Terrorisme et extrémisme
Les mesures de protection que les entreprises peuvent prendre

Sara Neven

Table des matières

Préface

Par cette brochure, nous essayons de vous donner un aperçu général des mesures de protection contre des actions terroristes et extrémistes dans le secteur privé. Elle a pu être réalisée grâce à la collaboration entre le secteur privé – la FEB[1] – et le secteur public au sein du groupe de travail « Terrorisme », créé dans le cadre de l'organe de concertation privé/public, PCPE[2]. Le but de cette brochure n'est nullement d'élaborer des nouvelles mesures de sécurité, mais uniquement de réunir, de manière synoptique, toutes les mesures de sécurité existantes et appliquées dans le domaine de la lutte contre le terrorisme et l'extrémisme.

Ce groupe de travail s'est fixé comme double objectif, d'une part, le développement d'un canal de communication entre les deux secteurs en cas d'actions terroristes ou extrémistes et, d'autre part, la rédaction, par le secteur public, d'une brochure destinée au secteur privé devant lui permettre de voir comment il peut se protéger contre d'éventuelles actions de nature terroriste ou extrémiste.

Le premier objectif est réalisé par la création d'un « Early Warning System », c.-à-d. un système d'avertissement rapide basé sur le carré d'information permettant une meilleure communication entre le secteur privé et le secteur public.

Pour couper le mal à la racine, les actions entreprises par les autorités publiques peuvent être complétées par des démarches préventives émanant des entreprises. En effet, celles-ci doivent tenir compte du fait que les terroristes ou les extrémistes peuvent, par leurs actions, causer des dégâts dont les conséquences peuvent être considérables et de diverses natures. En élaborant une politique de prévention, il est possible de prévenir une action terroriste ou extrémiste ou, en tout cas de réduire les éventuels dégâts.

[1] FEB = Fédération des Entreprises de Belgique
[2] PCPE = Plate-forme de concertation permanente en matière de protection des entreprises

La brochure comprend trois parties. La *première* partie consiste en une analyse du phénomène du terrorisme visant les entreprises. La *deuxième* partie explique comment les principes du « management de prévention » peuvent être mis en œuvre dans l'entreprise et de quels facteurs on peut tenir compte pour que ce management soit effectif. Après avoir évoqué l'analyse des menaces et des risques, elle aborde différentes étapes d'un *Continuity Plan* (plan de continuité) permettant de surmonter des situations imprévues. La *troisième* partie fournit les tuyaux, recommandations et conseils en matière de prévention pour que l'entreprise soit à même de répondre efficacement aux menaces concrètes ou potentielles d'actions terroristes ou extrémistes, et ce tant au niveau de l'organisation, de l'architectonique, de l'électronique, des TIC[1], que des RH[2].

Enfin, nous voulons remercier tous ceux qui ont prêté leur contribution à la réalisation de cette brochure et plus particulièrement les services du secteur public (la Direction générale Centre de crise du Service Public Fédéral Intérieur, le Service de la Politique criminelle du Service Public Fédéral Justice, le Groupe Interforces Anti-terroriste, la Sûreté de l'Etat, la Police fédérale DGJ/DJP/Service Terrorisme et Sectes[3], où j'ai effectué mon stage et réalisé la présente brochure), ainsi que les responsables de la sécurité de plusieurs entreprises du secteur privé sans lesquels il n'aurait pas été possible de rédiger cette étude (Jan Steenlant de la FEB, Dirk Ceulemans de Food Security, Yvan De Mesmaeker d'Omega Risk, Paul Robrechts de La Poste, Karel Vankeirsbilck de Belgacom, Gilbert Geudens de Carrefour Belgium, Jean-Paul Vandenhoeck d'Interbrew, Freddy Pardon de BASF Antwerpen N.V, Bruno De Keyzer et Peter De Meyer de Janssen Pharmaceutica N.V). Je voudrais également remercier le maître de stage de la KULeuven, le prof. Dirk Van Daele,

Pour terminer, je remercie aussi toutes les autres personnes qui ont contribué à la réalisation de cet ouvrage.

Sara Neven, stagiaire en criminologie
2ème licence à la Katholieke Universiteit Leuven

[1] TIC = Technologie de l'Information et de la Communication
[2] RH = Ressources humaines
[3] DGJ = Direction générale de la Police judiciaire
DJP = Direction de la Lutte contre la criminalité contre les personnes

Introduction

Depuis longtemps, le terrorisme est une donnée géopolitique actuelle. Ce sujet n'ayant plus guère quitté l'actualité, la société civile s'est progressivement rendu compte que l'on ne peut ignorer le terrorisme et l'extrémisme. Non seulement les autorités publiques et les citoyens s'intéressent en priorité aux questions de sécurité et de protection, mais aussi le secteur privé. Lui aussi a pris conscience du fait qu'il peut être la cible des groupements terroristes et qu'il devra tenir compte d'éventuelles menaces permanentes de leur part.

On ne peut pas perdre de vue le risque que des attentats terroristes soient perpétrés et qu'ainsi, l'infrastructure industrielle pourrait en grande partie être détruite. En effet, les organisations terroristes et extrémistes connaissent très bien l'impact et l'importance stratégique qu'un attentat peut avoir. Ses conséquences peuvent être très divergentes. La population se trouvera confrontée à des sentiments d'insécurité et les conséquences économiques et politiques sur notre société se feront sentir encore longtemps après l'attentat.

Afin d'être mieux armées contre des menaces terroristes, les entreprises ont tenté de prendre des mesures de sécurité spéciales, et ce non seulement par des méthodes physiques classiques de sécurité, mais aussi par une politique de management de prévention.

A cet effet, une plate-forme permanente de concertation entre le secteur privé (la FEB) et les autorités publiques a été créée à l'initiative du ministre de la Justice en 2002 étant donné qu'une bonne collaboration entre ces deux secteurs peut contribuer de manière constructive à la prévention et à la lutte contre le terrorisme[1].

Il en est résulté, d'une part, un schéma de communication entre les acteurs concernés par le terrorisme. Ce carré d'information ou Early Warning System tente de produire un flux d'informations structuré à partir des entités locales vers les partenaires fédéraux et vice versa.

[1] La collaboration entre le secteur privé et le secteur public ne se manifeste pas seulement dans le cadre du groupe de travail 'terrorisme', mais aussi dans celui des groupes de travail « criminalité organisée », « protection du potentiel scientifique et économique » et « criminalité informatique »

D’autre part, le but était de rédiger une brochure destinée au secteur privé, lui permettant de voir comment il peut se protéger au maximum contre les menaces et les crimes terroristes[1].

[1] DGJ/DJP/ Service terrorisme et sectes, *Rapportage sur l’exécution du plan national de sécurité, Bruxelles*, DGJ/DJP/ Service terrorisme et sectes, 2004, 5

PARTIE 1

Analyse du phénomène : Le terrorisme dans le monde des entreprises

PARTIE 1
Analyse du phénomène : le terrorisme dans le monde des entreprises

1 Définitions du terrorisme

Tant le Code judiciaire que le code pénal prévoient des définitions des infractions terroristes.

Le Code judiciaire définit le terrorisme comme « le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces »[1], définition que l'on retrouve également dans la loi organique des services de renseignement et de sécurité.

En outre, depuis le 19 décembre 2003, le Code pénal belge prévoit des articles relatifs aux infractions et aux groupements terroristes. Selon cette loi, une infraction terroriste est « une infraction […] qui, de par sa nature ou son contexte, peut porter gravement atteinte à un pays ou à une organisation internationale et est commise intentionnellement dans le but d'intimider gravement une population ou de contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte, ou de gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou d'une organisation internationale. »[2]

Le terrorisme a la particularité d'utiliser une autre infraction comme moyen d'atteindre un objectif terroriste. Une infraction terroriste est par exemple l'utilisation d'un incendie criminel associé à un message idéologique, politique ou religieux.

Une infraction terroriste peut donc entraîner des dégâts économiques importants. La destruction ou la dégradation massives d'infrastructures causent des pertes dans divers domaines.

[1] Art. 8.1°, Loi organique des services de renseignement et de sécurité du 30 novembre 1998, ainsi que l'art. 144ter § 1, 2° du Code judiciaire, *M.B.* 18 décembre 1998

[2] Art. 137 §1, §2, Code pénal, inséré par l'art. 3, Loi 19 décembre 2003, *M.B.* 29 décembre 2003.

Les actes susceptibles d'être perpétrés par des terroristes sont l'incendie volontaire, l'explosion d'engins, le détournement de moyens de transport, la libération de substances dangereuses, la perturbation de l'approvisionnement en eau et en électricité, les menaces, l'enlèvement ou la prise d'otage de membres du personnel,…[1] De plus, les terroristes peuvent être à même de manipuler la production.
La conséquence est que de nombreuses personnes sont en danger (de mort). L'impact psychologique qui en découle n'est pas à sous-estimer. Finalement, l'entreprise n'est pas seulement victime de dégâts structurels et économiques, le terrorisme intimide et victimise aussi le secteur, l'environnement et le personnel de l'entreprise, les fournisseurs, les clients,… Bref, le terrorisme crée l'angoisse et la stupeur dans la société au sens large.

Le secteur public fait généralement la distinction entre le terrorisme national et international. La première forme concerne principalement la sphère d'intérêt, les habitants et le territoire d'une seule nation, visés par exemple par le terrorisme d'extrême gauche, le terrorisme d'extrême droite, l'éco-terrorisme, ainsi que le terrorisme nationaliste ou séparatiste. Il est évident que ces phénomènes/groupements ont souvent des liens avec l'étranger, surtout ces dernières années, les voyages étant devenus de plus en plus faciles et la communication par internet de plus en plus rapide.
Par contre, le terrorisme international, comme par exemple le terrorisme islamiste radical[2], vise plutôt la sphère d'intérêt, les habitants et le territoire de plusieurs nations.
Du reste, une attention est accordée aux formes particulières telles que le terrorisme NBCR[1] et le cyberterrorisme.

[1] Art. 137 §1, Code pénal, inséré par l'art. 3, Loi 19 décembre 2003, *M.B.* 29 décembre 2003.
[2] DGJ/DJP/ Service terrorisme et sectes, *Présentation PowerPoint relative à la Direction générale de la Police judiciaire ; Direction de la lutte contre la criminalité contre les personnes ; Service terrorisme et sectes*, Bruxelles, DGJ/DJP/ Service terrorisme et sectes.
[1] NBCR = Nuclear Biological Chemical and Radiological

2 Les différentes formes d'apparition du terrorisme

2.1 Généralités

Personne ne prétendra que le phénomène du terrorisme a évolué dans le bon sens. Le 11 mars 2004, des attentats horribles ont été perpétrés par des radicalistes islamistes en Europe (Madrid) et les attentats récents à Londres confirment cette tendance. D'autres en Afrique et en Asie montrent que le radicalisme islamiste y est tout aussi actif et violent.

De plus, l'Europe est confrontée aux attentats terroristes d'origine nationaliste européenne, comme en Espagne (ETA) et en France (mouvement séparatiste corse).

Des actions policières menées dans toute l'Europe ont en outre démontré que tant les groupements d'extrême droite que d'extrême gauche n'hésitent pas à utiliser la violence brutale pour atteindre leurs objectifs politiques, religieux ou idéologiques[1].

[1] DGJ/DJP/ Service terrorisme et sectes, *Rapportage sur l'exécution du plan de sécurité national*, Bruxelles, DGJ/DJP/ Service terrorisme et sectes, 2004, 1

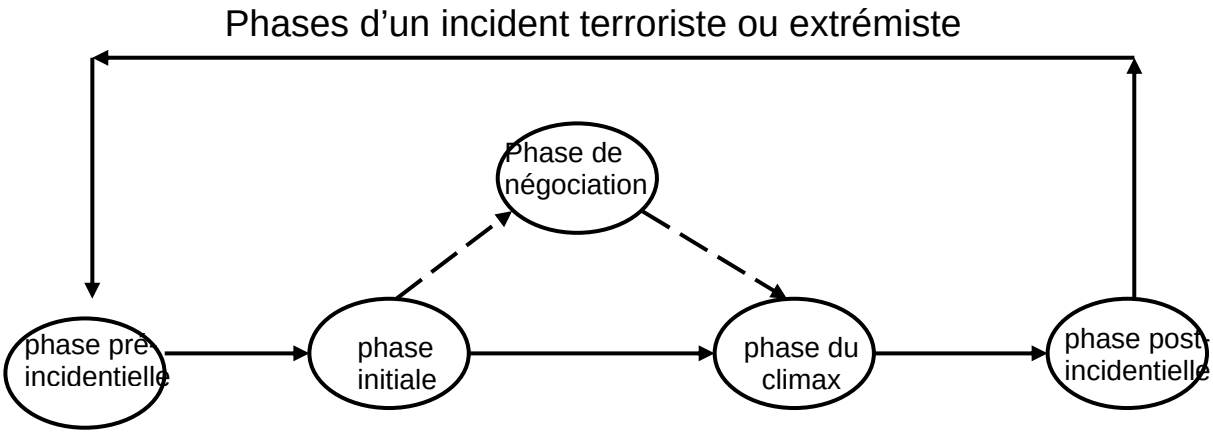
2.2 Le terrorisme face aux entreprises

De par la spécificité de leur secteur, leur « nationalité », la nature de leur processus de production, certaines entreprises courent plus de risques d'être victimes de menaces ou d'actions terroristes et extrémistes que d'autres.

- Au milieu des années 80, les CCC[1] ont perpétré plusieurs attentats à la bombe, dont un fut dirigé contre le bâtiment de la Kredietbank à Leuven.
- L'Animal Liberation Front (ALF) a organisé des actions écoterroristes, notamment contre des restaurants « fast-food » comme le Quick et le Mc Donalds, ainsi que contre des industries de transformation de la viande.
- Plus récemment – en 2003 et 2004 – des lettres contenant des produits toxiques ont été envoyées à plusieurs instances par la poste.
- Ces dernières années, le SHAC[2] a proféré des menaces à l'encontre de l'industrie pharmaceutique, chimique, cosmétique et des industries connexes.
- En ce qui concerne le cyberterrorisme, toute firme pourra tôt ou tard se trouver incommodée par des virus qui affectent ses systèmes informatiques. Les dégâts peuvent être énormes lorsque les terroristes parviennent à immobiliser des processus de production informatisés ou perturber des appareillages de contrôle (p.ex. l'aviation, les paiements, l'approvisionnement en eau, en électricité, etc.).
- En outre, il faudra également protéger l'industrie alimentaire qui pourrait être sensible aux manipulations de produits biologiques (ou chimiques).
- Enfin, on ne peut pas perdre de vue que les médias sont eux aussi un moyen utile pour atteindre un but terroriste. En effet, l'usage des médias fait partie de la lutte terroriste.

[1] CCC = Cellules Communistes Combattantes
[2] SHAC = Stop Huntingdon Animal Cruelty Life Sciences (HLS)

3 Les phases de l'organisation d'un crime terroriste[1]



Avant de passer à l'acte terroriste, les groupements terroristes suivent généralement un cycle d'activités opérationnelles.

Un attentat terroriste compte plusieurs phases. Celles-ci nous aident à comprendre les méthodes utilisées par les terroristes dans leurs opérations.

Cela nous permet de développer des mesures préventives.

- Premièrement, il y a la *phase pré-incidentielle ou préparatoire*. Dans cette phase, le terroriste planifie ses actions. Il y tient compte des objectifs à court et à long terme. L'organisation terroriste tient également compte de ses propres possibilités et limites en fonction de l'information qu'elle a pu recueillir, des observations effectuées et des expériences acquises par le passé. Cette phase du planning est l'une des plus cruciales de la préparation de l'attentat terroriste. Elle commence par le recrutement des forces exécutives et la répartition des tâches. Les actions que peuvent déployer les terroristes dans cette phase sont en premier lieu la collecte de données par l'observation, la recherche des « meilleures » cibles, le recours à des informateurs,… Les préparations logistiques incluent la mise à disposition des moyens de transport, la recherche des documents utiles, la collecte d'armes et d'explosifs,…

[1] J. FRASER, *Terrorisme: an overview. Clandestine Tactics and Technology. A Technical and Strategic Intelligence Data Service. Is your agency prepared to cope with political violence and terrorism*, Gethersburg, International Association of Chiefs of Police (IACP), s.d., 7-8.

Dans cette phase, les entreprises risquent d'être confrontées plusieurs fois à des actions violentes sans toutefois que celles-ci puissent être imputées aux terroristes. Il s'agit en l'occurrence surtout d'opérations d'autofinancement pouvant prendre différentes formes, à savoir : des hold-up (tant contre des institutions financières que des entreprises ou des personnes), des extorsions (appelées « impôt révolutionnaire »),… Le vol d'armes et de véhicules font aussi partie des modi operandi. Cette phase sera élaborée minutieusement afin d'assurer le succès de l'attentat.

- Deuxièmement, il y a la *phase initiale ou d'exécution*. Pendant cette phase, les terroristes lancent leur opération, et ce sans plus pouvoir faire marche arrière. Le processus sera déclenché. Il s'agit de la phase de l'attentat terroriste proprement dit, souvent revendiquée par le groupement en question et accompagnée d'exigences ou de griefs. Parfois les terroristes perdent le contrôle de leurs activités pendant cette phase. De nombreux événements imprévus peuvent se produire dans une situation pareille et entraîner davantage de violence.
- La troisième *phase* est celle *de la négociation*. Elle a rarement lieu et n'est certainement pas toujours prévue par les terroristes. Ceux-ci peuvent être gênés par la police pendant leur opération. Ils essayeront alors de trouver une issue, ce qui peut les amener à négocier avec les autorités. Cela peut donner beaucoup de publicité à leur action.
- L'avant-dernière *phase* est celle *du climax*. Ici, l'incident se termine. La fin peut se produire immédiatement après l'action ou se faire attendre plus longtemps en cas de prise d'otage.
- Enfin, il y a la *phase post-incidentielle* pendant laquelle l'action menée sera évaluée et analysée de manière critique. Les groupements terroristes tireront les conclusions de leurs actes. Pour eux, il s'agit donc d'une phase très importante pour la préparation d'attentats ultérieurs.

PARTIE 2

Le management de prévention

PARTIE 2
Le management de prévention

La première partie a clairement démontré que les entreprises peuvent effectivement être victimes d'actions terroristes ou extrémistes et qu'il serait donc raisonnable qu'elles élaborent des mesures préventives. Outre l'aspect purement criminologique, il existe d'autres raisons importantes pour le faire :

- le travailleur a un sentiment de sécurité subjectif. Après l'attentat du 11 septembre 2001 à New York, on s'est rendu compte plus que jamais que « le côté humain » des affaires doit lui aussi être protégé. Qui dit sécurité, dit personnel et ses besoins mentaux.
- le fait de « s'occuper de la sécurité » donne également un sentiment de « sécurité » au client et à l'actionnaire. Ainsi, les compagnies aériennes ont collaboré avec les instances publiques afin de garantir plus de sécurité après le 11 septembre. Par conséquent, la « peur de l'avion » du citoyen n'a pas duré très longtemps, la croissance économique a redémarré et de nouveaux emplois ont été créés[1].
- il est très important de faire une bonne estimation des risques en cas de menace ou d'attentat terroriste potentiel, et ce pour deux raisons : premièrement parce que cela permet de limiter les conséquences négatives sur l'activité commerciale de l'entreprise, comme p. ex. des pertes importantes par rapport à leurs concurrents, perte de la bonne réputation, faillite, paiement d'une prime d'assurance plus élevée,…[2]. En outre, une évaluation exacte de la menace évite que l'entreprise réagisse exagérément en matière de mesures de sécurité et que les conditions de travail soient trop perturbées.

Chaque entreprise a donc tout intérêt à prendre suffisamment de mesures de prévention pour se protéger contre d'éventuelles actions terroristes ou extrémistes.

[1] J.N., KAYYEM & P. E., CHANG, *Perspectives on Preparedness: Beyond Business Continuity: The Role of the Private Sector in Preparedness Planning,* s.l., U.S. Department of Justice, 2000, nr 6, 6-7.
[2] NATIONAL COUNTER TERRORISM SECURITY OFFICE, *Expecting the unexpected. Business continuity in an uncertain world.,* London, London First, 2003, 3.

1 Prévention

Selon le Dr. Muller, la prévention concerne des mesures pouvant être prises afin de réduire, voire empêcher les menaces potentielles d'actions de terrorisme et d'extrémisme[1]. Il s'agit d'un processus bien réfléchi visant à scruter les risques. Sur la base de la compréhension de ces derniers, on décide quelles mesures seront prises et mises en œuvre pour réduire le risque à un certain niveau, et ce à un prix acceptable. Le but de cette approche et donc d'identifier et d'évaluer les risques et de les limiter[2]. Le contexte général du terrorisme et de l'actualité internationale, comme décrit au chapitre précédent, sera un des piliers d'une analyse des risques approfondie.

L'objectif stratégique du Plan national de sécurité de la Police fédérale est de contribuer à la prévention des attentats terroristes. Il faut essayer de découvrir les activités terroristes qui se préparent sur le territoire belge et de les contrer de manière adéquate. Les groupements terroristes actifs sur le territoire belges devraient être déstabilisés[3].

L'estimation ou l'évaluation de la menace potentielle émanant de groupements terroristes en Belgique et dirigée contre les intérêts belges (tant officiels que privés) à l'étranger, a été confiée, par le gouvernement belge, au Groupe Interforces Anti-terroriste (GIA), créé le 17 septembre 1984 (A.R. du 17 octobre 1991). Cette évaluation est rédigée sur la base des données fournies par les services représentés au sein du GIA, à savoir : la Police intégrée, la Sûreté de l'Etat et le Service Général du Renseignement et de la Sécurité (SGRS) de l'armée, ainsi que par des sources ouvertes et fermées en Belgique et à l'étranger. Il s'agit tant d'évaluations (stratégiques) globales que d'évaluations (opérationnelles) ponctuelles. Les évaluations ponctuelles ou opérationnelles sont généralement effectuées à la demande de la Direction générale Centre de crise (DGCC[4]) du Service Public Fédéral Intérieur (A.R. du 18 avril 1988

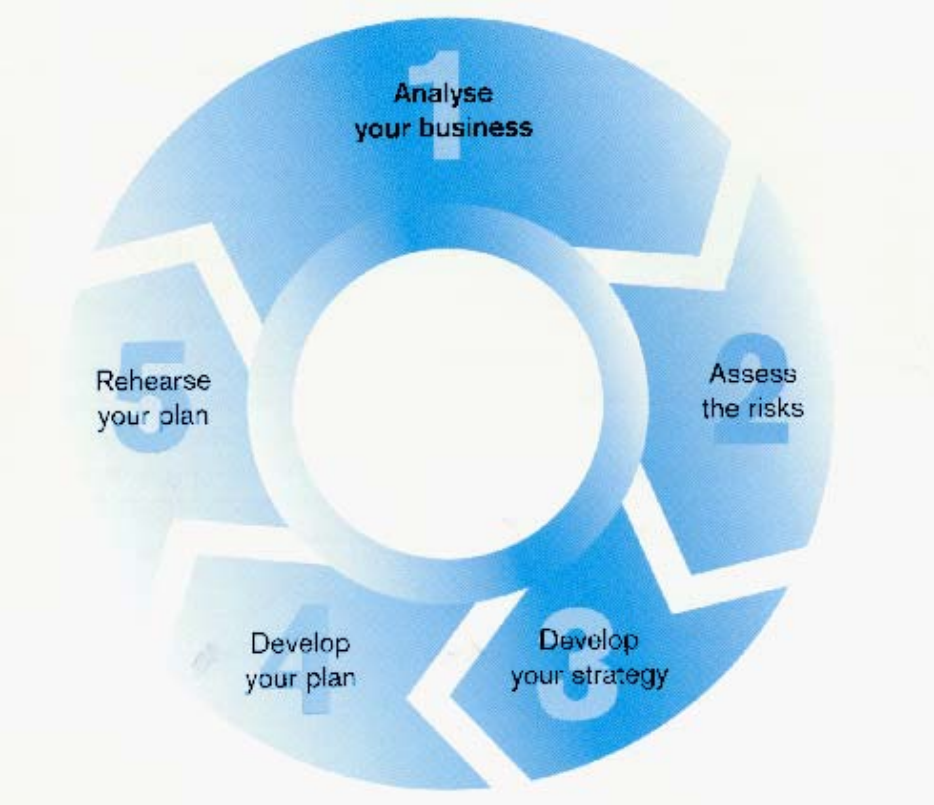
[1] E.R. MULLER, Terrorisme en terreurbestrijding na 11 september 2001, in B. PATTYN en J. WOUTERS (ed.), *Schokgolven. Terrorisme en fundamentalisme*, Leuven, Davidsfonds, 2002, 26-31.
[2] COMMISSION DES COMMUNAUTES EUROPEENNES, *Lutte contre le terrorisme : protection des infrastructures critiques*, Bruxelles, Commission des Communautés européennes, 2004, 6.
[3] DGJ/DJP/ Service terrorisme et sectes, *Rapportage sur l'exécution du plan national de sécurité,* Bruxelles, DGJ/DJP/ Service terrorisme et sectes, 2004, 1
[4] DGCC = le service public compétent qui décide au nom du Ministre de l'Intérieur quelles mesures la police administrative doit prendre pour protéger les personnes et les institutions dans le pays et qui donne les instructions nécessaires à cet effet aux services de police (pour les institutions, voir : www.crisis.ibz.be).

portant création du Centre gouvernemental de Coordination et de Crise, M.B. du 4 mai 1988, modifié par l'A.R. du 11 mai 1990, M.B. du 1er juin 1990).

Il est clair que tout ceci nécessite une bonne collaboration entre le secteur privé et le secteur public, qui peut contribuer à la prévention du terrorisme et à la lutte contre celui-ci. C'est pour cette raison que des canaux d'information permettant d'échanger des informations pertinentes sont développés (cf. Préface et introduction).

2 Analyse du risque par l'entreprise

Pour parvenir à une analyse adéquate du risque, il faut que l'entreprise soit à même de faire une bonne estimation de l'ampleur de la menace, notamment en se situant correctement dans le contexte (géo)politique général et qu'elle tente également de se faire une idée précise des dommages qu'une telle menace peut engendrer.



2.1 Analyse de la menace

Pour connaître l'ampleur du risque que court une entreprise déterminée de devenir la victime d'un acte de terrorisme, il est nécessaire de procéder à une analyse de la menace. Grâce à une estimation des points forts et des points faibles de l'entreprise, on peut en effet évaluer ses risques d'être victime d'un acte terroriste éventuel.

Il est recommandé d'impliquer le personnel dans cette démarche, afin qu'il se sente concerné. Dans certains cas, il est utile, dès ce stade, de consulter un expert en matière de prévention, de protection et de sécurité. Celui-ci est en effet à même d'analyser l'entreprise de manière objective, ce qui ne peut qu'apporter une plus-value au Business Continuity Plan (voir infra).

Il faut par ailleurs vérifier si l'entreprise dispose déjà de plans de crise tenant compte de la menace d'un éventuel acte terroriste. Si c'est le cas, ces plans doivent faire l'objet d'une analyse critique et les aspects qui sont réutilisables peuvent être intégrés dans le nouveau Business Plan.

Dans cette phase, il est donc important avant tout que l'entreprise apprenne à se « comprendre » elle-même[1] :

- il est utile de vérifier si l'entreprise est reprise sur la liste de l'Infrastructure Critique Nationale, disponible au niveau fédéral auprès de la Commission des Problèmes Nationaux de Défense (CPND), qui fait partie de la DGCC. Cela vaut également pour les entreprises établies à proximité de ces secteurs critiques, vitaux ou sensibles. En étant « voisines » d'une telle entreprise, elles courent plus de risques d'être également victimes d'acte terroristes ou extrémistes ;
- il faut prêter attention à la nature et à la durée des processus de production (par ex. les matières premières qui sont dans le collimateur de certains groupes extrémistes, comme des organismes manipulés génétiquement, des produits testés sur des animaux, la fourrure, le foie gras, la transformation de la viande, …). Il y a lieu aussi de vérifier si, par le passé, ces processus de production n'ont pas déjà fait l'objet de menaces ou d'actions, fût-ce à l'étranger ;

[1] NATIONAL COUNTER TERRORISM SECURITY OFFICE, *Expecting the unexpected. Business continuity in an uncertain world*, London, London First, 2003, 6-8.

- il est en outre utile de se pencher sur les interactions internes entre le personnel, les partenaires commerciaux, les fournisseurs et les clients (certains clients ou fournisseurs ont-ils déjà été la cible de groupements extrémistes ?) ;
- une analyse critique de la structure et de l'infrastructure des bâtiments s'avère également nécessaires (par ex. situation à proximité d'un port, entrées, postes de contrôle, …) ;
- enfin, une entreprise doit pouvoir se situer dans le contexte (géo)politique. Elle devrait tenir compte de son rayonnement auprès de certains groupements extrémistes (banques en tant que symbole du capitalisme, industrie pétrolière, …). En effet, certaines entreprises sont davantage dans le collimateur des groupements extrémistes en raison de la nature de leur processus de production ou de leurs produits (par ex. produits en provenance du Moyen-Orient, …).

2.2 Analyse des risques

Lors de l'évaluation des risques, il faut essayer d'identifier les menaces les plus susceptibles de viser l'entreprise, le risque de survenance d'une telle menace et les impacts possibles sur l'entreprise[1]. Ceci permet à l'entreprise de savoir quand elle doit prendre des mesures de sécurité supplémentaires[2]. Idéalement, les entreprises devraient toujours tenir compte du « *worst case scenario* »[3].

Dans la pratique, il est préférable de créer un tableau comparatif entre les variables « *gravité des dommages éventuels* » et « *probabilité ou menace* ». Plus ces variables sont élevées, plus le risque est important. L'application d'une gestion des risques permet de se concentrer sur les domaines où le risque est le plus élevé. Ceci implique une vigilance accrue, ce qui devrait entraîner une multiplication des mesures préventives spécifiques[4].

[1] NATIONAL COUNTER TERRORISM SECURITY OFFICE, *Expecting the unexpected. Business continuity in an uncertain world*, London, London First, 2003, 10.
[2] D.A. MOORE, *présentation Powerpoint: The Challenge of Making Risk Decisions for Port Security*, Anvers/San Francisco, AcuTech Consulting Group, 2004.
[3] NATIONAL COUNTER TERRORISME SECURITY OFFICE, o.c., 2003, 10.
[4] Ibid., 10.

L'analyse permet de savoir si une entreprise fait ou non partie de l'infrastructure industrielle critique. Font partie de cette infrastructure critique des réseaux ou des chaînes d'approvisionnement pour la livraison continue d'un produit important ou d'un service essentiel. La destruction ou la détérioration d'infrastructures matérielles et des technologies de l'information, de réseaux, de services et d'actifs peut avoir de lourdes conséquences[1], et ce non seulement pour l'entreprise concernée mais aussi pour les entreprises voisines ou qui partagent la même infrastructure et/ou qui sont dépendantes de par le processus de production (effet domino : en cas de panne d'électricité découlant d'une attaque, cela peut entraîner aussi l'arrêt de la turbine de l'alimentation en eau). Ainsi une cyberattaque réussie ne produit que peu voire pas de victimes, mais elle peut entraîner l'arrêt de services d'infrastructure vitaux. Une attaque réussie sur le réseau téléphonique peut empêcher les clients de téléphoner. Une attaque sur le système de commande d'une installation chimique ou gazière pourrait déboucher sur des pertes importantes et des dégâts matériels considérables[2].

De manière globale, on peut distinguer cinq catégories de conséquences[3] :

- des conséquences pour la population (victimes mortellement atteintes, blessés, maladies, victimisation secondaire, problèmes d'évacuation, facteurs psychologiques tels une traumatisation, une dramatisation des événements, …) ;
- des conséquences pour l'environnement ;
- des conséquences économiques (ampleur des pertes et/ou baisse de la qualité des produits ou services, conséquences indirectes pour le PIB) ;
- conséquences politiques ;
- conséquences combinant plusieurs aspects des catégories susmentionnées.

Dans notre « stratégie », il va de soi que nous devrons tenir compte du fait que toutes les infrastructures ne peuvent pas être protégées contre toutes les menaces. Ainsi, certains réseaux de distribution, celui de l'électricité par exemple, sont trop grands pour pouvoir être clôturés ou surveillés[4].

[1] COMMISSION DES COMMUNAUTES EUROPEENNES, *Lutte contre le terrorisme: protection des infrastructures critiques*, Bruxelles, Commission des Communautés Européennes, 2004, 4.
[2] Ibid., 3.
[3] COMMISSION DES COMMUNAUTES EUROPEENNES, o.c., 5-6.
[4] Ibid., 6.

3 Le développement d'une stratégie

Il ressort de ce qui précède qu'il faut tenir compte de la menace, du risque voire même de la mesure dans laquelle l'infrastructure peut être considérée comme critique, et du niveau de protection existant. Ceci doit nous amener à suivre une certaine stratégie qui nous permette d'en appréhender les conséquences et de garantir la continuité de l'activité, et ce conformément aux possibilités et à la vision de l'entreprise[1]. Sur la base de l'analyse des risques, un choix peut être fait parmi les stratégies suivantes[2] :

- l'entreprise peut accepter les risques et décider de ne rien changer ;
- l'entreprise peut décider de ne pas s'imposer des mesures internes mais de conclure un partenariat avec d'autres entreprises/organismes susceptibles de leur donner des avis basés sur l'expérience acquise après l'un ou l'autre incident ;
- l'entreprise peut décider de prendre des mesures (supplémentaires) afin de réduire et d'éviter les risques ;
- l'entreprise a la possibilité de prendre elle-même quelques mesures, tout en contactant des partenaires (y compris les autorités publiques) afin de s'assurer de la disponibilité de l'expertise en cas d'incident ;
- l'entreprise peut tenter de réduire les risques au point qu'elle sera à même de les assumer tous, sans devoir faire appel à l'aide extérieure.

[1] COMMISSION DES COMMUNAUTES EUROPEENNES, *o.c.*, 2004, 6.
[2] NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.*, 14-16.

4 Le développement du plan

4.1 Le Business Continuityplan: le contexte

Sur base de l'approche stratégique choisie, il faudra développer un plan de gestion qui permette de réfléchir aux mesures pouvant être prises avant (préventives), pendant (actions entreprises durant la période de l'incidence) et après (gestion de reconstruction) l'action terroriste.

On oublie parfois ce dernier aspect. Un Business Continuity Plan peut aider l'entreprise à préparer les cas d'urgence et à surmonter les « situations imprévues ». Le planning doit permettre le retour rapide au « cours habituel des choses ». Le Business Continuity Management peut donc être défini comme « un processus de management holistique » qui tente d'identifier l'impact potentiel d'une menace (terroriste) proférée contre une organisation. Il tente de proposer des réponses efficaces aux éventuelles menaces et attaques (terroristes) dirigées contre une entreprise[1].

Le Business Continuity Management peut s'avérer utile tant pour les petites que pour les grandes entreprises. Grâce à l'approche planifiée, on peut tenir compte de manière simple et efficace des besoins de l'organisation. Un plan phasé détaillé permet de ne pas oublier des éléments cruciaux. Lorsqu'un incident se produit, son impact négatif sur le bien-être (économique) de l'entreprise sera moins important[2].

[1] NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.,* 2.
[2] D. BLUNKETT, *Expecting the unexpected. Business continuity in an uncertain world.*, London, London First (National Counter Terrorism Security Office), 2003, 1.

4.2 Business Continuity Plan: Concrétisation[1]

Les Business Continuity Plan diffèrent d'une entreprise à l'autre. Toutefois, les meilleurs plans sont souvent fondés sur les mêmes composantes de base. Un plan doit avoir une bonne structure stratégique[2], tactique[3] et opérationnelle[4].

- Il est important que toutes les divisions de l'entreprise soient consultées lors de l'élaboration du plan.
- Il est souhaitable que le plan soit rédigé dans un langage accessible à tout le monde. Sa structure doit être simple. Il ne sera jamais possible de prévoir tous les détails. L'important est de savoir comment réagir rapidement et de manière adéquate en cas d'urgence.
- Il faut indiquer clairement qui devra prendre quelles mesures dans quelles situations. Faites une checklist des mesures à prendre et des instructions à suivre pendant les premières heures cruciales suivant l'incident (procédures standards). Par exemple : qui appellera la police ? Utilisez un schéma subdivisé en plusieurs points facilement contrôlables.
- Lors de l'élaboration du plan, il est nécessaire de le tester préalablement et de le corriger le cas échéant. En outre, il doit être évalué régulièrement et adapté constamment aux risques du moment.
- Idéalement, on devra aussi tenir compte du « *worst case scenario* ». Ainsi, le plan pourrait prévoir un endroit où l'activité peut être poursuivie.

[1] NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.*, 18-21.
[2] stratégique = la capacité d'atteindre un objectif ou de réaliser un plan d'action par les moyens disponibles
[3] tactique = la méthode la plus appropriée pour atteindre l'objectif ou pour réaliser le plan d'action
[4] opérationnel = un plan d'action prêt à être utilisé pour atteindre l'objectif fixé

5 Evaluation du plan

L'exercice ne se termine pas par la réalisation d'un plan de prévention.
Un plan est un document qui nécessite des adaptations continues. C'est pourquoi il est conseillé d'exécuter activement les plans de sécurité, d'organiser régulièrement des inspections et des exercices et de les évaluer de manière approfondie[1]. Il est nécessaire de tester régulièrement le plan pour qu'il soit à jour. Cela permet également de repérer ses points faibles et d'y remédier.

6 Conclusion

L'approche planifiée de la sécurité dans le cadre du terrorisme incite les secteurs privé et public à unir leurs forces. En effet, grâce à une collaboration proactive de ces deux secteurs, les différents acteurs du processus économiques pourront être protégés[2].
De toute façon, il est recommandé aux entreprises de rédiger un Business Continuity Plan de sorte que tout un chacun connaisse mieux ses points forts et ses faiblesses et que le fonctionnement de l'entreprise puisse être amélioré et la continuité garantie.

[1] COMMISSION DES COMMUNAUTES EUROPEENNES, *o.c.*, 10.
[2] D. BLUNKETT, *o.c.*, 1.

PARTIE 3

Mesures préventives

PARTIE 3
Mesures préventives

Cette troisième partie concrétise les deux premières. Nous y donnerons des conseils, proposerons des mesures et formulerons des recommandations permettant à l'entreprise de mieux se protéger contre les menaces et/ou actions terroristes. Comme déjà indiqué, une réponse préventive réussie à une action terroriste concrète ou potentielle dépend de la qualité du Business Continuity Plan et des mesures de sécurité adoptées. Il est évident que quasi toutes les mesures pouvant être prises dans le cadre du terrorisme sont également d'application à la plupart des autres formes de criminalité.

Les mesures de sécurité prévues peuvent prendre différentes formes.

Puisque les moyens disponibles sont généralement limités, il faudra faire une bonne analyse des coûts et bénéfices pour obtenir un rapport équilibré entre les risques et les mesures de protection. En effet, s'agissant des mesures à prendre, on songe souvent immédiatement à des solutions techniques et des investissements onéreux. La conséquence d'une telle approche est qu'on oublie parfois les mesures d'organisation simples, ce qui réduira l'efficacité de l'équipement technique, souvent très coûteux. A cela s'ajoute, que les frais sont relativement élevés par rapport à la réduction du risque.

Idéalement, le plan de sécurité devra mettre l'accent plutôt sur les aspects de qualité et d'organisation comme la participation des travailleurs, la responsabilité, la communication et la motivation ; ceux-ci sont souvent plus efficaces que les dispositifs techniques et électriques onéreux.

Par ailleurs, la collaboration entre le secteur public et le secteur privé facilitera le processus de prévention du terrorisme[1].

Si on veut prévenir au maximum les actions terroristes ou extrémistes, il vaut mieux combiner plusieurs mesures. Celles-ci peuvent varier considérablement d'une entreprise à l'autre. Toutefois, les recommandations ci-après sont de nature tellement générale qu'elles peuvent s'appliquer à toute entreprise[2].

[1] J. WILLEMS, *Terrorisme en scheepvaart,* Antwerpen, Police fédérale : DGA/DAC/SPN/SPN-Antwerpen, 2004, 27.

[2] SERVICE PUBLIC FEDERAL INTERIEUR, *Veilig zelfstandig ondernemen,* Bruxelles, DIE KEURE, Direction Générale Politique de Sécurité et de Prévention, Sécrétariat permanent pour la politique de prévention, 2004, 44.

Les mesures que l'on peut appliquer pour garantir une meilleure prévention des actions terroristes ou extrémistes peuvent être subdivisées en 5 catégories : *mesures d'organisation, mesures architectoniques, mesures électroniques, mesures TIC, mesures personnelles (Ressources humaines)*. C'est dans cet ordre qu'elles sont le plus efficaces. Le coût des moyens électroniques est souvent le plus élevé alors que celui des mesures d'organisation est quasiment nul[1]. Il est à noter que certaines mesures préventives pourraient être rangées dans différentes catégories.

1 Mesures organisationnelles

Les mesures organisationnelles peuvent être considérées comme prioritaires. Donc, si un problème spécifique se pose ou un incident se produit, nous recommandons de ne pas chercher une solution immédiate sans en examiner les causes profondes. En effet, celles-ci ne résident pas toujours dans le disfonctionnement de l'appareillage de sécurité, mais dans le manque d'attention prêtée à la prévention au sein de l'entreprise[2]. En outre, ces mesures coûtent relativement peu (engagement de l'entreprise et de son personnel).

Quelques exemples en sont notamment la rédaction d'un plan qui permette d'évacuer les lieux le plus vite possible, ou la réflexion sur ce qui doit se faire en attendant de l'aide professionnelle.

1.1 Actions de sensibilisation et entraînement des travailleurs

La politique de sécurité doit avoir sa place réservée dans la vie quotidienne de l'entreprise. La sécurité doit être un thème récurrent dans les discussions du personnel et avec le personnel. Il peut être utile d'organiser des entraînements et des actions de sensibilisation visant certains risques de sécurité. Ainsi, le personnel apprendra à distinguer les critères de reconnaissance. Chaque travailleur deviendra plus conscient des risques et acquerra un réflexe de sécurité. Il est important de se mettre d'accord sur

[1] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 15, 30.
[2] Ibid., 40.

les méthodes d'annonce et de centralisation des incidents de sécurité. Les instructions destinées au personnel doivent être brèves et claires. Les numéros de téléphone importants seront affichés de manière visible[1]. De telles actions peuvent être organisées de différentes façons ; le personnel peut être sensibilisé à la problématique par le biais d'affiches, de dépliants et d'e-mails sur l'intranet et l'internet. L'organisation de ces actions peut être confiée au service de communication interne à l'entreprise ou à des firmes externes qui organiseraient des sessions de sensibilisation.

1.2 Contrôles de qualité des produits

En organisant régulièrement des contrôles de qualité, l'entreprise peut repérer, à la source, des manipulations de nature terroriste ou extrémiste. Si les terroristes savent que l'entreprise fait régulièrement des contrôles de la qualité des produits dans les différentes phases de la production, certains d'entre eux seront sans doute moins tentés de manipuler ce processus. En outre, on peut éviter ainsi que le produit manipulé fasse des victimes ou puisse faire la une. Il est évident toutefois, que le terroriste « avisé » ne se laissera pas intimider par cette mesure.

1.3 Un aménagement clair de l'entreprise et une administration ordonnée

Si l'entreprise respire l'ordre et la maîtrise (tant au niveau interne qu'externe), il sera plus facile de remarquer la présence de visiteurs non désirés.
Il est recommandé d'avoir une très bonne vue d'ensemble de toute la surface d'exploitation. Un bon éclairage des endroits obscurs est indiqué.
Le rayonnement externe de l'entreprise est tout aussi important. Ainsi, l'environnement – p. ex. le parking – sera bien ordonné et propre.

[1] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 51, 57.

1.4 Les entrées et les sorties

Le nombre d'entrées et de sorties de l'entreprise sera limité au maximum.

1.5 Les voies d'accès[1] [2]

Il faut éviter que des clients, visiteurs et fournisseurs puissent entrer dans l'entreprise sans être vus. Les personnes étrangères à l'entreprise doivent toujours avoir le sentiment qu'on peut les voir.

L'idéal serait d'avoir une seule entrée où le visiteur, le client ou le fournisseur peut se présenter à l'accueil. Il obtiendra l'autorisation d'accéder au terrain de l'entreprise (de préférence muni d'un badge) après le contrôle de l'authenticité du rendez-vous ou de la livraison. Il est facile de prévoir des badges informatisés avec photo pour le personnel de l'entreprise. L'informatisation du badge permet de limiter l'accès à certains endroits de l'entreprise pour certains travailleurs.

Si l'entreprise ne dispose pas d'une réception, elle peut installer une caméra digitale qui filmera les visiteurs à l'entrée ; la caméra transmettra les images à un moniteur interne. Sur la base de celles-ci, un responsable décidera si le visiteur, le client ou le fournisseur peut entrer ou non.

Il est souhaitable que quelqu'un de l'entreprise ou de la sécurité interne accompagne les visiteurs, et qu'on limite l'accès aux parties du bâtiment accessibles à tous les travailleurs. Il est préférable de fermer et/ou de contrôler ces lieux. Par ailleurs, il est souhaitable que les visiteurs portent un badge d'accès, à remettre à la sortie du bâtiment. Les visiteurs non désirés se feront remarquer s'ils ne sont pas accompagnés d'une personne de l'entreprise et/ou s'ils ne portent pas de badge.

---

[1] HOME OFFICE, *Bombs: Protecting People and Property: a handbook for managers*, s.l., Home Office, s.d., 11.

[2] Attention ! Les contrôles d'entrée et de sortie, ainsi que les contrôles d'identité, doivent être conformes à la législation en matière de sécurité privée : voir http://www.vigilis.be. En outre, il faut tenir compte de la réglementation en matière de protection de la vie privée, notamment lors de la vidéo-surveillance : voir http://www.privacy.fgov.be

Dans certains cas, il est recommandé de contrôler – dans les limites des possibilités légales – les bagages ou marchandises à livrer avant de donner accès à l'entreprise. Le/la réceptionniste doit être prudent(e) lorsque des visiteurs non annoncés se présentent à l'accueil.

1.6 Contrôle visible au sein de l'entreprise[1]

Certaines mesures pouvant influencer le comportement ont un effet dissuasif sur les terroristes. Une disposition stratégique du personnel permet un contrôle de tous les coins et recoins de l'entreprise. Il est recommandé d'installer des caméras de manière tant visible qu'invisible. Les terroristes potentiels entreprendront plutôt des actions là où ils ne peuvent être vus ni filmés.
Les « faux » systèmes bon marché peuvent être une solution alternative mais à long terme, ils perdent de leur efficacité.
Le contrôle par des personnes (en uniforme, éventuellement travaillant pour des firmes de sécurité externes) dissuade les clients et fournisseurs « peu fiables ». Il vaut mieux que les travailleurs de l'entreprise se distinguent clairement par un uniforme adapté ou un badge personnalisé. Il est préférable que les clients, fournisseurs et visiteurs voient que l'entreprise est bien protégée. Ainsi, ils se rendront compte que la possibilité d'être pris en flagrant délit est réelle.

1.7 Le contact avec la clientèle, les visiteurs et les fournisseurs

Il est déconseillé de donner aux clients des informations sensibles sur les transactions financières, les mesures de sécurité ou certaines procédures de sécurité appliquées dans l'entreprise.

[1] SERVICE PUBLIC FEDERAL INTERIEUR, o.c., 44-48

1.8 Le plan des clés et leur gestion[1]

L'entreprise doit établir un *plan des clés*, qui indique, entre autres :

- quelles sont les fenêtres, portes et armoires pourvues d'une serrure ;
- à quels moments il faut fermer ;
- qui est/sont la/les personne(s) habilitée(s) à se rendre dans certains locaux ;
- qui est le/la responsable de la fermeture des locaux spécialement protégés ;
- qui garde les clés à quels endroits ;
- quel est le type de serrure à utiliser (clé ou code) ;
- quelle est la procédure exacte à suivre pour la fermeture.

La *gestion des clés* par contre, comprend un ensemble de procédures permettant de garder les clés de manière efficace et sûre. Il faut éviter d'abandonner des clés ou de les distribuer à un trop grand nombre de personnes.

Voici quelques mesures recommandées :

- il faut limiter au maximum le nombre de personnes disposant des clés ;
- les clés de réserve doivent être conservées à un endroit sûr et non accessible à des personnes non-autorisées ;
- on ne peut attacher des étiquettes d'identification aux clés qui permettraient de savoir quelle clé va avec quelle serrure. La solution alternative consiste à numéroter les clés ou à y appliquer un code couleur ;
- on peut faire signer un registre par les personnes qui ont reçu une ou plusieurs clés, et ce au moment de la réception ;
- le vol ou la perte d'une clé doit être signalé immédiatement ;
- on ne remet pas des clés aux travailleurs temporaires ;
- les barillets de serrure se combinent avec des clés de sécurité ; sans production de certificat, les clés ne seront pas reproduites puisque le profil est protégé ;
- il faut désigner un responsable de la fermeture de l'entreprise et du contrôle régulier de la serrurerie (fonctionnement, détérioration,…) au moment du départ ;

[1] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c*, 49-53

- S'il y a un système d'alarme, le personnel peut en être informé. Il y a lieu d'expliquer au personnel comment on peut l'activer ; toutefois, la procédure de désactivation sera de préférence réservée au(x) responsable(s) de l'ouverture et de la fermeture.

Par ailleurs, il y a lieu d'être vigilant lors de l'ouverture et de la fermeture de l'entreprise. Il faut rester attentif afin de pouvoir remarquer des personnes ou des circonstances suspectes. L'entrée doit donner une vue générale sur les environs et être suffisamment éclairée. Avant la fermeture totale, toute l'entreprise doit être contrôlée pour repérer d'éventuels « traînards ».

1.9 Alerte à la bombe[1]

Lorsqu'une entreprise est confrontée à une alerte à la bombe, il est difficile de réagir calmement et efficacement. Dans ce cas, huit règles d'or devraient être respectées :

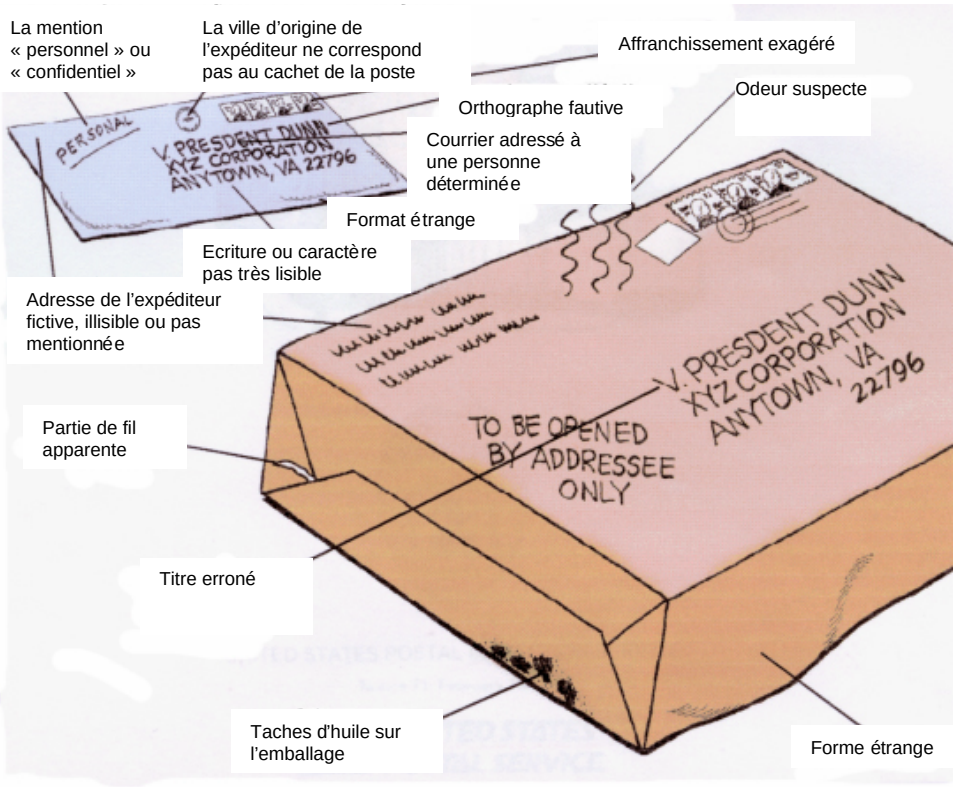
- restez calme ;
- essayez d'obtenir un maximum d'informations de l'appelant (sexe, motif, …). Gardez-le en ligne et notez tout ce qu'il dit ;
- transmettez immédiatement l'alerte au responsable de la sécurité de l'entreprise et prévenez la police. En principe, l'entreprise n'est pas légalement obligée d'informer la police de l'alerte à la bombe. Néanmoins, s'il ne s'agit pas d'une « fausse alerte » et que des dégâts importants sont occasionnés, elle peut être jugée responsable d'avoir négligé l'alerte. Il est important de préciser que la communication d'une alerte à la bombe aux instances policières n'implique pas automatiquement une suspension du processus de production ;
- dès que vous avez été informé d'une alerte à la bombe, ne touchez aucun colis suspect ;
- utilisez une liste de contrôle (checklist) afin de n'oublier aucune action. Cette liste doit se trouver en un endroit où elle est immédiatement accessible ;

[1] N. SCHOOFS, *Bommen op kantoor*, www.vacature.com, 21.08.2004
HOME OFFICE, *Bombs: Protecting People and Property: a handbook for managers,* s.l., Home Office, 10.

- en cas d'évacuation, ne restez jamais devant une fenêtre ou une porte vitrée ;
- ne bloquez pas des issues pouvant être utilisées comme sortie de secours ;
- prévoyez préalablement un endroit où le personnel peut se rassembler en cas d'évacuation. Après un incident, nous vous conseillons d'en changer car il est déjà arrivé, par le passé, que ce lieu d'évacuation soit également touché par une explosion.

Il est utile d'organiser régulièrement des exercices de simulation d'alerte à la bombe afin de tester la procédure d'évacuation et de remédier aux problèmes éventuels.

1.10 Colis suspects (et véhicules suspects)[1]



[1] DGJ/DJP/SERVICE TERRORISME ET SECTES, *colis piégés – éléments d'appréciation et recommandations*, Bruxelles, DGJ/DJP/SERVICE TERRORISME ET SECTES, s.d., 1-4.

Les colis postaux et les lettres devraient, idéalement, être triés dans un local fermé par un membre du personnel expérimenté. Lorsqu'on suspecte qu'une *lettre contient de la poudre*, il faudrait suivre les conseils suivants :

- ne la secouez pas et évitez toute autre manipulation ; n'ouvrez pas l'envoi, même partiellement. Evitez tout contact inutile avec celui-ci ;
- le colis en question doit être isolé, au minimum dans un sachet plastique (idéalement dans deux sachets plastiques fermés hermétiquement) afin d'éviter la « dispersion » de son contenu ; à défaut de sachet plastique ou de tout autre contenant, veillez à ce que personne d'autre ne puisse manipuler le colis ;
- évacuez et fermez le local où se trouve le colis ;
- évitez de ventiler ce local et arrêtez l'air conditionné ;
- si vous avez laissé tomber de la poudre, ne la nettoyez pas mais couvrez-la d'un vêtement, de papier, etc., afin d'éviter qu'elle ne se répande davantage ;
- les personnes qui sont entrées en contact avec le produit devront se laver minutieusement à l'eau et au savon les parties du corps qui ont été en contact direct avec le produit.

Lorsqu'il s'agit d'une *lettre piégée* ou d'un *colis piégé* :

- ne touchez pas le colis et essayez de mémoriser un maximum de détails ;
- la lettre doit être manipulée délicatement ; évitez les vibrations ; quittez le local en emmenant les collègues éventuellement présents ;
- fermez le local, afin de garantir que d'autres collègues ne puissent plus y pénétrer ;
- un périmètre doit être installé aux alentours du local, afin d'organiser une « surveillance » à distance ;
- n'utilisez plus vos GSM, radios portables, etc.

Lorsqu'il s'agit d'un *véhicule suspect* :

- il faut avoir les mêmes réflexes que dans le cas précédent. Un périmètre d'environ 200 mètres doit être envisagé.

Un *colis suspect* ou une *lettre suspecte* peuvent être décelés comme suit :

- une forme bizarre et/ou un poids inhabituel ;
- leur manipulation donne une autre sensation que lorsqu'il s'agit de papier ;
- utilisation de quantités inhabituelles de papier collant ;
- présence de taches de graisse ou de décolorations sur le colis (éventuellement dues à la poudre) ;
- l'adresse de l'expéditeur n'est pas mentionnée, illisible ou incontrôlable ;
- la lettre est inattendue et/ou a été envoyée par un expéditeur totalement inconnu/inhabituel ;
- le pays/la ville d'origine de l'expéditeur ne correspond pas au cachet de la poste ;
- l'adresse contient des fautes ;
- l'écriture utilisée est étrange ou l'adresse est mal dactylographiée (avec éventuellement des fautes d'orthographe) ;
- l'affranchissement est nettement exagéré : il y a trop de timbres sur la lettre ;
- le colis est spécifiquement adressé à une personne déterminée ;
- l'enveloppe porte la mention « personnel » ou « confidentiel » ;
- mode de livraison inhabituel ;
- utilisation de matériaux étranges tels que des cordes, du ruban adhésif ;
- présence de fils électriques/métalliques visibles, utilisation de papier aluminium et/ou présence de trous dans l'enveloppe (éventuellement occasionnés par les fils métalliques) ;
- la lettre dégage une odeur étrange ;
- détection d'un faible bruit de tic tac.

Lorsqu'il s'agit d'une *lettre de menaces* :

- les lettres de menaces doivent être prises au sérieux. Lorsque quelqu'un reçoit une telle lettre, il convient qu'elle soit mise immédiatement dans un emballage en plastique ou en carton. Il faut éviter en effet qu'elle soit manipulée par plusieurs personnes, car cela complique l'analyse d'ADN que peut réaliser la police scientifique.
- le destinataire devrait prévenir la police locale qui, conformément aux procédures internes de la police intégrée, informera les services spécialisés.

1.11 Autres incidents NBCR[1]

Lorsqu'un objet dégage une odeur suspecte ou de la fumée, il faut songer aussitôt aux poudres et sprays suspects. Leurs effets peuvent se manifester soudainement par, entre autres, des problèmes respiratoires, des vomissements ou des troubles de l'orientation auprès du personnel ou des animaux (p.ex. les chiens de garde).
En cas d'incident NBCR *en dehors* du bâtiment :

- éteignez la climatisation, les ordinateurs, les photocopieuses et les radiateurs avant d'évacuer le bâtiment ;
- fermez les fenêtres et les portes lorsqu'on quitte la pièce. Il est conseillé de laisser la clé sur la porte ;
- quittez le bâtiment et éloignez-vous le plus possible du lieu de l'incident ;
- en cas de doute, attendez l'autorisation des services de secours avant de quitter le bâtiment ;
- éloignez-vous le plus possible de l'objet suspect. Attention à la direction du vent, et mettez vous dos au vent en regardant le lieu de l'incident ;
- prévenez les services de secours.

[1] METROPOLITAN POLICE, *Business Response to Terrorism*, London, Anti Terrorist Branch Counter Terrorism Section New Scotland Yard, s.d., 3-4.

Au cas où un incident NBCR se produit *à l'intérieur* du bâtiment :

- si l'objet est encore intact, ne le secouez pas et ne l'ouvrez pas. Si vous avez déjà touché l'objet ou si l'avez encore dans les mains, mettez-le dans un sac en plastique transparent ou dans un conteneur. S'il n'y a pas de conteneur, couvrez-le par un objet à portée de main comme p. ex. un vêtement, du papier, … et n'enlevez ou ne déplacez pas ce dernier ;
- ne touchez aucun objet suspect et ne le déplacez pas ;
- éteignez la climatisation, les photocopieuses, les imprimantes, les ordinateurs et les radiateurs ;
- fermez toutes les fenêtres et les portes tout en laissant la clé dans la pièce et évacuez la pièce ;
- si possible, mettez un avertissement bien visible sur la porte ;
- rendez-vous dans une pièce isolée et évitez, dans la mesure du possible, le contact avec d'autres personnes ; ceci est nécessaire, notamment lorsque l'emballage risque d'être toxique ou que son contenu pourrait causer une maladie contagieuse ;
- ne vous frottez pas les yeux, ne vous touchez pas le visage et évitez le contact physique avec d'autres personnes ;
- prévenez les services de secours.

1.12 Documents secrets[1]

Il est préférable de détruire les documents spéciaux, les enregistrements, les photos qui ne sont plus indispensables après un laps de temps ou de les conserver dans un coffre ou dans des pièces accessibles uniquement aux personnes habilitées.

2 Mesures architechtoniques

En complément des mesures d'organisation, il y lieu de prendre des mesures architectoniques afin de garantir un bon niveau de sécurité.
Par mesures architechtoniques, on entend toutes les mesures de sécurité relatives au bâtiment. Il s'agit, entre autres, du vitrage anti-effraction, grillage, éclairage de sécurité, protection mécanique des fenêtres, des portes, des portes de garages, des quais de chargement et de déchargement, la serrurerie. Si possible, il faudrait prévoir ces équipements dès la phase de projet d'une construction neuve. Les frais seront beaucoup moins élevés que lorsqu'on doit les installer après la réception du bâtiment. Outre l'organisation et l'aménagement du bâtiment, les mesures architectoniques tiennent également compte de l'environnement immédiat et de l'extérieur de l'entreprise, de l'aménagement du terrain, de l'implantation du bâtiment et de son accès, ainsi que de l'utilisation de l'éclairage et des clôtures appropriées.
Les mesures architectoniques s'expriment dans le choix des matériaux, l'organisation, la structure du bâtiment et sa protection mécanique et physique. Les conseils et suggestions ci-dessous se limitent aux portes et à l'éclairage[2].

[1] OVERSEAS SECURITY ADVISORY COUNCIL (OSAC), *Guidelines for protecting U.S. Business Information Overseas*, s.l., United States Department of State, 1994, 9.
[2] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 41, 43, 57

2.1 Les portes[1]

Toutes les portes d'accès doivent être suffisamment solides et peuvent être équipées de serrures spéciales. Les portes vitrées méritent une attention particulière : d'une part, leur transparence offre l'avantage que le personnel de l'entreprise remarque plus facilement les situations suspectes, mais d'autre part, le verre n'est pas le matériau le plus sûr ni le plus solide pour une porte.
En cas d'explosion, les éclats de verre projetés par des portes vitrées et des fenêtres causent souvent beaucoup de dégâts. La meilleur solution est d'installer du vitrage muni d'une pellicule anti-éclats et d'adapter l'épaisseur du verre en fonction des endroits qui présentent le plus de risques de faire l'objet de menaces terroristes.

2.2 Eclairage[2]

- On ne peut sous-estimer l'importance d'un éclairage de sécurité. Un terroriste potentiel veut perpétrer son acte sans être dérangé ni vu. Le manque de temps et la possibilité d'être découvert forcent l'intrus à se dépêcher. Un bon éclairage a un effet dissuasif et est essentiel pour la qualité du film des caméras de sécurité.
- L'éclairage de sécurité, combinée avec d'autres barrières physiques et d'une alerte rapide, peut amener le terroriste à renoncer à ses projets.
- Un bon éclairage permanent du parking a également un effet dissuasif puisqu'il met l'intrus en pleine lumière. Un éclairage de nuit permanent peut être allumé et éteint automatiquement par un interrupteur crépusculaire ou par une minuterie.
- un « éclairage dissuasif » a l'avantage incontestable d'allumer une lampe très puissante grâce à un détecteur de mouvement, ce qui attirera notre attention tout en ayant un effet dissuasif sur l'intrus, a fortiori, lorsque les abords sont surveillés.

[1] HOME OFFICE, *Bombs: Protecting People and Property: a handbook for managers*, s.l., Home Office, s.d., 11-12.
[2] Ibid. 11.
SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 60

3 Mesures électroniques[1]

Les mesures électroniques sont de nature complémentaires et ne peuvent être dissociées des mesures d'organisation et architectoniques.
Leur efficacité dépend de la manière dont on les utilise. Ainsi, la valeur préventive d'une caméra ne sera pas utilisée de manière optimale si personne ne regarde les images en direct à l'écran du moniteur. Un système d'alarme électronique coûteux ne sera pas utile si personne ne sait exactement comment il faut s'en servir. En outre, les inventions technologiques dans le domaine de la sécurité sont presque impossibles à suivre. Le responsable du système a la lourde tâche de suivre les évolutions les plus récentes. Par ailleurs, l'électronique est très sensible aux perturbations. Il est donc nécessaire de bien entretenir les systèmes d'alarme et de surveillance par caméras et par vidéo,… pour que ces moyens de protection restent efficaces.

3.1 Les systèmes d'alarme[2] [3]

Il existe plusieurs systèmes d'alarme. Le choix du système le plus approprié sera déterminé par la disposition du bâtiment et les circonstances. Une sirène externe est un appareil sonore que l'on entend à l'extérieur de l'immeuble protégé. Un système d'alarme avec système externe doit également être équipé d'un éclairage externe dont les signaux lumineux sont visibles depuis la voie publique. L'éclairage externe doit fonctionner jusqu'à ce que l'alarme soit désactivée.
Un système d'alarme est une installation complexe. Un bon système d'alarme est fait sur mesure. A cet égard, il faut tenir compte de la nature de l'immeuble à protéger, des activités exercées par l'entreprise et des habitudes de l'utilisateur.

[1] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*,41,43
HOME OFFICE, *o.c.*, 11.
[2] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 69-70
[3] Attention! L'installation et l'utilisation de systèmes d'alarme fait l'objet d'une réglementation spécifique : voir http://www.vigilis.be

3.2 Systèmes de caméras[1] [2]

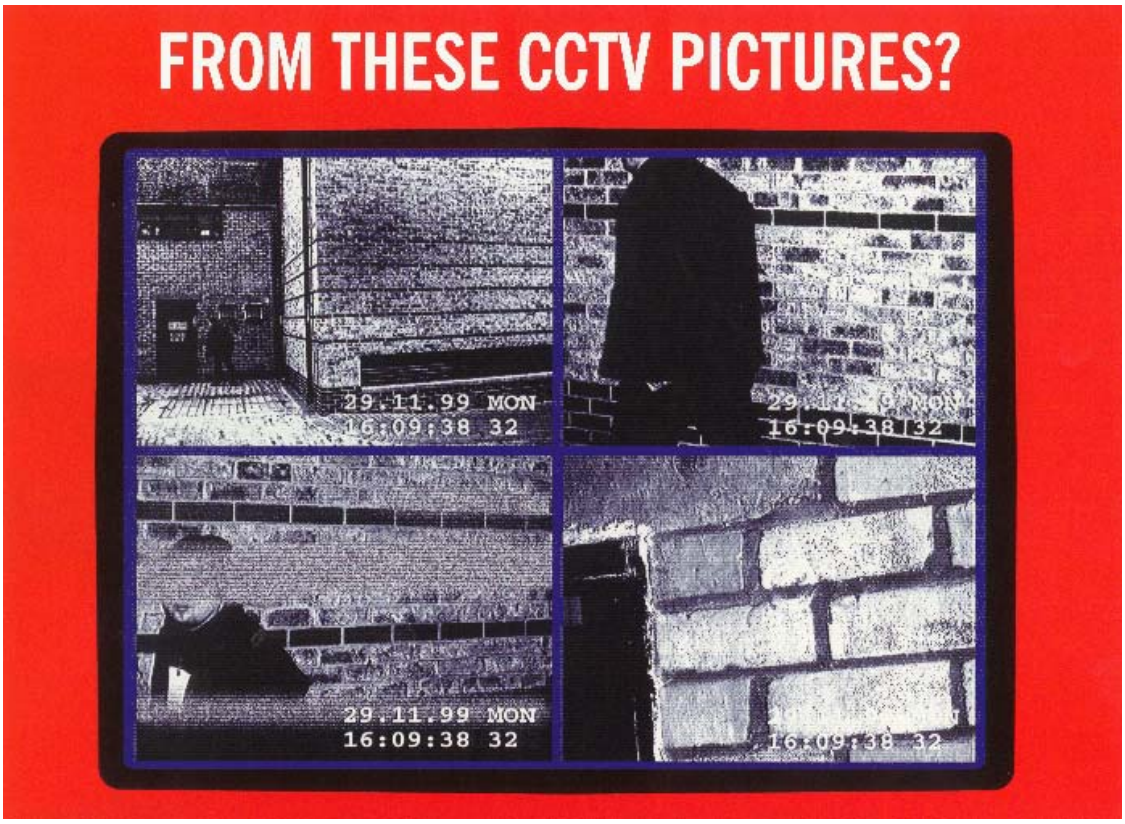
Les caméras sont très importantes pour assurer la sécurité interne et externe de l'entreprise. Bien placées, elles peuvent contribuer à la prévention du terrorisme. Leur présence permet en outre de filmer les terroristes, ce qui, à un stade ultérieur, facilitera l'éventuelle identification des auteurs d'un délit ou des témoins. *La surveillance par caméras* assure l'enregistrement en temps réel à l'aide d'un moniteur. Les images sont transmises à un poste de contrôle où les moniteurs sont surveillés et les caméras réglées si nécessaire. Lorsqu'il s'agit de *surveillance par vidéo*, les images sont enregistrées sur cassette vidéo. Afin d'assurer un fonctionnement optimal de la surveillance par caméras, il faut opter pour un appareillage et une installation de haute qualité. Il n'y a pas que les qualités techniques des composants qui détermineront le résultat final, mais aussi la façon dont l'appareillage est installé. Des facteurs importants sont :

- un manque d'information sur les possibilités des systèmes de caméras ;
- l'absence d'un objectif clair avant l'installation de caméras ;
- une attention disproportionnée pour la technique par rapport à la fonctionnalité du système ;
- l'absence de test d'enregistrement ;
- l'absence de bonnes instructions d'emploi ;
- l'absence d'entretien de l'appareillage ;
- l'absence d'une bonne gestion des cassettes. Il faut remplacer régulièrement les cassettes vidéo. En effet, des caméras mal entretenues donnent des images de mauvaise qualité (et donc inutilisables) ;

[1] HOME OFFICE, o.c., 11
SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*,73-75
METROPOLITAN POLICE, *Could you identify this criminal from these CCTV pictures?*, London, Metropolitan Police, s.d.

[2] Attention! Il faut respecter les règles en matière de protection de la vie privée : voir http://www.privacy.fgov.be

- les cassettes vidéo doivent être conservées pendant au moins un mois après l'enregistrement ;
- l'heure et l'affichage doivent être correctement paramétrés;
- il faut utiliser des cassettes de bonne qualité ;
- les caméras doivent être posées de manière à ce qu'elles puissent filmer clairement les gens et les véhicules ;
- la plupart des criminels reconnaissent rapidement les caméras factices.



4 Mesures TIC[1]

4.1 Recommandations préventives générales relatives aux TIC

Les ordinateurs peuvent donner lieu à d'énormes problèmes de sécurité. Ils contiennent de grandes quantités d'information. Si les systèmes informatiques ne sont pas protégés, le terroriste peut facilement s'approprier des informations ou influencer négativement le processus de production. La criminalité informatique vise à attaquer des systèmes informatiques, des réseaux de télécommunication ou des infrastructures critiques telles que des systèmes de contrôle ou des systèmes financiers.

Depuis la naissance de l'Internet, les terroristes peuvent opérer au niveau mondial. En propageant des virus, ils peuvent causer des dommages importants aux systèmes et fichiers informatiques. Ainsi, il leur est également possible d'arrêter des processus (de production) informatisés. Par ailleurs, le piratage leur permet d'obtenir des informations utiles. Par la propagation de virus dans certains mails, ils sont à même d'obtenir les adresses e-mail ou les données cruciales dont ils ont besoin. Les ordinateurs en réseau peuvent être facilement infectés.

Le terrorisme informatique permet donc de frapper la technologie informatique de trois manières :

- soit de manière directe contre le système informatique même, p.ex. par le hacking ;
- soit de manière physique, contre l'infrastructure TIC critique ;
- soit par le biais d'une personne qui jouit de la confiance de l'entreprise ou qui parvient à pénétrer celle-ci afin de pouvoir accéder au système.

Il existe plusieurs mesures de protection contre les différentes formes de terrorisme informatique.

[1] NCPC, *United for a Stronger America: Citizens Preparedness Guide,* s.l., USA Freedom Corps Department of Justice, s.d., 84.
OVERSEAS SECURITY ADVISORY COUNCIL (OSAC), *Guidelines for protecting U.S. Business Information Overseas,* s.l., United States Department of State, 1994, 2.
SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 51.

Pour faire obstacle aux virus, il faut d'abord se demander si le logiciel, les disquettes et les CD viennent d'une source fiable. Si le logiciel vient de l'extérieur, il est nécessaire de le faire scanner par un programme anti-virus constamment mis à jour pour détecter d'éventuels virus à temps. Par ailleurs, les ordinateurs doivent être protégés par des mots de passe. Dès que l'utilisateur d'un ordinateur quitte son poste, ne fût-ce que pour quelques minutes, il doit fermer sa session. Les e-mails suspects ou venant d'expéditeurs inconnus doivent être traités avec prudence.
Il est préférable de garder les ordinateurs à des endroits fermés à clé et les ordinateurs portables – qui méritent toujours une attention particulière – dans un coffre. Des vols temporaires d'ordinateurs ont souvent lieu aux aéroports dans le but de transférer certaines données et informations vers un autre ordinateur.
Enfin, il est souhaitable de copier chaque jour les fichiers importants pour les conserver à un autre endroit. Il est toutefois déconseillé de les emporter chez soi.

4.2 Recommandations préventives concrètes relatives aux TIC[1]

- Installez des programmes anti-virus récents et mettez-les à jour régulièrement.
- Installez un « pare-feu » pour repousser les « hackers ».
- Faites régulièrement des « backups » des programmes et des données et gardez-les à un endroit sûr.
- Rédigez un document général reprenant des directives pour l'usage normal des systèmes TIC.
- Etablissez des consignes de sécurité pour l'utilisation des TIC.
- Il est souhaitable d'expliquer à tous les travailleurs qu'ils ont aussi un rôle à jouer au niveau de la protection des données de l'entreprise en général et de l'infrastructure TIC en particulier.
- Le respect de la politique d'utilisation des TIC doit être contrôlé.
- Il est souhaitable de désigner un responsable de la sécurité des TIC.
- Si possible, les systèmes de TIC qui sont cruciaux pour l'entreprise devraient être tenus à l'écart de l'Internet.
- L'horloge système du serveur doit être synchronisée régulièrement avec l'horloge atomique sur Internet.

- Activez les applications de connexion des pare-feu, serveurs proxy et accès aux réseaux.

4.3 Recommandations aux victimes de la criminalité informatique[2]

- Interrompez les connexions avec des systèmes externes, tels que l'Internet.
- Notez les données suivantes :
  - les derniers sites visités / pseudonyme de l'interlocuteur / l'adresse Internet (IP) du correspondent ;
  - l'heure exacte à laquelle les faits se sont produits (si possible à la seconde près).
- Evaluez si le dommage est plus important que le redémarrage des connexions TIC
  - si le redémarrage est plus important, faites un backup complet avant de réinstaller le système ;
  - si c'est le dommage qui est le plus important, ne touchez à rien et appelez la police.
- Conserver tous les fichiers de connexion dans leur forme originale.
- N'échangez pas d'e-mails sur l'incident via votre propre système TIC.
- Changez tous les mots de passe et, si possible, les noms des utilisateurs.
- Vérifiez sur Internet les problèmes de sécurité connus relatifs à votre système d'exploitation.
- Intégrez les mises à jour disponibles en matière de sécurité dans votre système d'exploitation.
- Ne rétablissez les connexions Internet que si vous êtes sûr que toutes les mesures de sécurité ont été prises.

[1] L. BEIRENS, *Algemene aanbevelingen voor een veiliger ICT-gebruik,* Brussel, FCCU, 2001, 1.
[2] Ibid., 1.

5 Protection personnelle

L'implication du personnel est la clef de voûte de la sécurisation de l'entreprise. Un plan de sécurité intégral nécessite plus qu'une série de dispositifs techniques, surtout lorsque la structure du personnel de l'entreprise est complexe. C'est pourquoi les mesures personnelles sont considérées comme un complément des mesures architectoniques et électroniques. Très souvent, l'efficacité de ces moyens dépend de l'implication du personnel et de sa connaissance de leur utilisation correcte. Par ailleurs, le personnel est souvent à la base des mesures d'organisation. En d'autres termes : quels arrangements ont été pris en matière de responsabilités, comment réagit-on aux problèmes,… Bref, quels sont les arrangements et les règles qui existent pour le personnel[1] ?

Les grandes entreprises font souvent appel à des *sociétés de sécurité externes*. Les plus petites peuvent aussi avoir une vue générale sur l'ensemble du terrain de l'entreprise en postant le personnel de manière dispersée. Parfois, il peut être souhaitable d'utiliser des chiens de garde. Certaines entreprises peuvent également conclure un accord avec les entreprises voisines du même zoning industriel pour confier la surveillance à une société de sécurité externe.

[1] SERVICE PUBLIC FEDERAL INTERIEUR, *o.c.*, 41.

Conclusion

Les entreprises peuvent être victimes d'actions terroristes ou extrémistes. Leur vulnérabilité réside dans le fait que les terroristes ou les extrémistes peuvent les utiliser comme moyen ou les prendre pour cible. Une action terroriste peut donc avoir des conséquences très diverses. Aussi est-il préférable que les entreprises interviennent de manière préventive si elles veulent essayer d'éviter, ou pour le moins de limiter les conséquences de telles actions.

Les entreprises devraient d'abord avoir une perception concrète du terrorisme et de l'extrémisme et de leurs tendances actuelles. Ensuite, elles peuvent utiliser un Business Continuity Plan, dont la structure systématique présente un avantage non négligeable.

Enfin, une analyse des menaces et des risques leur permettra de prendre certaines mesures de protection préventives dont le contenu peut être adapté aux besoins et attentes spécifiques de l'entreprise.