Potentiel scientifique et technique d'un laboratoire : Favoriser l'innovation, protéger les savoirs : un équilibre délicat

Jean-Pierre Damiano

Potentiel scientifique et technique d'un laboratoire :
Favoriser l'innovation, protéger les savoirs : un équilibre délicat

Jean-Pierre DAMIANO
Ingénieur de recherches (UCA CNRS LEAT, Sophia Antipolis)

RESUME :

Le potentiel scientifique et technique d'un laboratoire de recherche confère un caractère stratégique à la protection de son système d'information. Les atteintes peuvent tout aussi bien toucher ses données scientifiques ou technologiques que ses outils ou ses moyens scientifiques, techniques ou humains. Le laboratoire vit souvent dans un environnement complexe par la diversité de ses tutelles et la diversification de ses ressources, tout en étant confronté à une compétition scientifique croissante. Face aux risques encourus, il convient d'identifier ce qui doit être protégé, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et de mettre en œuvre les parades adaptées au niveau de sécurité retenu. Un tel plan d'actions conduit à des règles. Pour qu'elles soient acceptées, elles ne doivent pas entraver la recherche, la compétitivité, les échanges et les coopérations nationales et internationales, la diffusion à travers les brevets, les publications et les congrès, etc. C'est un équilibre délicat à trouver et à maintenir.

ABSTRACT:

The scientific and technical potential of a research laboratory gives a strategic character to the protection of its information system. The security breaches can easily affect scientific or technological data as well as their scientific, technical or human potential. The laboratory often lives in a complex environment by the diversity of its guardian ship and the diversification of its resources, while being confronted with an increasing scientific competition. In front of incurred risks, and in its functional and organizational context, it is advisable to identify what must be protected, to quantify the corresponding stake, to formulate objectives of safety and to implement the parades adapted exactly reserved level of safety. Such an action plan leads to rules. So that they are accepted, they do not have to hamper research, competitiveness, exchanges and national or international cooperation, patent production, publications and participation to congresses, and so on. It is an appropriate balance has to be found and to be kept.

Sommaire

Introduction

Les laboratoires de recherche publics (rattachés à des services de l'état, universités, CNRS, etc.) ou privés (affiliés à des industries) évoluent au sein d'un environnement complexe par la diversité de leurs tutelles (pour le public) et par la diversification de leurs ressources. Ils sont confrontés à une compétition scientifique en constante expansion. Chaque jour sont échangées sur leurs réseaux de très nombreuses informations, des données scientifiques (résultats de recherche et d'expérimentation, coopérations, brevets, contrats industriels etc.), mais aussi des données de gestion comptable, financière ou encore liées aux ressources humaines, la messagerie, etc.

En accord avec le domaine d'activité concerné, une partie de ces informations peut être considérée comme stratégique et sensible. Il s'agit de la part qui participe à la création de savoirs et savoir-faire innovants qui conditionnent la pérennité de la recherche et ses résultats. Tous les membres du laboratoire contribuent à cet effort et sont directement intéressés par la préservation de ce patrimoine informationnel et la constitution d'un climat de confiance vis-à-vis des partenaires extérieurs, qu'ils soient académiques ou industriels.

Dans ce contexte, il convient d'identifier ce qui doit être protégé, d'en quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et d'identifier, arbitrer et mettre en œuvre les parades adaptées [1-3]. La sécurité du système d'information (SSI) s'impose donc comme une composante essentielle de la préservation du laboratoire dans ses intérêts propres et dans ceux liés à des enjeux nationaux et internationaux. Les objectifs sont établis en prenant en compte les exigences de sécurité telles que la réglementation et les référentiels en vigueur, les besoins « métiers » et les enjeux de sécurité.

Cet article se propose d'exposer une approche méthodologique destinée à donner des éléments d'appréciation des risques liés à la perte des savoirs, des savoir-faire, etc. dus aux vulnérabilités non traitées. Les conséquences qui en résultent pourraient provoquer une perte de confiance, une dégradation de l'image de marque pouvant par exemple conduire à la perte de contrats. Les mesures de sécurité doivent être simples et pragmatiques pour constituer une réponse bien appropriée et acceptée par tous les acteurs de la recherche. Car cela peut introduire, dans certains cas, de nouvelles contraintes dans leur quotidien, lors d'échanges et de coopérations internationales, de préparation de collaborations, etc. Pour cela, la sensibilisation et la formation à la sécurité de l'information de tous constitue toujours une initiative à privilégier.

Le potentiel scientifique et technique d'un laboratoire de recherche

Le potentiel scientifique et technique se définit comme l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée, au développement technologique. Ainsi, dans le cadre d'un laboratoire de recherche, au-delà du personnel qui le compose, il comprend le plus souvent (i) les équipements, les matériels d'expérience, les bases de données,(ii) les savoirs et savoir-faire, (iii) les travaux de recherche et d'expérience en cours et futurs, les brevets en cours de dépôt, etc. (iv) la réputation, l'image du laboratoire. Ce potentiel confère donc un caractère stratégique à la protection du patrimoine scientifique et technique. Les atteintes peuvent tout aussi bien cibler les données scientifiques ou technologiques que les outils ou moyens qu'ils soient scientifiques, techniques ou humains. Tous les domaines de la science et de la technologie sont concernés : biologie,

sciences agronomiques et écologiques, chimie, médecine, santé sans oublier évidemment les sciences de l'information et de la communication, etc.

La protection de ce potentiel concerne tous les acteurs de la recherche. La sensibilisation et la formation des membres du laboratoire aux enjeux de la maîtrise de l'information conduisent à la mise en œuvre de pratiques et d'outils juridiques appropriés. Car, quel que soit son domaine d'activité, cette production intellectuelle est devenue une source de convoitise de la part de diverses entités (laboratoires ou industriels) désirant exploiter au mieux des informations sur les études en cours, les nouveaux concepts et les brevets, etc. Dans la littérature, on définit souvent une information comme étant sensible si elle requiert une attention, des précautions particulières. Ainsi pour un chercheur ou un doctorant, la synthèse de ses travaux ayant demandé des années d'études et de collaboration est considérée comme une information sensible, alors que pour le gestionnaire, c'est la base de données contenant les contrats en cours, leur financement, les partenaires, qui est vitale. Donc, il convient de définir le système d'information du laboratoire et d'en préciser son étendue et les enjeux de sa sécurité.

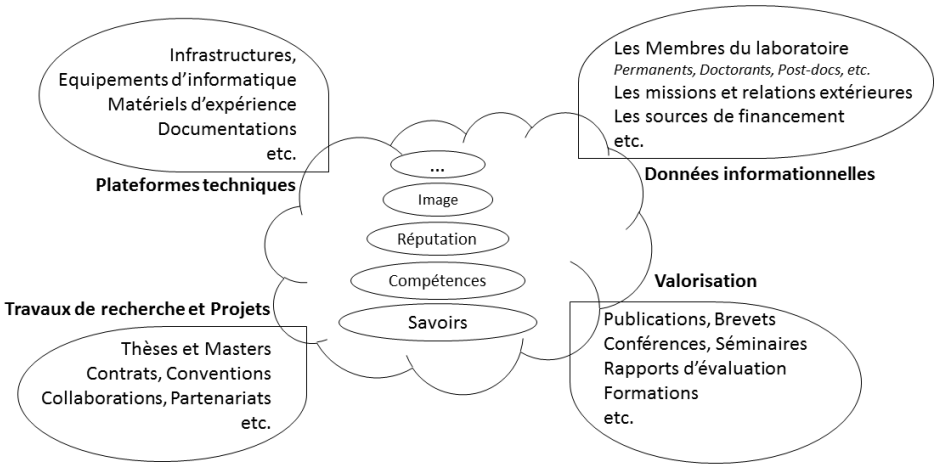

Figure 1: Potentiel scientifique et technique d'un laboratoire de recherches

Le système d'information

Le système d'information (SI) d'un laboratoire est un ensemble organisé de ses ressources permettant d'acquérir, de stocker, de structurer et de partager des informations sous forme de textes, images, sons, vidéos ou de données codées et autres [4]. Le SI inclut les équipements (ordinateurs, réseaux, etc.), les logiciels, les bases de données et les supports qui sont sous la responsabilité du laboratoire, sans oublier les traces des opérations informatiques. La mise en œuvre du système d'information s'inscrit dans un cadre législatif et réglementaire destiné à protéger les droits de propriété intellectuelle et industrielle ainsi que ceux de la vie privée. Dans certains cas une partie des infrastructures de réseaux utilisée n'est pas maîtrisée. Elle peut relever de la responsabilité du ministère de tutelle, d'un opérateur, etc. Cette répartition dépend des organisations et de leur taille. On ne s'étendra pas, dans cet article, sur ces aspects qui nécessitent un développement important. A cet aspect technologique s'ajoutent les compétences, les savoirs et savoir-faire des chercheurs, des ingénieurs et des techniciens dans le cadre de leurs projets en cours et futurs, les travaux de recherche et d'expérience, les innovations, les brevets en cours de dépôt, les publications en cours, etc. Les

enjeux essentiels SSI d'un laboratoire consistent à protéger et à assurer la disponibilité de ses éléments. Un équipement électronique pilotant une expérience en temps réel peut être une ressource sensible. Si c'est le cas, un matériel de secours permet d'assurer sa disponibilité en cas de dysfonctionnement du premier. La SSI propose un rempart contre les accidents naturels et les actes malveillants (sécurité physique), contre les signaux parasites compromettants (sécurité électronique).

Pour atteindre les objectifs de la SSI, des mesures de sécurité sont mises en œuvre afin de limiter les impacts d'une attaque. Il est possible de classer ces critères (liste non exhaustive) :

- La disponibilité : l'information est accessible et utilisable sans faille. L'accès aux services et ressources installées est garanti avec le temps de réponse prévu.
- L'intégrité : l'information est exacte et exhaustive. Elle n'est pas altérée ou détruite de manière non autorisée, volontairement ou non.
- La confidentialité : l'information n'est accessible qu'aux personnes ou processus autorisés. Tout accès indésirable doit être bloqué.
- La traçabilité : c'est la garantie que les accès ou les tentatives d'accès sont recensés et que ces traces sont conservées et demeurent exploitables.
- L'authentification : c'est l'exactitude de l'identité d'une personne, d'une machine, etc. pour maintenir la confiance dans les relations d'échange et de partage.
- La non-répudiation : un utilisateur ne peut contester les opérations réalisées.
- L'imputation : un tiers ne peut pas s'attribuer les actions d'un autre.

Le risque

Le risque peut être défini comme la probabilité qu'une menace exploite une vulnérabilité d'un composant du SI et ainsi cause un préjudice au laboratoire. Après avoir cerné le contexte et le périmètre à sécuriser, une appréciation des risques est nécessaire. Elle permettra de définir les objectifs de sécurité et les mesures à prendre suite à l'identification des menaces, l'analyse des vulnérabilités, l'évaluation de la vraisemblance des attaques et de leur impact. Une défaillance du système d'information affecte directement les activités du laboratoire (un vol de documents relatifs à un dépôt de brevet, par exemple). Elle peut aussi conduire à la perte de crédibilité, à la dégradation de l'image, à la perte de confiance des partenaires, à la perte de parts de marché (impossible de valoriser une innovation une fois les informations divulguées), etc.

L'usage de supports externes de stockage tels les clés USB ou encore le recours à des mots de passe faiblement robustes, participe au risque. Il en est de même pour le partage personnel et professionnel des *smartphones*, le transfert de fichiers non sécurisé ou l'utilisation non raisonnée de serveurs distants de stockage (*cloud computing*). La participation à des réseaux sociaux sans modération peut induire le risque de divulgation d'éléments de la vie professionnelle ou privée autre qu'un simple CV. L'usage immodéré des bornes Wi-Fi des lieux publics peut aussi se révéler délicat.

Pour chacun des risques identifiés lors de l'analyse, une décision doit être prise, acceptée par l'ensemble des membres du laboratoire. Grâce à une politique fondée et applicable, les risques peuvent être : (i) réduits en appliquant des mesures de sécurité, (ii) transférés (ex. avec une assurance), (iii) évités (ex. en arrêtant un service), (iv) acceptés en fonction de critères préalablement définis dans la mesure où ils ne remettent pas en jeu l'activité de l'organisation.

Les menaces

Les systèmes d'information, au sens large, présentent des vulnérabilités qui peuvent être exploitées par diverses menaces existantes. Ces dernières peuvent être environnementales, intrinsèques, humaines, etc. [5]. Les menaces majeures identifiées peuvent être d'origine externe (compromission ou vol de données, physique, électronique, etc.) mais aussi internes (négligence du personnel, utilisation malveillante des matériels, présence de nombreux non permanents, etc.). Une menace est dite « passive » si elle ne modifie pas l'information et porte essentiellement sur la confidentialité, ou « active » si elle modifie le contenu de l'information ou le comportement des systèmes de traitement.

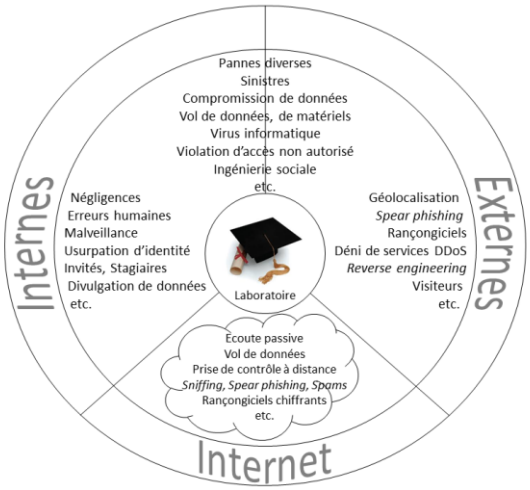

Figure 2: Panorama des principales menaces

L'organisation de ces menaces permet à un intrus de composer des attaques ayant pour objectif, par exemple, de prendre le contrôle du SI pour une utilisation ultérieure à un moment opportun. L'intrus peut aussi tenter de récupérer de l'information sur le système, ou encore d'utiliser le système compromis comme point d'entrée vers un réseau ou un autre système. Il peut aussi, tout simplement, empêcher l'accès à une ressource particulière, ce qui peut mener à un déni de service. Désinformer et tromper les utilisateurs font partie aussi de la panoplie des actions malveillantes. La combinaison d'une attaque informationnelle (exploitation des réseaux sociaux par exemple) avec une attaque informatique (exploitation de faille dans les réseaux, les systèmes, etc.), facilite la divulgation d'informations (exemple du réseau social FaceBook dont une vulnérabilité favorisait l'usage de données de réinitialisation de mots de passe - Le Monde.fr, 9 mars 2016).

Pour arriver à leurs fins, les attaquants adaptent leurs tentatives d'intrusion au niveau de protection de la cible. La typologie de ces atteintes au SI peut se décliner ainsi (liste non exhaustive) :

- électronique : interception ou brouillage des communications, utilisation de signaux parasites compromettants, détection et interception du contenu des étiquettes de type RFID (*Radio Frequency Identity*).
- logicielle : intrusion, exploration, altération, destruction de systèmes par des moyens logiques. Les attaques les plus connues sont les virus, les vers, le pourriel ou *spam*, l'hameçonnage ou *phishing*, le canular informatique ou *hoax*, les logiciels espions ou *spywares*, l'enregistreur de frappe ou *keylogger*, les défigurations de site *web*, les rançongiciels (*ransomware*), attaques par point d'eau (*watering hole*) et également des

pannes organisées ! Une atteinte bien connue est la saturation, dénommée déni de service (attaque provoquant la saturation d'une des ressources du SI).

- organisationnelle : un attaquant cherchera à abuser des défauts de l'organisation et de sa sécurité pour accéder aux ressources sensibles (exemple de prestataires de service qui sont des vecteurs privilégiés pour s'introduire au sein du périmètre physique du laboratoire).
- etc.

De nos jours, les menaces sont d'un niveau technique de plus en plus élevé. Elles ont souvent pour origine une organisation munie de moyens importants [6] : cela peut être le fait d'activistes, de criminels, de cyber-terroristes, d'agences gouvernementales, etc. Dans le cas d'attaques par rançongiciel, par exemple, comme cela a eu lieu récemment, le système d'information a dû être totalement interrompu, y compris la téléphonie. Dans un hôpital anglais, des interventions chirurgicales ont dû être réalisées en mode « médecine de guerre » car les patients ne pouvaient attendre le retour du fonctionnement normal [7].

Les vulnérabilités

Une vulnérabilité est une faiblesse qui rend sensible à une menace. Par exemple, un accès au bâtiment mal réglementé, sans contrôle d'accès des fournisseurs, l'absence de surveillance des entreprises lors de leurs interventions, des trous de sécurité dans les logiciels, etc. constituent des vulnérabilités [8]. Concernant les laboratoires, les coopérations internationales, la visite de professeurs invités, l'accueil de stagiaires, etc. nous imposent de rester vigilants, particulièrement lorsque la relation entre le projet de recherche visé et le profil du "partenaire" présente une sensibilité particulière (cas d'une équipe de recherche d'un laboratoire étranger concurrent par exemple, etc.).

Pour déterminer les failles d'un système d'information, il convient de savoir si le système fait uniquement ce qu'il doit faire et le fait correctement. Si ce n'est pas le cas, il faut mettre en œuvre des parades, le temps restant un facteur essentiel. Le délai entre la détection de la vulnérabilité et la mise en place de correctifs efficaces est un facteur décisif de succès pour le personnel en charge de la sécurité. Dans la littérature, le terme *zero-day* signifie que la faille n'est pas encore connue de l'utilisateur, le *zero-day* n'est connu que de l'attaquant. Dans ce laps de temps, le système est alors vulnérable et suivant les techniques offensives, les dégâts occasionnés peuvent être graves. Une vulnérabilité cesse d'être *zero-day* dès qu'elle a été identifiée par la communauté de la sécurité informatique. On voit facilement qu'un long délai, avant l'application de correctifs, est une période où le système est sans défense, parfois à l'insu même de l'administrateur en charge du SI, et généralement proportionnel aux dégâts potentiels.

De nouvelles vulnérabilités sont liées à l'introduction d'objets connectés dans notre vie quotidienne tant professionnelle que privée. Il en est de même pour le domaine industriel, avec le développement des systèmes d'acquisition et de contrôle des données (SCADA, Supervisory Control And Data Acquisition).

A l'horizon 2020, le nombre d'objets connectés dans le monde approchera les 30 milliards d'unités (selon le cabinet IDC) dont 90% concerneront l'Asie, l'Europe occidentale et l'Amérique du Nord (selon L'Express/L'Expansion). D'ici 2025, il est prévu que le produit intérieur brut (PIB) européen augmente de 1 000 milliards de dollars grâce à la vente de ces objets et services, à la création de valeur ajoutée [9].

Cette prolifération d'objets connectés (*IoT, Internet of Things*), communiquant par radiofréquence, bouleverse nos habitudes [10-12] et présentent des vulnérabilités potentielles. Ainsi la prise de contrôle d'ampoules « intelligentes », grâce à des failles de sécurité, permet de générer un *black-out*. Dans le cas de jouets connectés, comme il n'y a pas d'authentification, il est possible à des interlocuteurs malveillants de parler aux enfants (cas des poupées Cayla, en Allemagne, en 2017 ou Hello Barbie, aux Etats-Unis, en 2015, etc.). Il en est de même avec les bracelets connectés capables de diffuser des informations personnelles. Des vulnérabilités dans les systèmes de caméras de surveillance permettent des attaques en réseau et ainsi provoquer des blocages d'un quartier, d'une ville, etc. Les failles d'un drone ou d'une flotte de drones pourraient favoriser une intrusion à fin de prise de contrôle [13] et donc de changer les objectifs prévus des missions. Il en est de même pour les véhicules autonomes dont des logiciels embarqués peuvent subir une injection de code malveillant pour inhiber telle ou telle action programmée (freinage, etc.). Le *hacker* Banarby Jack, aujourd'hui décédé, avait démontré que certains pacemakers étaient sensibles à des attaques sans fil. Leurs détournements pouvaient ainsi générer des chocs électriques de plus ou moins intenses en agissant directement sur le stimulateur cardiaque (lemonde.fr, juillet 2013). De telles vulnérabilités peuvent être dues à la complexité de ces systèmes. Leurs concepteurs ont pu, en toute bonne foi, ne pas les voir bien qu'elles soient présentes dès la conception. On peut considérer que ces problèmes sont en partie une conséquence de la politique d'innovation qui pousse les entreprises à créer et produire, en un temps réduit, des objets connectés à large diffusion auprès du public, en n'accordant pas assez de temps de réflexion à la sécurité. Cette problématique devrait être traitée à la fabrication afin d'empêcher la violation de la vie privée, de favoriser le chiffrement des données et des communications, de prendre en compte la gestion des risques, etc.

En ce qui concerne le domaine industriel, des systèmes d'acquisition et de contrôle de données (SCADA : Supervisory Control And Data Acquisition [14]) sont des systèmes de gestion et de contrôle, à grande échelle, surveillant, gérant et administrant des infrastructures complexes dans des activités aussi variées que le transport, le nucléaire, l'électricité, le gaz, etc. Ces systèmes connectent des automates, des capteurs, des dispositifs de mesures ou d'analyse, des systèmes de commande et de contrôle, etc., sans oublier les interfaces homme-machine. De tels systèmes existent depuis une cinquantaine d'années, quand le secteur industriel n'était pas encore concerné par les cyberattaques actuelles. La sécurité, jugée non nécessaire, n'était pas intégrée à la conception.

Suite à diverses attaques par logiciel (Stuxnet, DragonFly, BlackEnergy), la sécurité est devenue une des principales préoccupations des industriels. En 2010, Stuxnet (introduit probablement par une clef USB corrompue) avait réellement ralenti le programme nucléaire iranien d'enrichissement de l'uranium par un dérèglement du contrôle des centrifugeuses. Dès 2011, le groupe DragonFly (connu sous le nom de Energetic Bear) visait plus particulièrement des entreprises de défense et d'aviation aux Etats-Unis et au Canada, mais à des fins d'espionnage. En 2013, DragonFly cibla les domaines de l'énergie en Europe également. En 2015, mais plus fortement en décembre 2016, BlackEnergy a privé d'électricité, durant une heure, une partie de la ville de Kiev en Ukraine.

Les parades sont complexes, tel, par exemple, l'isolation du réseau de l'environnement SCADA au sein des infrastructures, la dissociation des systèmes homme-machine vis-à-vis des automates et dispositifs de mesure, des systèmes de supervision, des unités de contrôle à distance. Les systèmes SCADA doivent être traités comme des SI à part entière en fonction de leur sensibilité.

Les systèmes SCADA sont principalement répandus dans l'entreprise, mais sont aujourd'hui également présents chez les particuliers (par exemple, avec les compteurs communicants). Chez ces derniers, en cas d'attaque, il pourrait y avoir des dénis de service, une utilisation malveillante des données prélevées sur les compteurs communicants, sans oublier les bornes de recharge des véhicules électriques, l'équipement domotique, etc. en relation directe avec le mode de vie des personnes. Dans le cas d'un laboratoire de recherche, les appareils de mesure, les stations d'analyse, sont en communication via des réseaux informatiques internes, mais sont aussi en relation avec d'autres types de réseaux informatiques pour la validation des jetons d'utilisation d'une application, par exemple.

Récemment, en 2017, la société ESET® a mis en évidence l'existence d'un logiciel malveillant et très dangereux car conçu pour perturber les processus des infrastructures critiques, qu'elle a nommé Win32/Industroyer. Il peut parfaitement persister dans le système et interférer directement avec le fonctionnement du matériel industriel, par exemple, capable d'attaquer l'alimentation électrique d'une infrastructure de fournisseur d'énergie. Son caractère modulaire en fait une menace redoutable. Pour parvenir à ses fins, il se sert des différents protocoles de communication utilisés par les infrastructures d'alimentation électrique, les systèmes de contrôle du transport, etc. Ainsi il est possible d'arrêter la distribution d'électricité, de déclencher des pannes de fonctionnement de machines-outils, de provoquer des dégâts importants aux équipements industriels.

La protection des données

Les chercheurs doivent avoir une stratégie de protection de leurs savoirs et savoir-faire. Les mesures de sécurité adoptées ne doivent pas entraver la recherche et la compétitivité du laboratoire. Elles doivent être pragmatiques, cohérentes et applicables. Le sécuritaire sans discernement est contre-productif. Le challenge est donc de trouver un équilibre entre la dissémination des connaissances, les échanges et coopérations internationales d'un côté et les contraintes de la protection de l'autre [15-16].

Au-delà des raisons historiques, le chiffre a été longtemps interdit, puis réglementé en France. Aujourd'hui, le chiffre n'est pas encore assez utilisé. Il y a encore peu de prise de conscience des vulnérabilités, mais cette situation évolue. Les systèmes de chiffrement peuvent cependant faire l'objet d'un agrément par les services de l'état.

Dans un autre contexte, si un rapport d'avancement de projet doit demeurer intègre, donc non modifiable par des tiers non autorisés, la protection est assurée par signature électronique. Pour la non-répudiation d'un message, il convient d'utiliser un système basé sur la signature pour l'expéditeur et l'accusé de réception pour le destinataire. Pour valider l'authentification de documents, l'usage de certificats numériques et de tiers de confiance est une solution. En effet les certificats numériques servent à prouver que la clef utilisée par une machine, par exemple, est bien celle de l'utilisateur à laquelle elle est associée.

Ainsi, les utilisateurs sont acteurs de la protection. Ils veillent à la sécurisation de leur poste de travail et des moyens nomades mis à leur disposition. Parmi les mesures simples, ils peuvent utiliser des mots de passe plus robustes que le simple prénom d'un proche. L'idéal serait un mot de passe différent pour

chaque application, chaque accès réseau ou encore le verrouillage du poste de travail. Cela reste difficile à réaliser dans notre vie quotidienne. Il est souvent recommandé de choisir des mots de passe assez long de plus de 10 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux). Mais aujourd'hui la tendance est l'utilisation d'une phrase de passe au lieu d'un mot de passe. Ces phrases sont composées de mots disposés les uns à la suite des autres, ne provenant pas d'un proverbe connu, sans lien direct avec soi (noms, naissance, etc.) et sans logique exploitable. Les mots de passe constituant eux-mêmes des données personnelles et confidentielles, ils ne doivent pas être divulgués ni laissés sans protection. Au vu des limites de l'utilisation des mots de passe, il existe d'autres solutions comme l'usage de la biométrie ou encore l'OTP (*One Time Password*) générant un mot de passe utilisable une seule fois, donc « jetable ».

La Charte de l'utilisateur des ressources informatiques et des services réseaux, régit les pratiques informatiques des utilisateurs. Si ces derniers la signe sans la lire ni l'appliquer, elle constituera, en cas de problème, un document opposable au signataire. Pour assurer un bon niveau de sécurité, le comportement responsable du personnel est prépondérant. L'utilisation de supports comme les clefs USB doit être menée avec discernement. Pour transporter des données sensibles, l'utilisation de clefs cryptées, constitue une bonne solution. Dans tous les cas, la séparation entre les données personnelles et professionnelles doit être assurée.

En dehors du laboratoire, il faut être encore plus vigilant et n'utiliser que des communications sécurisées de type SSH, IMAPS, ou HTTPS pour des échanges professionnels. Cependant, même pour des communications personnelles, il faut être attentif aux éventuelles demandes de mise à jour de logiciels durant l'utilisation des bornes Wi-Fi de sites extérieurs, tels les hôtels, par exemple. Ces demandes peuvent masquer une éventuelle prise de contrôle de la machine pour accéder à son contenu.

Au sein d'un laboratoire, la mise en place d'une politique de sécurité des systèmes d'information (PSSI) permet de dégager des propositions et des recommandations en évaluant les impacts en fonction des conditions locales de cohabitation avec d'autres organismes et de leurs propres politiques. Elle tient compte des aspects légaux et réglementaires sur la protection des personnes et des données personnelles, la délocalisation des *datacenters*, les obligations de notification des failles et incidents de sécurité, etc.

Conclusion et perspectives

En cette période de transition numérique importante, de dématérialisation et d'hébergement de données dans des systèmes virtualisés, il est nécessaire de se doter de moyens pertinents et d'adapter la sécurité des systèmes d'information à l'évolution des métiers et des nouvelles menaces. En effet, les spécialistes font état d'un développement des techniques offensives et une diminution certaine de l'efficacité des moyens défensifs qui va en s'amplifiant. Il est établi que les actions de renseignement (laboratoires, industriels nationaux ou étrangers) ont tendance à se concentrer vers le monde de la recherche. Dans les laboratoires, le manque de décision est parfois dû à des budgets étriqués, à des choix à effectuer, à des dénis de la réalité, etc. Cependant, la protection doit être une préoccupation majeure et constante. De plus suivant les domaines de recherche et les effectifs, la politique de SSI devrait parfois intégrer l'intelligence économique afin d'anticiper et de prévenir le risque [17-18]. La sécurité n'est jamais acquise définitivement, elle est évolutive.

Un petit nombre de mesures pragmatiques, applicables et respectées est préférable à pas de mesure du tout ou à une politique totalement obscure et mal expliquée. La sensibilisation et la formation à la protection des informations sont essentielles. La communication et le dialogue, les démonstrations *in-situ*, l'implication de tous les acteurs sont nécessaires pour trouver les actions efficaces avec le minimum de contrainte. Les membres d'un laboratoire sont tous concernés, ils sont partie prenante de la valorisation des travaux de recherche.

Bibliographie

[1] J.-L. Archimbaud, F. Berthoud, T. Dostes, M. Libes, N. Neyroud, J. Prévost, A. Rivet, Le Système d'Information dans un laboratoire de recherche : Guide de spécification des services, JRES, Strasbourg, 20-23 novembre 2007.
[2] La sécurité des SI, un enjeu majeur pour la France :
http://www.ladocumentationfrancaise.fr/rapports-publics/064000048/index.shtml
[3] La sécurité globale: réalités, enjeux et perspectives, sous la direction de Jacques Roujansky, SEE, Paris: CNRS Editions, 2009.
[4] J.-F. Pillou, P. Caillerez, Tout sur les systèmes d'information (Grandes, moyennes et petites entreprises), Collection "Commentcamarche.net", Paris, Dunod, 3ème édition, Février 2016
[5] P. Rascagneres, Sécurité informatique et Malwares. Analyse des menaces et mise en œuvre des contre-mesures, ENI Editions, Avril 2016
[6] Ph. Trouchaud,La Cybersécurité au-delà de la technologie, Odile Jacob, Février 2016
[7] L'actualité des systèmes d'information hospitaliers et de la e-santé :
http://www.dsih.fr/article/2492/rancongiciel-propagation-massive-et-mondiale-l-anssi-sonne-l-alerte.html
[8] V. Bensoussan-Brulé,Ch. Torres, Failles de sécurité et violation des données personnelles, Coll. Lexing - Technologies & Droit, Larcier, Juillet 2016
[9] C. Erhel, L. de La Raudière, Rapport d'information déposé par la commission des affaires économiques sur les objets connectés, n°4362, enregistré à la Présidence de l'Assemblée nationale le 10 janvier 2017
[10] Ph. Wolf, Internet of Everything et sécurité, REE n°2, 2017, p.78-88
[11] La sécurité de l'Internet des objets : https://cesin.fr/uploads/publications-documents/5145e4f18c2b57563045969d510af967021c6732.pdf
[12] La sécurité de l'Internet des Objets, Livre blanc, Digital Security Econocom, OSIDO, juillet-août 2016.
[13] Y. Roudier, T. Tanzi, A State of the Art of Drone (In)Security, Journées scientifiques URSI-France, Radio Science for Humanity, 1-3 février 2017, Sophia Antipolis
http://webistem.com/ursi-f2017/output_directory/cd1/data/articles/000023.pdf
[14] Maîtriser la SSI pour les systèmes industriels, ANSSI, juin 2012.
[15] J.-F. Carpentier, La Sécurité informatique dans la petite entreprise. Etat de l'art et Bonnes Pratiques, ENI Editions, Janvier 2016
[16] A. Fernandez-Toro, Sécurité opérationnelle. Conseils pratiques pour sécuriser le SI, Eyrolles, Avril 2015
[17] Pôles de compétitivité et intelligence économique, J.-P. Damiano, Techniques de l'ingénieur, octobre 2009, AG 1610 et Doc AG1610 v2, http://www.techniques-ingenieur.fr/book/ag1610/poles-de-competitivite-et-intelligence-economique.html
[18] Sécurité Economique et Compétitivité des Entreprises en Méditerranée (SECEM) Magazine, Dossier spécial Intelligence économique, n°7, Janvier - Mars 2016

Pour en savoir plus :

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : http://www.ssi.gouv.fr/
- Bulletins du Computer Emergency Response Team (CERT-FR) du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques : http://www.cert.ssi.gouv.fr/
- Club de la Sécurité de l'Information Français (CLUSIF) : https://clusif.fr/
- Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) : https://cesin.fr/
- Club Informatique des Grandes Entreprises Françaises (CIGREF) : http://www.cigref.fr/
- CyberEdu (initié par l'ANSSI) - La sécurité par l'enseignement supérieur des nouvelles technologies de l'information et de la communication : https://www.cyberedu.fr/
- CYBERSURVEILLANCE.GOUV.FR : Assistance et Prévention du risque numérique : https://www.cybermalveillance.gouv.fr/
- Les Journées RESeaux (JRES) / enseignement supérieur et de la recherche : https://www.jres.org/
- Observatoire de la Sécurité de l'Internet des Objets (OSIDO) : https://www.digitalsecurity.fr/fr/
- Observatoire de la Sécurité des Systèmes d'Information et des Réseaux (OSSIR) : https://www.ossir.org/
- Vigi@net : Vigilance pour internet et les systèmes d'information / La lettre SSI du Haut Fonctionnaire de Défense et de sécurité : https://www.pleiade.education.fr
- Wikipedia : https://fr.wikipedia.org/