Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Service de renseignement de la Confédération SRC

PROPHYLAX

Cette brochure fait partie de
l'action de prévention et de sensibilisation
du Service de renseignement de la Confédération SRC

Table des matières

1. 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, de biens d'équipement, matériaux et technologies nécessaires à leur fabrication (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.

Contrôle des exportations; bases légales

- 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
- Ordonnance sur le contrôle des produits chimiques DFE (OCPCh-DFE); RS 946.202.211
- 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 (OExpl); RS 941.41
- Loi sur les embargos (LEmb); RS 946.231
- 18 Ordonnances aux termes de la Loi sur les embargos

Pays à risques

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. Ces pays représentent un danger pour la stabilité régionale et internationale et ils font partie des pays définis comme « pays à risques », une catégorisation qui n'est pas seulement d'ordre technique, mais aussi politique. Aujourd'hui, sont généralement considérés comme pays à risques l'Iran, la Corée du Nord, le Pakistan et la Syrie. En outre, certains pays sont utilisés comme zones de transit pour des affaires importantes en matière de prolifération. Une attention particulière doit aussi être accordée aux transactions commerciales d'autres États

supposés avoir des ambitions dans le domaine de la prolifération, par exemple le Myanmar ou le Soudan.

Les divers pays à risques présentent des différences en ce qui concerne l'avance de leurs programmes de recherches et de développement d'armes de destruction massive et de leurs vecteurs. Du point de vue de la technique 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. Par ailleurs, ils aspirent à atteindre le plus d'indépendance possible au niveau de leur armement.

Les pays à risques essayent de se procurer les procédés, les biens et les technologies nécessaires à leurs propres infrastructures de développement et de fabrication. Confrontés aux mesures internationales de contrôle, ils en taisent ou en dissimulent l'utilisation finale.

Conséquences de la prolifération

La lutte contre la prolifération est l'affaire de toute la communauté internationale. A cet effet, des régimes de contrôle des exportations existent sur le plan international. En ce qui concerne les armes chimiques et biologiques, des conventions internationales juridiquement contraignantes visent en outre à bannir ces armes dans le monde entier. La Suisse est membre de tous ces régimes et conventions. La politique suisse en matière de contrôle d'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

L'installation iranienne d'enrichissement d'uranium à Natanz [GEOEYE-1 Prise de vue du 1er septembre 2009]

en particulier pour une non-dissémination d'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.

Les activités de prolifération en Suisse peuvent violer le droit national ou contrevenir aux engagements internationaux, ainsi que 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 recherches 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.

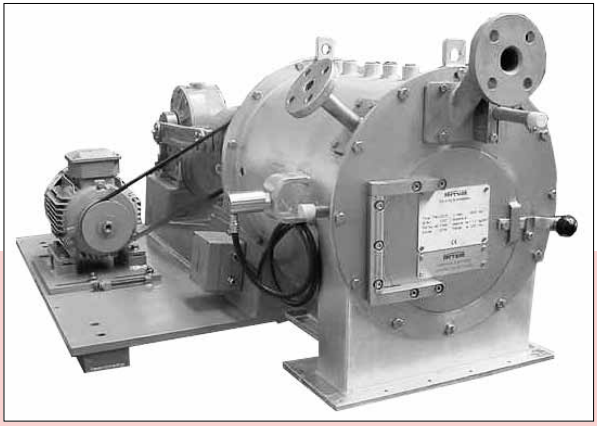
Efforts d'acquisition

Les armes de destruction massive ne sont pas disponibles sur le marché libre et les mesures de la communauté internationale sont destinées à faire échec aux efforts d'acquisition des pays à risques. Pour contourner ces obstacles, les acteurs importants dans le domaine de la prolifération utilisent différentes méthodes et des réseaux d'acquisition clandestins:

- ils utilisent les services de renseignement; leurs agents se présentent aux fournisseurs comme commanditaires ou comme acheteurs;
- des entreprises d'État, en partie ou totalement contrôlées par les services de renseignement, se présentent comme des entreprises conventionnelles pour tromper les fournisseurs;
- les utilisateurs finaux se dissimulent derrière des noms anodins d'entreprises ou derrière une université;
- des titres de projets neutres ou trompeurs sont utilisés;

- les acteurs importants dans le domaine de la prolifération créent une petite firme dans le but de camoufler une transaction et la ferment dès que l'affaire est liquidée; de telles firmes ont notamment été repérées dans des pays de transit;
- ils profitent de l'inexpérience de certains fournisseurs dans le domaine des exportations;
- ils utilisent abusivement des entreprises dans le pays producteur ou le pays fournisseur pour dissimuler les acquisitions illégales derrière des affaires légales;
- ils répartissent les acquisitions en une série de petites commandes, rendant ainsi difficile d'en détecter l'importance au niveau de la 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;
- ils présentent des documents d'exportation falsifiés ou des certificats d'utilisateurs qui ne correspondent pas à la vérité.

A cause de ces méthodes, les fournisseurs ont de la difficulté à déterminer à quelle utilisation finale leurs produits sont destinés. Sont particulièrement problématiques les biens à double usage (dual-use), qui peuvent être utilisés à la fois dans le domaine civil et militaire.



La centrifugeuse qui, selon des informations, aurait du être utilisée en Syrie pour la production d'oxydants pour carburants de fusées [Photo privée]

Comment reconnaître des affaires illégales ?

Une simple commande ne permet pas toujours de juger si un produit est destiné ou non au développement d'armes de destruction massive. Il s'agit donc d'examiner avec soin les modalités de la commande, du transport et du paiement de la marchandise. Cela exige une recherche d'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 être des indices pour une affaire en rapport avec la prolifération:

- la destination finale de la marchandise se révèle imprécise ou n'est pas plausible;
- l'acheteur ne peut pas indiquer pour quoi le produit sera employé ou l'utilisation qui en est prévue s'écarte considérablement de la finalité du produit indiquée par le fournisseur;
- l'acheteur refuse de communiquer l'usage final du produit;
- l'acheteur fait normalement du commerce avec des fournitures militaires et tente peut-être même de le dissimuler;
- l'acheteur ne dispose pas des connaissances techniques nécessaires;
- l'identité d'un nouveau client ne peut pas être clairement déterminée;
- des intermédiaires se manifestent sans motif apparent;
- l'acheteur souhaite un étiquetage spécial, une inscription ou une désignation particulière de la marchandise;

- les biens sont destinés à être stockés dans un entrepôt douanier;
- les conditions de paiement proposées sont particulièrement avantageuses (paiement comptant ou acomptes très importants, provisions très élevées);
- l'acheteur renonce à l'instruction technique, à la garantie et au service après-vente;
- les voies de transport prévues ne sont pas plausibles;
- des collaborateurs de l'entreprise acheteuse sont envoyés en Suisse pour être formés chez le fabricant alors qu'une formation sur place serait plus pratique et plus judicieuse;
- les membres d'une délégation ne sont pas présentés par leurs noms;
- d'autres contacts commerciaux en Suisse sont dissimulés.

Transfert 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. Il en va tout autrement lorsqu'on en abuse à des fins de prolifération.

A ce sujet, le transfert immatériel de technologie (Intangible Transfer of Technology, ITT) est particulièrement problématique. Il peut s'opérer par le biais d'un transfert de savoir-faire dans le cadre de consultations ou de formations techniques ou lors de la transmission d'informations techniques sous une forme immatérielle, par exemple par l'intermédiaire de messages électroniques, télécopies ou sites web. Ce type de transfert a considérablement augmenté avec l'extension d'Internet et il représente un défi particulier pour le contrôle des exportations puisque il ne peut pas – comme l'exportation de marchandises – être contrôlé à la frontière nationale.

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 technologies, acquérir les connaissances scientifiques et techniques indispensables au développement d'armes de destruction massive et de leurs vecteurs.

Par ailleurs, les pays à risques n'hésitent pas à employer leurs services de renseignement et leurs services secrets en engageant leurs propres agents ou des agents recrutés ou en utilisant d'autres méthodes relevant de l'espionnage pour essayer de se procurer les expertises nécessaires dans les pays fournisseurs (voir 2. Espionnage économique).

Les agissements de ces agents dans les instituts de recherches ou les hautes écoles sont très difficiles à détecter et à combattre. Pour protéger les informations confidentielles ou intéressant la prolifération et pour minimiser le risque de perte de réputation et de crédibilité, les instances concernées doivent avoir conscience du problème et adapter les mesures de protection interne.

Que font les autorités ?

Ce sont les entreprises et institutions scientifiques qui sont en premier lieu 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 informer sur les procédures et les produits soumis au régime du permis ou à l'obligation de déclarer (voir aussi www.seco.admin.ch, Politique économique extérieure, Contrôles à l'exportation). D'autres instances fédérales, comme la Direction générale des douanes (DGD), les services fédéraux de protection de l'État (SRC) et ceux des cantons, ainsi que le Département fédéral des affaires étrangères (DFAE), sont également impliquées dans l'exécution de ces prescriptions.

La science et l'économie ne sont souvent pas en mesure de reconnaître les intentions feintes de leurs partenaires des pays à risques. Des actions punissables, par exemple des exportations interdites ou des activités de renseignement prohibé, peuvent ainsi être commises involontairement. En revanche, elles seules disposent des connaissances nécessaires pour juger si les quantités et les biens commandés correspondent au but indiqué par l'acheteur.

A cet effet, le SRC contacte, conseille et sensibilise à ces questions les représentants de la science, de l'économie et de l'industrie avec discrétion et dans un climat de partenariat.

2. Espionnage économique

Définition

Par espionnage, on entend l'ensemble des actions en faveur d'un État, d'une entreprise ou d'une personne dans le but de rechercher des informations protégées ou secrètes dans les domaines militaire, politique, économique, scientifique et technologique au préjudice d'un pays, d'une entreprise ou d'une personne. La violation du secret de fabrication ou du secret commercial ou le service de renseignement prohibé sont mentionnés dans le Code pénal suisse (art. 162, 271, 272, 273, 274 et 301 CP).

Recherche légale d'informations

OSINT

La recherche d'informations à partir de sources accessibles au public, désignée sous le terme de Open Source Intelligence (OSINT), n'est pas interdite. 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. 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 des entreprises, les investissements en rapport avec des projets, les activités de recherche et développement, les clients, les futurs contrats et sur des personnes à l'occasion d'expositions, de conférences et de projets de recherche internationaux.

La mise en valeur et l'analyse de publications accessibles au public et l'échange 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.

Ce sont les personnes qui publient des informations qui décident de leur étendue et des détails quelles veulent donner sur un projet, un produit, une institution ou une entreprise, ses collaboratrices 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), le renseignement fondé sur l'interception de transmissions (Signal Intelligence, SIGINT) et l'espionnage électronique par l'écoute de télécommunications (Communication Intelligence, COMINT). HUMINT désigne le recrutement d'informateurs et la collecte de renseignement auprès d'individus alors que dans le cas de SIGINT et COMINT, ce sont des moyens électroniques très développés qui sont employés: l'intrusion dans les réseaux TI, l'utilisation de téléphones portables comme dispositifs d'écoute et les recherches sur Internet font partie des méthodes modernes d'espionnage. Les services de renseignement et les entreprises font aussi appel à des agences privées (détectives, fiduciaires ou bureaux de renseignement, sociétés de conseil ou firmes de restructuration, etc.) et à des pirates informatiques pour accéder à des données et des informations confidentielles.

HUMINT

Camouflage

Camouflés en diplomates, journalistes ou hommes d'affaires, des officiers de services de renseignement étrangers parviennent en Suisse à accéder aux décideurs dans les domaines de la politique et de l'économie. 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. Les interprètes et les traducteurs peuvent également avoir accès à des informations confidentielles et

des stagiaires et doctorants peuvent collecter de précieuses informations pour des services de renseignement étrangers.

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 qui travaillent dans le domaine de la haute technologie. Ces personnes les invitent à prendre part à des expositions, des séminaires et des congrès internationaux. Ils montrent de l'intérêt pour ce qui se passe au sein de l'entreprise, demandent des offres très détaillées pour du matériel ou se renseignent sur des manuels à usage interne.

Du contact ouvert au contact à des fins d'espionnage

Les officiers de renseignement étrangers mettent progressivement en place une relation de confiance et éventuellement même de dépendance avec les personnes cibles. Au début, ils essayent 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 qu'elle dévoile finalement des informations secrètes. La personne cible prise ainsi au piège ne peut plus s'en sortir; en lui rappelant les informations secrètes qu'elle a déjà dévoilées, la personne est soumise à une pression qui peut aller jusqu'au 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, de relations extra-conjugales, d'une infraction à la réglementation sur les devises ou l'acceptation d'argent.

Entreprises visées

A côté des méthodes mentionnées, d'autres moyens sont également habituels dans le domaine de l'espionnage économique:

- visites de délégations étrangères auprès des entreprises, accompagnées ou non d'un représentant de l'ambassade;
- offres de service à des instituts de recherches, des universités ou des entreprises d'armement;
- participations à des entreprises (joint ventures) et à des projets de recherches communs;
- acquisition de technologie et achat de sociétés dans le but de placer de nouveaux collaborateurs dans des domaines sensibles;
- recherche de renseignements auprès d'anciens employés ayant eu accès à des informations confidentielles.

SIGINT

Avec le SIGINT, des transmissions électroniques et de télécommunications (appels à partir de téléphones (portables), télécopies, messages électroniques, etc.) d'entreprises et de particuliers sont interceptées, écoutées, analysées ou manipulées pour accéder à des informations utiles sur des buts économiques ou stratégiques. Les messages électroniques et les télécopies peuvent systématiquement être fouillés à l'aide de mots-clés et les appels téléphoniques décryptés avec des systèmes automatiques de reconnaissance vocale.

Conclusions et contre-mesures

Compte tenu de la situation de concurrence qui s'accentue de plus en plus au niveau international et de la dépendance par rapport à des systèmes modernes d'information et de communication de plus en plus marquée, il est primordial de protéger son savoir de toute utilisation illégale. De petites et moyennes entreprises, en raison de leur savoir-faire et de leurs activités innovatrices dans les domaines de la recherche et du développement, sont souvent la cible d'actes d'espionnage. La multiplication des réseaux de communication 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.

Il n'existe aucune protection globale contre la fuite d'informations. Mais des mesures appropriées peuvent offrir une protection efficace et financièrement supportable dans ce domaine. Les mesures de prévention suivantes peuvent notamment être prises:

- élaboration 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;
- formation initiale et continue et sensibilisation des collaboratrices et des collaborateurs concernant les risques d'espionnage;
- contrôles d'accès;
- protection des documents sur papier et des données informatiques;
- définition des droits d'accès aux données et aux dossiers sensibles;
- enquêtes détaillées sur les personnes avant leur engagement;
- contrôle des informations que l'entreprise ou l'institution publie par exemple sur Internet;
- comportement correct et irréprochable des collaboratrices et des collaborateurs lors de voyages à l'étranger;
- application stricte des mesures de sécurité dans le domaine des technologies de l'information et de la communication.

Le SRC, en collaboration avec les organismes cantonaux de protection de l'État, aide à informer, à sensibiliser et à conseiller les entreprises et les hautes écoles sur les questions ayant trait à l'espionnage économique.

Sécurité dans le domaine des technologies de l'information et de la communication (TIC)

A l'ère des réseaux d'information planétaires, la cybercriminalité se développe de manière exponentielle. Ce danger n'est pas perçu à sa juste mesure. Au contraire, pour beaucoup de personnes, il ne semble être qu'un phénomène virtuel et par conséquent relativement anodin. Cette perception fait obstacle à la prévention.

Le Code pénal suisse différencie 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.

Aujourd'hui, à quels dangers les entreprises et les hautes écoles se voient-elles confrontées ?

Espionnage et vol de données

Des criminels, certains concurrents et quelques États utilisent les technologies de l'information et de la communication (TIC) pour se procurer des informations auxquelles ils ne peuvent pas accéder par des moyens normaux. Le marché noir des programmes malveillants [maliciels tels que chevaux de Troie, enregistreurs de frappe (keylogger), analyseurs de réseau, etc.] est accessible à tous. L'offre de plus en plus importante pour les adeptes de ce genre de commerce a fait baisser

les prix. Aujourd'hui, le fait que ces maliciels puissent être utilisés pratiquement par toutes les personnes disposant de matériel informatique joue également un rôle important: ces programmes sont faciles à mettre en place et ils sont aussi commercialisés par des particuliers.

Des attaques de systèmes informatiques peuvent être perpétrées de l'extérieur (par des courriels ou des sites web infectés, par des interfaces et des ports externes) ou de l'intérieur (vols de données par des employés).

Détérioration de données

L'accès indu à un système informatique peut aussi avoir pour but de détruire des informations. La raison de telles actions est souvent l'intention de dépasser un concurrent ou de vouloir bloquer une négociation. Les entreprises et les hautes écoles doivent prendre conscience que les informations sont un bien qu'elles doivent protéger. Leur valeur définit les mesures de sécurité qui doivent être prises.

Utilisation abusive de ressources

Sur le marché noir, les moyens informatiques ont une valeur d'échange déterminée. Lorsque le service informatique d'un ordinateur ou d'autres détails techniques, par exemple la fréquence de la bande passante d'une connexion au réseau, sont connus de personnes aux intentions frauduleuses, ils peuvent devenir une arme dangereuse. Des attaques de déni de service distribué (Distributed-Denial-of-Service, DDoS) peuvent être lancées à partir du réseau infecté d'une entreprise ou d'une haute école. Il est donc primordial que les entreprises et les hautes écoles protègent leurs ressources de tout abus.

Par quelles mesures les entreprises et les hautes écoles peuvent-elles éviter de telles attaques ?

Protection technologique des données

Des solutions techniques telles que des pare-feu, des programmes anti-virus et des mises à jour régulières doivent être la règle dans chaque entreprise et haute école. Mais d'autres mesures sont également nécessaires: codage du disque dur des ordinateurs portables (surtout s'ils sont utilisés à l'extérieur de l'entreprise), blocage sur les ordinateurs de l'entreprise de la connexion à des ports externes, séparation (virtuelle ou physique) du réseau interne et externe.

Règles de comportement et formation du personnel

L'utilisation des moyens de travail informatiques par les employés doit faire l'objet d'une réglementation. Ces directives ne doivent pas seulement être valables pendant le travail, mais aussi dans la vie privée. Dans les directives internes pour l'utilisation des moyens informatiques, l'entreprise ou la haute école doivent aussi fixer des règles pour l'utilisation d'Internet, de la messagerie à des fins privées ou les recherches professionnelles ou privées sur Internet. Les employés doivent être formés et suivre des cours de perfectionnement sur les risques et les dangers des nouvelles technologies.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Service de renseignement de la Confédération SRC

Sensibilisation des entreprises et des hautes écoles

Sécurité dans le domaine des technologies de l'information et de la communication (TIC)

A l'ère des réseaux d'information planétaires, la cybercriminalité se développe de manière exponentielle. Ce danger n'est pas perçu à sa juste mesure. Au contraire, pour beaucoup de personnes, il ne semble être qu'un phénomène virtuel et par conséquent relativement anodin. Cette perception fait obstacle à la prévention.

Le Code pénal suisse différencie 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.

Aujourd'hui, à quels dangers les entreprises et les hautes écoles se voient-elles confrontées ?

Espionnage et vol de données

Des criminels, certains concurrents et quelques États utilisent les technologies de l'information et de la communication (TIC) pour se procurer des informations auxquelles ils ne peuvent pas accéder par des moyens normaux. Le marché noir des programmes malveillants [maliciels tels que chevaux de Troie, enregistreurs de frappe (keylogger), analyseurs de réseau, etc.] est accessible à tous. L'offre de plus en plus importante pour les adeptes de ce genre de commerce a fait baisser les prix. Aujourd'hui, le fait que ces maliciels puissent être utilisés pratiquement par toutes les personnes disposant de matériel informatique joue également un rôle important: ces programmes sont faciles à mettre en place et ils sont aussi commercialisés par des particuliers.

Des attaques de systèmes informatiques peuvent être perpétrées de l'extérieur (par des courriels ou des sites web infectés, par des interfaces et des ports externes) ou de l'intérieur (vols de données par des employés).

Détérioration de données

L'accès indu à un système informatique peut aussi avoir pour but de détruire des informations. La raison de telles actions est souvent l'intention de dépasser un concurrent ou de vouloir bloquer une négociation. Les entreprises et les hautes écoles doivent prendre conscience que les informations sont un bien qu'elles doivent protéger. Leur valeur définit les mesures de sécurité qui doivent être prises.

Utilisation abusive de ressources

Sur le marché noir, les moyens informatiques ont une valeur d'échange déterminée. Lorsque le service informatique d'un ordinateur ou d'autres détails techniques, par exemple la fréquence de la bande passante d'une connexion au réseau, sont connus de personnes aux intentions frauduleuses, ils peuvent devenir une arme dangereuse. Des attaques de déni de service distribué (Distributed-Denial-of-Service, DDoS) peuvent être lancées à partir du réseau infecté d'une entreprise ou d'une haute école. Il est donc primordial que les entreprises et les hautes écoles protègent leurs ressources de tout abus.

Par quelles mesures les entreprises et les hautes écoles peuvent-elles éviter de telles attaques ?

Protection technologique des données

Des solutions techniques telles que des pare-feu, des programmes anti-virus et des mises à jour régulières doivent être la règle dans chaque entreprise et haute école. Mais d'autres mesures sont également nécessaires: codage du disque dur des ordinateurs portables (surtout s'ils sont utilisés à l'extérieur de l'entreprise), blocage sur les ordinateurs de l'entreprise de la connexion à des ports externes, séparation (virtuelle ou physique) du réseau interne et externe.

Règles de comportement et formation du personnel

L'utilisation des moyens de travail informatiques par les employés doit faire l'objet d'une réglementation. Ces directives ne doivent pas seulement être valables pendant le travail, mais aussi dans la vie privée. Dans les directives internes pour l'utilisation des moyens informatiques, l'entreprise ou la haute école doivent aussi fixer des règles pour l'utilisation d'Internet, de la messagerie à des fins privées ou les recherches professionnelles ou privées sur Internet. Les employés doivent être formés et suivre des cours de perfectionnement sur les risques et les dangers des nouvelles technologies.

Rédaction

Service de renseignement
de la Confédération SRC

Clôture de la rédaction

Juillet 2010

Prophylax
Service de renseignement de la Confédération SRC
Papiermühlestrasse 20
CH-3003 Berne
Téléphone: +41 (0)31 323 95 84 / www.src.admin.ch