Sécurité informatique et criminalité informatique : une nécessaire maîtrise des risques

Autor(en): **Ghernaouti-Hélie, Solange**

Objekttyp: **Article**

Zeitschrift: **Revue économique et sociale : bulletin de la Société d'Etudes Economiques et Sociales**

Band (Jahr): **61 (2003)**

Heft 3: **Lutte contre la criminalité économique : prévenir, détecter, réprimer**

PDF erstellt am: **23.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-141370

REVUE ÉCONOMIQUE ET SOCIALE, SEPTEMBRE 2003

SÉCURITÉ INFORMATIQUE ET CRIMINALITÉ INFORMATIQUE: UNE NÉCESSAIRE MAÎTRISE DES RISQUES

Solange GHERNAOUTI-HÉLIE
Professeure à l'Ecole des HEC
Directrice du DEA en Droit, Criminalité et Sécurité des Nouvelles Technologies
Université de Lausanne,
sgh@hec.unil.ch

1. Sécurité informatique: des enjeux de société

On assiste de nos jours à une prise en considération croissante des besoins de maîtrise des risques informatiques opérationnels du fait de l'usage extensif des nouvelles technologies, de l'existence d'une infrastructure informationnelle globale et de l'émergence de nouveaux risques. De plus, l'intégration des nouvelles technologies dans toutes les activités et infrastructures accroît la dépendance des organisations et des individus aux systèmes d'information et aux réseaux.

L'augmentation de la dépendance aux technologies du numérique, des menaces et des risques, nécessite de doter les individus, les organisations et plus globalement la société, de mesures, procédures et outils qui autorise une meilleure gestion des risques technologique et informationnel. Les enjeux de cette maîtrise des risques sont ceux de l'ère numérique et de la société de l'information en devenir.

Le succès de la révolution informationnelle pouvant conduire à un certain âge d'or de la société de l'information, dépend de cette bonne maîtrise des risques.

Enjeux de société, enjeux économiques, enjeux politiques, enjeux humains, qu'elle soit dénommée sécurité de l'informatique et des télécoms, la sécurité informationnelle touche à la sécurité du patrimoine numérique et culturel des nations. Enjeux colossaux s'il se doit, la problématique soulevée est non seulement de première importance, elle est avant tout multiforme et très complexe.

La maîtrise du patrimoine numérique informationnel, la distribution de biens intangibles, la valorisation des contenus ou l'existence d'une fracture numérique par exemple, sont autant de problèmes d'ordre économique et social, dont la résolution ne pourra être réduite à la seule dimension technologique de la sécurité informatique.

La réalisation de la société de l'information nécessite donc de disposer :

- d'infrastructures informationnelles fiables et sécurisées (accessibilité, disponibilité, sûreté de fonctionnement, continuité des services) ;
- de politiques d'assurance et d'un cadre légal adaptés ;
- d'outils efficaces de gestion du risque informationnel ;
- de procédures et moyens pour développer la confiance dans les applications et services offerts par les nouvelles technologies (transactions commerciales et financières, e-santé, e-gouvernement, e-vote, etc.).

Il est constaté, que la démarche sécuritaire est souvent limitée à la mise en place des mesures, de réduction des risques pour les valeurs informationnelles des organisations. Or, l'approche sécuritaire doit également répondre aux besoins de sécurité des individus, notamment pour ce qui concerne la protection de leur vie privée et du respect de leurs droits fondamentaux.

2. De l'insécurité informatique à la criminalité informatique: une question d'opportunité

La réalité de l'insécurité des technologies de traitement de l'information et des communications trouve ses origines dans les caractéristiques des technologies et du monde virtuel.

La dématérialisation des acteurs, les accès à distance, un relatif anonymat, les problèmes de conception, de mise en œuvre, de gestion, de contrôle de l'informatique et des télécoms, associés aux pannes, dysfonctionnements, erreurs, incompétences, incohérences ou encore aux catastrophes naturelles, confèrent de facto un certain niveau d'insécurité aux infrastructures informatiques. Dans ce contexte, les possibilités d'exploitation de ces vulnérabilités et de malveillance sont nombreuses. La réalité de ces dernières : usurpation d'identité, leurre de systèmes, accès indus, exploitation frauduleuse des ressources, infection, détérioration, destruction, modification, divulgation, déni de service, vol, etc. met en évidence les limites des approches sécuritaires actuelles, tout en révélant paradoxalement, une certaine robustesse des infrastructures.

Quelles que soient les motivations des acteurs de la criminalité informatique celle-ci engendre toujours des conséquences économiques non négligeables et constitue dans sa dimension de cybercriminalité, un fléau grandissant, transfrontalier et complexe.

La sécurité informatique doit d'une part s'adapter aux paradigmes mouvants de l'informatique et des réseaux ainsi qu'à leurs dimensions internationale et dynamique et d'autre part à celui de la criminalité informatique, tout en s'inscrivant dans une logique de rentabilité.

La démarche de prévention sécuritaire est par définition pro-active. Elle touche aux dimensions humaine, juridique, organisationnelle, économique (ratio coût de mise en œuvre / délais de

mise en œuvre / services offerts) et technologique. Jusqu'à présent, seule la dimension technologique a été prise majoritairement en considération dans la sécurisation des environnements informatiques. Cette manière d'appréhender la sécurité informatique, sous un angle essentiellement technologique, qui néglige la dimension humaine, pose un véritable problème dans la maîtrise du risque technologique d'origine criminel. En effet, la criminalité est avant tout, une question de personne et non de technologie. Une réponse d'ordre uniquement technologique est donc inappropriée à la maîtrise d'un risque humain.

L'appréhension de la criminalité informatique s'inscrit, le plus souvent dans une démarche de réaction et de poursuite. Celle-ci s'effectue à posteriori, c'est-à-dire après la survenue d'un sinistre qui traduit ainsi la défaillance des mesures de protection.

S'il est nécessaire de prévenir et de dissuader les cyber-abus en développant des mécanismes de justice et d 'investigation, il est tout aussi primordial d'identifier dans les politiques de sécurité les mesures qui permettront de réagir aux attaques et d'en poursuivre leurs auteurs. Pour cela, il est impératif de concevoir et de réaliser des plans de secours et de continuité qui intègrent les contraintes liées à l'investigation et à la poursuite de la criminalité informatique.

Cela se résume à la résolution d'une problématique de ratios notamment entre les coûts des mesures et les impacts des délits potentiels et entre les délais d'intervention des investigateurs et les délais de restauration des contextes de travail par les responsables de sécurité. Investigateurs et responsables de sécurité répondent à des logiques de travail et à des objectifs différents, dans des échelles de temps distinctes.

3. La maîtrise du risque criminel informatique: un nécessaire partenariat, une implication de tous les acteurs

Bien que le marché tente de développer des mécanismes pour réduire, transférer ou partager le risque informationnel, le secteur privé ne peut résoudre seul, la question de maîtrise du risque criminel.

L'état possède des responsabilités importantes pour la réalisation d'une sûreté numérique. Ceci est particulièrement vrai pour la définition d'un cadre légal approprié, c'est-à-dire unifié et applicable. De plus, il doit non seulement favoriser et encourager la recherche et le développement en matière de sécurité mais aussi promouvoir une culture de la sécurité, imposer le respect d 'un minimum de normes de sécurité (la sécurité devrait être intégrée en natif dans les produits et services), tout en renforçant la lutte contre la criminalité.

Se pose alors la question du modèle financier sous-jacent à ces actions et à la réalisation du partenariat entre le secteur privé et public, pour des plans d'action aux niveaux national, européen et international.

Une maîtrise globale, centralisée et coordonnée de la criminalité informatique nécessite une réponse politique, économique, juridique et technologique homogène et adoptable par les différents acteurs de la chaîne numérique, co-partenaires de la sécurité.

Au niveau stratégique, il faut assurer la prévention, le renseignement, le partage d 'information, faire connaître les meilleures pratiques de gestion du risque et de la sécurité, la gestion des alertes, la coordination, l'harmonisation des systèmes légaux, l'assistance pour promouvoir la sûreté et la sécurité, la définition des coopérations éventuelles (Formelle / informelle, Multilatérale / bilatérale, Active / passive, dimensions Nationale / supra-nationale, etc.).

Il est également nécessaire d'éduquer, d'informer et former aux technologies de traitement de l'information et des communications et non uniquement à la sécurité et aux mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la promotion d'une certaine culture de la sécurité et d'une cyber-éthique. En amont de la culture sécuritaire, il doit y avoir une culture de l'informatique.

Il faut donner les moyens aux différents acteurs d'apprendre à gérer les risques technologique, opérationnel et informationnel qui les menacent en fonction de l'usage fait des nouvelles technologies.

Services de justice et police mais aussi ceux de la protection civile, les pompiers, l'armée ou la Gendarmerie trouvent leur place tant au niveau tactique qu'opérationnel dans la lutte contre la criminalité informatique afin de protéger, poursuivre et réparer. Des centres de surveillance, de détection et d 'information aux risques informatique et criminel doivent être opérationnels afin d'assurer la prévention nécessaire à la maîtrise de ces risques.

4. Du compromis à l'équilibre

Bien que des solutions de sécurité existent, elles ne sont pas absolues et ne répondent le plus souvent qu'à un problème particulier dans une situation donnée. Elles déplacent le problème de sécurité ou reportent la responsabilité de la sécurité et de plus, elles nécessitent d'être sécurisées et gérées de manière sécurisée.

Fort est de constater qu'elles ne répondent peu ou prou à la dynamicité du contexte dans lequel elles doivent s'intégrer. Les technologies ne sont pas stables, les cibles sont mouvantes, le savoir-faire des malveillants évoluent ainsi que les menaces et les risques. Ceci fait que la pérennité des approches sécuritaires, comme le retour sur investissements de celles-ci, ne sont jamais garantis.

La diversité et la pluralité des acteurs (ingénieurs, développeurs, auditeurs, intégrateurs, juristes, investigateurs, clients, fournisseurs, utilisateurs, etc.), la diversité d'intérêt de visions d'environnements, de langages rendent difficile la cohérence globale des mesures de sécurité. Or

seule une appréhension globale et systémique des risques et des mesures de sécurité, une prise de responsabilité de l 'ensemble des acteurs et intervenants pourraient contribuer à offrir le niveau de sécurité attendu pour réaliser en confiance, des activités via les technologies de l'information et des communications ainsi que la confiance dans l'économie numérique.

Entre besoins et solutions de sécurité, entre facilité d'utilisation et efficacité des solutions de sécurité, entre délais de disponibilité de solutions efficaces et conviviales et coûts de développement et d'intégration de ces solutions, entre niveaux de sécurité et coûts des solutions, l'équilibre à trouver passe par un compromis.

Ce dernier, résultera du choix consistant à privilégier un facteur au détriment des autres.

En effet, un équilibre est à obtenir entre les besoins de sécurité et les dimensions financières et humaines de la mise en oeuvre opérationnelle des solutions de sécurité viables. Le niveau de sécurité des infrastructures résulte donc d'un compromis entre trois facteurs : le coût, le niveau de service de sécurité et le temps de livraison. Il est illusoire de croire que ces trois facteurs pourraient être satisfaits simultanément. Des choix doivent être effectués pour déterminer quel sera le facteur à privilégier et à partir duquel les deux autres devront être adaptés.

5. De l'importance du juridique dans la sécurité des systèmes d'information

Par ailleurs, l'intelligence juridique devient le facteur clé de succès de la réalisation de la sécurité informatique et le droit devient omniprésent. La responsabilité pénale des acteurs, responsable sécurité ou directeur de systèmes d'information par exemple, est de plus en plus invoquée lors de sinistralité lorsque les ressources informatiques qu'ils gèrent sont l'objet ou le moyen d'une fraude. Il est nécessaire que les responsables puissent alors démontrer que des mesures suffisantes de protection du système d'information et des données aient été implantées afin de se protéger contre un délit de manquement à la sécurité. Ils sont une obligation de moyens mais non de résultats. Les responsables d'entreprises doivent donc être extrêmement attentifs à l'égard du droit des nouvelles technologies et leur système d'information doit être en conformité juridique. Les enjeux juridiques liés à la sécurité informatique sont devenus prépondérants qu'ils soient relatifs à la conservation des données, à la responsabilité des prestataires techniques ou hébergeurs, à la gestion des données personnelles des clients, à la cybersurveillance des employés, à la propriété intellectuelle, aux contrats informatiques ou à la signature électronique par exemple. Ils constituent maintenant autant de points à prendre en considération lors de la mise en place de solutions de sécurité. Ainsi le droit dans le domaine du numérique, peut devenir un atout stratégique pour les organisations qui le maîtrise.

6. Pour une approche de gestion du risque

L'application des principes de précaution, de coopération, d'économie, de décentralisation et de séparation des pouvoirs en matière de sécurité informatique serait de peu d'utilité si elle ne desservait pas une politique de sécurité résultant d'une gestion efficace des risques techniques, organisationnels, financiers, juridiques et humains. Dotons donc la société de l'information d'outils efficaces pour cela!