SÉCURITE ÉCONOMIQUE ACTIVE : ENTRE BON SENS ET PARANO

Janvier 2012

Au cours de cet après-midi de sensibilisation, organisé par la direction technique de la FIM, la DCRI (Direction Centrale du Renseignement Intérieur) a rappelé aux nombreux industriels présents les risques quotidiens de pertes d'informations stratégiques et a donné des conseils pratiques pour éviter cet espionnage économique. En effet, l'industrie mécanique n'est pas épargnée, puisqu'elle représente 16% des attaques informationnelles.

CONTEXTE DE LA SÉCURITÉ ÉCONOMIQUE

La « sécurité économique » est le volet défensif de l'intelligence économique (la veille et le lobbying étant les volets offensifs).

Nous sommes dans un environnement de plus en plus mondialisé où l'information numérique circule de plus en plus vite. L'information est devenue une matière première stratégique, et sa circulation un vrai business.

Dans ce contexte, la DCRI (service du ministère de l'Intérieur, fusion des Renseignements Généraux et de la Direction de surveillance du territoire) intervient notamment dans le domaine du contre-espionnage et de la protection du patrimoine.

CIBLES, MÉTHODES ET PARADES

Sur quelles cibles d'informations les acteurs du renseignement économique vont-ils focaliser leurs efforts ?

Classiquement, on retrouve :

- le savoir-faire d'une entreprise (ex : process de fabrication) ;
- l'image (notoriété, réputation, rumeur) ;
- la finance ;
- les structures physiques (entreprise, usine et même domicile, ex. vol d'ordinateur professionnel au domicile, où les protections sont moins importantes ;
- les systèmes de communication ;
- l'humain.

De nombreuses méthodes « ouvertes » sont employées pour récupérer des informations stratégiques.

- Exploitation des informations rendues disponibles par vos entreprises dans les publications, sur les sites Internet, ou sur les stands des salons.
- Écoute active dans des cocktails, les lieux de restauration collective partagée, les « annexes » (café ou restaurant habituel), les machines à café.
- Passage de personnes étrangères dans vos locaux : visites de délégations (il faut préparer le parcours de visite et interdire les photos), stagiaires (veiller à valider l'information qui se trouve dans les rapports et celle que le stagiaire peut diffuser sur Internet).
- Vulnérabilité lors des déplacements (utiliser les filtres de confidentialité, surveiller ses conversations notamment à l'étranger).

- Exploitation de l'environnement professionnel quotidien : ménage, poubelles, maintenance, intérim, traduction, externalisation de services (comptabilité, formation, informatique), audits.

Dans certains cas, des méthodes clandestines sont utilisées.

- Outils techniques : interception de communication, système de suivi de véhicule, etc.
- Manipulation humaine, mise en fausse situation (recrutement, test, etc.).

Quelques parades peuvent être utiles face à ces attaques informationnelles.

- Le code du travail.
- Les protections internes à l'entreprise : clauses contractuelles, charte informatique, plan de sécurité interne, prévention.
- Un comportement personnel adapté au sein de votre entreprise : discrétion, faire attention aux interlocuteurs inconnus notamment au téléphone, destruction (broyeuse) des papiers stratégiques et des traces laissées sur les paper-boards, verrouiller son écran d'ordinateur.
- À l'extérieur de l'entreprise, être encore plus vigilant (400 vols d'ordinateurs par an dans le Thalys). Ne pas mettre d'informations professionnelles sur son ordinateur personnel.
- Avant de partir à l'étranger, voir le site du ministère des affaires étrangères (http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/) pour se renseigner. Faire attention aux « cadeaux numériques » (ex : clés USB) qu'on peut vous proposer. Ne pas laisser d'informations stratégiques à l'hôtel, même dans les coffres.
- En cas de doute, faire un rapport d'étonnement pour expliquer comment on s'est fait piéger (REX).

RISQUES SPÉCIFIQUES A LA SOCIÉTÉ NUMÉRIQUE

Nos pratiques actuelles et les nouvelles technologies de l'information et de la communication offrent des failles de plus en plus importantes.

- Facebook : 900 millions de comptes dans le monde, 75 milliards de photos. On met sur Facebook des informations que les services de police n'ont pas le droit d'avoir sur leurs fichiers !
- De plus en plus de photocopieurs sont gérés par des sociétés extérieures. Or, leurs disques durs contiennent beaucoup d'informations (le mieux est de négocier pour en avoir la propriété).
- Les Smartphones (17 millions en France) constituent une nouvelle cible, car ils n'ont en général pas de fire-wall ni d'antivirus. Pourtant, de nombreuses données transitent par eux. Il faut impérativement : verrouiller son téléphone à chaque fois ; ne jamais confier son Smartphone à quiconque ; ne jamais le brancher n'importe où ; remplacer le code à 4 chiffres par une phrase mot de passe.
- Dans certains pays, une loi permet de confisquer les outils numériques. Il est donc préférable de voyager avec uniquement les données utiles.
- Ne pas hésiter à chiffrer ses données sensibles. Parmi les logiciels disponibles : Security Box, ZoneCentral ou le gratuit TrueCrypt.
- Cloud Computing. Avec cette nouvelle tendance, on ne sait pas où se trouvent les données, ni si elles seront vraiment détruites quand on le souhaite. Consulter les guides sur le site de l'Agence nationale de la sécurité des systèmes d'information (http://www.ssi.gouv.fr/).
- Les clés USB. Elles permettent très facilement d'infecter un réseau informatique. Il est conseillé de passer les outils numériques qui viennent de l'extérieur sur un poste blanc, non relié au réseau. À l'inverse, on peut très rapidement copier toutes les données contenues sur une clé USB que quelqu'un branche sur votre ordinateur.

- Un « cheval de Troie » (ex : SubSeven) permet de prendre la main sur un ordinateur, de modifier des fichiers, de les supprimer.
- Pour véritablement effacer le contenu d'un support numérique, utiliser CCleaner ou Eraser. À l'inverse, un logiciel comme Recuva permet de récupérer les données effacées sur une clé USB formatée.
- Enfin, il est prudent de surveiller la présence de chacun (nom, prénom, société) sur Internet, ne serais-ce que pour détecter d'éventuelles usurpations d'identité. Essayer par exemple de rechercher votre nom sur le site http://www.123people.fr/.

DERNIERES PARUTIONS

PAGE2RSS pour surveiller un site Internet
http://www.cetim.fr/cetim/fr/Mecatheque/Veille-technologique/PAGE2RSS-pour-surveiller-un-site-Internet

Lettre informative - Outils et services du WEB2
http://www.cetim.fr/cetim/fr/Mecatheque/Veille-technologique/Lettre-informative-Outils-et-services-du-WEB2

Partagez vos documents avec Sky Drive and Google Docs
http://www.cetim.fr/cetim/fr/Mecatheque/Veille-technologique/Partager-vos-documents-avec-Sky-Drive-and-Google-Docs

Stratégie NET 2011
http://www.cetim.fr/cetim/fr/Mecatheque/Veille-technologique/Strategie-NET-2011

Ensemble pour les entreprises de la mécanique

Département
Veille Technologique et Stratégique

Contact
Laurent Couvé
Cetim - B.P. 80067
60304 Senlis Cedex
Tél. : 03 44 67 35 65
laurent.couve@cetim.fr

Retrouvez nos notes de veille dans la Mécathèque du site Cetim :
http://www.cetim.fr/cetim/fr/Mecatheque

Consultez le guide des Technologies prioritaires 2015 sur le site Cetim :
http://www.cetim.fr/cetim/fr/Mon-espace - Cliquez sur : ★ technos 2015