Sécurité de serveurs

Service de conseil sur la sécurité de vos serveurs physiques ou virtuels, hébergés dans nos datacenters ou non. Il peut comprendre un scan du serveur et la mise en place d'un firewall local.

- Documentation publique
  - Sécurité de serveurs

Documentation publique

Documentation publique

Sécurité de serveurs

Service de base

Le service permet de scanner et analyser un serveur pour détecter des failles ou des risques de sécurité. Le Ci utilise l'outil « Nessus » qui, avec une base de données de signatures régulièrement mise à jour, permet de relever les failles de sécurité de l'OS, ainsi que celles des applications installées. Ces failles de sécurité pourraient être exploitées par des hackers pour prendre le contrôle de machines à distance. Un rapport d'analyse de sécurité complet est soumis à la fin de l'opération.

Le périmètre du service se limite aux serveurs présents sur le campus UNIL.

Les failles détectables sont :

- L'état de patches de sécurité de l'OS et des applications installées.
- Liste de services activés ou ports ouverts & Classification des risques d'attaque liés.
- Liste des applications installées, leurs versions et vulnérabilités découvertes.

Les menaces que l'on peut détecter sont :

- Brèches de sécurité connues et risques liés.
- Vulnérabilités aux tests de pénétration (pen-test).

Les menaces que l'on ne peut détecter sont :

- Failles de sécurité encore inconnues ou non répertoriées.
- Nous ne faisons pas de tests d'attaque type « Denis of Service » (DoS) » ou « Distributed Denis of Service » (DDoS).

La sécurité étant l'affaire de tous, les tâches suivantes sont de la responsabilité de l'administrateur :

- Faire la mise à jour régulière de l'OS et des applications installées. S'inscrire aux listes de distribution des mails de sécurité.
- Restreindre les services actifs au strict minimum.
- Installer l'antivirus.
- Protéger le serveur par le firewall « Authentic »

- Restreindre l’accès aux stricts gestionnaires système, ainsi que le mode d’accès depuis UNIL, à distance (VPN-Crypto).
- Sécurisation d’accès physique.
- Détection incendie, inondation.
- Système redondant, alimentation électrique redondante, batterie de secours.
- Tester, valider la sauvegarde – 1/an.
- Plan de « disaster-recovery » : à établir en cas de problème majeur, il permet de restaurer le serveur au plus rapidement possible.
- Activer le firewall local : filtre des requêtes non désirées ou des attaques venant des machines intérieures ou extérieurs au campus UNIL.

Remarque : le Centre informatique n'effectue pas de support pour les logiciels installés, ni la configuration du firewall local.

Certificats pour serveurs Web : Recommandations

Tout serveur web de l’UNIL doit être configuré pour fonctionner avec le protocole sécurisé HTTPS. Pour cela, à l’exception des cas ci-dessous, nous recommandons l’utilisation des certificats Let’s Encrypt. Le site https://letsencrypt.org/ donne tous les détails sur le fonctionnement de cette plateforme ; aucune intervention de la « UNIL Registration Authority » ou du Ci n’est nécessaire.
Dans les cas suivants, nous recommandons de continuer à utiliser les certificats DigiCert :
1.- Les serveurs web récupérant le mot de passe de l’utilisateur (par exemple Login AAI, Login OTRS, …).

2.- Les serveurs web et les services très exposés (par exemple owa.unil.ch).
3.- Les serveurs web de production de l’informatique administrative (par exemple applications.unil.ch, sapcent.unil.ch, …).

En cas de doute, chacun peut s’adresser à pki@unil.ch

Recommandation du 1.11.2018