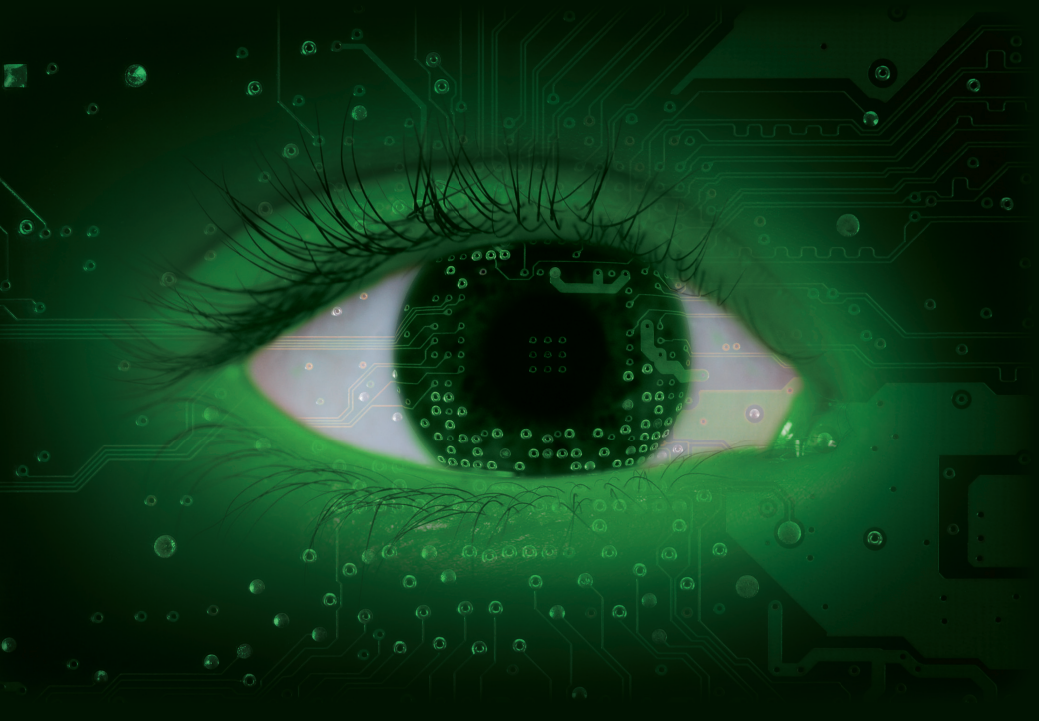
VSSE

ESPIONNAGE ECONOMIQUE

Conseils pratiques pour se protéger contre l'espionnage économique



ESPIONNAGE ECONOMIQUE

Conseils pratiques pour se protéger contre l'espionnage économique

TABLE DES MATIERES

1. Introduction 5

2. Protection du Potentiel Economique et Scientifique..... 6

3. Espionnage économique..... 7

3.1. Origine..... 7

3.2. Informations recherchées..... 8

3.3. Méthodes..... 9

3.4. Conseils pratiques pour se prémunir contre l'espionnage 15

3.4.1. Conseils généraux..... 15

3.4.2. Bureaux..... 16

3.4.2. Voyages (d'affaires)..... 18

3.4.4. Personnel 19

3.4.5. ICT..... 20

4. Contacter la Sûreté de l'Etat 23

1. INTRODUCTION

Cette brochure a pour objet l'espionnage économique. Elle est destinée en premier lieu aux entreprises belges. Les services publics et les départements de recherche qui traitent des informations technologiques, scientifiques et économiques sensibles peuvent également y trouver un intérêt.

C'est en 1998 que la Sûreté de l'Etat s'est vue confier la tâche de protéger le Potentiel Economique et Scientifique (PES). En comparaison avec les deux autres missions de renseignement dévolues au service que sont la protection de la sûreté intérieure et extérieure du pays, la sauvegarde du PES constitue sans conteste une relative nouveauté. La Sûreté de l'Etat s'acquitte des deux premières missions depuis la création du service, peu après l'indépendance de la Belgique.

La charge de sauvegarde du PES nouvellement confiée à la Sûreté de l'Etat en 1998 ne relève toutefois pas du hasard. Depuis la fin du vingtième siècle, nous assistons en Belgique comme à l'étranger à un regain d'intérêt de plus en plus soutenu des services de renseignement et de sécurité nationaux au problème de la sûreté économique. Ceci peut s'expliquer par l'importance accrue de cette dernière au sein du concept de sûreté nationale. Le monde occidental ayant connu un développement et un succès économique sans précédent depuis la Seconde Guerre mondiale. Certes, tous les pays bénéficiant d'un bien-être économique souhaitent le conserver voire l'augmenter. Aussi, les plans nationaux de sécurité intègrent-ils la protection des facteurs de croissance économique contre les pays concurrents. La mondialisation de l'économie étant à l'œuvre, l'intensification de la concurrence économique internationale et le déplacement des intérêts stratégiques au-delà les frontières y contribuent.

2. PROTECTION DU PES

La sauvegarde du PES fait partie de la mission de renseignement dévolue au service. Dans ce cadre, la Sûreté de l'Etat peut rechercher, analyser et traiter le renseignement relatif aux activités susceptibles de menacer le potentiel économique et scientifique belge. Le législateur n'autorise toutefois pas le service à recueillir n'importe quelles informations. Celles-ci doivent avoir un rapport avec au moins une des sept menaces mentionnées dans la loi, à savoir : l'espionnage, l'ingérence, le terrorisme, l'extrémisme, la prolifération, la criminalité organisée et les organisations sectaires nuisibles.

La protection du PES par la Sûreté de l'Etat n'implique pas pour autant la protection physique de l'infrastructure critique. Le service n'est pas davantage chargé de protéger les réseaux informatiques ni de déployer des agents de surveillance dans les laboratoires. Il incombe par contre à la Sûreté de l'Etat de recueillir de manière active les informations relatives à des menaces potentielles ou existantes.

3. ESPIONNAGE ÉCONOMIQUE

Il existe plusieurs sortes d'espionnage: politique, militaire, scientifique et technologique, économique, industriel, commercial, etc. Les définitions de ces formes d'espionnage ne font hélas l'objet d'aucun consensus. Chaque pays possède ses propres définitions. La nature du donneur d'ordre (gouvernement/société/particulier) et/ou les informations recherchées sont autant d'éléments qui justifient ces différences. Ainsi, la Sûreté de l'Etat définit l'espionnage économique comme étant toute forme d'espionnage qui vise le recueil d'informations exploitables sur le plan économique.

L'espionnage économique constitue un phénomène particulièrement difficile à appréhender. Sa représentation demeure en effet fragmentaire et anecdotique, tant en Belgique qu'à l'étranger.

Ceci s'explique aisément. Premièrement, de nombreuses sociétés ignorent avoir été la cible d'espionnage. Deuxièmement, la plupart des entreprises ayant découvert les manœuvres d'espionnage dont elles ont été les victimes sont réticentes à les mentionner. Craignant pour leur image et redoutant les réactions des actionnaires, elles se refusent à communiquer à ce propos et à déposer une éventuelle plainte.

3.1. ORIGINE

Il est frappant de constater que le domaine de l'espionnage économique ne s'accommode pas des représentations traditionnelles que nous nous faisons de l'ennemi ni des alliances classiques. Tant les pays alliés que ceux qui le sont «moins» (ou encore les entreprises ou les ressortissants de ces pays) peuvent constituer une menace sur le plan de l'espionnage économique. Les alliances classiques partagent des objectifs de sécurité politiques, militaires ou autres. La concurrence économique internationale implique cependant des divergences entre

les coalitions existantes. Dès lors, la plupart des pays concurrents - et certainement ceux qui disposent d'un service de renseignement offensif - sont susceptibles de menacer le potentiel économique et scientifique belge.

Les rapports belges et étrangers nous enseignent que plus de cent pays sont impliqués dans l'espionnage économique. Il s'agit tant de pays industrialisés développés que de nations émergentes. Si nombre de pays se livrent à l'espionnage économique, la majorité des tentatives les plus agressives peuvent être attribuées à quelques-uns, dont la Chine et la Russie.

L'espionnage économique n'est cependant pas le monopole de gouvernements. Il peut être commandité par des acteurs aussi divers que des entreprises publiques ou privées, des gouvernements étrangers ou des entités entretenant des liens avec eux (une société sous contrôle gouvernemental, par exemple) ou même de simples particuliers. En effet, les informations disponibles démontrent que l'espionnage est tout autant le fait d'entreprises commerciales que de gouvernements étrangers. La proportion de ces commanditaires non-gouvernementaux tend encore à s'accroître.

3.2. INFORMATIONS RECHERCHÉES

Le terme «espionnage économique» est spontanément associé au vol de secrets en matière de recherche et de développement (R&D). Si les informations dans ce domaine sont certes convoitées, le champ visé par l'espionnage économique s'avère, dans la pratique, sensiblement plus vaste. L'espionnage cible avant tout l'obtention d'informations concernant indifféremment la R&D, les prototypes, les données de fabrication, les spécifications des produits, les plans stratégiques, les listes des clients , ainsi que les données financières et les informations concernant les fusions/acquisitions

Nous pouvons opérer un certain nombre de rapprochements entre les cibles des tentatives d'espionnage et l'origine de ces dernières. En effet, l'espionnage ne vise pas toujours «les joyaux de la couronne». Les tentatives d'espionnage émanant des pays émergents ou des nations qui œuvrent activement à résorber leur retard technologique et économique pour se hisser au niveau de l'Occident ciblent principalement la technologie, le *know-how* et les informations destinées à faire progresser leur propre industrie. Cependant, les technologies de pointe ne constituent pas nécessairement des cibles prioritaires.

En dehors des évolutions technologiques susceptibles de venir renforcer leur position de concurrence, les pays industrialisés peuvent également s'intéresser à la stratégie, au marketing ou encore aux informations commerciales. Par ailleurs, il convient de prendre en compte le rôle joué par la situation géopolitique actuelle du pays d'origine. Ainsi, certains pays ciblent plus spécifiquement la technologie en matière d'armement ou dans le domaine nucléaire.

3.3. MÉTHODES

Les méthodes utilisées pour le recueil d'informations et l'espionnage économique sont très diversifiées et ne sont pas forcément illégales. Elles vont des simples techniques de collecte de renseignements

aux activités d'espionnage au caractère clandestin indiscutable. Étonnamment, les techniques légales sont plutôt efficaces. Ce qui s'explique par le fait que nombre d'entreprises traitent de manière inadéquate leurs informations secrètes ou sensibles.

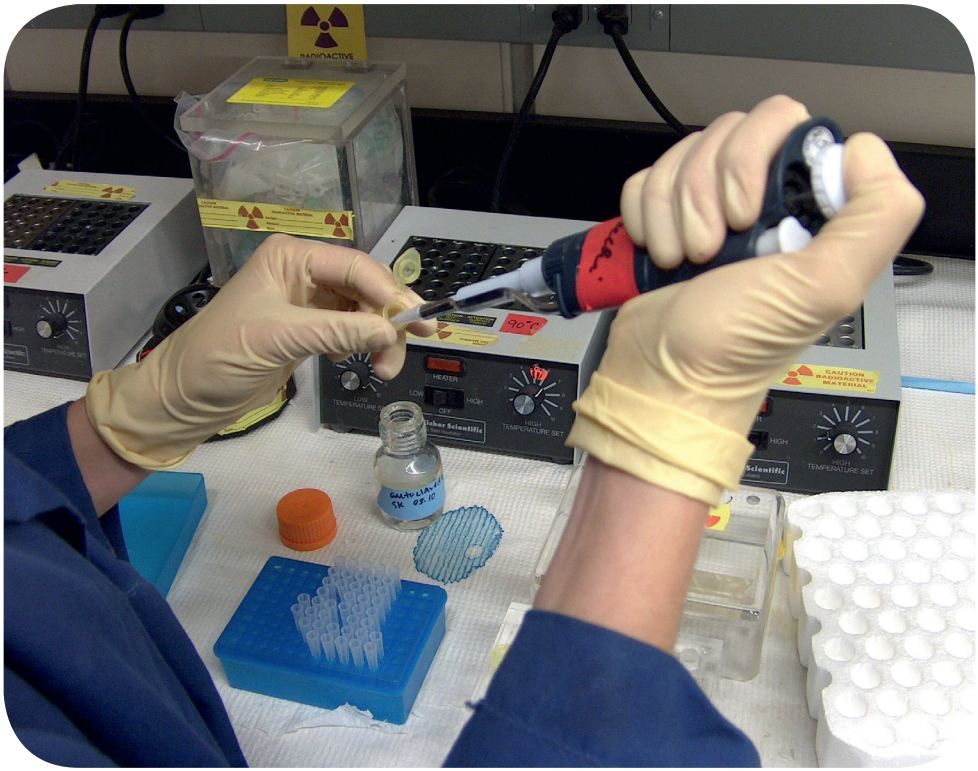
Voici un aperçu des méthodes les plus souvent usitées:

1) ***Simple question.*** La manière la plus évidente d'obtenir des informations est simplement de les demander. Cette méthode est prodigieusement efficace. Car l'entreprise ne précise pas toujours à ses employés les informations en leur possession qu'il convient de considérer comme sensibles. Toute personne à la recherche d'informations - et qui est à même de créer un contexte adéquat – peut ainsi parvenir à son but sans éveiller de soupçons. La plupart des tentatives d'extorsion d'informations relèvent de cette méthode.

2) ***Achat direct.*** Cette technique est utilisée pour l'acquisition de technologie protégée par la législation soumise au contrôle à l'exportation ou relative à la prolifération (il s'agit principalement de technologie militaire et nucléaire). Le vendeur ignore parfois que son produit entre dans le champ d'application de la législation relative à l'exportation et à la prolifération. Il arrive également que l'acheteur potentiel falsifie les informations concernant l'utilisateur final (*end*-user) afin de faciliter l'achat ou de tromper les autorités.

3) ***Offre de services et de produits.*** Sous couvert de la conclusion d'une vente, l'accès à des informations sensibles peut constituer l'objectif réel d'entreprises proposant leurs services à des fins d'espionnage économique. Des techniques variées sont utilisées à cette fin: l'introduction de travailleurs sous-traitants au coeur même de la firme ciblée, la livraison de d'équipements et services (réseaux informatiques, centraux téléphoniques, etc.) permettant le recueil *a posteriori* d'informations, ou encore l'accès temporaire au réseau informatique ciblé afin d'y introduire chevaux de Troie, virus ou autres logiciels espions.

4) ***Manipulation d'hommes d'affaires et d'experts à l'étranger.*** Les personnes en séjour professionnel à l'étranger ne sont pas toujours conscientes des risques qui peuvent se présenter à elles sur le plan de la sécurité: la douane ou les services de sécurité des aéroports ou des frontières peuvent fouiller les documents et les ordinateurs, la sécurité des chambres d'hôtel est bien moindre que celle des bureaux du pays d'origine. De même, l'interception des télécommunications est plus facile à l'étranger et il est bien plus aisé pour les agents de renseignement d'approcher des personnes ou de les attirer dans des situations compromettantes.



5) ***Visites des entreprises.*** Les visites dans les entreprises constituent une méthode classique d'accès au(x) bâtiment(s) qui abrite(nt) une firme ou une institution. Dans de nombreuses entreprises, il arrive que les visiteurs soient emmenés dans des locaux abritant des informations confidentielles. La personne en quête d'informations peut alors discrètement s'éloigner du groupe d'invités et s'attarder «fortuitement» dans des locaux où sont stockées des informations sensibles. Il convient dès lors de refuser l'accès à l'entreprise, ou du moins de considérer comme suspect tout membre d'un groupe de visiteurs qui n'a pas préalablement communiqué son identité.

6) ***Exploitation des liens de coopération entre firmes.*** L'étroite collaboration entre firmes - étrangères ou non - par le biais de *joint ventures* par exemple, permet la réalisation d'objectifs communs. Une telle coopération est cependant susceptible d'être détournée à des fins d'espionnage. Ce dernier peut notamment se traduire par une proposition de transfert unilatéral d'informations, l'exercice de pressions afin d'obtenir un accès illimité au réseau informatique, un dévouement excessif du personnel employé par le partenaire, des demandes d'informations qui sortent du cadre de l'accord de coopération, etc.

7) ***Espionnage par Internet.*** La majorité des entreprises disposent actuellement d'une connexion Internet. Celle-ci, si elle offre de nombreuses opportunités, n'en présente pas moins des risques au niveau de la sécurité. Les réseaux des entreprises sont sans cesse exposés aux accès illégaux et malveillants et aux tentatives d'infiltration. L'ignorance et l'utilisation insouciante d'Internet ouvrent la porte aux menaces de sécurité. Souvent, les victimes d'espionnage par Internet ignorent, par exemple, que des informations ont été volées et que celles-ci sont accessibles sur la toile. L'attaque ciblée par e-mail vecteur d'un cheval de Troie est une des techniques les plus utilisées. Il s'agit d'un courriel innocent en apparence, qui est accompagné d'un fichier joint dans lequel se dissimule un logiciel malveillant qui pourra être utilisé à des fins d'espionnage. Il est fréquemment fait appel à des techniques d'ingénierie sociale afin d'inciter le destinataire du courriel

à ouvrir le message et son fichier joint. L'adresse de l'expéditeur peut ainsi être falsifiée et le contenu comme le contexte du message se présenter de manière à ne pas éveiller les soupçons du destinataire.

8) ***Bourses, conférences et colloques internationaux.*** Ces événements peuvent viser à établir un contact avec d'autres entreprises et à recueillir des informations. Les demandes d'informations ne constituent *a priori* pas une activité suspecte dans ce contexte. Cependant, ce milieu ouvert peut être mis à profit pour des tentatives d'espionnage: de tels événements représentent, en effet, l'occasion rêvée de repérer des personnes intéressantes et des cibles potentielles au sein d'une entreprise. Par ailleurs, ces événements se tiennent fréquemment à l'étranger, ce qui accroît la vulnérabilité des membres du personnel qui y prennent part.

9) ***Stagiaires et étudiants.*** Les entreprises et les départements de recherche peuvent tirer profit de la collaboration avec des étudiants et des stagiaires prometteurs. Ces derniers sont souvent invités à travailler sur un projet spécifique. Dans la pratique, il semble toutefois que des mesures de précaution insuffisantes au sein de la firme et/ou la négligence de celle-ci permettent aux stagiaires d'accéder à davantage d'informations que celles dont ils ont strictement besoin pour l'exécution de leur mission. Il y a d'ailleurs des cas avérés d'étudiants et de stagiaires qui ont tiré avantage de leur liberté d'accès aux informations confidentielles de l'entreprise pour les dérober.

10) ***Mise à profit de l'origine ethnique.*** La population belge compte des individus d'origines géographiques et ethniques fort diverses. Cette diversité se reflète évidemment parmi les membres du personnel des entreprises. L'origine de ceux-ci peut être mise à profit à des fins d'espionnage: l'appel à la loyauté du travailleur envers son ethnie ou les menaces proférées à l'encontre de sa famille restée au pays d'origine peuvent constituer autant de moyens de pression à son encontre.

11) ***Les méthodes d'espionnage traditionnelles.*** Les techniques traditionnelles telles que le cambriolage, les écoutes et le recrutement de personnes internes à l'entreprise sont encore utilisées de temps à autres. Le taux de réussite des autres méthodes, associé aux risques importants des techniques classiques, engendre une diminution du recours aux méthodes clandestines.

Mentionnons finalement la menace interne, le danger qui émane de l'intérieur de l'entreprise ou de l'organisation même. La plupart des tentatives d'espionnage ne font cependant appel à aucune collaboration au sein de l'organisation. Cela étant, les activités d'espionnage qui impliquent une personne interne à l'organisation sont susceptibles d'être à la fois les plus réussies et occasioneront les dégâts les plus graves. Il apparaît souvent *a posteriori* que certains indices potentiellement révélateurs concernant des espions actifs au sein du personnel auraient permis de trahir leurs intentions. A cet égard, citons entre autres les soudains signes de richesse, les voyages à l'étranger tenus secrets, les conflits et les frustrations professionnelles. Ces signaux, bien qu'observés, ne sont hélas pas souvent signalés. Néanmoins, le service du personnel, le service social et les collègues peuvent jouer un rôle majeur dans la prévention de la menace interne.

3.4. CONSEILS PRATIQUES POUR SE PRÉMUNIR CONTRE L'ESPIONNAGE

Il est impossible d'assurer une protection totale contre l'espionnage sans perturber sérieusement les activités régulières de l'entreprise. Le respect de certaines directives de sécurité peut cependant écarter une grande partie de la menace. Voici une série - non exhaustive - de conseils qui peuvent servir de base à la mise en œuvre d'une politique de sécurité contre l'espionnage.

3.4.1. Conseils généraux

- Evaluez la réalité de la menace et la nécessité de protéger les informations sensibles. La reconnaissance de la problématique constitue toujours la première étape d'une politique de prévention de qualité.

- Mettez en œuvre un plan de protection des secrets d'entreprise qui soit utilisable. Dans l'éventualité où la transposition du plan de sécurité dans la gestion journalière de l'entreprise présente trop de difficultés, les travailleurs n'appliqueront pas les directives de manière cohérente.

- Identifiez, au sein de la firme ou de l'institution, les informations qu'il convient de considérer comme des secrets d'entreprise. Ceci permet de déterminer quelles sont les données à protéger et de ne pas gaspiller de moyens pour la protection d'informations non sensibles. Par ailleurs et dans la mesure du possible, il y a lieu d'attribuer une valeur monétaire à l'information protégée. Ceci permet de se faire une idée du risque que représente la perte/le vol éventuel de ces informations.

- Déterminez quelles informations sont accessibles et par qui (principe du «*Need to Know*»). S'il est possible de déchiqueter un document et d'effacer les données enregistrées sur un disque dur, les personnes, par contre, emportent leurs connaissances partout avec eux.

- Limitez l'accès aux informations aux seules personnes qui sont effectivement autorisées à en disposer.

- Veillez à ne pas publier par inadvertance dinformations sensibles dans la communication de l'entreprise (site Internet, Intranet, publications, rapports annuels, etc.).

- Ne vous débarrassez pas sans réfléchir de documents comportant des secrets d'entreprise ou des informations confidentielles. Il importe de les détruire de manière appropriée ou de les effacer des supports informatiques lorsqu'ils ne sont plus nécessaires.

- Ne laissez jamais de documents ou autres supports comportant des secrets d'entreprise (ordinateurs portables, clés usb, etc.) sans surveillance hors de l'entreprise (dans un véhicule, à l'hôtel, lors de conférences ou de réunions, etc.).

3.4.2. Bureaux

- Contrôlez l'accès au bâtiment abritant les bureaux. Il convient d'en faire surveiller tout accès par l'entremise du personnel de sécurité et/ou par le biais d'un système d'alarme. Le périmètre aux alentours doit être suffisamment éclairé et sécurisé afin de prévenir toute intrusion nocturne dans le bâtiment.

- Les travailleurs et les visiteurs doivent porter des badges d'accès visibles. Cette recommandation vaut particulièrement pour les lieux où sont conservées les informations confidentielles. Il est souhaitable de pouvoir distinguer les badges des visiteurs de ceux que portent les travailleurs afin que chaque membre du personnel soit à même de reconnaître un visiteur.

- Aménagez, dans le bâtiment, une zone de sécurité renforcée réservée aux informations les plus sensibles et dont l'accès sera autorisé aux seuls membres du personnel habilités à en prendre connaissance. Il

est déconseillé d'autoriser les visiteurs à pénétrer dans cette zone de sécurité renforcée. Dans l'éventualité où l'accès de tierces personnes à celle-ci s'avère nécessaire (pour le nettoyage, par exemple), il y a lieu de les faire accompagner par un membre du personnel dûment autorisé.

- Une politique adaptée en matière de clés s'impose afin de contrôler les accès à l'intérieur du bâtiment. Dans ce cadre, il importe de définir qui peut disposer de clés et lesquelles. Les membres du personnel en possession de clés engagent leur responsabilité à cet égard. Toute perte ou tout vol doit être signalé(e) dans les plus brefs délais afin de pouvoir changer les serrures si nécessaire.

- Il convient de mettre à disposition des travailleurs un nombre suffisant d'armoires fermant à clé ou de coffres-forts afin qu'ils puissent y entreposer leurs documents ou leurs supports comportant des données confidentielles. Si nécessaire, il est indiqué de mettre

en œuvre une *clean desk policy* afin d'éviter que des informations confidentielles ne soient laissées sans surveillance.

- Les hommes d'affaires ont pour habitude d'emporter chez eux des informations sensibles de l'entreprise afin d'y poursuivre leur travail. Dans la mesure du possible, il y a lieu de respecter à domicile des mesures de sécurité identiques à celles appliquées au bureau. Il ne faut pas perdre de vue que le risque de perdre des informations confidentielles s'accroît sensiblement en dehors du bâtiment abritant les bureaux. Le contrôle des informations sortantes s'impose dès lors par la tenue d'un registre de toutes les données confidentielles qui sont emportées hors du bâtiment de l'entreprise. Seuls les membres du personnel dûment habilités sont autorisés à emmener les informations confidentielles de l'entreprise en dehors de celle-ci.

3.4.3. Voyages (d'affaires)

- N'emportez avec vous que les appareils et les informations strictement nécessaires à votre voyage.

- Transportez les supports comportant des informations et les appareils informatiques dans votre bagage à main. Vous pourrez ainsi les garder à l'œil lors des vérifications de sécurité et des contrôles effectués aux frontières à l'étranger.

- N'abandonnez jamais d'informations confidentielles sans surveillance dans une chambre d'hôtel ou dans tout autre endroit.

- N'utilisez que des clés usb et autres supports portables fournis par votre propre entreprise et ne les reliez jamais à des ordinateurs étrangers. Par prudence, partez du principe que l'ordinateur portable ou les supports amovibles peuvent avoir été contaminés au contact de matériel étranger.

- Evitez si possible de vous connecter à des réseaux sans fil.

- Veillez à ce que les personnes présentes à proximité ne puissent pas déchiffrer ce que vous êtes en train de lire, que ce soit à l'écran ou sur papier. La même précaution s'applique à l'égard des personnes susceptibles d'entendre vos conversations.

- Informez-vous avant votre départ de la législation applicable dans votre pays de destination en ce qui concerne l'importation de matériel informatique et l'utilisation des techniques de cryptage.

- Attendez-vous à ce que les moyens de communication (téléphone, fax, GSM, etc.) ne présentent pas les mêmes garanties de sécurité à l'étranger que dans votre pays. Limitez dès lors, dans la mesure du possible, le recours à ces moyens de communication. Il importe de transmettre les informations classifiées par le biais de canaux de communication sécurisés et de les protéger par cryptage.

3.4.4. Personnel

- Veillez à sensibiliser les membres de votre personnel à la sécurité des informations sensibles ou secrètes de l'entreprise et à leur offrir une formation suffisante en la matière. Il y a lieu, à cet égard, de ne pas se limiter à une campagne de sensibilisation et à une offre de formation uniques mais bien de renouveler celles-ci à intervalles réguliers.

- La loyauté entre l'entreprise et le travailleur n'est pas à sens unique. La menace interne surgit souvent au détour de frustrations professionnelles. Un bonne politique du personnel constitue une composante importante de toute politique de sécurité.

- Lors du recrutement de membres du personnel amenés à prendre connaissance d'informations confidentielles de l'entreprise, il est indiqué de procéder à une présélection sur dossier qui s'inscrit dans le cadre légal (le contrôle des références, par exemple). Il est également souhaitable de faire figurer dans le contrat de travail les obligations qui incombent au travailleur en matière de sécurité. De même, l'ajout

d'une clause de non-concurrence pour certaines fonctions importantes au sein de l'entreprise peut s'envisager.

- Les membres du personnel qui quittent l'entreprise doivent rendre toutes les clés et badges d'accès en leur possession. Par ailleurs, il y a lieu de supprimer le plus rapidement possible leurs codes d'accès au réseau informatique.

3.4.5. ICT

- Limitez l'accès physique au matériel informatique, ce qui limite, en effet, le vol d'informations. Il importe dès lors d'interdire à toute personne non autorisée d'accéder à ce matériel. Ceci vaut tout particulièrement pour le matériel transportable tel que les ordinateurs portables, les disques durs externes et les clés usb.

- Concluez des accords clairs et contraignants en termes de procédure et d'accès avec les tierces personnes qui doivent utiliser le réseau informatique (les stagiaires et les prestataires de services, par exemple).

- N'employez que le matériel et les logiciels mis à disposition par l'entreprise. Soyez particulièrement prudent avec les clés usb qui vous ont été offertes en cadeau.

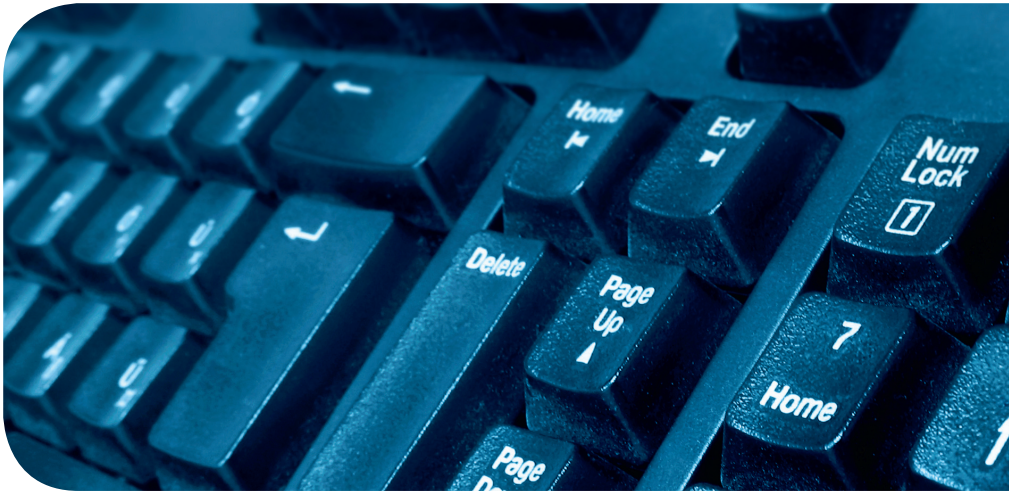
- Procédez aux mises à jour de vos logiciels. Les virus, les chevaux de Troie et autres logiciels malveillants utilisés à des fins d'espionnage tirent profit des failles de sécurité des programmes. Les concepteurs de logiciels proposent régulièrement des mises à jour et des *patches* visant à éliminer ces failles. Il est également indiqué d'élaborer une politique qui permet à l'entreprise ou au service d'installer sur tous les ordinateurs les mises à jour et les *patches* les plus récents.

- Employez des mots de passe complexes (c'est à dire difficile à deviner) et modifiez-les régulièrement (surtout après un voyage à l'étranger). Il convient de ne pas les choisir sur la base d'informations

qui peuvent être connues d'autres personnes (tels que, par exemple, les dates de naissance et les noms des enfants). Les mots de passe complexes se composent de préférence de lettres, de chiffres et de signes de ponctuation.

- Désactivez les fonctionnalités informatiques que vous n'utilisez pas ou dont vous n'avez pas besoin. L'offre standard des ordinateurs comporte souvent des possibilités qui ne sont pas utiles ou nécessaires à tous les utilisateurs. Les vulnérabilités qui caractérisent principalement les connexions sans fil (la *Wifi* ou le *Bluetooth* par exemple) et les applications Internet (entres autres les serveurs Web et FTP) profitent aux *hackers* et à ceux qui veulent tirer profit de ces fragilités. Il est dès lors conseillé de désactiver ces fonctionnalités ou, si possible, de les supprimer lorsqu'elles ne sont pas nécessaires.

- Cryptez vos fichiers de données. Le cryptage des fichiers empêche les personnes non autorisées de lire les informations confidentielles qu'ils comportent, et cela même lorsque ces personnes ont pu accéder d'une manière ou d'une autre au système informatique. Il y a bien sûr lieu d'employer des mots de passe complexes pour le cryptage des fichiers.



- Gardez à l'esprit que les moyens de communication modernes tels que les courriels, les GSM et les PDA ne présentent jamais aucune garantie totale de sécurité et ce, particulièrement lorsqu'ils servent aux communications internationales. Aussi convient-il, ici encore, de recourir à des techniques de cryptage pour l'envoi de secrets d'entreprise par voie électronique. Les documents sur papier ou les supports de données physiques peuvent si nécessaire être acheminés par porteur.

- N'employez pas de logiciels copiés illégalement. Les copies illégales de programmes disponibles sur Internet constituent une des méthodes les plus utilisées afin de disséminer des virus et autres logiciels malveillants.

- L'emploi d'un logiciel à même de détecter les virus garantit dans une large mesure la protection du réseau de l'entreprise. Une mise à jour régulière de la base de données de ce programme s'impose également.

- N'ouvrez aucun courriel ou fichier joint à celui-ci qui vous est envoyé par un expéditeur inconnu. En cas de doute, prenez contact avec l'expéditeur afin de vérifier l'origine du fichier joint. Faites également preuve de prudence lorsqu'il s'agit de cliquer sur des hyperliens repris dans un message. Ceux-ci peuvent avoir été falsifiés afin d'établir une connexion illicite.

4. CONTACTER LA SÛRETÉ DE L'ETAT

Vous pouvez contacter la Sûreté de l'Etat à l'adresse suivante:

Sûreté de l'Etat

Section PES-WEP

Boulevard Roi Albert II, 6

1000 Bruxelles

Téléphone: 02/205 62 11

Fax: 02/205 57 72

E-mail: wep.pes@vsse.be

INFORMATIONS UTILES

Législation

- Loi du 8 décembre 1992 sur la protection de la vie privée à l'égard du traitement des données à caractère personnel

- Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées

- Loi du 25 novembre 2000 relative à la criminalité informatique

- Loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Internet

www.fedict.be

www.fccu.be

www.vbo-feb.be

www.cpni.gov.uk/productsServices.aspx

www.enisa.europa.eu

www.iso.org (voir ISO-norme 27001)

D/2010/7951/FR/842 — Editeur responsable : A. WINANTS - Boulevard du Roi Albert II, 6 1000 Bruxelles — Photos : VSSE - sxc.hu

VSSE

Sûreté de l'Etat
6 Boulevard du Roi Albert II
1000 Bruxelles
info@vsse.be