PAESSLER

LIVRE BLANC

Surveillance de réseau : un élément indispensable de la sécurité informatique

Livre Blanc

PRTG NETWORK MONITOR

Auteur : Daniel Zobel, Responsable Developpement Logiciel, Paessler AG
Publication : juillet 2013

Sommaire

Introduction

Selon une enquête de Paessler AG, les entreprises souhaiteraient se protéger plus efficacement contre les cyber-menaces dans le futur. Plus de 1200 utilisateurs ont été interrogés lors de cette enquête sur l'intérêt de la mise en œuvre du logiciel Paessler-Software PRTG Network Monitor. Le résultat montre qu'environ 75% d'entre eux considèrent cet outil comme l'élément le plus important pour leur réseau en termes de sécurité. Ce livre blanc éclaire le rôle de la surveillance de réseau comme entité sécuritaire supplémentaire dans le réseau de l'entreprise. Il étudie les challenges à relever et préconise des solutions.

Situation actuelle

SÉCURITÉ INFORMATIQUE

Des études concernant la sécurité informatique en France révèlent que les entreprises ressentent le besoin de se rattraper quant aux mesures de sécurité mises en place. Entre-temps, les cybercriminels conçoivent des programmes nuisibles de plus en plus intelligents qu'ils mettent en œuvre par le biais de canaux divers. Leur cible privilégiée devient le Smartphone, avec une augmentation de 614 % des menaces visant les appareils mobiles en un an. Pour lutter contre les cyberattaques, la protection renforcée des systèmes d'informations des entreprises est devenue un élément « vital ».

Quelques 200 entreprises réparties dans 12 secteurs jugés vitaux pour la nation vont donc devoir revoir de façon drastique leurs systèmes de sécurité informatiques afin de pouvoir répondre aux nouvelles exigences en la matière.

Si l'on considère l'« État des lieux 2011 » en matière de criminalité sur Internet, présenté en septembre 2012, la superficialité de ces mesures de sécurité peut surprendre. En effet, selon ce même rapport, 52% des utilisateurs en ligne ont été confrontés à la cybercriminalité, mais aussi un grand nombre d'entreprises. Les dommages occasionnés par les virus, l'espionnage, le phishing etc., s'élèveraient à au moins 71,2 millions d'euros. C'est pourquoi à l'heure actuelle, il est indispensable que les entreprises accordent plus d'importance à l'aspect sécuritaire de leur infrastructure informatique.

PROTECTION DES SYSTÈMES INFORMATIQUES

Un grand nombre d'entreprises partent du principe que leur infrastructure informatique est suffisamment protégée par un pare-feu et un antivirus. Ceci dit, les cybercriminels développent des méthodes de plus en plus professionnelles pour attaquer les ordinateurs ou serveurs des entreprises. Chevaux de Troie, Vers, etc. ne sont souvent reconnus par les programmes de sécurité que lorsqu'il est trop tard. Dès que les intrus requièrent l'accès à un ordinateur du réseau, la compromission de l'ensemble du système n'est plus qu'une question de temps. Le résultat : manipulation et pertes des données, captage de l'ordinateur à des fins criminelles. Tout dérangement des systèmes internes de l'entreprise par l'attaque de logiciels malveillants peut empêcher la communication entre les différents sites de l'entreprise ainsi que le traitement des commandes et la communication avec le client. L'administrateur système, quant à lui, se retrouve confronté à une recherche longue des causes précises du dérangement. Quelles parties du système sont hors service ? Quels domaines ou composants ont été atteints par des logiciels malveillants ? La panne de système peut-elle avoir été provoquée par une autre cause ?

Pour éviter au maximum ce type de situations, il est nécessaire de protéger l'ensemble de l'infrastructure informatique. Pour ce faire, les entreprises ont besoin d'une protection complète. Ce type de protection inclut régulièrement, en plus d'un antivirus et d'un pare-feu, un logiciel de cryptage, un logiciel de sécurisation des données, un filtrage Internet, un scanner de ports et d'autres outils. Ceci dit, la surveillance de réseau, entité supplémentaire de sécurité, est indispensable pour aboutir à une protection complète.

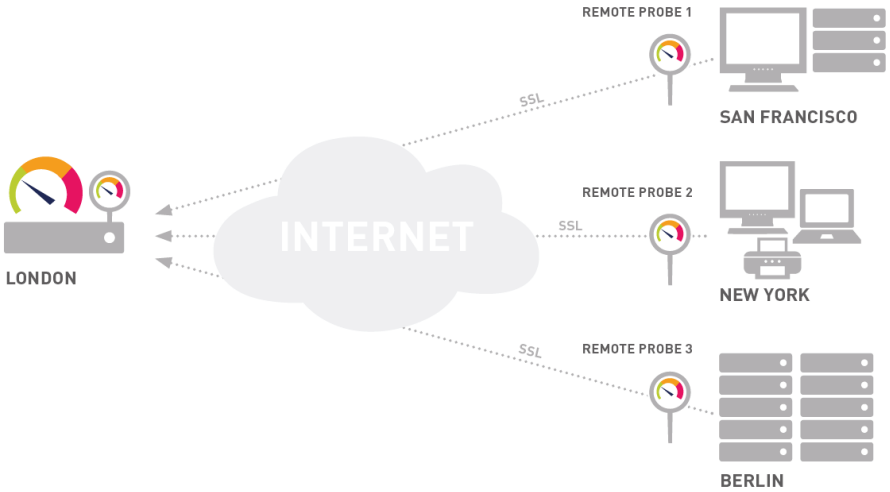
Systèmes d'avertissement précoces intégrés au réseau

La fonction de base d'une solution de contrôle du réseau est de garder un œil sur l'ensemble de l'infrastructure informatique, ses appareils et ses systèmes. En principe, les administrateurs sont en mesure de surveiller tout ce qui dispose d'une connexion définie et livre des informations concernant son état par le biais d'un protocole standard. Le logiciel de contrôle ne nécessite qu'une simple adresse IP pour le contact avec l'appareil ou le service, lui permettant de demander un état des lieux actuel. Ainsi, le responsable informatique est en mesure de vérifier toutes les heures le statut de toute zone de l'infrastructure informatique. L'objectif consiste à aboutir à une disponibilité et une performance optimale du réseau. Pour ce faire, le système de surveillance du réseau doit couvrir trois aspects différents en termes de sécurité :

- le contrôle des systèmes de sécurité eux-mêmes ;
- l'identification d'évènements inhabituels ;
- le contrôle des paramètres environnementaux.

Les entreprises travaillant sur différents sites peuvent garder un œil sur l'intégralité de leur réseau par le biais de « remote probes », actives dans ces trois catégories. Une « probe » est un petit logiciel permettant de surveiller un réseau à distance et qui envoie les données de surveillance au serveur central. Un logiciel de surveillance de réseau adapté contrôle de cette façon tous les composants d'un réseau, au siège comme dans les succursales d'une entreprise. Pour ce faire, il faut configurer les « capteurs » de surveillance qui permettent à l'administrateur de surveiller l'ensemble de son réseau depuis son bureau.

ILLUSTRATION :
Supervision répartie sur plusieurs endroits via les « remote probes »



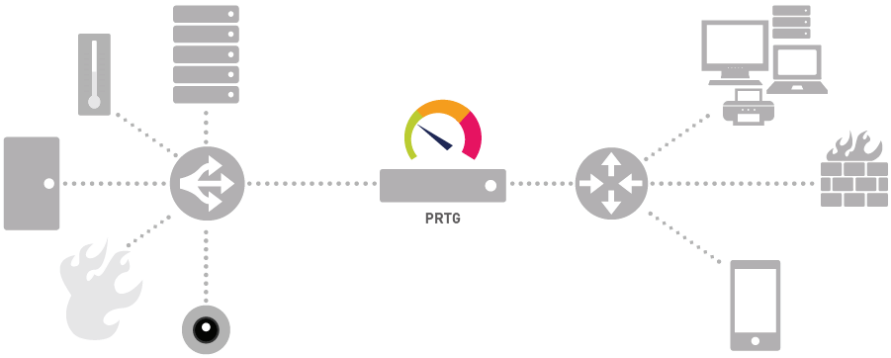
Si le logiciel de surveillance détecte une panne ou des évènements inhabituels, il envoie immédiatement une alarme par SMS ou e-mail à l'administrateur responsable. Ceci permet à ce dernier de rester informé d'un évènement où qu'il se trouve et en temps réel, et de réagir rapidement. Le système d'avertissement est basé sur des valeurs seuil prédéfinies. Dès que celles-ci sont dépassées, le logiciel donne l'alarme.

Grâce à l'interface web ou l'application Smartphone, l'administrateur a la possibilité de rester constamment connecté avec l'installation de surveillance et de donner directement l'alarme. À partir des données « live » de la surveillance, il peut évaluer directement la portée de la panne et prendre les mesures correctives adéquates.

Surveillance des aspects sécuritaires

Les responsables informatiques souhaitent être en mesure de réagir rapidement en cas d'attaques potentielles de logiciels malveillants. Si les solutions antivirus et les pare-feux découvrent les attaques trop tard, les effets occasionnés peuvent immobiliser entièrement une entreprise. Les administrateurs sont alors en situation réactive plutôt que proactive et ne peuvent ni prévenir ni empêcher le problème à temps. Ceci explique pourquoi les antivirus et les pare-feu ne suffisent pas à assurer une sécurité complète du réseau. Si les entreprises intègrent une solution de surveillance du réseau dans leur concept de sécurité, les dangers potentiels pour le réseau de l'entreprise sont alors prévenus à temps.

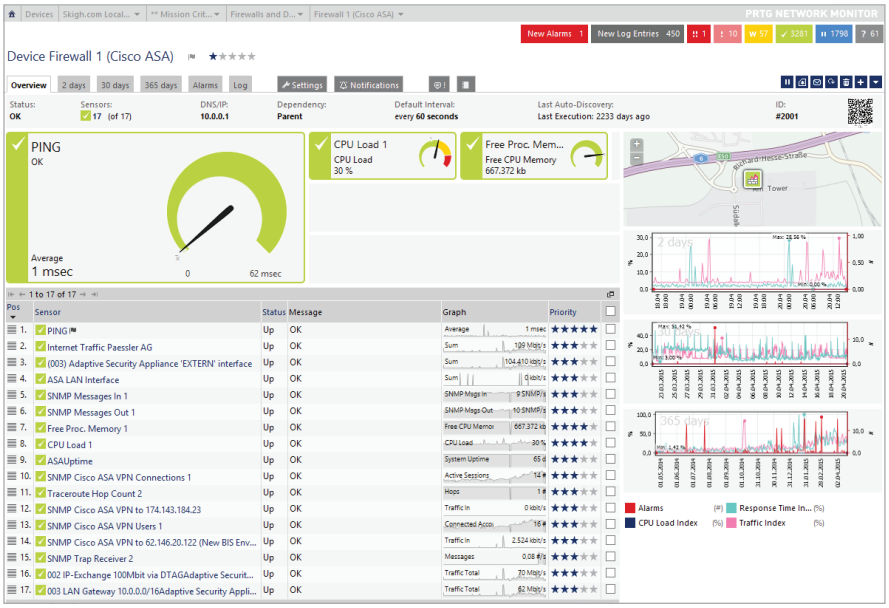
ILLUSTRATION :
Assure l'ensemble de la sécurité du réseau



VÉRIFIER RÉGULIÈREMENT LE PARE-FEU ET L'ANTIVIRUS

Une des missions importantes de la solution de contrôle du réseau consiste à vérifier le bon fonctionnement des systèmes de sécurité existants comme les pare-feu et les antivirus. D'autre part, la solution de surveillance fournit par exemple toutes les heures des données détaillées concernant la production et l'état du pare-feu. Un mauvais fonctionnement augmente le risque d'infection du réseau par un logiciel malveillant.

ILLUSTRATION :
Le logiciel surveille le statut du pare-feu



Ces attaques malfaisantes peuvent entraîner l'exécution non coordonnée de programmes par le CPU et l'ouverture de ports qui ne devraient pas l'être. Pour empêcher que cela n'arrive, les administrateurs sont informés à temps de toute anomalie du pare-feu.

Le logiciel de surveillance peut non seulement examiner le pare-feu, mais également le programme antivirus d'un serveur central d'e-mail, pour une surveillance complète et continue. Grâce à des capteurs spéciaux, la solution de surveillance examine aussi le Windows Security Center et détermine par exemple si l'antivirus et le programme anti logiciels malveillants sont à jour et fonctionnent sans heurts. Ceci permet de s'assurer que les ordinateurs clients du service informatique de l'entreprise sont eux aussi protégés des logiciels malveillants à tout moment.

CONGESTION DE LA BANDE PASSANTE COMME INDICATEUR DE PROBLÈME

Une solution de surveillance de réseau aide aussi l'administrateur à mesurer la bande passante de lignes spécialisées, de connexions de réseau ou d'appareils (routeurs, commutateurs) etc. Grâce à une surveillance accrue de l'utilisation de la bande passante, il est possible de détecter les attaques de logiciels malveillants. Une réponse ralentie des applications et sites Internet peut être un indicateur efficace. Un programme malveillant qui s'arroge une vaste partie de la bande passante peut être une des causes de congestion du réseau. Pour détecter ce type d'irrégularités, le logiciel de contrôle surveille différentes adresses IP, noms de ports, protocoles, etc. par le biais de Sniffing ou Flow-sensors. Ces capteurs xFlow rassemblent les données expédiées et les envoient au logiciel de surveillance pour évaluation. L'administrateur est alors en mesure d'analyser les données, de reconnaître les problèmes à temps et de prendre les mesures adéquates pour les résoudre. Ce type de surveillance de la bande passante convient particulièrement aux réseaux à très haute circulation de données. Si l'utilisation de la bande passante dépasse la valeur seuil déterminée, ou si elle diffère fortement de la moyenne des disparités habituelles, cela peut être le signe d'activités inhabituelles - par exemple une attaque par un logiciel malveillant. Le cas échéant, l'administrateur peut, avec son logiciel de surveillance, déterminer quelle adresse IP, connexion ou protocole occupe la plus grande partie de la bande passante, et réagir de façon adéquate.

SURVEILLER LES PARAMÈTRES DE L'ENVIRONNEMENT PHYSIQUE

Pour finir, un protocole de surveillance réseau contribue à la sécurité du bâtiment, car il veille également les indicateurs environnementaux. Des appareils spéciaux avec capteurs de fumée et de gaz permettent de signaler rapidement des incendies et autres évènements. Des capteurs de fermeture présents dans un bâtiment par exemple peuvent être configurés de façon à envoyer une alarme dès l'ouverture de portes, fenêtres ou armoires de serveurs. D'autre part, les responsables IT peuvent mesurer la tension du courant électrique à l'aide de matériel informatique adéquat, puis remettre ces données au logiciel de surveillance du réseau. Ce dernier identifie les disparités dans l'alimentation électrique et en informe l'administrateur. Grâce aux différents types de surveillance, l'équipe IT sait si un changement à court, moyen ou long terme doit être effectué dans l'environnement du réseau.

Évaluer les résultats

Les solutions de surveillance des réseaux de pointe exploitent les diverses données de surveillance et les communiquent ensuite clairement sous forme de graphiques ou de tableaux de bord. Les rapports élaborés par le logiciel résument les valeurs identifiées des composants individuels et des systèmes sous forme de messages faciles à lire. L'administrateur reçoit non seulement un rapport des activités de logiciels pare-feux et antivirus, mais aussi les paramètres concernant les prestations actuelles, comme la charge du CPU et du RAM de tous les serveurs et du matériel informatique. D'autre part, la disponibilité des divers appareils du réseau peut être visualisée par les responsables IT. Le rapport indique également les tendances pertinentes en matière d'utilisation de la bande passante et du réseau. Si cela s'avère nécessaire, l'administrateur peut élaborer des comparaisons entre données actuelles et historiques dans différentes situations. Lorsque les valeurs actuelles sont moins bonnes que les valeurs historiques, cela montre un besoin clair d'optimisation. Une analyse automatique des données de surveillance permet également de détecter un comportement identique de différents capteurs, et d'identifier ainsi des relations inconnues entre composants individuels du réseau. L'analyse des données historiques et l'identification de capteurs avec des modèles de comportement analogues sont particulièrement utiles lors d'études comparatives de réseaux complexes. Ils servent à explorer la charge et le type d'utilisation du réseau et à clore les boucles potentielles de sécurité.

ILLUSTRATION :
Analyse des données de surveillance sous forme de graphiques

Résumé

Seul un concept de sécurité englobant tous les domaines offre aux entreprises une sécurité optimale dans le cadre de sa gestion des risques. Ici, la surveillance du réseau constitue un élément supplémentaire indispensable au sein d'un concept de sécurité informatique. Ce concept doit aller au-delà de l'utilisation de pare-feu et de scanners de virus. Pour s'assurer que l'ensemble du réseau de l'entreprise est protégé efficacement des attaques de logiciels malveillants ou de pannes, l'ensemble des domaines de l'informatique doit être couvert. Dans ce cadre, reconnaître les tendances et les développements constituent des facteurs essentiels de détection des menaces. Un logiciel de surveillance du réseau inclut également un rôle d'avertissement précoce. Il justifie par conséquent une extension du concept de sécurité et aide à créer la sécurité et le contrôle souhaités par l'entreprise.

À PROPOS DE PAESSLER AG

Depuis longtemps, Paessler AG est le leader dans le domaine de la surveillance réseau. La société développe des logiciels de haute performance à des prix abordables et faciles à utiliser. Quelque soit la taille de l'entreprise (bureau à domicile (SOHO), TPE, PME, multinationales), les logiciels de Paessler apportent à la fois tranquillité, confiance et confort dont les services informatiques ont besoin. Grâce à la renommée de ses produits, Paessler dont le siège se trouve à Nuremberg (Allemagne), a déjà en charge plus de 150.000 installations à travers le monde. Fondée en 1997, Paessler AG est toujours une société privée et est à la fois membre de la Cisco Solution Partner Program et aussi partenaire de VMware Technology Alliance.

Des versions gratuites et d'évaluation de tous les produits peuvent être téléchargées sur www.fr.paessler.com/prtg/download.

Paessler AG · www.paessler.fr · info@paessler.com