

# LES FOCUS SOLUCOM

## 2015 : une révolution pour la sécurité ?

The power of simplicity  
« *Ce qui est simple est fort* »

**solucom**   
management & IT consulting

**La sécurité a accompagné les évolutions du SI sur les quinze dernières années pour aboutir à un modèle de confiance périmétrique. Sécurité physique, interconnexion sécurisée à internet, antivirus, pare-feu... Les mesures mises en place ont été nombreuses et efficaces en leur temps. Mais aujourd'hui, le SI fait face à de nouvelles évolutions dont l'impact est suffisant pour ébranler la confiance périmétrique. Dans un environnement qui évolue si fortement, le RSSI doit donc répondre à la question suivante : comment maintenir la confiance ?**

### Un long chemin parcouru pour créer la confiance périmétrique

La sécurité du SI est une discipline qui existe depuis l'apparition du SI et qui a accompagné son évolution. Initialement, elle reposait avant tout sur deux principes appliqués dans les environnements *mainframes* : la sécurité physique, bloquant l'accès aux terminaux et aux systèmes, et le contrôle d'accès, empêchant des utilisations anormales.

Avec l'arrivée d'internet et les premières initiatives d'interconnexion sécurisée avec les entreprises, le modèle de confiance périmétrique a émergé. Il repose sur la mise en place d'un rempart d'équipements, notamment le pare-feu, séparant un monde inconnu et dangereux du réseau interne, dit « de confiance ».

L'évolution des usages du SI dans les entreprises d'une part, et l'arrivée des premières menaces très médiatisées, telles que les vers massifs, *Blaster*, *Sasser*, d'autre part, ont entraîné une prise de conscience des

limites d'une sécurité s'appuyant sur un rempart périmétrique seul et de la nécessité d'une sécurisation de l'intérieur du réseau. Ce fut l'ère de l'industrialisation de l'antivirus, du pare-feu personnel, du déploiement de correctifs et de la gestion opérationnelle de la sécurité. Ces mesures centrées sur les infrastructures, associées à des processus de maintien en condition de sécurité des systèmes, visaient à mettre en place un socle de sécurité réparti sur le SI et en assurant un niveau de sécurité global. Ce niveau de sécurité « homogène » ayant été mis en place, est apparu le besoin de comprendre davantage les enjeux métiers afin de piloter la sécurité non plus en aval, par les incidents, mais en amont, par les risques. De cette démarche découlent les premières approches métiers, les alignements ISO 27001, les boucles d'amélioration continue et l'industrialisation des audits et du contrôle permanent.

### Un modèle de confiance périmétrique aujourd'hui ébranlé

Ces actions, efficaces en leur temps, doivent être conservées, mais doivent également accompagner les évolutions majeures à venir. Et celles-ci sont nombreuses !

Les informations et les traitements sont amenés à sortir de plus en plus du périmètre de l'entreprise, morcelant toujours plus le SI. L'arrivée du *cloud computing*, les évolutions liées à la mobilité des utilisateurs, le renforcement des logiques de raccordement à des partenaires externes, clients ou fournisseurs, constituent autant de facteurs de cet éclatement du SI.

D'autre part, les utilisateurs disposent souvent, dans leur vie personnelle, d'une innovation

d'avance sur la DSI. L'appétence pour l'ergonomie, la mobilité, le confort des technologies grand public, telles que les *smartphones*, les tablettes, le wifi, etc. se transpose dans l'entreprise. La DSI y voit, par ailleurs, un gain potentiel de productivité.

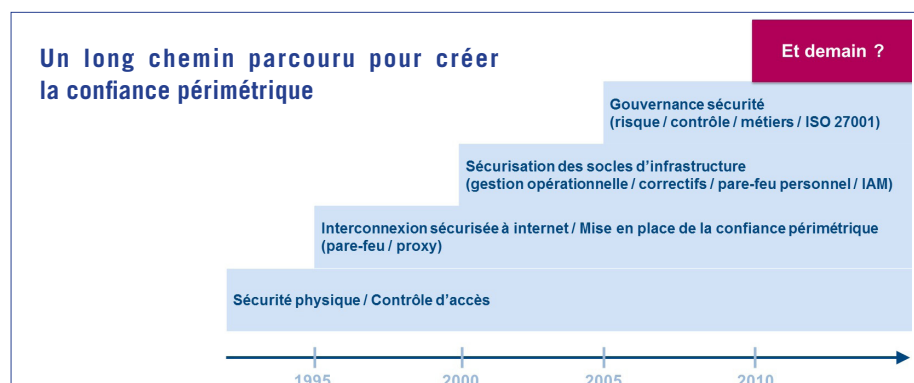
L'environnement de l'entreprise connaît également de fortes évolutions. Les standards et réglementations continuent à se multiplier et à se complexifier. Ils deviennent de plus en plus précis et ciblent des données toujours plus spécifiques (santé, paiements, données à caractère personnel, etc.). Si bien que la DSI voit apparaître quantité de silos particuliers ayant des niveaux de sécurité hétérogènes et implémentant des règles parfois contradictoires.

Par ailleurs, les menaces deviennent de plus en plus ciblées, et leurs motivations évoluent de la recherche de notoriété à une logique lucrative liée au vol d'informations confidentielles. Des exemples récents comme les attaques visant le Ministère des finances, Google, Sony ou encore les sociétés du secteur pétrolier, montrent également que la facilité d'exploitation des vulnérabilités a été largement accrue par des outils d'attaque ergonomiques et facilement accessibles.

Enfin, la frontière du réseau interne tend à s'ouvrir. Parfois même, elle a cédé la place à une illusion de sécurité. En effet, la forte évolution de l'interpénétration des réseaux de l'entreprise et de ses partenaires et l'accueil de tiers sur le réseau interne amènent à réaliser que le réseau « privé » ne l'est plus vraiment, et que les infrastructures auxquelles il est exposé ne sont pas toujours maîtrisées. Ajoutons à cela le caractère statique des briques de sécurité aujourd'hui disposées éparpillées sur le SI, comme les pare-feu dont les politiques de filtrage ne sont revues que rarement. On peut alors imaginer l'impact à moyen terme si l'on ne change pas la manière de faire de la sécurité. Mais si la sécurité telle que l'on la connaît disparaît, comment rétablir la confiance ?

### De la confiance périmétrique à la « confiance dynamique » : une sécurité centrée sur les données

Il faut aujourd'hui faire évoluer le modèle sur lequel la confiance repose pour passer d'un modèle de confiance périmétrique à un modèle de confiance dynamique.



La confiance périmétrique repose aujourd'hui sur trois piliers :

- L'identité de l'utilisateur
- Une séparation physique entre les réseaux interne et externe
- Un socle d'infrastructure maîtrisé

Cette confiance périmétrique est statique : elle est connue et maîtrisée à un instant donné selon des critères prédéfinis qui ne sont pas fréquemment réévalués.

Il est nécessaire de faire évoluer les piliers de la sécurité :

• **L'identité de l'utilisateur**

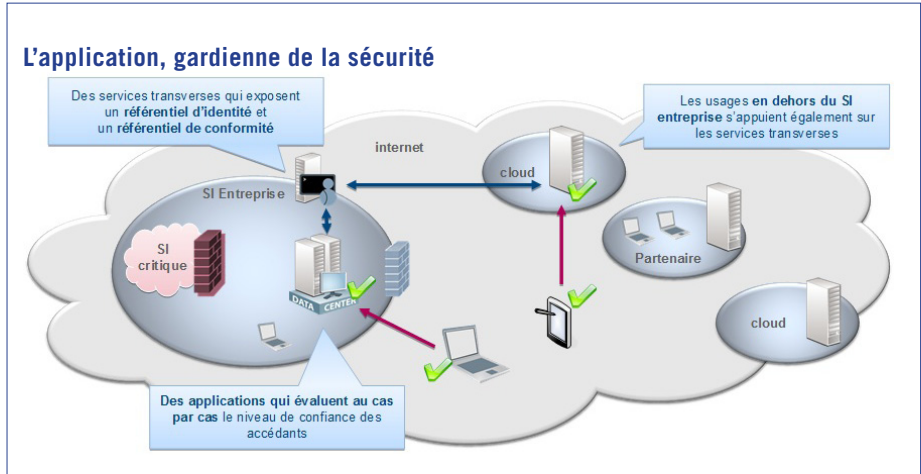
Le pilier relatif à l'identité de l'utilisateur va persister et jouer un rôle de plus en plus important. Il faut donc continuer à investir dans ce domaine, non seulement pour le contrôle d'accès aux informations, mais aussi pour assurer la traçabilité et détecter les comportements anormaux. Le référentiel d'identité doit devenir transverse et partagé, en interne comme en externe.

• **Un socle d'infrastructure conforme**

L'utilisation de terminaux personnels, les situations de mobilité ou l'outsourcing impliquent que le socle d'infrastructure ne peut plus être systématiquement maîtrisé. Il faut donc être capable de contrôler la conformité des éléments accédant à l'information en regard d'un référentiel transverse de conformité à construire.

• **Des applications sécurisées**

Celles-ci doivent devenir porteuses de l'évaluation de la sécurité et remplacer progressivement la sécurité apportée par des périmètres réseaux.



**Les données et les applications au cœur du futur de la sécurité**

La refonte du modèle va progressivement entraîner une exposition accrue des applications et de leurs données à des environnements moins sains. Elles devront donc être plus résistantes et embarquer les fonctions de sécurité nécessaires à l'évaluation de la conformité des socles d'infrastructure clients et de l'identité des utilisateurs. Associées aux référentiels de conformité et d'identité, elles devront également assurer une traçabilité avancée et détecter les comportements anormaux.

De plus, la confiance doit être dynamique, c'est-à-dire évaluée en temps réel lors de l'accès à l'information. Les référentiels de conformité et d'identité devront donc être portés par des services transverse de sécurité accessibles en interne comme en externe et sécurisés à la mesure de leur exposition. Ces derniers restent aujourd'hui à construire en capitalisant sur les référentiels existants.

tent un challenge.

Tout d'abord, une protection périmétrique minimale va persister mais être plus légère. Une capacité d'isolation devra être conservée en cas d'incident sur une zone du SI, et certains périmètres resteront isolés au sein même du SI – zones critiques devant être particulièrement protégées, ou zones historiques, difficiles à mettre en conformité avec le nouveau modèle. Le réseau perdra son rôle d'isolation mais gagnera en capacité à détecter des comportements anormaux et à réagir en conséquence (blocage, alerte...). Des initiatives réelles et concrètes existent. Elles sont appuyées par des organismes internationaux et des éditeurs comme le *Trusted Computing Group*, ou le *Forum Jericho*. Cependant, l'absence de normalisation et la maturité faible des solutions nécessitent d'attendre des évolutions avant d'envisager des déploiements larges.

Sur le volet applicatif, l'historique à gérer est important et amplifié au quotidien par la non évaluation des développeurs sur le respect des règles et processus sécurité. Si les briques techniques de la sécurité applicative existent de manière unitaire, elles sont rarement déployées car leur coût et leur complexité, à financer dans chaque projet, sont trop importants.

**Que faire, dès aujourd'hui, pour tendre vers la cible ? Sécuriser les applications et créer la tour de contrôle sécurité du SI** Premier chantier, **construire les services transverse de sécurité, essentiels à la confiance dynamique.** Les investissements engagés sur



Ce nouveau modèle permet ainsi d'améliorer flexibilité et sécurité en autorisant plus d'usages et de terminaux clients, et en construisant des règles de protection basées sur la conformité et l'identité et non plus uniquement sur des périmètres réseaux. Il assure également une meilleure sécurisation des applications dont le niveau d'exposition ne cesse de croître. Et surtout, il centre la protection sur la donnée !

**La confiance dynamique : une cible qui reste un challenge**

Ces changements fondamentaux représen-

le référentiel d'identité doivent être poursuivis pour le finaliser, mais aussi l'ouvrir vers l'extérieur et en définir la gouvernance, en particulier sur le volet de la traçabilité et de la détection des événements anormaux. Quant au référentiel de conformité, des initiatives peuvent d'ores et déjà être lancées, notamment sur la définition de la cible, le choix des outils de contrôle de conformité et, pourquoi pas, le lancement de pilotes sur le volet contrôle d'accès au réseau. Ces services transverses seront aussi la destination des informations de traçabilité issues du réseau et des applications. Ils joueront un rôle de tour de contrôle du système d'information.

Deuxième chantier, **renforcer la sécurité applicative**, avec des évolutions organisationnelles fortes sur la responsabilisation des développeurs et des chefs de projets, mais également l'inscription de revues sécurité tout au long du processus projet. Une phase d'industrialisation des solutions techniques permettant de créer des offres de service mises à disposition des applications pourra également être un facteur de création de valeur.

Enfin, il est essentiel que la démarche entreprise cible la valeur métier ! Comment ? Par exemple en identifiant le TOP 10 des données et traitements sensibles, en sensibilisant la direction et les métiers, et en montrant le résultat concret des actions réalisées. La mesure de l'efficacité dans le temps est également un facteur déterminant, par exemple en réalisant régulièrement des audits ou en suivant des indicateurs.

### Quel rôle pour le RSSI et la DSI dans ce nouveau modèle ?

Toutes ces évolutions et cette démarche font réfléchir au rôle de la DSI. Elle ne devra plus être un constructeur de services dans l'avenir, mais bien un assembleur de services internes ou externes, garante d'une cohérence globale vis-à-vis de ses utilisateurs métiers.

Quant au RSSI, il demeure avant tout un gestionnaire de risques, à la fois proche de la direction et du métier, pour comprendre les enjeux de sa société et être apte à justifier les décisions et les budgets à engager. Il reste également un garant des processus de sécurité, il se doit d'être proactif, réaliste et ouvert pour anticiper les nouveaux usages.

### Les chantiers prioritaires



#### Construire les services transverses de sécurité

- Finaliser le référentiel d'identité, l'ouvrir vers l'extérieur et en définir la gouvernance
- Définir les modalités de traçabilité et de détection des comportements anormaux
- Lancer des initiatives sur le contrôle de conformité



#### Renforcer la sécurité applicative et des données

- Responsabiliser les développeurs et les chefs de projet
- Inscrire des recettes sécurité bloquantes dans le processus projet
- Créer une offre de service de sécurité applicative (chiffrement, intégrité, authentification...)



#### Et toujours cibler la valeur métier !

- Identifier le TOP 10 des données et traitements sensibles
- Sensibiliser et responsabiliser la direction et les métiers
- Montrer la valeur des actions réalisées (analyse de risques et contrôle)

Mais il devra aussi devenir un offreur de services proposant des solutions concrètes pour implémenter ce modèle et faciliter les nouveaux usages. Son rôle de MOA de l'ensemble des services de la confiance dynamique est une nouvelle opportunité pour lui.

### Le RSSI, facilitateur des évolutions métiers



### Conclusion

Maintenir la confiance dans un environnement qui évolue fortement nécessite de faire évoluer les piliers de la sécurité pour la centrer sur la donnée. Dans ce contexte, l'application, canal d'accès à la donnée, devient la gardienne de la confiance, et ce de manière dynamique. À chaque accès à une donnée, l'application s'appuie sur des référentiels transverses de sécurité, accessibles en

interne comme en externe, pour contrôler l'identité des utilisateurs et la conformité des clients, et ce, en fonction des besoins en sécurité de cette donnée. Ces référentiels sont la tour de contrôle de la sécurité du SI, autorisant les accès et contrôlant les actions réalisées de manière dynamique.

Mais cette cible reste aujourd'hui un challenge en raison de l'absence de normalisation, de la faible maturité de certaines solutions et d'un manque d'effort chronique sur la sécurité applicative. Des initiatives doivent donc être lancées en priorité pour augmenter la sécurité des applications, et de leur processus de création.

Enfin, ces évolutions accentuent le nécessaire rôle de relais du RSSI entre les métiers et les SI. Plus que jamais, il doit être un facilitateur des évolutions métiers en implémentant un modèle de sécurité souple, flexible et dynamique, capable de faire face à de nouvelles évolutions du SI.



Ce focus a été rédigé par Jérôme Billois, manager au sein de la *practice* Sécurité & risk management de Solucom, en collaboration avec Ali Fawaz, consultant.