SYSTÈMES D'INFORMATION

Sécurisation mode d'emploi

FABRICE FRADE
Directeur technique
Intranode

Les systèmes d'information bancaires *se caractérisent par leur forte hétérogénéité. Leur sécurisation n'en est que plus compliquée. Elle doit faire appel à des moyens multiples, des plus ponctuels comme les firewalls aux plus étendus comme les audits systématiques.*

LES CONTRAINTES D'UN SYSTÈME d'information bancaire peuvent se résumer à assurer un niveau de sécurité et de disponibilité élevé dans un environnement fortement hétérogène. L'hétérogénéité résulte de la cohabitation de différentes générations d'équipements et d'applicatifs, fruit de la migration de l'architecture mainframe vers le modèle client-serveur. Cette hétérogénéité est renforcée par le phénomène de regroupement des ressources informatiques entre régions ou lors de fusions entre acteurs.

L'exigence de sécurité est liée à la criticité des données traitées et à la sensibilité des transactions effectuées. Elle se double de la nécessité de maintenir intactes la réputation de l'établissement et la confiance qui en découle. Ces contraintes sont d'autant plus sensibles dans un contexte internet. Pourtant les moyens existent, des plus simples aux plus étendus.

LES ÉLÉMENTS RÉSEAUX

■ Les firewalls : comme toute machine accessible depuis l'internet, le serveur web bancaire doit être protégé contre l'utilisation frauduleuse d'un service. Le firewall veille à ce que seul le service web puisse être accessible depuis internet, à l'exclusion de toute autre composante du système d'information (*graphique*).

■ Serveurs et firewalls redondants : afin d'assurer un service continu, les serveurs web et les firewalls qui les protègent sont répliqués localement ou sur un autre site. Des équipements ou logiciels spécialisés sont chargés de la répartition des flux.

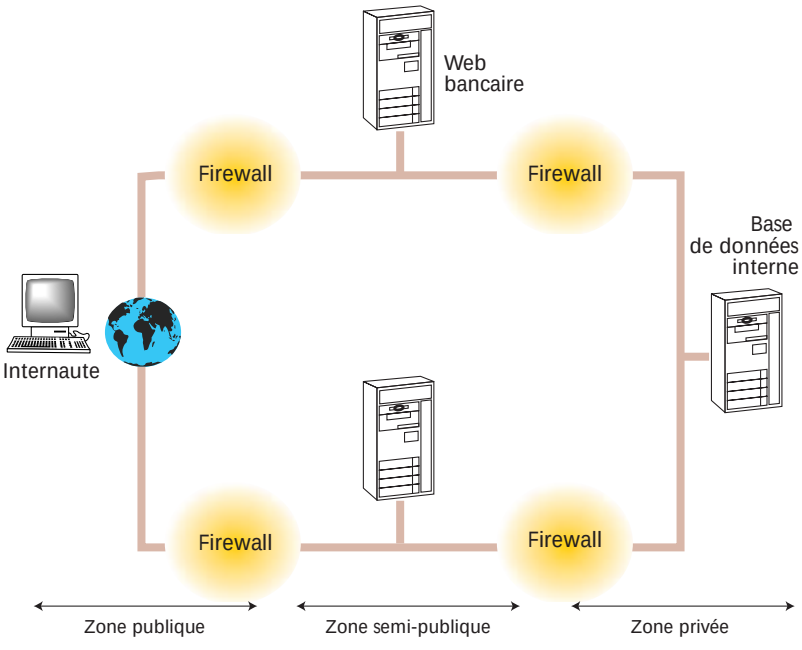
■ Double barrière : le serveur web bancaire, accessible depuis internet, est particulièrement vulnérable. En cas de compromission, les ressources internes doivent rester protégées. Le serveur web sera donc isolé du réseau interne par un second firewall. Celui-ci restreint aussi les connexions possibles au strict nécessaire.

LES ÉLÉMENTS APPLICATIFS

Il faut maintenant s'assurer que les connexions autorisées ne soient pas détournées de leur usage prévu.

■ Sécurisation du serveur web : il convient d'apporter un soin parti-

Les éléments réseaux : les firewalls



culier au paramétrage du serveur web, car toute faille pourrait immédiatement être exploitée par un tiers malveillant. Des erreurs classiques de configuration concernent l'affichage par le serveur du contenu d'un répertoire, voire de sa configuration et des éléments annexes utilisés. De même, il est important d'organiser une veille permanente sur les nouvelles failles qui pourraient affecter le serveur.

■ Sécurisation de l'application : le serveur web exécute une application, en général représentée par plusieurs «scripts», chacun en charge d'une partie des fonctionnalités. Chacun de ces éléments est potentiellement vulnérable.

Le niveau minimal de sécurisation à ce stade passe par l'utilisation d'une clé de chiffrement de 128 bits. Le protocole entre le client et le serveur web est SSL (Secure Sockets Layer). Toutefois SSL ne contrôle aucunement la nature des données. On peut donc très bien transporter des requêtes exploitant des vulnérabilités de la manière la plus confidentielle qui soit. Le serveur web étant un élément à accès public, il ne se trouve pas dans une zone de confiance. Une protection supplémentaire, par exemple un chiffrement SSL ou un réseau privé virtuel, devra donc être mise en place pour les communications entre le serveur web et le réseau interne.

L'accès à une application bancaire nécessite une authentification. Un process vérifie l'identité de l'utilisateur en lui demandant un mot de passe. Ce mot de passe doit être suffisamment long et non «devinable».

Si les deux éléments ci-dessus sont en général mis en œuvre, l'habilitation est souvent négligée. Cette fonction permet de corréler l'authentification de l'utilisateur avec les données qu'il manipule. En effet, le fait d'être reconnu comme un client valide ne doit pas autoriser la consultation de l'ensemble des données, en particulier celles des autres clients. Toutes les transactions devront donc mettre en confrontation l'identité de l'utilisateur et ses droits sur les données accessibles.

La sécurisation globale…

Maintenir à jour la sécurité d'une telle architecture, association d'éléments très différents, est une tâche à part entière, car ni le système ni son environnement ne connaissent un état stable. Les mises à jour logicielles et les modifications de configurations sont quotidiennes. Il en découle des erreurs humaines, inévitables.

Par ailleurs, la vitesse d'apparition de nouvelles failles logicielles sur les éléments du système d'information et du réseau est élevée, de l'ordre de deux failles identifiées par jour en moyenne en 2000.

Ces deux facteurs augmentent le niveau de vulnérabilité global, bien souvent à l'insu des exploitants. La connectivité internet vient ajouter à ces risques en démultipliant l'exposition du système au monde extérieur. Comment connaître alors l'état de vulnérabilité internet du système dans sa globalité à un moment donné ? Comment savoir si des failles sont présentes et y remédier à temps ?

… de façon systématique et continue

Une réponse fréquemment apportée est de mener des audits réguliers du périmètre internet, grâce à des équipes hautement qualifiées. Toutefois, le défi auquel sont confrontés les responsables de la sécurité est de pouvoir systématiser ce processus d'audit sur la totalité du système d'information, et ce de manière continue.

Pour mener à bien cette mission, de nouvelles solutions existent. Elles consistent à automatiser tout ce qui peut l'être dans la démarche d'audit :

- la veille sur l'apparition de nouvelles vulnérabilités,
- l'exécution des audits,
- la cartographie des vulnérabilités,
- l'analyse de l'évolution de la vulnérabilité globale système,
- la préconisation des nouvelles parades à mettre en place.

L'ensemble est délivré sous forme logicielle, voire de service clé en mains. Ce type de solution, déployée en complément aux audits fondamentaux, permet d'obtenir l'évaluation en continu du niveau de sécurité réel, pour une prise de décision efficace dans la gestion du risque internet. ■