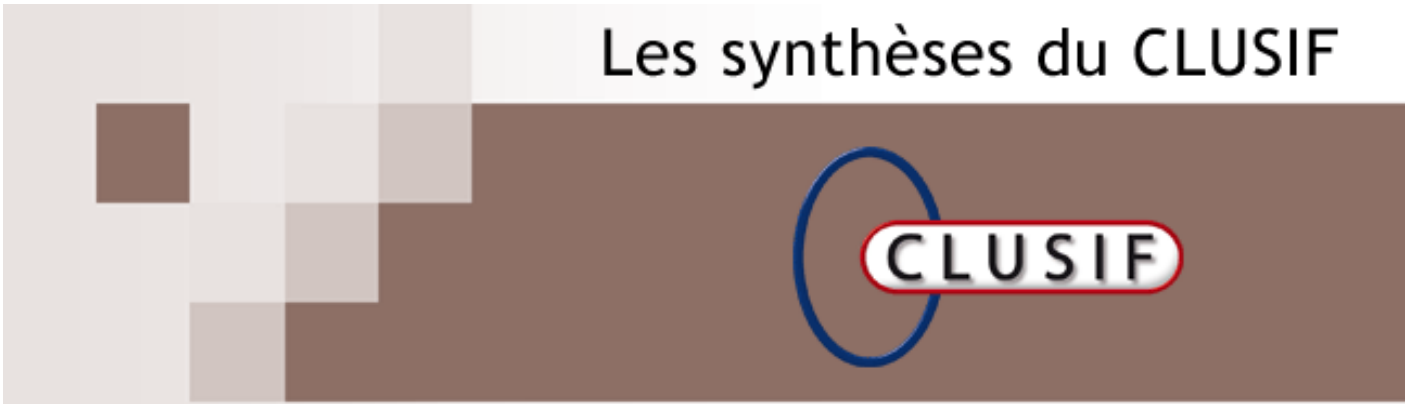

Sécurité de l'Information et Sécurité Physique - *Synthèse de la conférence thématique du CLUSIF du 15 décembre 2015.*

Si les enjeux liés à la sécurité de l'information sont, aujourd'hui, reconnus comme fondamentaux, la sécurité de l'information ne signifie pas uniquement sécurité informatique. La sécurité de l'information doit être vue comme une finalité et la sécurité informatique comme l'un des moyens permettant de l'assurer. Un autre moyen essentiel est la sécurité physique. En effet, quelle serait l'utilité d'une gestion des identités et des accès logiques si tout individu pouvait rentrer dans le Datacenter et voler ou détruire les serveurs? Bien entendu, une gestion efficace des accès logiques est fondamentale mais un contrôle des accès physiques l'est tout autant. Inversement, la sécurité de l'information, ou plutôt un déficit de sécurité de l'information, peut avoir des conséquences sur la sécurité physique : les serrures pilotées par des réseaux informatiques en sont un exemple.

Sécurité physique et sécurité informatique doivent donc être considérées comme deux constituants majeurs et complémentaires de la sécurisation de l'information, donc de la sécurisation des organisations et de leur processus.

Pour rendre compte de ces problématiques, le CLUSIF donne aujourd'hui la parole à trois intervenants, Sylvain CONCHON (Responsable opérationnel CONIX), Damien CHAMINADE (Expert Sureté et Sécurité Indépendant) et Alexis MILLOT (Expert Sécurité Physique OFC) qui chacun à leur manière éclaire ce lien entre sécurité physique et sécurité de l'information. Ces retours d'expertises ont été suivis par une table ronde animée par Jean-Marc GREMY (CLUSIF).

La vision du CLUSIF

Par Lazaro Pejsachowicz, Président, CLUSIF

La composante humaine est une des composantes essentielles des systèmes d'information. Après une première conférence sur la sensibilisation des collaborateurs de l'entreprise, la présente conférence apporte un éclairage supplémentaire sur l'environnement physique des systèmes d'information. D'autres conférences sur la même thématique suivront dans les mois à venir.

Les systèmes d'information évoluent dans un environnement physique vulnérable. Hormis les entreprises qui ont d'importants problèmes de protection physique telles EDF, Renault, la SNCF, la plupart des sociétés improvisent leur démarche de protection des biens et personnes. Et dans cet environnement, l'homme est un point faible.

Au vu de ce constat, comment organiser une convergence entre sécurité physique et sécurité logique ? Toute la difficulté est de trouver le bon point d'équilibre dans la collaboration. La frontière entre ces deux domaines est de plus en plus floue. Pour mettre en place cette collaboration, le RSSI doit se mettre en relation avec le Directeur de la Sécurité, également en charge de la sécurité physique.. Cette bonne coopération est d'autant plus indispensable que les frontières entre les éléments de sécurité physique et de sécurité logique ont tendance à s'effacer. Ce qui était avant une simple porte est aujourd'hui une porte télécommandée. Ce qui était avant un gardien est aujourd'hui une caméra d'identification 3D.

Aussi, bien que des progrès notables aient déjà été effectués, les voies de cette coopération ont tout intérêt à être développées.

Intégration de la sécurité physique à l'analyse de risque

Vers une méthode unifiée d'identification et d'appréciation des risques
Par Sylvain Conchon, Responsable opérationnel, CONIX

En préambule, quelques constats. S'il y a une maturité des pratiques pour la sécurité physique et une maturité des méthodes d'analyse des risques pour la sécurité de l'information, on observe une faiblesse de la prise en compte de la sécurité physique dans les analyses sécurité de l'information tout comme une difficulté à exprimer le risque dans le domaine de la sécurité des biens et des personnes. Pour faire converger ces deux domaines, il faut définir un cadre de référence analytique commun et une approche méthodologique reproductible, pertinente et réaliste. C'est ce que nous avons tenté de faire pour Orange dans le cadre de référence formel ISO 27005.

Comment avons-nous procédé? D'abord, je considère que le risque a une définition universelle : il est une fonction des vulnérabilités, des menaces et des impacts. Il faut donc caractériser ces trois variables. Les menaces et impacts sont caractérisés par ce qui a de la valeur, les actifs essentiels que l'on souhaite protéger d'une part, et les actifs «en support» sur lesquels porte la vulnérabilité, d'autre part. Les critères de sécurité (notamment la disponibilité, l'intégrité et la confidentialité) sont d'autres éléments à prendre en compte. Définir ces critères permet d'associer les scénarios de risques et les impacts et donc de réussir à mesurer le risque.

Tout un travail sémantique est à réaliser. Le vocabulaire RSSI et celui de la sécurité des biens et personnes peuvent différer, même si les terminologies utilisées en sécurité physiques sont souvent plus compréhensibles et imagées. Ainsi, les actifs primordiaux et actifs en support sont désignés comme des objets de risques et des cibles dans le vocabulaire de la sécurité physique. De même, les informations et fonctions sont des personnes ou des biens meubles ou immeubles ou des flux en sécurité physique.

Si les critères de sécurité bénéficient quasiment du même vocable dans les deux domaines, les cibles sont différentes. En matière de sécurité de l'information, l'ensemble des supports de l'information sont protégés : logiciels, matériel, réseau, site, organisation...et toutes les informations contenues dans les ordinateurs. A l'inverse, en matière de sécurité physique, on protège principalement des «tangibles», à savoir des personnes et des biens meubles et immeubles.

Une fois que le cadre de référence commence à prendre forme, il faut ensuite le peupler avec une base de connaissances d'objets de risque et de cibles permettant de construire des scénarios. Il faut pour cela identifier les menaces par catégories et associer chacune des menaces à un critère et à un objet de risque.

Pour notre base de connaissance, nous avons par exemple identifié chez Orange une quarantaine de menaces réputées exhaustives de différents niveaux tels les vols, agressions, dégradations, incendies (niveau 1) ou encore les cas de séquestrations et de pollution (niveau 2). Il a fallu ensuite construire le scénario et travailler sur les bases de connaissance de vulnérabilité en commençant par identifier des cibles en mentionnant la catégorie de la cible (bien immeuble, meuble ou personne), sa nature (bâtiment, équipements, personnel) et enfin la cible elle-même (équipement électrique, batteries, alarmes d'évacuation, détection d'incendie, détecteurs de gaz, câbles électriques, gaines et canalisations,...).

Nous avons construit ces bases de connaissances en nous appuyant sur les référentiels CNPP (Centre National de Prévention et de Protection) et sur les référentiels de sécurité de l'information mais aussi et surtout sur du bon sens. Certes, ces bases de connaissances restent à construire en matière de sécurité physique. C'est un travail conséquent mais assez simple lorsque l'on peut s'appuyer sur les retours des auditeurs terrain.

En conclusion, cette méthodologie de modélisation des cibles, menaces et vulnérabilités permet de créer un cadre de référence analytique qui apporte de la cohérence et de la complétude aux conclusions de l'audit terrain. En aucun cas, il n'est conçu pour le remplacer. Il se sert des conclusions du terrain pour mieux les représenter. La sécurité de l'information ne doit pas faire de la sécurité physique, ce n'est pas son métier.

Notons, en outre, que travailler avec une telle méthodologie permet d'avoir une démarche reproductible et répétable dans de nombreux domaines comme la sûreté de fonctionnement, les risques psycho-sociaux, les risques projet ou encore les risques de responsabilité sociétale.

Enfin, si le management unifié des risques n'est peut-être pas pour demain, les domaines de la sécurité physique et logique peuvent se chevaucher (exemple pour les droits des contrôles d'accès), c'est pourquoi il est indispensable d'arriver à des modèles communs.

Retour d'expérience : Exemple de convergence entre sécurité logique et sécurité physique

Par Damien Chaminade, Expert Sureté indépendant

Dans le cadre d'une entreprise de retail de 20.000 salariés, j'ai été en charge de l'installation d'un système de vidéoprotection, de contrôle d'accès par badge et de détection d'intrusion sur 110 sites du groupe. En voici le retour d'expérience.

Ce groupe était confronté à de nombreux incidents : des vols (palettes, ordinateurs, prototypes...), du vandalisme, de l'espionnage, ou encore des intrusions et agressions de salariés. Suite à un audit, nous avons constaté que les mesures de protection physiques étaient largement perfectibles. Les locaux notamment étaient mal protégés avec des flux des piétons et véhicules insuffisamment organisés. De même, il y avait des problèmes de gardiennage (manque de formation des gardiens, déploiement non sécurisé des outils). Enfin, la gouvernance de la protection de l'information se devait d'être renforcée pour disposer notamment d'un pilotage global et d'une architecture logicielle sécurisée.

Ces constats ont permis de dégager trois enjeux : réduire le coût des actes malveillants, mieux protéger les informations sensibles et les actifs et enfin dégager des synergies avec le business. Pour y répondre, il fallait renforcer la sécurité physique sans que la sécurité logique de la nouvelle architecture ne constitue un risque supplémentaire (d'où une vigilance particulière sur la confidentialité, la disponibilité, l'intégrité, mais aussi la conformité à la réglementation). A ces deux objectifs, s'en ajoute un troisième essentiel, la sensibilisation des résidents (salariés, visiteurs) aux risques et aux enjeux. Les incidents, outre leur coût financier, peuvent également avoir un coût social.

La gestion de projets a été mise en œuvre avec un audit de sûreté, un cahier des charges, la validation du CE, puis la réalisation des travaux. Ainsi, de nouveaux systèmes de vidéosurveillance, de contrôle d'accès et de détection d'intrusion ont été déployés dans une architecture locale séparée mais interfacée avec l'architecture centrale de l'entreprise. Lecteurs de badge, barrières infra-rouge, détecteurs de présence, lecture automatique de plaque d'immatriculation...Cette mise en œuvre a été réalisée en coordination avec l'ensemble des services de l'entreprise. En particulier la RH pour le côté gestion des identités et contrôle d'accès, le CE pour l'autorisation de la vidéo et le CIL et la CNIL pour vérifier le respect des réglementation en vigueur.

A ce jour, le déploiement a été réalisé sur 90% des sites et a permis de réduire le nombre d'incidents de plus de 70%. L'aspect dissuasif de la vidéo n'y est sans doute pas étranger.

De même, l'analyse post incident s'est également améliorée. Le fait de disposer d'outils sur le contrôle d'accès et l'historique des accessions sur un site a permis de mieux analyser les incidents et d'avoir un taux de résolution de ceux-ci beaucoup plus élevé (80% dorénavant).

Le fait de centraliser l'architecture et de nommer un chef de projet conformité s'est traduit par 100% de conformité sur l'ensemble des sites. Nous avons eu pour cela l'assentiment des représentants du personnel qui nous ont même demandés de rajouter des caméras dans certaines zones.

En termes de RH, le badge unique a facilité les visites de salariés inter-sites et renforcé le sentiment d'appartenance à l'entreprise. La nouvelle solution a aussi permis de réduire les coûts de maintenance de 40% et les coûts des incidents jusqu'à -95% sur certains sites. Ces bons chiffres ont eu pour conséquence de nouveaux gains comme la réduction des primes d'assurances (1 million d'euros d'économie) et des notes de frais (car le badge unique permet aux salariés de pouvoir déjeuner dans les restaurants de n'importe quel site). De même, nous avons pu réduire les coûts de climatisation et d'éclairage des salles de réunions grâce à un système de géolocalisation anonyme du support de badge nous permettant de savoir si une salle est vide et donc de couper l'électricité le cas échéant.

En conclusion, il est à souligner que les objectifs ont été atteints au-delà des espérances, avec un retour sur investissement d'à peine un an. En revanche, de nouveaux risques sont apparus. La règlementation française impose parfois, en cas d'alerte incendie ou d'évacuation de bâtiment, de désactiver le contrôle d'accès physique.

N'oublions pas non plus que la composante humaine, si elle rend vulnérable des Fort-knox et autres sites ultra-sécurisés, est elle est aussi une parade : un salarié bien sensibilisé sera en effet toujours plus efficace que n'importe quel lecteur de badge et caméra.

Enfin, dernier conseil, pas de déploiement efficace sans une gouvernance centralisée ou a minima une attention sur l'adhésion (top management, utilisateurs, salariés…), surtout dans un contexte matriciel.

Escalade de privilège en sécurité physique

Obtenir le Passe Partout d'un Organigramme de Clefs
Par Alexis Millot, Expert en Sécurité Physique, OFC

Je veux attirer votre attention sur l'importance des systèmes de clés pour garantir la sécurité physique et logique. En effet, la gestion des clés est l'un des points faibles de la sécurité des entreprises. Très souvent, on se sert de passes universels pour ouvrir toutes les portes et de passes partiels pour avoir accès à certaines salles. Ces passes sont souvent réservés aux personnels d'entretien, informaticiens ou encore aux sous-traitants. Problème, le piratage de ces clés, quel que soit leur type, est très aisé. Ainsi, l'organigramme conventionnel, très utilisé notamment dans les PME sur lequel chaque cylindre possède la combinaison du Passe Général peut poser des problèmes de sécurité. En la matière, plusieurs clés ouvrent une même serrure, or plus il y a de clés, plus il y a de failles. Comme le cylindre contient la combinaison du Passe, il suffit d'analyser son contenu et fabriquer plusieurs clés (nombre de clés généralement très faible) pour trouver le Passe. Un attaquant est alors sûr de posséder la combinaison du Passe Général (PG), et ainsi de pouvoir ouvrir toutes les portes du bâtiment concerné !

Dans les grandes sociétés, on préfère utiliser un organigramme positionnel, il s'agit de clés de type « micropoints ». Le codage de la clé est réalisé par la positon des trous. Le cylindre ne contient donc pas la combinaison du PG. Celui-ci correspond à la somme de toutes les combinaisons de clés possibles. Si deux clés différentes n'ont pas les trous positionnés aux mêmes emplacements, en pratique, très peu de clés sont nécessaires pour réaliser un Passe Partiel ou un Passe Général (selon la complexité de l'organigramme). Il suffit d'ajouter quelques trous à la clé pour qu'elle devienne un Passe Général.

Comment se prémunir contre tous ces risques ?

Première mesure possible, protéger les cylindres contre le démontage. Autre parade contre la fabrication frauduleuse, sélectionner des clés protégées que l'on ne trouve pas dans le commerce. L'utilisation d'organigrammes composés d'un codage à la fois positionnel et conventionnel est une autre voie.

Attention en revanche aux armoires à clés, très séduisantes sur le papier. Il suffit à une personne malveillante de prendre des photos voire des empreintes des clés dans cette armoire pour se fabriquer ensuite des passes. De même, proscrivez l'utilisation de cylindres d'organigramme sur les lieux les plus sensibles. Et enfin, n'oubliez pas de sensibiliser vos équipes et de leur demander de faire remonter toute activité inhabituelle, comme la disparition de serrures ou de clés, même de bas niveau.

Table Ronde et session de questions/réponses animées par Jean-Marc GREMY, Vice-Président du CLUSIF

La convergence entre sécurité physique et logique n'est-elle pas inéluctable ?

> **Sylvain Conchon :** La sécurité physique doit s'appuyer sur les pratiques de la sécurité logique et réciproquement. Ces deux domaines partagent souvent des problématiques communes et, dans certains cas, un vocabulaire identique, exemple, la notion de détection d'intrusion est utilisée dans les deux mondes. En cela, les domaines convergent déjà et sont de plus en plus indissociables.

Les aspects de conformité comme par exemple la protection des données individuelles ne sont-ils pas un obstacle à cette convergence ?

> **Damien Chaminade :** La direction de la conformité et les correspondants Cnil en interne doivent plus être perçus comme des garde-fous que des obstacles. Outre ces deux instances, les formations au maniement de données des acteurs de la direction juridique, la direction sûreté, la direction de la sécurité informatique sont indispensables.
>
> **Alexis Millot :** Si la CNIL préserve les données personnelles, on peut cependant travailler sur des données non nominatives et comparer des données statistiques d'un site à l'autre de manière intéressante afin de repérer des anomalies.

Comment faire en sorte que les salariés portent leur badge de manière apparente et visible?

Damien Chaminade : Le top management doit s'appliquer la règle à lui-même : si le président et les membres de la direction portent un badge alors tous les salariés auront tendance à suivre. On pourra mettre en œuvre des sensibilisations différenciées en fonction des publics de l'entreprise : pour les uns on insistera sur les aspects sociaux ou financiers, pour les autres sur les aspects sécuritaires par exemple. Ces sensibilisations régulières permettent de rappeler les bonnes pratiques et d'obtenir des remontées d'incident. Mais attention, parfois dans certaines entreprises la protection de l'info n'est pas naturelle. Avant d'entreprendre des actions, il faut bien mesurer la culture d'entreprise et son rapport à la sécurité.

Alexis Millot : Plus le badge est un outil indispensable (café, imprimante, accès aux différents secteurs de l'entreprise,) à la vie dans l'entreprise, plus le salarié va l'utiliser et le porter. S'il sert à tout, le salarié l'aura en permanence sur lui le plus souvent de manière apparente. Autre voie, le bâton et la peur du gendarme. Le non-respect du port du badge peut se traduire par une sanction prévue par exemple dans le règlement intérieur. Après tout, l'employeur n'a-t-il pas l'obligation légale d'assurer la sécurité de ses salariés ?