Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Service de renseignement de la Confédération SRC

PROPHYLAX

Programme de prévention et de sensibilisation
du Service de renseignement de la Confédération

Table des matières

Introduction

Les produits suisses jouissent d'une excellente réputation dans le monde entier. Le savoir-faire et la capacité d'innovation des entreprises et des instituts de recherche locaux sont des facteurs-clés pour la compétitivité de l'économie suisse. Ils forment la base de son rôle de pionnier international dans de nombreux domaines de l'économie et de la recherche. Ce savoir-faire et les produits de haute technologie fabriqués en Suisse suscitent non seulement l'intérêt d'entreprises concurrentes, mais aussi celui d'États étrangers. L'acquisition de produits et de technologies inaccessibles sur le marché en raison de sanctions et de contrôles des exportations, ainsi que la recherche de renseignements sur des entreprises étrangères comptent parmi les missions principales de nombreux services de renseignement étrangers.
Dans l'optique de sensibiliser les entreprises et instituts de recherche suisses à ces menaces, le service suisse de renseignement intérieur[1] de l'époque a créé le programme de prévention et de sensibilisation Prophylax en 2004. Aujourd'hui encore, ce programme accomplit son mandat légal de mise en œuvre de programmes d'information et de sensibilisation aux menaces pour la sûreté intérieure et extérieure de la Suisse[2].
En étroite collaboration avec les services de renseignement cantonaux, le Service de renseignement de la Confédération (SRC) sensibilise les entreprises, hautes écoles et instituts de recherche suisses et liechtensteinois aux menaces liées à l'espionnage et à la prolifération. L'objectif de Prophylax consiste à renforcer les

1 Le Service de renseignement extérieur et le Service de renseignement intérieur ont fusionné en 2010 pour former le Service de renseignement de la Confédération.
2 Cf. art. 6, al. 6, de la loi fédérale du 25 septembre 2015 sur le renseignement (loi sur le renseignement, LRens).

contrôles des exportations de biens et technologies critiques et pertinents en matière de prolifération (notamment les biens à double usage[1]) en identifiant et en empêchant les activités d'acquisition illégales de manière précoce. Cette tâche est d'autant plus importante que la Suisse est l'un des principaux exportateurs mondiaux de biens à double usage (dual-use). De nombreux États mettent en œuvre des programmes similaires de sensibilisation de leurs entreprises dans les domaines de l'économie et de la technologie. Grâce à Prophylax, le SRC soutient les efforts internationaux visant à endiguer la prolifération d'armes de destruction massive.

La prolifération et l'espionnage économique peuvent être intimement liés. Le SRC et les services de renseignement cantonaux sensibilisent également les entreprises et les instituts au risque d'espionnage, y compris à la menace posée par le cyberespionnage, afin qu'ils adoptent une démarche plus prudente vis-à-vis d'informations sensibles dans le but de prévenir les pertes de savoir-faire et les fuites de données.

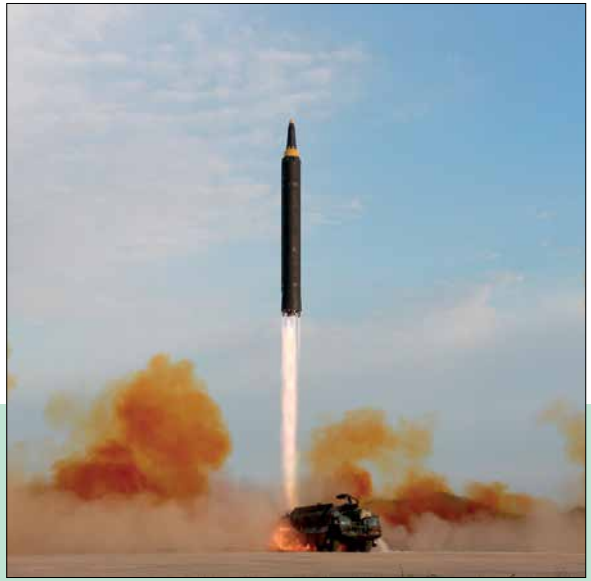
1 Les biens à double usage ont des applications dans le domaine civil comme dans le domaine militaire.

Prolifération

Définition

On entend par prolifération d'une part la dissémination d'armes de destruction massive et de leurs vecteurs (missiles balistiques, missiles de croisière et drones), et d'autre part celle d'équipements, de matériaux et de technologies pouvant également être employés dans la fabrication de ces armes (biens à double usage).

Réservée initialement au domaine nucléaire, la notion de prolifération couvre aujourd'hui l'ensemble des armes de destruction massive – nucléaires, biologiques et chimiques – et des produits de base.



À droite :
un missile balistique nord-coréen à portée intermédiaire (IRBM) HWASONG-12 lors du lancement (Agence centrale de presse nord-coréenne, KCNA)

États préoccupants *(states of concern)*

La prolifération est une menace pour la paix et la sécurité dans le monde. Elle est le fait de pays qui veulent défier l'ordre international ou régional pour asseoir leur pouvoir politique. En développant des armes nucléaires, biologiques et chimiques (dites armes NBC) ainsi que leurs vecteurs, ces pays tentent de renforcer leurs moyens de guerre, d'améliorer leur potentiel de menace et de dissuasion militaire et d'imposer des revendications politiques. Ces pays représentent un danger pour la stabilité régionale et internationale et font partie des pays désignés comme États préoccupants. Cette catégorisation repose sur des considérations à la fois techniques et politiques. Elle contraint la communauté internationale à prendre des mesures actives à l'encontre de certaines activités de ces pays. Aujourd'hui, l'Iran, la Corée du Nord, le Pakistan et la Syrie sont considérés comme des États préoccupants. Il est établi que ces États mènent des programmes de développement d'armes de destruction massive ou qu'ils produisent déjà de telles armes. Ils sont néanmoins tributaires de biens et de savoir-faire étrangers en ce qui concerne le développement, la fabrication et l'étoffement d'arsenaux existants, et ils tentent de contourner les mécanismes de contrôle internationaux au moyen d'activités d'acquisition clandestines en dissimulant par exemple l'usage final d'un produit ou en créant des sociétés-écrans. Certains pays comme la Malaisie, les Émirats arabes unis (notamment Dubaï) ou Singapour sont en outre utilisés comme zones de transit pour des transactions liées à la prolifération. Une attention particulière doit aussi être accordée aux transactions commerciales d'autres États supposés avoir des ambitions dans le domaine de la prolifération.

Les divers États préoccupants présentent des différences en ce qui concerne l'état d'avancement de leurs programmes de recherche et de développement d'armes de destruction massive et de leurs vecteurs. Du point de vue militaire, ces pays veulent poursuivre leurs programmes pour compléter leurs arsenaux, améliorer la sécurité du stockage, les possibilités d'engagement, la précision, la portée et l'efficacité de leurs armes. Ils aspirent par ailleurs à être aussi indépendants que possible en matière d'armements.

Contrôle des exportations et bases légales

La lutte contre la prolifération est l'affaire de toute la communauté internationale. La résolution 1540 du Conseil de sécurité de l'ONU adoptée le 28 avril 2004 demande aux États membres de « prendre et appliquer des mesures efficaces afin de mettre en place des dispositifs internes de contrôle destinés à prévenir la prolifération des armes nucléaires, chimiques ou biologiques ou de leurs vecteurs, y compris en mettant en place des dispositifs de contrôle appropriés pour les éléments connexes ». À cet effet, quatre régimes de contrôle des exportations existent sur le plan international. Des conventions internationales juridiquement contraignantes visent en outre à bannir les armes chimiques et biologiques dans le monde entier.

À gauche :
installation suspectée d'armes chimiques du Scientific Studies Research Center en Syrie, bombardée le 7 septembre 2017 par Israël (prise de vue PLE du 24 septembre 2017)

La Suisse est membre de tous ces régimes et conventions. La politique suisse en matière de contrôle de l'armement et de désarmement a pour objectif de garantir la sécurité nationale et internationale avec un niveau d'armement aussi faible que possible. La Suisse s'engage pour une non-dissémination des armes de destruction massive (non-prolifération) et pour leur élimination totale (désarmement). En tant que membre des régimes internationaux de contrôle des exportations, la Suisse s'emploie à être un maillon solide de la chaîne des pays qui appliquent des mesures contre la prolifération. La Suisse dispose des bases légales nationales suivantes en relation avec le contrôle des exportations[1]:

- Loi sur le contrôle des biens (LCB) ; RS 946.202
- Ordonnance sur le contrôle des biens (OCB) ; RS 946.202.1
- Ordonnance sur le contrôle des produits chimiques (OCPCh) ; RS 946.202.21
- Loi sur le matériel de guerre (LFMG) ; RS 514.51
- Loi sur l'énergie nucléaire (LENu) ; RS 732.1
- Loi sur les armes (LArm) ; RS 514.54
- Loi sur les explosifs (LExpl) ; RS 941.41
- Loi sur les embargos (LEmb) ; RS 946.231
- 24 ordonnances aux termes de la Loi sur les embargos.

1 Voir aussi www.seco.admin.ch/fr (Economie extérieure et Coopération économique → Contrôles à l'exportation et sanctions → Maîtrise des armements et politique de la maîtrise des armements (Matériel de guerre) → Bases légales).

Il convient de noter que des biens ne figurant pas explicitement dans les listes des régimes de contrôle des exportations sont également soumis à une obligation d'annonce et d'autorisation lorsque l'exportateur sait, ou qu'il a des raisons de penser qu'un bien est destiné à la fabrication ou à l'utilisation d'armes de destruction massive (clause *catch-all*). Le contrôle des exportations s'applique également à certaines technologies.

Les activités de prolifération en Suisse peuvent non seulement violer le droit national ou contrevenir aux engagements internationaux, mais aussi mettre en danger les relations politiques et commerciales avec l'étranger et nuire à la crédibilité de la politique suisse en la matière. Les entreprises, instituts de recherche ou hautes écoles impliqués – même involontairement – dans des activités de prolifération perdent leur bonne réputation, peuvent subir de lourdes pertes financières ou faire l'objet de mesures de rétorsion.

Dans quelle mesure les entreprises, hautes écoles et instituts de recherche sont-ils touchés par la prolifération ?

Efforts d'acquisition

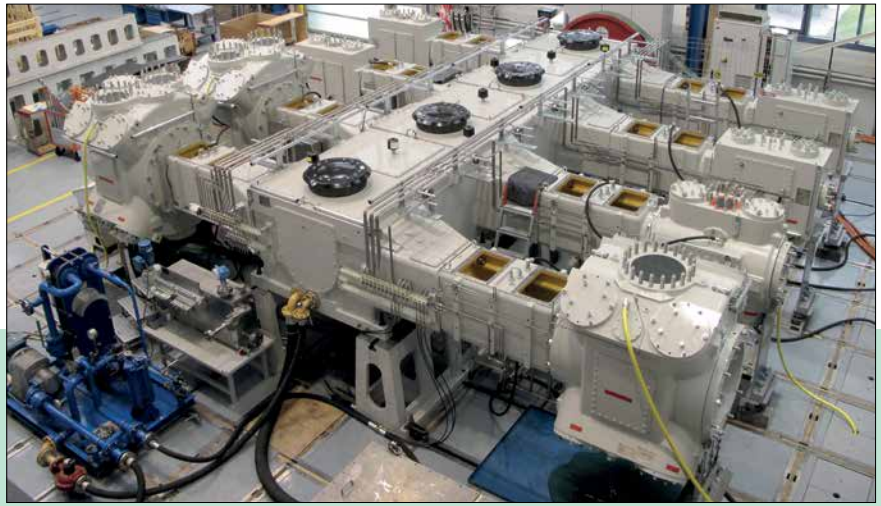
Les armes de destruction massive et leurs vecteurs ne sont pas disponibles sur le marché libre, et les mesures de la communauté internationale sont destinées à faire échouer les efforts d'acquisition des États préoccupants. Les tentatives d'acquisition ne se limitent cependant pas aux biens, mais concernent également les connaissances qui s'y rapportent. Les universités, hautes écoles spécialisées et instituts de recherche sont particulièrement exposés au risque de transfert immatériel de technologie (Intangible Transfer of Technology, ITT).

Pour contourner les contrôles à l'exportation et se procurer des biens sensibles, les acteurs importants dans le domaine de la prolifération recourent à diverses méthodes et à des réseaux d'acquisition clandestins :

- Les utilisateurs finaux étatiques se dissimulent derrière un nom d'entreprise anodin, une organisation d'armement traditionnelle ou une université qu'ils représentent en tant que mandant ou acheteur, ou ils créent une société-écran. Ce faisant, ils disposent également du soutien du service de renseignement de leur pays.
- Des sociétés commerciales neutres sont employées pour ne pas révéler aux fournisseurs qu'une entreprise d'État se cache derrière cette transaction.
- Les acteurs importants dans le domaine de la prolifération créent une petite entreprise pour les besoins de la transaction, puis la liquident à sa conclusion. Pour dissimuler l'identité du véritable utilisateur final, ils font appel à plusieurs intermédiaires pour la livraison et le paiement de la marchandise et la font transiter via des pays tiers (livraison détournée). De telles sociétés ont notamment été repérées dans des pays de transit.
- Les acteurs importants dans le domaine de la prolifération recourent à des noms de projet semblant relever du domaine civil et n'attirant pas l'attention. Ils profitent également de l'inexpérience de certains fournisseurs dans le domaine des exportations et recherchent tout particulièrement des sociétés, notamment des PME, qui ne respectent pas strictement les prescriptions légales en matière de conformité et de contrôle des exportations.

- Ils détournent des entreprises dans le pays de production ou de livraison pour masquer des acquisitions illégales derrière des transactions légales, et ils produisent des documents d'exportation falsifiés ou des certificats d'utilisateur final ne correspondant pas à la réalité.
- Ils divisent l'acquisition en une série de petites commandes, empêchant ainsi d'en détecter l'importance en matière de prolifération.
- Ils cherchent des matériaux et des équipements de substitution pour remplacer les produits figurant sur les listes des biens soumis aux contrôles à l'exportation.

À cause de ces méthodes, les fournisseurs éprouvent des difficultés à déterminer la finalité réelle de leurs produits. Les biens à double usage, qui peuvent être utilisés à la fois dans le domaine civil et militaire, sont particulièrement problématiques.



À droite :
selon des informations, des compresseurs similaires de production suisse auraient dû être utilisés au Pakistan dans le cadre du programme d'armes nucléaires (photo privée)

Comment reconnaître les affaires illégales ?

Une simple commande ne permet pas toujours de déterminer si un produit est destiné ou non au développement d'armes de destruction massive ou d'un système de missile. Il s'agit donc d'examiner avec soin les modalités de la commande, du transport et du paiement de la marchandise. Cela exige de rechercher des informations détaillées sur le pays destinataire, sur l'utilisateur et sur les éventuels intermédiaires.

L'expérience a montré que les méthodes ou comportements suivants de la part de l'acheteur peuvent suggérer une affaire en rapport avec la prolifération.

Utilisateur final

- L'identité d'un nouveau client ne peut pas être clairement déterminée : il fournit des réponses évasives au sujet du profil de l'entreprise et des interlocuteurs, ou n'est pas en mesure de fournir de références convaincantes.
- Le client ne pose aucune question d'ordre commercial ou technique qu'il est pourtant d'usage de poser lors de négociations commerciales ou dans les documents correspondants.
- Le client demande l'achèvement d'un projet commencé par une autre entreprise.
- Le client exige un degré de confidentialité inhabituel et exagéré en rapport avec la destination ou la nature des produits à livrer. Il refuse au vendeur l'accès à ses installations sans motif vérifiable. L'entreprise acheteuse envoie des collaborateurs se faire former en Suisse au sein de l'entreprise productrice, alors même qu'une formation sur place serait plus pratique et plus cohérente, ou le client renonce totalement à la formation, à la garantie et au service après-vente.

Utilisation prévue

- La description des biens demandés n'est pas claire, ou les biens semblent être très spécifiés alors que cela n'est pas nécessaire.
- Le client ne dispose pas des connaissances spécialisées nécessaires et n'est de toute évidence pas au courant des mesures de sécurité usuelles en lien avec les biens commandés. Il ne peut pas indiquer l'utilisation prévue pour le produit (ou refuse de fournir cette information).
- L'utilisation du bien prévue par le fabricant diffère sensiblement de celle prévue par l'acheteur.
- La destination finale de la marchandise n'est pas clairement connue ou n'est pas plausible.

Relation commerciale

- Des intermédiaires se manifestent sans motif apparent.
- Le client propose des conditions de paiement particulièrement avantageuses (avances en espèces ou importantes, commissions supérieures à la moyenne).
- Le client exige des mesures de sécurité qui semblent exagérées au vu de l'utilisation prévue. Les exigences du client en matière d'emballage ne sont pas plausibles (p. ex. emballage maritime pour une livraison au sein de l'Europe), ou il réclame un étiquetage / une identification spécifique.
- Les voies de transport prévues par le client n'ont aucun sens du point de vue géographique ou économique.
- Les biens sont destinés à être stockés dans un entrepôt douanier.

Partage de connaissances et prolifération

L'universalisation des connaissances de la science et de la recherche est souhaitée et elle ne doit pas être empêchée ou contrôlée. La collaboration scientifique peut toutefois être détournée à des fins de prolifération.
À ce sujet, le transfert immatériel de technologie (ITT) est particulièrement problématique. Il peut s'opérer par le biais d'un transfert de savoir-faire dans le cadre de consultations, de conférences, de formations techniques, de programmes d'échanges académiques, de projets communs de recherche et développement ou lors de la transmission d'informations techniques, p. ex. au moyen de courriels, de fax, de sites Internet ou de clouds. Ce type de transfert a considérablement augmenté avec la numérisation, la diffusion et le développement des technologies de l'information et de la communication (TIC) et il représente un défi particulier pour le contrôle des exportations puisqu'il ne peut pas – contrairement à l'exportation de marchandises – être contrôlé aux frontières nationales.

L'un des exemples les plus édifiants de transfert illégal de savoir-faire et de technologie provient du réseau global opéré par l'ingénieur et scientifique nucléaire pakistanais Abdul Qadeer Khan, connu comme étant le « père du programme atomique pakistanais ». Après avoir étudié la métallurgie en Europe de l'Ouest dans les années 1960 et obtenu son doctorat en 1972, Khan a rejoint le Physics Dynamics Research Laboratory aux Pays-Bas afin d'y mener des études sur les métaux à haute résistance pour la construction de centrifugeuses à gaz. Ce laboratoire était un sous-traitant du groupe Urenco, qui gère notamment une usine d'enrichissement d'uranium aux Pays-Bas et produit de l'uranium enrichi pour des centrales nucléaires néerlandaises et étrangères. Chargé de la traduction de documents en néerlandais pour le compte des partenaires allemands et britanniques du consortium Urenco, Khan s'est vu accorder l'accès aux plans des centrifugeuses à gaz. À la suite du premier essai nucléaire indien en 1974, Khan a volontairement mis ses connaissances à disposition des autorités pakistanaises, permettant ainsi la construction d'une usine d'enrichissement d'uranium destinée au programme nucléaire pakistanais. Il a par la suite fourni ses connaissances ainsi que des biens à l'Iran, à la Corée du Nord et à la Libye, leur permettant de mettre sur pied et de développer leurs propres programmes nucléaires.

Les acteurs importants dans le domaine de la prolifération profitent de l'échange libre des informations et peuvent, par le biais du transfert immatériel de technologie, acquérir les connaissances scientifiques et techniques indispensables au développement d'armes de destruction massive et de leurs vecteurs. Ils s'intéressent particulièrement aux domaines spécialisés ayant des applications en matière de développement d'armes de destruction massive et de leurs vecteurs, comme la construction mécanique, l'ingénierie, la métrologie, les sciences naturelles, etc.
Les États préoccupants n'hésitent par ailleurs pas à faire appel à leurs services de renseignement pour se procurer les expertises nécessaires dans les pays fournisseurs par le biais d'officiers de renseignement, d'agents recrutés, ainsi que d'autres méthodes relevant de l'espionnage. Les agissements de ces agents dans les instituts de recherche ou les hautes écoles sont très difficiles à détecter et à combattre.
Pour protéger les informations confidentielles ou pertinentes en matière de prolifération et pour minimiser le risque de perte de réputation et de crédibilité, les entreprises, les hautes écoles et les instituts de recherche doivent avoir conscience du risque lié au ITT, contrôler leurs directives internes et les lignes de conduite qui en découlent et les ajuster en conséquence.

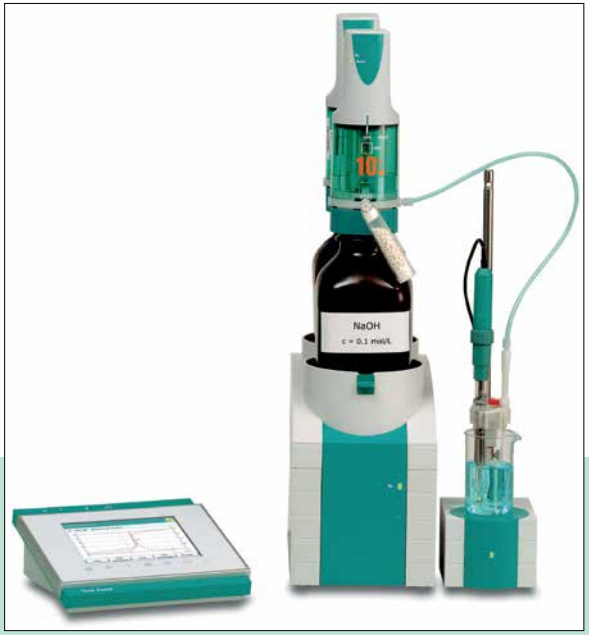
Que font les autorités ?

Les entreprises et instituts scientifiques sont en premier lieu eux-mêmes responsables du respect des prescriptions légales en matière de contrôle des exportations. Le Secrétariat d'État à l'économie (SECO), en tant qu'instance qui autorise les exportations, peut fournir des informations sur les procédures et les produits soumis à autorisation ou à l'obligation de déclarer[1]. D'autres instances fédérales et cantonales, comme l'Administration fédérale des douanes (AFD), le Département fédéral des affaires étrangères (DFAE), le SRC et les services de renseignement cantonaux, sont également impliquées dans l'application de ces dispositions.

La science et l'économie ne sont souvent pas en mesure de reconnaître les intentions réelles de leurs partenaires des pays critiques. Une entreprise ou un institut de recherche peut alors commettre un acte punissable à son insu en transmettant des biens ou des technologies critiques employés dans le cadre d'un programme d'armes de destruction massive. En revanche, elles seules disposent des connaissances nécessaires pour juger si les quantités et les propriétés des biens commandés peuvent correspondre au but indiqué par l'acheteur et dans quelle mesure les biens ou les technologies peuvent être détournés.

À cet effet, le SRC et les services de renseignement cantonaux contactent, conseillent et sensibilisent à ces questions les représentants du monde scientifique, économique et industriel avec discrétion et dans un climat de partenariat.

1 Voir aussi www.seco.admin.ch/fr → Economie extérieure et Coopération économique → Contrôle à l'exportation et sanctions.



À droite :
un instrument d'analyse qui, selon des informations, aurait dû être utilisé au Pakistan dans le cadre du programme d'armes nucléaires (photo privée)

PROLIFÉRATION

Espionnage

Définition

L'espionnage désigne l'acquisition d'informations et de données des domaines de la politique, de l'économie, de l'armée, des sciences et des technologies, tenues volontairement confidentielles ou secrètes, ainsi que la transmission de ces informations et données à des acteurs étrangers (État, groupe, entreprise, individu, etc.) au détriment de la Suisse, de ses entreprises, ses institutions ou de personnes en Suisse.

L'espionnage économique consiste notamment à découvrir un secret commercial ou de fabrication et à le mettre à disposition d'un organisme officiel étranger, d'une organisation étrangère, d'une entreprise privée ou de leurs agents.

La violation du secret de fabrication ou du secret commercial et l'espionnage sont mentionnés dans le Code pénal suisse (art. 162, 271, 272, 273, 274 et 301).

Les entreprises et hautes écoles suisses comme cibles d'espionnage

Place de haute technologie, siège de multinationales et d'organisations internationales, théâtre de négociations internationales et site d'implantation de centres de données importants, la Suisse constitue une cible intéressante pour des acteurs aussi bien étatiques que non étatiques.

Plusieurs raisons peuvent expliquer pourquoi une entreprise en particulier est la cible d'espionnage économique. Elle peut disposer d'un savoir-faire critique et produire des biens de haute technologie soumis aux contrôles des exportations, mais les leaders mondiaux dans des domaines de niche *(hidden champions)* présentent également un intérêt en matière d'espionnage. Les entreprises et hautes écoles investies dans la recherche appliquée ainsi que dans le développement entretenant des contacts avec des États critiques (p. ex. sous la forme de joint-ventures ou d'accords de recherche et de collaboration) sont également exposées à un risque accru d'espionnage.

Si les nouvelles technologies de l'information et de la communication ont permis d'accomplir de nombreux progrès, notamment dans le domaine du stockage et de l'analyse des données, elles sont également vulnérables et leur mise en œuvre imprudente peut constituer un facteur de risque pour les entreprises et les hautes écoles. Le nombre d'attaques de cyberespionnage est en hausse dans le monde entier : chaque entreprise, chaque haute école et chaque organisme de recherche peut devenir une cible.

Certains services de renseignement étrangers ont pour mission explicite l'acquisition de savoir-faire à l'étranger afin de soutenir activement l'économie et les entreprises de leur pays et de combler le retard de développement de leurs technologies. Les actes d'espionnage visant les entreprises et les instituts de recherche suisses ont des conséquences néfastes durables sur la compétitivité économique et technologique de la Suisse.

Recherche légale d'informations

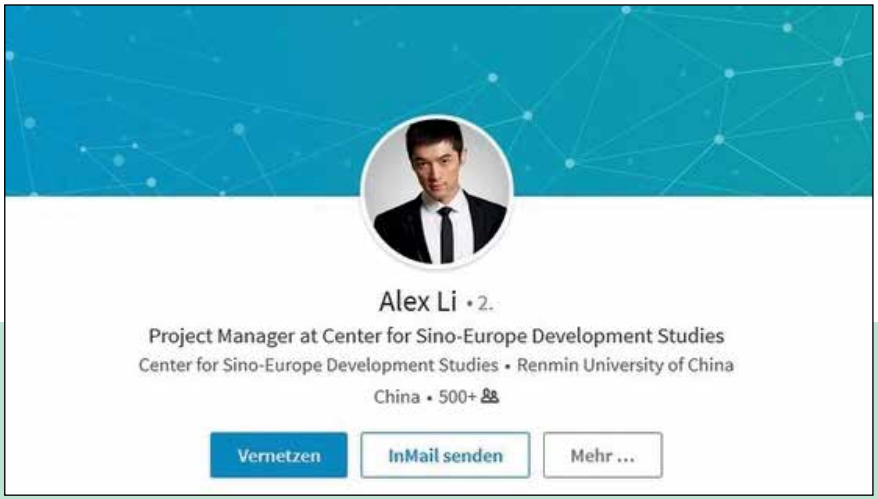
Open Source Intelligence

La recherche d'informations à partir de sources accessibles au public (comme les sites Internet, les brochures produit ou les réseaux sociaux), désignée sous le terme de Open Source Intelligence (OSINT), n'est pas interdite. La collecte d'informations dans le cadre de conférences, de foires ou d'événements diplomatiques compte également parmi les activités routinières de délégués étrangers en Suisse. Toutefois, il faut attirer l'attention sur le fait que ces informations permettent à des services de renseignement étrangers et à des entreprises concurrentes d'évaluer de potentielles cibles d'espionnage (entreprises, organisations, personnes, etc.). Le problème réside d'une part dans le fait qu'une entreprise ou un institut doit présenter ses produits de manière attrayante pour les faire connaître, et d'autre part que trop de détails sur ces produits ne doivent pas être publiés car ils pourraient être mis à profit par la concurrence. Des informations peuvent aussi être acquises par OSINT sur des technologies, sur la situation économique d'une entreprise, les investissements en rapport avec des projets, les activités de recherche et développement, les collaborateurs ainsi que les clients et les futurs contrats à l'occasion d'expositions, de conférences et de projets de recherche internationaux. Le partage d'informations personnelles et professionnelles sur les réseaux sociaux en ligne offre aux services de renseignement étrangers la possibilité de rechercher des personnes ainsi que des profils ciblés et de tenter de recruter des individus.

L'analyse de publications accessibles au public et le partage de résultats de recherches scientifiques permettent d'accéder à un large éventail de connaissances, donnent des indications précieuses sur des projets en cours et permettent de mettre sur pied des actions ciblées contre les responsables. Il incombe aux personnes publiant des informations de décider de leur étendue et des détails qu'elles fournissent sur un projet, un produit, une institution ou une entreprise et ses collaborateurs.

Méthodes d'espionnage

Les services de renseignement étrangers, mais aussi les acteurs privés, se servent de différentes méthodes pour leurs activités d'espionnage. Ils utilisent toujours, dans l'ombre, des moyens traditionnels tels que le renseignement d'origine humaine (Human Intelligence, HUMINT) et l'espionnage électronique par l'écoute de télécommunications (Communications Intelligence, COMINT). HUMINT désigne le recrutement d'informateurs et la collecte de renseignements auprès d'individus. Des moyens électroniques très développés sont employés dans le domaine COMINT, permettant d'espionner toutes sortes de transmissions électroniques, c'est-à-dire de les lire et de les analyser. La numérisation croissante des informations, des données et des processus commerciaux entraîne la création de fichiers de données toujours plus volumineux et plus sensibles. La multiplication des systèmes composés d'appareils et d'objets interconnectés (Internet des objets), souvent peu sécurisés, les rend également vulnérables, ce qui entraîne une recrudescence des actes d'acquisition illégale d'informations et de données sensibles par des moyens relevant du cyberespionnage. Les services de renseignement et les entreprises font aussi appel à des agences privées (détectives, fiduciaires ou bureaux de renseignements, sociétés de conseil ou firmes de restructuration, etc.) et à des pirates informatiques pour accéder à des données et des informations confidentielles.



Communications Intelligence

COMINT permet d'intercepter et d'analyser les communications d'entreprises ou de particuliers transmises via câble, satellite ou ondes radio (p. ex. conversations téléphoniques, courriels, SMS) dans le but d'obtenir des informations utiles quant à leurs objectifs économiques ou stratégiques. Les messages électroniques et les télécopies peuvent systématiquement être explorés à l'aide de mots-clés, et les appels téléphoniques analysés au moyen de systèmes automatiques de reconnaissance vocale.

Human Intelligence

Camouflage

Camouflés par exemple en diplomates, en journalistes, en scientifiques ou entrepreneurs, des officiers de services de renseignement étrangers parviennent en Suisse à accéder aux décideurs dans les domaines de la politique, de l'armée, de l'économie et des sciences. Ils peuvent ainsi collecter des premières informations et contacter des personnes sans se faire suspecter. Ces officiers assistent souvent à des manifestations publiques et y recherchent des personnes pouvant détenir des informations qui les intéressent. Ils recourent notamment à des tactiques d'ingénierie sociale, c'est-à-dire à des tentatives de manipulation ciblées afin d'obtenir des informations spécifiques. Les interprètes et les traducteurs ont souvent accès à des informations confidentielles, tout comme les stagiaires et doctorants. Eux aussi constituent des cibles de choix pour des services de renseignement étrangers.

Lors d'une conférence publique sur la cybersécurité, un officier de renseignement étranger sous couverture diplomatique a approché un spécialiste suisse en informatique. Il s'est ensuit une rencontre au cours de laquelle l'officier de renseignement a abordé avec le spécialiste des questions ayant trait à la cybersécurité en Suisse. Le but de l'officier de renseignement était d'obtenir des informations détaillées et, si possible, confidentielles sur le sujet.

À gauche :
un faux profil sur Linkedin utilisé par un service de renseignement chinois pour contacter des personnes potentiellement intéressantes (Office fédéral allemand de protection de la Constitution)

Plus qu'une simple représentation commerciale diplomatique

Ce sont précisément des membres de représentations commerciales étrangères camouflés en diplomates et actifs dans le renseignement qui essayent d'établir des contacts avec des entreprises du domaine de la haute technologie. Ces personnes invitent leurs cibles à des expositions, des séminaires et des congrès internationaux, mais se présentent aussi spontanément dans les locaux des entreprises et des instituts de recherche. Elles manifestent leur intérêt pour des projets de recherche et des processus opérationnels, sollicitent des offres très détaillées sur le plan du matériel ou demandent à obtenir des manuels à usage interne.

Du contact ouvert au contact sournois

Les officiers de renseignement étrangers mettent progressivement en place une relation de confiance, voire de dépendance avec les personnes cibles. Ils essayent initialement d'obtenir des informations non classifiées et accessibles au public. De petits cadeaux et invitations entretiennent l'amitié – et la personne cible communique de plus en plus d'informations confidentielles. La relation de confiance se développe jusqu'à ce que la personne cible finisse par révéler des informations secrètes. La personne prise ainsi au piège ne peut plus s'en sortir ; en lui rappelant les informations secrètes qu'elle a déjà dévoilées, l'officier de renseignement lui fait subir un chantage.

Chantage

Le fait d'accepter de l'argent compromet et lie la personne cible à l'officier du service de renseignement étranger. Mais des possibilités de chantage peuvent aussi être créées par les services de renseignement eux-mêmes. Dans certains États, par exemple, il est reproché à des personnes cibles d'avoir enfreint la loi. Ces reproches peuvent être fondés ou feints, par exemple dans le cas d'un accident de la route. Le service de renseignement propose alors à la personne cible de l'aider et lui demande des informations ou une collaboration en contrepartie. Des possibilités de chantage peuvent aussi être créées à partir d'activités de surveillance, par exemple par la documentation d'une relation amoureuse, d'une consommation de stupéfiants, d'une infraction à la réglementation sur les devises ou l'acceptation d'argent.

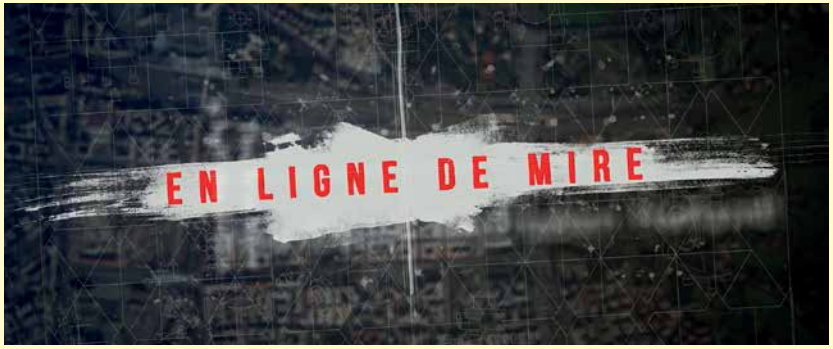
Entreprises et instituts de recherche en ligne de mire

Outre les méthodes mentionnées, d'autres moyens sont couramment employés dans le domaine de l'espionnage économique pour accéder à des informations confidentielles :

- visites de délégations étrangères, accompagnées ou non d'un représentant de l'ambassade ;
- intentions d'investissement en provenance de l'étranger (notamment dans les start-up), participation à des entreprises communes (joint-ventures) ou acquisition d'entreprises à des fins de transfert de technologie et de placement de nouveaux collaborateurs dans des domaines sensibles ;
- collaboration de recherche avec des entreprises à des fins d'appropriation de savoir-faire technique pour la construction et l'exploitation d'une unité de production ;
- coopération scientifique avec des hautes écoles et des instituts de recherche dans le but d'avoir accès à des équipements et des installations de recherche de pointe ;
- attaques contre des clients, des prestataires externes, des consultants ou des fournisseurs d'une entreprise qui constitue la cible réelle ;

- exploitation de points faibles dans l'organisation de l'entreprise, p. ex. lorsque les collaborateurs sont autorisés à raccorder des terminaux mobiles personnels comme des ordinateurs portables, des tablettes ou des smartphones au réseau de l'entreprise ;
- mise en place de restrictions réglementaires ou légales dans d'autres États visant des succursales étrangères afin de les contraindre à stocker leurs données dans le pays d'implantation de la succursale ;
- recrutement d'un employé en qualité d'informateur pour avoir accès à des informations confidentielles, mais aussi recours à d'anciens employés ayant disposé d'accès à des domaines et des informations sensibles et connaissant les processus internes.

Le court-métrage « En ligne de mire » du SRC montre les méthodes des officiers de renseignement étrangers et les moyens qu'ils mettent en œuvre pour se procurer le savoir-faire confidentiel d'une entreprise suisse[1].



1 Disponible sous www.ndb.admin.ch/espionnage-economique.

Auteurs internes

Dans de nombreux cas d'espionnage, les propres collaborateurs de l'entreprise transmettent des informations confidentielles à des personnes non autorisées (concurrents, services de renseignement étrangers), que ce soit volontairement ou sous la contrainte. Les motivations d'un tel acte sont diverses, mais des signes précurseurs sont souvent négligés ou ignorés. Les comportements suivants peuvent suggérer un auteur interne :

- heures d'arrivée inhabituelles sur le lieu de travail ou dans les locaux (p. ex. très tôt le matin ou tard le soir pour être de préférence seul dans le bureau) ;
- nombre d'impressions ou de photocopies de documents d'entreprise supérieur à la moyenne ;
- stockage de données particulièrement volumineuses sur des supports électroniques ;
- sortie non autorisée de documents confidentiels du site de l'entreprise ;
- présence non autorisée d'appareils électroniques dans des zones de travail sensibles ;
- accès à des données de l'entreprise dont le collaborateur n'a pas besoin pour sa fonction ;
- frustration sur le lieu de travail, p. ex. désillusion en raison d'une promotion non obtenue ou autres prétendues offenses, conflits avec la hiérarchie et les collègues de travail ;
- fortune soudaine et inexpliquée ;
- prédisposition au chantage (p. ex. en raison d'une relation extraconjugale, de la consommation de drogues ou d'infractions à la loi) ;

- discrétion insuffisante ;
- goût du risque, imprudence et violation délibérée des consignes de sécurité ;
- contacts personnels avec des représentants d'ambassades étrangères ou des diplomates inconnus de la direction de l'entreprise et non autorisés par celle-ci.

Il convient d'informer immédiatement la personne responsable de la sécurité de l'entreprise lors-qu'un tel comportement est constaté de la part d'un collaborateur.

À quelles menaces les TIC exposent-elles les entreprises et les hautes écoles ?

Cyberespionnage et vol de données

Le Code pénal suisse distingue les délits suivants :

- Art. 143 soustraction de données
- Art. 143bis accès indu à un système informatique
- Art. 144bis détérioration de données
- Art. 147 utilisation frauduleuse d'un ordinateur

Au cours des dernières années, l'utilisation des technologies de l'information et de la communication (TIC) pour accéder à des informations confidentielles a fortement augmenté. Les TIC sont utilisées par des criminels, des concurrents industriels, des États, des terroristes ou des groupes indépendants pour s'introduire dans

des systèmes informatiques et disposer d'un accès aux données sensibles. Le cyberespionnage et le vol de données via Internet permettent à l'agresseur de garder l'anonymat et de réduire les coûts liés à une telle acquisition illégale d'informations. De manière croissante, ces acteurs perpètrent des attaques ciblées en utilisant des logiciels malveillants sophistiqués. Des ressources financières et personnelles importantes sont mobilisées sur une période relativement longue afin d'attaquer des cibles désignées (advanced persistent threat, APT). De telles attaques complexes sont principalement le fait d'acteurs étatiques dont l'objectif est de maintenir une présence incognito et à long terme dans le réseau d'une entreprise ou d'une organisation à des fins d'espionnage ou de sabotage. Ils sont également susceptibles de détourner le réseau pour lancer des cyberopérations contre d'autres cibles. Une cyberattaque criminelle suspectée recourant à un rançongiciel peut en outre servir de couverture à une attaque plus sérieuse : l'attaquant est alors moins intéressé par une rançon que par le vol ou la suppression de données.
Les entreprises et les hautes écoles ne font pas seulement face à des petits délinquants avec des moyens limités, mais se voient confrontées à des menaces et des attaques lancées par des groupes organisés ayant une grande expertise technique. Cette menace n'est toutefois pas perçue à sa juste mesure. Au contraire, pour beaucoup de personnes, il ne s'agirait que d'un phénomène virtuel et par conséquent relativement anodin.

Collecte étendue de données

Des entreprises mandatent souvent des fournisseurs externes en matière de services dans le secteur des TIC. Ce faisant, elles transmettent l'infrastructure TIC de l'entreprise ainsi que les données qu'elle contient à des tiers dont elles ne peuvent pas toujours contrôler suffisamment les activités. Dans le cadre des activités économiques et de recherche, la communication est indispensable. Les communications via les réseaux informatiques et de communication mobile peuvent attirer

l'attention d'États tiers détenant des technologies de collecte étendue de données. Ces pays sont capables d'analyser ces communications et de les exploiter à leur avantage ou au profit d'une entreprise ou d'une organisation concurrente. Les entreprises et les hautes écoles doivent tenir compte du fait que chaque information qui quitte leur réseau informatique peut être collectée, analysée et utilisée d'une manière abusive par un acteur externe. La garantie de la confidentialité est donc un élément fondamental de la sécurité.

Corruption de données

L'accès non autorisé à un système de traitement de données peut aussi avoir comme but la destruction de ces données. Dans la plupart des cas, ces activités sont liées au souhait de bénéficier d'un avantage sur la concurrence ou à une tentative de bloquer une transaction commerciale en cours. Une information est un bien particulièrement sensible et doit être protégée en conséquence. Les mesures de sécurité qui doivent être mises en place pour la protection d'une information dépendent aussi de la valeur de l'information.

Perturbation de réseaux

La non-disponibilité d'un service réseau pour les utilisateurs autorisés pendant une période étendue peut causer un préjudice important à l'entreprise ou la haute école. L'attaque par déni de service distribué (Distributed Denial-of-Service (DDoS) attack) constitue un exemple typique de cette pratique. En envoyant un très grand nombre de requêtes de communication externes, ces attaques cherchent à saturer un ou plusieurs éléments d'une infrastructure ciblée afin d'affecter les performances du réseau et de rendre un service Internet inopérant. Les entreprises qui dépendent partiellement ou complètement d'un accès à Internet nécessitent un fonctionnement quasiment permanent de leur système informatique. Dans l'éventualité d'une attaque du système, l'entreprise pourrait faire face à des pertes de bénéfices et de contrats si son système n'est pas suffisamment protégé.

Comment les entreprises et les hautes écoles peuvent-elles se protéger des fuites d'informations et de données ?

L'exacerbation du contexte concurrentiel international et la dépendance croissante envers les systèmes modernes d'information et de communication entraînent de nouvelles vulnérabilités et des défis inédits pour les entreprises, les hautes écoles et d'autres organismes. Il est de plus en plus important de se protéger contre l'utilisation illégale de ses propres connaissances par des personnes non habilitées. Certaines petites et moyennes entreprises, en raison de leur savoir-faire et de leurs activités innovatrices dans les domaines de la recherche et du développement, constituent des cibles d'espionnage intéressantes. L'interconnexion croissante fait de la sécurité des infrastructures de l'information une priorité. Les interruptions de réseaux de communication ainsi que le vol, la manipulation ou la perte de données peuvent représenter un risque existentiel pour l'économie, la société et l'État.

La sécurité de l'information ne doit pas s'arrêter aux portes de l'entreprise ou à la frontière d'un État. Les entreprises internationales doivent être conscientes que des informations peuvent se perdre au niveau de leurs succursales, des sociétés appartenant à leur groupe ou de partenaires commerciaux à l'étranger. Au cours des dernières années, certains États ont introduit des lois sévères en matière de cybersécurité, contraignant les entreprises étrangères à stocker leurs données sur des serveurs situés dans le pays hôte. Si elles souhaitent transférer leurs données vers l'étranger, ces entreprises sont tenues d'obtenir une autorisation officielle des autorités locales. Certains États exigent en outre que le code source des technologies commercialisées sur leur territoire soit contrôlé par leurs propres instances, exposant les entreprises étrangères à un risque croissant de fuite ou de détournement de données et d'informations pour le compte de tiers.

Mesures préventives

Il est impossible de se prémunir totalement contre la fuite d'informations. Mais des mesures appropriées d'atténuation des risques peuvent offrir une protection efficace et financièrement viable. Les mesures de prévention suivantes peuvent notamment être prises.

Sécurité de l'information

- Élaboration et mise en œuvre d'un concept et désignation d'une personne préposée à la sécurité de l'information, qui, avec le soutien de la direction, effectue des contrôles et fait appliquer les mesures de sécurité qui ont été fixées.
- Réglementation et limitation des droits d'accès des collaborateurs aux données et aux documents.
- Interdiction des téléphones mobiles dans les réunions d'affaires traitant de sujets sensibles, et interdiction des conversations confidentielles par téléphone mobile.
- Directive Clean Desk (« bureau propre ») : lorsqu'ils ne sont pas présents à leur poste de travail, p. ex. à la pause de midi ou en dehors des heures de travail, les collaborateurs sont tenus de mettre l'ensemble des documents sous clé (notamment les informations confidentielles et secrètes). Les ordinateurs doivent toujours être verrouillés, même lors de courtes absences (verrouillage de session).
- Destruction sécurisée de documents confidentiels (p. ex. au moyen d'une déchiqueteuse) et de supports de données comme les clés USB.

- Enquêtes détaillées sur les personnes avant leur engagement (p. ex. extrait du casier judiciaire, contrôle de sécurité relatif aux personnes).
- Formation initiale, formation continue et sensibilisation régulière des collaborateurs à la sécurité de l'information, la sécurité informatique et la menace d'espionnage.
- Contrôles systématiques et centralisés des informations publiées par l'entreprise et ses collaborateurs (sur le site Internet de l'entreprise, sur les réseaux sociaux, dans les brochures produit, etc.).
- Consignes de comportement des collaborateurs lors de foires, conférences, événements et voyages d'affaires.

Externes

- Contrôle des accès et accompagnement systématique des visiteurs et délégations externes, entre autres vérification des données personnelles des membres de la délégation, badges pour visiteurs, garantie d'un accompagnement adéquat de la délégation et sensibilisation des personnes responsables de l'accompagnement ainsi que d'autres employés recevant des visiteurs, définition d'un agenda, interdiction pour les membres de la délégation d'introduire des appareils électroniques, etc.
- Contrôle des fournisseurs, consultants et autres prestataires de services.

Sécurité informatique et sécurité des données

Des informations et des données peuvent finir entre de mauvaises mains à la suite d'actions involontaires lors de la fourniture et l'exploitation de TIC, p. ex. erreurs humaines ou défaillances techniques, ou bien d'actions délibérées et illégales (cyberattaques). Au sein des entreprises, des hautes écoles, mais aussi dans le domaine privé, des solutions techniques comme les pare-feux qui filtrent le trafic de données entrantes et sortantes, des antivirus et des mises à jour régulières des systèmes d'exploitation et des logiciels employés doivent être la règle. Cependant, d'autres mesures sont également nécessaires telles que le cryptage des disques durs (notamment ceux des ordinateurs portables utilisés en dehors de l'entreprise), le blocage de l'ensemble des ports destinés aux supports de stockage externes (clés USB, cartes SD, etc.) sur les ordinateurs de l'entreprise, ainsi qu'une séparation (virtuelle ou physique) du réseau informatique interne et externe.

Les accès personnels aux ordinateurs de bureau, ordinateurs portables et comptes de messagerie doivent recourir à l'authentification à deux facteurs (p. ex. au moyen de jetons d'identification ou de clés USB de sécurité) ou à l'authentification par carte à puce (p. ex. carte PKI). Il est également recommandé d'utiliser des solutions de sécurité pour la transmission de données. Les informations sensibles doivent être cryptées avant de transiter via un réseau externe (p. ex. envoi par courriel), et les données doivent passer par des canaux sécurisés comme des VPN (Virtual Private Network), notamment lorsque des collaborateurs accèdent au réseau de l'entreprise depuis l'extérieur. La prudence est de mise lors de l'utilisation de services cloud pour le stockage de données, en particulier lorsque les serveurs se situent à l'étranger. L'utilisation de courriels constitue souvent la principale vulnérabilité d'une entreprise ou d'une organisation en matière de sécurité contre les cyberattaques. Une utilisation imprudente de cet outil peut ouvrir grand la porte à un adversaire, qui peut alors s'introduire dans le réseau de l'entreprise ou de l'organisation (p. ex. au moyen d'une attaque de harponnage[1] ou spearphishing).

Les entreprises et les hautes écoles ont également besoin d'outils pour détecter les intrusions illégales dans l'infrastructure de leur réseau informatique. Des solutions spécifiques telles que les systèmes de détection d'intrusion (Intrusion Detection Systems, IDS) ou les systèmes de prévention d'intrusion (Intrusion Prevention Systems, IPS) se prêtent à augmenter le niveau de sécurité du réseau informatique. La sécurisation de terminaux sur le réseau ainsi que la surveillance des activités sur ces derniers et l'enregistrement des accès réseau (adresses IP, ports) et fichier permettent la détection et le traitement des incidents. Afin d'empêcher un abus de ressources, des solutions protégeant le réseau contre des attaques externes doivent aussi être mises en œuvre. De telles solutions (anti-DDoS) sont souvent mises à disposition par les fournisseurs d'accès à Internet.

Formation et règles de conduite

Le secteur informatique requiert des directives qui peuvent être appliquées non seulement pendant les heures de travail, mais aussi dans la vie privée. Ces directives sur l'utilisation des ressources informatiques au travail doivent fixer le positionnement de l'entreprise ou de l'institut de recherche par rapport à l'utilisation d'Internet, des programmes de courriel privés et des réseaux sociaux par ses employés. L'entreprise ou l'organisme de recherche doit en outre organiser des sessions de formation initiale et continue régulières destinées à tous les collaborateurs et traitant des risques liés à l'utilisation des TIC.

1 Méthode d'hameçonnage (phishing) visant des personnes ou des groupes en particulier au sein d'une entreprise ou d'une organisation. Contrairement aux courriels d'hameçonnage envoyés en masse, un courriel ou un SMS de harponnage est adapté à la personne ciblée et à ses intérêts. Celle-ci est invitée à divulguer des informations personnelles (p. ex. identifiants de connexion et mots de passe) ou à ouvrir une pièce jointe / à cliquer sur un lien contenant un logiciel malveillant qui infecte alors le réseau de l'entreprise via son ordinateur.

Sélection des partenaires et des solutions informatiques

Les PME en particulier ne disposent souvent pas de ressources humaines et financières suffisantes pour garantir la sécurité de leurs réseaux informatiques. Il est donc recommandé de recourir à des prestataires externes. Divers facteurs doivent cependant être pris en compte lors du choix d'un partenaire informatique. Incontestablement, les compétences techniques d'un prestataire ainsi que la qualité de ses services jouent un rôle fondamental. Il faut néanmoins être conscient du fait que le fournisseur pourrait être soumis à d'autres conditions juridiques et politiques ou qu'il pourrait participer à des programmes étatiques de collecte de données. Il est important de tenir compte de ces facteurs afin d'empêcher une fuite de données ou une atteinte au réseau informatique.

Assistance / soutien

L'Office fédéral pour l'approvisionnement économique du pays a défini une norme minimale pour les TIC, qui fournit des consignes concrètes afin d'améliorer la résilience informatique[1]. Ces dernières s'adressent en particulier aux exploitants d'infrastructures critiques, mais sont applicables à toutes les entreprises et organisations. L'autoévaluation ainsi qu'un outil d'évaluation permettent d'estimer l'avancée de la mise en œuvre des mesures recommandées.

ICTswitzerland a spécialement développé un test rapide en ligne[2] permettant aux PME d'évaluer leur niveau de cybersécurité et de contrôler si elles remplissent bien les exigences minimales pour leur type de structure.

1 Disponible sous www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html
2 Disponible en allemand et en anglais sous www.cybersecurity-check.ch

Sécurité lors de voyages d'affaires à l'étranger

Le risque d'être victime d'actes d'espionnage augmente sensiblement lors de voyages à l'étranger. Un service de renseignement étranger ou un concurrent est susceptible de prendre un collaborateur pour cible du fait de son activité, de son savoir-faire ou encore des informations et des données qu'il emporte avec lui. Les appareils électroniques comme les ordinateurs portables, les smartphones, les tablettes ainsi que les supports de données comme les clés USB constituent un matériel sensible permettant à des acteurs mal intentionnés d'obtenir des informations incognito. Certains États surveillent le trafic Internet, les télécommunications et le courrier postal. Ils fouillent les bagages et manipulent les appareils électroniques et les supports de données des voyageurs. Parfois, ils sont en outre prêts à créer des situations compromettantes, à simuler des accidents de la circulation ou à empêcher la sortie de leur territoire afin de contraindre la personne ciblée à leur remettre des informations confidentielles, voire de la recruter au rang de leurs informateurs. Les autorités locales récoltent également des informations avant même l'arrivée de la personne, par exemple via des recherches sur les réseaux sociaux. Une demande de visa permet à un service de renseignement étranger de déterminer si elle constitue une cible intéressante, en particulier ses réponses aux questions sur son activité professionnelle, qui révèlent de nombreux détails.

Scénarios possibles

- Lors du passage d'une frontière, un douanier demande au voyageur de lui remettre temporairement ses appareils électroniques. Le voyageur ne sait pas ce que le douanier en a fait. Les données privées et professionnelles des voyageurs peuvent aussi susciter l'intérêt d'organes étatiques étrangers.

- Un collaborateur de l'entreprise se trouve à l'étranger et doit transmettre des données sensibles via son téléphone portable. Le signal téléphonique est crypté, mais seulement sur la partie transitant par les ondes radio et avec une technologie bon marché. Il est donc possible de décrypter le signal et d'intercepter la conversation, car le signal n'est plus sécurisé dès qu'il passe du réseau radio au réseau fixe.
- Une représentante de l'entreprise a besoin d'une information et se connecte à Internet depuis l'étranger : sa communication peut être interceptée en une multitude de lieux (hôtel, aéroport, gare, café, etc.).
- Lors d'un voyage d'affaires, le responsable de recherche décide d'aller faire un tour en ville. Il laisse ses appareils électroniques dans sa chambre d'hôtel. Sa chambre d'hôtel (y compris le coffre-fort de la chambre) pourrait être fouillée par des tiers afin d'accéder à des données intéressantes.
- Lors d'une conférence les participants quittent la salle pour la pause-café en laissant leur ordinateur portable ouvert sur la table. Il est possible qu'une personne se tienne prête avec une clé USB afin de copier les données enregistrées sur leur ordinateur ou d'y charger un logiciel malveillant.
- Un représentant de l'entreprise reste en contact avec un collaborateur de l'entreprise étrangère après un rendez-vous d'affaires. Ce collaborateur lui offre un cadeau de valeur ou l'invite à visiter son pays au titre de voyage privé en prenant en charge les coûts. Il est alors susceptible d'attendre une contrepartie, p. ex. sous la forme d'informations commerciales sensibles.

Mesures de sécurité personnelles

- Lors de voyages à l'étranger n'emmenez avec vous que les appareils électroniques dont vous avez absolument besoin et qui ne contiennent pas d'informations sensibles. Il est conseillé d'utiliser des ordinateurs portables et téléphones mobiles destinés exclusivement aux voyages d'affaires et configurés de manière à pouvoir être réinitialisés sans grand effort après votre retour. Même si vous les conservez sur vous en permanence, les appareils restent vulnérables.
- Assurez-vous que les systèmes d'exploitation ainsi que les applications installées sur vos appareils électroniques sont toujours à jour. Recourez à des mots de passe forts et à usage unique (caractères alphanumériques, minuscules et majuscules, caractères spéciaux) ne contenant aucune information personnelle comme une date de naissance. Il est recommandé d'utiliser des mots de passe comprenant au moins 12 caractères, composés par exemple des premières lettres de plusieurs mots (le mot de passe MDpsctlmà7h! signifie p. ex. **M**onsieur **D**upont **p**romène **s**on **c**hien **t**ous **l**es **m**atins **à 7 h**eures**!**).
- Il est conseillé de crypter le disque dur de votre ordinateur, plus précisément les données qui y sont enregistrées. Étant donné que certains pays interdisent aux voyageurs d'entrer sur leur territoire en possession de données cryptées, emportez un ordinateur qui ne contient aucune donnée sensible. Une fois arrivé à l'étranger vous pouvez télécharger les données via une connexion sécurisée (réseau privé virtuel, VPN) et les supprimer complètement à l'aide d'un logiciel approprié quand vous n'en avez plus besoin.

- Ne remettez vos appareils électroniques à un fonctionnaire (par exemple lors du passage d'une frontière) que si vous êtes en mesure de les suivre physiquement. Ainsi vous savez ce qui se passe avec vos appareils. Si vous n'êtes pas en mesure d'observer vos appareils, partez du principe qu'ils ont été manipulés.
- Ne laissez jamais vos affaires sans surveillance (par exemple pendant une pause-café lors d'une conférence ou même pour aller aux toilettes).
- N'utilisez pas d'appareils périphériques externes qui vous ont été prêtés ou offerts (clés USB, disques durs externes, téléphones portables, appareils photo numériques, etc.) et ne laissez personne brancher un périphérique externe sur votre ordinateur (par exemple pour utiliser votre ordinateur pour une présentation ou pour charger le téléphone portable de quelqu'un d'autre). Au cas où vous auriez branché un périphérique à un ordinateur inconnu, il est conseillé de le formater avant de l'utiliser à nouveau.
- Les accès Internet via des connexions WiFi publiques – y compris ceux protégés par un mot de passe – proposés notamment dans les hôtels, les cafés ou les aéroports ne sont généralement pas cryptés et donc pas sécurisés. Ne les utilisez que par l'intermédiaire d'un VPN ou, si les VPN sont bloqués dans le pays hôte, accédez à Internet via une connexion 3G/4G/5G en mode itinérance (roaming). Assurez-vous que les échanges entre votre navigateur Internet et l'adresse Internet sélectionnée soit cryptés (https://...).
- Désactivez les interfaces sans fil comme le WiFi et le Bluetooth ainsi que les services de localisation lorsque vous n'utilisez pas l'appareil.

- Si vous ne pouvez pas emmener votre téléphone portable à une réunion de travail ou dans un bâtiment, coupez-le et conservez-le dans un emballage sécurisé (sachet ou boîte de sécurité).
- Faites preuve de prudence vis-à-vis des informations personnelles que vous divulguez sur les réseaux sociaux ou les réseaux professionnels en ligne.
- La prudence est de mise lorsqu'une personne inconnue qui n'a rien à voir avec votre voyage d'affaires tente de prendre contact avec vous.
- Avant votre départ, prenez connaissance des lois en vigueur ainsi que des coutumes culturelles du pays cible.
- Restez attentif et prenez garde aux inconnus qui pourraient regarder votre écran par-dessus votre épaule, par exemple dans le train, dans l'avion ou lors d'une conférence.

Après votre retour

- Changez tous les mots de passe que vous avez utilisés lors de votre voyage à l'étranger.
- En cas de soupçon, faites contrôler et réinitialiser au besoin vos appareils électroniques par le service informatique de votre entreprise ou par un prestataire informatique privé.
- Signalez les événements suspects à votre service de sécurité et au SRC.

Contact

Comment le SRC peut-il vous prêter assistance ?

En collaboration avec les services de renseignement cantonaux, le SRC informe, sensibilise et conseille les entreprises, hautes écoles et instituts de recherche suisses et liechtensteinois en matière de prolifération et d'espionnage.

- www.ndb.admin.ch
- prophylax@ndb.admin.ch

Sensibilisation à l'espionnage économique

www.ndb.admin.ch/espionnage-economique

- Court-métrage sur l'espionnage économique « En ligne de mire »
- Explications relatives aux méthodes d'espionnage présentées dans le film et aux mesures de protection correspondantes
- Aide-mémoires et fiches d'information sur les thèmes de la prolifération et de l'espionnage
- Brochure Prophylax

Procédure en cas de soupçon

En cas de soupçon d'espionnage ou d'activités de prolifération (p. ex. demandes ou commandes douteuses), n'hésitez pas à prendre contact avec le SRC ou avec votre police cantonale. Conservez les preuves potentielles et ne supprimez pas les courriels suspects. Le SRC récoltera et analysera les indices. Il garantit un traitement discret de l'affaire.

Informations complémentaires

Secrétariat d'État à l'économie

www.seco.admin.ch/fr

→ Économie extérieure et Coopération économique → Contrôles à l'exportation et sanctions

- Elic (e-licensing) : système électronique d'autorisation pour la saisie et le traitement de demandes soumises au contrôle des exportations (biens à double usage, matériel de guerre et biens militaires spécifiques). Consultable également sous www.elic.admin.ch.
- Sanctions/embargos : recherche de personnes, d'entreprises et d'organisations faisant l'objet de sanctions (base de données SESAM)
- Produits industriels (dual-use) et biens militaires spécifiques (Licensing) ;
  - Aide-mémoire pour le contrôle interne du respect des prescriptions en matière de contrôle à l'exportation (programme interne de conformité, PIC / Internal Compliance Program, ICP)

Département fédérale des affaires étrangères

www.dfae.admin.ch

→ Représentations et conseils aux voyageurs

Évaluation des propres mesures de sécurité informatique

Centrale d'enregistrement et d'analyse pour la sûreté de l'information

www.melani.admin.ch
www.antiphishing.ch (signalement de courriels d'hameçonnage)

Office fédéral pour l'approvisionnement économique du pays

www.ofae.admin.ch
→ Thèmes → Norme minimale pour les TIC
Norme minimale pour les TIC afin d'améliorer la résilience informatique des exploitants d'infrastructures, d'entreprises et d'organisations critiques (y compris outil d'évaluation)

ICT Switzerland

www.cybersecurity-check.ch
Test rapide en ligne de cybersécurité des PME (disponible en allemand et en anglais)

Rédaction
Service de renseignement de la Confédération SRC

Clôture de la rédaction
Février 2019

PROPHYLAX
Service de renseignement de la Confédération SRC
Papiermühlestrasse 20
CH-3003 Berne
www.src.admin.ch