Optimisation de la sécurité d'entreprise via la surveillance du réseau et des applications

Grâce au déploiement d'outils performants d'analyse du réseau et des applications au sein de votre infrastructure, vous êtes en mesure de gérer les attaques, quel que soit le point d'origine des attaques ou la défense qui a fait défaut. Visual UpTime® Select™ vous fournit la visibilité et les fonctionnalités d'analyse nécessaires pour détecter les attaques, limiter les dégâts et rétablir les activité qui limitent les risques et l'exposition à des failles de sécurité.

Table des matières

FLUKE networks

Chicago Business Examiner

Règlement du procès en action collective des actionnaires de ProviCare

NEW YORK, 4 février 2006 – Le conglomérat de soins de santé ProviCare Holdings, Inc. vient d'annoncer le règlement d'actions intentées en justice par 19 actionnaires, pour un montant de 368 millions USD en actions, en liquide et en bons de souscription d'actions afin de mettre un terme à des accusations de négligence qui remontent à janvier 2000.
Dans un communiqué de presse paru hier, la société établie à Chicago n'a admis aucune erreur dans le cadre du règlement, qui dépend encore de l'approbation finale du tribunal. La réclamation portait sur 19 procès séparés, et notamment un procès en action collective des actionnaires devant la cour fédérale américaine de Chicago alléguant que la société s'était montrée négligente au niveau de la protection de ses systèmes d'information contre le piratage informatique.
La société a subi 976 millions de dollars de perte après que le public ait appris le vol de quelque 40 000 dossiers de patients et la fin de relations commerciales essentielles. Les actions de la société, qui s'échangeaient il y a un an à plus de 46 dollars l'unité, ont terminé la journée d'hier à 3,19 dollars.

Difficile à croire ? L'histoire est complètement plausible et ce n'est qu'une question de temps avant qu'un récit semblable ne paraisse en première page. Des normes définies par la législation récente telle que la loi Sarbanes-Oxley de 2002 sont corroborées par la menace d'amendes et de poursuites au pénal. Ces mêmes normes entraînent des poursuites civiles lorsque des pratiques en dessous de la norme exposent les bénéfices d'entreprise à des risques exagérés ou encore lorsque des failles de sécurité réelles mènent à de véritables pertes commerciales. Ces types de réglementations affecteront presque toutes les entreprises dans un futur proche.

Une réglementation pour chaque occasion

Avant même les attentats terroristes et les scandales financiers, les législateurs et autres corps dirigeants surveillaient et examinaient de plus près les entreprises de l'ère de l'information. Depuis lors, la cadence s'est accélérée de façon notable, peut-être à raison.

Les technologies de l'information ont modifié de façon fondamentale la majorité des entreprises. Les processus d'information et de système d'information constituent un atout essentiel ainsi qu'un différenciateur concurrentiel fondamental. La perte ou la compromission de ces informations (ou de la capacité à les utiliser) représente un risque important pour la valeur actionnariale. Elle est bien souvent d'une nature hautement sensible et confidentielle et doit être sauvegardée afin de protéger les relations avec les clients.

Des réglementations qui ont un impact sur l'informatique et affectent presque toutes les entreprises sont désormais en place et d'autres se profilent à l'horizon. L'une des réglementations les plus mentionnées est la loi Sarbanes-Oxley de 2002, qui s'applique à toutes les entreprises à la valeur négociée sur les marchés publics et se focalise essentiellement sur la gouvernance financière de l'entreprise. Dans la mesure où les entreprises modernes dépendent beaucoup de l'informatique pour la comptabilité, la loi Sarbanes-Oxley contient également des dispositions obligatoires au sujet des contrôles informatiques et de la sécurité.

Même sans compter les amendes, les poursuites et les peines de prison, les coûts d'une sécurité informatique inadéquate sont importants. Si l'on en croit un article récent paru dans le magazine Optimize, les coûts indirects des incidents de sécurité informatique (ventes perdues, détérioration des relations avec la clientèle et dommages légaux, par exemple) dépassent largement les dépenses directes en matière de personnel et d'équipement de sécurité. L'étude indique que les délits informatiques impliquant une violation de la confidentialité (divulgation d'informations médicales ou financières, par exemple) ont causé une diminution moyenne de plus de 5 % de la valeur marchande de l'entreprise de la victime.[1]
La perception du marché est qu'un abus de confiance se convertira directement en perte de futurs revenus car les clients s'adresseront ailleurs.

Une autre étude menée auprès de 162 entreprises par le cabinet d'étude Aberdeen Group a révélé qu'une entreprise moyenne perd chaque année deux millions de dollars de revenus en raison d'attaques sur Internet. Les entreprises sont

généralement confrontées à une interruption significative chaque année, durant laquelle les systèmes requièrent une indisponibilité moyenne de 22 heures pour récupérer.[2] Quant aux entreprises qui ont jusqu'à présent évité des interruptions à cette échelle, il semblerait qu'elles aient simplement eu de la chance. Selon le rapport rédigé par Symantec au sujet des menaces de sécurité sur Internet (Internet Security Threat Report), « plus de 40 % d'entreprises reprises au palmarès Fortune 100 ont contrôlé des adresses IP qui servaient de point de départ pour la propagation d'attaques de vers ».[3]

Le message est clair : toutes les entreprises connaîtront à un moment ou à un autre une attaque réussie, qu'elles s'en rendent compte ou pas. Alors, comment peuvent-elles se protéger ?

Détournement des problèmes

Le secret de la protection de votre entreprise réside dans les mesures prises avant, pendant et après une attaque. Si l'impensable devait survenir et que vous deviez vous défendre, vous devrez faire preuve d'une compréhension approfondie des risques ainsi que d'un schéma clair de mesures à prendre pour y répondre. Votre réussite dépend de l'approche de votre entreprise en termes de planification quotidienne. Ne perdez pas de vue trois éléments clés lorsque vous formulez vos plans :

Un peu comme l'évolutivité et le coût total d'exploitation, la sécurité est une dimension dont vous devez tenir compte dans chaque décision liée à l'informatique.

La sécurité est une dimension. Un peu comme l'évolutivité et le coût total d'exploitation, la sécurité est une dimension dont vous devez tenir compte dans chaque décision liée à l'informatique. La gestion continue de la sécurité au sein de votre infrastructure informatique permet d'élaborer des bases solides et de réduire le besoin d'ajouts personnalisés onéreux.

Les attaques peuvent venir de partout. L'essentiel du battage médiatique autour des solutions de sécurité actuelles se focalise toujours sur le périmètre du réseau. La plupart des attaques passent néanmoins par la grande porte et ne rencontrent jamais le périmètre du réseau.
Exemple :

- Un employé ramène une disquette infectée de son ordinateur à domicile pour mettre à jour les derniers pronostics du football.
- Un intérimaire ouvre une session avec un ordinateur portable infecté.
- L'ordinateur infecté d'un fournisseur se fixe par inadvertance sur un point d'accès sans fil indésirable de votre réseau lors de sa participation à une réunion dans votre salle de conférence.
- Un ancien employé mécontent laisse derrière lui une bombe à retardement.

Attendez-vous à une brèche de vos défenses. Etablissez le meilleur périmètre de défense que vous puissiez vous permettre. Installez les pare-feu les plus sophistiqués qui soient, des mécanismes d'authentification, des systèmes de détection des intrusions, des filtres des courriers électroniques et autres RPV pour des communications à distance sécurisées. Exécutez le dernier logiciel antivirus en date comme dernière ligne de défense. Configurez-les de façon aussi conservative que votre entreprise peut le supporter et que votre patience le permet. Partez du principe que toutes vos défenses soigneusement élaborées seront débordées par un élément aussi simple qu'une nouvelle façon de déguiser l'attaque d'un ver porteur d'un cheval de Troie sous la forme d'un courrier électronique ou encore qu'un employé bien intentionné qui utilise un élément jugé inoffensif. Que faire alors ?

Prévention des attaques

Vos stratégies de réponse aux incidents de sécurité sont tout aussi importantes que vos plans visant à les empêcher de se produire. D'un point de vue pratique, toute la planification de la sécurité moderne découle du principe classique de « protection, détection, réaction et restauration ».
La réponse aux incidents se focalise sur les trois derniers éléments de ce principe et comporte trois phases d'action distinctes :

- Détection des attaques
- Limitation des dégâts
- Restauration des activités

Détection des attaques

Il n'existe pas de technique, de mécanisme ou d'outil unique qui permet de détecter tous les types d'attaque. Les attaques peuvent prendre toutes les formes et toutes les dimensions. Plusieurs nouvelles attaques ont certainement vu le jour depuis votre première tasse de café du matin. Certaines attaques sont automatisées, comme par exemple les virus, les vers et les attaques de refus de service distribuées (DDoS). D'autres sont manuelles, comme lorsqu'un pirate s'installe sur l'un de vos serveurs hautes performances. Les attaques automatiques sont souvent systématiques et passent à l'attaque lorsqu'il y a correspondance du profil algorithmique. La plupart des attaques manuelles sont basées sur votre identité (exemple : énorme entreprise monopolistique) ou sur ce que vous avez (c'est-à-dire des processeurs et une connectivité à bande passante élevée et un espace de stockage important). La grande majorité des attaques ont une chose en commun : elles font des choses que ne font pas vos utilisateurs d'ordinaire.

Dans le domaine de la sécurité informatique, les signes reconnaissables d'une attaque sont souvent désignés sous le nom d'« indicateurs ». Ces signes comprennent des preuves manifestes d'une attaque, comme par exemple des graffiti à l'écran ou sur le site Web, mais aussi des preuves moins évidentes, telles que la modification de fichiers (indicateurs de fichier) et d'entrées dans le fichier journal d'un serveur (indicateurs système). Tous ces indicateurs apparaissent « après les faits ». Ils indiquent que les dégâts sont déjà là. Le dernier type d'indicateur est l'indicateur réseau. Les indicateurs réseau sont les signes d'une attaque qui sont visibles sur le réseau même et qui peuvent vous avertir assez tôt que quelqu'un ou quelque chose tente d'attaquer lorsqu'il est encore temps de réagir.

Exploitation des indicateurs réseau au maximum

Pour identifier une attaque avant que des effets négatifs ne se fassent sentir et que les utilisateurs en soient affectés, le secret est de reconnaître les comportements anormaux (suspects) des réseaux. La première génération de systèmes de détection d'intrusion (IDS) fait de son mieux, mais en est toujours à ses balbutiements et il faudra encore des années avant qu'ils ne puissent repérer les anomalies avec autant d'efficacité que le cerveau humain.
A l'heure actuelle, les systèmes de détection d'intrusion doivent bénéficier du soutien de l'intellect humain ainsi que d'autres outils. Comment les humains procèdent-ils ?

Le trafic applicatif et les performances réseau sont les éléments les plus faciles à étudier à la recherche de comportements anormaux associés à une attaque.

Le trafic applicatif et les performances réseau sont les éléments les plus faciles à étudier à la recherche de comportements anormaux associés à une attaque. A titre d'exemple, si votre entreprise utilise Microsoft Exchange Server comme plate-forme de courrier électronique, des sonnettes d'alarmes devraient se faire entendre lorsqu'une quantité significative de trafic SMTP submerge subitement votre réseau interne. Il pourrait s'agir d'un signe de début d'infection par l'un des nombreux vers propagés grâce au publipostage. Pour détecter les anomalies, vous devez commencer par savoir quelle est la norme.
Voici comment procéder :

1. Elaborez un référentiel. Il s'agit d'un rapport détaillant les conditions normales de votre réseau. C'est une combinaison d'informations au sujet du flux, de l'état et de l'utilisation des applications sur le réseau qui permet de bénéficier d'un aperçu complet que vous pouvez utiliser plus tard, lorsque la situation a changé. Les éléments que vous devez inclure dans votre référentiel sont les éléments les plus susceptibles d'être modifiés par une attaque quelconque.
A chaque moment de la semaine, vous devez connaître les points suivants pour chaque site de votre réseau :

- Quelles adresses se comportent comme des serveurs « autorisés » ?
- Quels sont les protocoles « autorisés » ?
- Quels sont les protocoles les plus utilisés ?
- Quelles sont les sources et destinations du trafic les plus utilisées ?
  - Quelle quantité de trafic génèrent-elles ?
  - Quels protocoles utilisent-ils ?
- Quelle est l'importance du trafic échangé avec d'autres sites ?
  - Quels protocoles utilisent-ils ?

Le fait que vous décidiez de créer un référentiel aujourd'hui ne rend pas les conditions actuelles « normales ». Des individus malveillants pourraient déjà être à l'œuvre dans votre entreprise, contribuant à une augmentation des charges de trafic applicatif et à une dégradation des performances. N'acceptez pas votre référentiel avant de vous assurer qu'il s'agit bien d'un rapport précis des conditions normales.

2. Analysez le trafic à l'aide du référentiel. Maintenant que vous avez établi le référentiel, vous devez régulièrement analyser vos activités réseau en procédant à une comparaison.

Commencez par les protocoles d'application. Y a-t-il de nouveaux protocoles que vous ne reconnaissez pas ? Certains des protocoles du référentiel présentent-ils un trafic considérablement plus élevé qu'avant ? Il pourrait s'agir d'une indication que le protocole est utilisé pour du trafic entre homologue ou pire encore. Y a-t-il des applications actives à des heures inhabituelles pour votre entreprise, comme par exemple Telnet à 3 h du matin ? Ces constatations sont facilitées par des outils qui analysent l'utilisation des protocoles et la comparent avec le référentiel au fil du temps.

Examinez maintenant vos serveurs. Tout d'abord, y a-t-il de nouveaux serveurs qui n'étaient pas là auparavant ? Vous attendiez-vous à leur présence ? Les serveurs présentent-ils la même quantité relative de trafic entrant et sortant ? Des stations client sont-elles à présent devenues des serveurs d'une sorte ou l'autre ? L'un de ces éléments pourrait indiquer la présence d'un ver ou encore des activités de piratage ou de nouveau partage de fichiers entre homologues. Les outils d'analyse peuvent vous aider en identifiant automatiquement les serveurs de votre réseau.

Connaissance du flux

Un flux applicatif est la séquence de trames liées à une session d'application unique dans une direction entre une paire d'extrémités. Cela signifie que pour la plupart des applications, il y aura au moins deux flux applicatifs pour chaque session : l'un du client au serveur et l'autre du serveur au client. Chaque flux applicatif est généralement caractérisé par plusieurs facteurs caractéristiques qui comprennent l'adresse IP de la source et de la destination, le port de source et de destination, les indicateurs d'état de la connexion TCP ainsi que le protocole d'application utilisé. Ces éléments rendent possibles la reconstruction des attributs clés d'une session applicative pour l'analyse de la sécurité et des performances.

Pour créer des données de flux applicatif, des agents sont déployés qui inspectent passivement le trafic des utilisateurs sur le réseau. Les agents peuvent faire partie des périphériques d'analyse réseau ou peuvent être intégrés à des périphériques tels que des routeurs et des CSU. Si les données de flux d'applications elles-mêmes sont importantes, l'analyse dont elles font l'objet après leur collecte est encore plus essentielle. Etant donné le nombre impressionnant de données produites par les applications (même sur les réseaux les plus réduits), il est essentiel de disposer d'un outil intelligent qui reconstruit les flux et présente des analyses de façon à vous aider à faire votre travail le plus efficacement possible. Des fonctionnalités telles que les listes des protocoles, hôtes et flux les plus utilisés ainsi que l'identification automatique des serveurs et les alertes de nouveaux protocoles améliorent de façon spectaculaire votre capacité à déceler des comportements anormaux.

Etudiez ensuite les flux applicatifs. Les ordinateurs ou stations de travail de certains utilisateurs finaux sont-ils inconsciemment à l'origine de nombreux petits flux vers un grand nombre d'adresses ? Un grand nombre de tentatives de connexion présentent-elles des échecs et des répétitions ? Peut-être une station est-elle en train d'initier des flux vers des adresses invalides. Ces stations effectuent probablement des analyses ou des sonde réseau, à la recherche de failles. Des connexions sont-elles effectuées à des heures inhabituelles ? Certains clients téléchargent-ils un trafic plus important que ce à quoi vous vous attendiez ? Un outil qui fournit des volumes de flux applicatif et organise les informations de flux par protocole, par source et par destination rend l'analyse relativement aisée.

Un outil qui fournit des volumes de flux applicatif et organise les informations de flux par protocole, par source et par destination rend l'analyse relativement aisée.

Pour finir, examinez les volumes de trafic sur les liaisons clés de votre réseau. Les volumes de trafic sont-ils plus élevés pendant ce qui constitue normalement les heures de pointe ? Certains sites génèrent-ils davantage de trafic que ce à quoi vous vous attendez ? Il peut s'agir là des signes d'activités indésirables qui pourraient être liées à une attaque.

3. Analysez les différences. Prenez garde de ne pas rationaliser les différences entre le référentiel et les conditions actuelles. L'une de ces différences pourrait constituer un avertissement préalable d'un problème plus sérieux. Prenez des mesures pour enquêter à ce sujet. Il suffit parfois simplement de patienter un court instant pour voir si les niveaux de trafic retournent à la normale. Contactez un responsable de service afin de savoir s'ils ont déployé un nouveau serveur ou une nouvelle application. Sans en alerter le service informatique, certains responsables informatiques prennent des mesures sans poser de questions : ils bloquent les nouveaux serveurs et applications qui apparaissent sans avertissement, conscients que si leur existence est légitime, leurs propriétaires les contacteront bien assez tôt.

4. Mettez le référentiel à jour. Vos systèmes, réseaux et applications évoluent chaque jour. Cette complexité a permis la création de brèches où les attaquants se sont engouffrés et sur lesquelles ils comptent pour couvrir leurs traces. Une mise à niveau périodique de votre référentiel est nécessaire pour ajuster vos processus de détection. C'est aussi un bon moment pour identifier les modifications non intentionnelles et non autorisées apportées à votre infrastructure. Des outils qui surveillent en permanence les activités de votre réseau et qui en conservent un historique automatisent en grande partie ce processus pour vous, mais vous devez toujours l'examiner d'un œil critique et le valider vous-même.

En plus d'utiliser le référentiel pour détecter les indicateurs réseau d'une attaque, vous pouvez également utiliser différents types de déclencheurs. Il s'agit d'une ressource réseau réelle ou virtuelle qui vous envoie une alarme à chaque fois que des conditions particulières sont réunies. Si vous savez quelles activités sont normales dans votre environnement, vous pouvez concevoir de simples déclencheurs pour détecter la présence de certains types d'intrus en cas d'activité anormale. Choisissez soigneusement ces déclencheurs, pour que des applications légitimes et des individus honnêtes ne risquent pas de les déclencher. Considérez-les comme l'équivalent réseau de l'alarme déclenchée en cas de braquage d'une banque, lorsque le billet du dessous est ôté du tiroir-caisse.

Les fonctionnalités automatiques de génération d'alarme de certains équipements et sondes réseau rendent aisée la configuration de déclencheurs. Une fois configurés, les agents vous alerteront lorsque les conditions de déclenchement sont remplies sur les segments réseau surveillés. Choisissez les guides de déclenchement en fonction de vos connaissances de votre environnement applicatif, de votre référentiel et du mode de fonctionnement des attaques. A titre d'exemple, une tactique courante utilisée par de nombreux vers consiste à envoyer des courriers électroniques au moyen d'un relais SMTP interne d'acheminement du courrier pour atteindre l'extérieur. Si vous n'utilisez pas encore l'adresse courante de type « mail.votredomaine.com » souvent visée par ces vers, vous pouvez ajouter une fausse entrée à cet effet à votre DNS interne et bloquer tout le trafic SMTP (tcp/25) vers cette destination. Vous pouvez également définir des déclencheurs sur toutes les activités de sonde pour certaines des portes dérobées les plus populaires ainsi que d'autres adresses IP et ports vulnérables que les attaquants ont tendance à utiliser.

Limitation des dégâts

Une fois que vous êtes conscient d'être attaqué, limitez les dégâts en refusant tout accès ultérieur aux ressources que l'attaque vise à utiliser, l'empêchant ainsi d'atteindre de nouvelles cibles. Le défi consiste à comprendre suffisamment bien l'attaque à laquelle vous êtes confronté pour utiliser le type et le niveau de réponse appropriés pour ce type d'attaque particulier et son stade de développement. A titre d'exemple, un pirate à l'œuvre sur votre grappe de serveurs requiert une réponse complètement différente de celle exigée en cas de propagation d'un ver par messagerie électronique. Pour comprendre les attaques à cet effet, vous devez vous poser trois questions essentielles :

1. Comment est-elle arrivée sur votre réseau ?
2. Quelle est sa cible ?
3. Comment se propage-t-elle et jusqu'où est-elle arrivée ?

La recherche de réponse à ces questions devrait commencer par une analyse de l'historique du trafic réseau. Comment l'attaque a-t-elle d'abord été détectée et à quel endroit ? Existe-t-il une preuve que l'attaque était déjà en action auparavant et peut-être à d'autres endroits mais que d'une façon quelconque elle n'a pas été décelée ? Il y a des chances que le point d'origine se trouve à proximité de l'endroit où les premiers signes de l'attaque ont été détectés. Si vous parvenez à identifier le point d'origine, n'hésitez pas à le déconnecter, si possible. Dans le cas contraire, il pourrait s'avérer pratique de mettre en quarantaine la branche du réseau à l'origine de l'attaque afin de parvenir à une certaine amélioration si l'attaque ne s'est pas trop propagée. Votre exposition à d'autres attaques s'en trouvera également limitée, ainsi qu'une réinfection éventuelle si le point d'origine présente des points faibles qui sont exploités.

Pour répondre rapidement à ces questions et particulièrement pour déterminer la façon dont l'attaque est menée à bien et sa distance de progression, vous devrez utiliser des outils d'analyse réseau. Si le malfaiteur a impliqué un agent connu, votre logiciel antivirus à jour l'aurait presque certainement détecté à ce stade. Dans le cas contraire, vous êtes probablement confronté à un mutant qui n'a pas encore été signalé ou à une attaque de pirate. Grâce à l'analyse du flux applicatif, l'établissement d'un récapitulatif du trafic sur les liaisons et entre les extrémités pour exposer les schémas anormaux devient un jeu d'enfant. L'analyse de l'utilisation des liaisons et des top émetteurs (Top Talkers) vous permet d'effectuer le suivi des victimes les plus actives. Une fois l'infection dans votre ligne de mire, la capture et l'analyse des trames infectées peuvent être la clé de votre salut.

Non seulement vous devez acquérir des outils qui vous apportent les informations nécessaires, mais vous devez également les déployer à l'avance aux endroits adéquats. Vous souvenez-vous du principe de planification de réponse aux incidents qui dit que « les attaques peuvent venir de partout » ? Si votre visibilité est réduite à une seule portion du réseau, votre réponse ne peut pas vraiment commencer à limiter les dégâts avant que l'infection n'atteigne ce point. Avec un peu de chance il ne s'agit pas de votre site principal. Un système d'analyse distribuée qui vous fournit une visibilité de tous vos sites distants constitue le meilleur outil, aussi bien pour une détection précoce que pour le contrôle des dégâts. Une façon rentable d'aborder la fonctionnalité d'analyse distribuée consiste à l'intégrer à l'infrastructure du réseau. En choisissant un équipement réseau doté de fonctions d'analyse qui répondent à vos besoins en termes de sécurité et d'activités quotidiennes, vous bénéficiez de fonctionnalités plus puissantes et mieux intégrées à un prix plus réduit.

Si votre visibilité est réduite à une seule portion du réseau, votre réponse ne peut pas vraiment commencer à limiter les dégâts avant que l'infection n'atteigne ce point.

Restauration des activités

Une fois les dégâts maîtrisés et la propagation de l'attaque interrompue, les utilisateurs vous harcèleront pour vous pousser à restaurer les activités dès que possible. S'il est certain que vous vous ferez des amis en faisant le travail rapidement, ils ne tarderont guère à se muer en détracteurs si vous oubliez quelque chose et qu'il se produit une réinfection. Soyez des plus méticuleux.

Profitez des renseignements fournis par toute une série de ressources en ligne pour en apprendre avantage sur votre attaque et sur la façon de restaurer votre serveur. Rendez-vous sur le site DoSHelp (www.doshelp.com/trojanports.htm) ainsi que sur celui du fournisseur d'antivirus de votre société, comme par exemple Symantec, McAfee ou Trend Micro. Les sites de fournisseurs proposent tous des bases de données en ligne pour vous aider à identifier et dépanner une attaque, puis à vous en remettre. Ce sont également d'excellents centres de renseignements où vous pouvez obtenir des informations à propos des dernières infections.

Après avoir réparé les systèmes compromis et endommagés, fermez les brèches exposées en suivant les étapes prévues dans la phase « Limitation des dégâts ». C'est aussi un bon moment pour mettre à jour vos procédures de planification et de surveillance en fonction de ce que vous avez appris. Lorsque vous êtes prêt à remettre l'équipement en ligne, nous vous recommandons de procéder par étapes en utilisant vos outils de surveillance réseau pour rechercher des signes d'infection ou de certaines traces d'infection qui pourraient encore être présentes.

Mode de fonctionnement de Visual UpTime Select

Bon nombre des fonctionnalités dont vous avez besoin pour entretenir une surveillance sérieuse de votre réseau pour repousser les attaques sont les mêmes fonctionnalités dont vous dépendez de façon quotidienne pour utiliser des éléments stratégiques de votre réseau. Visual UpTime Select remplit ces deux rôles grâce à son analyse détaillée des sept couches OSI, son référentiel historique précis ainsi que ses fonctionnalités flexibles de génération d'alarmes.

Il est essentiel de disposer d'un aperçu récapitulatif qui fournit un compte-rendu complet de toutes les applications du réseau, y compris les inconnues.

Déployé dans le cadre de votre infrastructure, le logiciel Visual UpTime Select utilise une approche de système pour gérer les réseaux en fonction de l'instrumentation riche et détaillée des composants LAN, WAN et de routeur qui prennent en charge vos applications. L'instrumentation peut prendre l'aspect d'éléments ASE (Analysis Service Elements) ou d'agents matériels, qui peuvent être mis à niveau avec des informations supplémentaires à mesure de l'évolution des besoins, ainsi que celui d'une technologie d'agent logiciel intégrée aux composants réseau courants tels que les routeurs Cisco et autres périphériques d'accès.

Quel que soit leur mode de déploiement, les agents Visual UpTime Select fournissent une inspection des trames en profondeur pour toutes les données circulant à proximité afin de récolter des informations détaillées au sujet de l'utilisation et des performances des applications. Les agents chargent ces données sur un serveur Visual UpTime Select qui conserve, analyse et présente un aperçu complet de l'utilisation du réseau.

La base de données du serveur permet de bénéficier d'aperçus récapitulatifs à l'échelle du réseau qui fournissent un compte-rendu complet de toutes les applications présentes sur tout le réseau, y compris les inconnues. Conservées historiquement, ces données constituent la base de votre référentiel d'utilisation réseau en détaillant tous les facteurs clés :

- Serveurs et clients
- Protocoles utilisés
- Protocoles les plus utilisés
- Sources et destinations les plus utilisées, y compris les protocoles et les volumes de trafic
- Protocoles et volumes de trafic de site à site

Muni de cette compréhension détaillée des schémas d'utilisation de votre réseau, vous pouvez demander à Visual UpTime Select de vous avertir en cas d'anomalie au niveau du trafic et des schémas d'utilisation, où qu'elle se produise. Pour automatiser divers aspects de votre réponse en cas de notification et d'incident, vous pouvez exporter ces avertissements vers des systèmes tiers de gestion d'événements et de dépannages tels que Remedy.

Pour finir, lorsqu'il vous faut prendre les choses en main et examiner les trames à la recherche de nouvelles menaces ou autres attaques inconnues, Visual UpTime Select vous fournit des fonctionnalités de capture du trafic, de décodage des protocoles et d'exportation des trames en chaque point géré. Avec Visual UpTime Select, vous ne serez plus démuni face aux attaques réseau.

Gestion d'une attaque avec Visual UpTime Select

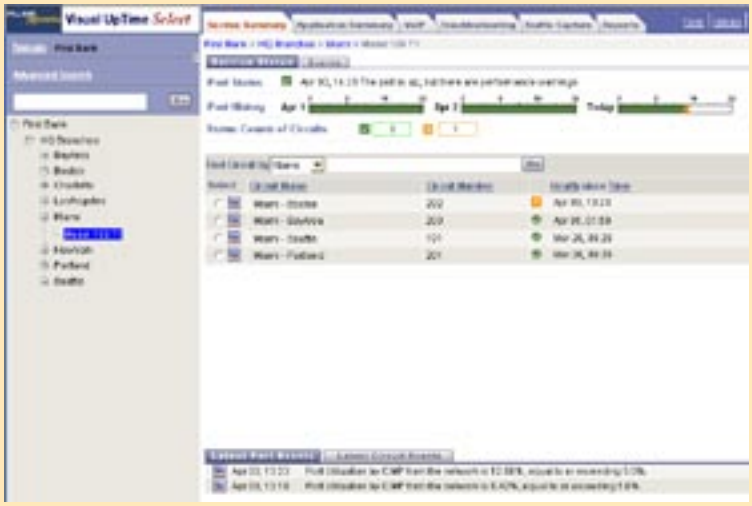

Figure 1 : *Utilisez les seuils personnalisables pour définir des déclencheurs sur le réseau.*

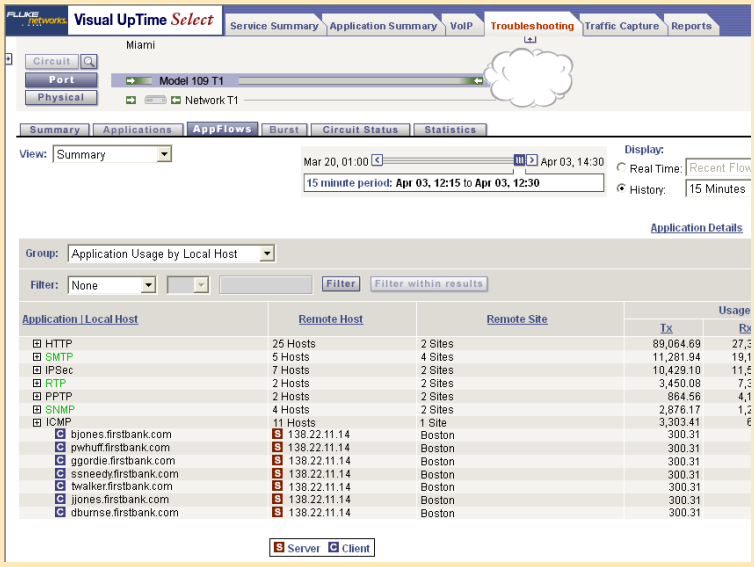

Figure 2 : *Les flux applicatifs soulignent les liens entre client individuel et serveur.*

Une plate-forme de gestion devrait être à même de détecter les attaques, de limiter les dégâts et de restaurer les activités. Visual UpTime Select vous fournit la visibilité stratégique nécessaire pour minimiser les risques et l'exposition aux brèches de sécurité.

Examinons un scénario où une attaque DDoS a infecté une entreprise. Une attaque de cette nature n'est pas identifiée avant que l'utilisation de la bande passante en plusieurs endroits dépasse le débit de port. Désormais d'autres utilisateurs et applications en subissent l'impact. Visual UpTime Select vous permet de définir des seuils personnalisables de façon à détecter des attaques potentielles plus rapidement et de façon plus efficace. Une alarme a été générée indiquant une augmentation du trafic ICMP au-delà de la cible du référentiel **(Cf. figure 1)**.

Une pointe du trafic ICMP ne signifie pas automatiquement que votre réseau subit une attaque ; il peut s'agir d'un symptôme d'une attaque ou peut-être simplement d'une pointe de l'utilisation autorisée de l'application. Muni de ces informations, examinez la situation plus en détails et étudiez les flux applicatifs. Visual UpTime Select identifie rapidement les flux individuels en effectuant un tri par ICMP. Vous pouvez constater que de nombreux utilisateurs autorisés accèdent au même serveur avec des quantités identiques de bande passante **(Cf. figure 2)**. Il s'agit d'une caractéristique d'une attaque de virus.

L'identification rapide d'une attaque potentielle et l'examen plus précis des flux applicatifs permet aux entreprises de vite limiter les dégâts et de restaurer rapidement des activités normales.

Conclusion

La sécurité de l'infrastructure informatique n'est plus quelque chose à quoi les entreprises peuvent simplement espérer prétendre. Les coûts d'une sécurité médiocre n'ont jamais été plus élevés. Il existe une tendance à la hausse d'élaboration de réglementations gouvernementales visant à instaurer des normes minimales obligatoires. L'obtention d'une infrastructure informatique sécurisée requiert planification et préparation bien avant qu'une attaque se produise.

Le principe de « protection, détection, réaction et restauration » constitue toujours une excellente façon de concevoir votre plan de sécurité global. Considérez la sécurité non pas comme un ajout mais bien comme une qualité que vous insufflez à chaque aspect de votre infrastructure. Ne focalisez pas uniquement vos plans de sécurité sur la défense du périmètre, car une portion non négligeable des menaces actuelles peut le contourner. Prévoyez plusieurs couches de protection et attendez-vous à ce que vos mesures de défense s'avèrent insuffisantes en élaborant et en mettant en œuvre une réponse efficace aux incidents pour vous remettre de n'importe quelle attaque.

Prévoyez plusieurs couches de protection et attendez-vous quand même à ce que vos mesures de défense s'avèrent insuffisante en élaborant et en mettant en œuvre une réponse efficace aux incidents pour vous remettre de n'importe quelle attaque.

Bon nombre des clés de mise en œuvre de votre plan de réponse aux incidents se trouvent dans les outils qui vous fournissent des fonctionnalités d'analyse et de surveillance de votre réseau à l'échelle de l'entreprise. Utilisez un référentiel périodique pour être au courant du mode de fonctionnement habituel de votre réseau. Vous apprenez ainsi ce qu'il faut chercher. Les entreprises qui effectuent des analyses de routine des flux applicatifs, de la source et de la destination ainsi que de l'utilisation du réseau peuvent utiliser les indicateurs réseau pour détecter rapidement les attaques. La configuration d'alarmes en cas de déviation du référentiel et de conditions anormales automatise bon nombre des tâches de surveillance les plus répétitives. Lorsqu'une attaque finit par se produire, vous êtes muni d'informations détaillées pour une réponse et une restauration rapides et efficaces. Grâce au déploiement d'outils performants d'analyse du réseau au sein de votre infrastructure, vous êtes en mesure de gérer les attaques, quel que soit le point d'origine des attaques ou la défense qui a fait défaut. Visual UpTime Select vous fournit la visibilité et les fonctionnalités d'analyse nécessaires pour détecter les attaques, limiter les dégâts et rétablir les activités qui limitent les risques et l'exposition à des failles de sécurité.

A propos de Fluke Networks

Fluke Networks fait partie des principaux fournisseurs de solutions de gestion des performances applicatives et des performances du réseau. Ses technologies permettent aux entreprises de gérer de façon fiable et sécurisée la disponibilité des applications stratégiques dans leur infrastructure. Les solutions de Fluke Networks permettent d'améliorer la disponibilité du réseau et des applications, d'optimiser l'utilisation de la bande passante et de réduire les coûts d'exploitation sur les infrastructures IP et traditionnelles. Pour plus d'informations, rendez-vous à l'adresse **www.flukenetworks.com**.

1 « The New Economics of Information Security », Lawrence Gordon et Robert Richardson, *Magazine Optimize*, avril 2004, numéro 30

2 *Corporate Losses From Internet-Based Attacks Average $2 Million*, TechWeb.com, 6 juillet 2004

3 Rapport Internet Security Threat Report de Symantec, tendances du 1er janvier 2004 au 30 juin 2004

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks est présent dans plus de 50 pays.
Pour connaître les coordonnées du bureau le plus proche, rendez-vous à l'adresse **www.flukenetworks.com/contact**.

Imprimé aux Etats-Unis. 11/2006 3025488 D-FRN-N Rév. A