



LES TENDANCES DU MOIS DE JANVIER 2006

LEXSI

Baromètre des failles du système d'information

	Microsoft Windows	Linux					Unix BSD			SCO Caldera	HP-UX	IBM AIX	Sun Solaris	SGI Irix	Novell
		Caldera	Debian	Mandrake	Red Hat	Suse	Free BSD	Open BSD	Net BSD						
Bulletins émis par les éditeurs	3	-	32	21	8	7	7	2	2	9	5	-	6	-	1
Classement	LEXSI														
Haute	4	-	4	4	2	5	1	-	-	1	1	-	-	-	1
Moyenne	-	-	12	9	6	4	3	-	-	4	-	1	1	-	-
Basse	3	-	16	14	17	8	7	2	2	4	4	1	5	-	-
Nombre total d'alertes	7	-	32	27	25	17	11	2	2	9	5	2	6	-	1

- Pour les Unix, il s'agit du nombre de vulnérabilités affectant l'OS en tant que tel ainsi que celles affectant les différents packages pouvant être installés dessus.
- Le nombre de vulnérabilités retenues concerne les nouvelles vulnérabilités (apparues au cours du mois de janvier 2006) ainsi que celles pour lesquelles de nouveaux patchs correctifs sont apparus.
- Un bulletin d'alerte émis par un éditeur peut concerner plusieurs vulnérabilités.



Joël Rivière,
fondateur de Lexsi
 Spécialiste des problèmes de sécurité, Joël Rivière a dirigé pendant cinq ans le département informatique de l'Institut de recherche criminelle de la gendarmerie nationale. En 1999, il fonde Lexsi, cabinet de conseil en sécurité*.

* Voir le site :
<http://www.lexsi.com>

Nouveaux comportements

Les risques associés aux utilisateurs itinérants sont connus : les équipements mobiles tels que les ordinateurs portables ont une nette propension à ne pas toujours revenir à temps dans l'entreprise pour, par exemple, faire mettre à jour l'antivirus, quand ils ne disparaissent pas pour toujours (vol). Et quand bien même ils reviennent, leur niveau de sécurité reste sujet à caution. De même, de trop nombreux réseaux Wi-Fi sont installés sans autorisation et sans contrôle, c'est-à-dire bien souvent sans aucune sécurité.

Mais la problématique s'étend à la gestion des données informatisées. Il n'a jamais été aussi simple de transporter, transférer et partager des volumes importants de données, incluant bien sûr des informations confidentielles. Il est ainsi de plus en plus courant que des collaborateurs décident d'embarquer un volume important de données sur un support de type disque dur USB pour les exploiter depuis leur domicile. Ces données, pour lesquelles de grands efforts de sécurisation du système d'information ont été mis en œuvre, se retrouvent parfois partagées et accessibles directement sur des réseaux *peer-to-peer* : on imagine facilement les conséquences.

De plus, l'arrivée de services en ligne s'apparentant à des espaces de stockage démesurés pose un nouveau défi à l'entreprise. Ainsi en est-il des messageries en ligne gratuites, aux capacités de stockage supérieures à celles de l'entreprise, que nombre de collaborateurs vont utiliser par commodité sans réfléchir aux conséquences, par exemple, de la compromission du mot de passe associé. C'est aussi le cas de fonctionnalités telle celle proposée par Google Desktop, qui permet à l'utilisateur, depuis n'importe quel point du globe, d'accéder à des données stockées physiquement sur des serveurs Google. L'intérêt évident du service peut entraîner, à plus ou moins court terme, son adoption par les utilisateurs de l'entreprise ; les risques liés seront alors pris sans aucune maîtrise.

L'entreprise est alors confrontée à un choix : soit elle se donne les moyens d'interdire leur utilisation, avec les difficultés que cela comporte ; soit elle devance l'usage en proposant sa version des services pour lesquels elle pourra contrôler mise en œuvre et utilisation. Déplacer les attaquants. Et savoir s'adapter aux changements de comportements de ses propres utilisateurs.

MÉTHODOLOGIE

Les équipes de Lexsi ont répertorié les vulnérabilités susceptibles d'affecter les systèmes d'information (voir tableau ci-dessus). Ce recensement provient de deux sources : les bulletins d'alerte des éditeurs/constructeurs et la surveillance sur le

terrain des spécialistes en sécurité du laboratoire. La cellule de veille technologique de Lexsi a classé les failles selon le degré d'importance des dégâts. L'ampleur des dommages a été évaluée en fonction de l'architecture des systèmes attaqués.