DOSSIER DE PRESSE

NordNet : Vers une stratégie de **sécurité** informatique globale

NordNet
Un monde de solutions Internet

Contact presse : Christophe Outier / Directeur commercial
Tél : **03 20 66 55 85** / Courriel : **presse@nordnet.fr**

NordNet :
Vers une stratégie
de **sécurité**
informatique
globale

Sommaire

NordNet

1 Histoire de la cybercriminalité

De la blague d'ingénieur…

Quand, en 1949, John Von Neumann présente les fondements théoriques des logiciels autocopiés, c'est-à-dire capable de se multiplier de manière autonome, il ne se doute pas qu'il vient d'ouvrir la voie à un nouveau type de crimes.
Son idée permet à de jeunes ingénieurs de créer des programmes qui imitent le cycle de vie des virus infectant les organismes vivant. Les logiciels ainsi créés pervertissent les fonctions de base de la machine pour assurer leur propre survie.
Ce qui n'est alors qu'un simple jeu permettant à des génies de l'informatique d'aiguiser leurs compétences devient entre 1986 et 1988 une démarche dont le but est clairement de nuire au plus grand nombre.
En 1988, Robert Morris est arrêté pour fraude informatique après avoir causé 15 millions de dollars de dommages sur Internet. En 1991, le virus Frodo/4096 s'attaque aux ordinateurs des particuliers au travers d'une disquette diffusée dans un magazine. En 1998, 17745 virus différents se propagent d'ordinateur en ordinateur. En 2000, le virus « I Love You » plonge dans le noir des centaines de milliers d'ordinateurs.

… à la menace globale.

Le passe temps ludique de quelques développeurs est devenu une menace réelle pour les particuliers et les entreprises. **Aujourd'hui, les pirates ne jouent plus** mais cherchent à s'emparer des coordonnées bancaires, des données personnelles, des accès aux comptes de jeux en ligne… des particuliers. Ils veulent couper des entreprises ou des organismes gouvernementaux du reste du monde en s'attaquant à leurs systèmes informatiques.

On n'a plus affaire à des amateurs éclairés, des petits génies de l'informatique finalement sympathiques. Les développeurs de virus ne sont plus des héros cherchant seuls à programmer des logiciels « vivants ». **Ce sont des réseaux mi-mafieux, mi-terroristes, cherchant à s'enrichir aux dépends de chacun d'entre nous.**
Devant cette menace, une prise de conscience globale est nécessaire. Les gouvernements s'organisent, les pays se concertent et définissent petit à petit les contours de la cybercriminalité.
Piratage, contamination virale, fraude à la carte bleue, vente par internet d'objets volés ou contrefaits, vol de propriétés intellectuelles, diffusion d'images pédophiles, de recette d'explosifs, d'injures à caractère racial, atteinte à la vie privée, phishing… **Les aspects de cette nouvelle criminalité sont nombreux, et personne n'est à l'abri.**
En 2010, il est donc plus que jamais indispensable d'être informé afin de mieux se protéger, de mieux protéger sa famille et son entreprise.

NordNet

2 Quels sont les risques encourus ?

Sans protection efficace, toute l'installation informatique est en danger. Les informations stockées sur les disques durs, les logiciels installés sur chaque poste, les mails échangés entre les collaborateurs, tous les contenus sont exploitables de l'extérieur, ou peuvent être détruits. On peut citer par exemple les risques suivants :

En tant que particulier

- Contamination de l'ordinateur par des virus venant perturber son bon fonctionnement et pouvant même mener à sa destruction
- Vol de données personnelles
- Vol de coordonnées bancaires
- Usurpation d'identité
- Exposition des enfants à des contenus violents, pornographiques…
- Exploitation à distance de l'ordinateur pour envoyer des mails permettant la propagation de virus
- Exploitation à distance de l'ordinateur pour mener des attaques sur d'autres serveurs (aussi appelé zombification)
- Téléchargement de contenus protégés par les lois sur la propriété intellectuelle

En tant que professionnel

- Tous les risques cités ci-dessus
- Atteinte à l'outil de production
- Vol de fichiers clients
- Destruction des données comptables
- Le chef d'entreprise peut être jugé pénalement responsable des utilisations frauduleuses de son réseau

3 Vers une stratégie de sécurité informatique globale

Protéger les hommes, protéger les données, protéger les outils : trois principes qui doivent s'appliquer avec autant de rigueur dans le monde de l'informatique que dans le monde réel.
A cette fin, NordNet accompagne les particuliers et les entreprises pour rendre leur environnement informatique plus sûr.

1. Mettre ses données critiques à l'abri

Pour s'assurer d'une sécurité optimale de ses installations informatiques et de ses données, la première règle relève simplement du bon sens : **pour éviter de perdre des informations importantes, il faut toujours en posséder une copie, à l'abri.**
Cette stratégie de duplication des informations, ou back up, permet de s'assurer qu'en cas de grave problème (vol de matériel, incendie, contamination virale…), une copie des données restera toujours disponible, saine et sauve.
Auparavant, cette duplication nécessitait de doubler les installations informatiques ou de réaliser régulièrement des copies sur support physique (disquettes, CD-Rom, DVD-Rom, disque dur amovible). Cette technique nécessitait surtout beaucoup de temps, et ne se soldait pas toujours par une réussite, les copies étant souvent placées dans les mêmes locaux que l'original, et étant souvent détruites en même temps en cas de sinistre.
La démocratisation de l'Internet apporte une révolution dans ce domaine : **les sauvegardes de secours peuvent à présent être automatisées et se faire au travers de la connexion**. Ainsi, chaque jour, à l'heure que l'utilisateur a planifié grâce au logiciel **Mes Documents Sauvegardés**, les données modifiées sont cryptées, puis envoyées sur un serveur sécurisé.
Ces données restent disponibles et peuvent être restaurées d'un simple clic en cas de destruction involontaire de l'original.

NordNet

2. Maîtriser l'usage de sa connexion Internet

Le chef d'entreprise peut être jugé pénalement responsable de l'usage frauduleux qui est fait de la connexion Internet de sa société. De plus, **certaines utilisations d'Internet sont naturellement dangereuses**, et peuvent provoquer la contamination de tout le réseau par des virus entraînant la destruction de données essentielles ou rendant inutilisable l'outil de production.

Afin de mieux maîtriser l'utilisation d'Internet dans l'entreprise, **une solution de gestion de la connexion peut accompagner efficacement le travail de management et d'éducation du personnel d'encadrement.** Un tel outil permet notamment d'autoriser ou de restreindre l'accès à certaines catégories de sites (sites marchands, sites de voyages, sites pornographiques…) ou de mettre en place des quotas d'utilisation permettant de limiter le temps passé à surfer.

Une stratégie de gestion de la connexion se doit d'être souple, puisqu'il s'agit d'éviter les utilisations dangereuses du réseau tout en augmentant la productivité de l'entreprise. Une politique trop stricte pourrait être nuisible à l'efficacité de certains postes. C'est pourquoi il est important de pouvoir adapter les règles d'utilisation aux différents profils des employés.

Le **Filtrage Professionnel** de NordNet est un outil complet de gestion de la connexion Internet d'entreprise permettant notamment de créer plusieurs profils et de paramétrer finement les règles d'utilisation en fonction des besoins de chaque salarié.

NordNet

3. Se protéger contre les attaques en provenance de l'Internet

Les virus, les spywares, les rootkits, les dialers, les pirates, le hammeçonnage, les pourriels, les backdoors… Les risques en provenance de l'Internet deviennent si variés que de nouveaux noms semblent être inventés chaque jour pour définir les nouvelles menaces.
En réalité, il n'existe que deux grandes familles : les logiciels malveillants qui agissent de manière autonome et les attaques directes pilotées par un humain. C'est en combinant ces deux techniques que l'on obtient les menaces les plus répandues. Ainsi, un virus infectant une machine peut créer une backdoor (porte de derrière) qui permettra à un pirate de fouiller impunément dans un ordinateur sans être détecté.

Lutter contre les Virus

Pour lutter contre les logiciels malveillants autonomes (virus, spywares, dialers, rootkits…), il faut s'équiper d'un antivirus. **Le rôle de l'antivirus est de surveiller tous les fichiers au moment où ils sont enregistrés, déplacés, ouverts ou modifiés.** Il compare ensuite les données contenues dans ces fichiers à une base recensant tous les virus connus. S'il trouve une correspondance, il avertit l'utilisateur et propose des solutions pour neutraliser le danger.
Cet outil est donc indispensable. Utiliser un ordinateur sans antivirus équivaut aujourd'hui à partir en vacances en laissant la porte et les fenêtres de son domicile grandes ouvertes, après avoir envoyé une invitation aux cambrioleurs : c'est tout simplement impensable.
Les deux défauts les plus communément cités concernant ces programmes, sont d'une part qu'ils sont consommateurs de ressource et peuvent entrainer un ralentissement de l'ordinateur et, d'autre part, qu'ils détectent uniquement les virus déjà connus.
Les plus performants, à l'image de **Securitoo AntiVirus Firewall** de NordNet, ont la capacité d'observer le comportement de l'ordinateur et de détecter la moindre anomalie pour neutraliser le risque avant même qu'il ne soit connu.
De plus, dans sa version 7, cet AntiVirus a été optimisé pour prendre moins de place sur l'ordinateur et être moins gourmand en ressources. C'est donc une solution plus légère, plus réactive, et plus intelligente qui permet d'être mieux protégé contre les virus.

Enfin, cette solution étant disponible pour PC et pour Mac et permettant de protéger jusqu'à 3 ordinateurs, elle offre une grande souplesse pour protéger tous les équipements de sa maison.

Lutter contre les intrusions

Pour éviter qu'un pirate ne profite d'une faille dans la protection d'un ordinateur, il est nécessaire de posséder un bon Firewall (ou pare-feu). Le firewall est un logiciel ou un équipement qui gère les portes entre un ordinateur et l'Internet.
Autrement dit, à chaque fois qu'une application ou qu'un utilisateur souhaite entrer ou sortir de l'ordinateur, il doit montrer patte blanche. Avec le firewall complet inclus dans **Securitoo AntiVirus Firewall**, cela se fait très simplement : la première fois qu'une application essaie d'envoyer ou de recevoir des données, la solution demande à l'utilisateur s'il autorise cet échange d'informations.
S'il s'agit d'une application de confiance (navigateur, logiciel de gestion du courriel…) l'utilisateur peut autoriser cet échange ponctuellement ou définitivement – auquel cas il ne sera plus importuné à l'avenir. Si, au contraire, il s'agit d'une application qu'il ne connait pas, ou qui lui semble douteuse, il peut refuser l'échange – là aussi ponctuellement ou définitivement.
En donnant à l'utilisateur une meilleure maîtrise des informations circulant dans son ordinateur, Securitoo AntiVirus Firewall lui offre une sécurité optimale, et améliore sa protection contre le vol de données privées ou bancaires.

Des solutions pour les entreprises

Afin de permettre aux entreprises gérant plus de 3 ordinateurs de mieux maîtriser le degré de protection de leur parc informatique, Securitoo Antivirus Firewall existe en version professionnelle. **L'AntiVirus Firewall Pro** de NordNet permet de gérer la sécurité de 10 à 100 .
La solution de sécurité s'installe simplement sur chaque ordinateur à protéger, et fonctionne de manière transparente pour l'utilisateur final.
Le chef d'entreprise ou le responsable de l'informatique accède de son côté à une interface complète. Il y visualise le niveau de sécurité de chaque ordinateur et paramètre à distance, sans devoir déranger l'utilisateur du poste, chaque module de la solution de sécurité.
Les utilisateurs finaux ne peuvent pas désactiver l'Antivirus, ni le Firewall, et les ordinateurs de l'entreprise (ainsi que le réseau auquel ils sont connectés) sont donc plus sûrs.

4. Protéger les membres de sa famille

Même s'ils l'utilisent avec une facilité déconcertante et un naturel indiscutable, les enfants ne sont pas toujours les maîtres de la technologie. Il est donc indispensable de les accompagner dans leur apprentissage.
Au travers de leur navigation, des dialogues en ligne avec des interlocuteurs inconnus et de leur utilisation de réseaux sociaux, les enfants peuvent être confrontés à des images, des paroles ou des situations que nous préfèrerions leur éviter le plus longtemps possible.
En tant que parents, il est important de ne pas les laisser seuls devant l'écran, de les aider à gérer leur temps de connexion, et de leur apprendre les limites de leurs libertés sur Internet. A cette fin, chaque fournisseur d'accès doit proposer un logiciel de Contrôle Parental permettant de restreindre l'accès à des sites au contenu discutable.

Le **Contrôle Parental** de NordNet permet non seulement cette gestion du contenu grâce à l'utilisation de listes de sites autorisés ou interdits et d'une analyse en temps réel du contenu de nouveaux sites pour les plus jeunes, mais il offre également la possibilité de gérer le temps de connexion ou les horaires d'accès à Internet pour accompagner les adolescents dans leur prise de liberté sur le réseau.
Grâce à un mot de passe inviolable, les parents peuvent continuer à exploiter tout le potentiel du Web, ou ouvrir un accès complet aux enfants lorsqu'ils sont présents avec eux, puis limiter l'accès aux sites approuvés lorsqu'ils sont moins disponibles pour les accompagner.

NordNet

4 NordNet, partenaire de la sécurité des particuliers et des entreprises

Depuis 1995, NordNet propose aux professionnels et aux particuliers, où qu'ils soient, tout un monde de solutions pour se connecter sereinement, en toute sécurité, exister sur Internet et exploiter au maximum toutes les ressources du Web.

Filiale de France Télécom implantée au cœur de la métropole lilloise, NordNet engage une dynamique de développement ambitieuse et occupe à ce jour une place prépondérante au sein des entreprises de nouvelles technologies, à l'échelle nationale et internationale.

Les équipes interviennent dans des secteurs aussi pointus que le dépôt de noms de domaine, le référencement de sites Internet, la sécurité informatique ou encore l'accès Internet par Satellite ou ADSL.

Experte de la sécurité informatique qu'elle a investie dès 1997, NordNet propose des solutions adaptées à toutes les situations et à tous les publics. Plutôt que de fournir un package unique quel que soit le profil de l'utilisateur, NordNet propose un éventail de services permettant de proposer des parades spécifiques à chaque risque identifié (lutte contre les virus, sauvegarde de données, contrôle parental…).
Basées sur l'expertise de spécialistes reconnus de chaque domaine visé, les solutions proposées par la filiale de France Télécom sont valorisées grâce à un service d'assistance téléphonique personnalisée en français.
Pour tout savoir sur les solutions de sécurité de NordNet, rendez-vous sur **www.nordnet.com** !

NordNet

5 Présentation et tarifs des offres de sécurité NordNet

Contrôle Parental

La solution de contrôle parental de NordNet est l'outil de surveillance idéal pour garantir la sécurité de vos enfants. L'accès à Internet est régulé, le contenu des sites Internet est analysé et les sites inadaptés sont bloqués.
Quatre types de navigation, plus ou moins restrictifs, sont adaptables, en fonction de l'âge des enfants. Plages ou quotas horaires, le Contrôle Parental offre la possibilité de définir des périodes d'accès à Internet. La connexion Internet devient alors un outil d'éducation pour apprendre aux enfants à rationnaliser leurs besoins, à gérer leur temps et à rester raisonnables dans leurs passions.

Inclus dans les offres de connexion Internet ou 5€TTC/mois

Securitoo AntiVirus Firewall

La suite de sécurité de NordNet protège jusqu'à 3 PC à la fois contre les virus, les spam, les spywares, et les tentatives d'intrusion en provenance d'Internet. Plusieurs moteurs d'analyse travaillent ensemble pour une vigilance maximale. Pour encore plus de tranquillité, les mises à jour sont automatiques à chaque connexion Internet.

5€TTC/mois

Mes documents Sauvegardés

Il vous suffit de sélectionner les fichiers et/ou les dossiers que l'on souhaite mettre à l'abri et de définir la fréquence de vos sauvegardes. Mes documents Sauvegardés permet de placer en sécurité tous types de données : documents bureautiques, photos, vidéos…
Celles-ci sont alors à l'abri des menaces telles que le vol, les incendies, une mauvaise manipulation… très facilement et sans investissement dans un matériel coûteux.

5€TTC/mois

AntiVirus Firewall Pro

L'AntiVirus Firewall Pro est une solution professionnelle assurant la sécurité des PC en entreprise (jusqu'à 100 selon la formule choisie). Notre solution protège à la fois contre les virus, les spams, les spywares, et les tentatives d'intrusion en provenance de l'Internet. Un portail d'administration centralise toutes les informations relatives à la sécurité des PC protégés par cette solution. Accessible 24h/24 et 7j/7 via Internet, il permet de visualiser l'état de sécurité de tous les ordinateurs, d'ajuster les règles de sécurité à chaque utilisateur et de gérer les licences en toute simplicité.

A partir de 29.90 €HT /mois

Filtrage Professionnel

Le Filtrage Professionnel garantit un bon usage d'Internet au sein de l'entreprise, en bloquant les sites inadaptés. Cet outil permet également de gérer les périodes d'accessibilité d'Internet en définissant un accès à Internet aux heures où les salariés en en réellement besoin.

A partir de 9.90 €HT /mois

NordNet