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

5 février 2018

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.

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
- Projets de recherche communs ou participations dans des entreprises à des fins de transfert de technologie
- Collaboratrices/collaborateurs qui remettent des informations ou des données commerciales confidentielles sans autorisation à des personnes externes à l'entreprise
- Contacts avec d'anciens collaboratrices/collaborateurs ou des collaboratrices/collaborateurs en fonction
- Ingénierie sociale (social engineering) : attaques de harponnage (spear phishing), prise de contact via réseaux sociaux ou téléphone, e-mails falsifiés au nom d'un supérieur (arnaque au président/CEO Fraud)
- Cyberattaques

Mesures de protection

- Contrôle systématique et centralisé des informations publiées par l'entreprise et ses collaboratrices/collaborateurs (direction comprise) (déterminer ce qui ne devrait pas être rendu public pour des raisons de prévention de l'espionnage)

- Règlementation et limitation des droits d'accès des collaboratrices/collaborateurs aux données, documents et produits, en particulier aux résultats de la recherche et aux prototypes (principe need-to-know/uniquement les informations nécessaires pour le travail)
- Segmentation des réseaux informatiques (le réseau du département recherche est par exemple séparé du reste du réseau de l'entreprise et n'est pas connecté à Internet)
- Interdiction de raccorder des clés USB privées, téléphones mobiles, ordinateurs portables, etc. au réseau de l'entreprise
- Contrôle des accès et accompagnement systématique des visiteurs et délégations externes
- Sensibilisation des collaboratrices/collaborateurs
- Interdiction de mener des conversations confidentielles au téléphone ou dans des lieux non sécurisés comme des restaurants, bars, chambres d'hôtel, taxis
- Cryptage des e-mails
- Interdiction d'utiliser des réseaux sans fil publics (WiFi/Hotspot) (le cas échéant, uniquement via des réseaux privés virtuels/VPN)

Voyages d'affaires à l'étranger

- N'emporter que les appareils électroniques indispensables, dont les contenus sont cryptés, et ne jamais laisser les appareils sans surveillance (aussi valable pour les documents sur papier)
- Utiliser un laptop 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 (VPN) et requiert une authentification à deux facteurs (carte PKI)
- Éviter les hotspots publics (WiFi gratuits), désactiver les fonctions WiFi et Bluetooth quand elles ne sont pas utilisées
- Accès Internet (aussi depuis le smartphone) uniquement via VPN ou réseau de données (roaming)
- Échange de cartes de visite uniquement avec des personnes de confiance
- Ne pas conserver de documents confidentiels dans le coffre-fort de l'hôtel
- 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
- Éviter d'emporter des répertoires contenant tous les contacts (concerne aussi le téléphone portable)
- En cas de soupçon d'accès non autorisé sur un appareil électronique pendant un voyage, le remettre pour contrôle au service de sécurité ou d'informatique après le retour

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 et les services de renseignement cantonaux traitent les soupçons d'espionnage en toute discrétion.

Liens utiles

- **Dossier « Espionnage économique » :** *www.ndb.admin.ch/espionnage-economique*
  - **Film de sensibilisation** à l'espionnage : **« En ligne de mire »** – espionnage économique en Suisse (peut aussi être visionné sur la chaîne Youtube du DDPS)
  - **Commentaires sur le court-métrage** « En ligne de mire »
  - **Brochure Prophylax :** programme de prévention et de sensibilisation Prophylax du SRC sur les menaces en matière d'espionnage et de prolifération
  - **Fiche d'information** « Que fait le SRC pour lutter contre l'espionnage ? »
- Questions ou informations en lien avec le **programme Prophylax :** courriel à *prophylax@ndb.admin.ch*
- **Centrale d'enregistrement et d'analyse pour la sûreté de l'information** (Melani) : *www.melani.admin.ch*
- Annonce de **courriels et sites Internet d'hameçonnage :** *www.antiphishing.ch*