GUIDE DES BONNES PRATIQUES POUR L'UTILISATION DU WEB ET DES SYSTÈMES DE MESSAGERIE

SOMMAIRE

PROTÉGEZ VOS SERVEURS.

1. INTRODUCTION

Entre 2011 et 2012, 94 % des cas de violation de données concernaient des serveurs, d'une manière ou d'une autre.[1] Rien d'étonnant à cela dans la mesure où, pour accéder à votre réseau, les cyber-criminels empruntent toujours le chemin le plus simple, à savoir les failles de sécurité. Malheureusement, il s'agit bien souvent de vos serveurs.

En tant que points d'entrée sur le réseau de votre entreprise, vos serveurs de messagerie et serveurs Web sont des cibles particulièrement vulnérables et convoitées. À l'affût de la moindre vulnérabilité logicielle ou erreur humaine, les criminels ont recours à un grand nombre de méthodes pour rechercher et exploiter les failles de votre système, pénétrer votre réseau, puis lancer des attaques de grande ampleur ou dérober des données stratégiques de votre entreprise.

Le rôle crucial que joue aujourd'hui la messagerie dans les communications en entreprise en fait également un vecteur d'attaque principal. Chaque jour, 89 milliards d'e-mails professionnels sont échangés dans le monde entier.[2] Les chercheurs de Kaspersky Lab ont d'ailleurs découvert que 72,5 % de l'ensemble des e-mails échangés en septembre 2012 sont en réalité des courriers indésirables, et que 3,4 % des e-mails contiennent des fichiers malveillants.

Sur le Web, les bots de Google détectent chaque jour 9 500 sites malveillants. Au cours du seul deuxième trimestre 2012, Kaspersky Lab a identifié et neutralisé plus d'un milliard de menaces et un total de 89,5 millions d'URL contenant du code malicieux. Selon les estimations, 80 % des attaques sont dirigées contre des systèmes Web.[3]

Les logiciels antivirus traditionnels seuls ne suffisent pas à faire face aux menaces actuelles, en perpétuelle évolution. Les professionnels informatiques, quant à eux, ne sont pas non plus en mesure de gérer l'ensemble des attaques contre leurs serveurs. Les meilleures pratiques préconisent une approche globale en matière de protection des serveurs reposant sur le recours à des technologies qui filtrent les menaces avant qu'elles n'atteignent votre réseau, interceptent le contenu malveillant sans bloquer pour autant les données légitimes et protègent vos serveurs sans compromettre les performances.

Voici les étapes que vous pouvez suivre et les technologies que vous pouvez appliquer pour garantir le fonctionnement de vos serveurs de messagerie et de vos serveurs Web dans des conditions de sécurité et de performance optimales.

1 Source : Verizon : Rapport d'enquêtes sur la violation des données, 2012
2 Source : Radicati : Rapport statistique sur les e-mails, 2012-1016
3 Source : Rapport sur les principaux risques en matière de cyber-sécurité, HP TippingPoint DVLabs, SANS Institute et Qualys Research Labs, septembre 2010

2. PROTECTION DES SERVEURS DE MESSAGERIE

Le rôle crucial que joue aujourd'hui la messagerie dans les entreprises, quelle que soit leur taille, représente le maillon le plus important et le plus vulnérable de la chaîne de communication professionnelle. Auparavant simple outil de communication, elle s'est dotée de fonctionnalités supplémentaires désormais exploitées dans le cadre de l'archivage de documents, de l'organisation des conférences, de la gestion d'agendas et de bien d'autres activités. D'après des travaux de recherche menés par Enterprise Strategy Group, les dossiers de messagerie contiennent jusqu'à 75 % des données de propriété intellectuelle. Il n'est donc pas surprenant que les serveurs de messagerie continuent d'attirer autant l'attention des criminels, qui voient en eux aussi bien un point d'entrée sur votre réseau qu'une source d'informations stratégiques d'un point de vue commercial.

PROBLÈME : l'administrateur n'est pas sans savoir que les systèmes de messagerie et les outils de collaboration font l'objet d'attaques pour ainsi dire incessantes de la part des spammeurs et des pirates informatiques. Si ces cyber-criminels ne parviennent pas toujours à dérober des données ni à compromettre la sécurité de votre réseau, il n'en reste pas moins que les spammeurs sont en mesure de paralyser votre bande passante et que les pirates ont la possibilité de compromettre l'efficacité de vos communications ainsi que de créer une instabilité sur votre réseau en commettant des vols par le biais de relais.

SOLUTION : bloquez l'accès des courriers indésirables à vos réseaux avant qu'ils ne provoquent des dégâts.

- **Filtrage efficace :** la meilleure contre-attaque consiste à intercepter les courriers indésirables avant même qu'ils n'atteignent vos réseaux, ce qui vous permet ainsi de limiter les dépenses engagées en termes de budget et de ressources. Les technologies de filtrage des courriers indésirables, à la fois intelligentes et de qualité, dépassent le cadre des listes traditionnelles de mots-clés ou de combinaison de mots. Elles incluent :

  – **Surveillance proactive :** les meilleures pratiques préconisent une solution que vous pouvez personnaliser de façon à ce qu'elle distingue le contenu que vous souhaitez bloquer des informations dont vous avez besoin. Il convient dans ce cas de surveiller en permanence et de façon automatique les messages, pour « former » les moteurs de courriers indésirables à comprendre ce qu'ils doivent rejeter immédiatement et ce qu'ils peuvent mettre en quarantaine ou accepter.

  – **Filtre de réputation :** les spammeurs ne cessent de changer de tactique. La simple modification apportée à un mot-clé suffit à perturber les filtres de courriers indésirables traditionnels. Le filtrage de réputation classe les courriers indésirables de façon à intercepter les nouvelles attaques, même en cas de différence minime dans le texte ou le message. Cette approche vous garantit une défense proactive doublée d'une protection quasiment en temps réel. Par ailleurs, une solution de qualité vous permettra de bloquer rapidement certains types d'attaques sans avoir à les soumettre à l'avis d'un analyste. Vous gagnez ainsi du temps et économisez des ressources.

  – **Mise en place du filtrage de contenus :** surveillez et filtrez les pièces jointes conformément à vos politiques de sécurité. Bloquez le trafic d'emails inappropriés (exemple : fichiers audio ou vidéos) et les fichiers potentiellement dangereux (tels que les fichiers exécutables). Optez pour une solution de filtrage de contenus qui analyse les fichiers en fonction du contenu et bloque les courriers indésirables, quel que soit le type de fichier ou l'extension affichée.

- **Listes blanches ET noires :** la liste noire basée sur le protocole DNS représente l'une des configurations les plus efficaces en matière de protection des serveurs de messagerie. Elle procède à la vérification des noms de domaine ou des adresses IP des expéditeurs des messages en les comparant à des listes mondiales recensant l'identité de spammeurs connus. Le choix d'une solution vous donnant accès au plus grand nombre de listes de blocage DNS (DNSBL) vous permettra de réduire considérablement la quantité de courriers indésirables reçus.

  Grâce à des fonctionnalités vous permettant de configurer des listes d'autorisation/de refus personnalisées tant au niveau de l'administrateur que de l'utilisateur, vous bénéficiez d'une plus grande flexibilité et d'un contrôle plus granulaire sur vos messages. Si la création de vos propres listes noires locales est plutôt fastidieuse, le jeu en vaut néanmoins la chandelle dans la mesure où elles vous aident à bloquer les attaques de spammeurs ayant pris pour cible vos serveurs.

- **Cap sur le cloud :** la mise à jour régulière de vos listes dans une base de données en temps réel hébergée dans le cloud vous offre une couche de protection supplémentaire, bien au-delà de ce que vous proposent vos listes locales et les listes enregistrées sur les serveurs de mise à jour de votre solution. Vous êtes ainsi en mesure de réagir rapidement à la réception de courrier indésirable.

- **Identification des attaques ciblées :** les attaques lancées par les criminels visent de plus en plus souvent une entreprise en particulier. Ce type d'attaque repose avant tout sur des courriers indésirables hautement personnalisés visant un aspect précis ou une faille particulière d'une entreprise spécifique. Les meilleures pratiques préconisent une solution capable de contrer les attaques visant spécifiquement votre réseau LAN. En effet, ce type de courrier indésirable est généralement adressé à un nombre restreint de destinataires ciblés. Une solution antispam associée à un antivirus permet d'éliminer ces attaques.

- **Application des mises à jour et suivi d'une approche de type « zero-hour » :** la cyber-criminalité à partir de courriers indésirables se distingue, entre autres, par la nature « éclair » de la plupart de ses attaques. Près de la moitié des attaques par courriers indésirables de chaque assaut sont lancées au cours des 10 premières minutes, ce qui implique que les temps de réponse doivent être tout aussi rapides. La nouvelle solution de Kaspersky Lab intègre des technologies intelligentes ainsi qu'un nouveau service assurant une mise à jour rapide de la base de données antispam. De cette façon, la plupart des courriers indésirables sont interceptés instantanément et en toute efficacité.

PROBLÈME : vol par le biais de relais. De nombreux spammeurs exploitent les vulnérabilités sur des serveurs de messagerie dans le but de s'approprier une partie de la bande passante dont ils ont besoin pour diffuser une quantité importante de courriers indésirables. En d'autres termes, ils utilisent vos serveurs pour distribuer leurs courriers indésirables, en vous obligeant ainsi à prendre en charge l'ensemble des coûts et des problèmes de ressource, sans parler du mécontentement des clients. Et comble de l'ironie, il arrive souvent que des communications professionnelles légitimes soient retardées sur vos serveurs surchargés tentant désespérément d'acheminer les courriers indésirables.

SOLUTION : tous les serveurs de messagerie vous permettent de définir des paramètres de relais de messagerie et de restreindre ainsi les destinataires auxquels votre protocole SMTP doit envoyer les e-mails. Pensez-y.

PROBLÈME : déni de service. Les attaques par déni de service sont en mesure de paralyser intégralement vos serveurs de messagerie (et vos serveurs Web) ainsi que votre réseau en les inondant de courriers indésirables et en leur envoyant un nombre de requêtes supérieur à ce qu'ils sont en mesure de traiter.

SOLUTION : limitez le nombre de connexions autorisées à votre serveur SMTP. Si la définition d'un nombre optimal de charges acceptables est parfois longue et dépend des spécifications des serveurs, telles que le processeur et la mémoire, il est toutefois recommandé de définir un seuil de connexion à partir du nombre total de connexions, du nombre de connexions simultanées autorisées et du nombre maximal de connexions pouvant être prises en charge.

3. PROTECTION ANTISPAM + PROTECTION ANTIMALWARES = DES SERVEURS ENTIÈREMENT SÉCURISÉS

Les courriers indésirables ne représentent pas seulement de simples problèmes de performances et de ressources, comme le souligne Maria Namestnikova, analyste senior de Kaspersky Lab, ils deviennent de plus en plus dangereux. « Les criminels ont aujourd'hui davantage recours aux programmes malveillants pour infecter un ordinateur par la simple ouverture d'un e-mail. Par ailleurs, les courriers indésirables contiennent de plus en plus souvent des liens malicieux et des messages frauduleux », explique Maria Namestnikova. « Il est très probable que les programmes malveillants aujourd'hui tapis dans les e-mails soient capables de muter fréquemment et de ne plus comporter de signature ni de schéma comportemental connu. Résultat : un filtre de courriers indésirables ou de contenu Web moyen risque fort de ne pas les intercepter à temps. »

En juillet 2012, Kaspersky Lab a constaté une augmentation de 50 % du nombre d'e-mails contenant des fichiers malveillants. Les programmes malveillants ouvrent souvent une brèche dans le réseau à la suite d'une attaque ciblée et couronnée de succès par courrier indésirable, comme un e-mail de phishing qui persuade un utilisateur de cliquer sur un lien apparemment légitime ou d'ouvrir un fichier tout aussi légitime en apparence. L'attaque de grande envergure dont a été victime RSA en 2011, par exemple, a été déclenchée par un fichier Flash infecté, intégré à une feuille de calcul Excel intitulée « Plan de recrutement 2011 ». Cet e-mail n'avait été envoyé qu'à quatre employés bien ciblés. Celui qui a ouvert la pièce jointe avait extrait l'e-mail de son dossier contenant ses courriers indésirables.

En renforçant votre protection contre les courriers indésirables par l'installation d'un logiciel antivirus, vous êtes en mesure de repousser les cybermenaces lancées contre vos serveurs et votre infrastructure réseau. Pour optimiser votre protection contre les courriers indésirables, pensez aux fonctionnalités suivantes :

- **Analyse des programmes malveillants à la demande :** analysez les messages et leurs pièces jointes au niveau du fichier, du dossier et du répertoire, ainsi que les périphériques tels que les lecteurs flash, les DVD-ROM et les disques durs.

- **Protection en temps réel / fonctionnalités « zero-hour » :** de fréquentes mises à jour automatiques, une analyse et une protection en temps réel, ainsi qu'un accès à une base de signatures mondiales de programmes malveillants, constamment mise à jour, vous permettent d'optimiser votre protection antimalwares.

- **Sérénité garantie :** les utilisateurs sont prompts à se plaindre et cherchent souvent à désactiver ou à contourner les processus dont ils estiment que leur application risque de compromettre les performances système. Choisissez une solution qui vous permette d'exécuter des analyses en arrière-plan sans interrompre le travail des utilisateurs.

4. PROTECTION DES SERVEURS WEB

Les serveurs Web représentent l'une des cibles privilégiées des criminels. Si de nombreux administrateurs prennent des mesures en vue de protéger le site Web de leur entreprise, véritable vitrine de cette dernière, contre ce type d'attaques, certains en oublient parfois le serveur qui l'héberge, ainsi que toutes les applications et les connexions réseau associées. Résultat : vulnérabilité pour tous ces éléments.

Voici quelques conseils à prendre en compte pour verrouiller votre serveur Web :

- **Désactivez les services inutiles et les extensions d'applications :** vous courez après le temps. Vous ne disposez pas des ressources nécessaires. Du coup, vous installez le système d'exploitation en appliquant les paramètres par défaut tout en croisant les doigts pour que rien n'arrive… Oui, mais dans ce cas de figure, de nombreux services réseau dont vous n'avez pas besoin s'exécutent malgré tout et consomment inutilement les ressources de votre système. Sans oublier leurs ports qui restent ouverts en permanence. Les coupables sont à rechercher généralement du côté des services de base de registre et d'accès à distance, ainsi que des serveurs d'impression. Ne vous contentez pas de les éteindre, désactivez-les de façon à vous assurer qu'ils ne s'exécuteront pas au prochain démarrage du serveur.

- **Contrôlez de près les accès à distance :** bien que cette mesure soit difficile à appliquer à une époque où les collaborateurs sont de plus en plus nomades, essayez, dans la mesure du possible, de vous connecter à vos serveurs Web uniquement localement. Si vous devez tout de même procéder à une connexion à distance, veillez au moins à ce que cette connexion soit sécurisée en exploitant les fonctionnalités de tunnellisation et de chiffrement. Essayez de restreindre au maximum les accès à distance à un nombre donné d'adresses IP et de comptes.

- **Effectuez vos tests dans des environnements privés :** imaginez que vous testiez votre nouveau site Web ou l'application que vous développez. Vous savez pertinemment que ces fichiers contiennent de nombreuses vulnérabilités. Pourquoi les avez-vous alors laissés dans un dossier public, qui plus est, nommé par exemple « test » ou « nouvelle application » invitant le moindre utilisateur malintentionné à les repérer et à les pirater ? Testez les nouveaux projets sur un serveur non connecté au réseau et tenez-le bien à l'écart des bases de données stratégiques.

- **Réduisez au minimum les autorisations :** affectez le moins de privilèges possible en octroyant uniquement ceux dont vos services ont besoin pour fonctionner. De cette façon, vous empêchez les pirates ou les parties de code malicieux qui ont réussi à pénétrer votre réseau d'exploiter ce service compromis pour effectuer d'autres tâches sur votre serveur.

- **Appliquez les correctifs rapidement et fréquemment :** optimisez la sécurité de votre système en veillant à exécuter la toute dernière version du système d'exploitation, systématiquement mis à jour à l'aide des correctifs de sécurité les plus récents. Dans ce domaine, les meilleures pratiques préconisent une solution vous permettant d'automatiser et d'appliquer les mises à jour de façon à garantir instantanément la sécurité de votre serveur.

- **Surveillez le moindre fichier :** consultez régulièrement les journaux pour repérer toute activité suspecte. Un aperçu unique et centralisé de votre réseau et de votre serveur Web vous permet d'avoir un œil sur tout ce qui s'y passe.

5. SÉCURISATION DE LA NAVIGATION

Les logiciels efficaces en termes de protection contre les programmes malveillants ajoutent une couche de sécurité supplémentaire aux passerelles Web et offrent à tous les utilisateurs de votre entreprise un accès sécurisé au Web. Si les meilleures pratiques préconisent la suppression automatique des programmes potentiellement malveillants dans les trafics HTTP(S), FTP, SMTP et POP3, il est également important d'opter pour une solution dotée de fonctionnalités d'équilibrage des charges de façon à réduire la charge de travail sur votre serveur ou votre passerelle et de garantir un fonctionnement en toute sérénité.

Une analyse intelligente et optimisée permet de soulager vos serveurs et vos passerelles. Gagnez en flexibilité en termes d'analyses et renforcez vos performances tout en réduisant les ressources nécessaires à des processus d'analyse efficaces en optant pour des solutions d'une grande flexibilité.

La situation ne se résume toutefois pas à une question d'analyse. Il est en effet possible de garantir aux administrateurs et aux utilisateurs une navigation Web sécurisée encore plus efficace à partir d'outils de gestion et d'autres fonctionnalités :

- **Filtrage combiné des URL et du contenu :** comme l'ont démontré les bots Google, de nombreux sites Web contiennent du code malicieux. Mais gardons-nous bien de penser que seuls les sites dont la sécurité est compromise sont concernés. En effet, des criminels lancent et retirent également quotidiennement de nouveaux sites délibérément infectés pour attirer des utilisateurs peu méfiants. La plupart du temps, les utilisateurs n'ont même pas besoin de télécharger quoi que ce soit : une simple visite du site suffit à les infecter via des vulnérabilités n'ayant pas fait l'objet de correctifs au niveau de leur navigateur ou d'autres applications Web.

  Contrairement aux administrateurs informatiques, il se peut que les utilisateurs n'aient pas conscience des risques qu'ils courent. Certes, vous ne pouvez pas verrouiller le Web. En revanche, grâce à des solutions de filtrage d'URL et de contenu, vous pouvez contrôler non seulement la façon dont vos utilisateurs interagissent en ligne, mais également la manière dont le Web interagit avec vos réseaux.

  Les solutions de filtrage d'URL reconnaissent les sites malveillants et empêchent les utilisateurs de s'y connecter. Les filtres de contenu, quant à eux, vous permettent de contrôler le type de contenu auquel les utilisateurs peuvent accéder ou de limiter les fonctionnalités des sites ayant éventuellement été infectés. Vous avez la possibilité d'utiliser ces deux types de filtre sans compromettre les performances système, en toute transparence vis-à-vis des utilisateurs.

  Appliquez vos politiques de sécurité basées sur les rôles en fonction :

  – de l'utilisateur ;
  – des groupes ;
  – de catégories d'URL ;
  – du contenu Web.

Veillez à ce que vos services et vos bases de données mondiales de filtrage d'URL et de contenu soient automatiquement mis à jour à partir d'une base de données en temps réel surveillée en permanence.

- **Surveillance et rapports :** bénéficiez d'un aperçu complet sur l'ensemble des activités de votre réseau en utilisant une solution qui vous permet d'accéder en toute simplicité aux données suivantes :

  - **Blocages par jour :** nombre de requêtes bloquées sur une période donnée.
  - **Catégories les plus fréquentes par connexion :** catégories de filtres Web les plus souvent sollicitées en fonction du nombre de requêtes.
  - **Utilisateurs les plus fréquents par blocage :** utilisateurs les plus souvent bloqués.
  - **Utilisateurs les plus fréquents par connexion :** utilisateurs les plus souvent connectés en fonction du nombre de requêtes.

Ce type de rapports vous permet de bénéficier d'un aperçu de la façon dont vos utilisateurs interagissent avec le Web et de renforcer vos politiques en toute efficacité. Elle vous permet également de soutenir les initiatives en matière de productivité au sein de l'entreprise tout en veillant à ce que les activités consommatrices de bande passante mais non productives des utilisateurs ne surchargent pas davantage des ressources déjà bien sollicitées.

6. CONCLUSION

Les entreprises ont besoin de compter sur des technologies intelligentes en matière de sécurité dans le but de protéger leurs données, ainsi que sur des outils informatiques à la fois intuitifs et simples d'utilisation, garants de l'efficacité de leurs opérations. Les 2 500 collaborateurs de Kaspersky Lab ont à cœur de répondre aux besoins de plus de 300 millions d'utilisateurs dont ils assurent la protection et des 50 000 nouveaux utilisateurs qui s'ajoutent chaque jour.

Les solutions Kaspersky Mail Security et Kaspersky Web Security offrent une protection de premier plan à tous les serveurs de messagerie et toutes les passerelles Internet. Ces deux produits sont réunis dans la solution Kaspersky Endpoint Security for Business. Outils primés de protection antispam et antimalwares, modules d'application des politiques informatiques, gestion centralisée, protection dans le cloud… Autant de caractéristiques faisant des solutions de sécurité des entreprises développés par Kaspersky le choix idéal pour votre organisation.

Contactez votre revendeur de solutions de sécurité et découvrez comment Kaspersky est en mesure de garantir la protection de vos serveurs, de vos passerelles et des réseaux !

IDENTIFIER. CONTRÔLER. PROTÉGER.

Avec Kaspersky, maintenant, c'est possible.
kaspersky.fr/business

Be Ready for What's Next

Kaspersky Lab ZAO, Moscou, Russie
www.kaspersky.com/fr/