WAVESTONE

LE RSSI AU CŒUR DE LA RÉVOLUTION DU SI

TENDANCES 2019 ET RADAR DU RSSI

Quelles priorités tirer du tumulte des sujets cyber ?

La cybersécurité est en constant renouvellement : évolution des menaces et des réglementations mais aussi renouvellement profond du fonctionnement des systèmes d'information. Devant ces nombreux changements, il peut devenir complexe de distinguer les tendances de fond et de positionner sa stratégie cybersécurité en conséquence. Face à ce constat, 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'actualité et les technologies émergentes à explorer. Cette année, les réflexions ont permis une analyse approfondie des grands axes de la révolution à venir, de ses enjeux pour les filières cybersécurité et, comme chaque année, l'actualisation du radar du RSSI. Cet outil est couramment utilisé par Wavestone et nos clients dans le cadre de réflexion stratégique comme la construction de schémas directeurs, lors de séminaires collaboratifs 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 2019 parmi les plus de 120 présents dans le radar du RSSI.

MÉTHODOLOGIE

Le radar du RSSI est un outil développé par le cabinet Wavestone depuis 2011. Plus de 40 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 120 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 connus ou pour lesquels il n'existe 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

DAVID RENTY
david.renty@wavestone.com

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

LES SUJETS D'ACTUALITÉ

Agilité : plus réactif, plus rapide, plus simple

Les grandes entreprises ont démarré, parfois à marche forcée, des migrations vers un fonctionnement agile à grande échelle. Face à cette transformation, le RSSI doit s'approprier ces méthodologies et travailler de façon rapprochée avec les équipes de développement pour qu'elles se saisissent des enjeux de la cybersécurité. Dans un premier temps, ce rapprochement permettra l'intégration de la sécurité dans les projets agiles par le biais d'*Evil User Stories*, de formation des équipes à la sécurité, de mise en œuvre d'outils d'intégration continue et d'intégration de tests d'intrusion dans le cycle de développement. Ce mouvement est déjà bien entamé avec des premiers accompagnements réussis.

Au-delà de l'intégration de la cybersécurité dans les projets agiles, c'est la cybersécurité qui devra prendre le tournant de l'agilité en s'intégrant dans un nouveau modèle opérationnel. Non seulement les équipes cybersécurité s'inscriront dans cette organisation agile en rejoignant les *Feature Teams* pour donner de la visibilité au RSSI sur les risques identifiés dans ces projets, mais elles seront également capables de fournir des services de sécurité en mode agile. Des *Product Owners* portant des services de sécurité apparaîtront pour délivrer de la cybersécurité *as a service* au sein de l'organisation.

Cloud : sécurisés par défaut, multiples, automatisés

En 2019, l'addition des premiers déploiements importants déclenchera une réaction en chaîne vers le *Cloud-first*, voire pour nos clients les plus avancés le *Cloud-Only*. Au-delà des applications, un mouvement naissant de migration des infrastructures est entamé, y compris pour des composants clé comme l'*Active Directory.*

Toutes ces avancées impliqueront un changement de métier des DSI. Dans ce contexte, le RSSI devra s'adapter à ce nouveau modèle opérationnel afin de s'assurer du maintien de la sécurité des configurations dans le temps et d'ouvrir le dialogue avec ses nouveaux interlocuteurs. Il pourra encourager l'utilisation des nouvelles capacités d'autoremédiation et de reconstruction des systèmes en cas d'incident de sécurité.

Cette situation nécessitera des adaptations pour fournir un haut niveau de maîtrise sur l'administration de la gestion des droits et la surveillance du SI. Dans un contexte où les infrastructures sont gérées par le fournisseur, les efforts devront se focaliser sur ces 3 piliers. La sécurité devra être intégrée dès la conception des nouvelles architectures et s'appuyer sur les briques des fournisseurs. Les droits pourront être attribués de façon granulaire pour limiter les risques d'accès illégitime aux ressources. Ils devront être revus de manière automatisée pour s'adapter aux changements fréquents.

Le *cloud*, c'est aussi un virage à prendre pour les filières sécurité : le RSSI sera en première ligne pour adopter et tirer le meilleur parti des offres du marché : analyse de vulnérabilités, contrôle d'accès, MFA, *Identity Governance*, filtrage de contenu… nombre de ces services disposent déjà d'une offre crédible dans le *cloud*.

A moyen terme, le *multicloud* basé sur deux fournisseurs doit être envisagé pour permettre la continuité des services.

API-fication : de multiples nouvelles portes d'entrée pour le SI

Poussée dans le secteur financier par la réglementation DSP2, l'*API-fication* touche tous les secteurs et permet de faire interagir des services en standardisant les moyens d'échanges de données.

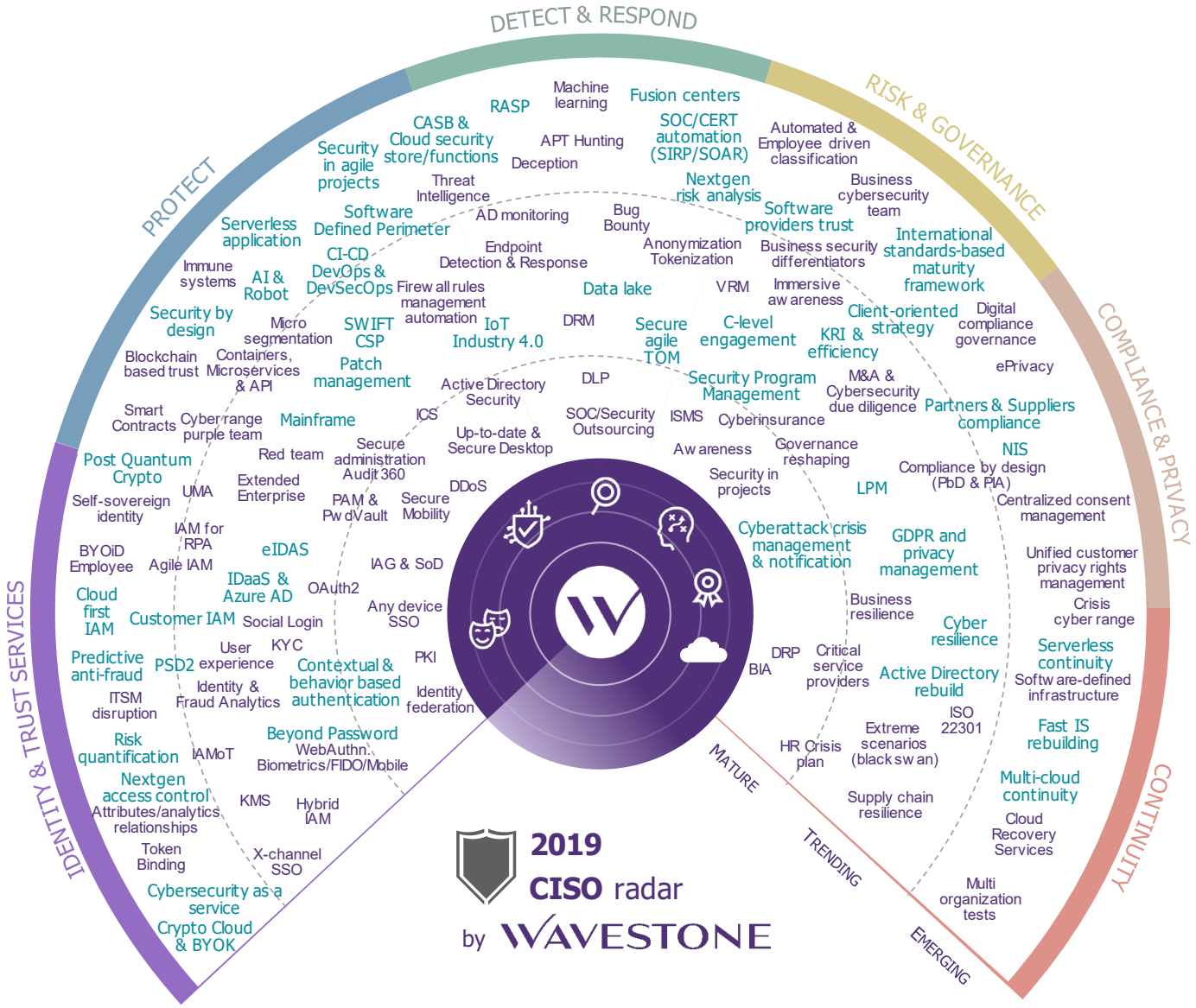
Nous constatons chez nos clients les difficultés de la filière sécurité à maîtriser ce nouvel enjeu. Si l'*API-fication* pourra être un levier pour faciliter la sécurisation des échanges machine à machine par l'uniformisation, le chiffrement ou l'authentification, elle présente certains risques liés à leur multiplication et leur large surface d'exposition. En effet, même de grands acteurs comme Google ou Facebook parviennent difficilement à maîtriser ce sujet comme l'ont montré les incidents de 2018.

Si le RSSI veut reprendre le contrôle sur l'*API-fication* des services, il doit, dès maintenant, investir ce théâtre d'opération avec tous les moyens existants, y compris les plus innovants. Il ne pourra pas se contenter de simplement définir une gouvernance ou tenter, dans un premier temps, d'inventorier les API exposées ; il devra anticiper et être en mesure de surveiller et contrôler un grand nombre d'API.

Une révision des fondamentaux

Révolution profonde du SI, réglementations toujours plus présentes et aux sanctions exponentielles ; comment les filières sécurité peuvent-elles sortir de l'étau qui les enserre ? Pour y parvenir, nous identifions 2 grands chantiers portant sur nos fondamentaux :

- Refondre la PSSI et la gouvernance. Elles devront être revues sur la base de la stratégie sécurité existante. Pour accélérer et cadrer la démarche, le RSSI pourra s'appuyer sur le *cybersecurity framework* du NIST, un référentiel cybersécurité américain en passe de devenir incontournable pour les grands groupes de tous secteurs.
- Revoir en profondeur les processus d'intégration de la sécurité dans les projets. Après avoir été amendés en 2018 pour les besoins du RGPD, ils devront être repensés dans le but de gagner davantage en agilité et en flexibilité. Les autorités ont rejoint ce mouvement, l'ANSSI ayant modernisé la méthodologie d'analyse de risques EBIOS, nouvellement nommée EBIOS *Risk Manager* par une approche combinant conformité et scénarios d'attaque.



AU-DELÀ DE LA REFONTE DES FONDAMENTAUX, NOS 5 PRIORITÉS POUR LES FILIÈRES SSI

- **La cyber-résilience bâtie sur le cloud : l'évolution des solutions permet d'envisager d'utiliser le cloud comme solution de continuité face aux cyberattaques comme c'est déjà le cas pour la messagerie.**
- **Les *Fusion Centers*, les futurs SOC : ils regroupent des savoir-faire techniques et métiers, permettant d'appréhender de bout en bout d'éventuelles fraudes ou intrusions dans le système d'information et de réagir au mieux.**
- **La fin des mots de passe : des initiatives comme le *0-password*, le déploiement de FIDO2, la biométrie dans le cadre du 2FA ou encore la généralisation des coffres-forts permettent de l'envisager.**
- **L'IA et le *machine learning* : ces technologies représentent des opportunités à moyen terme. La priorité de 2019 sera cependant de s'assurer de la prise en compte des risques et vulnérabilités spécifiques (inférence, empoisonnement…) dans les projets métier incluant de l'IA.**
- **Les tiers et les fournisseurs sous microscope : de nombreuses attaques sont aujourd'hui observées sur les fournisseurs, ce qui n'entache pas moins l'image de la société cliente qui reste responsable. Il y a un besoin, en 2019, de mieux cartographier les interactions avec les prestataires afin d'évaluer la sécurité de ceux-ci. C'est un travail complexe vu leur nombre, leur diversité et leurs imbrications.**

LES SUJETS ÉMERGENTS

Anticiper et s'adapter à une pénurie de talent récurrente.

Il n'existe pas de solution magique mais une multitude de pistes à tester pour faire face à la pénurie de compétences. D'un point de vue technique, l'automatisation, la migration vers le cloud, l'instauration d'un cadre fort instaurant les principes de *security by design* permettront des limiter les efforts. De même, la création d'offres de services sécurité, le *near* voire *offshoring* pour des services standardisés peuvent être des solutions.

Pour relever les défis de demain, le RSSI devra donner une nouvelle dynamique à la filière sécurité en créant un environnement stimulant, ambitieux et formateur permettant *l'empowerment* (ou « autonomisation ») des équipes. En ayant comme objectif de créer des vocations et des envies de mobilités internes.

Faire de la sécurité un différenciateur vis-à-vis des clients de l'entreprise

La sécurité a souvent été perçue comme une contrainte. En 2019, la sécurité ne pourra pas se contenter d'être une ligne de défense essentielle dans toute entreprise et devra être vue comme génératrice de valeur pour le *core-business*.

Ce changement concerne quasiment tous les secteurs d'activité. Le secteur bancaire s'est engagé sur cette voie avec la mise en place de systèmes de double authentification, de cryptogramme dynamique, de notification en cas de mouvements suspects… D'autres secteurs devront suivre rapidement :

- L'automobile, avec la sécurisation « visible » du véhicule connecté, avant de passer au véhicule autonome demain ;
- Les opérateurs télécom, dont certains promeuvent leur nouvelle box avec des services de cybersécurité comme la détection de vulnérabilités ;
- Les fournisseurs de services au grand public (transport, énergie, eau…) où la cybersécurité est requise dans les processus de vente et peut être un différenciateur.

Ainsi, sous l'impulsion du RSSI, la filière sécurité doit saisir ces opportunités pour se rapprocher des métiers et montrer son apport dans le cœur de l'activité de son organisation. Des acteurs de renom comme Apple ont adopté cette approche en mettant la sécurité et le respect de la vie privée au cœur de leur proposition de valeur.

On peut espérer que cet exemple sera suivi plus largement.