www.ac-rennes.fr

académie Rennes
Éducation nationale

Service informatique académique [SERIA]

Memento SSI

Sécurité des systèmes d'information

à l'usage du chef d'établissement

1/ Qu'est-ce que la Sécurité des Systèmes d'Information [SSI] en EPLE ?

Le Système d'Information de l'établissement scolaire représente l'ensemble des éléments participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein de l'établissement. La sécurité du SI de l'établissement comprend donc :

- la sécurité des infrastructures
- la sécurité des données
- la sécurité des usagers

En raison du caractère stratégique des SI dans l'éducation nationale (les pannes ou les incidents peuvent entraver gravement le fonctionnement du système éducatif), de la nature et du nombre des menaces qui pèsent sur eux, le ministère a décidé d'élaborer un **Schéma Directeur de la Sécurité des Systèmes d'Information**, qui définit des objectifs qualitatifs et quantitatifs à atteindre pour parvenir à l'équilibre optimal entre besoins d'usage et niveau de protection.

Dans le cadre de la mise en œuvre de ce Schéma Directeur, l'académie de Rennes s'est engagée dans un plan triennal qui inclut la dimension EPLE.

La SSI en EPLE s'articule autour de principes, de règles et de procédures qui relèvent de l'établissement. Il devra les organiser en définissant une politique locale SSI. Cette politique doit couvrir plusieurs domaines :

- l'organisation de l'information liée à la SSI au sein de l'établissement ;
- l'organisation d'une chaîne d'alerte en lien avec le niveau académique ;
- la définition des droits et des devoirs de chacun (chartes d'usage) ;
- la responsabilisation de la communauté éducative ;
- la mise en place de procédures de gestion d'incident, et notamment un plan de secours en cas d'incident majeur.

En pratique

La désignation d'un correspondant SSI, susceptible d'aider et de conseiller le chef d'établissement, est recommandée ; les correspondants, qui ne sont pas nécessairement des techniciens, reçoivent une formation d'une journée chaque année et disposent d'un accès privilégié à l'espace SSI académique sur http://www.ac-rennes.fr/ssi .

La mise en place d'une politique SSI au sein des établissements est avant tout une **question d'organisation** ; pour commencer, nous incitons les chefs d'établissement à mettre en place une structure expérimentale dans un premier temps, qui rassemblera les principaux acteurs de l'établissement et qui pourra se réunir une fois par trimestre par exemple. Cette structure pourra être chargée d'organiser par ordre de priorité :

1 - la diffusion des documents et des informations importantes (chartes, notes, alertes) ;
2 - l'activation de la chaîne d'alerte en cas d'incident (ce qui suppose une information préalable des personnels) ;
3 - des réunions de sensibilisation à destination des personnels, notamment des enseignants, en leur suggérant, dans le cadre du B2i par exemple, de travailler sur quelques questions liées à la SSI avec leurs élèves ; les fiches disponibles sur l'espace SSI constituent des ressources utiles tant pour les personnels que pour les élèves ;
4 - la vérification du bon usage des ressources informatiques de l'établissement, notamment à travers les traces de connexions.

Se lancer dans la mise en œuvre d'une politique de SSI passe par la mobilisation de compétences internes à l'établissement. En fonction de ses moyens, chaque établissement fixe ses objectifs : sensibilisation, contrôle des traces de connexion, suivi de la politique, bilan annuel SSI, etc.

La présence d'un correspondant "SSI" contribue à l'atteinte de ces objectifs.

Si vous souhaitez obtenir de l'aide ou des conseils dans la mise en place d'une politique locale de SSI :

- consultez l'espace SSI académique http://www.ac-rennes.fr/ssi ;
- contactez le SERIA

2/ Quels sont les droits et les devoirs de chacun ?

Présentation

L'observation des règles commence par le respect des lois que nul n'est censé ignorer. Tout utilisateur de l'établissement est tenu de respecter la législation en vigueur. Par exemple, si dans l'accomplissement de son travail un utilisateur est amené à constituer des "fichiers nominatifs" relevant de la loi "Informatique et Libertés", il devra auparavant faire une demande d'autorisation, sous couvert du chef d'établissement.

Les enjeux

Les lois et les règles, mêmes si elles peuvent par moment nous paraître contraignantes, sont faites pour nous protéger collectivement ; ne pas les respecter, c'est s'exposer, et c'est exposer les autres à des dangers que l'on ne soupçonne pas toujours, sans oublier le risque de poursuites civiles ou pénales dont on peut faire l'objet. Il est donc important d'être bien informé sur les textes qui encadrent l'usage de l'informatique et des réseaux de communications électroniques.

Les recommandations

ATTENTION aux téléchargements effectués depuis Internet. En plus des virus et autres logiciels malveillants que vous pouvez ainsi introduire sur le réseau de l'établissement, vous risquez d'enfreindre les lois sur la propriété intellectuelle.

ATTENTION à l'introduction de toute application informatique qui manipulerait des données nominatives ; la loi informatique et libertés encadre strictement l'utilisation des traitements de données à caractère personnel.

Veillez à utiliser les ressources informatiques de votre établissement dans le respect des missions de l'Éducation nationale. Ne vous exposez pas à des poursuites ou à des sanctions.

En savoir plus

- la loi du 6/1/78 dite "informatique et libertés" voir le site de la CNIL www.cnil.fr ;
- la loi du 5/1/88 relative à la fraude informatique, complétée par la loi du 22/7/92 dite "loi Godfrain" http://legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19880106&pageDebut=00231 ;
- la législation relative à la propriété intellectuelle - voir http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414&dateTexte=20080529 ; en particulier la loi DADVSI "Droit d'Auteur et Droits Voisins dans la Société de l'Information" http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000266350 ;
- l'article 8 du code civil http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&dateTexte=20080529 et l'article 9 de la convention européenne des droits de l'homme http://lexinter.net/UE/convention_europeenne_des_droits_de_l'homme.htm qui protègent la vie privée et le secret des correspondances ;
- la loi du 29 juillet 1881 sur la liberté de la presse, et plus particulièrement sa version consolidée le 19 avril 2006 (qui traite aussi des crimes et délits commis au moyen d'un système de publication électronique) http://www.legifrance.gouv.fr/texteconsolide/PCEAA.htm ;
- la législation applicable en matière de cryptologie www.ssi.gouv.fr ;
- la loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0200175L .

En pratique

A - Chartes

Si la **charte d'usage "élève"**, annexée au règlement intérieur de l'établissement et approuvée en conseil d'administration (CA), peut revêtir une valeur juridique contraignante au sens du décret du 30 août 1985, la signature de l'élève mineur ne constitue, en raison de son âge, qu'un engagement moral, dont les manquements sont toutefois exposés aux sanctions prévues au règlement intérieur.

Il est vivement conseillé de mettre en place également des chartes "personnel" et "administrateur réseau", en s'appuyant par exemple sur la métacharte de l'Éducation nationale de février 2007.

B - Vie privée résiduelle et secret des correspondances

On sera particulièrement attentif à l'usage des logiciels de surveillance et d'écoute discrètes (de type UltraVNC) qui, s'ils ne posent pas de problème en classe dans un cadre pédagogique par exemple, sont susceptibles de porter atteinte à la vie privée des personnes et en particulier au secret des correspondances. **Leur usage sur des postes en autonomie, au CDI par exemple, devra être proscrit**. De même, les dispositifs destinés à faciliter la gestion du parc informatique ou la détection d'activités suspectes, ne doivent pas porter atteinte au droit à la vie privée résiduelle.

C - Vidéosurveillance

L'implantation de dispositifs de vidéosurveillance dans des lieux qualifiés juridiquement de "privés" - lieux de travail n'accueillant pas de public, établissements scolaires,... - relève des dispositions de la loi du 6 janvier 1978 dès lors que ces dispositifs permettent une conservation sous forme numérique des images, c'est-à-dire constituent un traitement automatisé de données à caractère personnel.

Ils doivent dès lors respecter les dispositions de loi et en particulier n'être mis en œuvre que pour **des finalités déterminées et légitimes**, toutes dispositions devant être prises pour limiter la durée de conservation des données, garantir la sécurité des traitements et assurer une parfaite information des personnes sur leurs droits d'accès.

D - Porte-documents électronique : “personnel” ou “individuel” ?

Un porte-documents qualifié de “personnel”, qu’il appartienne à un élève ou à un personnel, constitue un **espace privé**, qui ne peut en aucun cas être ouvert par autrui **sans autorisation expresse de l’intéressé**. Même un administrateur réseau n’est donc pas fondé, à moins que le réseau ne soit en situation de danger grave et imminent et que la consultation d’un espace personnel soit nécessaire aux mesures visant à assurer son bon fonctionnement, à aller voir le contenu de ce type de porte-documents.

Pour éviter les dérives liées à leur utilisation (stockage et échange illégal de fichiers, volume disque occupé de plusieurs Go), plusieurs mesures peuvent toutefois être adoptées :

- un administrateur réseau peut imposer des quotas sur les espaces personnels ; de cette manière il s’assure que les élèves ne pourront pas utiliser leur porte-documents à des fins d’échange massif de fichiers mp3 par exemple, ou au stockage de fichiers très volumineux (films, applications piratées) ;
- il peut aussi utiliser des scripts lui permettant de contrôler l’espace effectivement occupé par les porte-documents ; en cas d’abus, il est fondé à demander aux élèves d’effacer les fichiers volumineux ou à effacer lui-même le contenu des porte-documents, sous réserve qu’il ait prévenu les intéressés de cet effacement suffisamment à l’avance pour leur permettre de sauvegarder les données qu’ils jugent utiles.

Une autre solution consiste à ne pas utiliser de porte-documents **“personnels”** élèves, mais **“individuels”**, ce qui autorise les enseignants, par exemple, à en visualiser le contenu. Ce choix doit être clairement porté à la connaissance des élèves et doit figurer dans la charte d’usage ; l’établissement considère alors que la vie privée résiduelle des élèves ne s’exerce pas sur le réseau mais sur les espaces privatifs dont ils peuvent disposer sur l’Internet, à travers leur messagerie par exemple, sur un Environnement Numérique de Travail ou tout autre support.

E - Traces de connexions

Les traces de connexions enregistrées sur le Netasq ne sont pas nominatives ; seul le croisement de ces traces avec celles du contrôleur de domaine permet de savoir qui a fait quoi et quand sur le réseau.
ATTENTION : toute preuve obtenue par croisement de traces n’est légalement **recevable que si elle est constituée par un personnel assermenté** (officier de Police Judiciaire, huissier de justice).

Par ailleurs, en vertu de la LOI n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme (décret n° 2006-358 du 24 mars 2006), “les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques.”

Les établissements scolaires, comme les entreprises ou les cybercafés, sont donc soumis aux mêmes règles que les FAI en matière de conservation de traces, ce qui veut dire qu’ils sont tenus de **conserver pendant un an les données relatives au trafic** des communications électroniques susceptibles d'aider à l'identification ou à la poursuite de personnes recherchées.

F - Environnements profilés

Les établissements scolaires utilisent souvent des logiciels permettant de gérer l’usage des ressources du réseau au sens large, ce qui inclut aussi bien les logiciels que l’espace de stockage, les imprimantes et les paramètres de certains programmes sensibles (système d’exploitation, navigateur internet par exemple). Si cette gestion profilée des droits se révèle indispensable pour protéger le réseau contre des utilisations hasardeuses ou malveillantes, elle suppose **l’existence d’une politique locale de sécurité**, décidée en concertation avec les différents acteurs de l’établissement, en l’absence de laquelle la sécurité du réseau est livrée à l’arbitraire.

En savoir plus

Le site Légamédia, proposé par le ministère et accessible sur http://www.educnet.education.fr/legamedia/ vous apportera tout complément utile. Vous pouvez également vous adresser aux services du rectorat, et notamment à la cellule juridique et au SERIA.

3/ Comment responsabiliser la communauté éducative ?

Présentation

Une politique de sécurité s'appuie sur des procédures techniques, une organisation et l'implication de tous. Elle repose également sur la prise en compte de son importance par les personnels et les élèves eux-mêmes. Comprendre le risque informatique, c'est commencer à le maîtriser. Face à l'accroissement du risque, le schéma directeur de la sécurité des systèmes d'information s'oriente aujourd'hui vers le concept de défense en profondeur.

Les enjeux

La lutte contre la criminalité informatique a longtemps été considérée comme une affaire de techniciens. La mise en œuvre de mécanismes de défense appropriés, aptes à lutter contre les attaques informatiques, a longtemps tenu lieu de seule politique de sécurité. Face à l'évolution des risques, à leur nature et à leur ampleur, une telle politique "techniciste" s'avère aujourd'hui inopérante. Le **concept de défense en profondeur** consiste en une **approche globale et dynamique**, qui vise à coordonner plusieurs lignes de défense couvrant l'ensemble du système d'information. Elle implique l'ensemble des acteurs de la communauté éducative et vise à une véritable gestion des risques à travers la remontée d'information, la planification des réactions, la correction et l'enrichissement permanents des procédures imposées par l'expérience.

Les recommandations

La sécurité est le plus souvent vécue comme une contrainte ; or à l'instar d'un feu rouge, d'un stop qui assure la sécurité du réseau routier, les règles et mécanismes de sécurité pour les systèmes d'information concourent à des usages sûrs et maîtrisés de l'informatique et des nouvelles technologies. L'implication des chefs d'établissements, dans une approche pédagogique, vise à les rendre acteurs, à les inciter à informer la communauté éducative sur la sécurité, ses enjeux et à obtenir son adhésion. La désignation d'un correspondant SSI constitue une étape importante de ce processus.

Nous recommandons comme point de départ :

- la signature des chartes élèves, personnels, administrateurs ;
- la diffusion des notes ou procédures de sécurité.

Il est important d'avoir en tête :

- que la sécurité et les notes de procédures sont là pour protéger les élèves et personnels ;
- qu'il est indispensable d'associer les personnels à la démarche sécurité ;
- que la responsabilité des personnels de l'Éducation nationale peut être engagée ;
- que la charte élève, si elle n'a pas de valeur juridique au sens strict, doit être lue, comprise et signée par tous les élèves : la signature de la charte par les élèves doit donc être associée à une action pédagogique permettant d'expliciter précisément le sens et la portée de ses différents éléments.

En pratique

- les notes de sécurité (flash-infos académiques) doivent être portées à la connaissance des personnels et consignées en un lieu unique facilement accessible dans l'établissement ;
- un bilan SSI peut être présenté annuellement au conseil d'administration de l'école ou de l'établissement. Celui-ci pourra fournir, par exemple, des informations sur les incidents, les notes de procédures diffusées, leur application au sein de l'établissement, les actions pédagogiques menées auprès des élèves, etc.

En savoir plus

On pourra consulter l'espace SSI académique sur http://www.ac-rennes.fr/ssi.

4/ La chaîne d'alerte

Présentation

La circulaire n° 2004-035 du 18 février 2004 http://www.education.gouv.fr/bo/2004/9/MENT0400337C.htm , parue au Bulletin Officiel de l'Éducation nationale du 26 février 2004, précise la mise en place d'une **chaîne d'information** qui doit être utilisée en **cas d'incidents liés à l'usage des technologies de l'information et de la communication dans le cadre pédagogique**.

Par extension, les chefs d'établissement doivent saisir la chaîne d'alerte au niveau académique pour tout incident SSI.

Les enjeux

La circulaire n° 2004-035 du 18 février 2004 vise à renforcer les dispositifs humains et techniques mis en œuvre pour garantir une utilisation plus sûre d'Internet. La mise en œuvre de cette chaîne d'alerte est un enjeu essentiel pour l'Éducation nationale.

Les recommandations

La chaîne d'alerte fonctionne comme suit :

- au sein de chaque établissement ou école, les membres de l'équipe pédagogique informent le chef d'établissement ou le directeur d'école des incidents constatés ;
- le chef d'établissement ou le directeur d'école alerte la cellule académique et informe l'IA-DSDEN ;
- en cas de besoin, cette cellule académique informe la cellule nationale de coordination par l'intermédiaire des dispositifs d'assistance mis à disposition (interface web et courrier électronique). Au besoin, le haut fonctionnaire de défense est informé.

La chaîne d'alerte doit être activée pour signaler TOUT INCIDENT de sécurité des systèmes d'information repéré dans les établissements scolaires et les écoles.

En pratique

La chaîne d'alerte a pour objectif d'engager les **mesures adaptées** dans les **meilleurs délais** et d'assurer la circulation de l'information utile afin de maintenir un niveau de **protection optimal**.

- La circulaire du 18 février 2004 doit être portée à la connaissance des personnels pédagogiques ;
- la cellule académique est constituée autour du RSSI (Responsable académique de la Sécurité des Systèmes d'Information) ;
- la chaîne d'alerte peut être saisie :
  - par courriel, en écrivant à : alerte.ssi@ac-rennes.fr
  - par fax au : 02 23 21 75 95
  - par téléphone au : 02 23 21 76 70

5/ Que faire en cas d'intrusion ?

Présentation

On considère qu'il y a intrusion sur un système d'information lorsqu'une personne réussit à obtenir un accès non autorisé. Dans la plupart des cas d'intrusions, une personne n'ayant en théorie pas de droit d'accès au système d'information, ou des droits limités, parvient à s'octroyer des droits d'administrateur.

Les enjeux

Les effets néfastes d'une intrusion sur un système d'information peuvent être amplifiés par une réaction inadaptée. Les actions entreprises doivent être conformes à la politique de sécurité et aux procédures définies. Sur le point plus particulier de l'analyse de l'intrusion, il est préférable de la confier à des professionnels expérimentés, à même d'en évaluer l'impact technique et juridique.

Les recommandations

ATTENTION : l'analyse technique d'une intrusion doit être confiée à des personnels compétents ;

ATTENTION : de mauvaises réactions face à une intrusion peuvent en amplifier les effets néfastes.

• Voici les actions à réaliser immédiatement :

- **SANS ETEINDRE LA MACHINE**, débrancher le câble réseau ; pour des ordinateurs connectés à un réseau sans fil, désactiver la carte réseau sans fil ;
- prévenir le responsable sécurité et le chef d'établissement

• Dans un second temps :

- saisir la chaîne d'alerte ;
- porter plainte surtout en cas de préjudice subi par des tiers (c'est le chef d'établissement, personne juridiquement responsable, qui doit le faire) ;

En pratique

Qu'est-ce qui peut trahir une intrusion ?

- une activité importante ou inhabituelle sur le réseau ou sur une machine ;
- l'impossibilité de se connecter sur une machine ;
- la présence de logiciels espions ;
- l'apparition, la disparition, l'altération ou la modification anormale de fichiers ;
- l'ouverture de services non autorisés ;
- l'altération, la création ou la destruction de comptes.

En savoir plus

Consultez le site du CERTA :
http://www.certa.ssi.gouv.fr

6/ Quelle protection pour les mineurs ?

Présentation

L'Internet, à l'image d'une ville de plus d'un milliard d'habitants, offre de nombreux services : bibliothèques, musées, théâtre, concerts, lieux de rencontres culturels ; mais ses mauvais quartiers n'ont rien à envier à la criminalité des grandes métropoles : jeux de hasard, pornographie, scènes de massacre, échanges de produits illégaux, vente d'armes... Il n'est d'ailleurs pas rare, lors de nos balades sur le web de tomber sur des pages dont le contenu nous agresse ou nous choque. Au-delà de ces contenus, l'Internet recèle des pièges qui peuvent s'avérer nocifs voire dangereux pour les élèves.

Les enjeux

L'atteinte à l'intégrité des mineurs est sans conteste le risque majeur pour l'Education nationale. Leur protection est donc une priorité absolue. Elle a fait l'objet de la publication d'une circulaire le 18 février 2004 (cf. http://www.education.gouv.fr/bo/2004/9/MENT0400337C.htm - circulaire n° 2004-035 du 18 février 2004) qui sert de point de référence. Elle précise les mesures à mettre en œuvre pour **limiter l'exposition des élèves à des contenus inappropriés**, dont les principales sont : le filtrage d'URL, la surveillance régulière des traces de connexion, la sensibilisation des élèves aux risques et aux enjeux de l'Internet.

Les recommandations

Le mécanisme de filtrage mis en place dans l'académie repose aujourd'hui sur les **listes maintenues par l'Université des sciences sociales de Toulouse**. Bien que ces listes soient régulièrement mises à jour, elles n'offrent pas un niveau de protection très élevé, et l'académie teste actuellement des solutions susceptibles d'améliorer sensiblement la qualité du filtrage offert aux établissements. Quelle que soit par ailleurs la qualité des outils de filtrage mis en place, la vigilance est indispensable ; elle passe notamment par l'examen régulier des traces de connexion.

IMPORTANT :

- La charte élèves est le premier élément du dispositif de protection des mineurs ; sa signature par un élève mineur n'a pas de valeur juridique ; c'est pourquoi il est indispensable de l'associer à une action pédagogique visant à la faire mieux comprendre et à en expliciter le sens et la portée ;
- les dispositifs de filtrage ne peuvent jamais être considérés comme sûrs à 100%, d'où l'importance des actions de sensibilisation menées auprès des élèves ; tous les collèges publics de l'académie ont reçu un coffret Educaunet, qui fournit des suggestions d'activités pour aborder le problème des dangers et des enjeux de l'Internet ; d'autres types d'actions peuvent être menées, notamment dans le cadre du B2i, y compris en lycée ; n'hésitez pas à contacter le SERIA.

En pratique

En fonction de la nature des contenus découverts sur un site inapproprié ne figurant pas dans les listes de Toulouse, on prendra les mesures suivantes :

- si le site a un caractère pornographique, on renseignera le formulaire de signalement accessible via http://www.ac-rennes.fr/ssi (cela ne prend que quelques secondes) ;
- si le site est de nature manifestement illégale (contenus pédopornographiques, incitation à la haine raciale, apologie du terrorisme, etc.), on devra renseigner le formulaire précité, mais il faudra aussi adresser un signalement aux "autorités légales" ; le site de l'AFA (Association des Fournisseurs d'Accès à l'internet) rassemble l'essentiel des informations utiles : cf. http://www.pointdecontact.net/signalements.html
- dans tous les cas, on activera la chaîne d'alerte SSI académique.

En savoir plus

- on pourra consulter le texte de la circulaire n° 2004-035 du 18 février 2004 : http://www.education.gouv.fr/bo/2004/9/MENT0400337C.htm ;
- la webographie proposée par le CRDP de Nantes pointe vers des compléments intéressants : http://www.crdp-nantes.cndp.fr/ressources/document/education_risques/index.htm .
- on pourra également lire le compte rendu de la table ronde "Internet, école et sécurité" organisée par l'académie dans le cadre des rencontres de l'Education accessible via http://www.ac-rennes.fr/ssi .

7/ L'établissement connecté à l'Internet : quelles bonnes pratiques ?

Présentation

Afin de simplifier et de rationaliser les opérations de pilotage d'une part, et de ne pas transformer les établissements en centres d'exploitation de l'autre, de plus en plus d'applications informatiques utilisées en établissement scolaire sont appelées à être hébergées ailleurs, généralement au niveau académique. C'est le cas de Sconet ou de l'ENT par exemple.

Cette tendance ne doit pas remettre en cause l'importance d'une politique locale SSI, d'autant que l'accès à ces applications en ligne requiert le plus souvent une identification/authentification personnelle. La négligence ou le vol de ces informations de connexion peuvent avoir des conséquences personnelles fâcheuses (usurpation d'identité, escroquerie, intrusion d'autrui dans sa vie privée, etc.), sans préjuger des conséquences possibles sur la sécurité de l'ensemble du SI.

Les enjeux

Les pratiques à risque peuvent porter préjudice à l'établissement ou à des tiers, sans parler des poursuites civiles ou pénales qu'elles peuvent entraîner. L'exposition à des contenus inappropriés peut également avoir des conséquences plus ou moins graves pour les élèves. L'instauration de bonnes pratiques et la mise en place de **procédures de contrôle a priori et a posteriori** réduisent sensiblement les risques.

Les recommandations

- éviter la mise en œuvre de serveurs ftp (serveurs de transfert de fichiers) avec une autorisation d'écriture pour tous ;
- interdire le trafic peer to peer ;
- ne pas autoriser le chat ;
- n'autoriser la connexion d'ordinateurs extérieurs au réseau de l'établissement qu'après avis de la personne qui s'occupe du réseau ou du correspondant SSI ;
- demander l'accord du SERIA pour l'ouverture d'un service sur l'Internet ;
- proscrire toute connexion qui contournerait l'accès Internet de votre établissement et les dispositifs de sécurité qui l'accompagnent.

La mise en œuvre de ces recommandations s'associe à des contrôles que vous pouvez effectuer au sein de votre établissement. La consultation régulière des traces de connexions enregistrées par la passerelle Netasq, à l'aide des logiciels Firewall Reporter et Firewall Monitor, permet de repérer les éventuels trafics anormaux ou illicites. Il convient cependant d'être extrêmement prudent dans l'interprétation que l'on peut faire d'un relevé de traces de connexions et il est préférable, en cas de doute, de demander l'avis d'un personnel qualifié (correspondant SSI par exemple).

Si l'on observe des anomalies répétées et graves, il est nécessaire d'activer la chaîne d'alerte académique.

ATTENTION : les preuves recueillies lors d'investigations menées en dehors de tout cadre légal ne sont pas opposables devant un tribunal ; elles peuvent en outre être utilisées contre leur auteur.

En savoir plus

Pour plus d'informations sur les risques associés à la divulgation de vos données personnelles, consultez la fiche "Comment assurer la confidentialité de ses informations personnelles ?"
ou l'espace SSI académique sur http://www.ac-rennes.fr/ssi .

8/ Comment assurer la confidentialité de ses informations personnelles ?

Présentation

L'analyse du risque montre que c'est sur le poste de travail que fonctions et données essentielles du système d'information sont exécutées et manipulées. Le poste de travail est utilisé tout à la fois pour échanger, stocker de l'information ou pour accéder à des applications sensibles. La confidentialité des informations à caractère personnel est donc étroitement liée à la sécurité du poste de travail que vous utilisez.

Les enjeux

La sécurité du poste de travail constitue un des éléments essentiels de la sécurité dans le concept de défense en profondeur. Si les mécanismes opérationnels sur les réseaux, serveurs ou systèmes logiciels constituent la première ligne technique de défense, il est dangereux de considérer que son poste de travail est protégé parce que situé derrière ceux-ci. La nature même des données manipulées sur le poste de travail nécessite de le prendre en considération dans la politique de sécurité.

Les recommandations

- ne divulguez jamais à personne votre mot de passe ou toute autre information sur votre compte ;
- ne laissez jamais ces informations en vue ni dans un lieu accessible sans surveillance ; a fortiori, ne créez pas de fichier contenant vos mots de passe ;
- ne quittez jamais votre poste de travail lorsque vous effectuez une opération sensible ; si vous y êtes obligé avant de terminer, verrouillez-le ;
- fermez toujours correctement les applications utilisées lorsque vous quittez définitivement votre poste de travail ;
- n'envoyez jamais d'information confidentielle par courrier électronique, sauf si elles sont chiffrées ;
- évitez d'utiliser un mot de passe simpliste (mot du dictionnaire, prénom, etc.) susceptible d'être deviné ;
- modifiez régulièrement votre mot de passe et ne réutilisez pas le même mot de passe trop rapidement ;
- dans la mesure du possible, n'utilisez pas le même mot de passe pour tous les services que vous utilisez (prenez un mot de passe différent pour vos applications métiers et vos applications privées par exemple) ;
- n'acceptez jamais que des applications, et en particulier les navigateurs internet enregistrent les données saisies dans les formulaires, et tout particulièrement les mots de passe ; si au moment de vous connecter à un service en ligne vous vous apercevez que la machine remplit toute seule le champ correspondant au mot de passe, c'est que le dispositif d'enregistrement des mots de passe est activé ; désactivez-le ; si vous ne savez pas le faire ou si vous ne disposez pas des droits nécessaires pour effectuer vous-même l'opération, faites appel rapidement à une aide extérieure ;
- la plupart des applications WEB qui requièrent une identification/authentification exploitent une connexion sécurisée, identifiable grâce à un logo représentant un cadenas fermé dans la barre d'adresse de votre navigateur ; attention toutefois : certaines pages sécurisées peuvent être composées d'éléments non sécurisés et à l'inverse, des pages non sécurisées peuvent contenir des éléments sécurisés, notamment des formulaires ; en cas de doute sur le niveau de sécurité d'un envoi de données, contactez le SERIA ;
- si vous utilisez une messagerie de type webmail, respectez les consignes de prudence relatives à la consultation et à l'envoi de messages sur l'Internet (cf. page suivante "comment bien utiliser la messagerie électronique?") ;
- pour payer par carte bancaire, préférez les cartes virtuelles à usage unique et montant préfixé ;

En pratique

- installez un antivirus, un logiciel anti-espions et un pare-feu, tout particulièrement sur les ordinateurs portables, les machines sensibles de l'établissement (celle du courrier électronique par exemple) ou sur votre machine personnelle, et veillez à leur mise à jour régulière ;
- mettez à jour régulièrement le système d'exploitation et le navigateur internet des machines mobiles ou sensibles ; ces logiciels disposent souvent de dispositifs de mise à jour automatique ;
- après avoir saisi des données sensibles sur le Web, effacez la mémoire cache du navigateur avant de quitter, si ce n'est pas fait de façon automatique.

En savoir plus

Consultez les recommandations du CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques) sur le choix d'un bon mot de passe :

http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html

Pour plus d'informations sur les risques associés à la divulgation de vos données personnelles, consultez l'espace SSI académique sur http://www.ac-rennes.fr/ssi .

9/ Comment bien utiliser la messagerie électronique ?

Présentation

La messagerie électronique est aujourd'hui devenue un moyen de communication d'usage courant pour la majorité d'entre nous. Et si sa puissance et sa facilité d'emploi en font un outil de choix pour transmettre des informations rapidement à un grand nombre de correspondants, la faiblesse native de la sécurité qui entoure son protocole d'envoi de courrier (SMTP pour Simple Mail Transfer Protocol - Protocole simple de transfert de courrier) en fait également **l'outil de prédilection des spammeurs** ; mais ceux-ci étendent désormais leurs nuisances sur les forums, les blogs, les téléphones mobiles, les messageries instantanées.

Les spams, ou pourriels, sont des messages électroniques non sollicités envoyés en masse. En janvier 2007, on estimait à plus de 8 milliards le nombre de spams envoyés par mois dans le monde. Des dispositifs techniques sont mis en œuvre au rectorat pour lutter contre le spam, mais aucun système de filtrage n'est efficace à 100%, d'où l'importance de la vigilance des utilisateurs.

Les enjeux

La pratique du spam continue à évoluer rapidement. Les spammeurs, qui utilisent aujourd'hui fréquemment des techniques proches de celles des pirates informatiques, n'hésitent pas à attaquer des serveurs d'annuaires pour récupérer des adresses électroniques.

Les jeunes ne sont naturellement pas épargnés par le spam, et si l'on considère le nombre de messages à contenus inappropriés aux mineurs ou carrément illégaux qui circulent par ce biais, on peut estimer que le spam est devenu un facteur d'exposition majeur à ce type de contenus.

La lutte contre le spam, dans une optique de défense en profondeur, implique l'ensemble des acteurs de la communauté éducative.

ATTENTION :

- l'expéditeur apparent d'un courriel n'est pas forcément l'expéditeur réel ;
- même si votre boîte de messagerie est régulièrement spammée, il ne sert à rien d'envisager des mesures de "rétorsion" : les adresses qui semblent à l'origine des messages n'existent certainement même pas ;
- un premier niveau de protection anti-spam est assuré au niveau de la messagerie académique, et la plupart des services de messagerie proposent une protection contre le spam ; si vous utilisez un client de messagerie, il est possible qu'il dispose de mécanismes anti-spam ; sinon, vous pouvez également utiliser un logiciel pour filtrer les messages que vous recevez ; il existe des programmes anti-spam gratuits comme SpamPal ; sachez toutefois que l'arme absolue contre le spam n'existe pas ;
- les canulars, qui font appel à la générosité des utilisateurs, ou qui jouent sur leur superstition, et les "scam 419", forme d'arnaque d'origine africaine, qui proposent des opérations attractives de transferts de fonds, sont des spams d'un genre particulier.

En cas de doute sur la fiabilité d'un message ou d'une information, consultez le site http://www.hoaxbuster.com, ou adressez-vous au SERIA.

Les recommandations

- face à un sujet de spam choquant ou provocateur, efforcez-vous de garder votre sang-froid ; abstenez-vous d'y réagir et/ou de le diffuser ; si le message a un caractère manifestement illégal (transmission d'images à caractère pédopornographique, incitation à la haine raciale, apologie de crime, etc.), activez la chaîne d'alerte SSI académique et écrivez à judiciaire@gendarmerie.defense.gouv.fr.

En pratique

- ne répondez jamais à un spam ;
- ne cliquez sur les liens de désabonnement présents dans le message que si vous êtes sûr qu'il permet un réel désabonnement (renseignez-vous sur le sérieux de la société expéditrice du courriel) ;
- plus généralement, ne cliquez jamais sur les liens hypertextes insérés dans le corps du spam ;
- n'ouvrez jamais un fichier joint à un spam ; ils peuvent contenir des virus ou des logiciels espions ;
- ne diffusez jamais à des tiers les adresses de messagerie d'autres personnes sans leur consentement ;
- ne placez jamais de copie d'un spam dans des forums auxquels vous participez ;

En savoir plus

Vous pouvez consulter le site de l'Association des Fournisseurs d'Accès et de Services Internet (AFA) : http://www.afa-france.com/t_spam.html

10/ La publication sur l'Internet : comment s'y retrouver ?

Présentation

L'explosion de ce que l'on appelle le WEB 2.0 en 2004-2005, c'est-à-dire, du point de vue utilisateur, d'un WEB où l'internaute n'est plus seulement consommateur mais contributeur, a donné au plus grand nombre la possibilité de publier facilement et rapidement sur l'Internet. N'importe qui ne peut cependant pas dire n'importe quoi sur l'Internet et lorsqu'on veut créer un blog ou un site internet, ou même si l'on souhaite seulement intervenir en laissant un commentaire sur le site de quelqu'un d'autre, il est indispensable de respecter un certain nombre de lois.

Les enjeux

La facilité d'accès à des outils simples et efficaces permettant de mettre en ligne rapidement tout type d'information accentue aujourd'hui le **poids des pratiques à risques en matière de publications internet**. Le phénomène des blogs rappelle aussi l'intérêt d'une éducation aux médias et rend nécessaire une action de sensibilisation des jeunes aux risques d'exposition de leurs données personnelles.

Les recommandations

1) Il est important de rappeler qu'ouvrir un service sur l'Internet n'est pas anodin et entraîne l'exposition de la machine hébergeant le service ainsi qu'éventuellement celle du réseau dans lequel elle est intégrée. C'est pourquoi il est déconseillé aux établissements de se transformer en prestataires de services internet sans s'être assurés de disposer des ressources nécessaires à la surveillance et à la maintenance des applications ainsi qu'à la sauvegarde des données.

L'académie propose un service de publication destiné aux établissements scolaires (cf. "http://pharouest.ac-rennes.fr" http://pharouest.ac-rennes.fr) et le projet PHARE a été l'occasion d'expérimenter des outils de publication simples adaptés à leurs besoins. L'ENT académique permettra bientôt de généraliser leur usage.

ATTENTION : L'ouverture de services hébergés par l'établissement doit faire l'objet d'une discussion préalable au sein même de l'établissement, et d'une demande de conseil auprès du Rrectorat ; les services exploitant un traitement de données à caractère personnel doivent être déclarés à la CNIL.

N.B. Conformément au B.O. N°35 du 24 septembre 1998, les établissements scolaires sont tenus de respecter le plan de nommage gouvernemental pour l'ouverture de tout service sur l'Internet ; les EPLE de l'académie doivent donc s'intégrer dans le domaine ac-rennes.fr.

2) les blogs, apparus à la fin des années 90, sont en principe des pages personnelles interactives dans lesquelles les "blogueurs" publient des articles qui peuvent contenir des éléments multimédias et que les lecteurs peuvent commenter. Le blog est donc avant tout un outil d'écriture, qui peut avoir un réel intérêt pédagogique. La plupart des sites de blogs sont cependant filtrés dans les établissements scolaires. Demandez conseil au SERIA si vous souhaitez ouvrir un blog en vue d'un usage pédagogique.

En pratique

Rappelons que le fait de publier des informations et des documents accessibles à tous sur l'Internet, quel que soit le moyen de les mettre à disposition, suppose que l'on respecte un certain nombre de règles, et que l'on s'abstienne notamment :

- des atteintes à la vie privée d'autrui (ATTENTION aux photos notamment), de la diffamation et de l'injure ;
- de la provocation à commettre des actes illicites ou dangereux (crimes, délits, suicide, usage de drogues, etc.) ;
- de la provocation à la discrimination, à la haine, à la violence ;
- de l'apologie des crimes (viol, de guerre, contre l'humanité) ; de la négation des crimes contre l'humanité ;
- de la reproduction, de la représentation ou de la diffusion d'une œuvre de l'esprit en violation des droits de l'auteur, du titulaire des droits voisins et/ou du titulaire des droits de propriété intellectuelle.

Si la plupart des blogs ne posent aucun problème, il est important de savoir comment se comporter en cas d'incident lié à un blog, sachant que chaque situation est particulière :

- avant toute chose, il peut être utile de conserver la preuve du problème ; il est important de se rappeler que seuls des agents assermentés (police, gendarmerie, huissiers, etc.) peuvent constituer des preuves légales ;
- en fonction des situations, on pourra ensuite s'adresser à l'hébergeur pour lui demander de fermer le blog incriminé et/ou s'adresser à l'auteur s'il est identifiable ; si l'auteur est mineur, il faudra prévenir ses responsables légaux ;
- si un tiers est mis en cause, il est généralement préférable de l'avertir, même si la situation est à apprécier au cas par cas ; toute victime est fondée à demander réparation du préjudice subi ;
- dans tous les cas, on cherchera avant tout à parvenir à une solution négociée et à ne porter l'affaire en justice que dans les cas graves, et après avoir mesuré les conséquences possibles d'un tel recours.

.../...

.../...

Pour plus d'information

On pourra se reporter à l'espace SSI académique sur http://www.ac-rennes.fr/ssi .

La signature électronique

Comme une signature manuscrite, une signature électronique identifie formellement l'auteur d'un document et **garantit l'intégrité de son contenu**. Elle repose sur un dispositif cryptographique permettant de créer une empreinte numérique associant un document et une information propre à son auteur (la signature), de sorte qu'une quelconque modification, même infime, du document ou de la signature provoque une modification de l'empreinte. Un message ou un document signé numériquement n'est donc pas forcément chiffré.

ATTENTION : une signature manuscrite scannée et enregistrée dans un format "image" ne peut en aucun cas permettre d'identifier formellement le signataire d'un document ; elle ne garantit pas davantage l'intégrité de son contenu.

Pour plus d'information, se reporter au site de la Direction Centrale de la Sécurité des Systèmes d'Information sur http://www.ssi.gouv.fr/fr/sigelec/index.html .

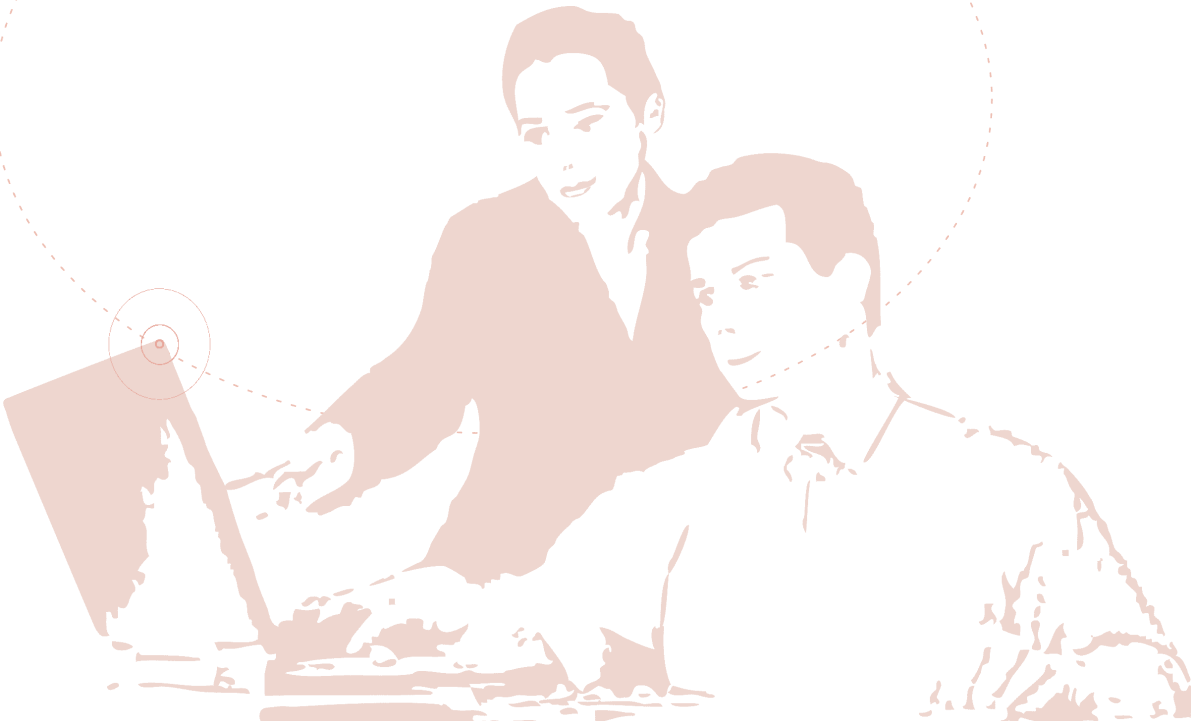
Les logiciels de messagerie instantanée, de téléphonie et de vidéo-conférence

Il existe aujourd'hui de nombreux logiciels permettant de communiquer par écrit ("chatter"), de téléphoner ou d'organiser des vidéo-conférences via l'Internet. Si certains de ces logiciels sont très populaires auprès des élèves, et si les fonctionnalités qu'ils offrent permettent d'envisager des applications de vidéo-conférence à faible coût, ils sont aussi parfois susceptibles de poser de graves problèmes de sécurité et d'exposer le réseau à des risques importants. En septembre 2005, le Haut Fonctionnaire de Défense du Ministère de l'Education nationale a ainsi demandé de proscrire l'utilisation du logiciel Skype pour des raisons de sécurité, et l'on soupçonne d'autres programmes propriétaires, y compris parmi ceux qui sont les plus utilisés par les jeunes, d'abriter des espions logiciels. Il est donc vivement conseillé de ne pas installer ni utiliser de logiciels qui ne reposeraient pas sur des protocoles ouverts.

Rappelons également que le phénomène de prédation pédophile, qui repose largement sur l'imprudence des enfants et des adolescents, exploite aujourd'hui de plus en plus ces outils de communication ; il est important de conseiller aux élèves de ne jamais accepter de connexion avec des inconnus.

En cas de doute ou pour obtenir des conseils

Rendez-vous sur l'espace SSI académique http://www.ac-rennes.fr/ssi ou contactez le SERIA.



11/ Comment faire face à l'évolution des réseaux sans fil et des technologies nomades ?

Présentation

L'introduction sans cesse plus importante de réseaux sans fil (WiFi, WiMax, GSM, GPRS, UMTS, etc.) dans les établissements, rend les architectures plus complexes et plus fragiles, souvent du fait de dispositifs de contrôle d'accès peu sécurisés.

Les problèmes spécifiques posés par les fonctionnalités de certains matériels mobiles, qui permettent d'enregistrer son, images et vidéos, disposent parfois d'énormes capacités de stockage et sont capables de communiquer sans fil (via des connexions Bluetooth ou infrarouges notamment) avec d'autres matériels, posent également de plus en plus de problèmes dans les établissements. Enfin l'usage des clefs USB, qui s'est banalisé depuis quelques années, doit faire l'objet de précautions particulières.

Les enjeux

Une machine, ou même un réseau, peut être compromis par l'introduction de logiciels malveillants provenant d'une clef USB par exemple ; à l'inverse, un logiciel malveillant peut servir à récupérer discrètement l'ensemble du contenu d'une clef USB au moment de son insertion ; les photos ou les vidéos prises par des téléphones portables ou des lecteurs MP3 disposant de fonctionnalités de prise d'images, peuvent être publiées sur l'Internet et porter atteinte à la vie privée de tiers ; les téléphones portables peuvent également être utilisés pour consulter et enregistrer des documents dont le contenu peut être inapproprié pour des mineurs ; l'échange illégal de fichiers musicaux, de films ou de logiciels est grandement facilité par les fonctionnalités de nombreux appareils mobiles.

Les recommandations

- afin d'éviter le lancement automatique de logiciels à l'insertion d'une clef USB, on veillera à désactiver les fonctionnalités dites "autorun" sur les postes de travail, en particulier si ces derniers sont sensibles (machine courrier électronique, serveurs, etc.) ; pour plus d'information, contacter le dispositif d'assistance ;
- le simple fait d'insérer une clef USB dans un système peut suffire à en recopier le contenu de manière invisible ; la mise en place d'environnements profilés et d'outils permettant de cartographier les applications installés sur le réseau réduit les risques sur les postes de travail de l'établissement, mais il est conseillé de ne pas connecter de clef sur une machine dont on n'est pas sûr, surtout si elle contient des informations personnelles ou confidentielles non chiffrées ;
- le moyen le plus efficace de prévenir la survenue de nombreux incidents est de mieux informer les utilisateurs, et les élèves en particulier, des dangers qui les menacent et de les inciter à éviter les pratiques à risques en adoptant une posture consciente et responsable ; la mise en place d'actions de sensibilisation associées à un travail sur les compétences du B2i peut être l'occasion de réfléchir collectivement sur les droits et les devoirs de chacun et sur la notion de responsabilité (à travers la charte d'usage notamment) ;

En pratique

- n'autoriser la connexion d'ordinateurs extérieurs au réseau de l'établissement qu'après avis de la personne qui s'occupe du réseau ou du correspondant SSI ;
- en ce qui concerne les réseaux WiFi installés dans les établissements scolaires, il est impératif de suivre les préconisations et les recommandations académiques ; en cas de doute, contacter le SERIA ;
- en France, le brouillage des réseaux GSM visant à rendre inopérants les téléphones mobiles n'est autorisé que dans les salles de spectacle sous certaines conditions (décision 03-704 du 12 juin 2003). Le conseil d'administration de l'établissement scolaire est en revanche compétent pour décider de l'interdiction ou de la limitation de l'usage des téléphones et autres appareils mobiles dans l'enceinte de l'établissement.

En savoir plus

Consulter l'espace SSI académique sur http://www.ac-rennes.fr/ssi ;

La note du CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques) No 2006-INF-006-001 du 09 novembre 2006 fournit des informations précises sur les risques associés à l'usage des clefs USB : http://www.certa.ssi.gouv.fr .

12/ Quels risques encourus ?

Présentation

Les risques encourus en cas de problème dépendent des responsabilités naturelles et/ou réelles de chacun.

Les enjeux

Réseau victime d'une intrusion, propos injurieux découverts sur un blog d'élève, accès accidentel de mineurs à des contenus pornographiques... En dépit des chartes, des incidents peuvent survenir. Pour les anticiper et encourager une gestion proactive, il est important de savoir identifier les responsabilités.

Les recommandations

- Dans la mesure où le chef d'établissement est la personne juridiquement responsable, il est important que son information soit complète et à jour. Aucune action engageant sa responsabilité ne devrait être entreprise, aucune décision prise, sans qu'il n'en ait été préalablement informé et qu'il ait pu donner son accord.
- A des degrés divers, la responsabilité d'autres personnes missionnées par le chef d'établissement sur des champs d'activités précis (administration réseau, Sécurité des Systèmes d'Information) ou d'autres personnels de l'établissement peut être engagée ; c'est pourquoi il est important que les orientations et les décisions fassent l'objet de concertations et soient prises en commun. On est toujours plus intelligent à plusieurs !
- L'attention des enseignants doit être attirée sur les risques d'incidents liés à l'utilisation en classe de ressources pédagogiques provenant de l'Internet : les activités des élèves sur le réseau devront être balisées précisément et l'on privilégiera, lorsqu'il s'agit de diffusion d'informations, l'enregistrement préalable des ressources à leur consultation en ligne devant la classe.

En pratique

- Le directeur de publication (chef d'établissement pour les EPLE, IEN de circonscription pour les écoles) est responsable des informations publiées au nom de l'établissement ou de l'école ; il devra être particulièrement attentif au respect des règles énoncées dans la fiche "La publication sur l'Internet", paragraphe "en pratique";
- La responsabilité des enseignants peut être engagée en cas d'incident lié à la consultation en classe de contenus inappropriés aux mineurs, ou en cas d'utilisation abusive d'une œuvre protégée par le droit d'auteur par exemple ;
- Il est important de rappeler que :
  - l'enregistrement, la détention et la diffusion de contenus illégaux (pédopornographie, révisionnisme, incitation au terrorisme, incitation à la haine raciale, etc.) constituent des délits passibles de poursuites pénales ;
  - les personnels de l'Éducation nationale ayant fait l'objet d'une condamnation judiciaire pour crime de droit commun ou délit contraire à la probité et aux mœurs, peuvent se voir radiés des cadres (art. 4 de la loi du 25 juillet 1919) ;
  - le Conseil d'Etat a également jugé que le recel d'images de mineurs présentant un caractère pornographique, obtenues à l'aide d'enregistrements par quelque moyen que ce soit desdites images, pouvait fonder la sanction de la révocation d'un personnel enseignant (cf. CE, 08.07.2002, ministre de l'éducation nationale c/ M. [...], n°237642, recel à son domicile par un personnel enseignant de cassettes pornographiques mettant en scène des mineurs).

En savoir plus

- Consulter l'espace SSI académique sur http://www.ac-rennes.fr/ssi ;
- Connectez-vous sur le site Légamédia, proposé par le ministère et accessible sur : http://www.educnet.education.fr/legamedia/ ;
- Consulter le site http://www.droitdunet.fr .

13/ Ressources sur la sécurité des Systèmes d'Information

L'Espace SSI académique

http://www.ac-rennes.fr/ssi

Direction Centrale de la Sécurité des Systèmes d'Information
(Service du Premier Ministre - Secrétariat Général de la Défense Nationale)

http://www.ssi.gouv.fr/fr/dcssi/

Légamédia - éducation et droit de l'Internet (Educnet)

http://www.educnet.education.fr/legamedia/

AIEDU (Accès Internet pour l'EDUcation - Educnet)

http://www.educnet.education.fr/aiedu/

Protection des mineurs - site de la Délégation aux usages de l'Internet

http://www.mineurs.fr/

Protection des mineurs - site interministériel consacré à la lutte contre la pédophilie

https://www.internet-mineurs.gouv.fr/

Site de la CNIL

http://www.cnil.fr

Portail officiel de la sécurité informatique

http://www.securite-informatique.gouv.fr/

Glossaire

Centre d'exploitation	Point névralgique d'une infrastructure informatique, qui s'occupe de l'administration de ses serveurs et de ses réseaux.
Contrôleur de domaine	Serveur contrôlant notamment l'accès des stations et des utilisateurs à une zone du réseau.
Cryptographie	Discipline rattachée à la cryptologie, qui s'occupe spécifiquement de la protection des messages ; l'objectif de la cryptographie est de ne rendre le message intelligible que pour ses destinataires ; elle exploite souvent des secrets partagés par les seules personnes habilitées à recevoir communication du message et se fonde aujourd'hui essentiellement sur des clefs et des algorithmes mathématiques permettant de chiffrer les messages.
Défense en profondeur	Concept hérité du domaine militaire, qui consiste à utiliser plusieurs lignes de défense indépendantes entre elles pour renforcer le niveau de sécurité de ce que l'on cherche à protéger.
F.A.I.	Sigle pour "Fournisseur d'Accès à Internet".
GSM/GPRS/UMTS	Normes liées à la téléphonie mobile et correspondant à ses différentes générations ; toutes permettent de se connecter à l'Internet, mais seules les technologies EDGE et UMTS sont dites "haut débit".
Logiciel malveillant	Programme élaboré spécialement dans le but de nuire (malware en anglais). On peut classer les logiciels malveillants en différents types correspondant à leur mode de propagation, à leur mode d'action ou à la nuisance qu'ils occasionnent. On distinguera notamment : les virus, qui se propagent le plus souvent par courrier électronique, et qui s'attaquent généralement à certains types de fichiers ou au système d'exploitation de l'ordinateur ; les vers (worms en anglais), qui se répandent via le réseau en profitant le plus souvent de failles non corrigées dans les systèmes d'exploitation ; les chevaux de Troie (trojans en anglais), qui permettent à un pirate de prendre à distance le contrôle d'un ordinateur ; les logiciels espions, qui sont programmés pour enregistrer et transmettre des informations sur l'utilisateur d'un ordinateur (logiciels employés, données de connexion, adresse électronique, numéro de carte bancaire, etc.)
Métacharte	Document cadre permettant de décliner différents modèles de chartes.
Peer to peer (P2P)	Désigne un modèle de réseau ou chaque élément joue à la fois le rôle d'un client et d'un serveur ; en d'autres termes un réseau P2P est une sorte de réseau participatif ou tous les maillons ont un rôle équivalent ; l'information y est distribuée et partagée.
Porte-documents électronique	Espace virtuel de stockage de documents et de ressources.
RSSI	Sigle pour "Responsable de la Sécurité des Systèmes d'Information".
SI	Sigle pour "Système d'Information". Un système d'information représente l'ensemble des éléments participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein d'une organisation.
Spam	Courrier non sollicité envoyé en masse à des fins de prospection commerciale, politique, idéologique, ou dans un but malveillant ; le mot de "pourriel" est également utilisé.
SSI	Sigle pour "Sécurité des Systèmes d'Information". La sécurité des systèmes d'information est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information et du système d'information.
Webmail	Messagerie électronique accessible via un navigateur internet.
WiFi	Technologie de réseau informatique sans fil ; le WiFi est fondé sur les normes de la famille IEEE 802.11.

Quizz sécurité en EPLE[1] : 11 points à vérifier en 22 questions

Lorsque vous n'êtes pas sûr de votre réponse, répondez NON

Etes-vous régulièrement informé de l'état de la sécurité informatique dans votre établissement ?	○ OUI	○ NON
Votre système informatique est-il protégé contre les problèmes d'électricité, d'élévation de température, d'inondation et d'incendie ?	○ OUI	○ NON
L'accès aux locaux informatiques est-il protégé par des fermetures adaptées et une alarme ?	○ OUI	○ NON
Existe-t-il des procédures de sauvegarde automatique des données, tests et restauration de sauvegardes ?	○ OUI	○ NON
Existe-t-il des procédures de protection contre les virus ?	○ OUI	○ NON
Toutes les bases de données utilisées dans votre établissement sont-elles recensées ?	○ OUI	○ NON
Existe-t-il un document qui précise les règles de sécurité, les droits, les devoirs et les responsabilités des élèves utilisant votre informatique ?	○ OUI	○ NON
Existe-t-il un document qui précise les règles de sécurité, les droits, les devoirs et les responsabilités des membres du personnel ?	○ OUI	○ NON
Chaque utilisateur est-il identifié lorsqu'il utilise votre système informatique ?	○ OUI	○ NON
Existe-t-il un filtrage des accès aux sites sur l'internet ?	○ OUI	○ NON
Le contenu de l'ensemble du site web de l'établissement est-il conforme aux textes en vigueur ?	○ OUI	○ NON
Une personne a-t-elle été chargée de s'en tenir informée ?	○ OUI	○ NON
Avez-vous un contrat de maintenance de ces systèmes ?	○ OUI	○ NON
Savez-vous précisément combien il existe de clés, qui les détient et qui a connaissance du code de l'alarme ?	○ OUI	○ NON
Les sauvegardes sont-elles régulièrement contrôlées ?	○ OUI	○ NON
Les mises à jour sont-elles régulièrement contrôlées ?	○ OUI	○ NON
Centralisez-vous les documents déclaratifs de ces bases à la CNIL ?	○ OUI	○ NON
Existe-t'il une charte signée par chaque élève ?	○ OUI	○ NON
Cette charte est-elle annexée au règlement intérieur ?	○ OUI	○ NON
La gestion des comptes et mots de passe garantit-elle leur confidentialité ?	○ OUI	○ NON
Les mises à jour de liste noire et le suivi des journaux sont-ils réguliers ?	○ OUI	○ NON
Un contrôle régulier du respect du droit à l'image, de la vie privée, de la conformité aux bonnes moeurs est-il effectué ?	○ OUI	○ NON

Comptez le nombre de OUI cochés

— plus de 17 :
Bravo ! Vous avez fait de réels efforts en matière de sécurité. Moins de 22, votre système reste encore exposé. Il faut étudier les quelques points qui restent.

— plus de 12 à 16 :
Vous pouvez faire face à certains problèmes mais votre dispositif est encore trop exposé. Il faut analyser la situation afin de déterminer les améliorations indispensables.

— de 0 à 11 :
La sécurité est désastreuse ! Vous êtes à la merci du moindre incident. Pour reprendre le dessus face à ces risques, un travail de fond doit être entrepris !

(1) Source : rectorat d'Amiens

Thématique
Mémento sur la sécurité des systèmes informatiques (SSI)

Éditeur
Rectorat de l'académie de Rennes
Service informatique académique (SERIA)

Contact
Alain Van Sante

accès internet
www.ac-rennes.fr

Date de parution
août 2008

Conception réalisation
© rectorat communication

Impression
Imprimerie Le Rimon - 1 000 ex

académie Rennes
Éducation nationale

Service informatique académique (SERIA)