

mai
2005

GUIDE SSI

Mettre en œuvre des moyens de défense minimums

Fiche 6



La mise en œuvre de moyens de défense minimums permet de :

- bloquer les attaques automatisées,
- d'éviter de laisser des brèches ouvertes,
- de limiter la prolifération virale,
- de détecter les anomalies (les événements pouvant affecter la sécurité du système d'information).

Pour être exhaustifs, ces moyens seront complétés par les mesures suggérées dans les fiches 3 (mettre en œuvre les moyens adaptés à la confidentialité des données), 5 (mettre en œuvre un plan de sauvegarde) et 7 (mettre en œuvre les moyens de défense minimums pour les connexions sans fil).

Bloquer les attaques automatisées : les firewalls (pare-feu)

■ **Rôle.** Le rôle des pare-feu est de protéger le réseau de l'entreprise des intrusions extérieures. Ils filtrent la couche IP (Internet Protocol) qui sert à transporter les données circulant sur l'Internet, inspectent et/ou examinent chaque paquet IP afin de détecter les flux illicites, et les bloquent avant qu'ils n'atteignent le réseau de l'entreprise (pare-feu périmétriques et pare-feu applicatifs) ou du poste de travail (pare-feu personnel). Ils peuvent prendre une forme logicielle ou une forme de boîtiers appelés « appliances ».

■ **Critères de choix.** La réflexion préalable au choix d'une solution pare-feu ne s'effectuera qu'après avoir établi une politique de sécurité minimum et portera sur les points suivants :

→ **Liés au niveau de sécurité requis.** Les pare-feu se différencient essentiellement par la finesse du contrôle qu'ils autorisent et leur capacité à traiter des flux élevés et à gérer un nombre important d'utilisateurs:

- Simple contrôle sur les services et sur les adresses IP autorisés pour les pare-feu simples,
- Contrôle sur la validité des protocoles et des flux applicatifs pour les pare-feu dit applicatifs (Plus de 75% des attaques portent sur l'exploitation des faiblesses applicatives). Attention au choix de ce type de pare-feu (white list, black list, ou les dernières génération basées sur les principes de l'intelligence artificielle) plus ou moins facile à mettre en œuvre et à administrer.
- Mise en œuvre de services associés tels que translation d'adresse, Proxy, passerelle anti-virus, serveur DHCP (Dynamic Host Configuration Protocol), service VPN (s'assurer que

l'autre extrémité du lien VPN est compatible avec la technologie VPN incluse dans le pare-feu sélectionné), services IDS (Intrusion Detection System) ou IPS (Intrusion Prevention System).

→ Liés à l'architecture des systèmes

- Caractéristiques de la connexion Internet
- Dimensionnement du réseau local (nombre d'utilisateurs)

→ **Liés aux compétences internes.** Quels sont les moyens d'administration disponibles ? Un pare-feu, quel qu'il soit, doit être administré. Toutefois la technicité nécessaire pour installer et configurer avec soin un pare-feu logiciel open source par exemple sera bien supérieure à celle requise pour brancher et configurer un boîtier pare-feu ADSL via une interface Web. Le choix de la technologie pare-feu devra donc prendre en compte les compétences dont dispose ou souhaite se doter l'entreprise. Un pare-feu n'a d'intérêt que s'il est configuré en accord avec la politique de sécurité établie. Si, par exemple, seuls les flux Web et e-mail sont autorisés depuis l'Internet, l'ensemble des autres flux devra être interdit. La configuration du pare-feu peut être très fine en attribuant des droits différents selon les catégories d'utilisateurs, elle peut également mettre en œuvre une politique variable suivant les plages horaires ou les jours d'ouverture de l'entreprise afin de limiter la consommation de bande passante durant les périodes de charge.

→ **Le coût.** Le plus souvent les pare-feu sont facturés en fonction du nombre d'utilisateurs, des flux et des services associés.

Limitier les brèches ouvertes : se protéger des vulnérabilités

Les logiciels, comme toute réalisation humaine, contiennent des erreurs, appelées vulnérabilités, dont certaines menacent la sécurité. Ces vulnérabilités peuvent être exploitées manuellement ou par des programmes développés spécifiquement qui le plus souvent permettent à leur utilisateur de contrôler des ordinateurs sans légitimité.

■ **Comment se protéger.** Mettre en œuvre un processus de gestion des mises à jour de sécurité de tous les logiciels présents dans l'entreprise afin de pouvoir éliminer les vulnérabilités connues et bénéficier au passage des dernières améliorations en matière de sécurité. Les derniers systèmes d'exploitation et les dernières applications intègrent des fonctionnalités de mise à jour automatique, dont il faut s'assurer qu'elles sont activées. Les administrateurs du système d'information suivront classiquement la démarche suivante :

- Audit automatisé des configurations installées, et/ou à défaut veille permanente minimum sur les vulnérabilités des systèmes d'exploitation et applications installées (www.cert.org),
- Test des nouvelles mises à jour ,
- Déploiement des correctifs de sécurité en commençant par colmater les failles les plus critiques sur les machines les plus sensibles,
- Application des correctifs, grâce à des outils spécialisés, en prenant soin de gérer la non régression des systèmes.

■ Exemples d'outils de mise à jour

- Un service de mise à jour automatique, Windows Update, est intégré à Windows 2000 et Windows XP. Il permet aux consommateurs et aux petites entreprises d'installer automatiquement les mises à jour dès qu'elles sont disponibles.
- MBSA est un outil gratuit d'inventaire des mises à jour manquantes pour les machines Windows www.microsoft.com/france/technet/themes/secur/info/mbsa.html

→ Software Update Services (SUS) peut être téléchargé gratuitement sur le site Web de Microsoft. Ce service est conçu pour simplifier le processus de mise à jour des systèmes Windows. SUS permet aux administrateurs de déployer rapidement et en toute sécurité les mises à jour importantes sur leurs serveurs Windows 2000, ou Windows XP Professionnel. www.microsoft.com/france/securite/outils/sus.asp

→ Les autres plateformes offrent des possibilités similaires (Linux, Unix, Mac...)

■ **Exemples d'outils de test de vulnérabilités.** Les outils de test peuvent être utilisés à des fins d'audit préalable et/ou pour tester les mises à jour effectuées.

→ **Outils gratuits.** Nessus est un outil gratuit de recherche de vulnérabilités (www.nessus.org). L'installation et la mise en œuvre sont réservées à des utilisateurs confirmés.

→ **Outils payants.** Ces outils existent pour tous les types de plateformes. Ils peuvent être installés dans l'entreprise ou être actionnés à distance, un rapport complet étant alors transmis de façon totalement sécurisée à l'entreprise. Ils peuvent être, dans un premier temps, testés à distance gratuitement puis par abonnement. **Il est vivement recommandé de procéder au moins à un test gratuit pour établir un état des lieux rapide du niveau de vulnérabilité des systèmes (offres multiples disponibles).**

limiter la prolifération virale : les anti-virus

La prolifération des virus (des vers, des spams et autres chevaux de Troie) impose l'adoption de logiciels anti-virus pour éviter une contamination rapide des systèmes. Comment choisir ? La bonne question n'est pas tant la marque que leur positionnement et leur nombre. **Trois solutions :**

■ **Un anti-virus disposé sur la passerelle d'accès Internet.** Le principe est de réaliser un filtrage applicatif sur l'ensemble des flux en clair (c'est-à-dire communications non chiffrées) qui transitent par la passerelle Internet. En particulier cet anti-virus analysera les flux Web à la recherche de logiciels malveillants. Ceci peut s'avérer intéressant dans le cas d'utilisation de service de courrier Web. En pratique, il est admis que ce niveau de filtrage est aujourd'hui à lui seul une garantie insuffisante pour se prémunir de l'ensemble des codes malveillants.

■ **Un anti-virus disposé sur le serveur de messagerie.** Le point névralgique de la communication d'entreprise est le serveur de messagerie d'entreprise. Le choix de traiter la lutte anti-virale à ce niveau présente donc de nombreux avantages : relative simplicité de mise en œuvre, efficacité maximale sur les infections par e-mail, ressources matérielles associées généralement limitées. L'inconvénient majeur est que l'ensemble des flux n'est pas traité par l'usage exclusif de cet anti-virus.

■ **Un anti-virus équipant les postes personnels.** La nécessité de disposer d'un anti-virus à jour sur chaque poste de travail de l'entreprise s'impose : d'une part les protections anti-virales réseau ne sont pas infaillibles (les fichiers chiffrés par exemple ne pourront jamais être analysés), d'autre part les usages personnels des ordinateurs sont par définition incontrôlables (insertion de CD, utilisation d'une connexion à domicile, ...).

En pratique ce déploiement indispensable peut impliquer une remise à niveau du réseau et du parc informatique :

→ le système doit permettre la mise en place de l'anti-virus mais aussi la mise à jour régulière des bases de signatures, sans laquelle l'efficacité de la détection est compromise ;

→ les systèmes d'exploitation doivent être suffisamment homogènes pour autoriser un déploiement uniforme de l'anti-virus.

L'usage est de combiner plusieurs de ces solutions, en essayant autant que possible de choisir deux fournisseurs distincts pour favoriser les chances de détection de nouvelles souches. La solution minimum est probablement le déploiement de l'anti-virus personnel, mais il sera raisonnable et confortable d'ajouter rapidement un dispositif anti-virus sur le serveur de messagerie.

Détecter les anomalies

■ **Identifier une activité anormale.** Il faut au préalable :

- définir ce que doit être une activité normale, c'est à dire les types de flux autorisés ainsi que les configurations associées. Cette action peut être menée par l'utilisation d'outils automatisés (voir fiche 1).
- détecter les flux contraires aux règles ou les modifications de configuration indues.

Sans ces deux démarches les intrus pourront d'une part s'introduire sur le système sans risque d'être détectés, et d'autre part, et c'est plus grave encore, se maintenir sur le système à demeure avec un accès de plus en plus large à l'ensemble des ressources informatiques.

■ **Surveiller les traces des systèmes sensibles.** Les équipements de sécurité mais aussi l'ensemble des serveurs du réseau d'entreprise génèrent des traces (logs) permettant de retracer une partie de l'activité du système. La surveillance de ces traces, rébarbative, est souvent négligée. Elle est pourtant essentielle pour détecter les incidents de sécurité en l'absence de dispositifs spécifiques de détection ou de prévention d'intrusion. Il faudra donc mettre en place une procédure simple de consultation de certaines traces sur les machines sensibles ou exposées, en s'aidant par exemple d'outils dédiés facilitant ce travail.

■ **Détecter les modifications de configuration.** Très souvent une agression sur un système d'information se caractérise par la modification de paramètres de configuration ou de fichiers système sans autorisation. Ces opérations indues peuvent être détectées facilement par le contrôle régulier et automatisé de l'intégrité de fichiers spécifiés. Le logiciel open source Tripwire permet par exemple de réaliser ce type de contrôle. Il sera essentiel de limiter l'usage du contrôle d'intégrité à un nombre réduit de fichiers sensibles pour conserver l'efficacité du dispositif.

■ **Détecter les intrusions.** De nombreuses sondes de détection d'intrusion ou de prévention d'intrusion sont proposées, parfois incluses dans des équipements de réseaux du type pare-feu. Elles peuvent constituer un complément efficace aux dispositifs présentés précédemment, toutefois la mise en œuvre et l'exploitation parfois délicates de ces outils incitent à un usage modéré.