

# Inventaire des composants



Université  
Paul Sabatier  
TOULOUSE III

Yannick Chevalier  
Université de Toulouse  
CSA M1, Security



# RETOUR SUR LES COMPOSANTS

## COMPOSANTS CONCRETS

- ▶ l'environnement physique (sites, bâtiments, salles, badges,...)
- ▶ l'environnement SI déployés (serveurs, clients, routeurs, ...)
- ▶ l'environnement SI réel (téléphones portables, tablettes, portables,...)
- ▶ les personnes recensées et les visiteurs

## CE COURS

- ▶ recensement systématique des composants
- ▶ avec un focus sur la sécurité dans les différents cas

# IDENTIFICATION DES COMPOSANTS

## ACTIFS PRIMORDIAUX

- ▶ données
- ▶ processus métiers (services propres à l'entreprise)

## ÉLÉMENTS SUPPORTS

- ▶ applications (mail, serveur SMB/NFS)
- ▶ système(s) d'exploitation

## ÉQUIPEMENTS

- ▶ biens propres : commutateur, routeur, serveurs, ordinateurs de l'entreprise
- ▶ biens des usagers : tablettes, smartphones

# INVENTAIRE DES DONNÉES

## IDENTIFICATION DES DONNÉES SENSIBLES

- ▶ pour la sécurité : mots de passe, badge, ...
- ▶ pour l'entreprise : plans marketing, stratégie industrielle, fichiers clients, contrats, ...

## PROCESSUS MÉTIERS

- ▶ il est important que certaines procédures restent secrètes
- ▶ dans l'informatique, l'architecture d'une application peut être le cœur d'une entreprise

# INVENTAIRE DES BIENS

## QUELQUES OUTILS

- ▶ Identification des ordinateurs connectés au réseau : ServiceNow, HP OpenView, arp-scan, nmap
- ▶ Liste des programmes sur les ordinateurs : AIDA64 (Windows, MacOS, iOS, Android), dpkg, find (Ubuntu, Linux)

## PROBLÈME PRATIQUE

- ▶ idéal : l'administrateur décide des machines et logiciels installés sur le réseau
- ▶ pratique : les utilisateurs installent des logiciels
- ▶ résolution : focus sur les parties maîtrisées, et séparation dans le réseau basée sur les parties non-maîtrisées

# PLAN

## INVENTAIRE ET SÉCURISATION DU RÉSEAU

### SÉCURISATION DES POSTES

# MAÎTRISE DU RÉSEAU

## ZONES INDÉPENDANTES

- ▶ zone : partie du réseau sécurisée par un pare-feu (entrant et sortant)
- ▶ séparation suivant des considérations diverses :
  - ▶ menace : public, visiteurs physiques, type d'emploi
  - ▶ biens à protéger : réseau par projet ou type de données (comptes de l'entreprise vs recherche)
  - ▶ importance du bien : **administration système et sécurité seulement à partir de certains ordinateurs**

## AUTHENTIFICATION DIVERSE

- ▶ méthode(s) d'authentification varient suivant la zone
- ▶ authentification à distance (Radius, Kerberos) par des serveurs protégés

### DÉFINITION

- ▶ le fait, par les utilisateurs, d'apporter leurs ordinateurs au bureau
- ▶ pratique interdite il y a quelques années pour raisons de sécurité
- ▶ smartphone, tablettes, etc : il faut s'en accomoder

### EN PRATIQUE

- ▶ standard : séparation dans une zone spécifique (e.g., eduroam)
- ▶ sécurité haute : besoin d'authentification cryptographique du matériel connecté dans les zones sécurisées (MAC insuffisant)
- ▶ vérification des logiciels installés possible mais lourde (droits administrateurs sur machines privée)



# CONTRÔLE DES ÉCHANGES ENTRE ZONES

## WHITE/BLACK LISTING

- ▶ white listing : n'autoriser que les (flux d'information) recensés et autorisés
- ▶ black listing : n'interdire que les (flux d'information) recensés et interdits
- ▶ white listing plus exigeant, mais apporte un meilleur niveau de sécurité

## INVENTAIRE DES FLUX

- ▶ lister les connexions utilisées entre les différents zones (nmap, inventaire des processus métier, sondages des personnes)
- ▶ pare-feux rejetant tous les flux sauf ceux autorisés

## CONTOURNEMENT

- ▶ un des motifs d'introduction des applications Web : passer par le port 80/443 qui est en général ouvert
- ▶ déplacement d'un ordinateur d'une zone vers une autre

# CAS PARTICULIER : INTERNET

## ZONE DÉMILITARISÉE (DMZ)

- ▶ intégrité moyenne, confidentialité basse
- ▶ zone à l'intérieur de laquelle on contrôle tous les accès
- ▶ filtrage des paquets provenant d'Internet plus contrôlé
- ▶ limite sévère des connexions entrantes : quelques ports utilisés
- ▶ mise place de **systèmes de détection d'intrusion** (IDS) et de **systèmes de protection contre les intrusions** (IPS)

## CONTRÔLE DES FLUX VENANT DU SI

- ▶ nécessaire de limiter les fuites d'information (fichier mis en téléchargement)
- ▶ nécessaire de protéger aussi l'intégrité de la DMZ (mise en ligne de programmes pouvant servir de relais vers d'autres parties du SI)

# ACCÈS À DISTANCE

## CAS D'UTILISATION

- ▶ remontées en temps-réel du terrain
- ▶ télétravail
- ▶ administration à distance

## RECOMMANDATIONS

- ▶ serveurs d'authentification (Kerberos, Radius)
- ▶ concentrateur VPN (remplacement IP par IPSec),ssh (au-dessus de TCP)
- ▶ serveur application dédié (Remote Access Server) au transfert authentifié des données
- ▶ dans tous les cas, le matériel utilisé par le client **doit** être fourni et géré par l'entreprise (pas de BYOD)

# MAIL

## POP, SMTP, IMAP

- ▶ pop, imap : protocole de synchronisation de boîtes mail
- ▶ pop marche par copies locales, imap par accès à distance à une unique boîte mail
- ▶ smtp : protocole d'envoi de mails

## AUTHENTIFICATION (POP,IMAP)

- ▶ ssh + mot de passe pour l'authentification du client (et accès à distance)
- ▶ BYOD : les mots de passe des utilisateurs se retrouvent un peu partout (Google, Outlook, mais aussi des applications “sympas”)

## AUTHENTIFICATION PAR EXTERNE (SMTP)

- ▶ pour l'utilisation d'un mot de passe, il faut accepter un niveau de protection plus faible par Google (car ils n'ont pas confiance en votre entreprise)
- ▶ alternative : enregistrer une clef publique d'authentification auprès de Google

# PLAN

INVENTAIRE ET SÉCURISATION DU RÉSEAU

SÉCURISATION DES POSTES

# LIMITE (BYOD)

## EXCLUSION DU BYOD

- ▶ impossible en pratique d'empêcher les utilisateurs d'amener leur téléphone portable
- ▶ il convient de fournir un réseau Wifi bien séparé du reste du réseau de l'entreprise (impression, partage de documents)
- ▶ mais le mail permet souvent un échange de documents incontrôlé (hors log)

## SUITE :

- ▶ focus sur les postes gérés par l'administrateur système
- ▶ recensement de bonnes pratiques

# DÉPLOIEMENT DE NOUVEAUX LOGICIELS

## PAR LES UTILISATEURS LAMBDA

- ▶ installer un logiciel, c'est donner les pleins pouvoirs (exception : android) à l'auteur sur son ordinateur
- ▶ extrêmement important de vérifier l'auteur (automatique sous Windows et apt/rpm) du logiciel
- ▶ il faut faire confiance aux procédures des fournisseurs (signature MS, Google Play, iTunes) pour vérifier que les logiciels distribués ne contiennent pas de virus
- ▶ note : faire un scan de son ordinateur à partir d'une page web fait courir les mêmes risques

Distribuer des logiciels gratuitement est une des principales méthodes pour infecter des ordinateurs

## FONCTIONNEMENT

- ▶ lit un exécutable pour retrouver des schémas d'appels de fonction ou de boucles, tests utilisés par des virus connus
- ▶ base virale : liste des virus à tester, toujours incomplète :
  - ▶ des virus sont enlevés lorsqu'ils ne sont plus utilisés
  - ▶ des virus pas encore découverts ne sont pas testés

## VIRUS MODERNES

- ▶ lors de la compilation, plein de variantes trompant les algorithmes de détection
- ▶ les anti-virus risquent de devenir complètement inefficaces
- ▶ il leur est aussi possible de passer à travers beaucoup de pare-feux



## FAILLES 0-DAY

- ▶ failles qui sont exploitées avant d'être découvertes officiellement
- ▶ Computer Emergency Response Teams : dès qu'une telle faille est découverte, patch fourni le plus vite possible (avec explication sommaire du problème)

## CONSÉQUENCE

- ▶ dès qu'un patch est disponible, toutes les menaces possibles sont au courant de la vulnérabilité
- ▶ si cette vulnérabilité affecte une partie du SI, il faut donc faire le plus rapidement possible une mise à jour pour la supprimer

# MISES À JOUR AUTOMATIQUES

## AVANTAGES

- ▶ permet d'assurer que les mises à jour les plus récentes sont installées dès que possible
- ▶ simplifie l'administration

## INCONVÉNIENTS

- ▶ le fonctionnement du SI est de la responsabilité de l'administrateur
- ▶ plus sûr pour le fonctionnement : MàJ sur machine test, vérification des fonctionnalités, sauvegarde de chaque machine en production avant MàJ

# MISES À JOUR EN PRATIQUE

## PATCH TUESDAY (EN COURS D'ABANDON ?)

- ▶ politique de Microsoft : déployer les patches de sécurité à travers Windows Server Update Service (maintenant Windows Update for Business) à une date fixe
- ▶ le second mardi du mois
- ▶ problème possible : faille révélée le lendemain

## LIMITES DU PATCH IMMÉDIAT

- ▶ test + observation + deploy : peut être très long
- ▶ dans la plupart des entreprises, il faut compter plus de 90 jours avant l'application d'un patch

# PROTECTIONS POSSIBLES

## INTÉGRITÉ

- ▶ faire des sauvegardes régulières
- ▶ limiter les accès des utilisateurs (pour que les logiciels qu'ils installent n'aient pas de droit sur la configuration de sécurité)

## CONFIDENTIALITÉ

- ▶ chiffrement des données (sur SI et dans les mails)
- ▶ canaux de communication hors SI pour les mots de passe et clefs
- ▶ utilisation de logiciels spécialisés pour le stockage dans le Cloud (délégation de la sécurité au serveur)