Fiches micro-informatique

SECURITE LOGIQUE — LOGIxx

Objectif

Présenter des préconisations pour sécuriser le poste de travail informatique et son environnement sous forme de fiches pratiques.

Public concerné

Tout utilisateur de l'outil informatique et plus particulièrement les petites entités ou entreprises : PME, travailleur indépendant, profession libérale, utilisateur nomade…

Utilisation du référentiel

Chaque fiche traite un sujet précis et peut être consultée indépendamment.
Ce référentiel est structuré par thèmes.

Contenu du thème

N° de Fiche	Titre de la fiche	Descriptif simplifié et résumé du sujet
LOGI01	Contrôle d'accès	Comment mettre en place une interface de contrôle d'accès permettant d'authentifier l'utilisateur d'un poste de travail.
LOGI02	Chiffrement	Comment se protéger des risques de divulgation et d'altération d'informations sensibles pour l'entreprise.
LOGI03	Lutte antivirale	Comment protéger les machines, les systèmes d'exploitation, les programmes et les données des utilisateurs contre les virus et les autres infections.

Contrôle d'accès — LOGI01

Contexte

Le poste de travail, en réseau ou en mode autonome, permet à tout utilisateur légitime en possession des connaissances suffisantes (par exemple : identifiant et mot de passe) d'accéder aux données, aux applications, aux programmes et aux fichiers.

Objectifs

La mise en place d'un mécanisme de contrôle d'accès permet :
- d'identifier et d'authentifier l'utilisateur ;
- de gérer et d'automatiser les connexions aux applications ;
- d'ouvrir une session utilisateur sur le système d'exploitation ;
- d'assurer la cohérence des différents maillons de sécurité ;
- de valider les différents niveaux d'accès aux systèmes et aux données ;
- d'identifier et de reconnaître tout poste ou ressource se connectant au SI de l'entreprise.

Recommandations

- Identifier et authentifier l'utilisateur qui souhaite accéder au poste de travail ;
- valider les connexions ;
- autoriser et valider les transactions ;
- s'assurer des mises à jour d'horodatage et de traçabilité ;
- vérifier périodiquement la validité de l'autorisation d'accès pendant la durée d'une connexion ;
- élaborer un annuaire de sécurité pour identifier tout poste se connectant au SI de l'entreprise.

Remarques

L'accès à l'ensemble des fonctionnalités et aux applications du poste de travail doit être sécurisé au minimum par un identifiant associé à un mot de passe.
Le niveau souhaité de robustesse du mécanisme de contrôle d'accès déterminera le choix de technologies adaptées. Pour l'identification et l'authentification forte, la carte à puce (ou à jeton) et à la biométrie sont des technologies appropriées (contrôle des empreintes, rétine de l'œil).

Pour les postes de travail autonomes ou en réseau, des solutions simples et accessibles sont présentes sur le marché (clé USB …), les systèmes d'exploitation actuels supportant les fonctionnalités de contrôle d'accès.

La tendance est de déléguer le contrôle d'accès aux systèmes fédérateurs que sont les annuaires (*LDAP*, *AD*), les méta-annuaires (Gestion d'identité, gestion de l'habilitation), le WebSSO qui facilite l'ergonomie en évitant de réitérer les étapes d'authentification pour chaque application sécurisée (proxy, intranet, application métier, …) et de généraliser l'utilisation de certificats de clé publique et d'attribut (X509).

Chiffrement

LOGI02

Contexte

Les risques de divulgation (confidentialité des données) et d'altération d'informations (intégrité des données) sont de plus en plus élevés ; la sensibilité des informations tend à aggraver ces risques.
Les causes identifiées les plus courantes sont :

- les vols, en tous lieux, de micro-ordinateurs et surtout de portables ;
- les intrusions et les écoutes à travers les réseaux en général ;
- les infections logiques (diffusion de fichiers par les vers ou récupération de données par la technique du cheval de Troie) ;
- les erreurs et les malveillances internes à l'entreprise ;
- les nouvelles technologies de stockage externe miniaturisées (clés USB, cartes à puce, disques, disques SSD, cartes mémoire flash…) ;
- les médias de communication sans fil.

Objectifs

A l'aide d'un logiciel de chiffrement des données, les personnes non habilitées ne peuvent pas accéder aux informations définies comme sensibles par l'entreprise ou l'organisme.

Recommandations

- Identifier les informations sensibles ;
- former (ou au moins informer) les utilisateurs de la sensibilité de ces informations et des risques que court l'entreprise en cas de divulgation et/ou altération ;
- chiffrer toute information sensible sur tout poste de travail, en particulier sur les portables ;
- concernant les portables, ne pas hésiter à chiffrer la totalité du support de stockage ;
- privilégier la centralisation de l'administration du logiciel de chiffrement ;
- formaliser par une procédure les principes liés à la conservation, à l'intégrité et aux sauvegardes des clés de chiffrement (en lieu sûr, sous forme chiffrée ou sous enveloppe cachetée…) ;
- utiliser des technologies à l'état de l'art, tout en respectant le cadre légal du pays concerné dans le domaine du chiffrement.

Remarques

Le chiffrement est l'opération qui consiste à transformer une donnée sous une forme inexploitable par un tiers qui n'en possède pas les clés.
Le chiffrement est consommateur de ressources et est susceptible de ralentir les performances, sachant que ces critères ne sont pas rédhibitoires pour l'emploi de ces technologies.

Lien utile : le site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), fournit la synthèse du cadre légal en matière de chiffrement (www.ssi.gouv.fr).

Lutte antivirale — LOGI03

Contexte

Les systèmes informatiques sont régulièrement la cible de programmes malveillants (virus, vers, chevaux de Troie…).
Il existe aujourd'hui plusieurs millions de ces programmes.

Des nouveautés techniques et donc de nouvelles familles d'infections ou d'attaques apparaissent régulièrement.

Objectifs

Des moyens doivent être mis en place pour bloquer et le cas échéant éliminer les virus et autres infections qui pourraient affecter les matériels, les systèmes d'exploitation, les programmes et les données.

Recommandations générales

- Définir une politique de sécurité du système d'information ;
- sensibiliser les décideurs ;
- rédiger une charte du bon usage des moyens informatiques (matériels et réseaux) et des applications associées (messagerie, réseaux sociaux…) pour la sensibilisation des utilisateurs ;
- privilégier l'installation des dernières versions ou correctifs des systèmes d'exploitation, des programmes, des navigateurs..., afin de se protéger au mieux des vulnérabilités connues ;
- valider leur mise en place ;
- s'assurer de leur actualisation ;
- s'inscrire aux listes de diffusion d'alertes des éditeurs d'antivirus et consulter les CERT (Computer Emergency Response Team), les fiches CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques) et le CERT-IST dédié à la communauté Industrie, Services et Tertiaire française ;
- concevoir :
  - une politique de lutte antivirale spécifique : elle formalise les mesures de prévention, de surveillance et de correction pour les postes de travail, les assistants numériques (PDA, Smartphone…), les serveurs de fichiers, les serveurs de messagerie, l'infrastructure d'accès Internet et les échanges avec les partenaires… ;
  - une politique de gestion de crise : elle anticipe le cas d'une infection virale sur un site ou au sein d'une filiale ;
  - un plan de secours : il décrit tous les moyens à mettre en œuvre pour disposer à nouveau de ressources informatiques intègres et fiables (pour les postes de travail, il sera souvent préférable de réinstaller le système d'exploitation et les applications) ;

- une politique de sauvegarde : elle intègre les données et les systèmes, tout en précisant les fréquences, le mode de traitement, les supports et le contrôle de la qualité ;
- une politique de contrôle des supports : elle doit permettre, en appliquant des règles simples, de limiter tout risque d'infection quelque soit le support (disque dur externe, clé USB…) et quelle que soit la nature de l'échange ;
- une conduite à tenir : elle consiste à former les utilisateurs et à organiser la remontée des incidents et des dysfonctionnements auprès du centre d'assistance technique.

Recommandations techniques

- **L'utilisateur**
  - Travailler en profil adapté et spécifique à sa fonction et à ses accès en évitant le mode administrateur.
- **Le poste de travail et les serveurs**
  - Déployer, si possible après validation, automatiquement les correctifs et les mises à jour (système, antivirus et outils bureautiques) ;
  - protéger l'accès aux ressources partagées par des mots de passe robustes ;
  - supprimer les comptes systèmes ou de privilège d'administration par défaut.
- **Les données**
  - Les stocker sur disque logique ou physique distinct du disque dédié au système d'exploitation et aux applications. Cela rend simplement plus aisée la réinstallation du système en cas d'infection.
- **Les applications**
  - Effectuer des contrôles d'intégrité tout au long de leur vie ;
  - affecter des droits de lecture seule, sauf impératif contraire, aux exécutables stockés sur une ressource partagée ;
  - attribuer les « justes » droits d'accès (accès uniquement aux informations nécessaires avec les droits strictement nécessaires).
- **L'antivirus et les conseils d'utilisation**
  - sauvegarder et centraliser les journaux d'événements ;
  - planifier des analyses régulières de ces journaux ;
  - prendre en compte l'analyse des disques distants, en entrée comme en sortie, même en cas d'éventuelle dégradation du débit ;
  - activer le mode d'analyse en permanence ;
  - planifier un scan complet automatique des disques durs ;
  - protéger la configuration par mot de passe.
- **Les autres produits conseillés**
  - Anti-spam, filtrage de contenu, d'URL et de port, système de détection d'intrusion (IDS/IPS).

Lutte antivirale

LOGI03

Recommandations d'ordre juridique et pratique

- Consulter la page informative et les liens sur le site Web du CLUSIF www.clusif.fr ;
- recenser les indices, les éléments d'information ou de preuves (gravure de CD, listing, journaux, témoins, procès-verbaux d'huissiers avec courriers recommandés …) à mettre à disposition des enquêteurs ;
- si le contrat d'assurance souscrit prend bien en compte les faits générateurs constatés et les types d'indemnisation (matériel, perte d'usage ...), effectuer la déclaration de sinistre auprès de sa compagnie d'assurance.