CYBERDÉFENSE : LES ENJEUX ET LES SOLUTIONS INFORMATIQUES OFFENSIVES

telindus
belgacom ICT

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SOMMAIRE

À PROPOS
DES DEUX PARTENAIRES

telindus
belgacom ICT

Telindus est l'un des leaders mondiaux des services et des solutions des technologies de l'information et de la communication adaptées aux entreprises et administrations.

Depuis plus de 40 ans, Telindus met au service de ses clients son expertise technologique dans les domaines du Data Center, du Réseau, de la Sécurité et de la Collaboration leur permettant ainsi d'intégrer des solutions technologiques innovantes et fiables. Telindus réalise des prestations de conseil, de déploiement, de support et d'exploitation déléguée, en s'appuyant sur des partenariats technologiques mondiaux à forte valeur ajoutée, tels que Cisco, EMC², Check Point, F5, Juniper et VMware pour lesquels il représente généralement le premier partenaire en France.

Pour répondre aux exigences qualité de ses clients, Telindus se doit d'être à la fois fiable et méthodologique et s'appuie sur des standards reconnus : PMI, ITIL, ISO 9001 et ISO 14001.

Parmi les clients de Telindus figurent les plus grandes entreprises, nationales et internationales, les opérateurs, les administrations et les grandes collectivités.

Telindus est une filiale du Groupe Belgacom, un des leaders dans le monde des télécommunications.

Pour plus d'informations, rendez-vous sur :
www.telindus.fr

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Software Technologies Ltd le leader mondial de la sécurité Internet, fournit à ses clients une protection sans faille contre tous types de menaces, tout en réduisant la complexité de la sécurité et le coût total de possession. Il est le pionnier de l'industrie avec FireWall-1 et sa technologie brevetée «stateful inspection».

Aujourd'hui, Check Point continue d'innover grâce à l'Architecture Software Blade et offre à ses clients des solutions flexibles, simples d'utilisation et entièrement personnalisables, afin de répondre aux besoins de sécurité exacts de toute organisation. Il est le seul fournisseur qui, par delà l'aspect technologique, définit la sécurité comme un processus business. Check Point compte parmi ses clients les 100 sociétés figurant au classement des Fortune 100 ainsi que plusieurs dizaines de milliers d'entreprises et d'organisations de toute taille.
Par ailleurs, les solutions ZoneAlarm protègent les PC de millions de particuliers contre les pirates, les logiciels espions et les vols de données.

Pour plus d'informations, rendez-vous sur :
www.checkpoint.com
et www.france.checkpoint.com

CHIFFRES CLÉS

338

Le coût annuel, en milliards de dollars, du cybercrime dans le monde.[2]

2,5 Coût, en milliards d'euros, de cybercrimes subis par des particuliers en France en 2012. La même année, au plan mondial, le cybercrime a coûté 110 milliards de dollars aux particuliers.[1]

5,9 Soit le coût moyen, en millions de dollars, du cybercrime pour une grande entreprise américaine (700 salariés et plus). Un chiffre en augmentation de 56 % par rapport à l'an dernier.[3]

72 Le nombre, par semaine, d'attaques informatiques enregistré par les entreprises américaines en 2012 (+ 44 % par rapport à 2011).[3]

1/4 Nombre d'ordinateurs connectés à Internet dans le monde qui serait sous le contrôle d'un botnet.[4]

63 Pourcentage des 888 entreprises et organisations auditées en 2012 dont les systèmes informatiques étaient infectés par des vers informatiques.[5]

5 000 Soit le nombre de nouvelles vulnérabilités découvertes en 2012, permettant aux hackers d'accéder aux systèmes informatiques et de causer des dommages.[6]

43 Soit le pourcentage des 853 responsables informatiques interrogés dans le monde déclarant avoir été ciblés par des attaques d'ingénierie sociale en 2012.[7]

4,5 C'est le nombre, en millions et en 2011, d'ordinateurs asservis à un botnet par TDL-4, quatrième version du cheval de Troie TDL apparu en 2008.[8]

20 Le ver informatique Flame, découvert en 2012 était 20 fois plus élaboré que le ver Stuxnet, découvert pourtant seulement deux ans plus tôt.[8]

500 Soit le prix moyen, en dollars, d'un kit de développement pour créer un Botnet vendu sur Internet.[5]

14 Soit le nombre, en milliards de spams quotidiens (!) envoyés tous les jours par les machines asservies au botnet Rustock, démantelé en 2011 par Microsoft et le FBI.[9]

1 : Norton Cybercrime Report 2012
2 : Commission européenne.
3 : HP 2012 cyber risk report.
4 : Estimation de l'ingénieur Vint Cerf, l'un des pères fondateurs d'Internet.
5 : Check Point 2013 security report.
6 : Statistiques du site Common vulnerabilities and exposures (cve.mitre.org).
7 : Etude 2011 Dimensional Reseach/Check Point.
8 : Kaspersky Labs.
9 : Microsoft.

ENJEUX DU MARCHÉ ET DES ENTREPRISES

En 2008, un livre blanc soulignait que la cybersécurité était un enjeu majeur pour la France et ses entreprises durant les 15 années à venir.
Vœu pieux ?

L'exemple de l'entreprise de télécommunication canadienne Nortel offre un mémorial cuisant à cet impératif. Car la banqueroute de Nortel, en faillite depuis 2009, a assurément été causée par un piratage non détecté de ses SI. Durant une décennie, les pirates ont accédé, quand ils le voulaient, aux documents financiers et à la R&D de l'entreprise, réussissant même à se logger aux systèmes Nortel – d'après le Wall Street Journal – grâce à des mots de passe volés à sept des plus hauts dirigeants de l'entreprise !

> Le cybercrime coûte, en moyenne en 2012, six millions de dollars par entreprise américaine, soit 56 % de plus qu'en 2011 !
>
> Source : HP2012 cyber risk report

Le Wall Street Journal ainsi que le New York Times ont eux-mêmes annoncé début 2013 que leurs systèmes informatiques avaient été infiltrés avec vol de mots de passe, détournement de compte e-mail et copies ou destruction de documents de leurs employés.

Le cybercrime ne mène pas forcément à la faillite comme Nortel, mais il coûte.
Cher : six millions de dollars, en moyenne en 2012, par entreprise américaine, soit 56 % de plus qu'en 2011 ! Face à l'évolution permanente des outils et techniques de piratage (vers, ordinateurs asservis à un botnet…), **les techniques classiques de protection** (pare-feu et antivirus), même régulièrement mises à jour (ce qui est loin d'être partout le cas) **gardent leur pertinence** pour le « tout-venant » des attaques **mais ne sont plus efficaces contre les plus élaborées**.

Exemple avec l'attaque « **Nitro** » en 2011. Pour récupérer les secrets de 48 entreprises de la chimie et de la défense, les pirates ont utilisé un outil de contrôle à distance des ordinateurs, appelé « **Poison Ivy** », implanté dans le SI des entreprises cibles via… un e-mail piégé envoyé à leurs employés qui avait ainsi contourné antivirus et firewall ! Car les cyberattaques emploient non seulement des outils techniques complexes, mais aussi de « l'ingénierie sociale » : ils abusent des employés via les réseaux sociaux (Facebook, Twitter) ou par e-mail et « passent » ainsi les premières défenses des SI des entreprises.

> Les cyberattaques emploient non seulement des outils techniques complexes, mais aussi de « l'ingénierie sociale ».

Les systèmes industriels ont quant à eux été longtemps jugés en sécurité du fait qu'ils ne sont pas connectés à Internet. Erreur, comme l'a prouvé le ver Stuxnet en 2010 (conçu originellement pour détraquer l'industrie nucléaire iranienne), erreur mainte fois prouvée depuis (déraillement d'un tramway en Pologne, rupture de pipeline, pollution des eaux…). **Rien n'est à l'abri** : gestion technique des bâtiments (GTB), gestions techniques centralisées (GTC), systèmes embarqués, supervisions de contrôle (SCADA, supervisory control and data acquisition)…
Les « pires craintes d'attaques sur les installations sensibles peuvent se réaliser » dixit l'ANSII (Agence nationale de la sécurité des services d'information).

Le front de la cybercriminalité s'est donc élargi : des seules attaques directes aux systèmes d'informations des entreprises, **la guerre porte désormais aussi sur la lutte contre l'ingénierie sociale et la protection des systèmes industriels**. La très populaire technologie du Cloud computing, si elle peut s'avérer un vrai atout concurrentiel pour l'entreprise, a, elle aussi encore élargi le champ de malfaisance des cybercriminels. Idem pour une mode managériale en vogue, le BYOD (« apportez votre appareil personnel ») qui complique la sécurité de terminaux, par nature hétérogène.

La lutte, impérieuse, contre le cybercrime va entraîner des changements dans les entreprises. Lesquelles ne peuvent plus raisonnablement considérer les dépenses de sécurité informatique « comme une variable d'ajustement », dixit une récente note du Centre d'analyse stratégique (CAS).

> Les « pires craintes d'attaques sur les installations sensibles peuvent se réaliser ».
>
> Source : l'ANSII (Agence nationale de la sécurité des services d'information)

> Une bonne politique de sécurité doit servir d'appui au business, pas à l'entraver.
>
> Source : rapport de sécurité 2013 de Check Point

Le CAS poursuit : « Le montant des investissements nécessaires à assurer la sécurité des systèmes d'information est connu : entre 0,5 et 2 % du chiffre d'affaires des entreprises. » Un montant important (mais relatif, le gouvernement américain investissant 50 milliards de dollars sur la cyberdéfense entre 2010 et 2015) à investir avec discernement dans une protection multi-couche : filtrage des URL, contrôle des applications, protection contre les malwares et les bots, formation du personnel aux risques informatiques, monitoring des activités réseau et outils d'analyses d'évènement.

Autant de briques non à empiler sans rime ni raison, mais à coordonner, car, ainsi que le rappelle le rapport de sécurité 2013 de Check Point : « **Une bonne politique de sécurité doit servir d'appui au business, pas à l'entraver.** »

TÉMOIGNAGES D'EXPERTS

NOËL CHAZOTTE

DIRECTEUR MARKETING SÉCURITÉ DE TELINDUS

telindus
belgacom ICT

LES CYBERMENACES ÉVOLUENT, LES SOLUTIONS TRADITIONNELLES SONT-ELLES ENCORE PERTINENTES ?

Firewall, proxy et antivirus restent indispensables et contribuent à la sécurité des réseaux. Mais il faut aujourd'hui les compléter par des solutions travaillant sur des aspects plus particuliers : sécurisation de certaines applications, vérification de l'authentification des personnes qui se connectent, …
C'est un complément aux briques actuelles qu'il va falloir mettre en place.

POURQUOI LA PROBLÉMATIQUE DE SÉCURITÉ PARAÎT-ELLE PLUS SAILLANTE AUX USA QU'EN FRANCE ?

Aux USA, une entreprise qui se fait voler des données, non seulement en subit l'impact direct sur son business, mais elle tombe aussi sous le coup de lois lui imposant des pénalités pour n'avoir pas mis en place de solution empêchant la fuite de données sensibles. N'ayant pas cette législation en France et en Europe – mais ça viendra, j'en suis convaincu – tout dépend de la prise de conscience, dans chaque entreprise, du risque encouru.

EXISTE-T-IL UN SCHÉMA « GÉNÉRIQUE » DE PROJET DE CYBERDÉFENSE ?

Il n'y a que des cas uniques : **presque chaque entreprise à ses spécificités et sa méthode de fonctionnement vis-à-vis d'Internet et de son système d'information**. L'industrie automobile n'a pas les mêmes problématiques qu'un établissement financier. **Nos consultants vont donc d'abord comprendre le métier du client, ses risques potentiels et les éléments critiques** qu'on pourrait retrouver sur leur réseau. C'est là que l'on parle « d'impact redouté » que l'on va identifier avec les directions métiers de nos clients. L'impact redouté est la réponse à la question « À partir de quel moment, en cas de cyberattaque, un incident sur mon système d'information impacte-t-il directement mon cœur de métier, ma production ? ».

PERFECTIONNER LA SÉCURITÉ INFORMATIQUE D'UNE ENTREPRISE IMPOSE-T-IL FORCÉMENT UN « BIG BANG » SUR LES SOLUTIONS DÉJÀ EN PLACE ?

À un moment, nos consultants se mettent à « jouer » le rôle d'un attaquant hypothétique en faisant des tests intrusifs ciblés autour de ces données sensibles. L'idée est de mieux évaluer le niveau actuel de sécurité de l'entreprise et d'être du coup plus précis et plus mesuré dans les règles à mettre en place pour améliorer le niveau de sécurité. On va ainsi travailler avec des partenaires comme Check Point et faire évoluer leurs éditeurs sans créer de big bang chez un client qui en serait déjà équipé, par exemple.

POUVEZ-VOUS EXPLIQUER LA STRATÉGIE SDR (SURVEILLER, DÉTECTER, RÉAGIR) QUI GUIDE VOS PROJETS DE CYBERSÉCURITÉ ?

Sur le principe, **il s'agit d'une analyse du système d'information se basant sur le modèle de la défense en profondeur, et prenant en compte le référentiel ISO 27001**. On identifie les barrières de sécurité protégeant le bien à préserver des attaquants potentiels. Sur chacune de ces barrières, on voit si l'on est capable d'effectuer une surveillance digne de ce nom.
Est-on aussi capable de détecter une menace et enfin, est-on capable de réagir ?
La surveillance, toutes les briques en sont, *a priori,* capables. La détection est déjà plus problématique puisqu'on ne détecte que ce que l'on peut voir or les attaques d'aujourd'hui sont souvent furtives. Enfin la réaction : elle sera automatique si les systèmes de sécurité sont suffisamment « intelligents », mais on aura toujours besoin d'une analyse et d'une réaction humaine. Si une alerte remonte, il faut que l'administrateur du SI sache les procédures à suivre face à cette alerte.
Nos consultants vont les aider à élaborer et mettre en place ces procédures, car la réaction doit être rapide pour empêcher ou limiter les dégâts.

UNE FOIS ACHEVÉ LE PROJET DE CYBERDÉFENSE, L'ENTREPRISE CLIENTE EST À L'ABRI ?

Toute solution de sécurité peut être efficace à l'instant T, mais les attaques évoluent constamment. La cyberdéfense c'est, selon nous, un service de sécurité qui s'inscrit dans le temps. Il faut faire évoluer les matériels, les logiciels et continuer à travailler sur l'interprétation des signaux et l'élaboration de nouvelles procédures. Un reporting constant est aussi vital pour aider les managers à prendre les décisions adéquates et à rester maîtres de leur cybersécurité dans le temps.

TÉMOIGNAGES D'EXPERTS

THIERRY KARSENTI

DIRECTEUR TECHNIQUE EUROPE CHECK POINT

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

QU'EST-CE QUE L'INGÉNIERIE SOCIALE ?

C'est la collecte, sur Internet et les réseaux sociaux personnels (Facebook) et professionnels (Linkedin…) d'informations sur une ou plusieurs personnes cibles. Ces informations, le hacker en a besoin pour que la fameuse cible soit en confiance et ouvre, par exemple une pièce jointe ou clique sur un lien dans un message. C'est ce qui est arrivé en mai dernier avec l'attaque sur l'Élysée.

Autre exemple : un hacker voit qu'une « cible » annonce sur Facebook qu'elle participe à un séminaire au Sofitel de Nantes. Le lendemain, il lui envoie un e-mail émanant soi-disant du Sofitel pour lui demander, par exemple, de répondre à un questionnaire de satisfaction. Il y aura peut-être même un gain à la clé pour que la « cible » soit encore plus motivée à cliquer sur le lien. La difficulté pour le hacker c'est d'avoir assez d'infos pour mettre en confiance sa cible afin qu'elle fasse ce dont il a besoin pour lancer techniquement son attaque. **Les attaques ciblées, pas celles de masse, ont toujours une composante d'ingénierie sociale.**

QUELLE EST L'ÉVOLUTION ACTUELLE DE L'INGÉNIERIE SOCIALE ?

L'ingénierie sociale existe depuis que le piratage existe. Mais le fait que les réseaux sociaux se soient multipliés rend cette collecte beaucoup plus facile. Et les hackers la font désormais à grande échelle. Au lieu de se focaliser sur un individu en particulier, ils automatisent la collecte sur les réseaux sociaux via des botnets, pour trouver ces infos personnelles et les mettre en correspondance sur une masse de cibles potentielles. Cette ingénierie sociale quasi industrielle est assez troublante.

COMMENT LES ENTREPRISES PEUVENT-ELLES LA CONTRER ?

On a coutume de dire qu'en matière de sécurité, la problématique est à 80 % humaine et 20 % technique. Faire prendre conscience à un individu de la manière dont pourra être exploitée une information qu'il envoie passe par l'éducation. En France, il n'y a qu'une entreprise sur 4 qui sensibilise ses employés aux problématiques de la sécurité informatique… Cette sensibilisation doit impérativement intégrer un projet de sécurité de l'information.

COMMENT ANALYSEZ-VOUS CETTE FAIBLE SENSIBILISATION DES SALARIÉS ?

C'est surtout une méconnaissance. Sensibiliser n'implique pas forcément un gros budget. Ça peut être une affiche à côté de la machine à café rappelant trois règles de base (ne pas mettre ses mots de passe sur un post-it ou changer ses mots de passe tous les 6 mois, etc.) Ça ne coûte rien et c'est pourtant assez efficace. **Il y a un manque de compréhension des enjeux.** Dans le train ou l'avion, quasiment aucune des personnes qui travaillent sur leur ordinateur professionnel n'emploie un filtre d'écran. Or, un filtre d'écran ne coûte que quelques euros et est 100 % efficace pour cacher aux indiscrets ce sur quoi vous travaillez. C'est donc bien qu'il faut sensibiliser les salariés à la valeur d'une information et au risque de la perte du contrôle d'une information.

QUELLE RÉPONSE PEUT FOURNIR UN CONCEPTEUR DE SOLUTIONS DE SÉCURITÉ TEL QUE CHECK POINT ?

La formation fait partie de notre discours, de notre stratégie et de la manière dont nous développons nos produits de sécurité. Ceux que nous fournissons interagissent avec l'utilisateur. Bloquer l'accès d'un utilisateur, dans le cadre professionnel, à Facebook ou YouTube peut être le premier réflexe d'un responsable sécurité informatique… mais c'est une fausse piste.

La personne réfléchira aussitôt à une voie de contournement. La réponse doit être plus fine, par exemple avec une interaction, un popup qui pose à l'utilisateur une question du type « Êtes-vous sûr de vouloir accéder à Facebook pour un usage professionnel et d'être en conformité avec la politique de sécurité de l'entreprise ? » Si la personne clique sur « oui », elle doit indiquer une justification. Le simple fait de dialoguer avec l'utilisateur, de l'informer du danger de se connecter à des sites impactant en matière de sécurité et de se savoir (entre guillemets), sous surveillance, fait qu'en général des bonnes pratiques se mettent en place automatiquement.

Les cyberattaques les plus dangereuses sont désormais à la fois ciblées, les plus furtives possible et progressent techniquement à pas de géant.

Chaque entreprise est un cas unique, chacune a des données sensibles spécifiques à son activité. **Toutes ont besoin d'une solution de cybersécurité sur mesure**. Une bonne cyberdéfense passe néanmoins par un certain nombre d'impératifs : la délicate détection des signaux faibles, un suivi au plus près des accès aux données sensibles et de leurs modifications, la reconnaissance de codes malicieux, même s'ils sont inédits et l'analyse en profondeur des flux transitant sur tout ou partie du SI.

LES SOLUTIONS TELINDUS

L'approche Telindus, basée sur une **méthodologie innovante (SDR pour Surveillance, Détection, Réaction)** transversale (multicouches) s'exprimant sur trois volets :

- **Un accompagnement stratégique** (analyse des risques et mise en lumière des impacts redoutés par l'entreprise en cas d'attaque).
- **L'intégration de solutions techniques** (détection-intrusions, protection contre les fuites, visibilité des échanges sur le SI), des services et de méthodes adaptées à l'activité de l'entreprise.
- Une fois les solutions installées, **une optimisation permanente des processus de sécurité,** la constante mise à jour des technologies de détection et l'offre de services de gestion en temps réel offrant des capacités de réactions hyper-rapides aux attaques.

Pour plus d'informations, rendez-vous sur :
www.telindus.fr

LES SOLUTIONS CHECK POINT

Check Point Software Technologies, leader mondial de la sécurité Internet, fournit une protection contre tous types de menaces à plus de 100 000 entreprises tout en réduisant la complexité de la sécurité et le coût total de possession.

Il est l'unique fournisseur qui définisse **la sécurité informatique comme un processus business** grâce à une approche triple : politique sécuritaire, mise en application et facteur humain.

Les appliances 2012 combinent des technologies d'accélération réseau à des capacités haute performance pour aboutir au plus haut niveau de sécurité sans compromettre la performance réseau.

L'architecture Software de Check Blade est la seule architecture de sécurité offrant aux entreprises une protection complète et souple. Administrable centralement, elle simplifie la gestion de la sûreté sur des terminaux hétérogènes par l'unification de toutes les fonctionnalités de sécurité via une seule console.

La lame logicielle Anti-bot est un outil révolutionnaire avant-pendant et post attaque qui offre une protection des dommages causés par les bots et les attaques APT (Advanced Persistent Threats ou menaces persévérantes avancées).

L'appliance DDoS Protector stoppe, quant à lui, les attaques par déni de service grâce à une protection multicouches personnalisée.

Pour plus d'informations, rendez-vous sur :
www.checkpoint.com

ILS EN PARLENT

« Plusieurs banques de Corée du Sud ainsi que des stations TV ont été frappées (fin mars 2013) par un virus destructeur - plus tard baptisé « DarkSeoul » ou « Jokra Trojan » - qui a effacé les disques durs et infecté des PC. (…) Les attaquants ont utilisé des identifiants et mots de passe volés (…) pour accéder au système de gestion des mises à jours et patches (…) qu'ils ont ensuite employés pour distribuer le malware sur les réseaux. »
The Register - 25 mars 2013 http://www.theregister.co.uk/2013/03/25/sk_data_wiping_malware_latest/

« Voici un exemple authentique de ce que l'équipe HP Fortify on Demand a découvert en 2012 lors d'un test d'intrusion effectué avec l'accord d'une entreprise. (…) Découverte d'un répertoire https://exemple.com/passwords/. Normalement il ne devrait pas y avoir de dossier passwords, ou au moins pas en accès public. Le dossier était lui accessible via un navigateur Internet, sans besoin d'authentification et listait utilisateurs et mots de passe, y compris ceux-ci : sysadmin :[password] admin :[password] !! »
HP 2012 Cyber Risk Report http://h71028.www7.hp.com/enterprise/downloads/software/HP_2012_Cyber_Risk_Report.pdf

« Toutes les infections signalées par Apple, Facebook, Microsoft et sans doute aussi (…)Twitter proviennent d'un seul site compromis à l'insu de son éditeur Ian Sefferman : iPhone Dev SDK (iphonedevsdk.com). Il s'agit d'un forum basé sur la plate-forme Vanilla et dédié (…) aux développeurs travaillant pour la plate-forme iOS (donc sur stations Mac). Ian Sefferman a reconnu qu'il avait appris que son site était infecté par hasard en lisant dans AllThingsD un article relatant l'attaque sur Facebook. »
Mag Securs - 26 février 2013 http://www.mag-securs.com/News/tabid/62/id/29690/La-faille-Java-a-touche-des-developpeurs-Mac-y-compris-chez-Microsoft.aspx

« L'éditeur du service Evernote réinitialise les 50 millions de mots de passe de ses utilisateurs suite à une attaque informatique. (…) C'est sa ressource la plus sensible qui a été compromise. Evernote précise que les pirates ont eu accès aux données de certains utilisateurs de son service. »
ZDNet - 4 mars 2013 http://www.zdnet.fr/actualites/evernote-pirate-reinitialise-50-millions-de-mots-de-passe-39787830.html

« La sécurité doit être conçue pour l'ensemble des éléments du système d'information. Une base de données fait partie d'un projet global. Elle doit être protégée. Mais, si l'outil utilisé pour s'y connecter est vulnérable, il ouvre la porte du système d'information. (…) Mais, il faut aussi prévoir une sécurité applicative, regroupant la sécurité de toutes les composantes qui permettent à l'application de fonctionner, c'est-à-dire la sécurité du serveur web, des serveurs d'applications et des développements spécifiques. »
Les Echos - 14 janvier 2013 http://lecercle.lesechos.fr/entrepreneur/internet/221162823/cyber-delinquance-applications-et-bases-donnees-sont-portes-ouvertes

« Les plans de maintenance des systèmes d'information industriels ne peuvent être dissociés des plans de maintenance des installations qu'ils pilotent. Les opérations de SSI devraient être suivies dans l'outil de gestion de maintenance des installations (GMAO). »
ANSSI – Guide « Maîtriser la SSI pour les systèmes industriels » http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-systemes-industriels/la-cybersecurite-des-systemes-industriels.html

« Les membres d'une des meilleures universités chinoises ont collaboré durant des années sur des documents de recherche techniques en collaboration avec la PLA 61398, une unité de cyber-espionnage de l'Armée populaire de Chine. »
Reuters Canada - 23 mars 2013 http://ca.reuters.com/article/topNews/idCABRE92N01120130324?pageNumber=1&virtualBrandChannel=0&sp=true

« Un programmateur grec de 35 ans a été arrêté en possession de neuf millions de fichiers contenant les identités, les adresses, les numéros fiscaux et les plaques d'immatriculation (de ses compatriotes). (…) Ce qui signifie que plus de 83% des grecs ont vu ainsi leurs données personnelles dérobées. »
Wired UK - 22 novembre 2012 http://www.wired.co.uk/news/archive/2012-11/22/greece-id-theft

« L'utilisation d'un parefeu personnel configuré au minimum pour bloquer les connexions entrantes non sollicitées sur chaque poste client est généralement indispensable. (…) Sur les systèmes qui le permettent (serveurs ou postes clients sous Linux par ex.), le durcissement du système d'exploitation par l'ajout de composants optionnels de sécurité (GRSec, PaX) doit être envisagé. »
ANSSI – Guide d'hygiène informatique http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html

TELINDUS

12, Avenue de l'Océanie
Z.A. Courtaboeuf 3
91940 Les Ulis
Tél : 01 69 18 32 32
E-mail : marketing.securite@telindus.fr

CHECK POINT SOFTWARE TECHNOLOGIES

1, place Victor Hugo
Les Renardières
92400 Courbevoie
Tél : 01 55 49 12 00
E-mail : info_fr@checkpoint.fr

telindus
belgacom ICT

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.