



Ce que tout dirigeant devrait savoir quant à l'importance d'une bonne gestion des rustines

La croissance soutenue du nombre de virus, de vers et d'attaques malicieuses fait en sorte qu'une bonne gestion des rustines est plus impérieuse que jamais. Les professionnels de l'informatique savent que la protection de l'infrastructure et des applications peut être aussi vitale que les prévisions de ventes et les bilans. Il peut être difficile d'en convaincre la haute direction, mais il est essentiel d'y parvenir afin de protéger la santé à long terme de l'entreprise. Fusepoint a conçu une marche à suivre simple en cinq étapes dont vous pouvez vous servir pour éviter que votre entreprise ne figure au rang des victimes en 2005.

1re Étape : Reconnaître les risques

Les questions de sécurité et de continuité des activités font constamment les grands titres de l'actualité du monde des affaires. Selon un sondage, 87 % des entreprises canadiennes craignent de voir leurs activités de nouveau interrompues par une panne d'électricité générale. Sans compter qu'elles doivent aussi se défendre contre des virus comme Mydoom, Nimba et Slammer (pour lesquels, ironiquement, une rustine existait deux ans avant les ravages qu'ils ont faits partout dans le monde, l'an dernier). Aucun ralentissement ne semble poindre en 2005 : seulement en janvier, Microsoft a diffusé 12 bulletins de sécurité concernant 17 rustines. Les chiffres parlent d'eux-mêmes :

- ▶ Les réseaux des fournisseurs reçoivent chaque jour quelque 120 000 alertes
- ▶ Le délai moyen d'exploitation d'une vulnérabilité n'est plus que de six jours (auparavant, six mois)
- ▶ Sept nouvelles vulnérabilités, en moyenne, apparaissent chaque jour
- ▶ 96 % des menaces sont de gravité modérée ou élevée
- ▶ Les applications de commerce électronique sont les plus souvent visées
- ▶ Le Canada se classe au 5e rang mondial pour ce qui est des menaces provenant de l'intérieur des frontières

Si de plus en plus d'entreprises canadiennes se rendent compte qu'elles ne peuvent plus négliger les menaces, la gestion des rustines en décourage bon nombre qui essaient tant bien que mal de suivre le rythme. Comme le souligne la société IDC, « Le temps qu'il faut pour mettre au point les rustines diminue, mais les entreprises ne les appliquent pas dans un délai raisonnable. La sécurité n'est pas qu'une question de technologie, mais aussi de temps et de ressources. »

2e Étape : Accepter le fait que les règles ont changé

Il y a des années, l'Internet n'existait pas. Le terme " nomade " renvoyait aux personnes qui n'avaient pas d'habitation fixe, et non aux travailleurs en déplacements continus. Ceux et celles qui opéraient « à distance » étaient reliés à leur bureau par des lignes exclusives : ou bien on était connecté, ou bien on ne l'était pas. Les réseaux d'aujourd'hui connaissent peu de frontières et deviennent de moins en moins une affaire de serveurs et de bande passante que de déroulement des activités essentielles des entreprises. Des profils d'utilisateur reposant sur des autorisations donnent à certaines personnes accès à certaines données où que soit dans le monde et en n'importe quel temps.

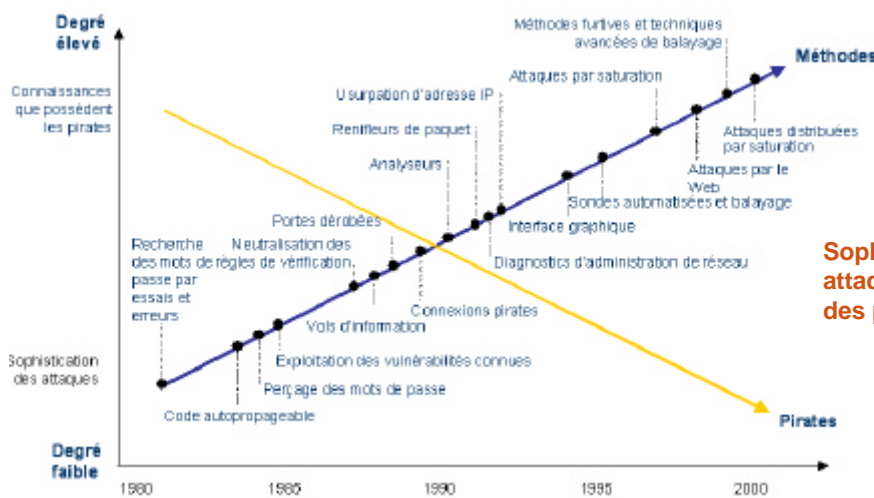
Des études ont montré que la sophistication des attaques s'est accrue tout autant qu'a diminué le niveau de connaissances qu'il faut pour les déployer. N'importe qui disposant d'un ordinateur domestique peut théoriquement lancer une attaque. Le graphique de la page suivante présente de récentes observations de l'Institut de la sécurité informatique de la police fédérale des États-Unis.

La sophistication croissante des attaques exige un niveau d'expertise plus élevé et une gestion constante. Les dirigeants canadiens prennent de plus en plus conscience du fait qu'en plus d'entraîner des pertes de revenus, les bris de sécurité et les perturbations d'activités nuisent grandement à l'image et à la crédibilité d'une entreprise. Le coût d' « évitement » doit être regardé de plus près.

Réduisez les risques et ne cherchez plus à tâtons avec la marche à suivre en cinq étapes de Fusepoint pour la gestion des rustines.

Ce que tout dirigeant devrait savoir quant à l'importance d'une bonne gestion des rustines

Une rustine importante est lancée à toutes les 6 minutes, ce qui signifie que 10 nouvelles rustines en moyenne sont diffusées pendant l'heure du lunch de votre personnel informatique.



3e Étape : Obtenir l'adhésion de la direction

Les services de l'informatique qui sont efficaces comprennent les besoins opérationnels de l'entreprise et font clairement voir leur rendement sur le capital investi et leur apport à la croissance du chiffre d'affaires, aux relations avec la clientèle et à la réputation de l'entreprise. Ils évaluent les problèmes, comme ceux qui concernent la sécurité et la gestion des rustines, et les portent à l'attention de leur équipe de direction et de leur conseil d'administration. Seule la présentation d'une évaluation objective à ce niveau peut faire en sorte que les risques pour l'entreprise deviennent une priorité et obtiennent l'attention qu'ils méritent.

La sensibilisation et l'engagement à évaluer sont une chose, mais que dire d'une évaluation et d'une mise en œuvre faites par des experts? Nombre d'entreprises canadiennes, et en particulier ceux du segment de marché particulièrement vulnérable du milieu de gamme, ne disposent tout simplement pas des installations, de l'expertise technique et des ressources humaines nécessaires pour se protéger contre les risques qu'elles décèlent. Quelques instants passés dans les sites web de McAfee, de Symantec ou de Microsoft suffisent à convaincre que la gestion des rustines peut facilement être un travail à plein temps. Une rustine importante est lancée à toutes les 6 minutes, ce qui signifie que 10 nouvelles rustines en moyenne sont diffusées pendant l'heure du lunch de votre personnel informatique. Comment une entreprise de taille moyenne peut-elle arriver à maintenir les ressources humaines et financières pour suivre les centaines de rustines diffusées chaque mois et continuellement mettre à jour son système de détection d'intrusion et ses coupe-feu. En pareille situation, la question qui se pose inévitablement est celle-ci : « Par où commencer? »

4e Étape : Rassembler les éléments de la gestion des rustines

Si vous préférez vous charger vous-même de la gestion des rustines, la démarche exposée à la page suivante devrait vous aider à établir votre stratégie. Une autre possibilité sûre et rentable est l'externalisation. Grâce à la spécialisation et aux économies d'échelle, un bon fournisseur de services d'infogérance peut mettre à votre disposition une infrastructure, des installations, une planification et une expertise technique que bon nombre d'entreprises ne peuvent tout simplement pas se permettre à l'interne. Si c'est ce que vous choisissez, assurez-vous que votre fournisseur puisse aussi prendre en charge les autres aspects de vos applications essentielles. Aussi importante qu'elle soit, la gestion des rustines n'est pas la seule solution à envisager pour assurer la sécurité et la disponibilité de vos données.



Ce que tout dirigeant devrait savoir quant à l'importance d'une bonne gestion des rustines

Un modèle pour une bonne gestion des rustines

1. Inventaire et évaluation de l'infrastructure et des applications - Sachez ce que comprend votre environnement et mettez-le sur papier. Vous ne pouvez protéger ce dont vous ignorez l'existence. Après avoir fait votre évaluation, repérez les maillons faibles.
2. Validation et maintenance - Déterminez quelles sont vos applications essentielles et établissez l'ordre de priorité des rustines.
3. Renforcement de l'environnement - Verrouillez le tout et évitez les maux de tête dans l'avenir.
4. Mise au point de la stratégie de gestion des rustines - Décrivez vos processus d'évaluation, d'essai et de maintenance pour vous assurer qu'ils soient clairement mis sur papier.
6. Contrôles et rapports - Établissez un processus de contrôle interne des rustines qui concernent vos applications et votre infrastructure (listes d'envoi, Microsoft, Redhat, groupes de discussion).
5. Déploiement des rustines - Exécutez cette étape selon les priorités établies lors de votre analyse des répercussions sur les opérations. Dotez-vous d'un plan de secours vous permettant de revenir en arrière si les rustines ne fonctionnent pas.
7. Validation et maintenance - Tenez le processus toujours à jour pour tous vos déploiements de réseau, d'application et de produit. Faites de la gestion des rustines une partie essentielle de votre processus de mise en œuvre de nouveaux produits. La maintenance continue est essentielle.

La sécurité est une affaire d'intégration de personnel, de processus et de technologie, et elle est une exigence de tous les instants.



5e Étape : Répandre la notion de sécurité

Il existe une foule de mesures que vous pouvez prendre pour vous prémunir contre les menaces provenant de l'extérieur de votre réseau. L'élément déterminant de la protection des applications et de l'information essentielles d'une entreprise, comme dans le cas de tout projet de quelque envergure, est un processus exhaustif d'examen et de diligence raisonnable. Que vous décidiez de confier la sécurité à l'interne ou de l'externaliser à un fournisseur de confiance, votre service de l'informatique doit répondre de la fiabilité, de la performance et de la disponibilité de votre infrastructure, de vos données sensibles et de vos applications. Tous les employés doivent toutefois collaborer avec lui en suivant les procédures appropriées et en signalant les problèmes qui surviennent.

Ce que tout dirigeant devrait savoir quant à l'importance d'une bonne gestion des rustines

Qu'est-ce que cela veut dire?

Le nombre croissant d'attaques signalées contre les réseaux et les systèmes d'information montre clairement que la sécurité doit venir à faire partie de la culture organisationnelle de toute entreprise. Les professionnels de l'informatique doivent se poser les questions suivantes :

- ▶ Dans quelle mesure nos applications et nos données sont-elles en sécurité?
- ▶ Combien de données perdues ou compromises pouvons-nous nous permettre?
- ▶ Pendant combien de temps pouvons-nous nous passer de nos cinq applications les plus importantes?
- ▶ À quand remonte la dernière mise à l'épreuve de notre programme de gestion des rustines?
- ▶ Combien nous coûtent les interruptions de service?
- ▶ Pouvons-nous nous charger de la gestion des rustines à l'interne?

Les professionnels de l'informatique doivent se tenir à l'affût des nouvelles technologies de protection et automatiser les alertes internes. Ils doivent en outre surveiller quotidiennement les menaces et mettre continuellement à l'épreuve leurs politiques et procédures de sécurité.

Les événements de l'an dernier auront au moins eu comme bienfait de sensibiliser les dirigeants au fait que les systèmes d'information représentent l'élément vital de leur entreprise - mais bon nombre d'entre eux doivent encore se le faire rappeler constamment. La protection des actifs et de la réputation d'une entreprise est l'affaire de chacun de ses employés - et non seulement celle de son service de l'informatique. Une entreprise doit prendre des mesures pour se doter d'une infrastructure, de services et de ressources adéquats bien avant d'avoir à faire face aux conséquences coûteuses d'une crise.

La décision d'externaliser

Si vous décidez de confier les besoins de sécurité à des experts externes, vous devriez aussi considérer, outre la gestion des rustines, les éléments suivants :

Coupe-feu infogéré - gestion et surveillance en temps réel d'une infrastructure entièrement redondante, permettant aux entreprises de créer une défense de première ligne contre les attaques d'intrus.

Système de détection d'intrusion - repérage et notification immédiate des codes malicieux et des menaces de la part d'utilisateurs non autorisés ou de pirates (des experts en sécurité devraient offrir une défense en tout temps, en surveillant et en gérant les données recueillies par des coupe-feu, des détecteurs d'intrusion et des dispositifs de RPV et en mettant fin instantanément à toute session non autorisée).

Réseau privé virtuel - mise à disposition d'un accès en ligne sécurisé grâce à la gestion du trafic des utilisateurs distants et de l'accès aux données en ligne essentielles de l'entreprise au moyen de serveurs hébergés et de pages en ligne privées.

Renforcement du paramétrage - élimination des processus potentiellement exploitables en créant des environnements hautement sûrs, extensibles et pratiques pour vos systèmes d'exploitation, vos bases de données et vos applications de commerce électronique, y compris un examen, une analyse et des mesures de protection exhaustives des applications essentielles de votre entreprise.

Le nombre croissant d'attaques signalées contre les réseaux et les systèmes d'information montre clairement que la sécurité doit venir à faire partie de la culture organisationnelle de toute entreprise.

