Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense, de la protection de la population et des sports

Service de renseignement de la Confédération SRC

Aide-mémoire sur l'espionnage économique

Introduction

Infraction au code pénal, le renseignement prohibé (espionnage) désigne l'acquisition d'informations ou de données politiques, économiques et militaires tenues volontairement confidentielles ou secrètes, ainsi que la transmission de ces informations à des acteurs étrangers (État, groupe, entreprise, individu, etc.) au détriment de la Suisse ou de ses entreprises, institutions ou personnes en Suisse.

Dans quelle mesure votre entreprise est-elle menacée par l'espionnage ? Comment reconnaître des actes d'espionnage et comment protéger votre entreprise ? Il n'existe pas de protection intégrale, mais le risque d'espionnage peut être réduit grâce à des mesures appropriées. Les énumérations suivantes ne sont pas exhaustives.

Pourquoi une entreprise devient-elle la cible d'espionnage ?

- Elle produit des biens dans un domaine de haute technologie et possède un savoir-faire spécifique
- Elle occupe une position dominante dans un marché de niche (*hidden champion*)
- Les biens qu'elle produit sont soumis aux contrôles à l'exportation
- Elle pratique de la recherche appliquée et du développement
- Elle entretient des relations d'affaires avec des pays à risques

Quelles peuvent être les conséquences pour une entreprise victime d'espionnage ?

- Perte de secrets commerciaux
- Perte de mandats
- Perte de clients
- Dégâts d'image, aussi pour la Suisse en fonction de l'entreprise concernée
- Pertes financières, voire mise en faillite

D'où provient la menace d'espionnage ?

- Visites de délégations étrangères
- Joint-ventures, projets de recherche communs, intentions d'investissement étrangères, participations dans des entreprises ou acquisitions de sociétés à des fins de transfert de technologie
- Collaboratrices ou collaborateurs qui remettent des informations ou des données commerciales confidentielles sans autorisation à des tiers, que ce soit par préméditation ou contrainte (*insiders*), ou par inattention
- Ingénierie sociale (*social engineering*) : attaques de harponnage (*spear phishing*[1]), prise de contact via réseaux sociaux ou téléphone, courriels falsifiés au nom d'un supérieur (arnaque au président/*CEO Fraud*)
- Prestataires de services et consultants externes, fournisseurs
- Foires, conférences
- Cyberattaques

[1] Contrairement aux e-mails de phishing envoyés en masse, un e-mail/SMS de harponnage (« spear phishing ») vise une personne ou un groupe en particulier au sein d'une entreprise ou d'une organisation. Son contenu est adapté en conséquence. La personne ciblée est invitée à divulguer des informations personnelles (identifiants de connexion et mots de passe p. ex : une technique appelée « credential phishing ») 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.

Mesures de protection

- Élaboration et mise en œuvre d'un concept de sécurité de l'information et désignation d'un(e) préposé(e) qui fait appliquer les mesures de sécurité ayant été fixées avec le soutien de la direction
- Contrôle systématique et centralisé des informations publiées par l'entreprise et ses collaboratrices et collaborateurs (direction comprise)
- Contrôle des accès et accompagnement systématique des visiteurs et délégations externes
- Segmentation des réseaux informatiques
- Règlementation et restriction des droits d'accès des collaboratrices et collaborateurs aux données, documents et produits, en particulier aux résultats de la recherche et aux prototypes
- Interdiction de raccorder des clés USB privées, téléphones mobiles, ordinateurs portables, etc. au réseau de l'entreprise
- Utilisation de l'authentification à deux facteurs pour accéder aux ordinateurs, aux ordinateurs portables et aux courriels
- Sensibilisation régulière des collaboratrices et collaborateurs aux questions liées à la sécurité de l'information et la sécurité informatique
- Interdiction de mener des conversations confidentielles dans des endroits publics comme les restaurants, trains, chambres d'hôtel, taxis ou encore au téléphone. Interdiction d'emporter des téléphones mobiles dans des réunions d'affaires traitant de sujets sensibles

Voyages d'affaires à l'étranger

- N'emporter que les appareils électroniques indispensables, chiffrer leur contenu et ne jamais laisser les appareils sans surveillance (aussi valable pour les documents sur papier)
- Utiliser un ordinateur portable réservé aux voyages à l'étranger, ne contenant aucune donnée sensible (ordinateur portable dit de voyage) et protégé par un pare-feu ainsi qu'un logiciel antivirus
- L'accès à distance au réseau de l'entreprise passe uniquement par un canal sécurisé (Virtual Private Network, VPN) et requiert une authentification à deux facteurs
- N'utiliser les réseaux WiFi publics – y compris une partie de ceux protégés par un mot de passe – que par l'intermédiaire d'une connexion VPN ou du mode itinérance (*roaming*) ; désactiver les fonctions WiFi, Bluetooth et services de localisation quand elles ne sont pas utilisées
- Ne pas conserver de documents confidentiels dans la chambre d'hôtel ni dans le coffre-fort de la chambre
- Attendre d'avoir passé le contrôle douanier à l'arrivée pour rallumer le téléphone portable, et l'éteindre au retour avant de passer le contrôle douanier
- Faire preuve de prudence lorsqu'une personne inconnue tente d'établir un contact, transmet une invitation ou offre des cadeaux de valeur (contrepartie)

En cas de soupçon d'espionnage

- Conserver les preuves
- Signaler l'incident dans les meilleurs délais :
  - à la police cantonale
  - au Service de renseignement de la Confédération (*www.src.admin.ch*)

Le SRC analyse les indices et garantit un traitement confidentiel du cas d'espionnage.

Liens utiles

- **Dossier « Espionnage économique » :** *www.ndb.admin.ch/espionnage-economique*
  - **Prophylax :** programme de prévention et de sensibilisation du SRC sur les menaces en matière d'espionnage et de prolifération (brochure disponible)
  - **Film de sensibilisation** à l'espionnage ***« En ligne de mire »*** ainsi que les **explications** relatives aux méthodes d'espionnage présentées et aux mesures de protection correspondantes
  - Divers **aide-mémoires et fiches d'information** sur les thèmes de l'espionnage et de la prolifération
- Questions ou informations sur le programme Prophylax : prophylax@ndb.admin.ch
- Centrale d'enregistrement et d'analyse pour la sûreté de l'information : www.melani.admin.ch
- Annonce de courriels et sites Internet d'hameçonnage : www.antiphishing.ch