

Alberto Pace
CERN, Internet Services Group leader
Information Technology Department

Dans les dernières années, quasiment la totalité des systèmes informatiques a été confrontée à des failles dans les logiciels, ce qui a fait naître des opportunités économiques pour de nombreux acteurs de la sécurité informatique. Les éditeurs de logiciels ont développé des nouvelles technologies pour la mise à jour dynamique par internet des correctifs de leurs produits (patch). Les fabricants de matériel réseau ont vu exploser la demande de certains produits (pare-feux, routeurs d'entreprises, serveurs proxy, zones démilitarisées, ...) et vécu l'essor de nouveaux marchés pour la sécurité informatique comme, par exemple, les produits antivirus pour les ordinateurs de bureau et les produits anti-spam pour les messageries électroniques.

Cette tendance a pu laisser croire qu'en achetant les produits réseau adéquats, en appliquant systématiquement les patches recommandés, en surveillant le trafic réseau et en installant une solution antivirus efficace on pouvait sécuriser globalement un système informatique d'entreprise. Le tout en suivant méticuleusement les étapes qui expliquent les mesures à prendre pour renforcer la sécurité d'un grand nombre de postes de travail.

Désormais il est clair que cette stratégie, quoique nécessaire, n'est malheureusement plus suffisante à améliorer significativement la sécurité d'un important système d'information.

Deux aspects supplémentaires doivent être intégrés dans la conception et la définition d'une stratégie de sécurisation efficace. Le premier est le « facteur humain » (en anglais « Social Engineering ») et le second est la gestion des identités et des accès au sein de l'entreprise.

Le facteur humain, qui est très souvent à l'origine des intrusions les plus simples, peut être résumé en « demandez le mot de passe ou les codes d'accès à l'utilisateur lui-même ». Les méthodes qui visent à tromper l'utilisateur n'utilisent pas exclusivement le système d'information (courrier électronique, site web - « phishing »), mais aussi des moyens de communication conventionnels comme le téléphone, un courrier traditionnel ou même une visite en personne.

Pour limiter les risques liés au facteur humain il faut souligner l'importance de la formation comportementale et technique que toute personne amenée à manipuler des informations confidentielles doit avoir reçue pour éviter de divulguer involontairement des secrets. A cela s'ajoutent motivation, efficacité et productivité qui peuvent être réduites en travaillant dans un environnement fortement sécurisé. Naturellement, les problématiques et les stratégies liées à la maîtrise du facteur humain sont très complexes et nécessiteraient une longue analyse qui ne peut être approfondie dans cet article.

La gestion des identités et des accès est l'autre aspect essentiel de la stratégie de sécurité de l'entreprise. Elle consiste à assurer la traçabilité de toutes les actions effectuées au sein du système d'information, y compris celles n'entraînant pas des modifications comme une simple lecture d'un document. Pour atteindre cet objectif, une série de mesures peut être envisagée, la plus commune étant la règle du AAA, de l'anglais Authentication, Authorization and Accounting, qui définit et identifie les trois composantes à implémenter d'une façon indépendante dans le système d'information de l'entreprise.

Le premier pilier, l' « Authentication » permet d'identifier sans équivoque l'identité de toute personne qui a accès au système informatique de l'entreprise. Il est constitué de plusieurs

composants dont la définition des processus internes, les procédures et tous les flux qui permettent la lecture, la création, la modification, la suppression de toute information au sein de l'entreprise. A ceux-ci s'ajoutent les outils et les technologies utilisés pour la mise en œuvre de ces processus qui font aussi partie du système de gestion des identités.

Le deuxième pilier, l' « Authorization » permet le contrôle d'accès aux ressources. Il s'agit de l'association entre une permission (de lecture, de modification, d'utilisation, de suppression, ...), une entité (personne, compte informatique, ordinateur, groupe) et chaque ressource de l'entreprise (fichiers, ordinateurs, imprimantes, documents, ...). Cette association définit les droits d'accès à chaque ressource et peut aussi contenir des attributs supplémentaires qui limitent ces droits dans le temps (exemple : droits restreints à certaines plages horaires) ou à certains emplacements (exemple : accès limité à l'intranet ou à partir de certains postes de travail). En option, le contrôle d'accès peut aussi être basé sur des groupes (« Role Based Access Control » - RBAC) qui limite à des ensembles d'utilisateurs (groupes) l'allocation des droits d'accès aux ressources. Dans ce cas, les autorisations sont déduites en gérant l'appartenance des utilisateurs à ces groupes.

Le troisième pilier, l' « Accounting » assure la traçabilité de toute action faite sur le système d'information. Il contient le journal de chaque opération (qui, quand, où, quoi) et il permet l'implémentation de la réversibilité de chaque changement. A noter que le système d'accounting ne peut pas remédier à une fuite d'information confidentielle mais il peut en identifier le responsable et réparer toute corruption de données qu'elle soit volontaire ou involontaire.

La règle du AAA est la base pour bâtir une infrastructure sécurisée pour un système d'information complexe. Le lecteur réalisera qu'entre la simple théorie décrite ci-dessus et l'implémentation pratique dans un contexte réel d'entreprise, avec un grand nombre de systèmes hétérogènes multi-plateformes souvent incompatibles, il peut y avoir un fossé insurmontable, qui oblige la petite ou moyenne entreprise à s'adresser à des professionnels de la sécurité informatique. Ceci représente une opportunité émergente qui est en train de donner un nouvel essor à ce marché très porteur. Celle-ci sera discutée pendant la conférence sur la sécurité des systèmes information qui se tiendra le 22 mai 2007 au CERN à Genève.

Alberto Pace (alberto.pace@cern.ch)