

Aud-IT

Sécurité et Organisation Informatique

News

Généralités

Bienvenue
Qui sommes-nous
Contactez-nous
Articles
Liens intéressants

Services

Audit informatique
E-Commerce
Self-Assessment
Politique de sécurité
Assistance et conseil
Formation

Normes

BS 7799
CobIT

Actualités

Archives avril 2001

[Virus et autres logiciels malicieux](#)

Les différents types de logiciels malicieux et comment se protéger contre (30.4.2001).

[Firewalls personnels \(mise à jour\)](#)

Analyse de firewalls personnels disponibles sur le marché (30.4.2001).

[Conseils de sécurité du NIPC](#)

Cette publication du NIPC fournit des conseils de sécurité, en particulier sur les risques des collaborateurs travaillant depuis leur domicile (30.4.2001).

[Alimentation électrique](#)

Si possible, considérez les risques et les besoins liés à l'alimentation électrique déjà lors de la construction des bâtiments. D'autre part, la libération du marché de l'électricité va probablement augmenter les risques d'indisponibilité (30.4.2001).

[Se former en jouant](#)

Des jeux simulant des attaques peuvent très bien servir à former les collaborateurs à la sécurité (30.4.2001).

[Hotfixes de MS infectés](#)

MS ayant oublié d'installer l'antivirus sur le serveur, des fichiers hotfix ont été infectés par un virus. [Autre article](#) à ce sujet et [commentaires de MS](#) (30.4.2001).

[W2K et SNMP](#)

Avantages et risques de sécurité en utilisant SNMP avec Windows 2000 (30.4.2001).

[Vulnérabilités des téléphones mobiles](#)

Selon des spécialistes, dont les vendeurs d'outils de sécurité, les attaques de PDA, téléphones mobiles, etc. vont augmenter et les utilisateurs de tels outils doivent être sensibilisés à ces risques. [Autre article](#) à ce sujet (30.4.2001).

[Degré de vulnérabilité de W2K](#)

Article abordant la question du degré de vulnérabilité de Windows 2000 (30.4.2001).

[Carko : Nouvel outil DDoS](#)

Le CERT informe sur un nouvel outil d'attaque par saturation de service, Carko, utilisant la vulnérabilité snmpXdmid (30.4.2001).

[Carnivore a changé de nom](#)

L'outil utilisé par le FBI pour surveiller les Emails a changé de nom, mais il reste très controversé (30.4.2001).

[Explications de l'ASP](#) (F)

Réponses à des questions sur ce que c'est l'ASP (30.4.2001).

[Vulnérabilité dans SmartDownload](#)

Des spécialistes ont découvert une vulnérabilité dans SmartDownload de Netscape pouvant rendre un PC vulnérable à une attaque (26.4.2001).

[Les soucis du responsable réseau](#)

Des problèmes (maîtrisables) sont apparus suite à l'installation d'un système plus sûr (26.4.2001).

[Nouvelle manière de combattre les virus](#)

Cette nouvelle méthode veut empêcher la propagation des virus, en avertissant l'utilisateur avant d'envoyer un message par exemple. [Autre article](#) à ce sujet qui ne partage pas cette idée (26.4.2001).

[Site international contre la fraude sur Internet](#)

La FTC va mettre en place un site permettant aux Internaute de déposer leur plainte à un seul endroit, en français, anglais, allemand ou espagnol (26.4.2001).

[Risques des systèmes de surveillance](#)

Histoire qui a failli mal tourner pour une personne identifiée par une caméra de surveillance, mais innocente (26.4.2001).

[Sites intéressants](#)

[Site dédié à la lutte contre la criminalité Internet](#) et [autre site dédié à Echelon](#) (26.4.2001).

[L'information sur la sécurité à un prix](#) (F)

Le CERT s'est joint à une association qui fournira à ses membres des informations non gratuites sur la sécurité. [Autre article](#) à ce sujet et [article](#) sur les risques de publier des vulnérabilités avant qu'il existe des correctifs (26.4.2001).

[Hacker & Cie](#)

Histoire d'un hacker qui se prend pour un saint (26.4.2001).

[Augmenter la confiance des E-Consommateurs](#)

Des associations américaines et européennes, établissant des codes de conduite, veulent développer des standards internationaux visant à augmenter la confiance des consommateurs à faire des achats en ligne (26.4.2001).

[Authentification biométrique](#)

Système d'authentification biométrique qui ne se base pas sur des données biologiques mais comportementales (23.4.2001).

[Protection des données personnelles](#)

Le L-Commerce, c'est de localiser le consommateur mobile lorsqu'il utilise son téléphone sans fil, afin de lui proposer une prestation, donc de faire avec lui du M-Commerce. Dans ce cas, il faudra protéger les données recueillies sur le consommateur (23.4.2001).

[IDS - Systèmes de détection d'intrusion](#)

Explications de base des IDS (23.4.2001).

[Risques ftp](#)

Explications des différents risques d'utilisation de ftp et de possibles mesures contre ces risques (23.4.2001).

[Sécurité des Emails sur Linux](#)

Les étapes d'installation de GnuPG (PGP) sur Linux et concept d'envoi et de réception d'Emails sécurisés à l'aide de PGP (23.4.2001).

[Protection des PC portables](#)

Serviette spéciale protégeant un PC portable, par exemple en cas de vol, et commentaire à ce sujet (23.4.2001).

[Se protéger contre les virus](#)

Il n'est pas possible de se protéger à 100% contre les virus, les mesures de protection ne doivent pas nuire à l'efficacité du travail et les risques humains permettront toujours à des attaques virales de réussir. Une [méthode de protection](#) consisterait à se protéger contre des actions malicieuses qu'un virus pourrait déclencher (23.4.2001).

[Se protéger contre les attaques](#)

Mesures de protection contre les attaques Internet. Par exemple le passage à IPSec ou IPV6, mais le chemin pour le faire n'est pas encore évident (23.4.2001).

[Types de virus](#)

Explication des virus script et html (23.4.2001).

[Tester votre sécurité](#)

Vous devez tester votre sécurité, si vous voulez mesurer son efficacité. Dans le cadre des tests d'intrusion, différenciez, si nécessaire dans le mandat, les tests techniques des tests sociaux (23.4.2001).

[Utilisation de la signature électronique](#)

Le chemin est encore long pour généraliser et favoriser l'utilisation de la signature électronique, par exemple instaurer des règles et des standards identiques entre les pays (19.4.2001).

[Nombre de fraudes Internet](#)

Selon la FTC, le nombre de fraudes Internet a augmenté, mais le nombre de fraudes relatives aux enchères en ligne a diminué. [Autre article](#) en F qui dresse le portrait robot du fraudeur (19.4.2001).

[Securitytracker](#)

Site intéressant sur la sécurité (19.4.2001).

[Vulnérabilités des modems ADSL d'Alcatel \(suite\)](#)

Réponse d'Alcatel (19.4.2001).

[Open source vs closed source](#)

Selon MS et contrairement à ce que certains croient, les logiciels ouverts sont moins sûrs que les logiciels propriétaires, car personne ne recherche des vulnérabilités dans les premiers (Peut-être la réciproque serait de dire que beaucoup de monde est occupé à rechercher des vulnérabilités dans les produits de MS par exemple [celle-ci](#) une des dernières en date). Cet [autre article](#) aborde la question de la vulnérabilité aux attaques des logiciels ouverts (19.4.2001).

[Risques des réseaux sans fil](#)

Article plus détaillé que celui du 8.4.2001 sur les risques des réseaux sans fil pouvant être accédés via une voiture correctement équipé (19.4.2001).

[PDA et virus](#)

Discussion sur les risques d'attraper un virus sur un PDA (17.4.2001).

[Installation de RPM](#)

Déchargement sûr et installation de "Red Hat Package Manager" (17.4.2001).

[Bulletin du NIPC](#)

Dernier bulletin des vulnérabilités et correctifs publié par le NIPC (17.4.2001).

[Limites des firewalls](#) (F)

Les firewalls ne sont pas les seules mesures de protection d'un réseau, mais font partie d'un ensemble de mesures basé sur l'évaluation des risques, par exemple le chargement des correctifs de vulnérabilité (17.4.2001).

[Dossier PKI et XML](#) (F)

La France se prépare à la mise en oeuvre de la signature électronique utilisant l'infrastructure à clefs publiques (PKI). Le langage [XML pourrait faciliter](#) l'intégration des diverses technologies PKI (17.4.2001).

[Technique de localisation des terminaux mobiles](#)

Présentation de 4 techniques de localisation des terminaux / téléphones mobiles (17.4.2001).

[Conférence RSA](#)

Articles sur la conférence RSA

- [Avantages et risques](#) de publier les attaques des hacker
- [Nouveaux produits](#) annoncés (F), [autre article](#)
- Les [hackers développent de nouveaux méfaits](#) plus rapidement que les chercheurs développent les parades (17.4.2001).

[Vulnérabilités des modems ADSL d'Alcatel](#)

CERT informe sur des vulnérabilités touchant des modems ADSL d'Alcatel (12.4.2001).

[L'attaque est la meilleure défense](#)

Le gouvernement allemand veut combattre des sites Nazis se trouvant à l'étranger par des attaques de dénie de service (DoS) (12.4.2001).

[Installer un réseau sûr selon un modèle](#)

Installer un réseau sûr selon le modèle de processus de développement des logiciels (12.4.2001).

[Sécuriser les accès via VPN](#)

Mesures de protection contre les connexions faites via VPN (12.4.2001).

[Tester, tester et retester](#)

Article intéressant sur les besoins de tester l'efficacité des procédures, en particulier la réaction des personnes concernées lors des tests (12.4.2001).

[Vulnérabilité de serveurs ftp](#)

CERT informe sur un vulnérabilité pouvant toucher des serveurs ftp, permettant à un hacker d'exécuter des commandes sensibles sur le serveur. Voici 2 autres articles à ce sujet : [1](#), [2](#)(12.4.2001).

[Nouveaux produits de sécurité](#)

Lors de la conférence 2001 de RSA, des entreprises vont annoncer de nouveaux produits améliorant la sécurité des informations (12.4.2001).

[Sécurité des paiements sans fil](#)

MasterCard développe avec une autre entreprise un système de paiement sans fil sécurisé (12.4.2001).

[Se protéger contre les Web bugs](#)

Désactiver JavaScript ou chiffrer les Emails fournit une bonne protection contre les Web bugs. De plus il existe des programmes qui recherchent la présence sur vos disques de ces espions comme Ad-aware de Lavasoft (12.4.2001).

[Infrastructure à clefs publiques](#) (F)

Explication de la signature électronique qui va être introduite en France (12.4.2001).

[MS et la sécurité des informations](#)

MS a revu les termes d'utilisation de son service Passport qui lui permettait un trop grand regard sur les données personnelles des utilisateurs. Mais ces termes ne concernent pas HailStorm. D'autre part, la [nouvelle version d'Outlook](#) (Outlook 2002) bloquera la lecture de certains types de fichiers attachés (10.4.2001).

[Vulnérabilités des réseaux sans fil](#) (F)

Des chercheurs de l'Université du Maryland ont découvert des failles de sécurité dans le protocole WEP (10.4.2001).

[Economiser les coûts informatiques](#) (F)

Gartner explique comment réduire les coûts informatiques, mais selon cet [autre article](#) les réductions ne devraient pas toucher la sécurité informatique (10.4.2001).

[Guerre de l'information et guerre économique](#) (F)

Site dédié à la manipulation de l'information à des fins économiques, de désinformation, etc. (10.4.2001).

[Authentification biométrique](#)

Analyse de certains outils d'authentification biométrique (10.4.2001).

[Sécurité des informations](#)

Série d'articles d'Infosecuritymag d'avril 2001 sur la sécurité des informations (10.4.2001).

[Ver Adore](#)

Information du SANS sur le ver Adore qui crée des portes dérobées dans le système attaqué et voici un [autre article](#) à ce sujet (10.4.2001).

[Informations mensuelles d'ISS](#)

Informations de mars 2001 des vulnérabilités publiées par ISS (10.4.2001).

[Transmission en clair des identifiants et des mots de passe](#)

Des tests confirment que des sites connus transfèrent en clair sur le réseau le mot de passe que vous avez introduit pour entrer dans le système (login) (10.4.2001).

[Glossaire des télécommunications sans fil](#)

Explication des principaux termes utilisés dans le domaine des télécommunications sans fil (6.4.2001).

[Risques des mots de passe partagés des comptes administrateurs locaux sur NT](#)

Mesures pour diminuer les risques des mots de passe des comptes administrateurs locaux qui sont identiques sur les différentes plates-formes NT (6.4.2001).

[Protection des Palm, PDA, etc. contre les virus](#)

Commentaires et suggestions pour protéger les Palm, PDA, etc. contre les virus (6.4.2001).

[Les soucis du responsable de la sécurité](#)

Rien n'est simple, ni évident pour le responsable de la sécurité, par exemple d'avoir deux ISP à la place d'un seul ou de chiffrer les Emails (6.4.2001).

[Se protéger contre les cookies](#)

Si des internautes ne savent pas ce que c'est un cookie, ils ne peuvent évidemment pas se protéger contre (6.4.2001).

[Respect des exigences légales](#)

Les entreprises utilisant Internet doivent s'assurer qu'elles respectent les exigences légales de leur pays et des pays avec lesquels elles échangent des informations (6.4.2001).

[Commentaire sur la vulnérabilité dans IE](#)

Certains utilisateurs ont des difficultés à installer le correctif de MS

(6.4.2001).

[Il faut en moyenne 8 heures pour hacker un site](#)

Selon des experts en sécurité informatique, il faut en moyenne 8 heures à un hacker pour s'introduire dans un site, respectivement 45 minutes si c'est une site universitaire. Cet [autre article](#) est tout aussi alarmant ou alarmiste (6.4.2001).

[Gestion des certificats](#)

Le problème lié à la remise par VeriSign d'un certificat à une personne se faisant passer pour un collaborateur de MS provient probablement d'une erreur humaine dans le processus de gestion des certificats (3.4.2001).

[Bombardement de spam](#)

A Amsterdam, si une personne déclare le vol de son téléphone portable, la police bombarde le téléphone de messages SMS (3.4.2001).

[Etude de KPMG](#)

Selon l'étude de KPMG, 70% des fraudes proviennent de l'intérieur de l'entreprise (3.4.2001).

[Alerte du CERT](#)

Vulnérabilité dans Solaris snmpXdmid permettant à un hacker d'obtenir des accès privilégiés au système (3.4.2001).

[Méfiez-vous des voitures qui rôdent autour de votre entreprise](#)

Selon cet article, des hackers roulant en voiture, munis d'un portable et d'une carte LAN essaient d'accéder au réseau des entreprises (3.4.2001).

[Correctifs de vulnérabilités MS](#)

Derniers correctifs de vulnérabilités soumis par MS, dont [celui-ci](#) (3.4.2001).

[Rapport de la CNIL sur la surveillance électronique des salariés](#)(en français)

Selon la CNIL, le dialogue permettra de trouver un juste milieu entre les employeurs qui risquent de trop contrôler et les salariés qui craignent pour leur liberté (3.4.2001).

[Virus sur Linux](#) (en français)

Des systèmes mal configurés ou des failles non corrigées peuvent rendre des systèmes Linux vulnérables aux virus (2.4.2001).

[Améliorer la sécurité de vos systèmes](#)

10 points à considérer permettant d'améliorer la sécurité de vos systèmes d'information (2.4.2001).

[SLA Service Level Agreement](#) (en français)

Suite d'articles sur le SLA ou le "niveau de qualité de service" ou la "qualité de service garanti" (2.4.2001).

[Choisir le bon antivirus](#)

Points à considérer lorsque vous évaluez différents logiciels

antivirus. Parmi des points intéressants, il y a l'installation du logiciel, la gestion des règles de contrôle des virus, la mise à jour des signatures, la réactivité du fournisseur suite à l'apparition d'un nouveau virus, la possibilité d'obtenir des bulletins d'alerte, etc. (2.4.2001).

[Vulnérabilité du firewall Raptor 6.5](#)

Dans certains cas, il est possible de transmettre des accès http à d'autres ports qu'au port 80 (2.4.2001).

[Attention votre PC vous écoute](#) (en français)

Un cheval de Troie dans votre PC pourrait enregistrer ce que vous dites et le transmettre à un destinataire externe (2.4.2001).

[Autre forme de vulnérabilité](#)


Pour une entreprise, la protection d'une marque peut être tout aussi importante que la protection des systèmes d'information (2.4.2001).

[Avez-vous sécurisé votre serveur BIND](#) (en français)

Résultats d'une étude en France sur la sécurisation des serveurs BIND (2.4.2001).

[Sécurité des télécommunications sans fil](#)

Présentation au CeBIT d'un système de sécurité PKI pour les sans fil. Cet [autre article](#) explique les améliorations au niveau de la sécurité entre les protocoles WEP1 et WEP2, mais que le second reste vulnérable (2.4.2001).



info@Aud-IT.ch

Copyright © 2000-2001 Aud-IT Sàrl. All rights reserved.