PRIMORIS
ASSOCIATES INC.

Évaluation des menaces, des risques et des vulnérabilités – Pourquoi ?

Livre blanc

LA FONDATION DE TOUTE SÉCURITÉ

Toutes les mesures de sécurité découlent de l'évaluation des menaces et des risques (EMR). Si l'on ne sait pas avec un degré de certitude élevé ce qui doit être protégé dans l'organisation et sa valeur, il sera difficile de choisir les mesures de protection appropriées pour éviter la perte de ces biens. Si l'on ne peut établir une liste de vulnérabilités et leur gravité, les mesures de protection appliquées peuvent être inappropriées ou inefficaces. Si l'on ne comprend pas l'efficacité des mesures de sécurité existantes, tous les actifs sont menacés. Et enfin, si une approche méthodique n'est pas adoptée pour comprendre les menaces pesant sur les actifs et l'organisation, des mesures de

sécurité, même s'ils sont efficaces, échoueront. L'évaluation des menaces et des risques déterminera tous ces aspects.

Dans notre métier, nous avons vu une grande diversité d'approches. Souvent, une organisation occupera un bâtiment et se verra remettre des clés, un système de contrôle d'accès, un système d'alarme et un système de caméra fourni par l'architecte. Cette approche présente un certain nombre de défauts évidents : l'architecte n'en sait peut-être pas assez sur l'activité principale de l'entreprise pour concevoir des systèmes de protection et ne conçoit généralement qu'un système pour le bâtiment de base ; bien souvent, l'organisation ne compte pas de professionnel de la sécurité dans ses rangs et le Département des installations est alors le de facto responsable de la sécurité. Aucune approche systématique n'a été mise en œuvre vis-à-vis des opérations d'affaires pour en sécuriser correctement l'entièreté. La vraie solution est l'EMR.

L'évaluation des menaces et des risques constitue la pièce maîtresse de toutes les mesures de sécurité.

La sécurité « par des rondes » ne fonctionnera pas

Ce que nous avons maintes fois constaté est qu'une brèche éventuelle dans la sécurité incitera un gestionnaire non formé à la sécurité à effectuer « des rondes de sécurité ». Dans le cas typique, une introduction par effraction et un vol se sont produits et un gestionnaire examine maintenant la zone concernée ; il indique alors où les nouvelles caméras et les nouveaux capteurs d'intrusion seront placés en pointant du doigt. Parfois, ces actions seront accompagnées par la présence d'un gardien se sécurité temporaire ou par une toute nouvelle approche de sécurité. Pour nous, c'est comme si un non-médecin dirigeait une opération : les solutions apportées coûteront cher et seront plus ou moins efficaces.

Après un tel incident, quelqu'un pourrait suggérer qu'un professionnel de la sécurité puisse éventuellement présenter des solutions et, effectivement, nous sommes souvent invités à faire un « examen de sécurité ». Dans telle démarche, l'entreprise s'attend à ce que nous examinions toutes les mesures de sécurité en place et présentions un diagnostic précis. Bien que ce soit un moment opportun pour expliquer et recommander une EMR, l'implication des professionnels de la sécurité à l'étape de la conception demeure des plus efficaces et économiques.

Les EMR utilisent des méthodologies connues

Les professionnels en matière de sécurité ont accès à diverses méthodologies d'évaluation des menaces et des risques. Étant donné que nous avons beaucoup travaillé avec le gouvernement fédéral, nous connaissons bien la Méthodologie harmonisée d'évaluation des menaces et des risques (2009). Nous sommes membres d'ASIS International et sommes très familier avec sa

méthodologie. Nous utilisons l'outil CARVER (Criticité, Accessibilité, Récupérabilité, Vulnérabilité, Effet et Reconnaissance). L'Australie et la Nouvelle-Zélande disposent de l'outil de gestion des risques AS-NZS 4360 qui est très crédible. MSHARPP (mission, symbolisme, histoire, accessibilité, reconnaissabilité, population, proximité) est également un outil populaire, semblable à CARVER et particulièrement utile dans les environnements militaires. Nous avons utilisé des méthodologies fournies par les banques et les installations nucléaires. Nous disposons d'une liste de 15 méthodologies pour les systèmes de technologie de l'information.

Quel que soit celle que vous choisissez, le processus et le résultat seront semblables. Chaque méthodologie aura besoin d'une approche méthodique pour : identifier et évaluer les actifs, évaluer les systèmes de sécurité, analyser les vulnérabilités et découvrir toutes les menaces existantes. Une fois cette information connue, le risque peut être calculé en utilisant une formule de risque commune R f Aval, T, V (Le risque est fonction de la valeur de l'actif, des menaces et des vulnérabilités). Regardons chaque composante individuellement.

Les composantes essentielles de l'EMR

La protection des actifs est la raison essentielle de la sécurité.
Si une organisation n'a rien de valeur, rien n'a besoin d'être protégé. Un magasin qui vend des vêtements d'occasion à partir de dons n'a pas besoin d'un système avancé de détection d'intrusion et de caméras de sécurité, leur coût ne pouvant logiquement être justifié dans les résultats fiscales. Alors, comprendre la valeur des actifs est la pièce maîtresse de l'EMR.

L'EMR catégorise les actifs

La plupart des EMR partagent les actifs dans quatre catégories : les ressources physiques, les personnes, l'information et les choses intangibles. Les ressources physiques dont une entreprise dispose pour fonctionner peuvent toutes recevoir une valeur monétaire, mais toutes ne sont pas comptabilisées dans une EMR. Nous comprenons ici que les actifs physiques de faible valeur comme les bureaux, les chaises et les ordinateurs qui ne feront que brouiller les résultats. Nous incluons plutôt les bâtiments, les systèmes informatiques, les véhicules, les gros équipements, etc. Généralement, une valeur en dollars est attribuée en fonction de la valeur relative de tous les actifs. Nous avons utilisé des chiffres aussi bas que 4 000 $ et aussi élevés que 100 000 $. Les actifs physiques peuvent également avoir une valeur intrinsèque ; nous entendons par là une valeur supérieure à la valeur monétaire. Par exemple, nous avons déjà fait une EMR où un technicien de laboratoire nous a indiqué un microscope électronique d'une valeur 300 000 $, disant que c'était l'équipement le plus coûteux du laboratoire. Mais vite il a montré un autre équipement avec une valeur relativement mineure disant que s'il n'avait pas cet équipement, il ne pourrait pas faire son travail. C'est ce qu'on appelle une valeur intrinsèque. Les pièces de rechange critiques de même que le système d'approvisionnement juste-à-temps entrent dans cette même catégorie.

Les personnes – un défi

Les personnes représentent un dilemme important dans les EMR. Toutes les entreprises ont tendance à utiliser le mantra « nos employés sont nos plus grands atouts ». Bien que cela soit sans doute vrai, pour l'EMR, les personnes n'ont pas une grande valeur. Nous avons tendance à dire que si un employé joue un rôle critique, de telle sorte que s'il était retiré de l'organisation, celle-ci s'arrêterait ou du moins tremblerait, alors cet employé aurait une grande valeur. Force est de constater qu'il s'en

trouve peu dans les organisations. En fait, une telle situation créerait une vulnérabilité pour l'organisation. Nous considérons que les groupes d'employés ont une valeur plus élevée, par exemple : les cadres supérieurs, les ingénieurs. Nous recommandons souvent une politique de déplacement qui interdit à toutes ces personnes de voyager ensemble sur le même mode de transport en raison de la vulnérabilité créée. En définitive, les personnes n'ont généralement pas une grande valeur dans une EMR et ce sujet doit être abordé avec soin avec le client. On peut imaginer le problème de l'EMR si une entreprise possédait 500 actifs ambulatoires de grande valeur.

L'informations en tant qu'actif

L'information a généralement une grande valeur dans une organisation, mais comme peu de sociétés privées souscrivent à des systèmes de classification de la sécurité de l'information, il est souvent difficile de l'établir concrètement. Nous donnons plus de valeur à l'information qui a une sensibilité plus élevée. Les gouvernements sont bien au fait de cela. Ils utilisent un schéma pour classer les informations afin de mieux comprendre comment les traiter, c'est-à-dire : création, transmission, stockage, élimination. Les entreprises privées ne font généralement pas l'effort de créer un tel système de classification. Néanmoins, le rôle de l'analyste est d'identifier cela comme un problème et de recommander des systèmes de classification de sécurité de l'information, même rudimentaires.

Qu'en est-il des actifs intangibles ?

Les actifs intangibles doivent être identifiés et évalués. Parmi ceux-ci on retrouve : la réputation de l'entreprise, sa crédibilité au sein de la communauté, le sentiment de bien-être des gens au travail, et la valeur de son image. Comme on peut l'imaginer, ce sont des choses difficiles à évaluer. Dans notre expérience, nous retrouvons des professionnels

dans des entreprises fièrement appliquant leurs compétences au mieux de leurs capacités. Pour eux, leur réputation professionnelle, et donc la réputation de l'entreprise, ont une grande importance. Nous retrouvons des organisations menant des processus dont la communauté locale peut se méfier. Ces organisations réalisent l'importance de la licence sociale qui leur a été accordée pour fonctionner. Nous comprenons également la valeur des employés satisfaits et l'importance de leur sentiment de bien-être au travail. Nous avons tendance à évaluer toutes ces choses comme étant élevées et parfois très élevées selon la sensibilité des activités de l'entreprise, par exemple : l'exploitation minière, la transformation nucléaire, gouvernement, etc.

La sécurité « par des rondes » ne fonctionnera pas

Les autres éléments de l'évaluation des menaces et des risques feront l'objet de futurs documents. Cependant, nous avons jugé approprié de discuter de ces facettes initiales des évaluations des menaces et des risques. En raison du nombre d'EMR que nous avons effectué, nous sommes fervents croyants que « la sécurité par des rondes » par des gestionnaires non formés à la sécurité ne peut jamais être efficace. Nous croyons également que la création d'une véritable sécurité nécessite une approche professionnelle. Nous avons vu de nombreuses organisations qui ont demandé aux employés de l'établissement de se préoccuper de la sécurité et de tenter de la maintenir. Nous avons également vu la sécurité assignée aux professionnels de la santé et de la sécurité, mais c'est toujours quelque chose qui se fait à temps perdu au coin de leur bureau. Nous avons vu des organisations se tourner vers les gardiens de sécurité sous contrat pour obtenir des conseils sur la sécurité d'entreprise. Nous ne pouvons pas imaginer comment cela pourrait fonctionner.

Conclusion

L'évaluation des menaces et des risques constitue la pièce maîtresse de toutes les mesures de sécurité. C'est une approche méthodologique pour identifier tous les biens à protéger et tous les éléments qui peuvent représenter des risques. Elle devrait être effectuée par un professionnel de la sécurité formé et expérimenté et toutes les recommandations devraient être évaluées pour un retour sur investissement et un calendrier pour savoir quand elles seront appliquées. Après l'application de toutes les recommandations, il y aura un risque résiduel et ce risque devrait faire l'objet d'un registre revu mensuellement par la direction. Nous espérons que ce court article apporte un certain éclairage sur à ce sujet important et vous fera réfléchir sur votre propre situation de risque dans votre entreprise.

Bureau: 514-418-4609 | info@primorisinc.ca | www.primorisinc.ca