WAVESTONE

RISKINSIGHT

LA LETTRE DES CONSULTANTS CYBERSÉCURITÉ ET CONFIANCE NUMÉRIQUE DE WAVESTONE

CYBERSÉCURITÉ ET DIRECTIVE NIS : L'UNION EUROPÉENNE FACE À UNE OBLIGATION DE COHÉRENCE

SOMMAIRE

EDITO

L'Europe de la cybersécurité, une opportunité à saisir aujourd'hui !

La directive NIS est une réalité depuis le mois d'août 2016. Cette directive pose les bases d'une Europe de la cybersécurité en mettant en avant l'enjeu pour chacun des pays de sécuriser ses propres infrastructures, mais aussi d'établir un cadre et un fonctionnement cohérent à l'échelle de notre continent. Cette cohérence doit passer par une harmonisation des postures et des pratiques de sécurité de chaque pays, une harmonisation nécessaire pour éviter que les grandes entreprise pan-européennes ne soient dans une situation réglementaire disparate qui disperse les efforts de mise en conformité.

L'histoire de réglementation sur la protection des données à caractère personnel le montre ; la directive est certainement une étape nécessaire avant un règlement européen, plus fort et plus marqué, mais qui doit se baser sur des premiers retours d'expériences concluants pour prendre forme. Notre conviction est qu'il faut prioriser dès aujourd'hui une mise en cohérence des principes de sécurisation à l'échelle européenne pour faire de NIS un succès. Nous détaillons ce point de vue dans notre dossier. Des réflexions sur un nouveau modèle de sécurité permettant d'aborder sereinement 2020, nos retours sur le sujets de la détection des incidents, les évolutions réglementaires à Hong Kong et une proposition pour la sécurité des voitures autonomes concluent le numéro de notre lettre Risk Insight.

Gérôme BILLOIS
Senior manager Cybersecurity & Digital Trust

CYBERSÉCURITÉ ET DIRECTIVE NIS : L'UNION EUROPÉENNE FACE À UNE OBLIGATION DE COHÉRENCE

La directive européenne NIS définit des mesures destinées à assurer « un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ». Pour ce faire, elle met en place un cadre formel de coopération sur la cybersécurité et impose aux Etats membres de renforcer leurs capacités nationales en identifiant leurs acteurs critiques afin de mettre en place des règles de sécurité et contrôler leur application.

Comme l'indique son nom, la directive NIS n'est ni une loi, ni un règlement. Elle donne un objectif à atteindre, mais laisse le choix des moyens pour y arriver. Comme pour toute directive, elle doit être transposée par chacun des pays membres en lois qui fixeront les moyens pour y arriver. La loi de Programmation militaire (LPM) française ou le IT Security Act allemand en sont des exemples. Pour qu'une diversité des mises en œuvre ne vienne pas nuire à une mise en œuvre efficace pour les entreprises pan-européennes, c'est bien un enjeu de cohérence qui attend les Etats membres et l'Union européenne d'ici 2018.

LA DIRECTIVE NIS : DÉCRYPTAGE

Contrairement à des textes comme le GDPR, la directive NIS opère une harmonisation minimale. Les Etats membres peuvent adopter ou maintenir des dispositions dans leur droit national pour atteindre un niveau de sécurité plus élevé que celui demandé par la directive NIS.

Établissement d'un cadre de coopération entre Etats membres de l'UE

A l'échelle européenne, la directive NIS institue un **Groupe de coopération** chargé de soutenir et de faciliter la coopération stratégique entre les États membres, notamment à travers l'échange d'informations et de bonnes pratiques. Ce groupe réunira la Commission européenne, l'ENISA - Agence européenne chargée de la sécurité des réseaux et de l'information - et les représentants des États membres.

Par ailleurs, la coopération se traduit par la mise en place d'un **réseau de CSIRTs** (*Computer Security Incident Response Team*), regroupant le **CERT-EU** et le **CSIRT** de chaque État membre dont l'existence est rendue obligatoire par la directive. Il est chargé de **promouvoir la coopération opérationnelle entre les États membres**. L'ENISA assurera le secrétariat de ce réseau et la Commission européenne aura un statut d'observateur.

Renforcement des capacités nationales de cybersécurité

Chaque État membre doit adopter **une stratégie nationale**, en définissant des objectifs et une législation appropriée dans le but d'atteindre un haut niveau de sécurité national.

Pour cela chaque pays doit se doter au moins d'une **autorité compétente**, chargée de la transposition de la directive en loi. Cette autorité peut être unique, comme c'est le cas en France avec l'ANSSI, ou peut être divisée selon les différents secteurs essentiels. Les dites-autorités sont invitées à se rapprocher de l'ENISA pour obtenir de l'aide. Un **CSIRT** national doit être désigné. En charge de la gestion d'incidents nationaux, il a pour mission d'alerter et de partager sur les risques et les incidents, et de reporter les notifications d'incidents aux entités adéquates.

Cette **gouvernance européenne de la cybersécurité**, résolument tournée vers la coopération entre instances européennes et États membres qui se décline au travers de la directive NIS est pour le moins inédite.

Sécurisation par chaque État de la cybersécurité de ses « Opérateurs de Services essentiels »

Les entités identifiées par les pays comme indispensables à la réalisation d'activités critiques doivent mettre en place des mesures pour appréhender les risques ainsi que leurs impacts. Ces opérateurs ont également l'**obligation de notifier immédiatement** à l'autorité compétente tout incident dont la nature pourrait impacter significativement la continuité, la disponibilité et l'intégrité du service. La notion d'impact, laissée à la libre évaluation de l'entité, dépend du nombre d'utilisateurs touchés, de la durée de l'incident et de la portée géographique.

Mise en place de règles européennes communes en matière de cybersécurité des fournisseurs de service numérique

La directive concerne aussi des acteurs nouveaux, rarement concernés par ces dispositifs : les « fournisseurs de service numérique » (hors TPE et microentreprises). Comprenez par-là, les entreprises qui

jouent un rôle important dans le secteur du numérique à savoir les moteurs de recherche (Yahoo, Google, etc.), le Cloud computing (Dropbox, Google Doc, etc.) et les sites de e-commerce (Amazon, e-Bay, etc.) ou encore les places de marchés en ligne. Leurs obligations sont légèrement moindres (règles spécifiques au niveau des Etats et obligation de notifications plus restreintes), comme leurs activités ne nuiront pas directement à la vie des personnes, mais plutôt à l'économie. C'est cependant un changement majeur pour ces acteurs qui sont aujourd'hui considérés comme essentiels pour le bon fonctionnement d'un pays et de son économie.

Quelle échéance de temps ?

Entre la date d'entrée en vigueur de la directive et sa déclinaison dans le droit national il faudra donc compter un délai de près de 2 ans.

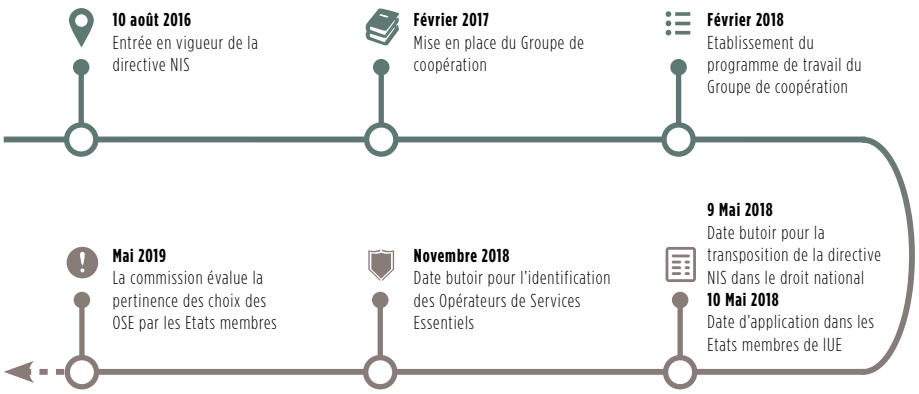
Cependant, même si la transposition dans le droit national est une échéance importante, ce n'est pas une finalité en soi. Au-delà de la déclinaison, se pose la question du délai jusqu'à une application effective des exigences auprès des opérateurs concernés. Celui-ci varie non seulement en fonction de l'état des lois en vigueur dans le pays mais aussi de l'approche retenue pour définir les mesures de sécurités. Un pays peut opter pour une approche collaborative avec les différentes parties prenantes qui se voudra donc plus chronophage qu'une simple application de bonnes pratiques de manière descendante.

QUELLES CONSEQUENCES POUR LES ENTREPRISES ?

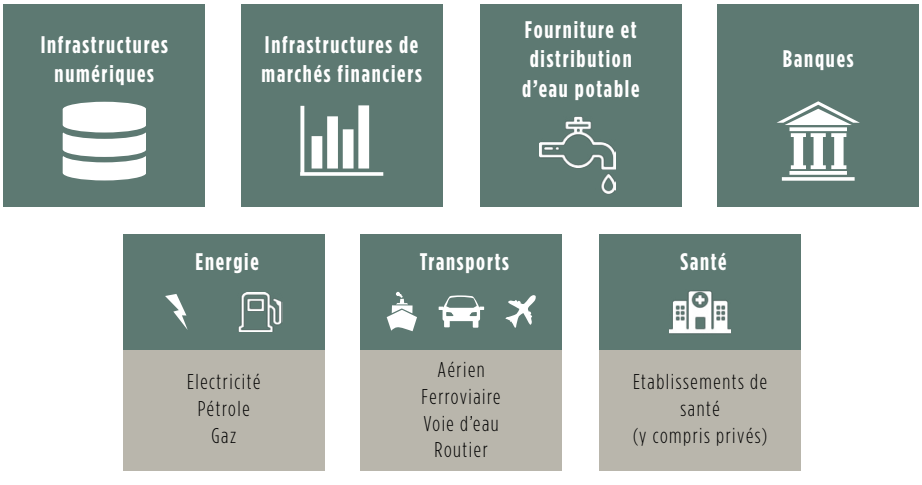
Une liberté d'implémentation par pays

La Directive s'adresse aux opérateurs publics et privés. Les entreprises concernées par

Déclinaison de la directive NIS



Secteurs retenus



l'obligation de sécurité sont celles ayant un rôle important dans la société et l'économie : les opérateurs fournissant des services essentiels (OSE). Les secteurs retenus sont les suivants : énergie, transports, banques, marchés financiers, santé, fourniture et distribution d'eau et infrastructures numériques.

Mais aujourd'hui chaque pays possède sa **liste propre**. Par exemple, la France en compte 12 dont ses « Activités militaires », les Britanniques en comptent 13 dont certaines très précises comme les « Gardes Côtes », la Pologne en compte 9 dont les « Systèmes ayant trait à la production, utilisation ou stockage des substances radioactives et pipeline ». Un travail de rationalisation et potentiellement d'identification de nouveaux acteurs sera nécessaire, en particulier les « fournisseurs de services numériques ».

Des principes et obligations fixés à défaut de mesures précises

Les obligations fixées par la directive en matière de cybersécurité des **opérateurs de services essentiels** sont plurielles.

Les opérateurs concernés doivent prendre des mesures appropriées pour prévenir les **incidents de compromission** de leurs réseaux et systèmes d'information. À cet égard, les autorités compétentes pour veiller au respect des obligations, peuvent demander des audits effectués par des organismes indépendants et donner des instructions contraignantes. Il incombe aussi aux opérateurs de prendre des mesures techniques et organisationnelles appropriées en matière de **gestion des risques** de sécurité.

Enfin, la directive prévoit une **obligation de déclaration** aux autorités compétentes en cas de piratage, d'intrusion dans les systèmes informatiques des OSE. C'est un changement majeur pour beaucoup de pays et d'acteurs dans le domaine de la cybersécurité.

La directive impose des actions similaires aux **fournisseurs de service numérique**. Leurs obligations sont légèrement moindres (règles spécifiques au niveau des Etats et obligation de notifications plus restreintes). Par ailleurs, ne sont concernés que les fournisseurs de service numérique relevant de la compétence d'un Etat membre. Celle-ci est reconnue lorsque s'y trouve son établissement principal. Si ce dernier se situe dans un Etat non-membre de l'UE mais qu'il fournit des services visés par la directive, il est alors qualifié de « représentant dans l'Union ». Il relèvera alors de la compétence de l'Etat membre dans lequel il opère ses services.

Dernier point marquant de la directive, c'est l'engagement de la responsabilité pénale des acteurs. Les Etats doivent en effet prévoir des sanctions effectives, proportionnées et dissuasives

En somme, la directive pose des principes et des obligations mais ne vient pas imposer des mesures de sécurité à proprement parler. Ce point sera à la charge des pays européens.

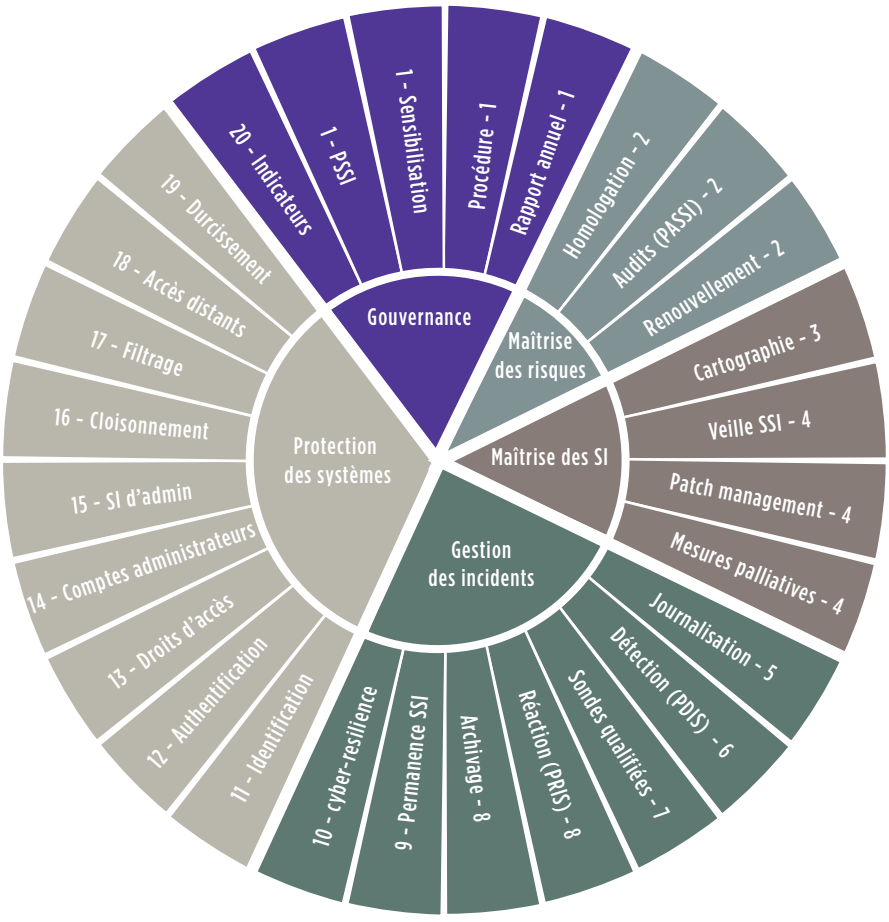
LA FRANCE, PIONNIERE, NOUS LIVRE UN PREMIER RETOUR D'EXPERIENCE

Un déploiement progressif sur 3 ans

Pionnière dans la mise en œuvre de règle de cybersécurité pour ses opérateurs d'importance vitale (OIV), l'équivalent des opérateurs de services essentiels de NIS, la France a intégré ces exigences dans la loi de Programmation militaire (LPM) suite aux orientations fixées par le Livre blanc sur la défense et la sécurité nationale 2013. La loi énonce des mesures relatives au renforcement de la protection et de la défense des systèmes d'information face aux attaques informatiques à des fins d'espionnage, de déstabilisation ou de sabotage. Elle constitue l'outil législatif qui permet aux opérateurs d'importance vitale (OIV) pour la nation, qu'ils soient privés ou publics, de mieux se protéger et à l'ANSSI de mieux les soutenir en cas d'attaque informatique.

Promulguée le 18 décembre 2013, les décrets d'application relatifs aux prestataires de service de confiance et à la sécurité des SI des OIV ne furent publiés que le 27 mars 2015. Les derniers arrêtés sectoriels ont été publiés et mis en application début décembre 2016. De plus il est important de noter que la LPM fait appel à des prestataires et produits qualifiés qui ne sont pas encore tous disponibles. L'expérience française donne donc à voir qu'au-delà d'une promulgation, les délais d'application

L'exemple français : 20 règles pour promouvoir les bonnes pratiques



peuvent être relativement longs. Il est à noter toutefois que la France a fait le choix d'une approche collaborative avec les OIV ce qui explique en partie les délais de déploiement.

Des règles précises et adaptées aux secteurs

Plusieurs exigences sont imposées : respect de règles de sécurité spécifiques, recours à du matériel et des prestataires qualifiés pour la détection des événements de sécurité, notification obligatoire des incidents de sécurité, contrôles de sécurité réguliers commandités par l'agence nationale de sécurité des SI (ANSSI). Les sanctions pénales applicables aux OIV lorsqu'ils ne satisfont pas aux obligations prévues s'élèvent à 150 000 € pour le dirigeant de l'OIV et à 750 000 € pour la personne morale.

Il est important de noter que les exigences portent uniquement sur les SIIV (systèmes d'information d'importance vitale), et non sur l'ensemble du SI de l'OIV. D'autre part, nos retours d'expérience sur l'identification des SIIV montrent que la logique « d'importance vitale » diffère entre une vision de l'entreprise (qui vise à assurer sa propre survie) et celle de l'État (qui vise à assurer la sécurité des citoyens). Concrètement, les systèmes commerciaux assurant les ventes ou la facturation, ne sont souvent pas répertoriés dans la liste des SIIV.

En matière d'organisation, la mise en conformité des OIV avec la LPM passe d'abord par une mesure des écarts entre l'existant et le requis. Il s'agit ensuite d'identifier les systèmes critiques et leur périmètre. En dernier lieu, l'OIV doit fournir le budget nécessaire à la mise en conformité. Les retours terrains montrent des budgets, dans un contexte de grande entreprise, allant entre 5 à 20 millions d'euros en fonction de la complexité et du nombre de SIIV.

Les directions générales impliquées

Force est de constater qu'aujourd'hui la LPM a réussi à mobiliser au plus haut niveau dans les entreprises. Elle est allée bien au-delà du périmètre classique de la cybersécurité devenant ainsi une réelle opportunité pour les RSSI de porter les enjeux sécurité jusqu'aux directions générales qui se sont saisies de ce sujet. Ce mouvement devra être confirmé à l'échelle européenne.

NIS, UNE INHERENTE OBLIGATION DE COHERENCE

Enjeu pour les grands comptes européens

La directive NIS **fixe un cap** à travers l'énonciation de principes et obligations. Pourtant, ce seront les pays membres qui auront la tâche d'identifier leurs secteurs critiques, leurs OSE, les fournisseurs de service numérique relevant de leur compétence ainsi que les mesures de sécurités qui en découlent. L'**harmonisation minimale** les laisse libre d'aller au-delà de la liste des secteurs fournie et de définir les exigences de sécurité. Mais en contrepartie d'un pays à un autre, les **obligations en matière de cybersécurité pourront donc varier** et ce… pour une même entreprise disposant de filiales dans différents pays européens. Une entreprise pourra également être identifiée comme un OSE dans un pays et pas dans un autre.

Il est donc primordial et absolument nécessaire que les acteurs concernés, qu'ils soient étatiques relevant des instances européennes ou du secteur privé, se saisissent dès aujourd'hui du sujet afin d'y apporter une cohérence. Sans celle-ci, la sécurisation des réseaux et des systèmes d'information européens pourrait devenir un réel **casse-tête** qui viendrait à l'**encontre même de l'esprit de la directive** : harmoniser à l'échelle européenne.

Le rôle clé de l'ENISA et de son évolution à venir

L'ENISA a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit en intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes, en **favorisant l'échange des bonnes pratiques** et en **facilitant les contacts** entre les institutions (nationales et européennes) et les entreprises. L'Agence européenne, via son rôle de facilitateur, a les **capacités d'apporter de la cohérence** dans les différentes stratégies nationales.

C'est d'ailleurs sur cette voie que se sont engagées plusieurs initiatives. Parmi celles-ci on notera le rapprochement de l'agence française (ANSSI) et allemande (la BSI) lors d'une réflexion sur la construction de l'Europe de la cybersécurité en janvier 2016. A noter aussi l'invitation de l'ANSSI par le gouvernement polonais lors du CyberGov forum en mai 2016 afin de partager les retours d'expérience français. Ces initiatives traduisent une prise de conscience des certains acteurs qui est plus qu'encourageante. Le défi reste donc la question de leur généralisation à l'échelle européenne et de leur capacité à voir émerger une Union européenne unie et harmonisée en mai 2018.

Gérôme BILLOIS
gerome.billois@wavestone.com

Étienne CAPGRAS
etienne.capgras@wavestone.com

Thibault JOUBERT
thibault.joubert@wavestone.com

Esther LYONNET
esther.lyonnet@wavestone.com

L'HEURE DU BILAN POUR LES SOC

De la création des premières équipes au début des années 2000 à la multiplication des initiatives pour répondre aux premières attaques ciblées dix ans plus tard, les équipes de sécurité opérationnelle ou SOC (Security Operational Center) doivent relever des challenges de plus en plus importants : détecter toujours plus efficacement et rapidement pour pouvoir réagir de manière appropriée.

À quelles difficultés font face ces équipes au quotidien ? Comment rester efficace alors que les attaques des cybercriminels deviennent extrêmement élaborées ?

LE SIEM : UN PILIER DU SOC… À CONDITION D'ÊTRE BIEN IMPLÉMENTÉ !

L'apparition d'outils comme le **SIEM** (*Security Information and Event Management*), il y a environ 10 ans, a permis aux équipes de sécurité opérationnelle d'**industrialiser** la surveillance en **simplifiant** l'analyse de multiples sources d'événements de sécurité (console antivirus, proxy, *Web Application Firewall*…). Cet outil a également rendu possible la corrélation de nombreux événements provenant d'équipements ou d'applications hétérogènes pour **détecter des scenarii de menaces avancés**.

Cependant, la mise en place d'un SIEM doit être le résultat d'un projet ayant un **investissement proportionnel à la complexité** du système d'information surveillé. En effet, la pertinence d'un SIEM repose à la fois sur :

- **La présence de contrôles contextualisés** au système d'information (notamment au travers de l'exploitation de la sensibilité des assets surveillés).
- **L'étude et l'implémentation de scénarii de menaces** avancés et adaptés aux enjeux du métier de l'entreprise.

Concernant le périmètre de surveillance, les premiers équipements habituellement intégrés sont les **équipements de sécurité** car ils sont nativement configurés pour laisser des traces exploitables pour les équipes opérationnelles. Il est néanmoins souvent constaté que leur intégration se limite à une **simple retranscription** des contrôles déjà existants ; ce qui ne permet pas de tirer parti de la corrélation d'évènements proposés par un SIEM.

En revanche, l'intégration d'applications métier est plus délicate en raison notamment des besoins différents entre les équipes métiers et sécurité : la principale préoccupation pour le métier se résume généralement à l'indisponibilité de son application (ou de certaines de ses fonctionnalités), alors que la sécurité adresse un **éventail de risques plus complet**, que ce soit de l'**indisponibilité**, de la **compromission** de l'**intégrité de données** ou encore de la **fuite d'informations** confidentielles.

Il s'avère donc primordial de **sensibiliser les métiers** aux enjeux sécurité dans leur ensemble pour pouvoir déterminer des scénarii de menaces réalistes et propres à chaque périmètre. De plus, ces applications n'ont traditionnellement pas de fonctionnalités avancées en termes de sécurité. Par conséquent, il est difficile de disposer d'un système de surveillance efficace (configuration d'envoi de logs complexe, fichiers de logs très peu verbeux…).

De manière générale, l'implémentation trop simpliste de contrôles dans un SIEM rend l'activité du SOC inefficace. Les équipes de surveillance se voient alors **noyées de « faux positifs »** et les évènements de sécurité sont traités unitairement au lieu d'être **analysés dans leur ensemble** afin de détecter de réels scénarii de menaces (par exemple : une authentification non autorisée sur un serveur puis la désactivation de son antivirus devra être traité comme un seul incident à investiguer).

DES ÉQUIPES PAS ASSEZ INTÉGRÉES DANS L'ORGANISATION DE LA SÉCURITÉ

Outre les problématiques liées à une mauvaise implémentation du SIEM évoquées ci-dessus, on constate également des problématiques d'ordre **organisationnel**.

En effet, le SIEM est souvent perçu comme une « boîte noire » par les analystes de niveau 1 et 2 au sein des équipes du SOC. Cela est généralement dû à la **méconnaissance** des problématiques réelles de production (identification des assets critiques, des interactions entre les différents systèmes…). Les incidents détectés par le SIEM se retrouvent alors tous traités au même niveau **sans aucune priorisation** et identification en amont des éléments les plus sensibles.

Pour maintenir un niveau de compétences suffisant au sein des équipes de sécurité opérationnelle, de la **veille technologique**

doit être réalisée par les investigateurs niveau 3 pour ensuite être communiquée aux analystes niveau 1 et 2. Des sujets tels que la **présentation de nouveaux IOC** (*Indicator Of Compromise*) venant compléter des règles de détection permettront aux équipes de gagner en efficacité dans leur manière d'appréhender les incidents. Ces types d'initiatives contribueront à l'**amélioration continue** du service en évitant sa dégradation dans le temps.

De plus, les équipes doivent **participer en continu aux nombreuses initiatives** sécurité initiées par la DSI telles que des projets de sécurisation des infrastructures ou applications. Par ailleurs, des **exercices de gestion de crise** doivent être organisés afin d'éprouver les différents processus et outils mis en place et de permettre aux interlocuteurs métier et sécurité de pouvoir échanger sur leurs rôles respectifs en cas de crise.

Dans un contexte où la cybercriminalité ne cesse de se réinventer (comme le démontre l'attaque sur les systèmes Swift récente), les équipes opérationnelles sont de plus en plus sollicitées pour intégrer de nouveaux périmètres. Cette **pression constante** exercée notamment par les décideurs accentue les phénomènes de **mauvaise implémentation des contrôles** et de méconnaissance des scénarii de menaces réels. Une bonne surveillance nécessite plus qu'un simple envoi de logs dans un SIEM ; les équipes projet doivent s'efforcer de respecter et faire respecter le processus complet d'intégration de nouveaux périmètres : identification des scénarii d'attaques, mise en place des mécanismes de collecte, création des règles de détection, tests et mise en production. L'oubli d'une de ces étapes risque de rendre la collecte des logs du périmètre inutile.

QUEL AVENIR POUR LES SOC ?

De nombreux facteurs vont venir bouleverser l'écosystème des prestataires de la sécurité opérationnelle.

En effet, la **LPM** (loi de Programmation militaire) va exiger de tous les OIV (opérateur d'importance vitale) de choisir des prestataires **certifiés PDIS** (Prestataires de Détection des Incidents de Sécurité), pour ceux qui font appel à de telles prestations externes. De nombreux prérequis seront nécessaires afin de pouvoir être certifié, tels que le **cloisonnement des données des clients** ou la **mise en place de zones d'administrations** (enclaves), uniquement accessible par le prestataire, par lesquelles les logs seront récupérés pour ensuite être transmis au SIEM. Ces facteurs vont entraîner de nombreux changements au sein des organisations et infrastructures mises en place actuellement.

Par ailleurs, la part grandissante du cloud dans les systèmes d'information des entreprises amène une nouvelle complexité : celle de la **collecte des logs auprès des fournisseurs**. De nouveaux acteurs sont donc apparus dans le marché de la sécurité : les **CASB** (*Cloud Access Security Brokers*). Leur promesse : répondre aux problématiques de sécurité pour le cloud. Ces entités se situent entre les utilisateurs et les divers services cloud et proposent de nouvelles briques de sécurité telles que l'utilisation d'API pour détecter directement des scenarii de menaces (création de fichiers de journalisation des accès aux applications, implémentation de ces données dans un SIEM…).

L'OBJECTIF DE DEMAIN : GAGNER EN MATURITÉ

La sécurité opérationnelle a encore de **nombreux défis à relever**. La plupart des entités assurent actuellement l'**hygiène minimum du système d'information** et la maturité des équipes leur permet de se prémunir des menaces diffuses (virus, spam…). Cependant, le dispositif actuel **doit se renouveler** afin de répondre aux nouveaux enjeux liés à la cybersécurité pour pouvoir lutter contre les **menaces opportunistes** (hacker isolé) et **ciblées** (cybermafia, gouvernement), plus complexes à détecter.

Dans ce contexte et face aux obligations légales, les SOC ont (et auront) un **rôle très important** à jouer nécessitant une **expertise technique approfondie** ainsi qu'une **intégration avec la sécurité dans les projets**.

Hamza KHARBACHI
hamza.kharbachi@wavestone.com

Hugo MORET
hugo.moret@wavestone.com

HONG KONG LANCE UN VASTE PROGRAMME DE CYBERSÉCURITÉ POUR SON SECTEUR BANCAIRE

Fin juin 2016, le système international de messagerie financière SWIFT annonçait des pertes considérables causées par les nombreuses cyberattaques dont il a fait l'objet. Les autorités de Hong Kong ont alors annoncé une nouvelle réglementation visant les institutions financières.

Au cours du Cybersecurity Summit de cette année, l'un des principaux événements de l'île autour de la cybersécurité, l'autorité des marchés de Hong Kong (Hong Kong Monetary Authority - HKMA) a annoncé le lancement du programme CFI, ou « CyberSecurity Fortification Initiative ». Il s'agit d'un plan pluriannuel visant à renforcer la sécurité des banques locales.

Voici les principaux points à retenir de cette initiative qui reprend les meilleures pratiques internationales en termes de cybersécurité, ainsi qu'une approche novatrice de la cyber *threat intelligence*.

UNE AMÉLIORATION DU NIVEAU DE SÉCURITÉ ARTICULÉE AUTOUR DE TROIS AXES

CFI est une initiative sur laquelle travaille la HKMA pour renforcer la cyber-resilience (i.e. la capacité à résister/survivre d'une cyberattaque) des organisations. Elle cible toutes les institutions autorisées *Authorized Institutions* (ou AIs), autrement dit l'ensemble des banques de Hong Kong et repose sur trois piliers suivants :

Un framework d'évaluation de la « cyber-résilience »

Chaque banque aura en charge le déploiement du framework sur son périmètre, ce qui permettra à la HKMA d'obtenir une vue globale du niveau de maturité des AIs individuelles ainsi que de l'ensemble du secteur bancaire ». Il se décompose en trois grandes étapes :

- **Évaluation des risques dit « inhérents »** : étude du niveau de risque de l'organisation sur les volets aussi bien métiers que technologiques - ce qui nécessite une bonne compréhension de ces deux domaines. Le niveau de risque sera évalué comme élevé, moyen ou faible.
- **Évaluation de la maturité** : une évaluation du niveau actuel de maturité de l'organisation en matière de cybersécurité
- **Simulations de cyber-attaques**, ou *Intelligence-led Cyber Attack Simulation Testing* (iCAST), pour les banques ayant un risque inhérent évalué comme élevé ou moyen. L'objectif de cette étape est de simuler les cyberattaques, non seulement d'un point de vue technique, mais aussi en prenant en compte les personnes et les processus.

Bien que tous les détails ne soient pas encore publics, les deux premières étapes rappellent l'outil FFIEC Cybersecurity Assessment Tool, mis en place par le régulateur américain, et qui a été déployé par de nombreuses grandes banques au cours de l'année passée. Une correspondance doit être faite entre le niveau de risque et le niveau de maturité réelle. En cas d'écart de ces deux indicateurs, la banque devra fournir une feuille de route pour le combler.

La troisième étape, elle, est plus innovante, en particulier de la part d'un régulateur. En effet, iCAST ne repose pas seulement sur des tests d'intrusion techniques, mais demandera aux banques de réaliser de véritables tentatives d'attaques, en s'appuyant notamment sur des données issues de la *threat intelligence*. Ce type de test « agressif » (aussi appelé « *Red Team* ») est l'un des moyens les plus efficaces pour tester le niveau de sécurité réel d'une organisation.

Un programme de développement professionnel

Le CFI vise également à professionnaliser le secteur de la cybersécurité à Hong Kong, en instaurant un système de certification et de formation offrant trois niveaux : « basique », « professionnel » et « expert ». Il est prévu que les certifications du CREST britannique intègrent ce programme de développement. Des équivalences seront par ailleurs mises en place pour « veiller à ce qu'une expérience ou une expertise dans le domaine de

la cybersécurité soit reconnue. ».

Une plateforme de partage CyberIntelligence

La *threat intelligence*, ou analyse des menaces, est devenue essentielle. Chaque entreprise peut développer ses propres compétences et méthodes, mais le succès même de l'approche passe par le partage de l'information. Par conséquent, la HKMA planifie de lancer une plate-forme de partage CyberIntelligence, accessible à toutes les banques agréées à Hong Kong. Son objectif sera d'offrir un système sécurisé et adapté pour partager des données pertinentessans compromettre la confidentialité des informations.

Quelles sont les prochaines étapes pour les banques ?

Trois étapes ont été fixées pour les banques à Hong Kong :

- **Une consultation du secteur bancaire** a commencé fin mai 2016 pour une durée de trois mois, afin de récupérer des retours sur la version préliminaire du framework de cyber-résilience.
- Il est important de noter que la HKMA requiert une **participation des conseils de surveillance ou de la direction générale** des banques. L'évaluation devra être menée par des « **professionnels qualifiés possédant les connaissances et l'expertise nécessaires** ».
- La HKMA travaillera avec les organisations professionnelles et publiques afin de **déployer les premiers cours de formation** et de **mettre en place de la plate-forme de partage** CyberIntelligence d'ici fin 2016.

L'ÉVOLUTION DES NORMES À HONG KONG

Cette initiative de la HKMA tombe dans un contexte réglementaire en rapide évolution à Hong Kong. Plusieurs approches susceptibles de changer la donne vont en effet y façonner l'avenir de la sécurité de l'information dans les années à venir.

En particulier, la circulaire récente sur la cybersécurité ciblant les organisations régulées par la Securities and Futures Commission (SFC), et la révision à venir sur les lois traitant des données à caractère personnel.

Avec près de 200 banques sur son territoire, Hong Kong se saisit ainsi pleinement du sujet de la cybersécurité, crucial pour maintenir sa position de centre financier de premier plan en Asie.

Chadi HANTOUCHE
chadi.hantouche@wavestone.com

LE MODÈLE DE SÉCURITÉ DU FUTUR N'EST-IL PAS CELUI D'UNE COMPAGNIE AÉRIENNE ?

Pour illustrer ses différentes approches, le monde de la sécurité s'est successivement référé à l'image du château-fort, puis de l'aéroport. Pour la prochaine évolution, l'image de la compagnie aérienne pourrait être utilisée.

Depuis des années, la filière cybersécurité tente d'expliquer simplement les concepts complexes qu'elle manipule tous les jours. Il s'agit d'un enjeu majeur pour convaincre les dirigeants, les métiers, ou tout simplement pour expliquer aux utilisateurs ce que fait la filière. Aujourd'hui, les systèmes d'information connaissent des évolutions majeures qui nécessitent de repenser la manière dont la sécurité est aujourd'hui déployée. Mais alors quelle image utiliser pour convaincre ?

DU CHÂTEAU FORT À L'AÉROPORT… MAIS APRÈS ?

En 2008, nous avions formalisé une première vision sur l'évolution des modèles de sécurité. Le modèle historique, celui reposant sur la sécurité périmétrique, était alors décrit par l'image d'un château-fort. Un château-fort avec des hauts murs normalement impénétrables (le périmètre), son pont-levis (le pare-feu), mais avec un cœur ouvert à tous (le réseau interne non cloisonné). Et puis, au fil des années, l'ouverture du SI est devenu un élément clé pour réussir la transformation digitale et autoriser certains usages innovants (cloud, BYOD…). Le château-fort s'est donc transformé en aéroport. Un aéroport ouvert par défaut, avec un hall permettant de récupérer des informations simplement ou de faire des achats. Mais un aéroport avec des zones sécurisées, comme le tarmac et les avions, protégeant alors les périmètres les plus critiques. Ce modèle permet d'ouvrir le SI tout en protégeant les actifs les plus critiques.

DEMAIN, UN SI DE PLUS EN PLUS DÉCENTRALISÉ

En analysant les évolutions actuelles, il est évident que le SI va encore fondamentalement changer. Le SI « interne » va se réduire et regrouper uniquement les périmètres historiques ou très critiques. Les fournisseurs externes et les clouds vont se multiplier et prendre une place prépondérante dans le SI. Ils échangeront directement entre eux des données et interagiront à plusieurs sur des traitements métiers complexes. Les terminaux consommant cette information vont se diversifier, avec les terminaux des clients, les objets connectés ou encore les terminaux personnels des employés. Les données vont donc circuler partout, sur des systèmes et des environnements sur lesquels il n'y a pas de contrôle direct.

UN MODÈLE INSPIRÉ DE CELUI D'UNE COMPAGNIE AÉRIENNE

Pour expliquer cette évolution, une autre image simple peut être utilisée. C'est celle de la compagnie aérienne. Aujourd'hui, une compagnie aérienne dispose d'avions. Ils sont l'équivalent des données de notre système d'information. Ces avions sont très critiques pour les compagnies, ils transportent les clients et les équipes de la compagnie aérienne.

Mais les compagnies aériennes font confiance à un écosystème complexe pour s'assurer que les avions arrivent à bon port ! Les aéroports accueillent les avions et les passagers comme un fournisseur de cloud peut accueillir des données et les traiter. Les aéroports sont capables d'accueillir des avions de plusieurs compagnies en garantissant la sécurité et la confidentialité, au même titre qu'un fournisseur cloud gère les données de plusieurs clients. Le contrôle aérien s'assure du fonctionnement global du secteur et de la sécurité des différents vols.

Quand une compagnie aérienne décide d'ouvrir une nouvelle ligne, elle évalue la sécurité du pays, de l'aéroport, avant de prendre une décision. Un processus nécessaire aussi avant de souscrire à des offres cloud. En fonction du niveau de sécurité du pays et de l'aéroport, la compagnie peut décider d'ajouter des mesures complémentaires de sécurité. Voir parfois de fermer temporairement des lignes en cas de changement brusque de contexte.

Surtout, une compagnie aérienne dispose d'un centre de contrôle opérationnel, qui va suivre et surveiller l'ensemble des vols, des avions, et s'assurer du niveau de sécurité des aéroports en fonction des informations qui lui remontent ou qu'il acquiert via les services de sécurité (*threat intelligence*). En cas d'incidents ou de crise, c'est le centre opérationnel qui va prendre la main et gérer la crise, imposant des mesures de sécurité nouvelles si besoin.

UN MODÈLE DIFFICILE À IMPLÉMENTER

C'est clairement ce modèle de « confiance dynamique », avec une évaluation des droits d'accès en fonction de la sécurité de ceux qui accèdent (terminaux, serveurs, personnes, etc.), avec la capacité à surveiller globalement les données où qu'elles soient et avec la capacité à pousser de nouvelles règles de sécurité dynamiquement, qui sera au cœur de la cybersécurité dans les années qui viennent. Ce modèle sera requis pour embrasser toutes les innovations à venir.

Ce modèle représente encore un défi, même si de nombreuses initiatives vont dans cette direction. Citons notamment le standard « software defined perimeter » de la Cloud Security Alliance ou l'initative « Beyond Corp » de Google. Une direction à suivre pour les années à venir. Et une image à garder en tête pour l'expliquer simplement.

Gérôme BILLOIS
gerome.billois@wavestone.com

CRASH TEST CYBER : LA SOLUTION POUR SÉCURISER LA VOITURE AUTONOME ?

Les voitures autonomes et connectées représentent le futur du secteur automobile et un vrai bouleversement dans nos habitudes de conduite au quotidien.

Mais les récentes démonstrations montrent que ces véhicules ne sont pas à l'abri d'une d'attaque cyber.

DES RISQUES BIEN RÉELS : LES EXEMPLES JEEP CHRYSLER ET TESLA

Une voiture autonome, c'est **par définition une voiture connectée** : GPS, capteurs, accès Internet par 3G/4G… Tous ces éléments sont autant de portes d'entrée vers une **voiture qui devient ni plus ni moins qu'un réseau où sont connectés des dizaines d'ordinateurs spécialisés**. Ces derniers sont en charge de gérer les différents composants du véhicule. Volant, frein, accélérateur, tous doivent être informatisés pour que le « cerveau » de la voiture autonome puisse les diriger.

La **combinaison de ces connexions externes et de l'informatisation des fonctions de conduites** pose aujourd'hui des **risques bien réels**. Pendant longtemps jugées théoriques, la capacité d'attaque des voitures connectées a été démontrée dans deux cas emblématiques. Le premier visait une Jeep Chrysler, a l'été 2015. Charlie Miller et Chris Valasek ont montré comment, après plusieurs années de recherche, ils ont pu prendre le contrôle du véhicule de série à distance. En aout 2016, ils ont montré qu'ils pouvaient aller encore plus loin dans la capacité à contrôler les fonctions de pilotage. Le deuxième a touché Tesla en septembre 2016, dans le même esprit une équipe de chercheurs chinois de Tencent a réussi à piéger une Tesla et à en prendre le contrôle intégralement.

Derrière, les **conséquences ont été lourdes** : impact sur l'image des constructeurs et surtout programme de rappel coûteux pour Jeep Chrysler via l'envoi de clés USB aux millions de clients concernés. Tesla, plus habitué à l'environnement cyber, disposait de moyens pour mettre à jour ces véhicules à distance et a réussi en une dizaine de jours à couvrir ces failles. À noter que ce délai est particulièrement court par rapport au contexte actuel des objets connectés.

UNE PRISE DE CONSCIENCE EN PROGRESSION

Ces **deux démonstrations ont fait prendre conscience au grand public et aux constructeurs des enjeux de la cybersécurité**. Beaucoup d'entre eux investissent et se renforcent sur cet aspect. Volkswagen vient par exemple d'investir pour créer la société Cymotive. Tesla a lancé historiquement un programme de « bug bounty » permettant aux chercheurs en sécurité d'être rémunérés s'ils trouvent des failles sur les véhicules, ceci pouvant éviter aussi que ces failles soient revendues sur les marchés noirs de la cybercriminalité.

LE CRASH TEST CYBER OU COMMENT BIEN CHOISIR SA VOITURE AUTONOME !

Tous les constructeurs ne sont pas au même niveau de prise de conscience et d'investissement. Mais alors **comment en tant que particulier choisir une voiture qui sera « cybersécurisée » ?** Aujourd'hui, au-delà de quelques papiers de recherche, il n'y a pas de moyens simples pour répondre à cette question. Il serait temps que les organismes en charge des crash-test, tels qu'EuroNCAP, s'empare du sujet et définissant des indicateurs de cybersécurité d'un véhicule ! **Quelques éléments simples peuvent permettre d'évaluer le niveau de sécurité** : niveau d'isolation des fonctions de pilotage de celles de connexion à Internet, capacité de mise à jour fiable et non bloquante, alerte du conducteur et du constructeur en cas d'attaque…

Gérôme BILLOIS
gerome.billois@wavestone.com

AGENDA

23.01.2017
HTCIA, Quel modèle de sécurité après 2020 ? (Hong Kong)

25-26.01.2017
Forum International de la Cybersécurité (Lille)

06.02.2017
CLUSIR PACA, Plier pour ne pas rompre (Nice)

Venez découvrir nos expertises
RISK INSIGHT
@Risk_Insight

Responsable de la publication : Frédéric Goux

Rédacteur en chef : Gérôme Billois

Contributeurs : Gérôme Billois, Etienne Capgras,
Chadi Hantouche, Hamza Kharbachi,
Esther Lyonnet, Hugo Moret,

Imprimeur : Axiom Graphics

ISSN 1995-1975

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods en dehors de France).

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.

Fort de 2 500 collaborateurs présents sur 4 continents, le cabinet figure parmi les leaders indépendants du conseil en Europe et constitue le 1er cabinet de conseil indépendant en France.