LA DEFENSE EN PROFONDEUR

C'est quoi la défense en profondeur ?

Defense in Depth ou défense par couche en français est un concept important. C'est un ensemble de contrôles de sécurité qui, mis bout à bout, permettent une sécurité efficace.

Plus on se rapproche de l'objet ou la donnée que l'on veut protéger et plus la sécurité est renforcée.

Si un groupe de personnes exploite une faille dans chacun des contrôles mis en place, la défense en profondeur permet de ralentir l'attaque pour que l'on ait le temps de réagir.

Chaque couche de sécurité (pare-feu, systèmes de détection d'intrusion, authentification forte, etc.) fonctionne indépendamment pour limiter l'impact d'une faille dans l'une d'entre elles.

Si une défense est contournée ou compromise, une autre couche peut encore offrir une protection.

Exemple de mesures :

- **Le pare-feu : première barrière contre les accès non autorisés.**
- **Contrôle d'accès (authentification forte) : empêche l'accès même si un attaquant franchit la première couche.**
- **Chiffrement : même si un attaquant parvient à accéder aux données, il ne pourra pas les exploiter sans la clé de déchiffrement.**
- **Surveillance continue : des outils de détection d'intrusions peuvent signaler des comportements suspects pour permettre une intervention rapide.**

On assimile souvent ce concept aux châteaux forts. En effet, ces ouvrages médiévaux proposaient plusieurs niveaux de défenses. On plaçait dans le donjon le "trésor". Pour qu'un assaillant l'atteigne, il devait traverser les douves, passer la muraille, ouvrir la porte du donjon… Ce sont autant de barrières qu'un hacker devra franchir pour atteindre son but.

Les problèmes de Cyber sécurité

Voici quelques-uns des problèmes courants auxquels les entreprises doivent faire face lors de la mise en œuvre d'une stratégie de cybersécurité :

- **Le logiciel antimalware n'a pas été mis à jour ou n'est pas installé sur tous les appareils.**
- **Les employés n'ont pas été formés et sont victimes de phishing.**
- **Les correctifs logiciels ne sont pas mis à jour.**
- **Les règles de sécurité ne sont pas appliquées.**
- **Le chiffrement n'est pas mis en œuvre.**
- **Les employés distants se connectent à des réseaux non sécurisés.**

- **Les failles de sécurité physique, telles que les salles de serveurs, n'ont pas de contrôle d'accès.**
- **Les partenaires commerciaux, tels que les fournisseurs de services cloud, ne sont pas entièrement sécurisés.**

La mise en place d'une défense en profondeur aide à prévenir ces menaces.

Cet exemple de modèle représente une stratégie de défense en profondeur pour protéger les actifs critiques (ce qui a de la valeur et qu'il faut absolument protéger) d'une entreprise contre les menaces externes et internes.

Chaque couche de sécurité joue un rôle spécifique dans la protection des systèmes.

- **Nuage Public et Cloud Privé : le Nuage Public représente les services et infrastructures en dehors des systèmes internes, accessibles via le cloud. Le Nuage Public inclut des stratégies comme la gestion des correctifs de vulnérabilité, l'application de pare-feu, et les solutions de protection antivirus. Le Cloud Privé contient des éléments plus sécurisés comme la virtualisation des serveurs et des infrastructures virtuelles, assurant une isolation supplémentaire et une meilleure gestion des accès.**
- **Perimeter Security (Sécurité Périmétrique) : cette partie protège les systèmes contre les attaques en bordure du réseau, en utilisant des pares-feux, des systèmes de détection et de prévention des intrusions (IDS/IPS) et des zones démilitarisées (DMZ). Elle permet de filtrer et d'inspecter le trafic réseau avant qu'il n'atteigne le LAN.**

- **Network Security (Sécurité du Réseau) : la sécurité réseau inclut des mesures pour protéger la circulation de données à l'intérieur du réseau, comme la protection des communications VoIP, le filtrage via les ACL, les VLAN et l'analyse de malware. Cette couche empêche la propagation d'attaques à l'intérieur du réseau.**
- **Endpoint Security (Sécurité des terminaux) : cette couche concerne la sécurité des appareils individuels comme les ordinateurs et téléphones portables, en utilisant des solutions antivirus, des pares-feux logiciels et des outils de sécurité mobile. Elle protège les points d'entrée pour réduire les risques.**
- **Application Security (Sécurité des Applications) : la sécurité des applications protège les logiciels contre les vulnérabilités, avec des pratiques comme les tests de sécurité d'applications, le contrôle d'accès et l'authentification (MFA), les mises à jour, la mise en place d'un pare-feu applicatif. Ces mesures réduisent les risques d'exploits par des failles dans les applications.**
- **Mission Critical Assets (Actifs Critiques de la Mission) : au cœur du modèle se trouvent les actifs critiques de l'organisation, que toutes ces couches visent à protéger. Ce sont les éléments essentiels au fonctionnement de l'organisation, tels que les données sensibles et les systèmes clés.**

Les logiciels DLP (Data Loss Prevention) ont pour objectif de protéger les informations critiques, qu'elles soient stockées, en transit ou utilisées.

Il y a des logiciels DLP basés sur le réseau : ils surveillent les données en transit à travers les réseaux pour détecter et bloquer toute tentative de fuite (par exemple, par e-mail ou téléchargement sur un cloud non sécurisé).

D'autres sont des logiciels DLP basés sur les terminaux : ils se concentrent sur la protection des appareils en surveillant les actions locales sur les fichiers et les données (comme la copie ou le déplacement de fichiers).

Enfin, il y a des logiciels DLP basé sur le stockage : ils protègent les données au repos (c'est-à-dire celles stockées sur des serveurs ou des bases de données).

Les objectifs de DLP sont :

- **Prévenir les fuites de données sensibles, qu'elles soient accidentelles ou malveillantes ;**
- **Garantir la conformité réglementaire, notamment vis-à-vis des lois comme le RGPD (Règlement Général sur la Protection des Données) ;**
- **Protéger la réputation de l'entreprise en évitant les violations de données.**

Operations : cette partie gère la sécurité opérationnelle, avec des fonctions comme la surveillance en temps réel, la gestion des incidents et l'analyse des comportements anormaux.

Policy Management (Gestion des Politiques) : la gestion des politiques couvre la gouvernance de la sécurité informatique, la gestion de la configuration et les audits réguliers (Pentest, formation des personnels, gestion du risque). L'approche en couches de ce modèle permet une défense multi-niveau, limitant la progression d'une menace à travers différentes couches et renforçant la sécurité globale.

Conclusion

En empilant les processus de sécurité, la probabilité d'une perte de données est minimisée. Une seule couche de sécurité n'est pas suffisante pour se protéger.

Si un hacker infiltre avec succès le réseau d'une organisation, la défense en profondeur donne aux administrateurs le temps de lancer des contre-mesures. Des logiciels antivirus et des pares-feux doivent être en place pour bloquer toute nouvelle entrée, protégeant ainsi les applications et les données de l'organisation contre toute compromission