LE RADAR DU RSSI

ANTICIPER POUR MIEUX PRIORISER

Quelles priorités tirer du tumulte des sujets cyber ?

La cybersécurité ne cesse de se renouveler et pas un mois ne se passe sans qu'une nouvelle technologie ou une solution innovante émerge. Face à cette déferlante continue, il peut être difficile de distinguer les tendances de fond et de positionner sa stratégie cybersécurité. Face à ce constat, et depuis 2011, les équipes d'experts cybersécurité du cabinet Wavestone se réunissent régulièrement pour échanger sur les tendances du marché et identifier les thèmes matures, les sujets d'actualités et les technologies émergentes à explorer. Ce travail a permis la construction du radar du RSSI. Il a pour but d'accompagner le responsable de la cybersécurité dans un exercice de prise de recul, pour se positionner et prioriser ses actions au milieu de ce tumulte de sujets cyber. Cet outil est couramment utilisé par Wavestone et nos clients dans le cadre de réflexion stratégique comme la construction de schémas directeurs, lors de séminaire collaboratif avec des collaborateurs pour construire un radar spécifique à une entreprise ou à un domaine, ou encore pour identifier les solutions innovantes à tester via des démonstrateurs.

Cette publication présente le radar et propose un extrait des sujets que nous avons identifiés comme les plus importants pour 2018 parmi les 130 présents dans le radar du RSSI.

METHODOLOGIE

Le radar du RSSI est un outil développé par le cabinet Wavestone depuis 2011. Plus de 35 experts se réunissent 3 fois par an pour discuter des actualités et des sujets clés basés sur ce que nous avons pu observer chez les clients que nous accompagnons. Le radar du RSSI c'est chaque année plus de 130 sujets explorés et décortiqués par nos experts. Le radar contient une large sélection de sujets qu'un RSSI est amené à manipuler dans son activité. Il est organisé en cadrans délimitant des thématiques clés (identité, protection, détection, gestion des risques, conformité, continuité) sur 3 niveaux. Le niveau Mature correspond aux sujets que chaque RSSI peut et doit maitriser. Le niveau Actualité contient les sujets qui sont actuellement en train d'être adressés, il s'agit de sujets nouveaux où les premiers retours d'expérience peuvent être partagés. Le niveau Emergent contient les sujets à venir, encore peu connu ou pour lesquels ils n'existent pas de solutions évidentes. Ces sujets sont identifiés pour anticiper au mieux les évolutions futures et se préparer à leur arrivée dans les entreprises.

AUTEURS

GÉRÔME BILLOIS
Gerome.billois@wavestone.com

DOMINIQUE YANG
Dominique.yang@wavestone.com

Cette publication a été réalisée avec la contribution de l'ensemble des experts cybersécurité et confiance numérique du cabinet Wavestone.

LES SUJETS D'ACTUALITÉS CLÉS

Stratégie orientée CLIENT

Digitalisation, désintermédiation, disruption… Les clients deviennent de plus en plus volatiles. Ils doivent être séduits régulièrement par de nouvelles solutions et leur confiance devient un actif clé pour la transformation numérique de l'entreprise. Et les clients deviennent plus attentifs à la cybersécurité, sensibilisés par les incidents à répétition relayés par les médias ou par les évolutions réglementaires qui leur rappellent leur droit sur ces données (accès, sécurité, portabilité…).

Le responsable de la cybersécurité ne doit donc plus uniquement s'occuper de « son » informatique et de « ses » données. Mais il doit de plus en plus se focaliser sur les clients de son entreprise. Il s'agit d'évaluer leurs attentes en matière de sécurité et de leur proposer des fonctionnalités pour assurer la sécurité des données confiées, simplement et efficacement.

Ce changement de posture nécessite de franchir une étape de plus pour le RSSI, celle de connaître les clients de l'entreprise. Les démarches les plus innovantes que nous avons vues peuvent aller jusqu'à réaliser des sondages auprès de clients finaux pour connaître leurs attentes et imaginer de nouveaux services. Ou encore la proposition de services de sécurité intégrés aux offres de l'entreprise avec ou sans surcoût.

Il est important que le RSSI soit mobilisé pour participer à la construction des discours clients et des parcours clients et qu'il y participe dans une logique facilitatrice pour les clients, et pas uniquement dans une approche sécuritaire jusqu'au-boutiste. Les RSSI d'offreurs de service numérique ont souvent pris de l'avance ! Eux sont confrontés aux questions des clients dans les processus d'appels d'offres depuis longtemps, ce qui n'est pas le cas dans beaucoup d'autres secteurs.

Adopter une stratégie centrée « client » permettra de mettre en lumière concrètement les apports des travaux de la filière SSI dans la fourniture de nouveaux services et dans la protection des intérêts des clients.

Cyber-résilience & Fast IS rebuilding

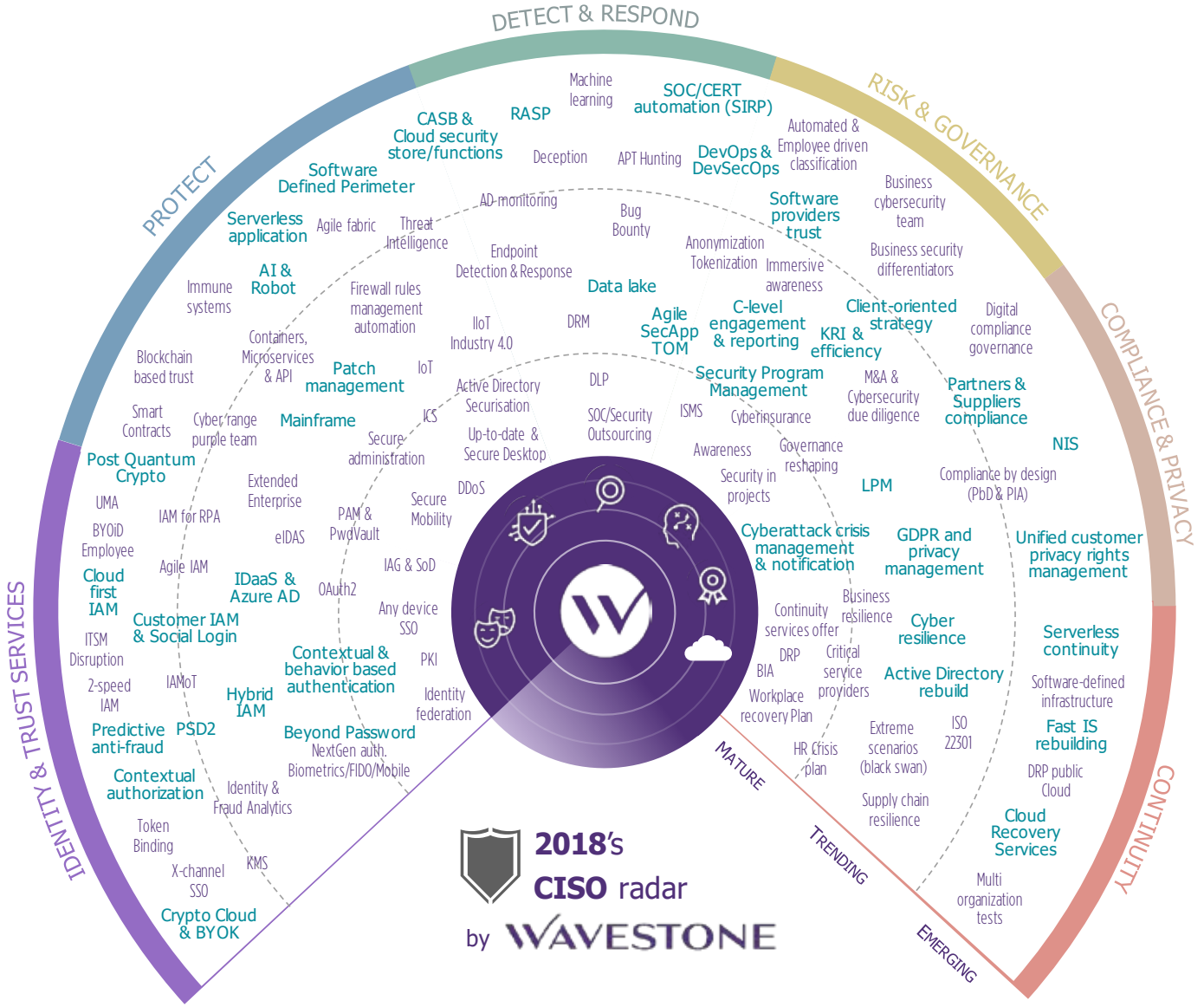
Wannacry et NotPetya ont démontré la capacité d'un malware à détruire en quelques heures des pans entiers de systèmes d'information avec des impacts financiers se chiffrant en centaines de millions de dollars pour les entreprises touchées. Cette menace destructive était jugée souvent théorique jusqu'alors. 2018 devrait être l'année de la définition des stratégies de cyber-résilience dans les grandes entreprises. Deux grands types d'actions sont à prévoir. Le premier vise à limiter l'occurrence de ce type d'attaque en s'assurant de l'hygiène sécurité de base et en particulier en adressant en profondeur le sujet toujours très complexe du *Patch Management*. Il s'agit aussi d'adresser la sécurisation des fournisseurs (*Partners & Suppliers Compliance*). Il est important de noter que NotPetya a pu se répandre initialement par le piratage d'un fournisseur de logiciel tiers (MeDoc) qui est devenu un cheval de Troie pour réussir à entrer facilement dans le *SI* (*Software Providers Trust*). Il s'agit d'une technique d'attaque à prendre en compte aujourd'hui dans l'évaluation de la menace. Le deuxième type d'actions vise à savoir gérer une crise de ce type et surtout à se préparer à reconstruire très rapidement son SI en cas d'attaque réussie (*Fast IS rebuilding / AD rebuild*).

Conformité : RGDP, LPM, NIS, DSP2

2018 marquera un tournant pour le sujet de la conformité avec l'entrée en application de plusieurs textes dont le Règlement Général sur la Protection des Données à caractère personnel. Au-delà du *RGPD* et des textes spécifiques à des secteurs comme *DSP2*, c'est en effet l'arrivée de la directive *NIS*, sa déclinaison en droit français et la future identification des OSE en France en novembre 2018 qui prendront le relais sur le sujet réglementaire. Ce sujet, européen par essence mais décliné nationalement, pourra aussi avoir des impacts importants quant à la localisation de certains services numériques. En effet les exigences et des règles de sécurité étant potentiellement différentes entre les pays européens, il faudra être attentif à ne pas voir se profiler un « dumping cybersécurité ». En France, les OSE déjà identifiés comme opérateurs d'importance vitale, OIV, dans le cadre de la *LPM* devraient être moins impactés. En effet, la *LPM* impose déjà de nombreuses obligations exigeantes (y compris sur des périmètres historiquement peu adressés comme la sécurité du *Mainframe*) dont les efforts de mise en œuvre, en cours, ne devraient pas concurrencer la mise en conformité à la directive *NIS*. Toutefois, il est à noter que le périmètre de la directive est susceptible d'être plus large que celui de la *LPM*, ceci pouvant entraîner l'ajout de nouveaux systèmes dans les périmètres sécurisés.

Intelligence Artificielle

L'intelligence artificielle aura certainement été LE buzzword de 2017. Mais sur le terrain les technologies de *Machine Learning* font leurs preuves et apportent des résultats tangibles. C'est particulièrement vrai pour la lutte contre la fraude sur les canaux numériques (*Predictive anti-fraud*). Vu les volumes et les exigences de réactivité, ces technologies (*Data Lake*) apportent des solutions là où les méthodes classiques atteignent leur limite. La gestion de l'authentification est un autre domaine qui peut profiter de ces avancées avec la mise en œuvre de système biométrique (*Beyond Password*) et/ou qui adapte dynamiquement le niveau d'exigences en fonction des actions de l'utilisateur (*Contextual & Behavior based Authentication / Contextual Authorization*). Toutefois ces technologies ne sont pas encore complètement matures sur des sujets de surveillance cybersécurité mais 2018 devrait voir des avancées majeures dans ce domaine. Et sans attendre immédiatement des solutions automatisées (*SOC/CERT automation*) de bout en bout, réaliser des premiers tests sur l'apport de l'intelligence artificielle dans la gestion d'un incident et dans sa résolution peut permettre de défricher le sujet.



C-level engagement & reporting

2017 a marqué un réel changement de dimension dans les relations entre la filière cybersécurité et les comités exécutifs. Dans près de 25% des groupes du CAC 40, des programmes massifs de sécurisation sont en place avec des investissements supérieurs à 50M€ (*Security Program Management*). Ces programmes sont suivis directement par les membres de la direction générale. C'est un vrai changement de posture pour la filière SSI qui va devoir en 2018 montrer l'efficacité des actions réalisées avec ces budgets (*KRI & efficiency*). Et la tâche n'est pas simple dans un contexte où les compétences manquent et doivent être fidélisées mais aussi où une faille remplace l'autre et où une stratégie peut être remise en cause avec un incident majeur. Un fort travail de pédagogie et une démonstration de maitrise des risques seront nécessaires. Pour ceux qui n'ont pas encore franchi la porte du COMEX, le contexte actuel n'a jamais été aussi propice à mettre en lumière ce sujet. Certes les incidents, de plus en plus relayés médiatiquement et avec des impacts financiers majeurs, peuvent aider. Mais c'est surtout les investissements comparativement réalisés dans d'autres grands groupes qui peuvent être un déclencheur. 2018 sera l'occasion pour beaucoup de monter un vrai programme et d'aller chercher les financements nécessaires pour transformer la cybersécurité.

Cloud

Le déploiement des services cloud est aujourd'hui une réalité. Le SaaS est largement répandu et requiert, au-delà de la confiance requise envers le fournisseur, une réflexion sécurité sur la gestion des comptes à privilèges et sur la gestion des identités, des accès des utilisateurs et du partage des données. Le responsable de la cybersécurité peut être aidé des *CASB* (*Cloud Access Security Brokers*) pour gagner en visibilité sur les services utilisés et mieux les sécuriser. Si le *CASB* est émergeant, il tend aussi à se rapprocher des solutions de IDaaS (Azure AD) où la gestion de l'identité et des accès est gérée ou co-gérée dans le Cloud. On parle aussi de *Hybrid IAM*

ou encore de *Cloud First IAM.* D'autre part les déploiements s'orientent aujourd'hui vers le IaaS avec l'utilisation grandissante des solutions d'Amazon ou de Microsoft entre autres. Leur mise en œuvre requiert une refonte en profondeur des modèles de sécurité et des réflexions sur des sujets émergeants comme le *Crypto Cloud*, qui concrétise le principe du *Bring Your Own Key*, ou encore le *Cloud Recovery Services*, qui met le Cloud au service de la cyber-résilience en fournissant une solution de continuité dans le Cloud en cas d'indisponibilité des applications.

LES SUJETS ÉMERGEANTS À SUIVRE

Serverless / Serverless continuity

Le *Serverless* est un nouveau paradigme Cloud qui vient se greffer entre le IaaS et le SaaS, assez proche du PaaS, qui vise à donner la possibilité de publier du code directement sur les plateformes Cloud sans avoir à se préoccuper du maintien en conditions opérationnelles et de sécurité des infrastructures sous-jacentes : les développeurs n'ont plus à se soucier du provisioning des serveurs et n'ont plus besoin d'accéder au niveau du système d'exploitation. Ce changement de paradigme doit être suivi par les équipes de sécurité opérationnelle pour adapter les procédures et leurs analyses afin de s'assurer que les fournisseurs de services Cloud apportent un niveau de sécurité approprié, en particulier pour réaliser la surveillance de ces systèmes. En effet, ils rendent encore un peu plus aveugle les équipes en charge de la surveillance. La question de la continuité d'activité, *Serverless continuity*, est aussi prégnante. Il est nécessaire de repenser les capacités de continuité d'activité dans un environnement où le client n'a plus la main sur les sauvegardes au niveau système et où la continuité doit être applicative, voir multi-plateformes.

Runtime Application Self-Protection

Le RASP est une technologie de sécurité qui est intégrée dans une application ou dans un environnement d'exécution dans le but de détecter et protéger l'application des attaques en temps réel via de l'analyse dynamique. Le *RASP* permet de translater la sécurité d'une couche supplémentaire au plus près de l'application et de ses données. Aujourd'hui, c'est un sujet adressé par les startups comme le canadien Immunio, très récemment acquis par *Trend Micro*, *Tcell* ou *Prevoty* aux Etats-Unis ou encore *Sqreen.io* en France.

Unified Customer Privacy Rights Management

Au-delà d'introduire la notion de portabilité, le règlement européen vient aussi renforcer les obligations concernant le recueil du consentement. Ces deux aspects peuvent être adressés par le *Unified Customer Privacy Rights Management* qui se traduit notamment par une plateforme ou interface unique pour l'accès aux données personnelles des clients. Ces solutions émergentes sont à surveiller avec en parallèle les plateformes de Customer IAM (*CIAM*) qui peuvent apporter plus de richesses fonctionnelles.

Software-defined Perimeter & Automation

Le *Software-defined Perimeter*, ou *SDP*, correspond à une série de technologies de sécurité qui permet d'introduire de l'agilité et de l'automatisation dans la sécurité. En effet, l'essor du Cloud et de l'agile accélère les cycles de déploiement et déprovisionnement de systèmes ou de services, parfois même en temps réel. Ces évolutions requièrent que la sécurité soit capable de suivre le rythme. En introduisant de *l'automation* et en apportant plus de granularité dans la segmentation du SI, le SDP va uniquement donner accès aux ressources nécessaires et suffisantes pour que le service puisse fonctionner ou que l'utilisateur puisse effectuer l'action souhaitée. Des premières initiatives existent chez Google « BeyondCorp » ou au niveau de la Cloud Security Alliance avec les produits de la startup Vidder.

Post Quantum Crypto

Le *Post Quantum Crypto* représente les nouvelles solutions techniques de chiffrement à prendre en compte en prévision de l'arrivée à maturité des capacités informatiques quantiques qui vont rendre possible la cryptanalyse sur les algorithmes de chiffrement considérés robustes aujourd'hui, comme RSA par exemple. Les géants du net, comme Google ou Microsoft, commencent à s'intéresser au sujet avec des premiers travaux sur des algorithmes de chiffrement résistants aux attaques quantiques. Le NIST, quant à lui, a débuté les travaux dès 2016 et espère publier de premiers résultats d'ici 2023-2025.