La cybersécurité devient un des enjeux principaux de l'avenir des sociétés au même titre que le développement durable

Comment y faire face ?

Introduction

Roberto Kung
Membre Senior SEE

Introduction

La numérisation croissante de la société (smartphones, objets connectés…) et des entreprises (IT, systèmes connectés…) augmente d'autant les opportunités de cyberattaques à des fins d'extorsion, de malveillance, d'influence ou d'espionnage. Avec la globalisation, les cyberattaquants peuvent venir du monde entier. La sophistication croissante des cyberattaquants rend le danger de plus en plus difficile à parer.

C'est le secteur industriel qui est le plus ciblé par les cyberattaques, notamment l'extorsion de fonds au moyen de rançongiciels. Par exemple (figure 1), la fameuse attaque Ransomware Wannacry en 2017 a entraîné des répercussions sur de nombreuses entreprises dans le monde [1]. L'entreprise taiwanaise TSMC, premier producteur mondial de chips à haute technologie, avait dû arrêter ses usines temporairement en 2018 à cause des répercussions de Wannacry.

La cybersécurité englobe les méthodes et les technologies pour protéger les informations numériques et les systèmes d'information contre les attaques et les exploitations malveillantes. Elle se retrouve au cœur du développement technologique et organisationnel de la société et devient une des principales préoccupations des entreprises. En effet, la cybercriminalité ne cesse de se professionnaliser et a atteint, grâce à l'émergence de l'IA et de nouvelles technologies ultra-performantes, un haut degré de maturité. L'heure est venue, pour les entreprises, d'investir fortement dans leur cybersécurité, car les cybercriminels vont développer des méthodes de plus en plus sophistiquées pour parvenir à leurs fins.

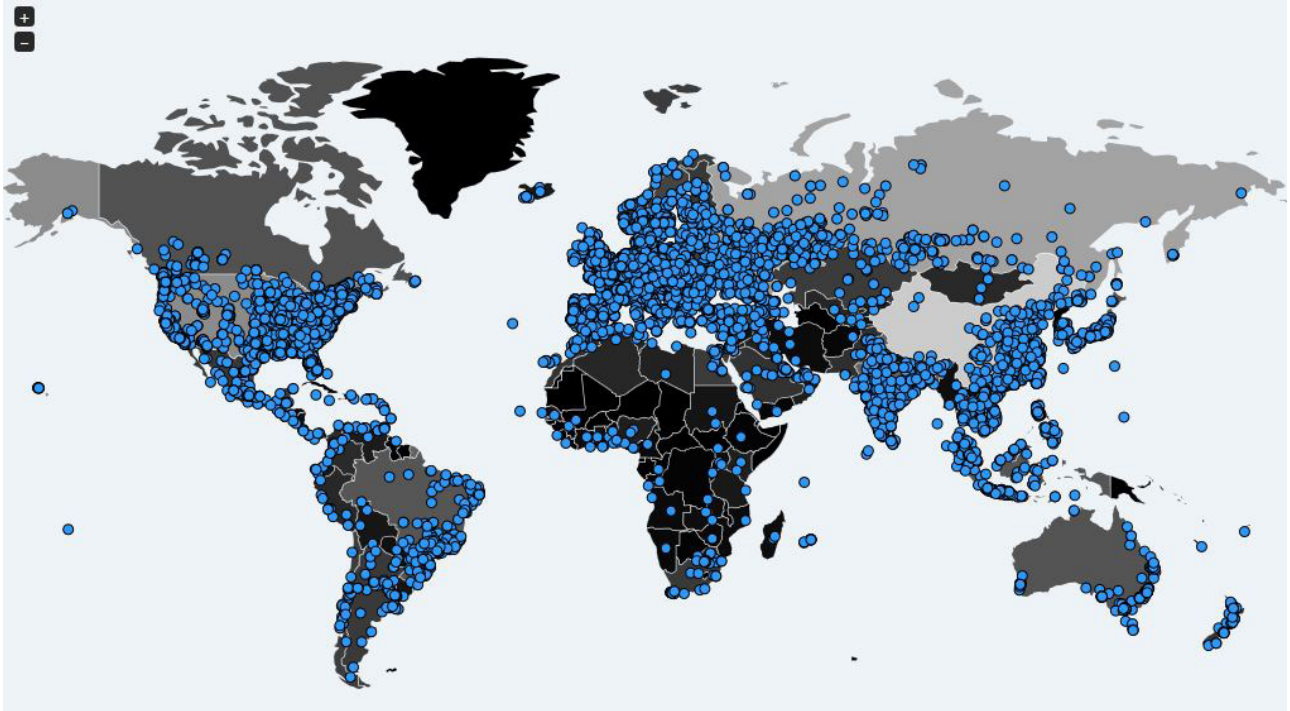


Figure 1 : Carte des attaques Wannacry [2].

Ce dossier apporte quelques éléments d'éclairage sur la façon dont les entreprises et la société peuvent faire face aux menaces liées aux cyberattaques. La gestion de la sécurité s'articule autour de la prévention et de la gestion proactive des risques liés aux opérations informatiques. Elle implique d'appréhender correctement les enjeux techniques de la numérisation selon chaque domaine de l'industrie et d'analyser l'architecture numérique de bout en bout de l'entreprise.

Elle associe réactivité en cas d'incidents et initiatives préventives car l'entreprise doit développer la capacité à détecter les attaques, se donner les moyens de se défendre et être capable de réagir en cas de crises. Avant tout, il est bien plus efficace de prévenir et d'empêcher les attaques que de réagir a postériori.

Les exigences spécifiques de la cybersécurité par domaine

Le dossier se concentre sur les domaines télécom et industriels (cf. articles d'Orange pour les Telecom ou de Siemens pour l'industrie 4.0). Cependant, chaque domaine industriel a des points de sécurité spécifiques. Certains domaines comportent des enjeux au niveau d'une nation comme les opérateurs d'intérêt vital dits entités essentielles (EE) tels que définis dans la directive NIS2. Nous pouvons par exemple mentionner les exigences spécifiques de quelques autres domaines [2b] :

• L'industrie automobile : la voiture est désormais un système qui comprend des centaines d'éléments intelligents et communicants. La voiture est de plus en plus exposée aux cyberattaques. Mais, il y aussi des menaces à chaque étape du cycle de vie des projets. Cela s'étend des usines de fabrication au véhicule connecté et aux opérations informatiques plus larges de l'entreprise.

• Énergie et services publics : les infrastructures critiques, telles que les réseaux énergétiques et les systèmes d'approvisionnement en eau, ont toujours exigé un niveau de sécurité élevé. Aujourd'hui, les progrès numériques font apparaitre un nouveau risque de sécurité : celui de la sécurité des compteurs intelligents. Si les compteurs intelligents offrent la possibilité d'une plus grande précision des informations relatives à l'utilisation, le défi consiste à s'assurer que ces informations sont protégées contre les cyberattaques. La menace est bien réelle, car on craint qu'un code malveillant ne coupe l'électricité dans les maisons ou qu'un pirate informatique n'accède aux données relatives à la consommation d'eau ou d'électricité pour repérer les moments où le propriétaire n'est pas là.

• Services financiers : la confiance des consommateurs est essentielle dans le secteur des services financiers. Les clients s'attendent à ce que leurs données personnelles et financières soient protégées contre les failles de sécurité. Avec le RGPD de l'UE qui impose de signaler toute violation de données dans les 72 heures suivant l'incident, les consommateurs sont plus que jamais conscients des problèmes de sécurité. Il y a donc une incitation claire à investir du temps et des ressources dans la protection des données des clients.

Le dossier, sans être exhaustif, donne un panorama de nombreux enjeux techniques à appréhender (réseau, industrie 4.0, logiciel, IA…). Il faut cependant mentionner deux enjeux particulièrement importants non couverts par les articles du dossier : ●●●

le cloud, infrastructure de plus en plus utilisée (en mode public, hybride ou privé) et la chaîne d'approvisionnement, stratégique pour tout industrie.

Protection des infrastructures cloud

L'adoption de technologies et contrôles appropriés est cruciale pour sécuriser les infrastructures critiques et les réseaux de données virtualisés avec le cloud.

Il s'agit d'abord de sécuriser l'infrastructure soit sous la responsabilité du fournisseur de cloud (cas le plus fréquent), soit sous celle de l'entreprise qui gère son propre cloud privé. Les fournisseurs de cloud mettent en œuvre les solutions de cybersécurité avec des exigences supérieures aux cloud privés du fait qu'ils doivent gérer la coexistence de plusieurs utilisateurs. Par ailleurs, l'ANSSI [1] impose une certification pour un cloud de confiance ou un cloud souverain pour se protéger d'éventuelles interférences étrangères. L'entreprise doit dans tous les cas travailler avec son fournisseur pour être certain qu'il n'y a pas de vulnérabilités involontaires, par ignorance de ce que l'entreprise doit faire pour bien travailler avec son fournisseur.

Il s'agit ensuite pour l'entreprise d'assurer la sécurité des données et applications qui se trouvent dans le cloud en mettant en œuvre les protections nécessaires :

• La gestion des identités et des accès par les salariés ou les clients de l'entreprise, de loin l'élément le plus important de toute politique de sécurité de l'entreprise.

• Le chiffrement indispensable et pour lequel il peut s'appuyer sur les solutions fournies par son fournisseur.

• La capacité de superviser globalement son architecture de systèmes (interne + cloud) pour savoir ce qui se passe à chaque instant et de vérifier que les règles de sécurité sont bien respectées et le cas échéant réagir. La plupart du temps cette tâche est menée par des prestataires spécialisés.

De plus en plus de solutions de cybersécurité pour le cloud apparaissent, telles les CNAPP (*Cloud-Native Applications Protection Platform*) formalisés par Gartner, les CASB (*Cloud Access Security Broker*) et les SSPM (*SaaS Security Posture Management*) [2c]. L'article sur la Recherche évoque les aspects spécifiques aux approches logiciels DevSecOps liés à l'approche cloud.

Pour les entreprises qui n'utilisent pas encore le cloud mais qui envisagent une migration vers le cloud, il est indispensable de préparer cette migration en tenant comptes des aspects sécurité notamment pour la sécurité des données et des accès dans le futur environnement cloud, avec une formation des salariés, des nouvelles pratiques, des changements de responsabilité, une mise à jour de la politique de sécurité, voire de nouveaux métiers etc... La sécurité dans le cloud passe donc aussi par un changement de culture à tous les niveaux.

Sécurisation de la chaîne logistique

La chaîne logistique, correspond aux différentes étapes liées à la chaîne d'approvisionnement, de l'achat des matières premières à la livraison d'un produit ou service au client. Elle représente tous les intervenants œuvrant à garantir et optimiser la production.

Les entreprises utilisent de plus en plus des composants ou des services réalisés par d'autres entreprises. La sécurité des services / produits d'une entreprise dépend ainsi du niveau de sécurité des composants ou des services des sous-traitants. Par exemple, la vulnérabilité d'un composant sous-traité peut se répercuter sur l'ensemble de l'entreprise comme le montre l'épisode CrowdStrike (cf. article sur la normalisation).

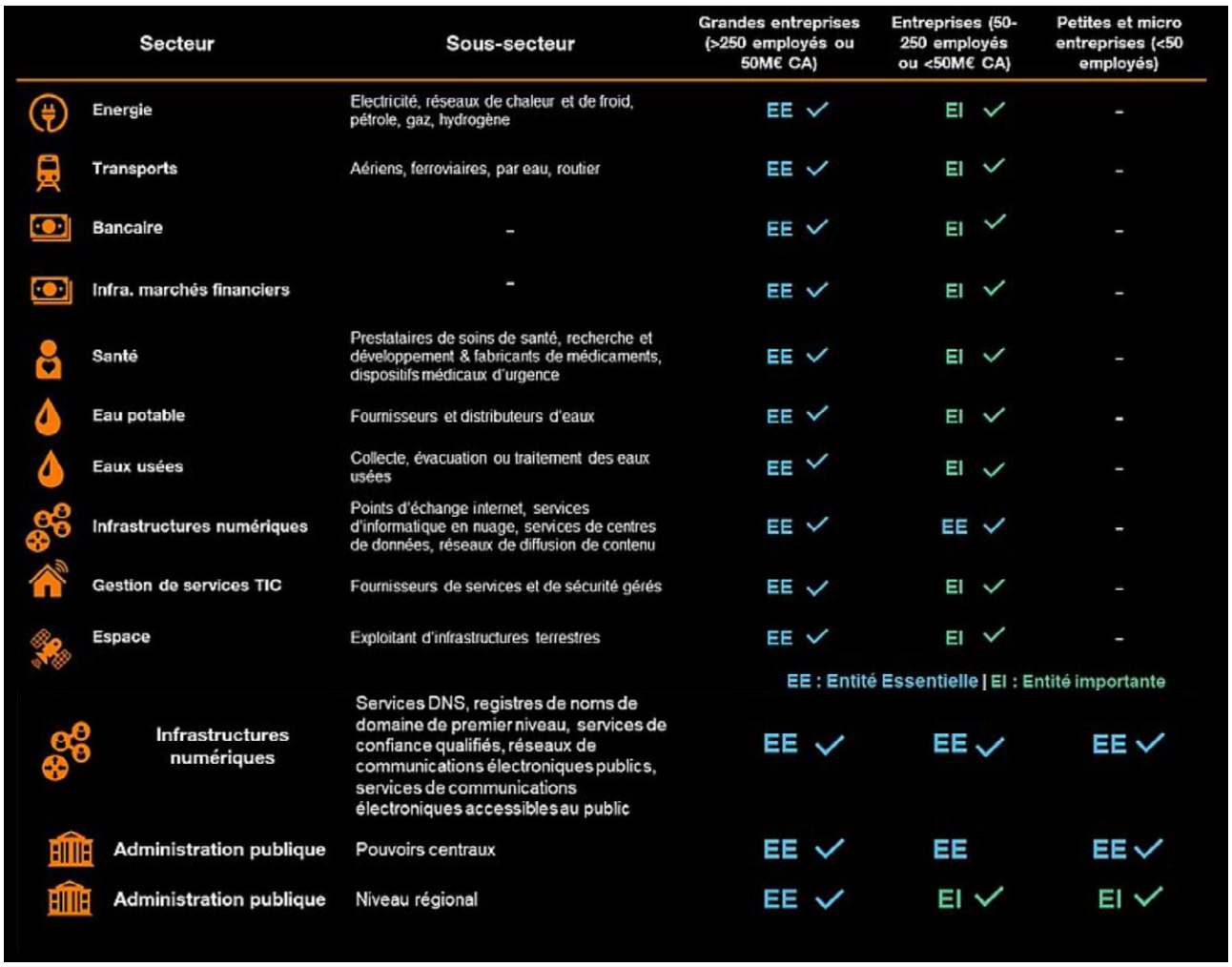
Il est donc indispensable de contractualiser avec tous les fournisseurs les garanties adéquates de cybersécurité. Les entreprises devront tenir compte des diverses directives en cours d'élaboration dont la directive NIS2, ainsi que les approches spécifiques par domaine (automobile, eau, aéronautique…). Par ailleurs, la chaîne logistique elle-même, composée de processus automatisés et manuels doit être sécurisée de manière adéquate. Cela concerne notamment l'utilisation des logiciels tiers notamment pour les mises à jour automatisées ou non des logiciels.

Analyse et gestion des risques

La prévention en amont devient une préoccupation constante, elle touche tous les aspects de l'entreprise. L'analyse des risques doit identifier et évaluer les risques susceptibles de compromettre la sécurité des systèmes d'information, elle implique l'entreprise dans tout son environnement technique, organisationnel et commercial. Tous leurs processus doivent intégrer la sécurité adéquate (par exemple la gestion des droits d'accès ou des mots de passe, l'introduction et la mise à jour des systèmes, la prise en compte des accès externes – fournisseurs, clients…). Les vulnérabilités sont nombreuses et augmentent vertigineusement avec la sophistication des technologies utilisées. Il est donc essentiel d'analyser constamment les éventuelles nouvelles vulnérabilités pouvant affecter l'entreprise, en se faisant aider des spécialistes dont c'est le métier, afin d'identifier celles qui comportent des risques pour l'entreprise, et de mettre en place les plans de prévention. De plus, il est important de constamment auditer l'entreprise pour vérifier si les processus sont respectés et si les plans de prévention sont bien mis en place et bien suivis car ils concernent les facteurs humains, les processus et les organisations.

Les gouvernements sont bien conscients de ces enjeux et mettent en place des guides et des certifications par le biais

1 Référentiel SecNumCloud afin de promouvoir, enrichir et améliorer l'offre de fournisseurs cloud à destination des entités publiques, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE).



Secteur	Sous-secteur	Grandes entreprises (>250 employés ou 50M€ CA)	Entreprises (50-250 employés ou <50M€ CA)	Petites et micro entreprises (<50 employés)
Energie	Electricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène	EE ✓	EI ✓	-
Transports	Aériens, ferroviaires, par eau, routier	EE ✓	EI ✓	-
Bancaire	-	EE ✓	EI ✓	-
Infra. marchés financiers	-	EE ✓	EI ✓	-
Santé	Prestataires de soins de santé, recherche et développement & fabricants de médicaments, dispositifs médicaux d'urgence	EE ✓	EI ✓	-
Eau potable	Fournisseurs et distributeurs d'eaux	EE ✓	EI ✓	-
Eaux usées	Collecte, évacuation ou traitement des eaux usées	EE ✓	EI ✓	-
Infrastructures numériques	Points d'échange internet, services d'informatique en nuage, services de centres de données, réseaux de diffusion de contenu	EE ✓	EE ✓	-
Gestion de services TIC	Fournisseurs de services et de sécurité gérés	EE ✓	EI ✓	-
Espace	Exploitant d'infrastructures terrestres	EE ✓	EI ✓	-
		EE : Entité Essentielle | EI : Entité importante		
Infrastructures numériques	Services DNS, registres de noms de domaine de premier niveau, services de confiance qualifiés, réseaux de communications électroniques publics, services de communications électroniques accessibles au public	EE ✓	EE ✓	EE ✓
Administration publique	Pouvoirs centraux	EE ✓	EE	EE ✓
Administration publique	Niveau régional	EE ✓	EI ✓	EI ✓

Figure 2 : Secteurs NIS2 [7].

d'autorités nationale telles que l'ANSSI [2] en France ou d'associations professionnelles telles que ComptIA [3] en Amérique du Nord [3, 4, 5].

Des directives européennes imposent des règlementations contraignantes en gestion de données utilisateurs et cybersécurité pour les entreprises (RGPD [4], NIS [5]…) selon leur catégorie (EE Entité essentielle, EI Entité Importante) définies en fonction de leur degré de criticité, leur taille et leur chiffre d'affaires, et avec souvent des aspects spécifiques par secteur ou sous-secteur (figure 2).

Ces contraintes concernent la gouvernance et la formation, les mesures de gestion des risques, la notification des incidents (ce qui permet à l'ANSSI en France de constituer une base de données des vulnérabilités [6]). Ce dernier point de notification est essentiel, sachant que les entreprises attaquées naturellement ne communiquent pas pour ne pas dévoiler leurs points faibles.

L'analyse des vulnérabilités d'une entreprise impose une connaissance complète de l'architecture numérique de bout en bout de l'entreprise, pour en comprendre les vulnérabilités. C'est souvent difficile, du fait des silos historiques d'une entreprise, des activités sous- traitées, des interconnexions avec les sous-traitants, des relations numériques avec les clients, de la porosité vie entreprise / vie personnelle des salariés (par ex via le mail, ou le smartphone). Les cyberattaquants vont viser les points faibles de l'architecture numérique de l'entreprise. Ils vont exploiter une faille (par exemple un site web de l'entreprise dont la version n'a pas encore été mise à jour et qui est donc mal protégé…) pour s'introduire dans le réseau de l'entreprise et l'explorer de façon discrète afin d'y installer des *backdoors* [6] pour des utilisations futures.

Malgré la montée en puissance des menaces cyber, l'intrusion physique demeure un risque fort, qui mérite une attention importante. Il ne faut pas oublier que certaines cyberattaques peuvent exploiter des failles de sécurité physiques et que le ●●●

2 Agence nationale de la sécurité des systèmes d'information

3 Computing Technology Industry Association

4 Le règlement général sur la protection des données

5 NIS2 : directive européenne sur la sécurité des réseaux et de l'information (Network and Information Security Directive).

6 Portes dérobées numériques

facteur humain reste une des principales causes de vulnérabilité. Par exemple, l'intrusion physique sur un site industriel isolé pour ensuite entrer dans le réseau de l'entreprise. La prévention doit se faire globalement au niveau de la sécurité physique et logique des systèmes.

La prévention pour les nouvelles technologies numériques

L'émergence des nouvelles technologies fait apparaître de nouveaux risques de sécurité pour les entreprises qui les conçoivent ou les utilisent. Une nouvelle technologie mal conçue ou mal utilisée est susceptible d'introduire de nouvelles vulnérabilités pour l'entreprise. C'est pourquoi, certaines entreprises ont adopté depuis quelques années l'approche «*secure by design*» où tous les principes de sécurité, de protection, de réactions aux attaques… doivent être pris en compte dès le début du projet de conception d'une nouvelle technologie (cf. articles d'Orange et de Siemens). Mais ce n'est pas suffisant. Il faut aussi être capable lors de l'utilisation opérationnelle de la technologie de corriger rapidement les failles de sécurité qui apparaîtraient. Cela peut impliquer l'arrêt momentané de systèmes, et avoir des impacts sur des systèmes de production.

Le problème est particulièrement complexe pour les systèmes logiciels (cf. article sur la recherche). Les logiciels doivent être 'secure by design', faciles à corriger en cas de vulnérabilité ou de problème, en utilisant l'approche DevSecOps (figure 3). L'utilisation systématique d'Open Source auquel tout le monde, y compris des personnes malveillantes, peuvent contribuer, impose une approche stricte de vérification.

La généralisation assez récente de l'utilisation de l'IA apporte aussi son lot de vulnérabilités par exemple quand l'apprentissage est biaisé par des données corrompues, ou que des LLM [7] sont corrompus avec des *backdoors* (par exemple fuite de données sensibles, injection de contenus malveillants…).

A contrario, l'IA est un levier puissant de compréhension et d'analyse des vulnérabilités : intelligence, détection, génération de code plus sûr, utilisation de LLM spécifiquement entraîné pour les vulnérabilités spécifiques de sous-secteurs de l'industrie…

La détection des attaques

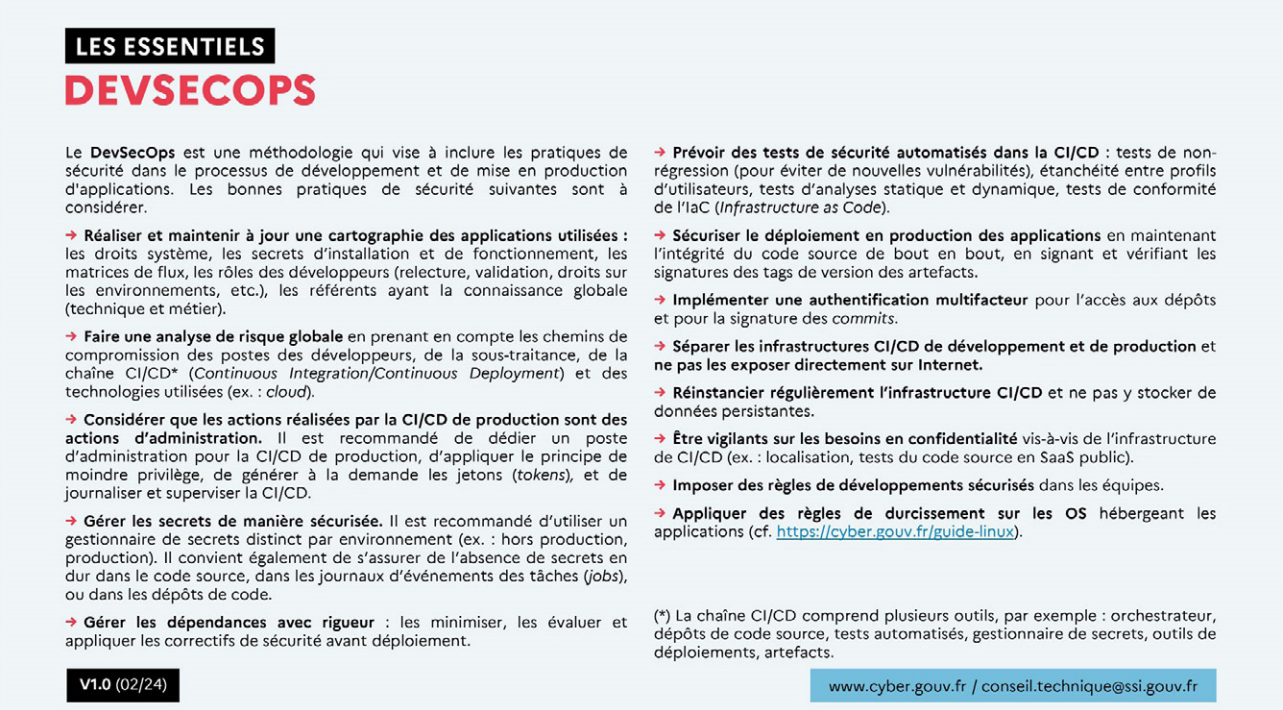
La détection des attaques doit se faire suffisamment en avance pour pouvoir se défendre et réagir. Elle se fait via un SOC (*Security Operation Center)* géré par l'entreprise ou partagé et infogéré par des sociétés spécialisées.

Le rôle d'un SOC est de savoir superviser des incidents de sécurité en se basant sur des bases de données de menaces connues à l'aide d'outils de type SIEM [8] (voir figure 4 exemples de quelques attaques).

Ces tâches sont souvent en dehors du cœur de métier de l'entreprise et sont, la plupart du temps, sous-traitées à des

7 Large Language Model

8 Security Information and Event Management



LES ESSENTIELS

DEVSECOPS

Le **DevSecOps** est une méthodologie qui vise à inclure les pratiques de sécurité dans le processus de développement et de mise en production d'applications. Les bonnes pratiques de sécurité suivantes sont à considérer.

→ **Réaliser et maintenir à jour une cartographie des applications utilisées :** les droits système, les secrets d'installation et de fonctionnement, les matrices de flux, les rôles des développeurs (relecture, validation, droits sur les environnements, etc.), les référents ayant la connaissance globale (technique et métier).

→ **Faire une analyse de risque globale** en prenant en compte les chemins de compromission des postes des développeurs, de la sous-traitance, de la chaîne CI/CD* (*Continuous Integration/Continuous Deployment*) et des technologies utilisées (ex. : *cloud*).

→ **Considérer que les actions réalisées par la CI/CD de production sont des actions d'administration.** Il est recommandé de dédier un poste d'administration pour la CI/CD de production, d'appliquer le principe de moindre privilège, de générer à la demande les jetons (*tokens*), et de journaliser et superviser la CI/CD.

→ **Gérer les secrets de manière sécurisée.** Il est recommandé d'utiliser un gestionnaire de secrets distinct par environnement (ex. : hors production, production). Il convient également de s'assurer de l'absence de secrets en dur dans le code source, dans les journaux d'événements des tâches (*jobs*), ou dans les dépôts de code.

→ **Gérer les dépendances avec rigueur** : les minimiser, les évaluer et appliquer les correctifs de sécurité avant déploiement.

→ **Prévoir des tests de sécurité automatisés dans la CI/CD** : tests de non-régression (pour éviter de nouvelles vulnérabilités), étanchéité entre profils d'utilisateurs, tests d'analyses statique et dynamique, tests de conformité de l'IaC (*Infrastructure as Code*).

→ **Sécuriser le déploiement en production des applications** en maintenant l'intégrité du code source de bout en bout, en signant et vérifiant les signatures des tags de version des artefacts.

→ **Implémenter une authentification multifacteur** pour l'accès aux dépôts et pour la signature des *commits*.

→ **Séparer les infrastructures CI/CD de développement et de production** et **ne pas les exposer directement sur Internet.**

→ **Réinstancier régulièrement l'infrastructure CI/CD** et ne pas y stocker de données persistantes.

→ **Être vigilants sur les besoins en confidentialité** vis-à-vis de l'infrastructure de CI/CD (ex. : localisation, tests du code source en SaaS public).

→ **Imposer des règles de développements sécurisés** dans les équipes.

→ **Appliquer des règles de durcissement sur les OS** hébergeant les applications (cf. https://cyber.gouv.fr/guide-linux).

(*) La chaîne CI/CD comprend plusieurs outils, par exemple : orchestrateur, dépôts de code source, tests automatisés, gestionnaire de secrets, outils de déploiements, artefacts.

V1.0 (02/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

Figure 3 : Approche DevSecOps ANSSI [8].

acteurs plus spécialisés comme Atos, Capgemini ou Orange Cyberdéfense. Par exemple, pour les jeux olympiques/paralympiques Paris 2024, le COJO a confié à Eviden (filiale d'Atos) cette supervision avec la coopération d'Orange et de Cisco (voir REE 2024-2).

Un SOC peut aussi faire de la prévention opérationnelle : tester et chercher des vulnérabilités en simulant des attaques (Pentest – test de pénétration), vérifier les configurations les droits d'accès, surveiller le bon format des actions internes de l'entreprise, en empêchant les données mal formées, en auditant les logiciels (virus…).

Des panoramas très détaillés des attaques cyber sur tous les secteurs de l'économie et de l'industrie sont publiés chaque année, citons par exemple les analyses suivantes d'Orange CyberDefense, de Dragos, de l'ENISA ou d'autres [9, 10 , 11, 12 , 13]. Des attaques spécifiques par domaine, tel que le domaine de traitement de l'eau [14] ou le domaine du transport du gaz naturel [15] apportent également des retours d'expérience sur la détection des attaques.

La cyberdéfense

La défense en cyber sécurité concerne, en premier lieu, la mise en place des réponses aux incidents de sécurité. Les incidents demandent des réponses d'urgence par exemple : mise à jour des pare-feux, interdiction de certains ou de tous les accès, patchs de sécurité… Par ailleurs, certains incidents amènent à des réponses d'ordre organisationnel et techniques pour résoudre les vulnérabilités structurelles découvertes avec les incidents.

Enfin, la cyberdéfense peut aussi concerner la gestion des crises cyber et l'accompagnement des autres parties de l'entreprise dont l'activité opérationnelle peut être sérieusement touchée. Cette gestion est très spécifique et doit être définie dans les plans de continuité et de restauration d'activité.

I Figure 4 : Exemples d'attaques [9].

En conclusion, il est essentiel pour une entreprise d'appliquer les bonnes pratiques de cybersécurité [16, 17, 18, 19, 20, 21, 22].

Le contenu du dossier

Le dossier vise à donner un éclairage sur l'état de l'art de la normalisation, les aspects télécom, les outils de production pour l'industrie et les systèmes d'information. Pour des raisons de confidentialité nous n'avons pas couvert des domaines sensibles plus spécifiques comme l'industrie automobile ou l'énergie.

Une meilleure cybersécurité intégrant des services de connectivité et de communication plus sécurisés.
Patrick Guyonneau,
Jean-François Audenard.

Orange, en tant qu'entreprise dite essentielle (EE Entité Essentielle) est une entreprise qui consacre une attention particulière à la sécurité et à la cybersécurité, d'autant plus que ses réseaux couvrent le monde entier. Cela commence par les bonnes pratiques de base en particulier dans le domaine humain notamment avec l'approche «*security by design*». La priorité absolue sur la sécurité de ses réseaux (infrastructures, liens d'interconnexion…) bénéficie naturellement aux services fournis à ses clients entreprises et résidentiels. Orange dispose à la fois de SOC (*Security Operation Center*) pour ses opérations internes, et de SOC à destination de ses clients pour traiter et réagir aux cyberattaques.

La protection des outils de production industrielle contre les cybermenaces, un enjeu majeur
Thomas Jauniaux

Les systèmes d'information IT (*Information Technology*) et OT (*Operational Technology*) convergent aujourd'hui grâce notamment aux réseaux. Les cybermenaces de l'IT se propagent aux environnements OT et peuvent donc impacter l'outil de production d'une entreprise industrielle. Par exemple, les outils de production peuvent aujourd'hui être maintenus à distance au travers de solutions de télémaintenance dont les flux passent par internet. Siemens en tant que fournisseur d'équipements et de solutions pour les systèmes d'informa- ●●●

tion de production (OT) a particulièrement renforcé les mesures de sécurité de ses propres usines avec une approche «*security by design*». Siemens propose également à ses clients des solutions et des services pour les aider à améliorer leur sécurité dans les usines.

L'évolution de la normalisation dans la cybersécurité
Antonio Kung, François Zamora, Jean Caire

Le besoin d'approches concertées contre les cyberattaques au niveau mondial ou au niveau d'un pays ont engendré un travail important au niveau de la normalisation et de la réglementation. Ceci est fait dans la perspective des menaces possibles et avérées. L'intérêt de cet article est d'une part de donner une vision assez complète des menaces possibles, et d'autre part de comprendre les évolutions nécessaires que les entreprises doivent mettre en place (certaines contraignantes, imposées par exemple par l'EU ou par la France). Ceci ne peut se faire qu'en connaissant l'architecture digitale de bout en bout de l'entreprise, avec des approches différentes selon les spécificités de chaque domaine.

Relations entre mondes industriel et académique pour la cybersécurité
Sébastien Canard, Hervé Debar, Adam Ouorou

L'article recommande aux mondes industriel et académique de travailler beaucoup plus en symbiose dans le domaine de la cybersécurité. En effet, l'utilisation par les industriels de technologies de plus en plus avancées (développement logiciel, virtualisation des services et des réseaux, IA …) rend de plus en plus difficile notre capacité à identifier les vulnérabilités modernes. Que ce soit en termes de développement sécurisé, de cryptologie ou d'utilisation de l'IA, le monde académique possède la compétence technique avancée pour les identifier mais aussi contrer les menaces sous-jacentes. Il n'est cependant que peu confronté directement aux attaques et ne bénéficie ainsi pas facilement des retours d'expérience. C'est le cas du monde industriel qui doit pour cela s'appuyer d'une part sur la recherche, mais aussi sur un pool d'étudiants diplômés rapidement opérationnels. Cela ne peut être possible qu'en montant des collaborations académique-industriel et en co-construisant les programmes de formation. Cela plaide pour une meilleure coopération entre les deux mondes. ■

Références

[1] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[2] https://www.silicon.fr/wannacry-2-0-renaultpas-seule-entreprise-touchee-france-174731.html
[2b] https://prod.ucwe.capgemini.com/wp-content/uploads/2023/11/CDC-External-Sales-Brochure.pdf
[2c] https://www.capgemini.com/fr-fr/perspectives/blog/cloud-et-cybersecurite-un-pas-de-deux-vers-la-maturite/
[3] https://cyber.gouv.fr/publications/guide-dhygiene-informatique
[4] https://cyber.gouv.fr/comprendre-la-certification
[5] https://en.wikipedia.org/wiki/CompTIA
[6] https://www.cert.ssi.gouv.fr/alerte/
[7] https://www.orangecyberdefense.com/fr/insights/blog/tout-savoir-sur-les-changements-de-la-nouvelle-directive-nis-2
[8] https://cyber.gouv.fr/publications/devsecops
[9] https://www.orangecyberdefense.com/global/security-navigator
[10] https://www.dragos.com/ot-cybersecurity-year-in-review/
[11] https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report
[12] https://blog.cloudflare.com/ddos-threat-report-for-2024-q2/
[13] https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/
[14] https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/
[15] https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/
[16] https://www.cisa.gov/stopransomware/ransomware-guide
[17] https://cyber.gouv.fr/guides-essentiels-et-bonnes-pratiques-de-cybersecurite-par-ou-commencer
[18] https://www.nist.gov/cyberframework
[19] A Zero Trust Based Framework For Accessing Data Securely : https://ieeexplore.ieee.org/document/9720872
[20] https://www.cisa.gov/securebydesign
[12] gestion des vulnérabilités https://www.yeswehack.com/fr
[22] Prévention et assistance en matière de cybersécurité https://www.cybermalveillance.gouv.fr

Les articles