

La Lettre Sécurité

Édito



L'actualité sécurité récente et à venir s'avère chargée : la cybercriminalité est sur toutes les lèvres, innovations technologiques et nouvelles réglementations obligent les acteurs de la sécurité de l'information à être en veille permanente, à prendre du recul, à s'adapter. Pour mieux vous accompagner, nous avons décidé de faire évoluer votre « Lettre Sécurité Solucom ».

Nous poursuivons cependant un objectif inchangé : vous apporter décryptage et analyse de l'actualité et des tendances de fond qui façonnent notre marché. Au-delà du format papier, nous adoptons le format *e-newsletter*. Nous nous appuyons ainsi sur le magazine en ligne de Solucom, **Solucom INSIGHT**, et sa rubrique sécurité www.solucominsight.fr/securite. Vous trouverez sur ce site l'ensemble de nos réactions à chaud sur les thèmes d'actualité.

Attaques ciblées, conformité PCI-DSS, gestion de risques, arrivée des systèmes de management de la continuité ou encore renouveau de la biométrie sont autant de sujets qui ont occupé le devant de la scène ces derniers mois ; nous sommes heureux de vous faire partager nos prises de position sur le sujet.

Nous espérons que cette nouvelle version vous plaira. N'hésitez pas à nous envoyer vos commentaires à lettresecurite@solucom.fr.

En vous souhaitant une bonne lecture.

Frédéric GOUX

Directeur de la *practice* Sécurité & risk management, cabinet Solucom

Dossier

Nouvelles menaces externes et attaques ciblées : quelle stratégie pour le RSSI ?

2010/11 : une augmentation sans précédent du nombre d'attaques

Ministère des Finances, Google, Sony, RSA, secteur pétrolier, entités gouvernementales... autant d'acteurs qui ont en commun d'avoir été victimes d'attaques informatiques. Ces dernières ont défrayé la chronique, faisant les grands titres des médias généralistes et économiques. Elles ont souvent généré des pertes sonnantes et trébuchantes : 170 millions de dollars pour Sony, 66 millions de dollars pour RSA ; sans compter l'impact d'image. Au-delà de cette explosion du nombre de cas, se cache une réalité complexe avec des points saillants aujourd'hui bien identifiés.

Tout d'abord, les attaques ne visent plus uniquement les entités gouvernementales ou leurs sous-traitants et leurs fameux « secret défense ». Les entreprises sont aujourd'hui la cible, soit pour les données de leurs clients, soit pour leurs propres données (stratégie, R&D, accords commerciaux...). Le phénomène est mondial et la France est concernée, même si cela est moins visible. Tous les secteurs d'activités sont touchés sans distinction.

Mais au-delà de ce *buzz* médiatique, que retenir de l'évolution de la sécurité de l'information sur ces 12 derniers mois ? Et que doit répondre le RSSI à sa direction générale qui l'interroge de plus en plus fréquemment sur ces affaires ?

Diffuses, opportunistes ou ciblées : savoir reconnaître les attaques

L'analyse des événements récents fait ressortir trois différents types d'attaques.

La première catégorie, « historique », correspond aux habituelles **infections virales ou encore au spam**. Il s'agit d'**attaques diffuses**. Ne visant pas une organisation en particulier, ces attaques vont avoir un effet néfaste sur le SI : déni de service, perte de données utilisateurs... Ces attaques sont souvent simples à éviter et simples à juguler. Elles ont marqué les entreprises dès les années 2000 pour connaître leur dernière itération majeure avec *Conficker* en 2008. Celles-ci ne seront pas abordées dans la suite de l'article.

La deuxième catégorie, **l'attaque opportuniste, est à but lucratif ou idéologique**. Elle vise soit à capturer de l'information facilement monnayable (données des clients, données de cartes bancaires, etc.), soit à avoir un effet médiatique important (déni de service distribué ou *defacement* de sites web publics, vols de données lambda ensuite publiées sur internet, etc.). Elle ne relève souvent pas d'un haut niveau de technicité et ses auteurs ne cherchent pas à nuire à tout prix à une organisation donnée. Aussi, si l'une est plus sécurisée qu'une autre, ils passeront leur chemin pour se jeter sur la proie la plus facile. Ce scénario est également majoritaire-

Suite en page 2

DÉCRYPTAGES

P4

Globaliser la gestion des risques : vers la mise en place d'un cadre unique

P5

PCI-DSS : l'externalisation est-elle une solution ?

ment vrai pour les attaques « idéologiques ». Il s'agit pour des groupes comme Lulzsec ou Anonymous de capturer, là où c'est facile, des données perçues comme sensibles et de les rendre publiques. La quasi-totalité de leurs attaques ont été rendues possibles par des manques criants de sécurité et des failles extrêmement simples dans les systèmes des organisations visées.

La troisième catégorie correspond à l'**attaque ciblée**. Celle-ci vise des informations sensibles et précises dans l'organisation. Ses auteurs sont mandatés pour viser une entité en particulier avec un objectif clair. Ils disposent de temps pour comprendre et analyser l'organisation, préparent des scénarios d'attaques et utilisent tous les moyens à leur disposition, techniques comme humains, internes comme externes, simples comme complexes, afin d'atteindre leur but. Le niveau de technicité et les moyens disponibles s'élèvent drastiquement, tout comme les enjeux. La communauté sécurité évoque ainsi le terme APT ou *Advanced Persistent Threat* pour décrire ces menaces avancées et persistantes. Google ou RSA en ont été victimes. De nombreux autres cas ont été recensés, y compris en France. Les attaques les plus courantes reposent sur des emails piégés émis à destination de personnes clés (*spear-phishing*), ou encore des attaques sur des plate-formes externes (site web) permettant ensuite des rebonds multiples sur le réseau interne pour atteindre les données de l'organisation visée.

Comment réagir ? Évaluer son exposition et adopter une stratégie de protection des données en fonction de leur sensibilité

Au regard de ces récents événements, le RSSI doit aujourd'hui plus que jamais évaluer l'ex-

position de son organisation à ces différentes attaques. Le secteur d'activité, la visibilité de la marque ou encore la sensibilité des données manipulées sont autant de critères à prendre en compte. Cette évaluation doit être faite de manière régulière en fonction de l'actualité de l'organisation et de son environnement. La direction générale doit être informée de cette évaluation de l'exposition.

En parallèle, il s'agit également d'identifier les données les plus sensibles de l'entreprise. Sans viser une classification exhaustive de l'ensemble des informations, il est important de bien identifier les données les plus sensibles et/ou les plus exposées, mais aussi qui elles peuvent intéresser, que ce soit des personnes malveillantes internes ou externes pour les protéger de la manière la plus efficace possible.

Ces éléments permettent à l'organisation d'évaluer le risque d'être visée par une attaque opportuniste ou ciblée. Ils permettent de mieux organiser les plans d'actions de protection.

Lutter contre les attaques opportunistes : retour aux fondamentaux

Les attaques opportunistes sont souvent simples. Elles utilisent des vulnérabilités évidentes dans le SI et visent les systèmes exposés publiquement. Il est facile de s'en protéger en investissant les moyens nécessaires pour mettre en place, concrètement, les bonnes pratiques de sécurité. Trois thèmes ressortent particulièrement :

- **La sécurité applicative** : les vulnérabilités web sont le vecteur principal d'attaque (injection SQL, mots de passe simples et stockés en clair, etc.). Il est crucial de rapidement renforcer la sécurité applica-

tive en agissant en amont sur les développeurs et les métiers, et en aval sur les audits avant mise en production.

- **Le maintien à jour de l'infrastructure** : même si des efforts ont été réalisés, la gestion des correctifs, le durcissement des systèmes (y compris des comptes administrateurs) et l'utilisation de zone d'isolation (DMZ) ne sont encore parfois mis en œuvre que partiellement.
- **La mise en place de contrôles réguliers** : que ce soit par l'intermédiaire d'audits, de tests d'intrusion ou par la mise en place de systèmes de détection d'intrusion ou de gestion des traces, des contrôles réguliers sont essentiels pour garantir le niveau de sécurité dans le temps.

Ces mesures matures et largement maîtrisées permettent aujourd'hui de lutter efficacement contre les attaques opportunistes. Aujourd'hui, elles sont efficaces car le système d'information repose sur un modèle de protection périmétrique, distinguant le réseau interne des réseaux externes, plus exposés. Dans le futur, ce modèle disparaîtra irrémédiablement et les applications internes seront de plus en plus exposées. Nous détaillons dans le focus « 2015 : une révolution pour la sécurité ? », disponible sur le site de Solucom, comment adapter sa stratégie pour répondre à ces évolutions et mettre en place une sécurité centrée sur les données en profondeur dans le SI.

Du « secret défense » au « secret entreprise » : des mesures avancées à déployer pour lutter contre les attaques ciblées

Les attaques ciblées, elles, sont difficiles à détecter, à juguler et à empêcher. Le périmètre de sécurité réseaux et les applications

3 cas et 3 motivations différentes en 2011

Lucrative : Citibank, parmi les plus grandes banques américaines.

Attaque : utilisation d'une faille dans le site web qui permet de rebondir entre les différents comptes des clients en modifiant l'adresse du navigateur.

Conséquences : 200 000 cartes bancaires à réémettre et 2,7 millions de dollars détournés. Les coûts totaux n'ont pas été révélés.

Idéologique : Vanguard, société du secteur de la défense aux Etats-Unis, spécialisée dans les drones.

Attaque : vol du mot de passe du DG grâce à une faille sur un site web de la société. Mot de passe simple (« Gloria88 ») ensuite utilisé pour accéder à sa boîte de messagerie personnelle qui contenait des documents professionnels.

Conséquences : plusieurs Go de messages publiés sur internet, des impacts encore à évaluer.

Attaque ciblée : RSA, fournisseur de solutions de sécurité.

Attaque : messages piégés ciblés à destination de collaborateurs. Prise de contrôle de leurs postes, puis rebonds progressifs jusqu'à l'atteinte de serveurs sensibles contenant des informations permettant de réduire le niveau de sécurité des solutions vendues.

Conséquences : 66 M\$ en direct, intrusion facilitée sur les SI de clients.

web ne sont plus forcément les premières portes d'entrée. L'attaque va souvent jouer sur plusieurs tableaux pour atteindre son objectif. Ingénierie sociale, faille applicative, attaque sur les réseaux internes... tout est envisageable et envisagé.

Il s'agit ici de situations similaires à celles observées dans le secteur de la défense depuis de nombreuses années. Mais aujourd'hui, les grandes organisations y sont confrontées au quotidien. Pour protéger les données extrêmement sensibles, il leur faut donc mettre en œuvre des moyens avancés, drastiques, similaires à ceux employés dans le secteur de la défense. Elles devront alors **créer un SI dédié, spécialisé, pour gérer le « secret entreprise » analogue au « secret défense »**. Et, si aucune mesure de sécurité n'est infaillible, ces éléments permettront d'augmenter la difficulté des attaques et donneront plus de temps pour les détecter et y répondre, le cas échéant.

Quatre grands chantiers doivent être envisagés :

- **Créer des sanctuaires pour les données sensibles.** Basés sur une infrastructure dédiée, ils associent un nombre important et varié de mesures de sécurité : filtrage, chiffrement, isolation inter-serveurs, authentification forte dédiée, contrôle de conformité... Mais ils disposent également de processus spécifiques de mise en production afin de s'assurer que tout nouveau système est sécurisé. Ces systèmes et leur réseau devront être différents de ceux utilisés dans l'entreprise de manière classique. Ces sanctuaires seront maintenus par des équipes dédiées internes, sans utiliser d'accès distant.
- **Spécialiser les terminaux clients.** Vecteur d'intrusion classique lors d'attaques ciblées, le poste de travail devra être spécialisé en fonction des usages. Si l'utilisation de postes distincts en fonction des usages est fréquemment rencontrée, elle reste complexe à généraliser. Le recours à de nouveaux OS virtualisés et isolant les machines virtuelles suivant leur sensibilité est une piste à explorer. L'utilisation de solutions de déport d'écran peut être une option temporaire intéressante avant la généralisation d'un poste de travail virtualisé. Les échanges avec la zone sanctuarisée seront bien entendu chiffrés et les

postes ne permettront pas de stockage local d'informations très sensibles.

- **Sensibiliser et contraindre.** Les utilisateurs manipulant les données les plus critiques sont souvent les plus difficiles à convaincre de l'importance de la sécurité. L'utilisation d'exemples concrets et surtout la mise en place d'un mécanisme coercitif en cas d'écarts permettront de diminuer les solutions de contournement. Sur ces périmètres spécifiques, il ne faudra pas tolérer d'écart aux politiques de sécurité, comme cela peut aujourd'hui être le cas, et composer avec les impacts métiers consécutifs.

Surveiller, réagir et prévoir la reconstruction

L'attaque étant très probable, elle doit pouvoir être détectée et son impact minimisé. Une équipe interne dédiée à la gestion des zones sanctuarisées et à la gestion des incidents et des crises devra être formée. La traçabilité devra être mise en place et suivie avec des moyens importants (H24, temps réel, etc.). De nouvelles générations d'outils devront être testées et déployées en particulier pour détecter les signaux faibles relatifs à la fuite d'information. Ces systèmes seront également d'une aide précieuse pour enquêter sur les fuites de données lors de l'intrusion. D'autre part, des actions de reconstruction devront être imaginées pour pouvoir repartir sur une base saine en cas de succès d'une attaque. L'utilisation du PCA/PCI peut également être envisagée.

Tous ces moyens sont contraignants et ont un coût élevé. Ils doivent être limités à un nombre restreint de traitements et de données. C'est le prix à payer pour conserver un niveau de sécurité important. L'armée américaine estime que la sécurisation des projets très sensibles entraîne un surcoût de 20%, du fait des mesures additionnelles, mais aussi de la complexité et des contraintes posées sur le travail au quotidien (cloisonnement de l'information, séparation des équipes, etc.).

Certaines entreprises sont prêtes aujourd'hui à franchir ce pas à la vue des risques encourus. Il s'agit en particulier du secteur de la défense, des sociétés fournissant des systèmes de sécurité, des sociétés où l'innovation est réalisée sur des cycles longs de recherche et de développement.

Pour d'autres, la sécurisation ne sera pas acceptable, soit pour des raisons de pra-

tiques internes, soit pour des raisons budgétaires (les coûts dépassant la rentabilité du SI ou bridant la compétitivité). Il faudra alors peut-être décider de réduire le périmètre de protection, et accepter consciemment de potentielles fuites de données qu'il faudra justifier et valider avec le management.

Le rôle du RSSI, entre évaluation des risques et pouvoir de conviction

Il est évident que chaque type de menace est amené à perdurer dans le temps. C'est au RSSI de réaliser l'évaluation des risques de sa structure face à ces menaces et de convaincre sa direction de l'importance des actions à mener. Se protéger à tout prix contre les attaques ciblées n'est pas envisageable et n'a pas de sens. Par contre, construire un socle solide résistant aux attaques opportunistes sur lequel viennent se greffer des sanctuaires sécurisés est une orientation à évaluer chez chacun.

Les priorités du RSSI

- Évaluer sa position par rapport aux menaces
- Orienter le SI vers une protection centrée sur les données
- Vérifier l'application des bonnes pratiques de sécurité des systèmes exposés
- Mettre en place des mesures avancées sur certains périmètres
- Sensibiliser et convaincre !

La sécurité vit une nouvelle étape, des orientations stratégiques fortes doivent être prises. L'implication des directions est facilitée maintenant que ces attaques font la « une » des journaux. Il ne reste plus qu'à les convaincre d'investir le bon budget au bon endroit !



Gérôme BILLOIS, manager

Globaliser la gestion des risques : vers la mise en place d'un cadre unique



Etienne BOUET, manager

Historiquement, la gestion des risques est abordée par silos au sein des entreprises. Chaque filière (SI, qualité, continuité, RH...) traite son périmètre en toute autonomie et sans réels échanges avec les autres. Cette gestion très cloisonnée rencontre aujourd'hui ses limites car elle n'apporte pas de réponses satisfaisantes aux questions clés qui régissent la gestion des risques pour toute entreprise :

Quelles actions de réduction des risques dois-je initier en priorité ? Comment mutualiser mes efforts pour un maximum d'efficacité et un minimum de coût ? Quel niveau de réduction de mes risques ai-je atteint ?

Aligner les démarches pour un partage et une consolidation des risques

La direction des risques, acteur majeur de la démarche, se retrouve aujourd'hui confrontée à un enjeu de taille : comment traiter globalement les risques de l'entreprise en s'affranchissant de cette structure par filière. Notre conviction est qu'elle doit, pour ce faire, mettre en place un cadre global de gestion en travaillant principalement sur deux axes :

- **Aligner et faire converger les pratiques :** si la notion de risque et les concepts associés sont très proches d'une filière à l'autre, il arrive trop souvent que les méthodes, les langages, les échelles... divergent, rendant ainsi la consolidation des risques remontés par chacune des filières difficile voire impossible.
- **Élaborer ou rationaliser la gouvernance des risques :** la mise en place d'une organisation intégrant les différentes parties et les faisant interagir permettra non seulement de décloisonner la gestion des risques mais aussi d'optimiser les plans de traitement et la maîtrise globale du risque.

Cette rationalisation doit également concerner les canaux de remontée des risques qui sont aujourd'hui extrêmement nombreux (au moins autant que de filières) entraînant une sur-sollicitation des opérationnels.

Au-delà du travail sur la méthode et l'adaptation de l'organisation, cette réponse globale doit s'appuyer sur un portefeuille de risques commun, réceptacle unique pour l'ensemble de l'entreprise. Véritable outil de pilotage, le portefeuille doit permettre, à la cible, un traitement plus adapté des risques par les différentes filières, basé sur des plans d'actions complémentaires et partagés.

S'appuyer sur l'existant pour une mise en place progressive

On ne passe pas d'une réponse éclatée à une approche globale en une seule étape, ou en faisant table rase de l'organisation et de ses contraintes. Face à ce challenge, la stratégie gagnante est, au contraire, celle qui implique l'ensemble des parties prenantes dans la réflexion pour en garantir l'acceptation et construire une véritable « culture du risque » au sein de l'entreprise. C'est également celle qui élargit pas à pas le spectre des risques couverts en commençant par la consolidation de risques de nature similaire, tels que les risques de sécurité et ceux liés au SI, avant d'inclure l'ensemble des risques opérationnels.

C'est en investissant sur l'organisation, en apportant de la cohésion entre les différentes filières et en appliquant une démarche progressive que les entreprises réussiront à transformer leur approche des risques.

Tribune écrite en collaboration avec Marion COUTURIER



PCI DSS : l'externalisation est-elle une solution ?



Mathieu Garin, manager

Les cartes de paiement ont envahi notre quotidien, que ce soit pour les achats en magasin comme pour la vente à distance en particulier via internet. Pour autant, cette généralisation de l'utilisation de la carte de paiement a entraîné une augmentation du montant total de la fraude de 9,8% par an en moyenne, pour atteindre 342,3M€ en 2009*. Les grands émetteurs de cartes comme Visa et Mastercard se devaient de réagir et de proposer de nouvelles mesures de sécurité.

PCI DSS, un standard de sécurité exigeant...

Pour contrer cette augmentation des fraudes, les acteurs majeurs des cartes de paiement ont défini le standard de sécurisation PCI DSS, dont les objectifs sont les suivants :

- Réduire les risques de fuite de données bancaires en renforçant et uniformisant à l'échelle mondiale leur sécurisation ;
- En cas de fraude, déplacer les responsabilités des sociétés de cartes de paiement vers les garants de la certification PCI DSS (banques et sociétés d'audit).

Le standard adresse douze thèmes classiques de la sécurité. Mais il est particulièrement exigeant ! Toutes les règles doivent être appliquées et elles sont précises. Durcissement des serveurs, revue quotidienne des logs, détection des points d'accès wifi pirates, sont autant de chantiers complexes à adresser dans le cadre

d'une mise en conformité. D'autant plus que leur application est contrôlée à travers des audits annuels pour les sociétés réalisant plusieurs millions de transactions par an.

Quelle stratégie de mise en conformité ?

Au vu de cette complexité, notre recommandation est d'initier tout projet de mise en conformité PCI DSS par la réduction du périmètre d'application du standard. Pour cela, plusieurs méthodes se détachent :

- **Aligner le périmètre applicatif avec les besoins métiers réels.** Cet exercice consiste à supprimer les données de cartes bancaires partout où leur présence n'est pas justifiée par un besoin métier réel.
- **Désensibiliser les données de cartes bancaires.** Il est possible de remplacer les données bancaires par une donnée non exploitable en cas de fraude - troncature**, *hash****, ou identifiant unique (*token*) - différente de la donnée bancaire. Des éditeurs se positionnent sur la fourniture de solutions de désensibilisation.

Cette étape effectuée, le périmètre d'application du standard PCI DSS se résume alors aux applications restantes et aux services d'infrastructures sous-jacents (réseau, postes de travail concernés, sauvegardes, base d'identifiants uniques...). C'est a priori sur ce périmètre que s'appliqueront donc les exigences de PCI DSS.

Sauf si... la réduction de périmètre se poursuit à travers l'externalisation de ces ressources applicatives. Et cette externalisation pourrait même servir à améliorer les services offerts !

L'externalisation : une solution à PCI DSS ?

Historiquement implantés dans beaucoup d'entreprises pour assurer un rôle d'intermédiaire avec les banques, les PSP (*Payment Service Providers*) peuvent jouer un rôle majeur dans une stratégie de mise en conformité, dans la mesure où toutes leurs offres sont proposées en standard sur des environnements entièrement certifiés PCI DSS.

En particulier, les PSP sont aujourd'hui en mesure de proposer l'externalisation de tous les composants de la chaîne de liaison du paiement par internet ou par téléphone : collecte des données, demandes d'autorisation et de paiement, contrôles anti-fraude avancés...

Et l'externalisation peut aller encore plus loin ! Les PSP proposent dorénavant des tables de correspondance « *tokenizer* » facilitant la désensibilisation des données carte de paiement. Lors de la collecte de données, un identifiant unique, personnalisable, est renvoyé à l'entreprise et peut donc circuler dans le SI sans aucune contrainte vis-à-vis de la norme PCI DSS.

L'externalisation permet ainsi de réduire de manière conséquente le périmètre applicatif, mais attention... ce n'est pas la solution ultime pour être conforme à PCI DSS. Certaines populations conservent souvent le besoin d'accéder au numéro de carte depuis leur poste de travail, pour des raisons réglementaires, entre autres. Nous pouvons par exemple citer les services de lutte anti-fraude ou les téléconseillers, dont les terminaux devront sans doute rester dans le périmètre PCI DSS. Il est donc difficile de penser qu'aucun composant du SI ne manipule de données cartes surtout dans une grande entreprise.

Mais bien plus qu'un simple levier de mise en conformité PCI DSS, un projet d'externalisation peut devenir stratégique pour l'entreprise en lui permettant de développer de nouveaux moyens de paiements (ex : cartes cadeaux), de nouveaux marchés internationaux (facilités de connexion aux acquéreurs étrangers) ou de nouvelles fonctionnalités (ex : paiement *one-click* sans renseignement des données CB). Le recours à ces acteurs peut aider à la conformité mais aussi faciliter de nouveaux usages.

Tribune écrite en collaboration avec Timoléon TILMANT et Ali FAWAZ

*Ces statistiques sont issues du rapport d'activité annuel 2009 de l'Observatoire de la sécurité des cartes de paiement publié en Juillet 2010

** Troncature : mécanisme de suppression d'une partie de l'information - ***Hash : mécanisme de calcul qui à partir d'une donnée source crée une empreinte unique et non réversible

ISO 22301 : un nouvel élan pour la continuité d'activité ?



Amal Boutayeb, manager

La publication de la norme ISO 22301, traitant des systèmes de gestion de la continuité, est attendue dans les prochains mois. En institutionnalisant à un niveau international de bonnes pratiques déjà souvent formalisées localement, elle devrait favoriser le franchissement d'un nouveau cap dans la maturité des organisations sur le sujet.

En effet, la réflexion autour des systèmes de management de la continuité d'activité n'est pas récente : de nombreux guides nationaux sont apparus ces dernières années, notamment dans les pays les plus mûrs sur le sujet.

Parmi ce foisonnement de publications, la BS* 25999 (publiée en 2007) a pris un rôle de premier ordre. Or l'ISO 22301 partage de nombreux points communs avec cette norme, notamment les notions relatives aux systèmes de management : amélioration continue, implication du management, pilotage par les risques et les enjeux métiers, etc.

S'inscrire dans une démarche de progression continue

Il s'agit là d'un point clé : inscrire le plan de continuité des activités (PCA) dans un système de management, c'est entre autres réfléchir à sa politique de couverture de risques et aux moyens affectés au PCA, impliquer le management et délimiter un périmètre en s'assurant de son adéquation avec les enjeux métiers ; et tout

cela de façon récurrente, de façon à garantir *in fine* l'alignement du PCA avec les objectifs de l'organisation.

Le point de départ est donc **la réalisation d'une analyse de risques et d'un bilan d'impact sur l'activité (BIA)**. Si ce dernier point est fortement détaillé dans la BS 25999, allant jusqu'au cadrage des critères d'expression des besoins, et assez largement répandu dans la pratique, l'analyse de risques est quant à elle plus rarement revue aujourd'hui. Or les dispositifs de secours ont vocation à couvrir des périmètres et des risques de plus en plus larges et surtout en permanente évolution : réaliser ou revoir l'analyse de risques qui supporte le PCA, c'est aussi apporter un regard critique sur son PCA.

Le contrôle, point clé de l'amélioration

Le deuxième levier à activer est celui du **contrôle du PCA, afin d'en mesurer la pertinence et l'efficacité opérationnelle**. À cet égard, la réalisation régulière de tests et exercices PCA est nécessaire mais pas suffisante, car sauf remise en question très régulière du scénario de test, la pertinence du PCA n'est pas analysée. Par ailleurs, force est de constater que la mobilisation des acteurs peut être difficile à maintenir dans le temps, et que les tests peuvent au fil du temps ne pas apporter toutes les certitudes sur l'efficacité du PCA. En outre, la mise en place d'un processus de contrôle force à s'interroger sur les indicateurs de mesures d'efficacité du PCA, utiles notamment pour le reporting auprès du management, et sur la politique d'audit du PCA.

Sensibiliser pour ne pas oublier l'humain

Enfin, peu déployée mais pourtant d'une nécessité évidente, la sensibilisation des collaborateurs permet d'assurer que le PCA n'est pas qu'un plan « sur le papier », et que son exécution dans la « vraie vie » est crédible. En ciblant le management, elle s'assure de son sponsorship, et peut l'aider dans la prise de décision le moment venu. En touchant les acteurs au quotidien du PCA, elle peut être

d'une réelle aide dans le maintien de leur implication. Et surtout, en ciblant les collaborateurs concernés lors du déclenchement des dispositifs, elle permet de renforcer le caractère opérationnel du PCA !

Au-delà de l'aspect médiatique, une évolution naturelle pour un sujet de plus en plus sensible

Le caractère international de l'ISO ne manquera pas de redonner un réel engouement pour le sujet, et de lui permettre de s'inscrire dans la lignée de ses glorieux aînés concernant la qualité (ISO 9001) et la sécurité de l'information (ISO 27001). Un intérêt qui viendra accompagner la maturité croissante des PCA des organisations, qui ont ces dernières années lancé de nombreux projets de mise en place, en réponse aux menaces qui pèsent sur leurs activités et aux exigences de disponibilité de leurs métiers.

Mais le PCA est plus qu'un projet. Le principal enjeu, plus que de le mettre en place, est bien de le maintenir en conditions opérationnelles, et c'est sur ce point que la norme peut apporter : par l'inscription du PCA dans un processus récurrent, dans un cycle de vie calé sur l'évolution de l'organisation.

Sans oublier que cette norme sera certifiante : pour ceux souhaitant aller au-delà d'une simple utilisation de ces bonnes pratiques, la certification permet d'afficher l'existence et l'importance du PCA de manière externe, vis-à-vis de clients, de partenaires, voire d'autorités réglementaires... Autant de bonnes raisons pour adopter cette norme au plus tôt !

*BS : British Standard

3 questions... sur la biométrie



Benoît Tanguy, directeur

On associe souvent biométrie et authentification forte. Qu'en pensez-vous ?

C'est une erreur assez classique. Authentifier un individu consiste à lui demander une preuve de son identité. Il existe trois catégories de facteurs d'authentification : ce que je sais, ce que j'ai, ce que je suis. La biométrie peut ainsi permettre d'authentifier une personne, avec cependant une marge d'erreur non négligeable. Ce n'est pas une science exacte : elle dépend de la qualité de la solution mise en œuvre (en particulier des capteurs) et du seuil de sensibilité choisi (un compromis est à trouver entre ergonomie et sécurité).

Une authentification forte nécessite la combinaison d'au moins deux facteurs d'authentifica-

tion. La biométrie seule ne peut donc pas être considérée comme une authentification forte.

Pourquoi les technologies biométriques ne sont-elles pas plus largement déployées et utilisées ?

Effectivement, la biométrie est encore relativement peu utilisée en entreprise, contrairement aux usages grand public. Les premiers usages sont apparus au milieu du XIX^{ème} siècle comme par exemple l'identification systématique de l'empreinte de la main sur des contrats en Inde pour éviter l'usurpation d'identité au moment de toucher les salaires. Les déploiements s'accroissent aujourd'hui autour des passeports et de cartes d'identité biométriques.

Même si cela a tendance à désormais s'estomper, les utilisateurs sont quelque peu réticents dès qu'on leur parle de biométrie (crainte de l'effet « *Big Brother* »). Par ailleurs, les réglementations, notamment la CNIL en France, sont très contraignantes : tout usage SI de la biométrie nécessite une demande d'autorisation préalable, et généralement celle-ci n'est pas accordée pour les biométries à trace utilisant des bases centralisées.

Enfin, d'un point de vue technologique, les coûts d'acquisition importants et l'absence de standardisation et d'interopérabilité, demeurent également deux freins notables.

Finalement, quels sont aujourd'hui les usages de la biométrie en entreprise ? Et quelles tendances se dessinent à moyen terme ?

En entreprise, les déploiements restent encore bien souvent circonscrits à des périmètres métiers spécifiques et limités à quelques centaines de personnes (ex : consolidation financière, *trading*), voire à des vitrines technologiques de la DSI. Seulement quelques entreprises ont déployé des solutions de biométrie / carte à puce sur des périmètres plus larges (quelques milliers de personnes).

Le développement de nouveaux usages domestiques (lecteurs sur les équipements grands publics...) et la généralisation des pièces d'identités biométriques vont faire entrer ces technologies dans le quotidien des utilisateurs et lever progressivement leurs craintes. De plus, l'essor de la biométrie sans trace devrait permettre un assouplissement du cadre réglementaire. Enfin, les coûts des capteurs individuels devraient baisser significativement dans les années à venir.

Tout semble donc réuni pour que l'usage de la biométrie en entreprise décolle... Reste à trouver la « *killer app* » !



Événements

l'atelier solucom

observatoire du management des systèmes d'information

Le DSI face au risque

Le 22 septembre dernier, Solucom a organisé au RITZ un atelier sur la thématique « Le DSI face au risque », avec l'intervention exceptionnelle de Patrick Perretti-Watel, sociologue du risque.

les assises

de la sécurité et des systèmes d'information

Solucom présent aux Assises de la Sécurité

Comme tous les ans, Solucom participe aux Assises de la Sécurité à Monaco, **du 5 au 8 octobre 2011**. À cette occasion, nous présenterons un atelier sur le thème « **Comment intégrer filière sécurité de l'information et filière risque ?** ».

Voici deux domaines connexes qui gagneraient fortement à travailler ensemble. En effet ils ont un dénominateur commun : les risques !

Même si on constate souvent une volonté de rapprochement, l'expérience montre que ces deux domaines évoluent sur des périmètres différents avec des équipes, des pratiques et des référentiels distincts. Comment arriver à tirer le meilleur parti de chacun des domaines ? Quelles actions entamer pour obtenir une vision unifiée des risques ? Quelle place pour le risque SI ? Comment gérer les nouveaux risques ? Et surtout comment communiquer auprès de la direction générale de manière coordonnée ?

Cette présentation sera réalisée conjointement avec un responsable risque / sécurité de l'information qui témoignera sur son retour d'expérience.



Solucom maintient sa certification ISO 27001 sur les prestations d'audits de sécurité des systèmes d'information

En septembre 2008, l'offre audit du cabinet Solucom a été audité et certifiée ISO 27001 par l'organisme LSTI, accrédité par le COFRAC. Il s'agissait d'une première en France pour des prestations d'audit.

Cette certification a été à nouveau confirmée suite à un audit de surveillance trois ans après la certification initiale. Ce succès souligne la maturité du Système de Management de la Sécurité de l'Information (SMSI) de Solucom.

Un double partenariat pour Solucom

Dans la lignée du plan stratégique « Solucom 2015 », Solucom a initié des partenariats internationaux avec pour objectif de mieux accompagner ses clients dans leur développement international. Solucom s'est ainsi associé à Hydra Partners, un cabinet de conseil espagnol spécialisé dans les nouvelles technologies de l'information et de la communication, et à DMW group, un cabinet britannique indépendant de conseil IT.



Directeur de la publication :

Patrick Hirigoyen

Responsable de la rédaction :

Frédéric Goux

Contributeurs : Gérôme BILLOIS, Etienne BOUET, Amal BOUTAYEB, Marion COUTURIER, Ali FAWAZ, Matthieu GARIN, Chadi HANTOUCHE, Benoît TANGUY, Timoléon TILMANT.

Photographies :

Getty images
Fotolia

Graphiques :

Solucom

Conception graphique :

les enfants gâtés

Impression :

Axiom Graphics
ISSN 1995-1975

La Lettre Sécurité

revue de la *practice*
Sécurité & risk management
du cabinet Solucom

Tour Franklin,
100-101 terrasse Boieldieu
La Défense 8
92042 Paris - La Défense

solucom@solucom.fr
<http://www.solucom.fr>