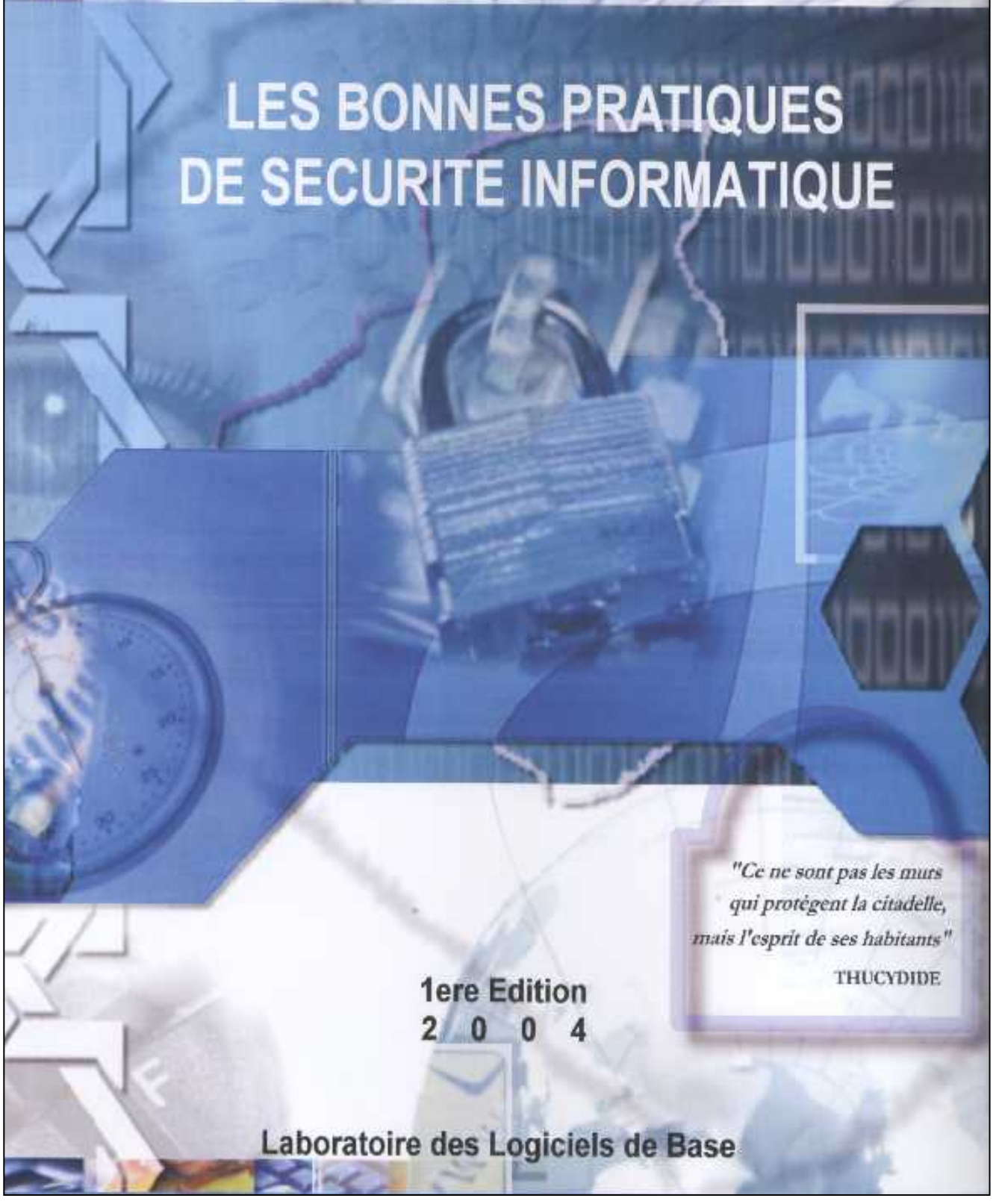
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre de Recherche sur l'Information Scientifique et Technique

LES BONNES PRATIQUES DE SECURITE INFORMATIQUE



"Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants"

THUCYDIDE

1ere Edition
2 0 0 4

Laboratoire des Logiciels de Base

LA SÉCURITÉ : PARLONS EN SÉRIEUSEMENT...

QU'EST CE QUE LA SÉCURITÉ INFORMATIQUE ?

- L'objectif de la sécurité informatique est la mise en œuvre de mécanismes de protection permettant d'assurer les propriétés suivantes :
- La confidentialité : assurer qu'une information n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.
- L'intégrité : assurer que l'information contenue dans les objets n'est ni créée, ni altérée, ni détruite de manière non autorisée.
- La Disponibilité : assurer qu'un objet est accessible et utilisable sur demande par une entité autorisée.
- L'utilisation légitime : assurer que les ressources ne sont pas utilisées par des personnes non autorisées ou de manière non autorisée.

Pourquoi la sécurité ?

Le nombre d'incidents de sécurité augmente de façon fulgurante. Le CERT/CC rapporte un nombre total de 82 094 incidents en 2002 et pas moins de 137 529 incidents pour l'année 2003.

VULNÉRABILITÉ, MENACE ET ATTAQUE ?

Une vulnérabilité est toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient.

Une menace est une violation potentielle de sécurité d'un système en utilisant les vulnérabilités de ce dernier. La concrétisation d'une menace est considérée comme une attaque.

QUELQUES EXEMPLES D'ATTAQUES UTILISÉES AUJOURD'HUI

- Virus, vers, cheval de troie.
- Déni de Service et déni de service distribué.
- Social engineering ; mail bombing.
- IP spoofing, DNS spoofing.
- Buffer overflow ; Ping flooding.

LES CINQ PLUS MAUVAISES ERREURS COMMISES PAR LES UTILISATEURS

1. Ouvrir les fichiers attachés aux e-mails sans vérifier la source ou le contenu.
2. Ne pas installer de correctifs de sécurité, particulièrement pour Microsoft Office, Microsoft Internet, Explorer et Netscape
3. Ne pas faire de sauvegardes et ne pas tester ces sauvegardes.
4. Ne pas exécuter de logiciel de détection de virus.
5. Connecter un modem à une ligne téléphonique alors que l'ordinateur est connecté à un réseau local.

LES ERREURS GRAVES COMMISES PAR LES GESTIONNAIRES

- Ignorer le problème de la sécurité et son importance.
- Charger un personnel non formé du problème de la sécurité.

LES ERREURS GRAVES COMMISES PAR LES ADMINISTRATEURS

- Connecter les systèmes à Internet avant de les durcir.
- Laisser des services non nécessaires disponibles.
- Connecter les systèmes de tests à Internet avec des comptes et mots de passe par défaut.
- Utiliser "telnet" et d'autres protocoles non chiffrés pour la gestion des systèmes, routeurs, firewalls...
- Donner les mots de passe des utilisateurs par téléphone ou changer les mots de passe des utilisateurs en répondant aux requêtes par téléphone sans authentifier le demandeur.
- Implémenter des firewalls avec des règles qui permettent un trafic malicieux et dangereux.
- Ne pas informer les utilisateurs sur la conduite à tenir lorsqu'ils rencontrent un problème de sécurité.

COMMENT INTÉGRER LA SÉCURITÉ DANS VOTRE SYSTÈME ?

PAR OÙ COMMENCER ?

- Créer une structure responsable de la sécurité informatique dans l'organisation.
- Recenser le patrimoine informationnel pour déterminer la valeur des différentes entités, particulièrement celles qui sont critiques et doivent être protégées.
- Faire une évaluation des risques encourus par les différents actifs.
- Exécuter des tests de vulnérabilité pour déterminer les menaces externes et internes à l'organisation.
- Définir une politique de sécurité qui comporte les règles d'administration et d'utilisation du système informatique ainsi que les procédures qui permettent le bon suivi de ces règles.
- Etablir un programme de sensibilisation et de veille qui touche tous les employés de l'organisation.

" La sécurité c'est 20 % de technique et 80 % de bon sens "

LE MINIMUM VITAL !!

- Documenter clairement et publier les missions des administrateurs système et des utilisateurs pour le respect de la sécurité informatique de l'organisation.
- Configurer correctement les routeurs d'accès pour rejeter tout le trafic inutile.
- Supprimer tout service inutile de votre système.
- Configurer correctement les serveurs de messagerie, et utiliser les règles de filtrage de mail pour se protéger contre les fichiers attachés contenant des codes malicieux.
- Utiliser des outils " freeware " de test de vulnérabilité pour faire un auto-test de vulnérabilités pour vos systèmes et publier les résultats au personnel administratif pour augmenter la prise de conscience.
- Installer des outils " freeware " d'audit et d'analyse de trafic réseau sur les systèmes critiques. Analyser quotidiennement les fichiers journal.
- Appliquer les correctifs de sécurité.
- Installer des programmes anti-virus et mettre à jour régulièrement leurs fichiers de signatures disponibles chez les vendeurs.
- Etablir une bonne politique de mots de passe .

ELÉMENTS CLÉS POUR UN PROGRAMME DE VEILLE RÉUSSI

- Engager des professionnels de communication pour organiser et mener le programme de veille.
- Envoyer des messages de veille périodiques dans différents formats (e-mails, infos sur sites web, vidéos en ligne,...)
- Planifier des cours de formation dans le cadre de programmes de formation globale de tous les employés.
- Cibler des formations/ messageries pour les différents groupes (gestionnaires, ingénieurs, administrateurs,...).
- Prévoir, dans le cadre de formations, des simulations d'incidents de sécurité pour évaluer la réponse des utilisateurs et du staff responsable de la sécurité informatique.
- Maintenir tout le personnel informé sur les tendances courantes des incidents de sécurité informatique. Ceci, en mettant à leur disposition les annonces et les alertes disponibles et les encourager à les lire.

RÉPONDRE À UN INCIDENT DE SÉCURITÉ

- Suivre la politique et les procédures de sécurité de l'organisation.
- Contacter le service responsable de la réponse aux incidents dans votre organisation.
- Faire une sauvegarde complète du système sur un support fiable et conserver le off-line.
- Documenter toutes les actions entreprises (appels téléphoniques, fichiers modifiés, processus systèmes arrêtés), prendre des notes précises et maintenir l'ordre chronologique.
- En cas d'incertitude sur les actions entreprises demander l'aide avant de supprimer un fichier ou d'arrêter un processus système.

LES PREMIERS RÉFLEXES D'UN BON UTILISATEUR

CHOISIR UN BON MOT DE PASSE ?

Les incidents de sécurité ont souvent pour point de départ l'acquisition par des moyens "frauduleux" de mots de passe. C'est en effet, la méthode classique la plus utilisée par les intrus pour prendre le contrôle d'un système. Choisir et sécuriser le mot de passe est principalement la mesure la plus importante à entreprendre. Pour cela :

- Le mot de passe doit être assez long : une chaîne de 8 caractères au minimum.
- Augmenter le degré de complexité de votre mot de passe en combinant des lettres majuscules et minuscules et en rajoutant des chiffres et des symboles spéciaux.
- N'utilisez jamais une information personnelle comme mot de passe, telle que votre nom, prénom, prénoms des proches, votre numéro de téléphone, matricule de votre voiture, etc....
- N'utilisez jamais un mot existant dans les dictionnaires ou dans des recueils de prénoms.
- Le mot de passe doit être difficile à deviner, mais facile à retenir.

Protéger son mot de passe

- Un mot de passe est une information sensible, évitez de le noter, gardez le dans votre mémoire.
- Un mot de passe est strictement personnel : ne le confiez à personne et ne le partagez pas avec d'autres.
- Un mot de passe doit être changé régulièrement même s'il est bien choisi à cause de l'écoute sur les réseaux.
- Ne pas reprendre les anciens mots de passe déjà utilisés.

VIRUS : COMMENT SE PROTÉGER ?

D'après une étude récente accomplie par Computer Security Institute, 68% des pertes financières sont dues aux virus.
Chaque mois, 250 nouveaux virus sont découverts et 30% des incidents reportés sont dûs à une infection virale.

Sources d'infections virales

- Disquettes, CD-ROM et documents.
- Programmes et documents infectés, téléchargés à partir d'Internet.
- Pièces jointes infectées dans les e-mails.

Prévention contre les virus

- Installer un antivirus et le mettre à jour régulièrement.
- Scanner les disquettes avant de les utiliser.
- Ne pas ouvrir les fichiers attachés à un e-mail provenant d'une source inconnue ou non éprouvée.
- Supprimer les e-mails spams sans les ouvrir.
- Contrôler toutes les applications à installer.
- Eviter les partages de fichiers sans mot de passe.
- Sauvegarder régulièrement vos données et la configuration de votre système.
- S'abonner à un service d'alertes virales par e-mail.

Pour plus d'informations sur les virus et les antivirus, consulter : www.sophos.com
www.symantec.com

"Un mot de passe c'est comme une brosse à dents : on l'utilise fréquemment, on le change régulièrement et surtout on ne le prête à personne"

POUR PLUS D'INFORMATION

OUTILS NÉCESSAIRES

OUTIL	RÔLE	EXEMPLES
Audit	Révèle et évalue le niveau de sécurité d'une architecture en place et compare ce dernier à la politique de sécurité	Nessus : http://www.nessus.org/ Nmap : http://www.insecure.org/nmap
Test de Vulnérabilités	Permet de déterminer les vulnérabilités et les correctifs disponibles	Nessus : http://www.nessus.org/ Sara : http://www.www-arc.com/sara/ Saint : http://www.wwdsi.com/saint/
Système de Détection d'intrusions	Surveille le trafic réseau ou analyse les fichiers logs d'un système et répond par des alertes en présence d'activité anormale	Tripwire : http://www.tripwire.com/ Snort : http://www.snort.org AIDE : http://sourceforge.net/projects/aide/
Firewall	Permet de mettre en vigueur la politique de contrôle d'accès entre deux réseaux	ZoneAlarm: http://www.zonelabs.com/ BlackIce: http://blackice.iss.net/ Iptables: http://www.netfilter.org/
Chiffrement	Assure la confidentialité des données	PGP : http://www.pgpi.org/ MD5:http://www.ietf.org/rfc/rfc1321.txt

LIENS PERTINENTS

Portails de sécurité : toute l'actualité de la sécurité informatique

SecurityFocus : www.securityfocus.com
Search Security : www.searchsecurity.com
Securiteam : www.securiteam.com
Infosyssec : www.infosyssec.com

Quelques portails francophones

www.securite.org
www.secuser.com

Organisations

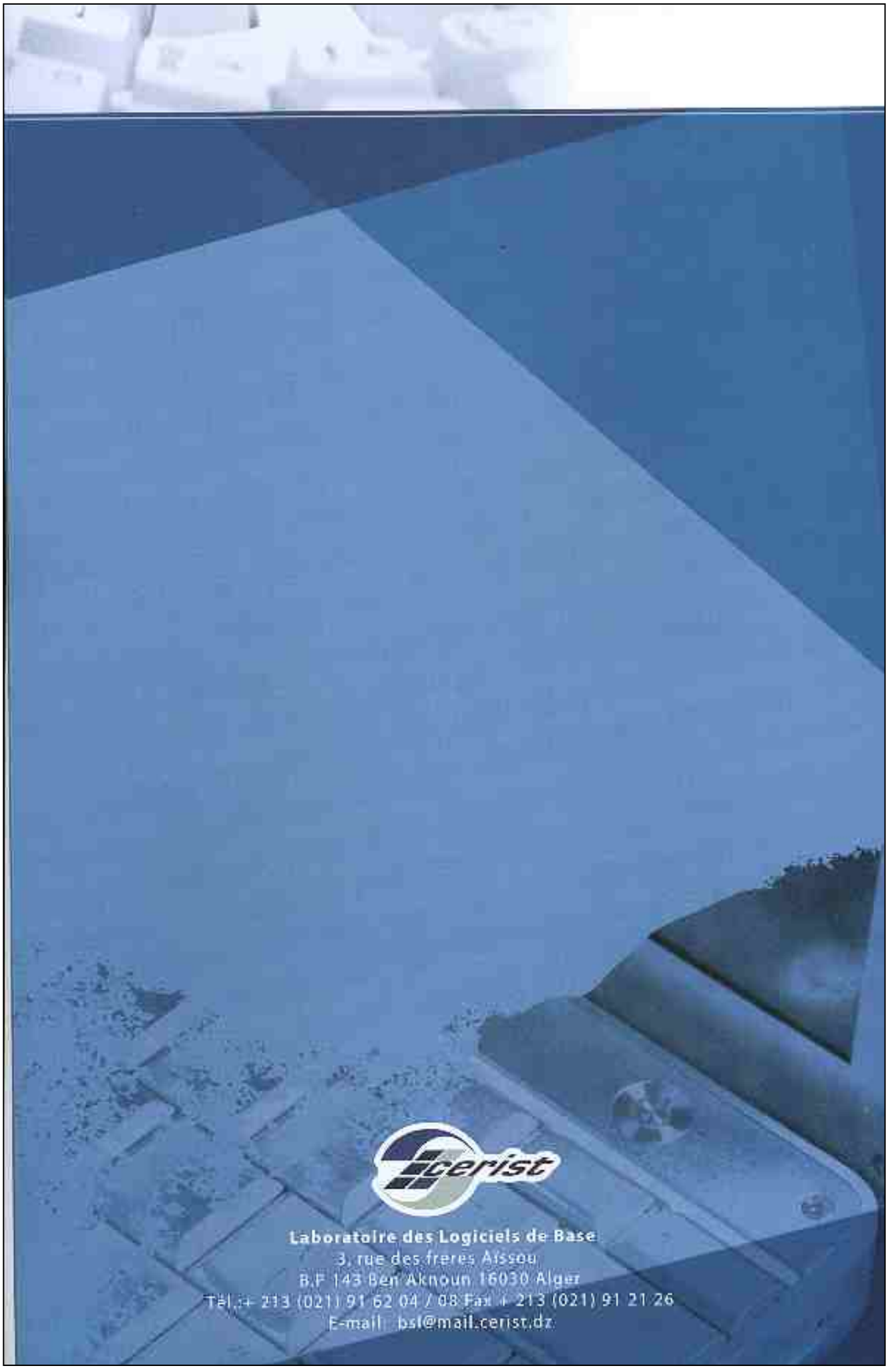
CERT/CC (CERT Coordination Center) : www.cert.org
CSI (Computer Security Institute) : www.gocsi.com
Sans Institute: www.sans.org
CVE (Common Vulnerabilities and Exposures) : cve.mitre.org

Rôle du CERIST dans le développement de la sécurité informatique

1. Formation : www.cerist.dz
- Formation à la carte.
- Post-graduation Spécialisé en Sécurité Informatique.

2. Recherche et Développement
bsi.cerist.dz

3. Workshop International en Sécurité : WSTI'03



Laboratoire des Logiciels de Base
3, rue des freres Aissou
B.P 143 Ben Aknoun 16030 Alger
Tél :+ 213 (021) 91 62 04 / 08 Fax : 213 (021) 91 21 26
E-mail : bsl@mail.cerist.dz