La cybersécurité

Par Hervé DEBAR
Professeur de l'Institut Mines-Télécom à Télécom SudParis

Les enjeux de cybersécurité sont devenus une problématique majeure des infrastructures numériques. La menace portée par des attaquants organisés, outillés et motivés ne laisse aucun doute sur le fait que ces infrastructures numériques sont sous attaque et que certaines seront compromises. Les méthodes et outils de la cybersécurité doivent donc être pris en compte dans la spécification et le déploiement de ces infrastructures numériques actuelles et futures, pour analyser le risque et l'impact des attaques, pour mettre en place des mécanismes de protection, de détection et de remédiation face à ces attaques.

Nous avons fait des progrès ces dernières années pour contenir les attaques informatiques, mais il reste absolument nécessaire d'inclure les problématiques de cybersécurité en continu dans le pilotage de ces infrastructures numériques. Cette prise en compte des problématiques de sécurité participera naturellement d'un fonctionnement plus efficace des services offerts aux utilisateurs de ces infrastructures.

Introduction

Les infrastructures numériques sont présentes dans tous les services que nous utilisons de manière quotidienne. De ce fait, ces infrastructures numériques sont devenues partie intégrante de services critiques et on trouve du code informatique et des besoins en communication dans de nombreux environnements. Ces outils sont utilisés d'une part pour capter et traiter des informations, d'autre part pour des infrastructures de commande et de contrôle. La collecte et l'acheminement des informations nécessaires au bon fonctionnement de ces infrastructures reposent donc en grande partie sur une connectivité ubiquitaire, donc sur des réseaux offrant des capacités de communication et de traitement d'une grande diversité.

Pourquoi la cybersécurité des réseaux est-elle un enjeu majeur ?

Tout d'abord, il est nécessaire de mentionner que le monde numérique est de plus en plus connecté et interconnecté, et ne peut fonctionner sans ces interconnexions. Par conséquent, l'approche par isolation (suppression de la connectivité) totale ou partielle est mise en difficulté par l'absence de périmètre à isoler (réseaux sans fil par exemple) ou par la difficulté de mettre en place des outils de filtrage des communications efficaces (déploiement très large du chiffrement de bout en bout, complexité d'analyser le contenu des données échangées plutôt que des métadonnées ou des enveloppes).

Dans la mesure où il devient difficile d'identifier et de localiser un objet numérique ou son propriétaire et son usage légitime, il devient de plus en plus difficile de mettre en place des politiques de sécurité pouvant répondre aux besoins croissant de protection de ces infrastructures numériques.

Un enjeu économique

Le coût global de la cybercriminalité est estimé à 7,08 T$ en 2022 et pourrait doubler en 6 ans[1].

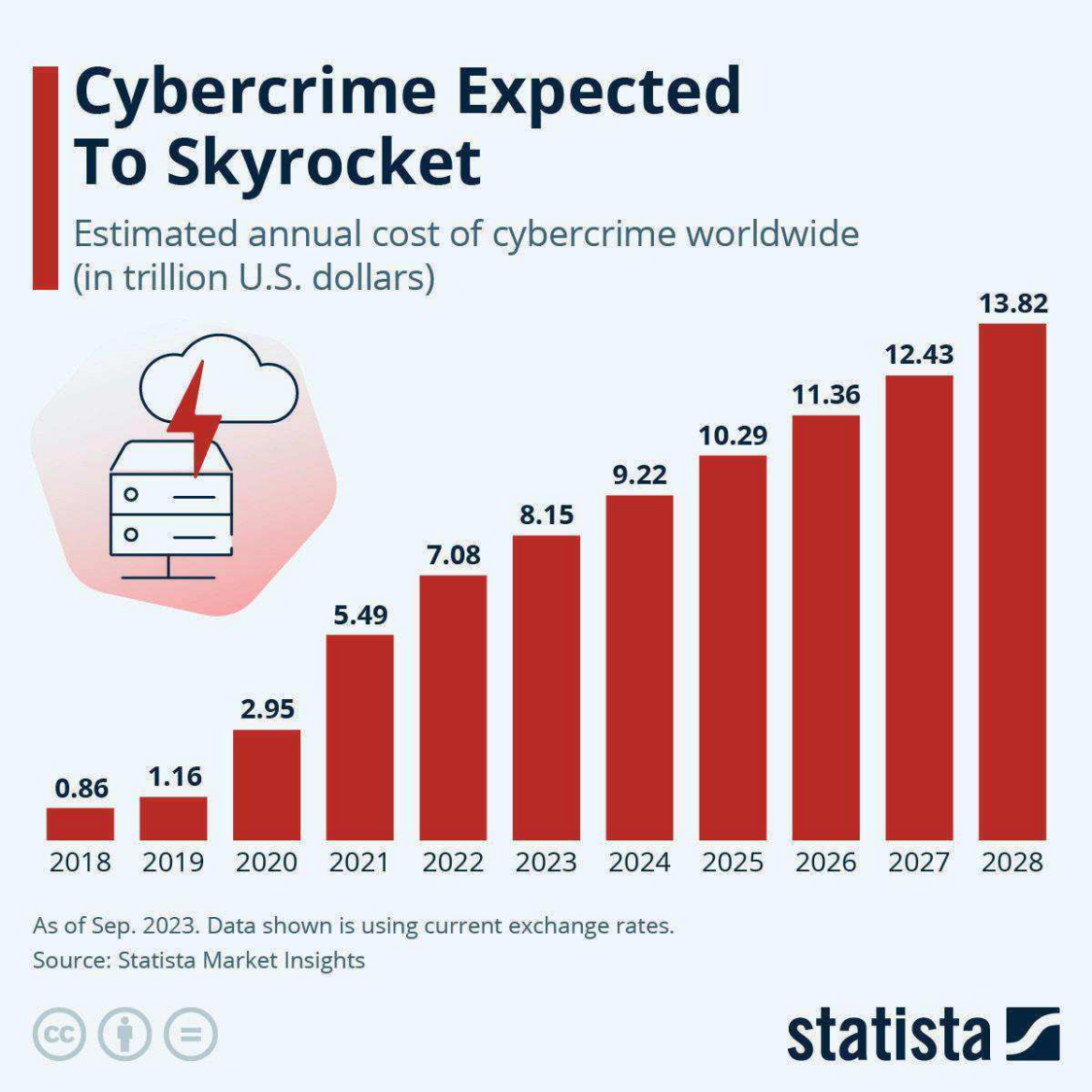

Figure 1 : La montée de la cybercriminalité, en trillions US dollars (Source : Statista Technology Market Outlook ; National Cyber Security Organizations, FBI, IMF).

Il est nécessaire de comprendre que les attaques cyber ne constituent plus un épiphénomène, mais une source de perte de valeur importante pour l'ensemble de l'économie. Le cybercrime est devenu une source de revenu majeure pour les cybercriminels (plus que le trafic de drogue), et il est particulièrement attrayant grâce aux attaques à distance. Il est en effet difficile de traquer les criminels et d'amasser les preuves nécessaires à une condamnation, et cette activité illégale est sensiblement moins risquée.

Même si les chiffres sont difficiles à établir, les dégâts d'une attaque cyber réussie sont très importants et prennent des formes multiples, amenant à une indisponibilité de fonctionne-

[1] https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

ment de l'organisation, à une perte de chiffre d'affaires et *in fine* à une perte de confiance des clients. Les coûts des mécanismes de protection sont également significatifs, et ils ne garantissent pas une protection absolue. Cependant, pour un grand nombre d'attaques, ils permettent d'empêcher la compromission ou d'en limiter les effets et la durée.

Notons également que les compromissions ne sont pas immédiatement détectées, même si la situation dans ce domaine s'améliore[2].

La Figure 2 montre qu'en 10 ans, nous avons divisé par 20 le temps qu'un attaquant passe en moyenne dans un système compromis avant d'être détecté. Le même rapport indique toutefois que la détection se fait le plus souvent par des sources externes alertant l'organisation d'une compromission. Ce temps pendant lequel un attaquant reste résidant dans un système d'information lui permet largement de cartographier le système et d'en extraire des informations sensibles, ce qui induit des dommages significatifs.

Figure 2 : Durée moyenne avant qu'une compromission soit détectée dans un système (Source : M-Trends 2023).

Attaques à grande échelle *versus* attaquants motivés

La connectivité a été un facteur majeur dans le développement des attaques cyber. On recense ainsi le premier vers informatique en 1988, ainsi que de premiers actes d'espionnage (The Cuckoo's Egg, 1988). Les réseaux, et la capacité de se connecter à distance, ont joué un rôle majeur, et ont créé des communautés de *hackers* souhaitant accéder à des infrastructures auxquelles ils n'avaient pas accès facilement.

Le profil des attaquants a cependant sensiblement évolué depuis les débuts d'Internet. Nous trouvons aujourd'hui deux grandes familles d'attaquants, catégorisés par leur motivation :

- Motivation économique : les attaquants guidés par un motif économique souhaitent tout simplement gagner de l'argent. Ils utilisent des outils disponibles à faible coût, louent leurs infrastructures, et se basent sur des attaques à grande échelle (par exemple des campagnes de *phishing*) pour toucher le plus de victimes potentielles possible. Même si leur taux de succès est faible, le faible coût d'investissement et le passage à l'échelle suffisent à rendre ces opérations rentables. L'usage de l'intelli-

[2] https://www.mandiant.fr/resources/blog/m-trends-2023

gence artificielle permet également de rendre ces opérations de plus en plus crédibles et difficiles à différencier d'opérations légitimes. Ces attaquants sont le plus souvent des criminels, individus ou groupes.

Cette motivation économique peut amener également à des destructions de données ou des destructions physiques d'équipements, causant des dommages majeurs aux victimes. Ces dommages peuvent être intentionnels, et toucher le monde physique, comme le montrent les attaques contre les hôpitaux et les objets connectés médicaux. Il est également possible de prendre le contrôle à distance d'objets (par exemple un véhicule) pouvant devenir une arme par destination.

- Motivation liée à la cible : certains attaquants choisissent une cible particulière et déploient de grands efforts pour compromettre cette cible. Ils disposent de beaucoup de capacités (financières, techniques, humaines) pour mener à bien leurs attaques. Leurs buts peuvent être parfois économiques, mais sont le plus souvent liés à de l'espionnage ou de la désinformation. Ces attaquants sont le plus souvent soutenus par des États-nations, soit directement (armée), soit indirectement (terrorisme, mafias).

Dans les deux cas, force est de constater qu'il est très difficile d'être complètement protégé des attaques, et qu'il est devenu indispensable de pratiquer une défense en profondeur pour limiter les dégâts.

Infrastructures et données

La cybersécurité s'applique à deux objets, les infrastructures numériques et les données qu'elles contiennent. Il est donc indispensable de penser sa cybersécurité suivant ces deux dimensions.

La cybersécurité des infrastructures numériques consiste à déployer des mécanismes de gestion du fonctionnement de ces infrastructures permettant de gérer le risque. Il s'agit donc, de manière très générale, de s'assurer que le fonctionnement de l'infrastructure est conforme aux règles décidées par l'organisation, et par ses régulateurs. Cela repose sur des architectures et des règles de fonctionnement qui doivent être systématiquement vérifiées lors de toute activité. Par exemple dans le cas du réseau, il s'agit de vérifier que l'utilisateur qui y accède est effectivement autorisé à le faire, et que les interactions qu'il entretient avec le réseau sont conformes à ces règles.

Même si le fonctionnement de l'infrastructure est sécurisé, il est nécessaire en complément de sécuriser la donnée. La donnée est comprise ici dans un sens très général et peut inclure les traitements que cette donnée doit subir, algorithmes, codes, etc. Une démarche de cybersécurité en profondeur ne peut se reposer sur le fait que l'infrastructure soit sécurisée pour assurer la sécurisation des données, mais doit en complément déployer ses propres mécanismes de protection. Dans le cas du réseau, cela peut prendre la forme de tunnels chiffrés, sur différentes couches, comme des réseaux privés virtuels.

Formalisation de la cybersécurité : le *framework* NIST

Pour raisonner sur les problématiques de cybersécurité, nous nous référons au *framework* produit par le NIST[3], et ici sa version 2.0. Les différents concepts du *framework* NIST sont résumés dans la Figure 3 page suivante.

[3] National Institute of Standards and Technology.

Figure 3 : Concepts du framework NIST (Source : National Institute of Standards and Technology).

Tableau 1 : Les fonctions et catégories du framework NIST (Source : National Institute of Standards and Technology).

Fonction	Category	Identifyer
Govern (GV)	Organizational content	GV.OC
	Risk management settings	GV.RM
	Cybersecurity supply chain risk management	GV.SC
	Roles, responsibilities and authorities	GV.RR
	Policies, processes and procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset management	ID.AM
	Risk assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity management, authentication and access control	PR.AA
	Awareness and training	PR.AT
	Data security	PR.DS
	Platform security	PR.PS
	Technology infrastructure resilience	PR.IR
Detect (DE)	Continuous monitoring	DE.CM
	Adverse event analysis	DE.AE
Respond (RS)	Incident management	RS.MA
	Incident analysis	RS.AN
	Incident response reporting and communication	RS.CO
	Incident mitigation	RS.MI
Recover (RC)	Incident recovery plan execution	RC.RP
	Incident recovery communication	RC.CO

Le *framework* NIST (https://www.nist.gov/cyberframework) est organisé en six fonctions, chacune découpée en plusieurs catégories indiquant les différents éléments à prendre en compte. Les cinq fonctions hors gouvernance (considérée comme transverse) relèvent d'une démarche d'analyse de risque, dans laquelle l'organisation commence par identifier ses biens et ses risques, puis met en place les mécanismes de protection nécessaires. Les risques non couverts sont ensuite traités par des mécanismes de détection, puis de réponse et de reprise si une attaque amène une compromission.

La gouvernance

La gouvernance de cybersécurité d'une organisation établit les différents éléments organisationnels qui vont piloter la politique de cybersécurité, tant sur le plan humain que sur le plan des règles et des process. C'est un point particulièrement critique pour les nouveaux réseaux, puisque le fournisseur d'infrastructure réseau et *cloud* peut héberger des services tiers, et doit inter-opérer avec d'autres fournisseurs d'infrastructure. Chaque fournisseur doit donc établir les règles d'interaction avec les organisations qu'il héberge et ses pairs, le déploiement des politiques de cybersécurité, et le traitement des incidents. Il doit également définir des mécanismes de confiance pour dialoguer avec eux et valider les informations échangées.

L'identification des risques

L'identification des risques repose sur l'identification des composants matériels et logiciels d'une part, sur la connaissance des vulnérabilités et des attaquants potentiels d'autre part. Cette identification des composants est plus difficile dans un contexte de réseaux du futur car ils sont par nature définis par le logiciel, et donc peuvent changer de surface d'attaque très rapidement. Certains composants, matériels ou logiciels, sont par ailleurs actifs dans le réseau mais ne sont pas la propriété de l'opérateur, ce qui accroît la difficulté de connaître leur fonction et leurs vulnérabilités.

La protection

La protection contre les attaques couvre de nombreux domaines, techniques et organisationnels. Ces mécanismes de protection forment la première barrière face aux attaquants, et ils sont les éléments clés de la mise en œuvre d'une politique de cybersécurité solide.

Les réseaux du futur vont cependant nécessiter des adaptations significatives de ces mécanismes classiques et bien maîtrisés. Leur taille et leur nombre d'utilisateurs vont rendre difficile le déploiement des outils d'identification, d'authentification et de contrôle d'accès, à cause de l'échelle, et également de la dynamique d'usage de ces réseaux lorsqu'il s'agira de fournir des services à la demande. L'ouverture de services à la demande implique une compétition pour l'accès à des ressources limitées, ce qui offre tout d'abord des possibilités d'attaque par déni de service. Plus significatif, la colocalisation de services peut rendre possible des fuites de données ou l'espionnage d'un client par un autre. Il sera donc nécessaire d'inventer de nouveaux mécanismes d'isolation, tant réseau que système, et d'exposer ces mécanismes aux clients pour leur permettre de piloter également leur propre politique de cybersécurité.

Détection

La détection des attaques s'est imposée comme un complément indispensable aux mécanismes de protection, qui malgré leur efficacité peuvent être submergés par des vagues importantes d'attaques, ou contournés par des attaquants très puissants. Il sera donc nécessaire de mettre en place dans les réseaux du futur des sondes permettant d'observer le comportement du réseau, et de l'analyser en temps réel pour détecter des modifications du comportement qui pourraient être symptomatique d'attaques.

En réponse aux besoins réglementaires, et pour optimiser la détection et la réponse, ces réseaux du futur devront être capables d'échanger des informations relatives aux vulnérabilités et aux incidents de sécurité. La mise en place de ce partage d'informations, par nature sensibles, devra également s'appuyer sur des mécanismes techniques et sur des relations de confiance entre opérateurs.

Réponse et remédiation

La réponse et la remédiation forment deux éléments distincts du *framework* NIST, qui sont cependant très proches. La réponse traite de l'incident dès qu'il est détecté, et a pour but de limiter l'impact de la compromission sur le fonctionnement du réseau. Cela implique des aspects techniques, comme la capacité à tracer les activités des attaquants pour identifier les composants compromis, et des aspects organisationnels, comme la communication de crise. Les infrastructures numériques à venir doivent être conçues en prenant en compte ce besoin de traçabilité, qui est souvent mal couvert dans les infrastructures actuelles.

À plus long terme, la remédiation a pour but d'éviter que la compromission se reproduise, et fait évoluer la configuration et le fonctionnement du réseau pour que ces attaques ne puissent plus réussir. Cela implique généralement des modifications dans la politique de cybersécurité.

Où en sommes-nous en France ?

Dans le cadre français, nous opérons les infrastructures numériques selon les règlementations européennes (RGPD, NIS et NIS2, DSA et DMA, et d'autres à venir). Nous participons à l'élaboration de ces règlements et nous sommes globalement actifs pour en assurer le bon déploiement sur le territoire national. À ce titre, l'Agence Nationale de Sécurité des Services d'Information (ANSSI) assume un *leadership* reconnu pour protéger les services de l'État, et peut intervenir dans des cas critiques.

En termes industriels, il existe un écosystème de grands groupes et de PME avec de fortes compétences en cybersécurité. Cependant, la plupart des produits déployés sont d'origine étrangère (américaine, israélienne, etc.). Un produit de cybersécurité ne peut être rentabilisé sur un marché national. L'émergence d'une industrie européenne de la cybersécurité nous semble absolument indispensable pour assurer l'indépendance technologique et la souveraineté numérique de chacun des États membres.

Conclusion : faire face aux nouvelles menaces

De nouvelles menaces apparaissent régulièrement, qui doivent être prises en compte. Plusieurs éléments ont cependant émergé ces dernières années, qui devront impérativement être pris en compte par les infrastructures numériques du futur :

- Les attaques sur la chaîne logistique logicielle : nous avons depuis quelques années ce type d'attaques qui touchent autant les logiciels fermés (exemple : SolarWinds) que les logiciels libres (exemple : LZ). Ces attaques ont des conséquences très importantes sur la maîtrise du logiciel inclus dans ces infrastructures, avec des conséquences majeures sur les privilèges que les attaquants obtiennent grâce aux chevaux de Troie inclus dans cette chaîne logistique logicielle. Il deviendra impératif de sécuriser cette chaîne logistique, pour assurer tant la disponibilité que l'intégrité du logiciel.
- Les attaques contre les modèles et algorithmes d'intelligence artificielle : si les attaques contre les outils d'IA ne sont pas nouvelles, elles ont un impact sensiblement plus grand pour des systèmes contrôlés par des IA. La complexité des algorithmes et la disponibilité des données et des matériels nécessaires à l'apprentissage peut

poser des problèmes de souveraineté, dans la capacité à se procurer lesdites données, matériels (GPU) et aussi les compétences nécessaires pour opérer les mécanismes d'apprentissage.

- La complexité des systèmes et des frontières : il devient de plus en plus difficile de comprendre le fonctionnement de systèmes numériques de grande taille, donc de définir leur politique de cybersécurité. Le nombre d'acteurs va également rendre nécessaire la délégation de responsabilités, ce qui engendre de nouveaux besoins d'audit et de contrôle.

Les infrastructures numériques doivent impérativement offrir à leurs utilisateurs des solutions de communication, de calcul et de stockage de confiance et être pérennes. Nous disposons de nombreux mécanismes pour protéger ces infrastructures, malgré le fait que les attaques cyber aient un impact significatif sur le fonctionnement de ces infrastructures. Les mécanismes de protection ont également un coût technologique et économique.

Le renforcement des mécanismes existants pour les adapter aux besoins des cas d'usage modernes (faible consommation d'énergie, faible latence, faible débit, etc.) des infrastructures critiques est absolument nécessaire pour faire émerger des infrastructures numériques de confiance, ou les aspects liés à la cybersécurité (contrôle d'accès et d'usage, gestion des identités et des accès, audit et contrôle) sont compris et acceptés par tous les utilisateurs de ces infrastructures. Le lien entre cybersécurité et sureté de fonctionnement, longtemps considéré comme important mais difficile à mettre en œuvre, doit également être renforcé pour assurer, dans le cas des infrastructures critiques, à la fois la sécurité des biens et des personnes.

Finalement, comme pour beaucoup de sujets touchant au numérique, conserver sa souveraineté demande à la fois des capacités technologiques pour développer ou déployer des outils, mais aussi les capacités humaines pour inventer de nouveaux outils ou pour opérer de manière adéquate des outils sensibles dans des environnements complexes, les conséquences d'une erreur pouvant être majeures.