Les laboratoires de recherche et la sécurité numérique

Jean-Pierre Damiano

Les laboratoires de recherche et la sécurité numérique

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

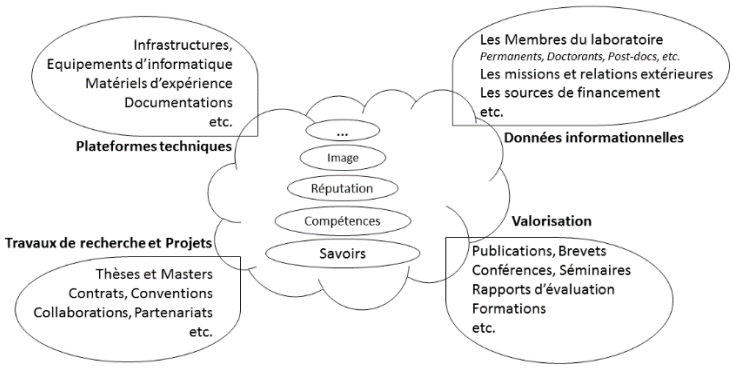
Introduction

Qu'ils soient publics (rattachés à des services de l'état, universités, etc.) ou privés (affiliés à des industries), les laboratoires de recherche évoluent au sein d'un environnement complexe. Ils sont confrontés à une compétition scientifique en expansion. Quotidiennement 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 membres du laboratoire (missions, par exemple), le contenu des courriels, sont échangées sur les réseaux de communication. Une partie de ces informations peut être considérée comme stratégique et sensible : c'est la part qui participe à la création de savoirs et savoir-faire innovants conditionnant la pérennité de la recherche (synthèse des travaux des doctorants, publications novatrices, dépôts de brevet, missions, partenariats, contrats en cours, etc.). Tout le personnel du laboratoire est concerné par la protection de ce gisement informationnel le plus souvent numérique et par la constitution d'un climat de confiance vis-à-vis des partenaires extérieurs, qu'ils soient académiques ou industriels.

Le potentiel scientifique et technique

Le potentiel scientifique et technique d'un laboratoire, se définit comme l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée, au développement technologique. Ainsi, au-delà du personnel qui le compose, il comprend le plus souvent les équipements, les matériels d'expérience, les bases de données, les savoirs et savoir-faire, les travaux de recherche et d'expérience en cours et futurs, les brevets en cours de dépôt, la réputation, l'image du laboratoire, etc. Les atteintes à ce potentiel 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 du potentiel scientifique et technique (PPST) revêt un caractère stratégique. Elle concerne tous les acteurs de la recherche. Car, quel que soit son domaine d'activité, cette production intellectuelle est une source de convoitise de la part de divers concurrents (laboratoires ou industriels). L'essentiel du capital informationnel d'un laboratoire est dématérialisé. Il est vraiment indispensable de le protéger et d'en permettre l'accès aux différentes personnes habilitées.



Potentiel scientifique et technique d'un laboratoire de recherches

La politique de sécurité des systèmes d'information

Les systèmes d'information (SI), au sens large, présentent des vulnérabilités (qu'elles soient d'ordre structurel, organisationnel, physique, informatique ou humaine, etc.). Les conséquences de leur exploitation malveillante 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, sans oublier les règles de droit, doivent donc être simples mais pragmatiques pour constituer une réponse appropriée et acceptée par tous les acteurs de la recherche.

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.). 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.

Ainsi il convient d'identifier ce qui doit être protégé, de quantifier les enjeux, de définir les objectifs de sécurité et d'élaborer une politique de sécurité des systèmes d'information (PSSI). Cependant un tel plan d'actions conduit à des règles qui ne doivent pas entraver la recherche, la compétitivité, les échanges et les coopérations nationales et internationales, le dépôt de brevets, les publications, les congrès, etc.

La sensibilisation et la formation des membres du laboratoire aux enjeux de la sécurité sont indispensables et conduisent à la mise en œuvre de pratiques et d'outils juridiques appropriés.

Pour atteindre ces objectifs de sécurité, des mesures sont mises en œuvre en tenant compte des critères :

- 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, ou d'une machine par exemple, 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.

La mise en place d'une stratégie d'intelligence économique (IE) peut être un atout véritable de l'enjeu de protection des systèmes d'information pour les laboratoires de recherche publics ou privés. Mais elle nécessite une véritable adhésion de la direction pour qu'elle soit efficace avec le soutien de l'ensemble des personnels.

A consulter

- J.-P. Damiano, Potentiel scientifique et technique d'un laboratoire. Favoriser l'innovation, protéger les savoirs : un équilibre délicat, *Revue de l'Electricité et de l'Electronique (REE)* Dossier 2, URSI, n°5, pp.85-92, décembre 2017. https://hal.archives-ouvertes.fr/hal-01633310v2
- J.-P. Damiano. Pôles de compétitivité et intelligence économique. *Techniques de l'Ingénieur*, 2009, p. AG 1610/1-8, Doc AG 1 1610/1-5. https://hal.archives-ouvertes.fr/hal-00519286

Conseils de sécurité

Préambule

D'après une analyse menée par le Centre de Cyberdéfense, composante du Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI-ANSSI), les principales lacunes de sécurité constatées sont :

- Des systèmes, des applications y compris les sites *web*, qui ne sont pas mis à jour de leurs correctifs de sécurité
- Une politique de gestion des mots de passe insuffisante
- Une absence de séparation des usages entre utilisateur et administrateur des réseaux
- Un laxisme manifeste dans la gestion des droits d'accès

- Une ouverture excessive d'accès externes incontrôlés au système d'information (nomadisme, télétravail ou télé administration des systèmes)
- Une absence de restrictions d'accès aux périphériques (supports USB, etc.)
- Une absence de surveillance des systèmes d'information (analyse des journaux réseaux et de sécurité)
- Un cloisonnement insuffisant des systèmes qui permet à une attaque de se propager au sein des réseaux
- Une sensibilisation et une maturité insuffisantes des utilisateurs et des dirigeants face à la menace dont ils ne perçoivent pas les risques.

L'essentiel de la production scientifique d'un laboratoire est dématérialisé, stocké sous forme de fichiers ou de bases de données, sur des serveurs locaux ou distants. Il est indispensable de les protéger et d'en permettre l'accès aux différentes personnes habilitées. Ceci a des implications sur les procédures opérationnelles, les moyens financiers mis à disposition sans oublier, évidemment, une formation spécifique des utilisateurs et quelques contraintes. Tous les membres du laboratoire ont un rôle important à jouer dans la sécurité du SI.

Sommaire :

Les mots de passe

Les mots de passe sont utilisés pour donner les droits d'accès aux équipements informatiques. Il est indispensable de suivre quelques règles simples dans ce domaine :

- Configurez les objets nomades communicants (ordinateur, tablette, *smartphone*, etc.) pour limiter le nombre de tentatives erronées d'entrée du mot de passe quand cela est possible.
- Activez le verrouillage automatique après quelques minutes d'inactivité avec entrée d'un mot de passe pour réactiver la session.
- N'enregistrez pas les mots de passe dans les applications ou les logiciels concernés.
- Évitez de stocker les mots de passe sur un support accessible par un tiers.
- Utilisez si nécessaire un gestionnaire de mot de passe, avec stockage local et des moyens cryptographiques forts.
- Ne communiquez jamais le mot de passe en réponse à quelque sollicitation que ce soit, même de la part de vos collègues ou de vos administrateurs.
- Prévoyez une double authentification lors de l'utilisation de logiciels ou d'applications présents dans un serveur de type *Cloud*.
- Evitez l'usage d'un même mot de passe sur plusieurs systèmes ; éviter des logins mutualisés
- Il était souvent recommandé de choisir des mots de passe assez long de plus de 10 caractères de type différent (majuscules, minuscules, chiffres, etc.). Aujourd'hui la tendance est l'utilisation d'une phrase de passe composée de mots disposés les uns à la suite des autres, ne provenant pas d'un proverbe connu, sans lien direct avec soi-même (noms, lieux, etc.) et sans logique exploitable.
- L'importance est la période entre deux changements du mot de passe. Elle définit directement le délai de cassage possible de ce mot de passe. Une phrase de 20 caractères alphabétiques demandera des centaines d'années à être dévoilée, de même qu'un seul de mot de 12 caractères alphanumériques : mais la première est plus facile à se souvenir donc plus facilement changeable.

Les systèmes d'exploitation, les logiciels, les applications et leur mise à jour

La notion de sécurité informatique est par nature évolutive. Le champ des menaces évolue, il en est de même des protections. Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows, etc.), dans chaque logiciel (navigateur, bureautique, antivirus, etc.) ou application, des vulnérabilités (failles) existent. Elles sont exploitables et souvent exploitées par les attaquants pour mener à bien leurs opérations de déni de service, par exemple, parfois longtemps après leur découverte et leur correction. Aussi la mise à jour de sécurité est nécessaire et vivement recommandée.

- Utilisez les sites internet officiels des éditeurs et désactiver les cases proposant d'installer des logiciels complémentaires. Suivez les consignes du responsable informatique.
- Une suite de sécurité antivirus à jour est importante, mais les dernières attaques montrent que cela est nécessaire mais pas toujours suffisant.
- N'installez que les applications utiles et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques, etc.).
- Détruisez les fichiers inutiles, temporaires, etc.
- Mettez une marque de propriété sur les documents créés (textes, images, etc.)

Les accès réseaux et équipements

Pour chaque équipement communicant, il convient de respecter la charte informatique et les règles de sécurité applicables du système d'information. Ainsi l'identification précise des utilisateurs et de leurs privilèges est vivement recommandée. Tous ne peuvent pas bénéficier de droits d'administrateur.

- Sécurisez les postes de travail, les serveurs, le réseau et les accès aux locaux. Il faut être conscient qu'un accès physique sur vos ordinateurs permet de s'en rendre maître. Seul un chiffrement intégral permet de limiter ces accès.
- Utilisez des communications chiffrées avec : SSL (Secure Socket Layer) ; VPN (Virtual Private Network) ; TLS (Transport Layer Security) ; SSH (Secure Shell) ; IMAPs: SSL version sécurisée de Internet Message Access Protocol (IMAP) ; HTTPs (Secure HyperText Transfer Protocol) ; SFTP (Secure FTP), etc.
- Suivez les procédures précises pour les arrivées et les départs des personnels non-permanents (stagiaires, visiteurs, etc.) concernant les contrôles d'accès aux réseaux, les privilèges, les mises à jour des logiciels et applications, etc.
- Dans le cadre du laboratoire, l'accès à Internet par un point d'accès Wi-Fi est à éviter généralement : une installation filaire reste plus sécurisée et plus performante. Si le Wi-Fi reste le seul moyen d'accès, il convient de paramétrer la borne d'accès avec des protocoles d'authentification de type WPA2 AES, et bientôt le protocole WPA3 (fonctionnement avec 192 bits) nettement plus sûr et mieux adapté aux petits objets communicants.
- Surveillez les bornes déployées dans les locaux du laboratoire.
- Evitez de partager la connexion Wi-Fi.
- Désactivez la borne d'accès Wi-Fi lorsqu'elle n'est pas utilisée quand cela est possible.
- Identifiez qui peut accéder à vos fichiers et gérer vos droits d'accès. Vos fichiers sensibles (confidentiels) ne doivent pas être accessibles sur vos ordinateurs ou sur des clefs USB sans protection ou autres objets communicants. Ceci implique notamment de chiffrer ces documents et de restreindre leur accès.
- Evitez d'utiliser un objet nomade pour se connecter aux réseaux professionnels, sinon il se trouve dans la PSSI du laboratoire et doit répondre aux critères de sécurité avant toute utilisation. En cas de vol ou de perte, il faudra prévenir votre responsable informatique pour qu'il prenne toutes les mesures conservatoires nécessaires.
- Ne pas utilisez un compte administrateur pour naviguer sur Internet.
- Verrouillez la session en cas d'absence.
- Ne faites pas transiter des données personnelles ou professionnelles sensibles.
- N'utilisez pas les bornes publiques pour des raisons de sécurité et de confidentialité.

Les sauvegardes régulières

Un système de sauvegarde est un élément obligatoire dans une politique de sécurité, c'est une condition de la continuité de l'activité suite à un dysfonctionnement ou attaque.

- Effectuez régulièrement des sauvegardes à partir d'un poste de travail sûr. Elles doivent être chiffrées et testées. Une copie doit être externalisée.
- Effectuez cette tâche sur des supports (disque dur amovible, clef USB, etc.) hors connexion *web*, en ayant conscience de leur durée de vie. L'utilisation de plateformes de stockage de type *Cloud* comporte des risques de perte de confidentialité (ou de disponibilité ou encore d'intégrité), des risques juridiques liés aux contrats proposés et à l'incertitude sur la localisation de tels sites.
- Utilisez aussi des sites de stockage recommandés par les administrations de tutelle.
- Avant un échange de matériel, réalisez une remise à zéro complète réelle, détruisez l'ancien disque dur et autre composant de stockage, mettez un support neuf.
- Dans le cas des objets communicants nomades et de tout matériel informatique, notez les identifiants comme le numéro de téléphone, le numéro de la carte SIM, le code IMEI (International Mobile Equipment Identity), le numéro MAC le cas échéant. Cela servira à bloquer l'usage de l'objet en cas de vol.

L'utilisation des messageries électroniques

Les courriels et les pièces jointes éventuelles jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.). Voici quelques conseils à suivre :

- Sauvegardez vos courriels importants.
- L'identité d'un expéditeur n'étant en rien garantie, il est nécessaire de vérifier la cohérence entre l'expéditeur présumé et le contenu du message.
- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.
- Ne relayez jamais des canulars ou des messages de type chaînes de lettres : risque d'induire des confusions et de saturer les réseaux.
- Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles peuvent comporter des codes malveillants. N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts connus. N'ouvrez pas des pièces jointes avec les extensions de type .pif, .com, .bat, .exe, .vbs, .lnk, par exemple.
- Utilisez l'envoi de pièces jointes avec des formats non explicites. Il ne faut pas faire confiance instinctivement au nom d'un expéditeur apparemment connu.
- Ne cliquez pas trop vite sur des liens : passez la souris sur le lien concerné sans l'activer pour examiner l'adresse *web* proposée. Copiez cette adresse du site dans un bloc-notes, puis fermez le service de messagerie et le navigateur. Activez à nouveau le navigateur et collez l'adresse dans la fenêtre appropriée.

La protection des équipements, des données, des informations personnelles et professionnelles

Dans le cas de déplacements professionnels, il est indispensable de suivre les consignes de l'ANSSI. Celles-ci sont aussi valables pour des voyages personnels. L'emploi d'ordinateurs portables, *smartphones* ou de tablettes, de tout autre objet communicant, facilite les déplacements professionnels ainsi que le transport et l'échange de données, mais nécessite une vigilance certaine.

Voyager avec ces équipements nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte aurait des conséquences importantes sur les activités du laboratoire. Il ne faut pas les laisser sans surveillance (surtout dans les transports, les halls de gare et d'aéroport). Il est utile de mettre un signe distinctif et d'éviter les échanges volontaires ou involontaires.

La séparation des usages personnels et professionnels est vraiment nécessaire bien que l'utilisation d'un même équipement à titre professionnel et personnel soit une pratique assez suivie. Cependant, elle pose des problèmes de sécurité des données (vol ou perte des objets nomades, intrusions, manque de contrôle, etc.).

- Ne faites pas suivre les messages électroniques professionnels sur des services de messagerie utilisés à titre personnel.
- N'hébergez pas de données professionnelles sur vos équipements personnels ou sur des serveurs de stockage en ligne non autorisés.
- Evitez de connecter des supports amovibles personnels (objets communicants, clés USB, disques durs externes, etc.) aux ordinateurs du laboratoire.

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel. Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet, par exemple à travers des formulaires que vous êtes amenés à remplir.

- Lors de l'usage de réseaux sociaux, ne divulguez pas d'informations précises sur votre activité professionnelle et sur votre identité personnelle.
- Fermez le navigateur après avoir consulté vos comptes bancaires ou tout autre service *web* impliquant votre identité personnelle.
- Soyez vigilant sur la géolocalisation.
- Désactivez par défaut les composants ActiveX et JavaScript susceptibles de présenter des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable.

Le 28 janvier 2018, le Conseil de l'Europe a célébré la Journée internationale de la protection des données, consacrée à la promotion et à la sensibilisation aux meilleures pratiques en matière de protection des données et de la vie privée (https://www.coe.int/fr/web/data-protection/home). C'est le point de départ d'une année dédiée avec l'entrée en vigueur le 25 mai 2018, du Règlement Général sur la Protection des Données (RGPD) relatif à la protection des données en Europe, avec de profondes implications pour les entreprises hors d'Europe, qui traitent des données sur les Européens ou qui exploitent des établissements et des centres de données européens.

Ce règlement est le seul instrument juridique international contraignant dans le domaine, de portée potentiellement mondiale. Il est prévu que chaque personne aura le droit d'accéder aux données détenues par une organisation, de les rectifier, de demander leur suppression et de les transférer à une structure concurrente. Il faut savoir que les données concernées sont tout aussi bien les finances que la santé, mais également les adresses IP, un numéro de téléphone ou un cookie. Il s'agira de les rendre difficilement identifiables.

Le chiffrement

D'une part, il faut savoir ce que l'on veut protéger et comment le réaliser. Il est donc nécessaire de définir les données sensibles concernées (établir une classification de sensibilité, les données destinées à être externalisées, les postes nomades, les contrats de sous-traitances, etc.).

Et d'autre part, il est nécessaire d'apprendre à utiliser le chiffrement en fonction des besoins définis, en suivant les préconisations des tutelles. En effet, suivant les possibilités et les moyens à mettre en œuvre, on choisit des solutions de chiffrement, en prenant soin de la gestion des clefs si nécessaire :

- Les conteneurs : une partition ou un fichier, l'outil s'occupe de chiffrer tout ce qui est écrit dans les dossiers vers le conteneur, avec le risque de données oubliées hors zone chiffrée, etc.
- Le chiffrement de surface : chiffrement du disque par le système ou tiers, les données sont accessibles après le démarrage. Peu de problème de performance, et peut être effectué en général après l'installation du système (sauf Linux)
- Les communications réseaux : protocoles pour accès distant chiffré (ssh, ssl, https, vpn, etc.).

En effet, des risques demeurent comme la panne de disque, la perte des clefs, l'oubli d'un mot de passe, un effacement accidentel ou volontaire ou même un remplacement par l'utilisateur. Outre les sauvegardes, il est indispensable de définir des procédures de récupération des clefs de chiffrement, de prévoir une méthode de séquestre (mots de passe, etc.) dans un coffre-fort physique ou électronique. Ainsi, la sauvegarde régulière des données est indispensable évidemment. Il existe des solutions de sauvegarde incluant un logiciel chiffrant.

La priorité peut être mise sur les ordinateurs portables et les supports de stockage amovibles qui, par définition, sont amenés à sortir des locaux du laboratoire.

Les ordinateurs portables neufs doivent, dans la mesure du possible, être achetés avec un disque chiffrant sinon des solutions logicielles existent (référencées par l'ANSSI, par exemple : TrueCrypt 7.1a (développement arrêté), Cryhod, Zed !, ZoneCentral, etc.).

La Commission Nationale de l'Informatique et des Libertés (CNIL) recommande fortement de protéger des informations personnelles et professionnelles confidentielles stockées sur ordinateur, supports amovibles ou sur les serveurs de stockage en ligne. La CNIL cite divers outils de chiffrement comme AxCrypt ou Zed !

Les antivirus, les antimalwares, etc.

Les antivirus doivent être configurés de manière à télécharger automatiquement les nouvelles signatures de la base virale. Ils sont efficaces dans la plupart des cas, aujourd'hui, mais ce ne sont pas des parades absolues !

- Ils doivent demeurés actifs
- Effectuez des analyses complètes de manière périodique
- Analysez automatiquement les nouveaux périphériques (supports amovibles, clés USB, etc.), sans oublier les courriels et la messagerie instantanée.

L'ANSSI est favorable à l'usage d'un antivirus pour le grand public, mais elle met en garde les structures travaillant dans des domaines sensibles. En effet, il faut savoir qu'un antivirus est un logiciel disposant de droits particuliers lui permettant d'accéder à toute l'information numérique de la machine et donc pouvant la transmettre facilement à son centre d'édition. Un antivirus est une cible privilégiée des attaquants dans le but d'en prendre le contrôle. Aucun n'a fait l'objet d'une démarche de qualification de la part de l'ANSSI pour être considéré comme un véritable produit de confiance. Il en est de même des antimalwares.

Pour approfondir

- 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/
- Commission nationale de l'informatique et des libertés (CNIL) : https://www.cnil.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