FORMATION : SÉCURITÉ

DS-131 – Infrastructure SSO avec SAML (2 jours)

Matériels et logiciels utilisés

Linux, simpleSAMLphp, Apache mod_auth_mellon

Présentation

La multiplication des applications hébergées (SaaS) oblige les DSI à proposer des solutions pour garantir la confidentialité des informations internes. A ce titre l'authentification des utilisateurs est un sujet majeur. En effet il est impossible de demander à chaque utilisateur de retenir un mot de passe pour chaque application. Pour autant il n'est pas pensable d'ouvrir à des applications externes un accès à la base d'authentification interne (souvent un Active Directory). C'est à cette problématique que les mécanismes SSO permettent de répondre, en autorisant un échange standard et sécurisé des informations d'identité entre des entités distinctes.

Objectifs

Ce stage permet aux administrateurs système, réseau et sécurité de découvrir les mécanismes de SSO disponibles avec un **focus sur SAML**. Ce protocole est le plus standard, il est disponible sur de nombreux systèmes et tend à remplacer les autres mécanismes existant. Des maquettes permettent de concevoir de A à Z un système basé sur SAML. Les **deux modes principaux (IDP et SP) sont couverts**, permettant d'appréhender l'intégralité des échanges nécessaires au bon fonctionnement. Un accent particulier est placé sur la phase d'analyse des dysfonctionnements propres au SSO.

Public Concerné

Administrateur système, réseau et sécurité

Compétences nécessaires

Notions sur le chiffrement SSL/TLS.
Notions sur HTTP/HTTPS.
Bases en système Unix : édition de fichiers, démarrage de processus.

Programme

JOUR 1 – Principes du SSO

Principes
- Présentation des mécanismes SSO
- Rappels sur HTTP
- Rappels sur Digest et Kerberos

Protocoles d'échange
- SAML
- OAuth
- Shiboleth

Les parties prenantes
- Identity Provider (IDP)
- Service Provider (SP)

Organisation
- Echange d'informations
- La fédération d'identité
- Clefs et certificats

JOUR 2 – Architecture SSO avec SAML

Définir son projet SSO et choisir les composants

Créer un IDP
- Maquette avec simpleSAMLphp
- Configurer les backends d'authentification
- Déclarer les SP

Créer un SP
- Maquette avec simpleSAML ou mod_mellon
- Configurer la délégation d'identité
- Déclarer les IDP

Diagnostiquer les incidents
- Méthodologie
- Comprendre les échanges
- Vérifications importantes

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.