

NetCost&Security HEBDO : chaque Vendredi l'HEBDO de la sécurité sur votre Email et Palm™ Pilot avec les liens HTML

Chaque trimestre, la revue *NetCost&Security* : 50 pages d'analyses, de reportages, d'interview, de projets SECUR : prochain numéro **Janvier 2000**

NetCost&Security Hebdo #6 : Vendredi 5 Novembre 1999

ATTENTION : dernier envoi gracieux pour les non abonnés !!!
renseignements : 01 39 69 01 01

1	- CONFIDENTIEL NETCOST&SECURITY : JEAN PHILIPPE BICHARD	1
2	- TENDANCES DE LA SEMAINE	2
3	- VEILLE SÉCURITÉ : OLIVIER CALEFF / APOGÉE COMMUNICATIONS	2
4	- SOLUTIONS : INSÉCURITÉ DES INTRANET STÉPHANE AUBERT/HSC (2 ^{ÈME} PARTIE).....	5
5	- STRATÉGIE : PHILIPPE DE MORRAS / ISS	8
6	- INDICATEUR ATTAQUES VIRALES : LABORATOIRE SARC DE SYMANTEC	10
7	- CHIFFRES ET SITE DE LA SEMAINE.....	10
8	- ANNONCES / PRÉ-ANNONCES DE LA SEMAINE	11
9	- BUSINESS / OPPORTUNITÉS.....	11
10	- ACCORD / DÉSACCORD :.....	11
11	- ABONNEMENT / PROCHAIN ENVOI / CONTACTS AVEC LA RÉDACTION.....	12

1 - CONFIDENTIEL NetCost&Security : Jean Philippe Bichard

EDITO : Quels services SECUR ?

En sécurité, les services occupent une place stratégique. A qui les confier ? Comment les distinguer ? installation, conseils, maîtrise d'ouvrage, maîtrise d'œuvre, intégration, audit, test d'intrusion, recherches de vulnérabilités, ingénierie sociale, veille réglementaire, technologique, concurrentielle, intelligence économique, reporting, externalisation.... Sur ce marché prometteur des éditeurs tels que *ISS, Axent, Network Associates*... n'hésitent pas à proposer de nouveaux services en coopération avec des "Big Five" type *Arthur Andersen, Frost&Sullivan* spécialisée en conseil de "hauts niveaux". Ces derniers semblent en revanche s'intéresser aux services proposés par les intégrateurs !

Jean Philippe Bichard
netcost@bichard.com

2 - Tendances de la semaine

Organisation et sécurité

Rencontre avec deux acteurs discrets et incontournables du monde la sécurité. Le premier travaille dans un grand ministère et occupe un poste stratégique. Le second dirige un cabinet d'audit et de conseils réputé. Les deux observent la même tendance au sujet de l'évolution du secteur. La sécurité au sein des entreprises évolue vers l'organisation et la réglementation. Le haut fonctionnaire veut davantage de transparence notamment au niveau des codes autorisés en France. Il réclame des labels de qualité et encourage le réaménagement du SGDN (Secrétariat Général de la Défense Nationale) notamment en cellule de lutte contre la criminalité informatique. Il souligne que la problématique sécuritaire ne se règle pas à coup de "réglementation".

Le consultant évoque davantage les risques que la sécurité en privilégiant une organisation interne basée sur les ressources humaines, la politique contractuelle... Un individu qui se sent mal au sein d'une organisation devient un facteur de risque. Un observatoire des menaces propre à chaque entreprises constitue à ses yeux la meilleure solution. Bref, l'organisation reste la clé de voûte d'une politique de sécurité.

3 - Veille Sécurité : Olivier Caleff / Apogée Communications

3.1 - Du côté des organismes officiels

Le CERT a publié une mise à jour des attaques détectées récemment. Il ne s'agit pas de nouveaux avis, mais simplement de mettre l'accent sur des vulnérabilités qui semblent être "*à la mode*" en ce moment : la rubrique est intitulée "*CERT/CC Current Activity*". Outre les "classiques" sondages de ports et tentatives d'exploitations de vulnérabilités sur les non-moins classiques applications DNS (TCP/53), FTP (TCP/21 et 20), RPC (TCP et UDP/111) et IMAP4 (TCP/143), il est noté une recrudescence d'attaques de type *Smurf* en ICMP et des serveurs Web avec IIS et MDAC (MS Data Access Components).

Le premier cas se règle en configurant les routeurs de façon adaptée.

Le second, nécessite de surveiller les journaux des serveurs Web avec IIS à la recherche d'expressions telles que "*POST /msadc/msadcs.dll*".

Le CIAC, a émis 3 avis cette semaine, référencés [K-004](#), [K-005](#) et [K-006](#).

Il s'agit tout simplement de la reprise des 3 derniers avis de *Microsoft*, déjà évoqués dans ces colonnes la semaine dernière et respectivement référencés :

- *MS99-044 : "Excel SYLK" Vulnerability*
- *MS99-045 : "Virtual Machine Verifier" Vulnerability*
- *MS99-046 : "Improve TCP Initial Sequence Number Randomness"*

Depuis, le Service Pack 6 est sorti en version US. N'oubliez pas d'appliquer les correctifs nécessaires qui ne seraient pas contenus dans le SP6, dont celui qui corrige la vulnérabilité mentionnée dans l'avis *MS99-046* !

Pour en savoir plus :

- http://www.cert.org/current/current_activity.html
- <http://www.cert.org/advisories/CA-98.01.smurf.html>
- <http://support.microsoft.com/support/kb/articles/q184/3/75.asp>
- <http://www.microsoft.com/security/bulletins/ms98-004.asp>
- <http://www.microsoft.com/security/bulletins/ms99-025.asp>

mais aussi :

- <http://ciac.llnl.gov/ciac/bulletins>
- <http://www.ciac.org/ciac/bulletins/k-004.shtml>
- <http://www.microsoft.com/security/bulletins/MS99-044.asp>
- <http://www.ciac.org/ciac/bulletins/k-005.shtml>
- <http://www.microsoft.com/security/bulletins/MS99-045.asp>
- <http://www.ciac.org/ciac/bulletins/k-006.shtml>
- <http://www.microsoft.com/security/bulletins/MS99-046.asp>

Les chiffres depuis le début de l'année 1999 :

- Le CERT Américain a publié 25 Avis. Ils se décomposent en 13 CA (CERT Advisories), 3 CS (CERT Summaries), 6 IN (Incident Notes), 3 VN (Vulnerability Notes) et aucun VB (Vendor Initiated Bulletins)
- Le CERT Australien a publié 105 Avis. Ils se décomposent en 99 ESB (External Security Bulletins), 4 AL (AusCERT Alerts) 2 AA (AusCERT Advisories)
- Le CIAC a publié 56 Avis. Ils se décomposent en 50 avis "J" (entre le 1^{er} Janvier 1999 et le 30 Septembre 1999) et 6 avis "K" (à partir du 1^{er} Octobre).

3.2 - Nouveaux Avis de Microsoft

Une fois n'est pas coutume, point d'avis Microsoft cette semaine ! Mais avec l'arrivée du SP6, il y a tout de même du travail de qualification et de validation à effectuer, dont les tests de non-régression vis-à-vis des correctifs . . .

Cette remarque ne vous est pas inconnue ? En effet, cela fait 4 fois que je la fais en 2 semaines. Il doit bien y avoir une raison ! Vous la trouverez facilement.

Depuis le début de l'année Microsoft a publié 46 Avis, dont 20 depuis 3 mois.

Quant au 47^{ème} avis, il se pourrait bien qu'il concerne un déni de service sur les plates-formes Windows NT, et plus particulièrement l'absence de contrôle sur le code de retour d'une fonction de décodage des RPC Netbios sur le port TCP 139. Le code d'attaque ayant été publié, et les correctifs non encore disponible, il convient de vérifier les mécanismes de filtrage mis en place, par exemple au niveau de routeurs frontaux des serveurs NT, sur le port TCP 139.

3.3 - Environnement de synchronisation de Palm Pilot™

Voici maintenant un avis qui va intéresser tous ceux d'entre vous qui lisez *NetCost&Security Hebdo* sur votre *Palm Pilot™* ou qui avez des adeptes du *PalmOS* dans votre entreprise (il y en a forcément !).

Une vulnérabilité du gestionnaire de synchronisation par le réseaux des *Palm Pilot™* (*Network HotSync Manager*) avec un système sous Windows 98 a été découverte.

Network HotSync Manager est le logiciel permettant la synchronisation des *Palm Pilot™* avec un serveur au travers d'un réseau local ou distant en TCP/IP.

La vulnérabilité est susceptible d'entraîner un déni de service. Elle a ainsi pour effets possibles de saturer le module serveur, d'en perturber son fonctionnement, et de pouvoir ensuite lui faire exécuter du code malintentionné.

Il n'y a pas encore de correctif, mais le problème a été reconnu par *3COM/Palm Computing*. Si vous avez mis en place une solution de synchronisation de *Palm Pilot™* par le réseau, il est recommandé d'utiliser une machine de type Serveur NT (non vulnérable), et en cas de non utilisation de *Network HotSync Manager*, d'ajouter le port TCP 14238 à la longue liste des ports "sensibles" dans les outils de détection d'intrusion.

Une autre solution est de migrer votre parc de *Palm Pilot™* sous *PalmOS 3.3*, puisqu'il y a maintenant des possibilités d'authentification par mots de passes non rejouables.

3.4 - Nouveaux virus à l'horizon

Certaines sources d'informations évoquent depuis 2 semaines des techniques pour faire passer des virus en environnement Windows dans des fichiers à l'extension anodine (jpg, gif, txt, . . .). Il s'agit en particulier de vulnérabilités qui seraient liées aux fichiers d'extension ".shs".

Un avis a été publié par [Finjan Software](#), sous le titre "*Microsoft Office Scrap File Exploit*". Par mesure conservatoire, il est utile de vérifier que votre anti-virus analyse bien TOUS les fichiers sur votre poste de travail, même ceux dits "systèmes" ou "cachés", c'est-à-dire avec certains suffixes, tels ".shs" ou ".lnk".

D'autre part, la société [Aladdin Knowledge Systems](#) a annoncé la découverte d'un nouveau type de macro virus qui contamine aussi les répertoires de démarrage de Microsoft Office.

Il contaminerait le fichier modèle général de Word "*normal.dot*", créerait un fichier spécial "*SNrml.dot*" dans le répertoire "*STARTUP*" d'*Office* et donc continuerait à infecter les documents même si le "*normal.dot*" redevient sain. Il modifierait aussi la configuration de Word de façon à en diminuer le niveau de protection général, comme pour préparer le terrain à d'autres virus plus nocifs.

Son nom ? *W97M.BMH* ... ou *BMH* en raccourci.

Comment le combattre ? Sa réputation est déjà telle qu'il semble qu'il faille disposer d'un anti-virus à jour et particulièrement efficace pour viser son "talon d'Achille" ...

Surveillez donc les arrivages de vos fournisseurs d'anti-virus dans les jours à venir ...

Pour en savoir plus :

- http://www.finjan.com/attack_release_detail.cfm?attack_release_id=18
- <http://www.stiller.com/shs.htm> (déjà mentionné en Août 1998)
- <http://www.informationweek.com/langaletter>
- <http://www.eAladdin.com>
- <http://www.cti.fr/virus.htm>

Olivier CALEFF, Directeur Technique, APOGEE Communications
o.caleff@apogee-com.fr

4 - Solutions : Insécurité des intranet Stéphane Aubert/HSC (2^{ème} partie)

4.1 - Écoutes de réseau

Très peu d'Intranets sont aujourd'hui protégés contre les écoutes de réseau. Sur l'Intranet sont amenées à transiter des informations comme des données comptables, des données sensibles liées aux applications métiers de l'entreprise, le courrier électronique, les mots de passe (indirectement les mots de passe Windows NT), etc... L'écoute du réseau est locale. L'écoute d'un sous-réseau distant, sur l'Intranet ou sur Internet, n'est généralement réalisable que par la prise de contrôle totale d'une machine à distance, soit un piratage.

Le *sniffer* nommé *linsniffer* est un petit programme de 240 lignes qui permet, par écoute du réseau, de capturer et d'afficher en clair les mots de passe des utilisateurs qui utilisent les protocoles POP3, IMAP, FTP, telnet et rlogin. POP3 et IMAP sont utilisés quotidiennement pour, par exemple, transférer depuis un poste sous Windows son courrier électronique reçu par le serveur de l'entreprise. FTP peut être utilisé par des utilisateurs ou des applications pour transférer des fichiers. Telnet et rlogin sont principalement utilisés pour se connecter de manière interactive non sécurisée sur un serveur.

L'exécution de ce programme fournit le résultat suivant (directement dans le fichier texte "tcp.log") lorsque l'utilisateur Pierre sur la machine VENUS lit son mail sur la machine MAIL via le protocole POP3 (110/tcp) :

```
Résultat de la commande : linsniffer
venus.hsc.fr => mail.hsc.fr [110]
USER pierre
PASS 123soleil
STAT
QUIT
```

Le mot de passe de cet utilisateur sur le serveur MAIL est 123soleil, il permettra de lire le courrier électronique à la place de son réel possesseur et donnera souvent la possibilité de se connecter à la place de l'utilisateur sur le serveur.

Ce *sniffer* permet, en écoutant les connexions telnet, de capturer aussi simplement les mots de passe des routeurs lorsque ceux-ci sont configurés depuis les postes des administrateurs. Prendre le contrôle des routeurs revient à prendre le contrôle du réseau.

Lorsque vous êtes sur un Intranet protégé par une passerelle de sécurité d'accès à Internet (en langage marketing : un firewall) et que cette passerelle vous demande un mot de passe pour vous identifier, ce mot de passe circule en clair (sans chiffrement) sur le réseau. Lorsque vous accédez à des informations sensibles sur votre serveur Intranet et que vous devez vous identifier avec votre mot de passe, il circule en clair sur le réseau.

Le *sniffer web_sniff* est spécialisé dans l'écoute de requêtes HTTP, le protocole utilisé pour visiter, sans chiffrement, les sites Web. Il permet de connaître les adresses des pages visitées et d'afficher les mots de passe utilisés soit pour sortir sur Internet soit pour accéder à des informations sensibles sur Intranet.

```
Résultat de la commande : web_sniff -v
[x.x.x.x] [3648] => [y.y.y.y] [3128]
GET http://rufus.chenil.int/ HTTP/1.0
...
User-Agent: Mozilla/4.5b2 [en] (X11; I; Linux 2.0.34 i586)
...
-----[ USER = pierre PASS = 123soleil ]-----
```

Le mot de passe ne circule pas en clair dans le cas d'un réseau utilisant uniquement Windows NT ou dans le cas de l'utilisation du protocole HTTPS (HTTP avec chiffrement). Toutefois, dans le cas de Windows NT un programme de cassage de mots de passe NT fonctionne très bien, il se nomme *L0phtCrack*. Toujours dans ce cas, il est important de savoir que même avec Windows NT dernière version, les pages visitées circulent en clair sur le réseau et peuvent être entièrement capturées avec le *sniffer sniffit*.

Dans le cas de l'utilisation du protocole chiffré HTTPS (limité en France à RC4 et 40 bits), les pages Web visitées peuvent être capturées chiffrées (avec *sniffit*) et décodées, avec par exemple, deux programmes client/serveur : *master.c* et *slave.c* (<http://pauillac.inria.fr/~doligez/ssl/press-conf.html>).

Le programme *L0phtcrack*, disponible sur Internet, a été détaillé dans une présentation de Denis Ducamp

- <http://www.ossir.org/ftp/supports/99/motdepasse/crackNT/>

au sein du groupe Sécurité Windows NT de l'Ossir (Observatoire de la Sécurité des Systèmes d'Information & des Réseaux).

Cet outil écoute les protocoles Microsoft sur le réseau pour capturer des empreintes chiffrées non réversibles de mot de passe NT et essaye par essais successifs de retrouver les mots de passe correspondants. Cet outil peut, dans

certaines entreprises, trouver jusqu'à 80% des mots de passe des utilisateurs en moins d'une journée.

La disponibilité de tous ces outils d'écoute de réseau, comme *snmpsniff* qui permet d'obtenir les communautés SNMP et administrer de nombreux équipements réseaux, met en danger de manière évidente les réseaux Intranets non sécurisés.

4.2 - Découverte de réseau

La découverte du réseau consiste à trouver des information sur ce réseau comme les adresses IP des machines connectées, l'emplacement logique des routeurs, des serveurs de nom (DNS), des serveurs Web, des serveurs de courriers électroniques, des serveurs sensibles (applications métiers, comptabilité, stations des directeurs).

Il y a deux méthodes pour découvrir le réseau. L'une est passive discrète mais peu exhaustive. L'autre est active, plus voyante, mais très complète.

La méthode passive est fondée sur l'écoute de réseau avec un *sniffer* comme *tcpdump*. Cette méthode permet de visualiser ce qui circule sur le réseau (flux Web, flux DNS, flux de courrier électronique) et de découvrir les clients et les serveurs pour chaque type d'application.

Une ligne de résultat de la commande : `tcpdump -q dst port domain` qui sélectionne sur le réseau les requêtes DNS :

```
14:55:09.998063 pluton.hsc.fr.1319 > ns.hsc.fr.domain: udp 30.
```

```
14:55:46.605247 neptune.hsc.fr.2657 > ns.hsc.fr.domain: udp 41
```

Le serveur ns.hsc.fr est très certainement, dans cet exemple, un serveur DNS.

Remarquons que l'écriture d'un sniffer est aujourd'hui possible en langage perl. Voici un exemple écrit pour l'occasion qui permet de découvrir des serveurs Web :

```
#!/usr/local/bin/perl -w
use Net::RawIP;
use Socket;

$a = new Net::RawIP;
$pcap=$a->pcapinit("eth0", "proto \\tcp and dst port 80",1500,30);
loop $pcap,-1,&dumpit,@a;
sub dumpit {
$a->bset(substr($_[2],14));
($ipsrc,$ipdst,$source,$dest,$data) = $a->get({ ip=>[qw(saddr daddr)],tcp=>[qw(data source dest)]});
print "Flux tcp/80 from ",inet_ntoa(pack("N",$ipsrc)), "[ $source ] to ",
inet_ntoa(pack("N",$ipdst))"\n";
# print $data, "\n" if($data =~ /^Proxy-authorization:/);
};
```

Résultat obtenus avec ce *sniffer* (13 lignes de langage Perl) :

```
Flux tcp/80 from 192.168.2.65[1689] to 192.168.1.50
Flux tcp/80 from 192.168.2.52[1312] to 192.168.1.50
Flux tcp/80 from 192.168.1.100[1725] to 192.168.1.50
Le serveur ayant l'adresse IP 192.168.1.50 héberge très certainement un serveur Web.
```

La découverte active est fondée sur des techniques de *scan*. Un des outils gratuits les plus connus est le programme Satan qui a beaucoup vieilli. Un des outils les plus performants (et gratuit) aujourd'hui pour effectuer le *scan* d'un réseau s'appelle *Nmap*. Il possède de nombreuses options de fonctionnement, il peut envoyer des paquets ICMP-echo-request (*Ping*) pour découvrir toutes les machines accessibles sur un réseau (même distant). Il peut aussi faire la même chose, lorsque ICMP est bloqué par les routeurs, avec des paquets TCP de type ACK et attendre les paquets de type Reset correspondants. Il est surtout capable d'établir rapidement la liste des ports TCP ou UDP accessibles sur toutes les machines de l'Intranet.

```
Résultat de la commande : nmap -O shootme.test.fr
Interesting ports on shootme.test.fr (192.168.1.77):
Port      State  Protocol      Service
21        open  tcp           ftp
22        open  tcp           ssh
42        open  tcp           nameserver
53        open  tcp           domain
80        open  tcp           http
139       open  tcp           netbios-ssn
1723     open  tcp           pptp
Remote operating system guess: Windows NT4 / Win95 / Win98
```

Pour en savoir plus :

- 3^{ème} partie dans le prochain numéro, à paraître le 12 Novembre 1999

5 - Stratégie : Philippe de Morras / ISS

- **Quels éléments différenciateurs distinguez-vous chez ISS parmi les services dédiés à la sécurité ?**

Différents éléments :

X-FORCE, 50 personnes qui travaillent sur la recherche de nouvelles failles et menaces, sur de nouvelles technologies (attaques non structurées notamment), et cela au niveau réseau, OS, base de données.

Reconnu mondialement comme le centre d'experts en sécurité, (les plus grands nous font confiance comme IBM, Microsoft,...), ce département unique et inexistant chez les éditeurs concurrents est à même de fournir la MEILLEURE réactivité gage de valeur des solutions de sécurité.

En effet, avec les "X-Press updates" qui permettent à l'utilisateur de gérer facilement la mise à jour des produits (sans rechargement, temps réduit au minimum,...) ISS offre la mise à jour la plus proactive/réactive (ex : BackOrifice 2000 solutionné en 24 heures, les clients ayant l'update immédiatement).

Cette différenciation touche aussi la notion de service. L'expertise en sécurité d'ISS est aussi disponible à travers le département "Professional services", qui présente une offre allant de SAVANT (expertise complète dans un classeur sur NT, UNIX,...), de l'assistance de très haut niveau tant dans la définition, la formation, l'implémentation des solutions ISS dans les grandes structures. Enfin, encore une spécificité d'ISS, c'est aujourd'hui aussi le seul éditeur à proposer une offre complète de gestion de la sécurité des clients pouvant aller jusqu'à l'"outsourcing" complet de la sécurité avec un niveau d'engagement sur la performance et l'efficacité.

- **Sur la stratégie Produit, considérez-vous que ISS doit persister à découper ses solutions en module ou offrir une plate forme unique et fédératrice ?**

La position d'ISS reste la même. N°1 incontesté dans son domaine, ISS affiche des résultats plus importants (voir les résultats Q3 et combinés depuis le début 99) que d'autres éditeurs ayant une "panoplie" d'outils, firewall, *Single Sign-On*, chiffrement, etc... ISS garde sa stratégie qui repose sur 2 axes :

- être et rester le N°1 dans le *vulnerability assessment* et *intrusion detection management* ainsi que les services associés
- être ouvert à l'ensemble des acteurs de la sécurité : l'Adaptative Network Security Alliance qui regroupe 55 des principaux acteurs mondiaux des télécoms-réseaux-sécurité (IBM, HP, 3COM, NORTEL, BAY, RSA, CHECKPOINT,...) permet au client final de choisir dans chaque domaine les meilleurs produits, puis SafeSuite Decisions, plateforme d'intégration, permet de compiler/analyser et reporter les informations/données qui viennent des diverses solutions ISS mais aussi d'autres éditeurs.

Donc, nous ne serons jamais un "*one stop shopping*" éditeur ; cette stratégie montre ses limites tant au niveau de la qualité que de la pérennité des produits car l'investissement en R&D pour rester au "top" niveau est trop important pour financer toute une gamme de produits différents comme un firewall, un outil de chiffrement, de l'*intrusion detection*, *Single Sign-On*,...

- **Quelle évolution envisage ISS pour diffuser ses produits auprès de partenaires tels que CheckPoint : existera t-il des versions restreintes de RealSecure par exemple ?**

Il est un fait incontestable, c'est que les "grands" OEMisent les produits... d'ISS ! Aussi, certaines questions peuvent venir à l'esprit des utilisateurs.

Aujourd'hui, certaines sociétés comme CheckPoint, ODS,... ont OEMisé nos produits ; les fonctionnalités de ces produits sont les mêmes que les produits "natifs" ISS, ex, RealSecure : cependant, dans ces versions OEMisées, le client

peut y trouver une intégration encore plus forte telle que l'intégration de RealSecure avec Firewall-1. D'autres OEMisations viendront, apportant à l'utilisateur final les meilleures fonctionnalités intégrées dans ses contraintes d'environnement. Aujourd'hui, la partie RealSecure agent-Reseau est l'objet de cette approche ; demain, nous pouvons imaginer la même chose pour la partie agent-système de RealSecure.

Pour en savoir plus :

- <http://www.iss.net>

Propos recueillis par Jean Philippe Bichard

6 - Indicateur attaques virales : Laboratoire SARC de SYMANTEC

Le Top 5 des virus en Europe est :

- Happy99.Worm
- W97M.Ethan.A
- W97M.Class
- W97M.Melissa.A
- W95.CIH
- 6. VBS.Freelinks

Le Top 5 des virus en France est :

- Happy99.Worm
- 2. W97M.Ethan.A
- 3. W95.CIH
- 4. O97M.Tristate.C
- 5. Prettypark.Worm

7 - Chiffres et site de la semaine

7.1 - Les Chiffres de la Semaine

NDLR: ces chiffres n'engagent que les sources citées entre parenthèse et en aucun cas NetCost&Security

- Selon IDC, d'ici la fin de l'année 1999, le nombre d'entreprises françaises proposant une offre en commerce électronique sera multiplié par cinq. En 1996 le commerce électronique a généré 1,6 milliard de FF de chiffres d'affaires. En 2003, IDC prévoit 277 milliards de FF. Les "cybervendeurs" estimés à 120 000 en 2003 devraient générer pour 9 MdF de ventes de logiciels, matériels et services. La part réservée à la sécurité n'a pas été étudiée par IDC mais des freins à la consommation via le canal du e-business sont constatés par de nombreux consultants au niveau de l'authentification, la confidentialité et l'accessibilité.

7.2 - Le Site WEB de la semaine, sélectionné par la rédaction

Intrusion Detection FAQ [Version 0.93]

- http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

8 - Annonces / Pré-annonces de la semaine

Stac annonce la version 2.0 de *Replica Network Data Manager*

- <http://www.stac.com>

APC propose le concept *Redudant Switch* et les prises anti foudre et anti surtensions *SurgeArrest*

- <http://www.apcc.com>

AB Soft rend disponible la version 4.7 de son logiciel antivirus *Norman Virus Cleaner*

- <http://www.absoft.fr>

Copernet, importateur, grossistes et éditeur en environnement NT lance *FileAudit*, outil d'audit des accès à NT

- <http://www.copernet.com>

9 - Business / opportunités

Remedy développe le plus grand projet de Help Desk au monde.

- <http://www.remedy.com>

Intel a effectué le 25 octobre son plus vaste lancement en proposant 15 processeurs rattachés à la famille *Pentium III* et *Pentium III Xeon*.

- <http://intel.com/français/pr>

Cisco se trouve à l'initiative d'un programme humanitaire sur le Web en collaboration avec les *Nations Unies*. Plus d'un millier d'organisations à but non lucratif ont rejoint le projet.

- <http://www.netaid.org>

10 - Accord / Désaccord :

Quadravec, éditeur de *Time Navigator*, s'implante aux États-Unis.

- <http://www.quadravec-software.com>

ODS Networks et Neurocom signent un accord de partenariat afin que la gamme SecuCom du premier soit commercialisée par le second.

- <http://www.ods.com>

11 - Abonnement / prochain envoi / contacts avec la rédaction

Pour vous abonner immédiatement : 01 39 69 01 01
<http://www.bichard.com>

ATTENTION
dernier envoi gracieux pour les non abonnés

NetCost&Security Hebdo #7 : Vendredi 12 Novembre 1999

Trimestriel 50 pages : Janvier 2000 (Publicité : 01 40 92 05 55)

Pour joindre la rédaction en cas d'urgence ! 06 09 61 84 68

Bonne lecture et excellente semaine "SECUR"

[Jean-Philippe BICHARD](#)
netcost@bichard.com