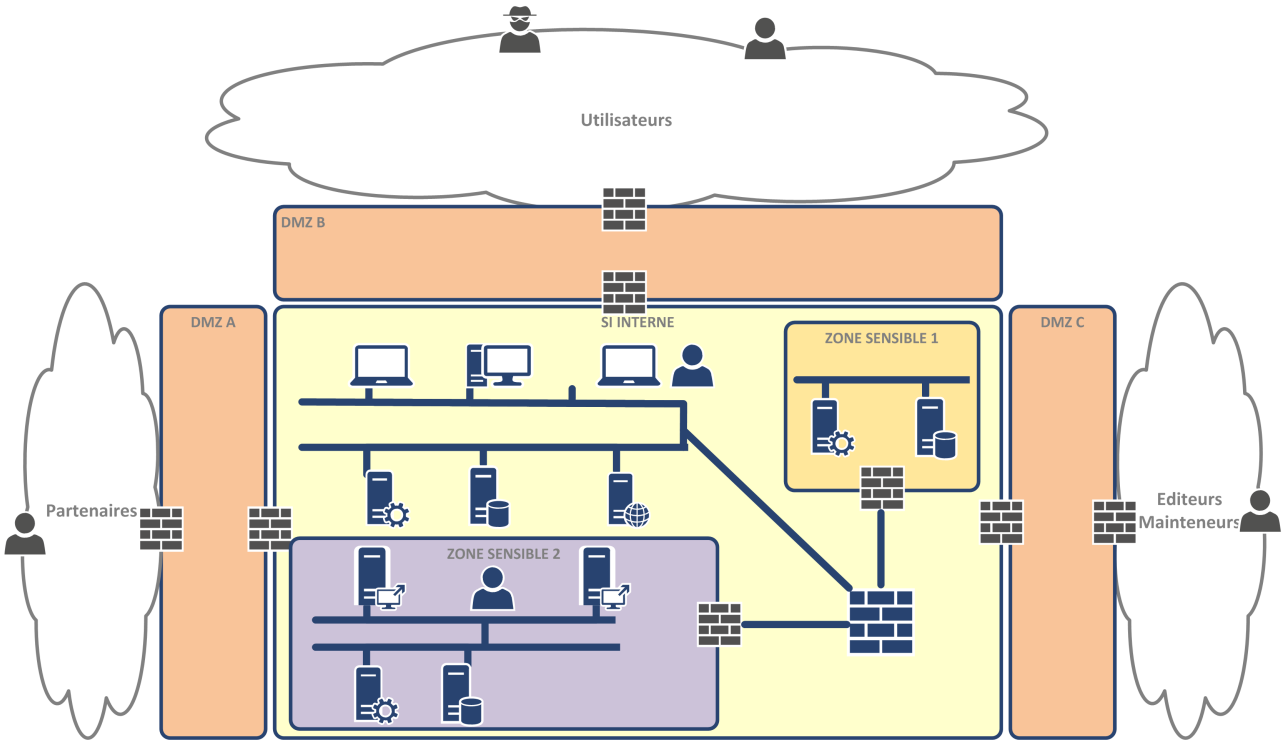

Figure 1.2 – Représentation d'un modèle d'architecture de type aéroport

Le principe de défense en profondeur [1], qui provient également de la doctrine militaire, naît de ce postulat : tout composant d'un système peut être défaillant ou compromis. Ce postulat, qui s'applique également aux fonctions de sécurité d'un SI, est confirmé régulièrement par l'actualité sur les vulnérabilités de nombreux produits et logiciels.

L'application du principe de défense en profondeur consiste à mettre en œuvre une série de mesures de sécurisation du SI :

- multiplier les fonctions de sécurité, pour limiter les conséquences de la perte de l'une d'entre elles ;
- sécuriser chaque fonction de sécurité afin qu'elle soit la plus robuste possible (réduction de la surface d'attaque, évaluation du code source, etc.) ;
- rendre indépendantes les fonctions de sécurité (diversité technologique, implémentations différentes, etc.) ;
- surveiller les fonctions de sécurité pour pouvoir détecter au plus vite une anomalie ou un dysfonctionnement.

Il peut être pertinent de prendre un exemple concret pour illustrer ce principe : une personne malveillante a la volonté de ternir la réputation d'une entreprise en s'attaquant à son site Web, ce site proposant des formulaires permettant aux utilisateurs d'envoyer des données et des fichiers. L'attaquant cherche ici à rendre le service indisponible ou bien à modifier le contenu du site Web de l'entreprise (défiguration).

La figure 3 illustre par un exemple le principe de défense en profondeur.

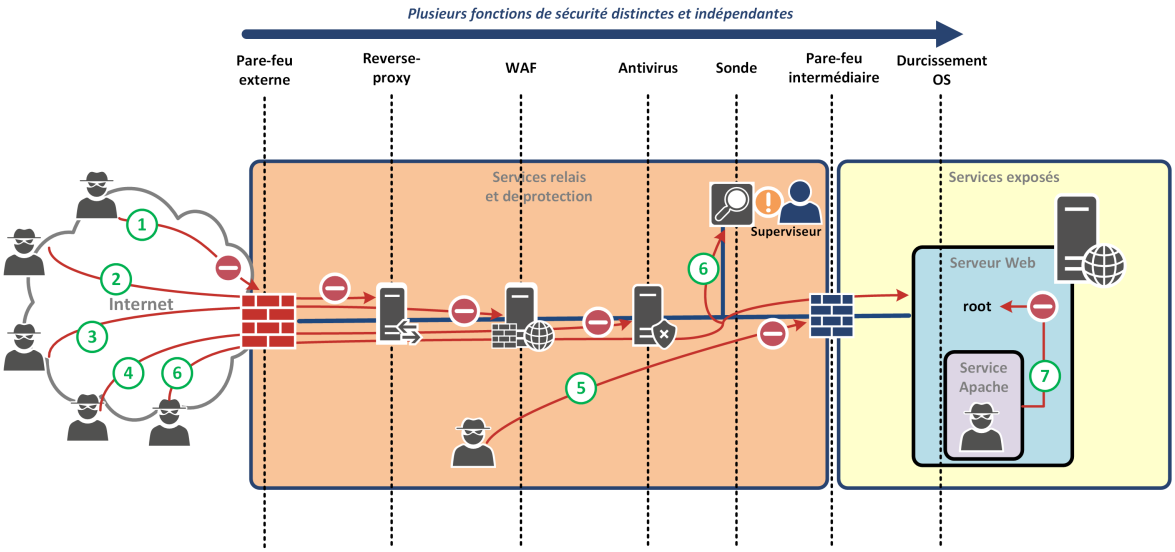

Figure 1.3 – Représentation du concept de défense en profondeur

1. l'attaquant tente une attaque en déni de service (DoS, *Denial of service*) sur le site Web de l'entreprise mais le pare-feu réseau externe bloque cette attaque en limitant le nombre de nouvelles tentatives de connexions (*rate-limit*) ;
2. l'attaquant tente d'envoyer un paquet réseau malformé afin de provoquer un dysfonctionnement dans le traitement de ce paquet. Le serveur mandataire inverse (*reverse-proxy*) n'est pas sensible à ce type d'attaque et reconstruit correctement la structure du paquet réseau avant de le transmettre au serveur Web ;
3. l'attaquant tente d'injecter du code malveillant au moyen d'un champ du formulaire du site Web (attaque XSS, *cross-site scripting*). Le pare-feu applicatif (WAF, *Web application firewall*) détecte cette tentative et bloque la requête ;
4. l'attaquant tente d'importer vers le serveur Web un fichier contenant un maliciel (*malware*). L'antivirus détecte l'empreinte du maliciel en analysant le fichier et bloque le transfert de celui-ci vers le serveur ;
5. l'attaquant a réussi à compromettre un équipement de la zone des services relais et de protection. Il tente alors d'accéder au serveur Web mais le pare-feu intermédiaire bloque ses tentatives d'accès par un filtrage strict ;
6. l'attaquant utilise un outil de test de pénétration de site Web (p. ex. *Burp Scanner*) qui va tenter d'exploiter plusieurs vulnérabilités connues. La sonde de détection réseau repère une activité anormale et reconnaît le séquencement de la suite *Burp Scanner*. La sonde envoie une alerte aux administrateurs du site Web pour qu'ils interviennent et bloquent l'attaque ;
7. l'attaquant a réussi à exploiter une vulnérabilité sur le serveur Web (p. ex. un serveur *Apache*) et il dispose d'un accès au serveur Web avec le compte de service *apache*. Le serveur Web ayant fait l'objet d'un durcissement de la configuration système (par exemple avec l'outil *SELinux*), l'attaquant se retrouve alors confiné et limité dans ses droits. Il ne réussit pas à élever ses privilèges et à devenir administrateur (*root*) du serveur. S'il peut modifier à sa guise le site Web de l'entreprise, il ne pourra pas étendre facilement son attaque à d'autres systèmes d'information, ainsi l'impact restera limité.

Pour résumer, la défense en profondeur peut se définir comme l'empilement de fonctions de sécurité de natures différentes et indépendantes entre elles, dans le but de complexifier au maximum la tâche d'un attaquant, afin que le coût de son attaque dépasse les bénéfices escomptés ou que son attaque soit détectée suffisamment tôt pour pouvoir être contrée.

On peut noter qu'il est également possible de réaliser une défense en profondeur à partir des différentes couches réseaux du modèle OSI (modèle de référence normé des communications réseaux, où chaque couche protocolaire remplit une fonction précise). Par exemple, lorsque l'on souhaite protéger une communication en confidentialité, il est possible de mettre en place un chiffrement au niveau de la couche réseau avec le protocole IPsec, ainsi qu'un second chiffrement au niveau de la couche application avec le protocole TLS. Ainsi, une vulnérabilité affectant l'un des deux protocoles n'affectera pas l'ensemble de la communication et permettra de garantir un niveau de confidentialité acceptable bien que dégradé.

Les modèles (forteresse et aéroport) et principes historiques présentent des avantages non négligeables pour sécuriser un système d'information. Ils permettent de mettre en place un socle de sécurité pour répondre à certaines menaces.

Néanmoins ces modèles peuvent également comporter des faiblesses et inconvénients. Par exemple, la confiance exagérée sur la sécurité des éléments internes dans un modèle de type forteresse peut conduire à faciliter une latéralisation des attaques lorsque l'un des éléments internes est compromis. Cette latéralisation permet ainsi à un attaquant d'« explorer » le système d'information de l'entreprise (postes de travail, serveurs) à la recherche de secrets d'authentification, dans le but d'élever ses privilèges, d'étendre la compromission, d'accéder à des données sensibles voire de se dissimuler dans le SI pour y demeurer de façon persistante.

Les nouveaux usages liés au nomadisme et au télé-travail (dont la crise sanitaire récente a accéléré la mutation) peuvent également poser des difficultés aux équipes sécurité des entreprises et créer des conflits sur certains usages comme l'utilisation d'équipements personnels (BYOD, *bring your own device*). Dans ces modèles historiques, les équipements permettant d'accéder aux données de l'entreprise sont considérés comme maîtrisés et les pratiques professionnelles cadrées. Est-ce que ces modèles sont encore valables à une époque où la plupart des développeurs d'applications préfèrent utiliser leur poste personnel ? Ou bien lorsque les collaborateurs font usage de leur *smartphone* personnel pour continuer à recevoir des messages de l'entreprise en dehors des heures ouvrées ? A l'ère de la recherche permanente de réduction des coûts, le BYOD réduit-il réellement les coûts de gestion et de sécurisation d'un SI ?

Enfin, les principes de défense en profondeur impliquent également de multiplier le nombre d'équipements de sécurité (pare-feu, sonde, proxy, etc.), ce qui peut être problématique d'une part sur le plan financier (achat du matériel et licence des produits), d'autre part en ressources humaines (formation des administrateurs, gestion opérationnelle au quotidien, dépannage, maintien en condition de sécurité, etc.).

Au final, cette situation peut entraîner un éparpillement et un certain désordre dans le SI, les acteurs étant pris en étau entre des modèles de sécurité historiques et des façons de travailler plus modernes. Dans certains cas, cela amène à une dégradation du service, non seulement pour les utilisateurs qui ne pourraient pas travailler correctement selon ces nouveaux standards, mais également pour les administrateurs qui se retrouveraient dans une situation de perte de maîtrise de leurs propres équipements de sécurité et même de façon plus globale de leur SI entier.

1.3 Nouveaux usages, nouvelles technologies, nouvelles réglementations

If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.

John von Neumann

Le phénomène de numérisation est global et touche tous les champs de l'activité humaine. Par les immenses opportunités qu'elle offre aux plans sociétal, économique voire écologique, la numérisation va encore s'accentuer dans les années à venir. D'ores et déjà ses conséquences sur les usages et la conception des architectures des SI sont perceptibles, notamment par l'ouverture des SI. Cet effacement progressif de la notion de *périmètre SI* résulte de la convergence de nouveaux modèles économiques et de nouvelles capacités technologiques.

Ainsi, des modèles commerciaux orientés services émergent. Désormais la valeur ajoutée pour une entité commerciale résulte moins de la vente d'un produit que de la commercialisation d'un service associé au produit. De même, la plateformisation de l'économie conduit les entreprises mais aussi les entités publiques à s'ouvrir toujours davantage aux écosystèmes de leurs domaines d'activité et à mettre en œuvre des *sas* d'interopérabilité à même de créer des nouveaux services et d'en tirer de la valeur. L'entreprise devient « étendue », l'État devient « l'État plateforme ».

Ces évolutions sont rendues possibles par les progrès technologiques tous azimuts de l'informatique : capacité à traiter des volumes toujours plus grands de données, démultiplication des puissances de calcul sur des équipements toujours plus compacts, accroissement des performances des réseaux (filaires et non filaires). Ainsi, avec l'avènement de la virtualisation massive des systèmes, dont le concept est poussé à son paroxysme avec l'informatique en nuage (*cloud computing*), les modèles d'architecture sécurisée présentés à la section précédente sont mis à mal : il devient de plus en plus difficile de délimiter le SI, d'identifier ce qui est *dans le SI* et ce qui est *hors du SI*.

Le *cloud* est un ensemble de technologies qui visent à mettre à disposition d'utilisateurs des ressources et services informatiques mutualisés accessibles via un réseau public ou privé. Ces architectures concentrent les capacités de calcul dans de grands centres de données (*datacenters*) et proposent des services facturables à la consommation. Elles ont la caractéristique d'être flexibles, évolutives et élastiques, c'est-à-dire de s'adapter dynamiquement aux besoins de traitement des données qui alimentent les applications. Se faisant, elles facilitent le passage à l'échelle et la résilience des services qu'elles portent.

Lorsque les technologies *cloud* sont mises à disposition du public, accessibles depuis Internet mais que leur emplacement, leur fonctionnement et leur exploitation ne sont pas connus des clients, on parle de *cloud* public. À contrario, les ressources qui constituent un *cloud* privé sont exclusivement dédiées au client voire, dans le cas le plus extrême, lui appartiennent et sont hébergées dans ses centres de données. La maîtrise du client sur le fonctionnement du nuage et des lieux de traitement et de stockage des données est donc beaucoup plus importante dans le cas d'un *cloud* privé.

L'optimisation du *traitement* de la donnée dans les *cloud* publics n'est pas sans conséquence pour la *donnée* elle-même : en externalisant le traitement des données et en cherchant à en améliorer la

disponibilité, la localisation de la donnée devient imprécise (il est difficile de savoir dans quel lieu, voire dans quels lieux, elle se trouve à un instant donné). Un corollaire pernicieux est la difficulté à déterminer le régime juridique applicable à la donnée. Et ce dernier constat interpelle d'autant plus que les fournisseurs de *cloud*, et en particulier du *cloud* public, constituent un oligopole de sociétés majoritairement étrangères et que le déplacement massif des informations dans le *cloud* concerne toutes les entités nationales, y compris celles dont les activités sont les plus sensibles.

La généralisation de l'informatique nomade est une autre cause de cette « dépérimétrisation » des SI. La crise sanitaire consécutive de la pandémie de Covid-19 force les directions d'entreprise dont les activités sont éligibles au travail à distance à reconsidérer leur rapport au télétravail. Cette évolution questionne aussi la notion de lieu de travail : celui-ci n'est plus nécessairement localisé dans une emprise physique contrôlée par l'entité (p. ex. il peut s'agir d'un télétravailleur à domicile ou d'un télétravailleur mobile en déplacement fréquent).

Le travail à distance, voire la mobilité permanente, devenant la règle générale applicable à de nombreux secteurs économiques, c'est la notion même de matériel d'accès distant qui doit être redéfinie. Par exemple, les postes de bureau dits fixes (*desktops*) sont progressivement remplacés par des postes portables. L'aboutissement extrême de cette tendance pourrait conduire à la disparition d'une multitude d'outils et de traitements sur le poste de travail, rappelant en cela un modèle historique d'architecture informatique que l'on aurait pu croire dépassé où les systèmes centraux étaient accessibles depuis des terminaux passifs. On notera que cette tendance à dématérialiser le poste de travail pourra s'avérer positive du point de vue de la sécurité des informations. Moins une information est dupliquée sur des moyens décentralisés et répartis, plus sa protection en confidentialité s'en trouve facilitée. Réduire la dissémination de l'information par la quasi suppression du poste de travail, tout en garantissant sa disponibilité et son intégrité par un stockage résilient au sein d'un centre de données, c'est agir plus efficacement pour sa sécurisation.

Ainsi, l'interconnexion généralisée des équipements terminaux à Internet devient la norme et l'absence de connectivité est synonyme d'arrêt du SI. Il ne s'agit plus seulement d'interconnecter le SI à Internet pour *surfer sur le Web* mais bien d'interagir au sein d'un écosystème aux fonctionnalités toujours plus riches et complexes (accès à des *cloud* multiples, maillage de réseaux de partenaires, etc.). Un exemple d'innovation qui démultiplie les capacités de connexion réseau tout en ayant un fort impact sur les usages est l'émergence des réseaux 5G. Sur le plan technologique, l'architecture d'un tel cœur de réseau est orientée *services* : toutes les briques applicatives d'un réseau 5G sont des fonctions virtualisées, sans état, pouvant être déployées sur des matériels de différents équipementiers. Certaines de ces fonctions peuvent être exécutées sur la même machine et voir leurs démarrages et arrêts orchestrés dynamiquement en fonction de la charge du réseau. On retrouve là l'élasticité déjà mentionnée plus haut dans le cas du *cloud*. Ces nouveaux réseaux radiomobiles deviennent, grâce à la virtualisation, polymorphes : ils ont une capacité à répondre à des besoins, et donc à des usages, très divers. Il peut s'agir de réseaux très haut débit (eMBB, *enhanced Mobile BroadBand*) proposant à des consommateurs des services de téléchargements performants. Il peut s'agir de réseaux à faible latence (URLLC, *Ultra Reliable Low Latency Communication*) pour les véhicules connectés. Il peut s'agir de réseaux à connectivité haute densité et faiblement énergétique (mMTC, *Massive Machine Type Communication*) pour les objets connectés. Ces exemples ne sont qu'un aperçu des possibilités offertes par les réseaux 5G. De nombreux autres usages ne manqueront pas d'être inventés qui seront autant de défis en matière de sécurité.

Tous ces changements de paradigmes ont pour conséquence de brouiller les domaines de responsabilité des différentes parties prenantes du SI. Jusqu'à récemment, une entité responsable d'un SI pouvait exercer un certain contrôle sur *son* SI (contrôles d'accès physiques, contrôles sur la nature des briques constitutives du SI, leur configuration et leur maintenance, contrôles sur les personnes en interaction avec le SI). Les illustrations de ces pertes de contrôle sont nombreuses : mélange des domaines personnel et professionnel, entreprises qui s'intègrent à des écosystèmes

où de nombreux acteurs collaborent sur des projets communs, etc. Le nombre d'acteurs est démultiplié et, avec lui, la complexité de garantir la sécurité de cette chaîne d'approvisionnement où chaque acteur est censé jouer un rôle dans sa sécurisation sans qu'aucun ne puisse réellement s'en assurer. La répartition des responsabilités devient plus floue et il est parfois difficile de savoir répondre à cette simple question : quelles règles de sécurité doivent s'appliquer ?

Si les nouveaux usages et les nouvelles technologies constituent des opportunités de développement, elles ont un revers : l'augmentation du niveau de la menace informatique. Ainsi, au cours de ces dernières décennies, le nombre des acteurs malveillants s'est trouvé démultiplié et leurs modes opératoires ont considérablement évolués (par l'industrialisation de leurs procédures, par la spécialisation les acteurs de la chaîne d'attaque, par l'émergence de véritables marchés d'échanges des vulnérabilités). Des motivations diverses et non exclusives de ces agents malveillants sont la cybercriminalité (avec l'augmentation des rançongiciels notamment), l'espionnage et la déstabilisation (d'entreprises privées ou d'États), l'activisme politique ou idéologique.

Dans cet univers où technologies, usages et menaces évoluent à grande vitesse, le législateur s'emploie, avec plus ou moins de succès, à élaborer un cadre juridique à même d'accompagner ces changements de fond. Ainsi, la dernière décennie écoulée a vu naître de nombreuses réglementations aux finalités diverses (développer la confiance des utilisateurs dans le numérique, accroître les capacités de protection des SI…) mais qui ont toutes eu une influence plus ou moins prégnante sur la conception des architectures des SI. Les lois fédérales étatusiennes *Clarifying Lawful Overseas Use of Data Act* (ou *CLOUD Act*) et *Foreign Intelligence Surveillance Act* (FISA) constituant deux exemples emblématiques de lois à portée extraterritoriale de nature à remettre en cause la souveraineté numérique des autres nations. À titre d'exemple, la France dispose de règles concourant au développement de la confiance dans le numérique et les règles applicables aux opérateurs publics et privés les plus critiques.

Règles concourant au développement de la confiance dans le numérique

Bien qu'applicable uniquement à l'Administration, le référentiel général de sécurité (RGS) est un ensemble de bonnes pratiques et de référentiels techniques en matière de cybersécurité qui sont transposables à des SI non étatiques. En mettant en exergue l'importance de développer un réseau de prestataires qualifiés par l'autorité nationale de cybersécurité (l'ANSSI), le RGS a ouvert la voie au développement d'un écosystème de prestataires aux compétences reconnues et dont la vocation est que leur champ d'intervention dépasse largement celui des SI de l'administration. Les prestataires de services de certification électronique (PSCE), les prestataires de détection d'incidents de sécurité (PDIS), les prestataires de réponse aux incidents de sécurité (PRIS), les prestataires d'audit de la sécurité des systèmes d'information (PASSI) sont des exemples de ces acteurs privés qui viennent démultiplier l'action des entités publiques.

Le règlement général sur la protection des données (RGPD) est le cadre réglementaire européen pour la protection des données à caractère personnel des résidents de l'Union européenne. Bien que la SSI ne soit pas au cœur des préoccupations de ce texte, il introduit néanmoins la notion de *sécurité par défaut* qui impose à tout organisme de disposer d'un système d'information ayant les fonctionnalités minimales requises en matière de sécurité tout au long de son cycle de vie.

Règles applicables aux opérateurs publics et privés les plus critiques

Ces règles contraignent certaines entités à mettre en œuvre des mesures de sécurité techniques ou organisationnelles pour prévenir et contrer les cyberattaques. Elles concernent les *opérateurs d'importance vitale* (OIV) qui gèrent les installations dont la continuité de fonctionnement est critique pour la Nation (Loi de programmation militaire de 2013), les *opérateurs de services essentiels* (OSE) et les *fournisseurs de services numériques* (FSN) qui jouent un rôle clé dans les activités

économiques et sociétales majeures (Directive européenne sur la sécurité des réseaux et de l'information, dite « directive NIS »), les entités privées ou publiques mettant en œuvre un SI *sensible* (Instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles).

Pour plus d'information concernant la réglementation relative à la cyberdéfense, il est possible de se reporter à l'annexe A.

L'espace numérique se transforme à grande vitesse. Parce qu'une partie conséquente des productions intellectuelles et économiques se trouvent désormais générées, exploitées et stockées en son sein, il devient un objet de convoitises tantôt saines et légitimes (p. ex. développement de nouveaux services et de nouveaux usages) mais, parfois aussi, malintentionnées. Ce nouveau monde devient le théâtre d'actions malveillantes toujours plus élaborées. La sécurisation d'un tel environnement, du fait de l'asymétrie entre la *facilité à attaquer* et la *difficulté à défendre*, est aujourd'hui un défi pour tous les responsables des systèmes d'information. C'est l'objet de la seconde partie de cet article de présenter des adaptations opérationnelles majeures menées sur les architectures des SI en réponse à ce défi au cours des vingt dernières années.

Information

À RETENIR

- Les modèles historiques d'architecture des SI ont été construits avec l'idée que l'entité qui les mettaient en œuvre en avait une parfaite maîtrise et que les menaces pesant sur le SI avaient une origine externe au SI.
- Cette idée est désormais dépassée du fait de l'évolution des usages, des technologies et des menaces.
  - Évolution des usages : les SI sont plus ouverts ; le recours à l'externalisation (notamment au *cloud* public) et à l'informatique nomade devient la norme et en conséquence, la notion de périmètre du SI devient floue.
  - Évolution des technologies : la protection des SI est complexe (multiplication des moyens de défense qui nécessitent un personnel hautement qualifié, généralisation du recours aux technologies de virtualisation) participe de la dépérimétrisation du SI.
  - Évolution des menaces : les attaquants se sont professionnalisés tandis que les scénarios de compromission se sont diversifiés (attaques indirectes de type *supply chain attack*) et que le SI interne n'est plus nécessairement considéré de confiance.
- En réponse à ces évolutions, une prise de conscience s'est développée au plus haut niveau des pouvoirs publiques et des entités privées qui se traduit notamment par une meilleure intégration de la dimension cyberdéfense dans l'arsenal réglementaire.

2
Adapter la défense à ces nouveaux terrains de jeu

2.1 Le cloud, levier de la sécurité by design et by default ?

> Un jour j'irai vivre en Théorie, car en Théorie tout se passe bien.
>
> Inconnu

Les concepts de *security by design* (intégration de la sécurité dès la conception d'un système) et de *security by default* (système sécurisé par défaut, sans nécessité de paramétrage complémentaire) sont désormais plus que souhaitables au regard de l'augmentation des cyberattaques, opportunistes ou ciblées, pour limiter les coûts et efforts nécessaires à la sécurisation d'un SI *a posteriori*.

Alors que le coût initial minimal de sécurisation d'un SI interne peut sembler élevé (humainement et financièrement) et donc constituer un frein pour de petites ou moyennes entités, l'offre de sécurité généralement incluse dans des infrastructures ou services de type *cloud* est un argument majeur de leur promotion. En effet, en concentrant des moyens techniques optimisés pour un usage partagé et un personnel hautement qualifié en sécurité des systèmes d'information, les fournisseurs *cloud* proposent des briques sécurisées prêtes à l'emploi qui profitent en premier lieu à leurs clients.

À titre d'exemple, un fournisseur *cloud* propose généralement un dispositif de supervision de la sécurité, permettant de remonter des alertes simples (p. ex. modifications des règles de filtrage, tentatives d'authentifications en échec). Cela représente une base intéressante pour une entité n'ayant pas le temps d'installer ses propres outils de supervision de sécurité. La capacité d'activer une authentification double-facteur pour la connexion des utilisateurs et des administrateurs est un autre exemple d'une fonctionnalité assez standard dans le *cloud*. En guise de dernier exemple, des politiques de filtrage par défaut, peuvent permettre de s'assurer qu'aucune connexion entrante vers des machines virtuelles nouvellement créées n'est autorisée une fois celles-ci démarrées dans l'environnement *cloud*. Ainsi, des services qui seraient installés et configurés au démarrage d'un serveur (SSH, partage NFS, etc.) ne pourraient pas être accessibles par défaut. Ces bonnes pratiques constituent une hygiène de base, permettant d'intégrer les bonnes pratiques de sécurité dès la conception d'un nouveau SI.

Le *cloud* offre ainsi des opportunités aux entités, quelle que soit leur taille, de sécuriser leurs informations moyennant néanmoins un minimum d'ingénierie de configuration avec un coût maîtrisé et quelques compétences spécifiques, et en restant bien conscientes que la sécurité numérique

est l'affaire de tous et non de quelques techniciens. En fonction du niveau de sensibilité des informations traitées, l'entité peut potentiellement placer la totalité de son patrimoine informationnel dans le *cloud* avec un niveau de sécurité supérieur à ce qu'elle aurait eu en créant, avec des moyens et des expertises limités, un SI interne pour héberger ce patrimoine. De plus, ces informations peuvent éventuellement être chiffrées pour leur protection en confidentialité, soit avec un service *cloud* – avec les réserves nécessaires sur le niveau de sécurité apporté par le chiffrement lorsque les clés sont hébergées dans le *cloud* – soit localement avant envoi.

Les entreprises qui ont une activité de service 100 % Web migrent aussi massivement vers le *cloud*. Le critère primordial pour elles est davantage la disponibilité. Les offres des oligopoles étasuniens (GAFAM) et, dans une moindre mesure pour l'instant, chinois (BATX) ont actuellement une longueur d'avance en la matière sur leurs homologues européens. Il est souhaitable de penser que ces derniers, portés par des politiques publiques volontaires puissent rattraper leur retard dans la décennie à venir. La maturité des offres *cloud* donnant des gages sur la sécurisation des données, l'enjeu est aujourd'hui la souveraineté des données qui y sont hébergées.

Par ailleurs, il ne faut pas oublier que des attaques spécifiques peuvent viser directement ou indirectement les services *cloud* de l'entité. Par exemple, des mécanismes de synchronisation de comptes et de fédération d'identités permettent de s'appuyer sur des ressources existantes au sein de l'entité pour s'authentifier auprès de services *cloud*. Suivant les possibilités techniques de l'entité et du fournisseur *cloud*, ces mécanismes doivent être configurés avec une grande attention. En cas d'interception de flux ou de compromission plus spécifique, c'est un accès direct au SI hébergé qui peut être obtenu ainsi par un attaquant. C'est une conséquence indésirable de la dépérimétrisation du SI.

Enfin, bien qu'il soit bénéfique de disposer de briques de sécurité prêtes à l'emploi dans le *cloud*, aussi efficientes soient elles, elles ne constituent pas à elles seules une architecture sécurisée mais y contribuent. Leur mise en œuvre peut accroître la sécurité globale du SI dans la mesure où une attention particulière est portée sur l'intégralité de leur paramétrage. Néanmoins, avec des besoins qui évoluent, parfois très régulièrement et rapidement, et une croissance de services numériques, l'automatisation sous contrôle de l'humain devient incontournable pour garantir que cette sécurité *by design* perdure dans le temps.

2.2 L'automatisation, source d'opportunités pour la sécurité

> L'automatisation : système simplifiant tellement le travail qu'on finira par avoir besoin d'un cerveau électronique pour se tourner les pouces.
>
> Noctuel

La tendance à l'automatisation, qui ne touche pas seulement la structure des systèmes d'information des entités, fait aujourd'hui partie intégrante des projets de développement d'applications, que ceux-ci s'appliquent au domaine physique (domotique, santé, villes intelligentes...), au secteur tertiaire (contrats intelligents, signatures électroniques...) ou à celui de la recherche.

Cette tendance prend plusieurs formes dans le SI : l'automatisation des déploiements d'infrastructures informatiques, l'automatisation des tests sur les applications développées, l'automatisation des procédures de contrôle et de livraison des mises à jour en production, l'automatisation de la détection d'événements, l'automatisation de la réponse à incident, etc.

L'*Infrastructure as Code* (IaC) permet de gérer plus sereinement la complexité lors d'un déploiement de ressources informatiques (serveurs, équipements réseaux, passerelles d'accès distant, configurations des outils, etc.) en rationalisant la manière de déclarer et d'instancier les ressources (via un langage comme YAML par exemple), et d'améliorer la granularité de la configuration des fonctions d'infrastructure et de sécurité (routage, règles de pare-feu, définition des sous-réseaux, gestion des comptes et des rôles, etc.).

Les outils d'automatisation IaC, qui incluent généralement un orchestrateur c'est-à-dire un ordonnanceur de tâches, permettent ainsi d'être réactifs, c'est-à-dire d'avoir une capacité à déployer et cloner un système d'information rapidement, de contrôler des écarts par rapport à des politiques de sécurité (par exemple si l'on a déclaré une règle d'ouverture de port entrant qui n'est pas habituellement autorisée), et de gérer des mises à jour d'infrastructure rapidement, voire de faire un retour arrière en urgence, puisque le déploiement de l'infrastructure est entièrement programmé à l'aide de fichiers de configuration versionnés. L'IaC peut apporter une assurance sur le paramétrage fin des ressources notamment dans les opérations de montée en charge et donne également des gages pour la réversibilité.

L'automatisation se retrouve aujourd'hui dans les technologies de SDN (*Software-defined network*) et dans les exemples bien concrets que sont le *cloud* et l'implémentation de la nouvelle norme 5G pour les réseaux mobiles [3]. Le SDN suppose la création d'une couche d'abstraction supplémentaire permettant de gérer n'importe quel matériel réseau, indifféremment de son constructeur, du modèle, du système d'exploitation qu'il exécute. L'objectif est de pouvoir automatiser par exemple une politique de routage, une politique de filtrage par la définition de modèles écrits dans un langage propre à cet usage. Chaque équipement cible applique alors les règles définies par l'orchestrateur en fonction du contexte. Il peut conserver dans un mode dégradé une autonomie et un pouvoir de décision local en cas de défaillance sur les liens réseaux et de coupure de communication avec l'orchestrateur. Ce mode de fonctionnement est particulièrement présent dans les nouveaux modèles de réseaux WAN ou MAN car ils permettent d'adapter de manière flexible les débits, les classes de services utilisées, les règles de sécurité, les types d'équipements devant être interconnectés, le mode d'authentification, etc.

Dans le même ordre d'idée, la tendance actuelle autour de la méthode DevOps a modifié la manière de fonctionner au sein des équipes IT [19]. Le DevOps vise à concilier dans des cycles courts et automatisés les étapes de développement d'une application (élaboration du code, intégration, tests) et d'administration système de l'infrastructure qui la porte (déploiement de l'application, exploitation et maintenance). C'est ainsi que se sont développées, en parallèle de cette méthode, les chaînes de déploiement et d'intégration continue (CICD, *Continuous integration and continuous deployment*) et la création de traitements automatisés permettant de tester plus rapidement les applications avant leur déploiement en production.

Si l'approche DevOps paraît séduisante à première vue, il convient de l'aborder avec un œil critique pour analyser les avantages et les inconvénients du point de vue de la sécurité informatique. L'automatisation des tests (notamment les audits statiques et dynamiques du code) et la mise en œuvre d'une chaîne CICD offrent une meilleure robustesse du code source et un cadrage plus précis des contrôles attendus. Ces contrôles doivent suivre l'évolution des applications, en particulier l'évolution des technologies utilisées (langages, *framework*) ainsi que les CVE (*Common vulnerability exposure*) correspondantes, des nouvelles fonctionnalités proposées (nouveau mode d'authentification, stockage de données personnelles, etc.) et des menaces en cours pesant sur l'entreprise (p.

ex. si une application qui était à l'origine accessible uniquement par une communauté réduite, est désormais accessible publiquement sur Internet). Tous ces facteurs influent sur les niveaux d'exigence et de granularité de ces tests, ce qui nécessite de réitérer périodiquement l'analyse de risque portant sur l'ensemble de la chaîne de développement.

Information

Une analyse de risque permet de se poser la question de ce qui fait la valeur de l'entreprise (informations, processus métier, code source, etc.), des événements redoutés sur ces valeurs, du type de menaces qui pèsent sur l'entreprise (profils d'attaquants et motivations) et *in fine* des risques à traiter sur le SI en fonction de leur impact (financier, image, dégâts humains, etc.) et de leur vraisemblance (probabilité d'occurrence).

En revanche , le DevOps peut engendrer des incompréhensions tant les définitions de rôles peuvent parfois être ambiguës entre les développeurs, les valideurs, les administrateurs, etc. En effet, pour des besoins de réactivité, de flexibilité et de rapidité de mise en place des applications développées, certains développeurs peuvent prendre la casquette d'un administrateur du SI, sans en avoir forcément la maturité ni les connaissances requises pour réaliser les opérations de manière sécurisée. Le risque est ici que le manque de segmentation des droits d'accès, mettant à mal le principe de moindre privilège, ne laisse place à une porosité sur les environnements et des dérives dangereuses dans le temps (outils de développement laissés à l'abandon et trop largement ouverts, restrictions insuffisantes sur les environnements de production, manque de rigueur dans le suivi des droits d'accès, ouverture de flux réseaux sur les pare-feu qui étaient supposées être temporaires, etc.).

Ainsi, « faire du DevOps » ne signifie pas que tout le monde a le droit de tout faire (développer, gérer des serveurs, administrer le réseau). Dans un environnement *cloud*, la facilité de déploiement d'outils, de machines virtuelles et de conteneurs, laisse penser à tort que toute personne un tant soit peu formée aux technologies *cloud* est en mesure de gérer de manière sécurisée un SI de production.

De manière générale, l'automatisation doit être vue comme un complément au travail d'analyse effectué par les personnes en charge de la sécurité du SI. Elle apporte donc réellement un gain de temps significatif sur les actions et contrôles élémentaires, et permet de détecter et d'éliminer la majorité des vulnérabilités standards (élément d'infrastructure ne respectant pas les règles SSI définies par l'entreprise, mauvaises pratiques d'écriture de code, usage de fonctions dangereuses non recommandées, etc.). Mais l'automatisation ne doit pas masquer le travail de réflexion et d'investigation nécessaire par les acteurs de la sécurité sur les conséquences possibles d'attaques plus sophistiquées, et les moyens techniques à mettre en place pour s'en prémunir.

2.3 La détection, fonction de sécurité indispensable d'un SI sécurisé

> Une armée sans agents secrets est un homme sans yeux ni oreilles.
>
> L'Art de la guerre, Sun Tzu

Une des fonctions de sécurité désormais primordiales au sein d'un SI, pour laquelle l'automatisation joue un rôle de plus en plus prépondérant, est la détection d'incidents de sécurité. Cette fonction vise à repérer des activités anormales ou suspectes, signes précurseurs de tentatives de compromission. Il s'agit de contrer des menaces provenant de l'extérieur, mais aussi de l'intérieur. La capacité de détection repose donc sur une toile judicieusement tendue, opérant à plusieurs niveaux dans le SI :

- détection au sein du réseau interne du SI (p. ex. avec des sondes réseau);
- détection sur tous les dispositifs nomades (postes de travail, tablettes, etc.) ou ayant une exposition externe au SI (serveurs d'applications, passerelles Internet, passerelles SMTP, passerelles ToIP, etc.);
- détection sur tous les dispositifs sur lesquels il est possible de connecter des supports de données externes (clé USB, disques amovibles, etc.);
- etc.

Cette toile permet de capturer des événements de sécurité, système et applicatifs qui seront ensuite concentrés dans une enclave de collecte dédiée du SI où des traitements spécifiques seront appliqués dans le but de déceler de potentielles activités suspectes. Ainsi la fonction de détection recouvre également les aspects de collecte de quantités d'événements de plus en plus nombreux, de traitements automatisés à l'aide d'outils spécifiques et d'analyses de ces traitements par des opérateurs spécialisés.

Aucun SI n'est à l'abri de tentatives de compromission. L'automatisation de certaines attaques touche potentiellement tous les SI dont le niveau de sécurité est faible. Il est même réaliste de penser qu'un attaquant motivé et disposant de gros moyens trouvera toujours une faille qu'il arrivera à exploiter. Dès lors, au regard des conséquences souvent désastreuses de ces compromissions, la détection se présente comme un élément majeur pour se prémunir contre les velléités néfastes d'acteurs malveillants.

La détection d'incidents de sécurité doit répondre aux défis liés à l'ouverture croissante des SI sur Internet, et aux interconnexions toujours plus nombreuses avec d'autres SI aux niveaux de maturité SSI souvent hétérogènes. La détection doit également prendre en compte la tendance visant à généraliser l'usage de protocoles chiffrés, potentiellement de « bout-en-bout », ce qui amoindrit grandement l'efficacité des sondes réseau et conduit à un déplacement des sources d'événements exploitables, du réseau vers les systèmes.

Un autre défi, et non des moindres, consiste à adapter les capacités de détection lorsque les données et les traitements associés sont hébergés dans le *cloud*. Dans ce cas, les éléments supervisés sont directement dépendants de la matrice de responsabilités entre le fournisseur et le bénéficiaire. Ainsi, un fournisseur de *cloud* proposant des services SaaS gère tous les événements liés au matériel, au réseau interne, et aux systèmes d'exploitation. Par contre, le bénéficiaire pourra superviser les événements applicatifs, les événements liés à l'authentification et aux habilitations, etc. Certaines parties du *cloud* constitueront donc une zone d'ombre pour le bénéficiaire.

Au-delà de cet aspect, une autre difficulté majeure dans une infrastructure de type hybride réside dans la corrélation des événements issus du SI interne (*on-premise*) avec ceux issus du *cloud*. Conscients de cette difficulté, la plupart des fournisseurs de *cloud* proposent des outils permettant d'agréger et de corréler les événements issus des deux environnements, même s'il est possible d'effectuer ces traitements sur une infrastructure interne à l'aide d'outils tiers. Ces évolutions proposées par les fournisseurs de *cloud* peuvent tout à la fois être perçues comme une opportunité et comme une source de complexité. D'une part, en mutualisant les capacités de supervision SSI, les acteurs du *cloud* optimisent les services de détection proposés à leur clients. D'autre part, les entités qui ne sont pas 100 % *cloud* doivent continuer à gérer un SI placé sous leur maîtrise directe.

Enfin, la menace qui pèse sur les SI a considérablement évolué ces dernières années, due notamment à un nombre croissant d'acteurs malveillants aux profils et motivations assez diversifiés. Ces acteurs disposent aujourd'hui d'une panoplie d'outils très riches, accessibles au plus grand nombre (*exploit-db*) ou aux plus initiés via les *black markets*. Ce marché très lucratif s'est fortement structuré au fil des années. Les domaines d'expertise y sont variés, ce qui a considérablement enrichi la qualité des outils proposés. Désormais, nul besoin d'être un expert en développement système pour se lancer dans des actions malveillantes, il suffit d'acquérir quelques outils sur ce marché pour tenter de s'introduire dans les SI et parvenir à ses fins. Citons à titre d'exemple les MaaS (*malware as a service*), espace qui permet la vente voire la location de *malwares* sur une durée limitée dans le temps. Les outils proposés couvrent tous les domaines, de l'hameçonnage en passant par la charge utile jusqu'aux serveurs de commande et de contrôle (C2). On notera que ces outils sont soit illégaux soit à double usage (utilisables à des fins d'audit pour des acteurs bienveillants ou à des fins d'attaque pour des acteurs malveillants).

Information

Les *black markets*
Transposé au monde numérique, un *black market* représente une zone de mise en relation permettant aux hackers du monde entier de vendre ou acheter des *exploits* ou des outils permettant de réaliser des attaques. Ces échanges majoritairement illégaux entre acteurs se font généralement au travers d'un *darknet*, c'est-à-dire un réseau « parallèle » à Internet pourvu de fonctions d'anonymisation et dans lequel toutes les ressources ne sont pas nécessairement indexées par les moteurs de recherche.

Toutes ces évolutions (menace, technologie) ont conduit à une remise en cause de l'approche sur la mise en œuvre de capacités de détection, à commencer par l'organisation humaine. Ainsi, beaucoup d'entités ont mis en place une équipe chargée d'analyser et d'intervenir en cas d'incident de sécurité : un SOC (*security operation center*).

Le travail des SOC a longtemps été l'apanage des agences gouvernementales et du secteur de la défense, et se réduisait à contrer des codes malveillants ou des attaques en déni de service. Durant la première décennie des années 2000, les attaquants ont progressivement fait évoluer leurs stratégies en commençant notamment à expérimenter des attaques inscrites dans la durée, persistantes. C'est l'émergence des « APT » (*advanced persistent threat*) [6]. Face à ces nouvelles

menaces, la technologie clé pour la détection était le SIEM (*security information and event management*), permettant de générer des alertes à partir de scénarios pré-définis correspondants à des attaques opportunistes ou ciblées. Puis, au début des années 2010, les professionnels de la sécurité ont réussi à ajouter des sources de renseignement externes (*threat intelligence*) et des analyses heuristiques au SIEM pour améliorer la qualité de la détection.

Plus récemment, avec le phénomène de numérisation généralisée et l'émergence de technologies disruptives (p. ex. IoT, *Internet of Things*), la surface d'attaque et les volumes de données à collecter se sont trouvées démultipliées. Les attaquants utilisent désormais des technologies adaptées pour une furtivité accrue, s'immiscer dans les SI et tirer avantage de l'exploitation des vulnérabilités des systèmes et des flux informatiques pour voler de l'information. Une des conséquences pour la détection est la nécessité d'une surveillance continue.

Il est désormais communément admis par les ingénieurs sécurité que les techniques de défense réactives ne pourront probablement pas aider à protéger les SI et réduire les conséquences d'une attaque. Trop de promesses ont été faites sur ce sujet, sans jamais avoir pu convaincre de leur efficacité. Plus sûrement, c'est l'analyse prédictive qui est susceptible de produire les résultats les plus prometteurs. S'appuyant toujours sur la pierre angulaire qu'est le SIEM, les nouveaux outils de détection intègrent désormais des capacités automatisées d'apprentissage (*machine learning*), seule solution en capacité de répondre au défi de l'élaboration de règles de détection pertinentes au regard de volumes de données gigantesques. Cette technologie permet de faire cohabiter les règles et les algorithmes de détection aux analyses statistiques pour accroître la capacité de détecter des anomalies ou des comportements inhabituels, révélateurs possibles d'une compromission, voire dans les meilleurs cas de pouvoir les prédire. Ainsi, une forme primitive d'IA (intelligence artificielle) se trouve désormais au sein des plateformes de réponse à incidents (SOAR, *security orchestration and automation response* ou SIRP, *security incident response platform*).

L'efficacité de ces technologies émergentes reste à démontrer. Les outils des attaquants s'adaptent sans cesse aux nouvelles solutions censées détecter leurs agissements. L'IA va aussi être incorporée à ces outils ce qui les rendra encore plus difficilement détectables. La structuration des entités, couplée à l'utilisation d'outils de détection intégrant les dernières technologies permettra d'accroître leurs capacités de détection et de réponse, limitant ainsi les risques de compromission.

2.4 Modèle Zero Trust Network, tendance ou graal de la sécurité ?

Le concept de *Zero Trust Network* a émergé il y a déjà une dizaine d'années outre-Atlantique. Visé par une attaque informatique avancée en 2009, Google a été un des premiers contributeurs à passer de la théorie à la pratique sur son propre SI avec le projet *BeyondCorp* [11]. Puis le concept s'est diffusé lors de conférences [5] et un livre de référence [4] a été publié en 2017. Le *Zero Trust Network* est avant tout un concept d'architecture et non une technologie ; il n'existe donc pas de produit ou de composant spécifiquement normalisé. Porteur de nombreux espoirs pour la gestion du nomadisme par les équipes informatiques, particulièrement sollicitées sur ce sujet lors de la crise Covid-19, ce concept apporte en effet des éléments de réponse à des difficultés opérationnelles émergentes : limite de capacité des infrastructures de nomadisme, forte exposition pour les applications hébergées dans le *cloud*. Toutefois il convient de ne pas réduire la résolution de ces difficultés à une solution et de garder à l'esprit le niveau de menaces. Certaines solutions préexistantes éprouvées restent parfois incontournables tandis que l'hygiène informatique demeure le b.a-ba de la sécurité.

Comme évoqué précédemment, le SI d'une entité n'a plus de limites pérennes du fait de l'externalisation d'applications dans le *cloud* et de la massification des utilisateurs nomades. Les ressources (clients et services) sont réparties de part et d'autre de la ligne de défense périmétrique de l'historique zone de confiance, les locaux de l'entité (modèle de forteresse). Par ailleurs, la généralisation

des attaques par latéralisation (c.-à-d. par rebond d'une ressource à une autre en profitant de mesures de sécurité inexistantes ou affaiblies) rend caduque la confiance implicite accordée au périmètre dit interne.

Alors que dans un modèle périmétrique, un tunnel VPN permet de prolonger le réseau de l'entité sur le poste d'un utilisateur nomade, le *Zero Trust Network* déporte la gestion de la sécurité sur la couche applicative. Chaque accès est donné par application, autorisé sur la base d'une identité réputée fiable de l'utilisateur, de son poste et potentiellement de paramètres exogènes (l'heure de connexion, la localisation géographique par exemple). Cette granularité permet l'application stricte du principe de moindre privilège. De plus, les accès sont dynamiques et donc autorisés juste le temps nécessaire (principe du « *just in time* ») contrairement aux règles de filtrage statiques d'un pare-feu. Par exemple, cela peut se traduire par une session privilégiée limitée en temps ou un certificat d'authentification de courte durée.

Concrètement, un point de passage obligé gère l'authentification de l'utilisateur, de son poste et applique les décisions d'autorisation, comme une sorte de super serveur mandataire inverse (*reverse proxy*). Cela permet entre autres de ne pas exposer les applications directement sur Internet. Comme tout point de centralisation, il faut veiller à ce qu'il ne devienne pas un point de défaillance unique (SPOF, *single point of failure*). C'est pour cela que les solutions du marché, majoritairement proposées en mode SaaS, prévoient plusieurs points de présence.

En complément, le modèle théorique de *Zero Trust Network* [4] introduit la notion de *score de confiance* (aujourd'hui peu reprise par les produits du marché). Cela permet d'associer à chaque requête (un utilisateur, un poste, une adresse IP source, un service destinataire) une variable discrète sur laquelle va reposer la décision d'autorisation, cette variable étant calculée sur la base d'indicateurs ou de journaux d'activité passée. Par exemple, un utilisateur se connectant à une heure habituelle depuis une localisation habituelle pourra être autorisé à accéder à sa messagerie. Le score de confiance de ce même utilisateur sera abaissé dans le cas d'une connexion depuis un pays étranger ; l'accès à la messagerie ne sera alors pas autorisé. Dans ce cas, une authentification complémentaire lui sera demandé pour rehausser le score de confiance et ainsi autoriser l'accès à la messagerie. Pour traiter ces données (potentiellement massives) et calculer ces scores de façon dynamique, le recours à l'automatisation est indispensable.

Par ailleurs, afin de protéger les communications à travers des réseaux qui ne sont pas de confiance par défaut (aussi bien Internet que le réseau local de l'entité dans le modèle *Zero Trust Network*), tous les flux doivent être chiffrés et authentifiés. Dans un contexte d'applications Web, le recours à TLS (donc à HTTPS) est assez simple et est d'ailleurs bien supporté par les solutions du marché. Les limites sont vite atteintes dès lors que des applications « historiques », ne supportent pas ce protocole. Par ailleurs, si cela constitue un allègement protocolaire certain par rapport au tunnel VPN avec un niveau de sécurité satisfaisant (dans la mesure où TLS est configuré à l'état de l'art), cela n'enlève en rien la pertinence d'un tunnel VPN non contournable pour les usages les plus sensibles (p. ex. l'administration de SI). Dans ce cas précis, le tunnel doit aboutir sur une zone de confiance restreinte du SI, pour garantir que tous les flux applicatifs soient protégés et ce, quel que soit le réseau sur lequel ils sont transportés. Le risque d'une attaque de type homme-du-milieu est considérablement réduit par rapport à l'utilisation seule d'HTTPS. En effet, les postes de travail et les navigateurs Web disposent par défaut d'une liste conséquente d'autorités de certification de confiance, contrairement à un client VPN IPsec censé faire confiance à un nombre très limité d'autorités de confiance configurées spécifiquement.

Dans une architecture *Zero Trust Network*, dès lors que la confiance ne repose plus sur le réseau mais sur l'identité de l'utilisateur et de son poste, une gestion stricte du parc des équipements et des identités ainsi que le recours à une authentification multi-facteurs à l'état de l'art sont des pré-requis indispensables. Par ailleurs, la bonne connaissance des applications du SI et de leurs

besoins de sécurité (cartographie) est nécessaire pour établir une politique de sécurité granulaire et efficiente.

Beaucoup de solutions du marché surfent sur la vague du *Zero Trust Network*. Elles restent très inégales dans les fonctionnalités proposées, allant du simple portail Web mettant en œuvre une authentification double facteur jusqu'à des fonctions plus avancées assurant la vérification de l'authentification du poste et l'analyse des journaux d'événements de sécurité.

Si le marché du *Zero Trust Network* est encore émergent, il convient d'être suffisamment critique sur sa mise en œuvre : cela permet de sécuriser des segments non traités ou difficilement traités dans des SI traditionnels (l'accès à des applications SaaS directement exposées sur Internet par exemple) mais ne doit pas se substituer systématiquement au tunnel VPN (pour l'accès nomade des administrateurs au SI de l'entité par exemple). Enfin, il convient de rester lucide : le ZTN permet d'atténuer les risques induits par l'utilisation d'équipements non maîtrisés (le BYOD typiquement) mais n'offre pas aujourd'hui des garanties suffisantes contre des attaques ciblées.

Information

À RETENIR

- Le *cloud* public est une opportunité pour déployer un SI sécurisé mais n'est pas une panacée, avec des risques spécifiques liés à l'augmentation de l'exposition du SI ou à la réversibilité par exemple.
- L'automatisation est un levier formidable de simplification pour les SI mais aussi pour leur sécurité avec des capacités renforcées de tests et de déploiement rapide de politiques de sécurité.
- La détection de sécurité est devenu un enjeu majeur des SI dans la mesure où le cumul des défenses n'est jamais une garantie de leur inviolabilité. Avec la croissance des volumes de journaux, l'automatisation de l'analyse est, là encore, un gain d'efficience.
- Le modèle *Zero Trust Network* offre une réponse aux tendances franches d'externalisation et de nomadisme mais ne doit pas être vu comme une solution surétagère. Il peut être opportunément déployé sur des périmètres bien identifiés du SI moyennant des référentiels sains pour les identités et les équipements.

3
Conclusion - Concilier les modèles historiques et émergents : une nécessité à l'épreuve du terrain

Au cours des vingt dernières années, les architectures de SI ont évolué depuis des modèles dits « historiques » où l'information était hébergée en interne et où le responsable du SI avait la capacité à contrôler qui pouvait y accéder et était le seul responsable de cette protection, vers un modèle plus ouvert, dit « hybride » où l'information est tantôt en interne et tantôt dans un *cloud*, voire dans des *clouds*. Dans ce nouveau modèle, la localisation de la donnée devient imprécise (quand elle n'est pas complètement inconnue) et sa protection n'est plus l'affaire d'un seul acteur mais devient une responsabilité partagée entre le responsable du SI et les fournisseurs *cloud*.

Les modèles de sécurisation d'un SI ont évolué en même temps que leurs modèles d'architecture, en apportant de nouveaux avantages plutôt qu'en se substituant à ceux existants. À cet égard, le concept de *Zero Trust Network*, qui répond à de nouveaux besoins de sécurité, n'éclipse pas les bénéfices d'une protection périmétrique efficace même si ce périmètre n'est plus physique et restreint aux frontières de l'entreprise.

Pour comprendre les bénéfices d'une stratégie de sécurisation d'un SI, il est utile de contextualiser sa genèse. La doctrine de défense périmétrique est intimement liée à la création des réseaux IP privés, avec la standardisation des adresses IP privées en 1994 dans la RFC 1597. À la fin du XX^{e} siècle, les principaux besoins d'interconnexion à Internet d'une entité étaient d'offrir un site Web vitrine, et de permettre les échanges de courriers électroniques. Ce faible niveau d'exposition, combiné à la faible sophistication des attaques de cette époque, rendait l'approche de défense périmétrique adaptée au regard du risque.

Depuis le début du XXI^{e} siècle, la numérisation des valeurs métier des entreprises entraîne une complexification des SI et une augmentation des interconnexions au point de rendre insuffisante l'utilisation seule d'un filtrage périmétrique comme mesure de protection. Ainsi, d'autres défenses doivent être érigées à l'intérieur du système d'information, en créant de nouveaux périmètres internes. Le niveau de protection est alors proportionnel à la granularité de ces périmètres et à la pertinence du filtrage et du contrôle d'accès qui leurs sont associés. Le modèle de l'aéroport cité à la section 1.2 est un exemple de stratégie de défense périmétrique mettant en œuvre plusieurs périmètres. Cette stratégie s'applique aux SI dont les interconnexions sont clairement identifiées et maîtrisées et suppose que le périmètre interne du SI n'est pas un vecteur d'attaques (périmètre de confiance).

En parallèle, le développement du nomadisme ou de pratiques de type BYOD réduit le niveau de confiance des équipements connectés du système d'information. En effet, un équipement personnel n'offre pas les mêmes garanties d'innocuité qu'un poste maîtrisé par l'organisation.

Il n'est pas anodin que le modèle *Zero Trust Network* ait été développé, en premier lieu, par des fournisseurs *cloud*. En effet, un fournisseur *cloud* ne maîtrise pas les équipements qui se connectent à son infrastructure, ces derniers étant la propriété de ses clients. Or, le fournisseur *cloud* héberge sur des mêmes ressources physiques, des informations, des traitements et des logiciels appartenant à des entités différentes, et dont le cloisonnement et la disponibilité sont essentiels. À cet effet, les technologies d'automatisation, décrites à la section 2.2, permettent de faciliter le déploiement massif de solutions de filtrage et de détection. Ces capacités de déploiement offrent

un contrôle des accès extrêmement granulaire et dynamique. C'est le fondement du modèle *Zero Trust Network*, dont la performance en matière de sécurité est directement liée à la pertinence et la finesse des règles de gestion des droits du système d'information. Cependant, le positionnement des solutions de filtrage et de détection reste tributaire d'un découpage judicieux du système d'information en périmètres de sécurité, que ces derniers soient des sous-réseaux ou des groupes d'applicatifs.

L'écosystème des SI évolue continuellement au regard des usages, des technologies et des menaces. Il semble acquis que les usages vont encore évoluer fortement dans les années à venir et que, même si faire des prédictions en la matière s'avère hasardeux, il y a fort à parier que ces évolutions entraîneront toujours plus d'ouverture et d'interconnexion de systèmes. De même ; les menaces vont continuer à s'accroître et à se complexifier. Si de trop nombreux SI restent aujourd'hui insuffisamment protégés et constituent des cibles faciles pour les attaquants, la prise de conscience des enjeux liés à la cybersécurité va accroître la maturité des « cyber-défenseurs » conduisant *in fine* à une augmentation du niveau de protection des SI. Toutefois, même dans un scénario optimiste d'augmentation de ce savoir-faire, la complexification et la furtivité des attaques justifieront une augmentation conséquente des capacités de détection et de réponse. La part prise par les capacités d'auto-apprentissage des systèmes (*machine learning*) sera dimensionnante pour la démultiplication de ces capacités.

S'agissant des technologies pouvant faciliter la cohabitation entre les modèles d'architecture « historiques » et « hybrides », le *confidential computing* semble un bon exemple. Si des solutions de chiffrement permettent aujourd'hui de répondre efficacement aux problématiques de sécurisation des données stockées (*data at rest*) et des données en transit (*data in transit*) du *cloud*, il en va différemment de la « donnée exécutée ». Le *confidential computing* est une approche novatrice où les actions de chiffrement et de déchiffrement des données sont réalisées au plus près du processeur (au moment du *fetch* des instructions dans les registres du processeur) à l'aide de clés éphémères générées par du matériel, au sein du processeur. La promesse est de rendre inaccessible la mémoire d'une machine virtuelle aux autres machines virtuelles et à l'hyperviseur qui les hébergent. En agissant au niveau des « couches basses », au plus près du matériel, cette technologie présente en outre l'intérêt d'être non-adhérente aux applications qui n'ont donc pas besoin d'être adaptées pour bénéficier de cette protection supplémentaire. En conséquence, même le fournisseur *cloud* serait dans l'incapacité d'accéder à la donnée quel que soit son état (stockée, en transit ou exécutée). Le principe de précaution est plus que jamais applicable à ce genre de nouveautés, trop récentes pour avoir démontré leur complète efficacité et qui posent l'éternelle question du niveau de confiance placée dans l'implémentation de technologies complexes et difficiles à évaluer (doute qui laisse penser que les « SI traditionnels » trouveront encore leur place dans les écosystèmes informatiques sensibles de demain).

Ainsi, les nouvelles approches de la sécurisation d'un système d'information, rendues possibles par le développement des technologies de segmentation, d'automatisation, d'apprentissage et de détection permettent de renforcer toujours plus l'application d'un principe aussi vieux que la sécurité de l'information, celui du moindre privilège.

Annexe A
Considérations relatives à la réglementation en matière de cybersécurité

Cette annexe rappelle quels sont les périmètres et les principaux objectifs des réglementations relatives à la cybersécurité votées au cours de la décennie écoulée. Tous ces textes ont des conséquences concrètes sur les architectures des SI.

Citons tout d'abord les *Lois de programmation militaires* ou LPM. S'appuyant sur les orientations stratégiques contenues dans le *Livre blanc sur la Défense et la Sécurité nationale 2013* [8], la LPM 2014-2019 [15] précise les règles de sécurité imposées aux Opérateurs d'importance vitale (OIV) qui opèrent des SI d'importance vitale (SIIV). Ces règles concernent différents champs de la SSI et nombreuses sont celles qui ont un impact direct sur la conception de l'architecture d'un SIIV (règles relatives à la journalisation, à la corrélation et à l'analyse des journaux, à la détection, à l'identification, à l'authentification, aux droits d'accès, au SI d'administration, au cloisonnement, au filtrage ou aux accès distants). En outre, un OIV a l'obligation de mettre en œuvre un système de détection exploité sur le territoire national par des prestataires de service qualifiés en matière de SSI par l'ANSSI (Article 22 de la loi n° 2013-1168 du 18 décembre 2013 [15]). La section 2.3 de cet article souligne l'importance de la détection des incidents de sécurité dans les systèmes d'information contemporains.

Information

La notion d'OIV est introduite dans le dispositif relatif à la Sécurité des activités d'importance vitale (SAIV) dont la cybersécurité ne constitue qu'un sous-ensemble. La définition d'un OIV est donnée à l'article L1332-1 du code de défense : *Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.*

S'appuyant cette fois sur les orientations données par la *Revue stratégique de cyberdéfense* [18], la LPM 2019-2024 [16] va venir renforcer les capacités d'intervention de l'État pour la détection des incidents de sécurité pesant sur les OIV et sur les opérateurs de communications électroniques. N'ayant que peu d'impacts architecturaux, nous ne nous étendrons pas sur la portée de cette loi.

Un deuxième exemple de réglementation influençant la conception des architectures des SI est le Référentiel général de sécurité (RGS) (dont la version en vigueur est dite « RGS version 2.0) a été publiée par arrêté du Premier ministre du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. ». S'inscrivant dans la démarche de l'État de faciliter l'accès des citoyens à des services publics de plus en plus dématérialisés, il a pour objet le renforcement de la confiance de ces derniers dans les SI mis à leur disposition par les autorités administratives. Bien que ce texte ne soit applicable qu'à l'Administration, sa place dans cette énumération est toutefois justifiée

pour au moins deux raisons. Tout d'abord, il formule un ensemble de bonnes pratiques et de référentiels techniques en matière de cybersécurité qui sont transposables à des SI non étatiques (les annexes B du référentiel donnent en particulier des règles et des recommandations dans le domaine cryptographique). Par ailleurs, en mettant en exergue l'importance de développer un réseau de prestataires qualifiés, le RGS a ouvert la voie au développement d'un écosystème de prestataires aux compétences reconnues et dont la vocation est que leur champ d'intervention dépasse largement celui des SI l'administration. Or, recourir à de tels prestataires influence la manière de concevoir le SI, certains référentiels imposant des exigences d'architecture sur les interconnexions entre le SI du prestataire et le SI du client. C'est par exemple le cas du référentiel PDIS qui s'applique aux prestataires de détection des incidents de sécurité et ce sera le cas avec le futur référentiel des prestataires d'administration et de maintenance sécurisées (PAMS).

Un troisième exemple concerne les textes qui ont vocation à donner un cadre juridique à la protection en confidentialité des informations. Il est ici fait référence à l'instruction interministérielle n° 901 (II 901) relative à la protection des systèmes d'information sensibles et à la nouvelle édition de l'instruction générale interministérielle n° 1300 (IGI 1300) relative à la protection du secret de la défense nationale dont la réforme, initiée fin 2017 sera pleinement applicable au 1er juillet 2021 après une période d'appropriation d'un an. Dans ces deux textes, sont posés les grands principes régissant les interconnexions de SI hébergeant des informations d'un niveau de sensibilité donné avec des SI hébergeant d'autres informations de niveau moindre ou supérieur. Ainsi, sous réserve de satisfaire des mesures de sécurité techniques et organisationnelles précise, l'II 901 prévoit des architectures de SI permettant d'assurer la protection d'informations Diffusion Restreinte (DR) quand bien même ces derniers sont connectés à Internet (se reporter à l'annexe 2 de l'II 901 où est définit le concept de « réseau de classe 1 »). De même, la nouvelle édition de l'IGI 1300 qui vise notamment à prendre mieux en compte la dématérialisation croissante des informations, à encadrer les interconnexions de SI classifiés avec d'autres SI, rejoignant en cela une tendance déjà évoquée plus haut, à savoir rendre possible l'interconnexion de SI qui étaient historiquement physiquement isolés de tout autre SI. Attention toutefois à ne pas être trop hâtif dans ses conclusions : bien qu'ouvrant des perspectives d'ouverture, les exigences posées par ces textes demeurent toutefois incompatibles des tendances technologiques de fond mentionnées plus haut dans cet article.

Enfin, difficile de ne pas terminer ce parcours des évolutions réglementaires qui influencent la conception des SI sans faire une évocation succincte de la question de la « souveraineté numérique ». Avec l'émergence de réglementations étrangères ayant des portées extraterritoriales les entités sont confrontées à la difficulté d'opter pour des architectures certes flexibles, redondantes et optimisées mais avec lesquelles la maîtrise de l'accès aux informations n'est plus garantie. Bien que cette approche soit trop simpliste, il est possible de voir dans la directive européenne sur la sécurité des réseaux et de l'information, dite « directive NIS », un contre-point à cette problématique d'extraterritorialité. Cette directive renforce notamment la cybersécurité des opérateurs de services essentiels (OSE) et des fournisseurs de services numériques (FSN) en les contraignant à appliquer des mesures de sécurité (définies au niveau de chaque État membre) et à déclarer les incidents de sécurité affectant ces SI à l'autorité nationale compétence en matière de SSI.

Information

L'extraterritorialité est un principe du droit international public où un État renonce à l'application de son autorité sur une partie de son territoire au profit d'un autre État ou d'une organisation internationale. Loi fédérale américaine *CLOUD Act*, pour *Clarifying Lawful Overseas Use of Data Act*, votée en 2018, est sans doute l'exemple le plus significatif d'une loi mettant en œuvre ce principe d'extraterritorialité.

Annexe B
Exemple de sécurisation d'un SI interne et d'un SI hybride

La sécurisation d'un système d'information hébergé en interne doit tenir compte de l'analyse de risque qui évalue le niveau de menace vis-à-vis de l'entité et des besoins de sécurité qui en découlent pour chaque élément qui compose le SI (applications métier, données, procédés industriels, etc.).

Concrètement cette sécurisation doit mettre en œuvre plusieurs fonctions de sécurité techniques et organisationnelles, dans l'objectif de protéger le système d'information au « juste niveau » :

- **PSSI** La définition d'une politique de sécurité des systèmes d'information permet de formaliser clairement les grands principes et règles de sécurité de l'entité regroupées par thématiques (exploitation du SI, gestion des identités, définitions des rôles, etc.). Elle s'accompagne généralement de la rédaction de chartes pour les utilisateurs ainsi que pour les administrateurs du SI, et de campagnes de sensibilisation à la SSI pour l'ensemble des acteurs de l'entité.
- **Cartographie** L'analyse de risque doit généralement permettre de faire l'inventaire de tous les composants du SI qui font la valeur métier de l'entité. L'objectif de cartographie du SI répond au besoin de maîtrise de son SI, et la bonne connaissance de tous les éléments celui-ci permet notamment d'être plus efficace et réactif dans les phases difficiles de réponse à incident. Dans un premier temps, il est par exemple important de disposer d'un inventaire matériel, de schémas réseaux logiques, ainsi que d'un inventaire détaillé des applications et de leurs besoins de sécurité respectifs. Une matrice des flux réseaux est également importante, pour pouvoir mesurer les impacts en cas de coupure d'un service ou d'une application par exemple.
- **Cloisonnement réseau** Cette action repose dans un premier temps sur la définition de zones réseaux homogènes en ce qui concerne les besoins de sécurité, la sensibilité des données, l'exposition des services, etc. Une fois cette définition réalisée, le cloisonnement doit être réalisé au minimum par le moyen d'un cloisonnement logique classique (VLAN) et peut être accompagné d'un « cloisonnement par le chiffre », c'est-à-dire par la mise en place de tunnels VPN IPsec ou TLS pour sécuriser la transmission d'informations au travers d'équipements réseaux mutualisés (commutateurs de desserte et de cœur de réseau, routeurs, etc.).
- **Filtrage des flux réseaux** Un filtrage strict des flux réseaux doit être opéré au moyen d'un pare-feu interne dédié à cet usage. Ce pare-feu doit également être utilisé pour gérer les règles de routage entre VLAN. Une revue des règles doit être réalisée régulièrement.
- **Gestion des interconnexions et des accès à distance** Des zones d'interconnexions de type DMZ doivent être créées pour les interconnexions vers des SI tiers non maîtrisés. Ces zones doivent protéger le SI interne au minimum avec des équipements de filtrage (p. ex. un pare-feu). L'accès à des réseaux publics (p. ex. Internet) doit faire l'objet d'une vigilance particulière, que ce soit dans le sens sortant, ou dans le sens entrant si l'entité souhaite exposer des services. Des équipements relais (*proxy, reverse-proxy*, etc.) doivent être mis en place afin d'assurer une rupture de session vis-à-vis des flux en provenance ou à destination d'Internet. Enfin, les accès en situation de nomadisme des utilisateurs (p. ex. en télétravail) doivent impliquer la mise en place d'un tunnel VPN IPsec ou TLS non contournable depuis les postes de travail (*full-tunneling*).

- **Gestion des identités et des droits d'accès** Les utilisateurs doivent systématiquement faire l'objet d'une identification et d'une authentification lorsqu'ils souhaitent accéder au SI de l'entité. Cette authentification doit être robuste et si possible reposer sur deux facteurs (2FA). La gestion des droits d'accès doit respecter le principe du moindre privilège. Des procédures de départ et d'arrivée doivent être mises en place et appliquées strictement. Une revue des comptes doit être réalisée périodiquement.

- **Administration sécurisée et gestion des comptes à privilèges** L'administration du SI doit se faire au moyen d'un réseau dédié (au moins logiquement dédié par le moyen de VLAN d'administration) et d'interfaces réseaux dédiées sur les équipements cibles. Les postes d'administration doivent être déconnectés d'Internet et ne doivent pas accéder aux outils bureautiques et collaboratifs (messagerie, navigation Web, etc.). Les comptes à privilèges doivent faire l'objet d'une sécurisation spécifique (p. ex. groupe *Protected Users* dans Active Directory) et doivent être segmentés en fonction du niveau de privilèges (p. ex. avec le découpage en *tier 0, 1 et 2* dans le cas d'un environnement Active Directory). En particulier, les comptes permettant un contrôle total du SI (p. ex. les comptes d'administrateurs du domaine) ne doivent pas être utilisés à d'autres fins que l'administration du domaine (interdiction de connexion vers des serveurs métier ou des postes de travail utilisateur). Enfin les comptes d'administration locale doivent être uniques par équipement et renouvelés régulièrement, de manière à éviter un rejeu et une latéralisation trop facile en cas de compromission de l'un d'entre eux (p. ex. cela peut se configurer avec l'outil LAPS dans les environnements Windows).

- **Durcissement système** Chaque équipement doit faire l'objet d'une étude pour réduire sa surface d'attaque. Au minimum, les applications, modules, périphériques (p. ex. USB), protocoles (p. ex. Bluetooth) et services réseaux non utilisés doivent être désinstallés ou au moins désactivés. En outre, un pare-feu local doit être implémenté, et il doit filtrer strictement les flux entrants et sortants sur l'équipement.

- **Maintien en condition de sécurité** Tous les équipements doivent être mis à jour le plus régulièrement possible avec les correctifs de sécurité, par le moyen de dépôts relais internes. Les mises à jour doivent être systématiquement contrôlées en intégrité avant déploiement. Toute dérogation à la politique de mises à jour doit être tracée et justifiée (p. ex. incompatibilité technique, impossibilité de couper le service à court terme).

- **Journalisation des événements** La journalisation d'événements doit être activée sur chaque équipement et centralisée dans un collecteur d'événements (p. ex. *syslog*) protégé dans une zone sécurisée (p. ex. au sein du SI d'administration). Au minimum, les principaux événements de sécurité doivent être collectés (ouverture et fermeture de session, échec et réussite d'authentification, connexion réseau vers Internet non légitime bloquée par le pare-feu, etc.);

- **Mise en place d'un dispositif de détection et de traitement des incidents** Un dispositif de détection doit être mis en place. Cela prend généralement la forme d'un SIEM (p. ex. Splunk ou ELK). Des règles simples de détection peuvent être implémentées dans un premier temps afin de ne pas être « noyé » dans un nombre d'alertes trop important. Un processus de gestion de crise doit être formalisé, documenté et testé (interlocuteurs, moyens de communication alternatifs, procédure d'isolation du SI interne vis-à-vis d'Internet, etc.);

- **Gestion des sauvegardes et du PRA / PCA** Les sauvegardes doivent respecter les mêmes exigences de sécurité que celles des serveurs de production (confidentialité, intégrité, etc.). Une des copies de sauvegarde doit être externalisée dans un environnement distant complètement déconnecté du SI (hors ligne). Des tests réguliers de restauration complète du SI doivent être réalisés.

- **Sécurité physique et contrôle d'accès** Un système de contrôle d'accès par badges doit être mis en place pour gérer les accès aux locaux de l'entité. Ce système d'information doit être isolé du

SI interne. En cas de dépendance avec le SI interne (application RH), les flux réseaux doivent être strictement filtrés et journalisés. Ce système de contrôle d'accès doit être sécurisé selon les mêmes principes que pour le SI de production, en respectant les recommandations ci-dessus.

- **Gestion de la sécurité des données** Les données les plus sensibles doivent faire l'objet d'un traitement spécifique : chiffrement, audit des accès utilisateur, marquage et classification.

La sécurisation d'un SI hybride, c'est-à-dire un SI interne avec certains services externalisés dans un *cloud* public, reprend les mêmes thématiques de sécurisation, avec quelques points d'attention supplémentaires :

- **PSSI** La PSSI doit prendre en compte les risques associés à l'usage d'applications externalisées (stockage de données sensibles, politique d'accès des utilisateurs, etc.).
- **Cartographie** La cartographie doit spécifier clairement quelles sont les applications hébergées dans le *cloud*, ainsi que les éventuels liens avec des applications internes (synchronisation des données, annuaire d'authentification, etc.).
- **Cloisonnement réseau** Le cloisonnement réseau dans un *cloud* peut généralement se réaliser avec les outils proposés par l'hébergeur (réseau privé virtuel, *network security group*, etc.). Dans le cas d'un hébergement dans un *cloud* public, le cloisonnement logique doit tenir compte de certaines limites, c'est-à-dire que des équipements physiques de l'hébergeur sont mutualisés entre plusieurs clients dont le niveau de sécurité et de confiance n'est pas connu.
- **Filtrage des flux réseau** Au même titre que le cloisonnement réseau, le filtrage des flux est rendu possible par l'outillage proposé par l'hébergeur *cloud*. L'interconnexion entre le SI interne et le *cloud* doit également faire l'objet d'une attention particulière, avec si possible une interdiction ou limitation des flux entrants depuis le *cloud* (moindre confiance) vers le SI interne (plus haute confiance);
- **Gestion des interconnexions et des accès à distance** L'interconnexion entre le SI interne et le *cloud* doit être protégée, si possible au moyen d'un tunnel VPN IPsec. Les accès aux applications sur le *cloud* depuis le poste de travail en situation de nomadisme doivent idéalement transiter par le SI interne, dans un objectif de maîtrise complète des flux réseaux. Dans le cas où ce n'est pas possible, un *split-tunneling* maîtrisé et limité au strict nécessaire peut être implémenté, en assumant les risques d'exfiltration de données que cela peut induire, depuis les postes utilisateurs.
- **Gestion des identités et des droits d'accès** La synchronisation des comptes utilisateurs et des droits d'accès entre le SI interne et le *cloud* doivent faire l'objet d'une attention particulière, ce processus étant critique (transmission d'empreintes de mots de passe, etc.). Les comptes administrateurs du *cloud* doivent être distincts des comptes administrateurs du SI interne, afin d'éviter que la compromission de l'un ne puisse être étendue à l'ensemble du SI.
- **Administration sécurisée et gestion des comptes à privilèges** Le SI d'administration doit disposer d'une enclave spécifique pour administrer le *cloud* (serveurs de rebond dédiés). Les accès aux interfaces d'administration *cloud* doivent être filtrés, *proxifiés* avec une liste d'autorisations, et disposer systématiquement d'une authentification double facteur.
- **Durcissement système** Les systèmes déployés sur le *cloud* doivent faire l'objet d'un durcissement équivalent à ceux déployés en interne.

- **Maintien en condition de sécurité** Une cohérence entre la politique de mise à jour du SI interne et du SI *cloud* doit être mise en place. Des dépôts spécifiques de l'hébergeur peuvent être utilisés pour les serveurs dans le *cloud*, afin d'éviter des flux entrants vers le SI interne.
- **Journalisation des événements** Les événements de sécurité générés dans le *cloud* doivent être journalisés et centralisés dans un collecteur au même titre que pour le SI interne. Des difficultés peuvent être rencontrées lorsque l'hébergeur ne propose pas de fournir ces informations, par exemple dans des offres de type PaaS ou SaaS, où les événements remontés se limitent à des événements applicatifs.
- **Mise en place d'un dispositif de détection et de traitement des incidents** La mise en place d'applications métier dans le *cloud* ne doit pas affaiblir de niveau de détection de l'ensemble. Dans le cas d'attaques ciblées, une compromission d'applications *cloud* peut entraîner une compromission totale du SI, dans la mesure où les deux environnements auront généralement des liens (synchronisation de bases de données) et des flux réseau autorisés entre eux. La plupart des hébergeurs proposent des outils de supervision et de remontée d'alertes, qui doivent être couplées avec le dispositif de détection du SI interne.
- **Gestion des sauvegardes et du PRA / PCA** La gestion des sauvegardes ne doit pas être mise à l'écart pour les environnements *cloud*, quand bien même l'hébergeur réplique les données entre plusieurs centres de données. En effet, en cas de compromission et d'attaque par rançongiciel, l'entité doit être en mesure de pouvoir reconstruire son système d'information *cloud* à partir de sauvegardes externes.
- **Sécurité physique et contrôle d'accès** Ce point doit être pris en compte dans l'analyse de risque et dans le contrat d'infogérance, puisque l'entité n'a aucun moyen de contrôle des personnes ayant accès aux centres de données et aux serveurs de l'hébergeur *cloud* (maintenance).
- **Gestion de la sécurité des données** Ce point est probablement le plus sensible dans le cas où l'entité fait le choix d'externaliser des applications dans le *cloud*. En effet, dans ce cas, l'entité perd une partie de la maîtrise de la sécurité des données. Il est donc recommandé de chiffrer avec des outils et des moyens du SI interne les données les plus sensibles, avant envoi dans le *cloud* (en utilisant une IGC interne). Si ces données doivent être traitées par des logiciels ou des applications fournis directement par l'hébergeur *cloud* (p. ex. avec la suite Office 365 en ligne), il faudra en conséquence que l'entité assume que cet hébergeur a la possibilité technique d'accéder aux données sensibles en clair (menace d'un administrateur *cloud* malveillant ou d'une entité étatique étrangère comme un service de renseignement).

Le référentiel *SecNumCloud* de l'ANSSI entre complètement dans cette démarche de proposer des offres *cloud* de confiance aux entités souhaitant externaliser l'hébergement de leurs données ou applications. Les prestataires *SecNumCloud* respectent des exigences de sécurité portant notamment sur la protection des données, l'administration, la maintenance et la supervision des infrastructures techniques, ou encore la sécurité physique des sites.

Glossaire

2FA	*Two factor authentication*
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APT	*Advanced Persistent Threat*
BATX	*Baidu, Alibaba, Tencent, Xiaomi*
BYOD	*Bring Your Own Device*
CICD	*Continuous Integration and Continuous Deployment*
CVE	*Common Vulnerability Exposure*
DoS	*Denial of Service*
eMBB	*enhanced Mobile BroadBand*
DevOps	*Development Operations*
FISA	*Foreign Intelligence Surveillance Act*
FSN	Fournisseurs de Services Numériques
GAFAM	*Google, Apple, Facebook, Amazon, Microsoft*
HTTPS	*HyperText Transfer Protocol Secure*
IA	Intelligence Artificielle
IaC	*Infrastructure as Code*
IETF	*Internet Engineering Task Force*
IoT	*Internet of Things*
MAN	*Metropolitan Area Network*
mMTC	*massive Machine Type Communication*
NFS	*Network File System*
NIS	*Network and Information System security*
OIV	Opérateur d'Importance Vitale
OSI	*Open Systems Interconnection*
PASSI	Prestataires d'Audit de la Sécurité des Systèmes d'Information
PDIS	Prestataires de Détection d'Incidents de Sécurité
PRIS	Prestataires de Réponse aux Incidents de Sécurité
RFC	*Request For Comments* - Documents publiés par l'IETF
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
SOAR	*Security Orchestration Automation and Response*
SDN	*Software-Defined Network*
SIRP	*Security Incident Response Platform*
SMTP	*Simple Mail Transfer Protocol*
SI	Système d'Information
SIEM	*Security Information and Event Management*
SOC	*Security Operation Center*
SPOF	*Single Point Of Failure*
SSH	*Secure SHell*
SSI	Sécurité des Systèmes d'Information
ToIP	*Telephony over IP*
TLS	*Transport Layer Security*
URLLC	*Ultra Reliable Low Latency Communication*
VPN	*Virtual Private Network*
XSS	*cross-Site Scripting*
YAML	*Yet Another Markup Language* ou *YAML Ain't Markup Language*
WAF	*Web Application Firewall*
WAN	*Wide Area Network*
ZTN	*Zero Trust Network*

Bibliographie

[1] *La défense en profondeur appliquée aux systèmes d'information*.
Guide Version 1.1, ANSSI, juillet 2004.
https://www.ssi.gouv.fr/defense-profondeur.

[2] AVAST.
The history of cybersecurity, 2020.
https://blog.avast.com/history-of-cybersecurity-avast.

[3] Alcardo Alex Barakabitze.
5G network slicing using SDN and NFV : A survey of taxonomy, architectures and future challenges, 2019.
https://arxiv.org/pdf/1912.02802.pdf.

[4] Doug Barth and Evan Gilman.
Zero Trust Networks : Building Secure Systems in Untrusted Networks.
O'Reilly Media, Inc., juillet 2017.

[5] Doug Barth and Evan Gilman.
Zero Trust Networks : Building Trusted Systems in Untrusted Networks.
San Francisco, CA, mars 2017. USENIX Association.

[6] *Attaques APT*.
PERNET Cédric.
Publication, Techniques de l'Ingénieur - H5842, 2020.

[7] CIGREF.
Histoire des virus, cauchemars de l'informatique, 2011.
https://www.cigref.fr/archives/histoire-cigref/blog/histoire-des-virus-cauchemars-de-l-informatique/.

[8] Ministère des Armées.
Livre blanc sur la défense et la sécurité nationale, 2013.
https://www.defense.gouv.fr/portail/enjeux2/politique-de-defense/le-livre-blanc-sur-la-defense-et-la-securite-nationale-2013/livre-blanc-2013.

[9] Le Figaro.
Les plus incroyables cyberattaques de l'histoire, 2020.
https://www.lefigaro.fr/secteur/high-tech/dossier/serie-d-ete-les-plus-incroyables-cyberattaques-de-l-histoire-tech-et-web.

[10] *Virus informatiques et autres infections informatiques*.
IROLLA Paul FILIOL Eric, DAVID Baptiste.
Publication, Techniques de l'Ingénieur - H5440V3, 2017.

[11] Google.
A New Approach to Enterprise Security, 2020.
https://beyondcorp.com.

[12] INSEE.
Les entreprises en France, 2019.
https://www.insee.fr/fr/statistiques/4255707?sommaire=4256020.

[13] *Pare-feu - Couteau suisse de la sécurité informatique*.
LAURENT Maryline.
Publication, Techniques de l'Ingénieur - TE7550V2, 2017.

[14] Le Monde.
Vingt ans après, le créateur du virus informatique « I Love You » témoigne, 2020.
https://www.lemonde.fr/pixels/article/2020/05/04/vingt-ans-apres-le-createur-du-virus-informatique-i-love-you-temoigne_6038636_4408996.html.

[15] Parlement.
LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, 2013.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028338825/.

[16] Parlement.
LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, 2018.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037192797.

[17] Fondation pour la recherche stratégique.
Du cyber et de la guerre, 2019.
https://www.frstrategie.org/publications/notes/cyber-guerre-2019.

[18] SGDSN.
Revue stratégique de cyberdéfense, 2018.
http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/.

[19] Anant Shrivastava.
DevSecOps What, Why and How, 2019.
https://i.blackhat.com/asia-19/Thu-March-28/bh-asia-Shrivastava-DevSecOps.pdf.

[20] Wavestone.
What is the next generation cybersecurity model ?, 2017.
https://www.wavestone.com/app/uploads/2017/07/generation-cybersecurity-model.pdf.