Dimitri Vlachos est vice-président du marketing, chez ObserveIT. Il affiche à son actif plus de 15 ans d'expérience en tant que responsable marketing aussi bien dans des jeunes pousses (start-ups) que dans des entreprises bien établies. Il a acquis une solide expérience auprès des analystes des marchés de la sécurité et des performances réseau et applicatives.

Surveillance des utilisateurs et respect de la vie privée

Le juste équilibre

Les attaques initiées par les utilisateurs, qu'elles relèvent d'actes de pirates informatiques utilisant des informations d'identification volées, d'erreurs commises par des fournisseurs tiers ou de la négligence (voire de la malveillance) d'initiés, représentent la plus grande menace en matière de sécurité informatique dans les entreprises. Pour autant, personne ne veut d'un environnement de travail où les activités font l'objet d'une surveillance permanente. Les entreprises doivent-elles épier les moindres faits et gestes de leurs employés ? Ou, au contraire, doivent-elles s'en remettre entièrement à eux pour protéger leurs données ? La réponse est simple : ni l'un ni l'autre.

NATURE DES ATTAQUES INITIÉES PAR LES UTILISATEURS

Les attaques initiées par les utilisateurs sont généralement le fait soit d'un employé mécontent, soit d'un pirate informatique utilisant des identifiants qu'il a volés. Les employés sont souvent en cause, que la faute soit volontaire ou non. 82 % des failles de sécurité proviennent ainsi d'erreurs commises par les employés[1]. Quoi qu'il en soit, ces individus peuvent contourner les protections de l'infrastructure avec leurs identifiants de connexion, et une fois à l'intérieur du système, il ne leur reste plus qu'à se mettre au travail.

Les solutions reposant sur la surveillance des activités utilisateur ont été conçues pour fournir des informations sur ces menaces, du point de vue de l'utilisateur. Elles peuvent détecter chacune des actions exécutées par des employés, des fournisseurs et des partenaires authentifiés, quels que soient leur mode de connexion ou les applications auxquelles ils accèdent. Elles regroupent sous la forme de captures d'écran des séquences vidéo montrant précisément ce que chacune de ces personnes a fait et à quel moment.

Résultat : plus de 67 % des failles de sécurité sont liées au vol d'identifiants[2]. Rien qu'en utilisant des informations d'employés de base ou de fournisseurs les pirates sont capables de trouver les moyens de contourner les obstacles internes, de désactiver les pare-feux, collecter les données et installer leurs programmes malveillants.

Contre ce type d'attaques, les outils d'analyse constituent la meilleure défense. En comparant les actions des utilisateurs à leurs profils, à leur fiche de poste, à leur mode d'utilisation et à d'autres données, les équipes chargées de la sécurité peuvent rapidement détecter les comportements inhabituels, suspects ou contraires à la politique. Par exemple, les entreprises savent immédiatement si un employé ou un fournisseur référencé a modifié la configuration d'un pare-feu, exécuté une commande DROP sur une base de données ou lancé une application de partage d'écran pendant sa consultation des dossiers client. De nos jours, les solutions sont extrêmement sophistiquées. Elles vont jusqu'à prévenir un hôpital qu'un médecin non traitant tente d'accéder au dossier d'un patient, ou signaler qu'un vendeur essaye d'accéder à un système de terminaux de point de vente.

IMPORTANCE DES ANALYSES D'INVESTIGATIONS INFORMATIQUES DANS LA RÉACTION AUX INCIDENTS ET LES AUDITS DE CONFORMITÉ

Les professionnels de la sécurité sont confrontés à l'une des tâches les plus ardues qui soient : reconstituer les actions d'un pirate informatique dans le système. Nombreux sont les services informatiques qui s'appuient sur les journaux système pour obtenir ces renseignements. Une méthode qui se veut aussi incomplète que chronophage. Ces journaux sont conçus pour fournir aux développeurs un éclairage sur les défaillances logicielles, pas pour consigner l'ensemble des activités des utilisateurs. De ce fait, il est pratiquement impossible pour un utilisateur lambda de repérer des informations utiles sur un utilisateur depuis des données système. Par ailleurs, les applications ne génèrent pas toutes des fichiers journaux. Ainsi, même en regroupant les données contenues dans les fichiers journaux par le biais d'un système centralisé de gestion des événements et des informations de sécurité (SIEM), les entreprises peineront à obtenir une vue claire et complète sur les activités de leurs utilisateurs.

Les solutions de surveillance, en revanche, suivent les utilisateurs authentifiés à la trace sur le réseau et lorsqu'ils accèdent aux fichiers ou aux applications, enregistrant dans le même temps chaque saisie effectuée, chaque préférence définie et chaque option sélectionnée. Ensuite, il ne reste plus aux enquêteurs qu'à visionner les séquences vidéo pour obtenir les données empiriques relatives à l'activité illégale. Surtout, les entreprises peuvent rapidement mettre le doigt sur le coupable, ou tout du moins l'utilisateur victime du pirate informatique, et fermer immédiatement son compte. Elles savent avec précision quelles données ont été volées, quels dossiers client ont été piratés et quels systèmes restent vulnérables. Ainsi armées, elles peuvent réagir plus vite.

En outre, ces solutions de surveillance apportent la preuve irréfutable de la conformité aux normes PCI (Payment Card Industry), NERC (North American Electric Reliability Corporation) et FERC (Federal Energy Regulatory Commission), ainsi qu'à la loi américaine HIPAA (Health Insurance Portability and Accountability Act), entre autres organismes régissant la consultation et l'utilisation des données sensibles.

TYPES D'ACTIVITÉS À SURVEILLER

En général, les entreprises ne s'intéressent pas à la vie privée des employés. Sauf, bien sûr, lorsque leur comportement peut avoir des répercussions néfastes sur leur sécurité. C'est la raison pour laquelle les actions qu'effectue un utilisateur sur le réseau de l'entreprise, après s'être authentifié, doivent être surveillées, enregistrées et consignées. Les pirates informatiques sont passés maîtres dans l'art du camouflage et savent faire profil bas une fois le système infiltré. Si le logiciel de surveillance devait ignorer les activités des utilisateurs sur Facebook ou ne suivre les activités qu'à l'aide de programmes spécifiques, il serait aisé de dissimuler des comportements illégaux. Même si la surveillance porte sur toutes les actions, seules les activités suspectes doivent déclencher des alertes.

COMMUNICATION RELATIVE À LA POLITIQUE DE SURVEILLANCE

Les entreprises doivent informer leurs employés et tout utilisateur tiers de cette surveillance. Pour commencer, il leur faut rédiger une politique et des procédures qui exposent clairement les activités placées sous surveillance, l'utilisation qui est faite des informations recueillies et le comportement attendu. Les utilisateurs doivent comprendre que toutes leurs actions, y compris leurs saisies, sont enregistrées, mais que seules celles liées à la sécurité sont examinées de près.

La politique de l'entreprise doit leur être communiquée en même temps que leurs identifiants de connexion. Selon la taille de l'organisation, cette information peut être relayée par les ressources humaines lors de l'accueil des nouveaux employés.

Cet article vous a plu ?

- Consultez le centre de connaissances pour obtenir plus d'informations, travailler en collaboration et entamer des discussions sur les tendances en matière de sécurité.

www.isaca.org/topic-security-trends

Les entreprises se doivent également de rappeler cette surveillance aux utilisateurs. Il est ainsi possible de paramétrer les logiciels de surveillance de sorte à afficher des notifications et des messages importants relatifs à la politique sur la page de connexion. En exigeant des utilisateurs qu'ils confirment ces messages avant de poursuivre, l'entreprise s'assure que l'information a bien été transmise.

CONCEPT DE DISSUASION INFORMATIQUE

En informant les employés, les fournisseurs, les partenaires et tout autre utilisateur reconnu disposant d'informations d'identification que leurs actions sont surveillées, vous dissuadez tout comportement anormal, illicite et contraire à la politique de l'entreprise. Personne n'est en effet enclin à agir illégalement devant une caméra.

LE JUSTE ÉQUILIBRE

En matière de sécurité des entreprises, tous les moyens sont bons pour protéger les actifs et les informations sensibles. Si la surveillance des activités utilisateur est la meilleure protection contre les vols commis en interne, les entreprises doivent penser à faire preuve de tact. Il est fondamental de s'assurer, par une communication ouverte, que les employés et les parties tierces comprennent les initiatives, politiques et procédures mises en place. Un tel système est utile pour réagir aux incidents, effectuer des audits de conformité, mais aussi pour éviter que des employés ne soient tenus responsables, à tort, des actions commises par un pirate informatique par le biais de leur compte. Employés et partenaires doivent comprendre que ce système n'est pas destiné à épier leurs activités quotidiennes, à scruter leur historique de navigation ni à les mettre mal à l'aise. En trouvant le juste équilibre entre surveillance et respect de la vie privée, les entreprises peuvent mettre en place des solutions de sécurité qui les protègent, elles et leurs utilisateurs.

NOTES DE BAS DE PAGE

[1] Fogarty, K., « *82% of Data Breaches Due to Staff Errors; 4% of IT Trusts Users; IT Is Still to Blame*, » *ITWorld*, 19 avril 2012, *www.itworld.com/article/2729066/security/82--of-data-breaches-due-to-staff-errors--4--of-it-trusts-users--it-is-still-to-blame.html*

[2] Verizon, *2014 Data Breach Investigations Report*, mars 2014, *www.verizonenterprise.com/DBIR/*