Augmentez le niveau de protection de votre entreprise face à la malveillance externe et interne

Les objectifs d'un système de protection

Pour qu'il soit efficace, un système de protection devra être conçu de telle manière qu'il puisse remplir les fonctions suivantes :

- Dissuader l'intrus
- Compliquer son accès au site
- Détecter son intrusion à temps
- Retarder sa progression
- Permettre son interception

Le dispositif se présente sous forme de cercles partant de l'environnement extérieur jusqu'à l'objet convoité.

La méthode choisie doit s'incorporer dans la culture et la politique générale de l'entreprise.

L'implication de la Direction dans la mise en place du système de protection et son engagement à faire respecter les procédures mises en œuvre sont donc essentiels.

La conception du système

En fonction des particularités du site à protéger, le système de protection se compose d'un mariage harmonieux d'éléments architecturaux, de protections mécaniques et électroniques ainsi que de procédures administratives. Nous en mentionnons ici les principaux :

- étangs ;
- monticules ;
- barrières architecturales, telles que portails et clôtures servant à délimiter l'ensemble du périmètre;
- contrôles et procédures d'accès ;
- systèmes de verrouillage;
- dispositifs d'éclairage ;
- réseau de télésurveillance facilitant la détection et la présentation de preuves en matière pénale;
- technologie électronique permettant la détection d'accès non autorisés;
- protection ponctuelle pour les objets de valeur représentant la cible de l'intrus;
- communication claire pour la transmission d'une alarme et la prise de décision rapide d'une méthode d'interception appropriée;
- procédures et règles de sécurité;
- protection des données et de la propriété intellectuelle.

Un système de protection bien conçu permet de déterminer avec précision et rapidité les causes d'une alarme.

Un système qui ne permet pas de déterminer les causes d'une alarme n'a aucune valeur puisqu'il empêche l'entreprise de prendre les mesures nécessaires à la neutralisation de l'intrus.

Le temps dont a besoin l'intrus pour atteindre sa cible, en tenant compte des obstacles qui sont dressés devant lui, est un critère déterminant pour mesurer la fiabilité de l'ensemble des mesures de protection.

Tel. ++41(0)32/724 11 24
www.cmr-services.ch
info@cmr-services.ch
Faubourg de l'Hôpital 13
Case postale
2001 Neuchâtel

L'identification des vulnérabilités

La vulnérabilité exprime la faiblesse du dispositif visant à protéger les biens de l'entreprise. Le terme englobe le bien digne de protection ainsi que le risque susceptible de le menacer.

Le risque peut être défini comme la combinaison de la probabilité de la survenance d'un événement et de ses conséquences. Pour exprimer le degré de vraisemblance qu'un événement se produise, on pourra recourir à des termes comme *rare*, *invraisemblable*, *modéré*, *presque certain*. Les conséquences peuvent englober des aspects positifs et des aspects négatifs. Les conséquences sont cependant toujours négatives pour les aspects liés à la sécurité. Leur impact peut être défini comme étant *négligeable*, *faible*, *moyen*, *important* ou *catastrophique* en fonction des ressources propres de chaque entité.

Cette adéquation entre vulnérabilité et risque permet de déterminer le degré d'acceptation d'un événement redouté. On dressera en premier lieu une hiérarchie des risques en fonction de la probabilité d'occurrence de l'événement et de la gravité des conséquences. On allouera les ressources qui doivent servir en priorité à réduire les risques dont la survenance pourrait entraîner de graves dommages pour l'entreprise.

Il faut donc toujours veiller à cet équilibre car tout système de sécurité doit être adapté aux vulnérabilités et ne pas constituer une entrave au bon déroulement des activités, ni entraîner une surcharge administrative ou procédurale qui conduiraient inévitablement au non-respect des règles par le personnel au quotidien.

Les procédures existantes, la sécurité du personnel ainsi que les éventuelles normes et exigences légales applicables doivent également être prises en considération lors de l'élaboration du concept.

La définition des menaces

La menace englobe la source et les éléments caractéristiques de l'événement redouté.

Dans le contexte de la sécurité, la source est un phénomène dangereux.

La menace peut être de nature criminelle, naturelle ou accidentelle.

En matière de malveillance, l'aspect criminel est prépondérant et le contexte géographique, politique et social est à prendre en considération pour déterminer l'ampleur de la menace.

Le niveau de sécurité à mettre en place dépend donc largement des capacités de nuisance de l'intrus qui constitue la menace.

Nous énumérons les catégories suivantes d'intrus :

- le criminel amateur (ne disposant pas de compétences spécifiques, acte commis de manière spontanée);
- le criminel professionnel (disposant de moyens et de connaissances techniques étendues);
- le collaborateur déçu (capable de causer un dommage par dépit ou sentiment de vengeance);
- l'individu désorienté (personne confuse, instable ou malade);

- l'activiste et le contestataire (personne opposée aux activités de l'entreprise);

- le terroriste (criminel mû par des motifs politiques ou religieux).

Ces catégories de personnes peuvent être externes ou internes à l'entreprise. Il arrive aussi qu'une personne externe à l'entreprise bénéficie de la complicité d'une personne travaillant dans l'entreprise.

Les intrus recourent à la tromperie, souvent à l'usage de la force, à l'intrusion furtive ou à la combinaison de ces différentes méthodes.

Les protections « physiques » constituent les moyens les mieux appropriés pour lutter contre l'intrusion externe alors que les procédures de sécurité mises en place représentent les moyens qui sont les mieux adaptés pour lutter contre l'intrusion interne.

La détermination des cibles

Dans la plupart des cas, les cibles qui sont visées par des intrus peuvent être identifiées sans difficulté.

Par contre, pour des sites plus complexes, il est nécessaire de recourir à des techniques d'analyses plus poussées qui permettent l'identification des objectifs et des moyens que l'intrus doit mettre en œuvre pour les atteindre.

CMR Services SA effectue une approche systématique en recourant à l'arbre des défaillances.

Cette méthode utilise une structure arborescente pour représenter les événements élémentaires (cause de défaillance) et leurs combinaisons conduisant à l'occurrence d'un événement redouté. Les combinaisons des événements élémentaires sont réalisés par des liens (ou portes) logiques. Cette méthode est utilisée à titre préventif.

L'arborescence inclut la cible et les différents chemins pour l'atteindre. La représentation graphique permet d'avoir une image intégrale du système de sécurité en place en mettant en évidence les éventuelles failles qui devront être corrigées. Le caractère évolutif du risque est pris en compte car il suffira ensuite d'adapter et de modifier ce diagramme lors de tout changement qui intervient dans l'organisation ou la structure de l'entreprise.

L'évaluation des performances

L'évaluation des performances constitue un élément vital du concept de sécurité car il évite un gaspillage des ressources et la création d'un système trop compliqué qui ne sera pas respecté par la suite. En fonction de l'identification des différentes cibles, le degré de sécurité à l'intérieur d'une même entreprise peut être maintenu à des niveaux distincts.

La performance est mesurée en fonction des paramètres de probabilité de détection, de la capacité à identifier le problème, des délais de riposte et de la qualité des moyens de communication.

L'unité de mesure employée par CMR Services SA est le point de détection critique (PDC). Celui-ci se situe sur l'itinéraire choisi par l'intrus au point précis où le délai dont il a besoin pour atteindre sa cible est encore légèrement supérieur au temps qui est nécessaire pour son interception après l'identification du problème.

Tel. ++41(0)32/724 11 24
www.cmr-services.ch
info@cmr-services.ch
Faubourg de l'Hôpital 13
Case postale
2001 Neuchâtel

L'itinéraire le plus vulnérable, c'est-à-dire, celui qui offre la probabilité de détection la plus faible, constitue le chemin critique.

Des améliorations ciblées sur ce maillon faible permettent ainsi d'augmenter la valeur de l'ensemble du dispositif en préservant un rapport coût/bénéfice approprié. Les probabilités cumulatives de détection de l'ensemble du dispositif permettent de déterminer avec précision le PDC et d'évaluer ainsi la qualité de la protection globale du site.

****