De l'intelligence économique à la sécurité informatique

Michel CHEMINAT
Directeur adjoint de l'ISIMA
Institut Supérieur d'Informatique, de Modélisation et de leurs Applications
1 Rue de la Chebarde, 63178 Aubière CEDEX
michel.cheminat@isima.fr

***Résumé* — L'un des piliers de l'intelligence économique est la protection du patrimoine informationnel, parfois appelé sécurité économique. Ce pilier fait souvent référence à la sécurité informatique. Il donc faut former les futurs ingénieurs en informatique aux aspects techniques de la sécurité mais aussi a sensibiliser tous les utilisateurs.**

***Mots clés* — Intelligence économique, sécurité informatique, sensibilisation.**

I. Introduction

L'intelligence économique (IE) est définie comme étant la maîtrise et la protection de l'information stratégique utile pour tout acteur économique. L'IE se décline en trois piliers : veille/anticipation, maîtrise des risques (sécurité économique) et action proactive sur l'environnement (influence). C'est sur le deuxième pilier que l'IE rejoint la sécurité informatique. En effet, lorsqu'un acteur économique (administration, entreprise) veut protéger son patrimoine informationnel, il est assez courant de penser que la sécurité informatique peut résoudre tous les problèmes mais le problème peut aussi venir d'erreurs humaines.

Le livre blanc "Défense et sécurité nationale" [1] commandé par François Hollande en 2012 et publié en 2013 indique "*La sécurité de l'ensemble de la société de l'information nécessite que chacun soit sensibilisé aux risques et aux menaces et adapte en conséquence ses comportements et ses pratiques. Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique*", ou encore "*Le cyberespace est donc désormais un champ de confrontation à part entière*". Par ailleurs, le ministère de l'enseignement supérieur et de la recherche a publié en 2013 un référentiel pour la sensibilisation à l'IE [2]. Un des thème développé concerne les principales vulnérabilités des acteurs économiques parmi lesquelles : sécurité physique des sites, fuites d'informations involontaires, négligences dans les déplacements professionnels, etc.
Sur un exemple concret : l'informaticien doit-il seulement se soucier que les logiciels soient à jour sur toutes les machines ? Il resterait vulnérable à une attaque zéro day. Il faut par exemple dans ce cas que chaque individu soit sensibilisé aux précautions à prendre à l'ouverture de pièces jointes.

L'ingénieur informatique a toute légitimité pour proposer aux équipes dirigeantes de mettre en place ces sensibilisations.

II. L'IE à l'ISIMA

L'ISIMA a mis en place depuis 2012 un cours d'intelligence économique obligatoire de 14 heures en tronc commun de dernière année. Sur le deuxième pilier de ce cours (maîtrise des risques, protection de l'information), ils apprennent donc pourquoi et comment sensibiliser le plus largement possible. Un des messages à faire passer aux étudiants, futurs ingénieurs en informatique, est que tout le monde est concerné par la sécurité informatique.

Un ingénieur qui se spécialise en sécurité informatique doit préconiser les bonnes pratiques, conseiller ses hiérarchiques sur les solutions techniques en matière de sécurité, organiser leur mise en œuvre. Lors de l'élaboration ou de la révision d'une Politique de

Sécurité des Systèmes d'Information (PSSI), il peut intervenir aussi bien sur les aspects techniques, il a été formé pour cela, mais aussi sur les aspects comportementaux des usagers. Et c'est sur ce dernier point que l'on rejoint le deuxième pilier de l'IE et que la formation dans ce domaine n'est pas encore suffisamment développée.

L'ingénieur informaticien n'est pas un utilisateur lambda et il peut lui être difficile de se mettre à la place d'un non informaticien. Par exemple une clé USB trouvée par terre devrait être considérée comme suspecte par l'informaticien alors qu'une personne non sensibilisée la branchera rapidement sur son poste de travail professionnel. La dispersion sur le parking d'une entreprise de clé USB infectée (avec le logo de l'entreprise !) par une personne mal intentionnée est une pratique connue des services de renseignements français, une nouvelle sorte de phishing.

Ainsi l'outil d'autodiagnostic [3] développé par la délégation interministérielle à l'IE (D2IE) propose quelques questions clefs : où sont stockées vos informations sensibles ? vos salariés sont-ils sensibilisés au vol d'information lors de déplacement professionnel ? donnez-vous des consignes relatives aux précautions à prendre sur les salons, dans les transports publics ? sur l'utilisation du wifi à l'hôtel ? etc.

Le maillon faible est bien souvent l'humain et même s'il est difficile de faire des statistiques (tout le monde ne veut pas reconnaître s'être fait avoir), certains services de renseignements français estiment que 3 fois sur 4, l'origine du problème est liée au comportement d'une personne (procédure inexistante ou non appliquée). Le maillon faible est l'interface chaise-clavier.

L'ingénieur informaticien doit donc être lui-même sensibilisé à ce volet moins technique et se tenir au courant des attaques récentes dans ce domaine. Il sera alors mieux à même de proposer des sensibilisations à destination de tous les collaborateurs, ce que le livre blanc préconise.

En poursuivant le raisonnement, il est essentiel d'expliquer à l'informaticien qu'il est lui même une cible privilégiée car sa fonction lui donne plus de droits. Les attaquants n'auront probablement pas besoin de chercher une élévation des droits pour parcourir le système d'information.

Une attaque classique commence souvent par une étape d'ingénierie sociale. L'attaquant cherche une cible ayant un profil attractif à l'aide d'organigrammes ou des réseaux sociaux professionnels tels LinkedIn ou Viadéo. Ces informations recoupées avec celles recueillies sur d'autres réseaux sociaux (Facebook, Google+, Twitter …), permettent de dresser un profil extrêmement précis de la personne ciblée et d'affiner ainsi les techniques d'approche.

Dans un "flash ingérence économique" du 4 février 2015 [4], la Direction Générale du Renseignement Intérieure (DGSI) relate des agissements dont plusieurs acteurs économiques français ont récemment fait l'objet : de faux entretiens d'embauche, orchestrées par le biais de faux cabinets de recrutement dans le but de soutirer des informations aux candidats sur leur entreprise actuelle. Pourquoi un ingénieur informaticien ne serait-il pas concerné ?

A titre d'information, le cours d'IE à l'ISIMA traite aussi des deux autres piliers à travers les notions suivantes :

- comprendre l'intérêt de structurer sa veille, les différents types de veille et les outils qui existent.
  Cycle de l'information, management de la connaissance.
- Comment fournir de l'information dans le but d'orienter les attitudes et les comportements d'individus ou de publics ?

Les ouvrages [5], [6] ont été précieux pour préparer ce cours, et il faut souligner aussi la qualité des différents guides publiés par l'Agence Nationale de la Sécurité des Systèmes d'Information [7].

III. Conclusion

Les évaluations des enseignements faits depuis l'instauration de ce cours montrent un réel intérêt des étudiants pour cette matière.
L'objectif n'est pas de former des experts en IE, mais il s'agit de sensibiliser à l'IE un public

d'élèves ingénieurs en informatique, avec les spécificités que cela peut comporter.

La sécurité informatique est quelque chose de trop sérieux pour être laissée aux seuls informaticiens.

Références

[1] Livre Blanc Défense et Sécurité Nationale, 2013, La documentation Française.

[2] Intelligence économique et nouveaux risques du 21e siècle, 2011, http://www.enseignementsup-recherche.gouv.fr/cid58914/referentiel-de-competences-intelligence-economique-et-nouveaux-risques-du-21e-siecle.html

[3] DIESE, Diagnostic d'intelligence économique et de sécurité des entreprises et DIESE-Lab, Diagnostic d'intelligence économique et de sécurité des laboratoires : http://www.intelligence-economique.gouv.fr/methodes-et-outils/logiciels-dauto-evaluation

[4] La Direction Générale de la Sécurité Intérieure, DGSI, ne dispose pas de site web, ses Flashs Ingérence Economique sont à chercher sur le web.

[5] La boîte à outil de l'intelligence économique, Christophe DESCHAMPS et Nicolas MOINET, 2012, Dunod.

[6] Influentia, la référence des stratégies d'influence, Ludovic FRANCOIS et Romain ZERBIB (dir), 2015, LaVauzelle.

[7] ANSSI, http://www.ssi.gouv.fr