CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS

Système & Matériel

Loïc Rouquette

Licence

Connaître le *Système d'Information* (S.I.)

Identifier les composants du S.I.

Au-delà de la connaissance des composants du S.I., l'inventaire permettra par la suite de mieux déterminer les menaces et les mesures de protection applicables.

Tout projet sécurité doit donc forcément intégrer un inventaire des biens.

L'inventaire des biens doit suivre une méthodologie logique afin d'être exhaustif, en commençant par l'inventaire des métiers.

Identifier les composants du S.I.

Différents éléments du S.I.

Identifier les composants du S.I.

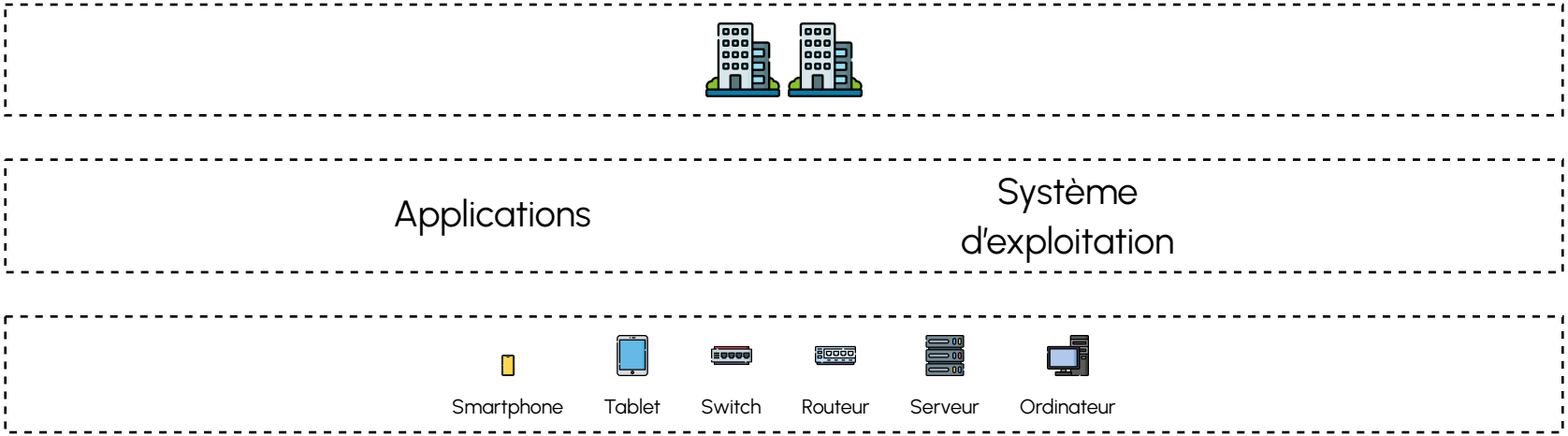
Différents éléments du S.I.

Applications

Système d'exploitation

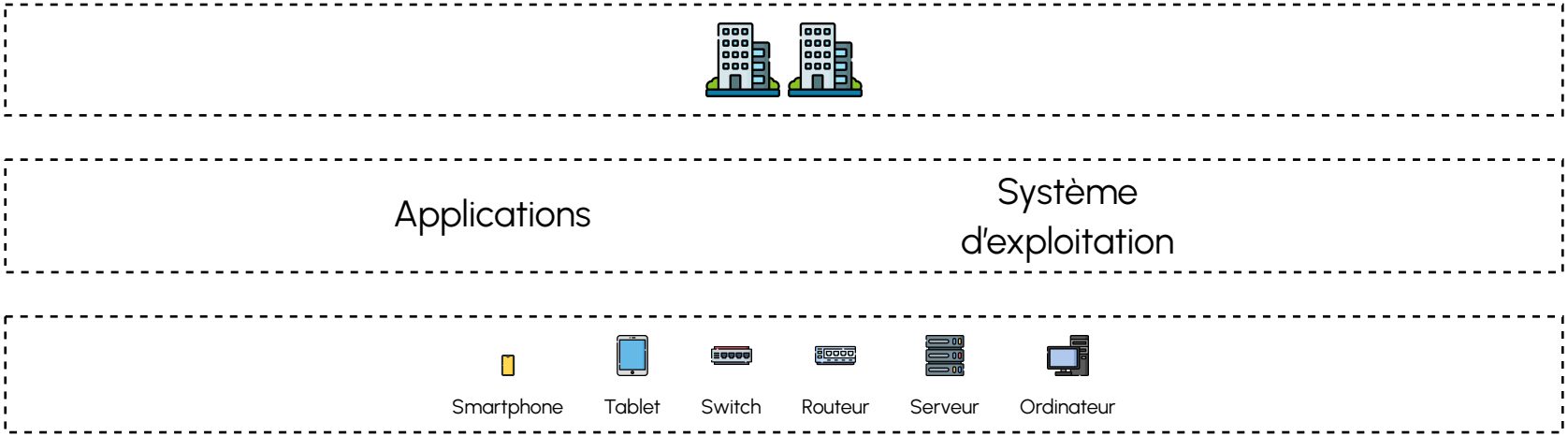
Identifier les composants du S.I.

Différents éléments du S.I.



Identifier les composants du S.I.

Différents éléments du S.I.



Comprendre son S.I. passe par l'identification de ses composants.

Inventorier les biens

Identifier

- Les données sensibles :
  - mots de passe, cartes de crédit, documents personnels, etc.
  - plan marketing, fichier client, brevets, contrats, etc.
- Les applications avec leur version
  - Office2010, Navigateur Web, etc.
- Les systèmes d'exploitation
- Les équipements
  - Ordinateur, tablette, téléphone, serveur, etc.

Inventorier

- Outil d'identification des ordinateurs en réseau
  - ServiceNow, HP OpenView
- Outil d'identification des logiciels installés sur un ordinateur/téléphone ainsi que les versions
  - Everest

Types de réseaux

- *Body Area Network* (BAN) : réseau composé de télé transmetteur utilisé dans le domaine de la santé ;
- *Personal Area Network* (PAN) : réseau centré autour d'une personne interconnectant ordinateur, téléphone, tablette, voiture... (moins de 10m) ;
- *Wireless PAN* (WPAN) : réseau PAN sans fil utilisant des technologies telles que : IrDA, ZigBee, Bluetooth, Wireless USB ;
- *Local Area Network* (LAN) : Réseau local interconnectant plusieurs périphériques et permettant l'échange d'informations entre plusieurs individus ;

Types de réseaux

- *Metropolitan Area Network* (MAN) : réseau plus large qu'un LAN et étendu par exemple sur une ville ;
- *Campus Area Network* (CAN) : réseau s'étendant sur plusieurs LAN, et de la taille d'une université ;
- *Wide Area Network* (WAN) : réseau d'une étendue nationale ou internationale. Exemple : Internet.

Interconnexion

Connaître et maîtriser les points d'interconnexion

- Accès internet via:
  - Box internet
  - Téléphone
- Interconnextion avec d'autres réseaux (universités, partenaires, prestataires, etc.)
  - Liaison dédiée : E1/T1 carrier, fibre noire ;
  - *Virtual Private Network* (VPN) ;
  - Liaison satellite.

Maîtriser le réseau

Sécuriser le réseau interne

Créer des zones dans le réseau interne

- Zone distinctes pour les serveurs, postes de travail, visiteurs ;
- Assurer la confiance par l'authentification mutuelle des composants ;
- Assurer le cloisonnement au moyen de VLAN, VRF, sous-réseaux et ne pas oublier d'implémenter un mécanisme de filtrage.

Restreindre l'accès aux réseaux internes

- 802.1X permet de contrôler l'accès réseau et d'assurer que l'autorisation n'est accordée qu'après authentification de l'utilisateur ;
- recourir à l'authentification avant d'autoriser l'accès au réseau :
  - l'authentification peut se faire par l'usage d'un certificat ou d'une carte à puce
  - l'authentification est centralisée sur un serveur qui donne les accès en fonction de l'identité de l'utilisateur

Bring Your Own Device

- Le réseau permet de partager des informations mais aussi de propager les infections de codes malveillants.
- Les terminaux personnels n'ont pas le même niveau de sécurité que les terminaux de l'entreprise / université :
  - Sur un terminal personnel, un utilisateur installe les logiciels de son choix, avec la configuration de son choix. L'antivirus n'est pas forcément à jour ;
  - Sur un terminal professionnel, les logiciels sont installés de manière centralisée, et les sources vérifiées.
- Les terminaux personnels sont connus pour être une source de fuite de données sensibles pour l'entreprise (de façon volontaire ou par erreur).

Bring Your Own Device

- Le réseau permet de partager des informations mais aussi de propager les infections de codes malveillants.
- Les terminaux personnels n'ont pas le même niveau de sécurité que les terminaux de l'entreprise / université :
  - Sur un terminal personnel, un utilisateur installe les logiciels de son choix, avec la configuration de son choix. L'antivirus n'est pas forcément à jour ;
  - Sur un terminal professionnel, les logiciels sont installés de manière centralisée, et les sources vérifiées.
- Les terminaux personnels sont connus pour être une source de fuite de données sensibles pour l'entreprise (de façon volontaire ou par erreur).

Le S.I. est un tout, un maillon faible affaiblit l'ensemble.

Contrôler les échanges internes

- Filtrer les flux pouvant être échangés entre les zones :
  - identifier les ports réseau utiles ;
  - identifier les protocoles réseau autorisés ;
  - disposer d'une matrice de flux indiquant les flux autorisés et interdits entre les zones.
- Autoriser explicitement des adresses IP (machines) d'une zone à échanger avec les adresses IP (machines) d'une autre zone
  - Utiliser une « liste blanche » d'adresse IP pour les échanges, et non pas une liste noire. Une liste noire ne peut en effet jamais être exhaustive, et est forcément d'un intérêt limité.

Appliquer le principe « Tout ce qui n'est explicitement autorisé est interdit » lors de la gestion des flux.

Protéger le réseau interne d'internet

- Le réseau internet est à protéger et est considéré comme « de confiance » ;
- Les équipements intéragissant avec Internet peuvent être :
  - placé dans une zone spéciale appelée « *Zone Démilitarisée* (DMZ) » ;
  - protégés d'Internet par des « pare-feux » filtrant les échanges de flux ;
- protégés derrière des *Intrusion Detection System* (IDS) et des *Intrusion Prevention System* (IPS).

Accès distant

Il est possible d'accéder à distance à un réseau pour faire :

- du télétravail ;
- de la téléassistance ;
- de la téléadministration.

Il est recommandé d'avoir des points d'entrée identifiés pour les accès distants :

- Serveur d'authentification : TACACS+, RADIUS ;
- Concentrateurs VPN ;
- *Remote Access Server* (RAS)

Accès distant

Utiliser des moyens sécurisés pour les accès distants :

- SSH (au lieu de telnet) pour l'établissement de connexion à distance sur un équipement ;
- Secure Remote Desktop : pour la prise en main à distance d'un bureau ;
- SFTP ou SCP : pour la copie à distance ;
- HTTPS : pour l'accès à une interface web ;
- *Virtual Private Network* (VPN) établit sur un réseau qu'on ne maîtrise pas (tel que internet) :
  - VPN IPSEC : permet l'authentification et le chiffrement ;
  - VPN SSL : protège essentiellement le trafic Web.

Sécuriser l'administration

Restreindre / Interdire les interfaces d'administration depuis Internet

- L'administration d'un composant ne doit pouvoir se faire que depuis le réseau interne (VPN si nécessaire).

Restreindre les accès aux interfaces d'administration sur les sites Web

- Notemment pour les applciations Web crées avec des *Content Management System* (CMS)
  - Le lien de page peut facilement être trouvé ;
  - Des attaques « brute force » peuvent fonctionner ;
  - Modifier le compte « admin » par défaut.

Utiliser un réseau d'administration dédié :

- Ce réseau doit être séparé du réseau de production de manière à ce que seul les postes autorisés puissent s'y connecter ;
- Avoir une liste blanche des administrateurs autorisés à se connecter à ce réseau ;
- Authentifier mutuellement les postes des administrateurs et les équipements à administrer.

Wifi

Pour sécuriser son réseau Wifi, il faut:

- Protéger la confidentialité des communications en effectuant un chiffrement à l'aide d'une clé ;
- Choisir la technologie WPA2 ;
- Choisir un algorithme *Counter Cipher Mode Protocol* (CCMP) si possible ;
- Modifier le *Service Set IDentifier* (SSID) ;
- Modifier les identifiants fournis par défaut pour accéder à l'interface d'administration ;
- Ne pas divulger sa clé Wifi.

Wifi : WPS

Ne pas utiliser le WPS.

Wifi : WPS

Ne pas utiliser le WPS.

Vulnérable à une attaque brute force sur le code PIN.

Wifi : privé vs public

Privé

peut être utilisé dans le réseau interne pour l'accès à des personnes de confiance. Dans un LAN on peut utiliser le Wifi comme moyen d'interconnexion. On parle alors de *Wireless Local Area Network* (WLAN).

- Possibilité de faire des connexions par certificats pour éviter de partager le mot de passe.

Public (hotspots)

fourni aux personnes de « non confiance » ou au grand public (généralement fourni pour un accès internet uniquement).

Être conscient que tous les utilisateurs connectés sur le même hotspot peuvent écouter toutes les conversations.

L.R.

Wifi : bonnes pratiques sur Wifi public

Désactiver les options de partage ;

- arrêter la découverte réseau ;
- arrêter le partage de fichier et d'imprimantes.

Activer le pare-feu ;

Utiliser un VPN si possible.

Sécuriser les terminaux

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connait pas forcement l'auteur ou le site hébergeant le logiciel ;

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connait pas forcement l'auteur ou le site hébergeant le logiciel ;
- Certaines personnes sont spécialisées dans la fourniture de chevaux de Troie.

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connait pas forcement l'auteur ou le site hébergeant le logiciel ;
- Certaines personnes sont spécialisées dans la fourniture de chevaux de Troie.

Préférer les sources sûres

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connait pas forcement l'auteur ou le site hébergeant le logiciel ;
- Certaines personnes sont spécialisées dans la fourniture de chevaux de Troie.

Préférer les sources sûres

- Utiliser les sources « de confiance » pour télécharger les logiciels
  - sites d'éditeur
  - paquets officiellement supportés

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connait pas forcement l'auteur ou le site hébergeant le logiciel ;
- Certaines personnes sont spécialisées dans la fourniture de chevaux de Troie.

Préférer les sources sûres

- Utiliser les sources « de confiance » pour télécharger les logiciels
  - sites d'éditeur
  - paquets officiellement supportés

Vérifier la signature si possible

Choisir les applications

Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?

- On ne connait pas forcement l'auteur ou le site hébergeant le logiciel ;
- Certaines personnes sont spécialisées dans la fourniture de chevaux de Troie.

Préférer les sources sûres

- Utiliser les sources « de confiance » pour télécharger les logiciels
  - sites d'éditeur
  - paquets officiellement supportés

Vérifier la signature si possible

- Calculer la signature du fichier téléchargé et comparer avec le site si possible.

Choisir les applications

« Crack » logiciels ?

- les sites proposant des « cracks » ou des logiciels gratuits sont souvent truffés de codes malveillants ;
- les versions « crackées » de logiciels contiennent souvent des codes malveillants.

Choisir les applications

« Crack » logiciels ?

- les sites proposant des « cracks » ou des logiciels gratuits sont souvent truffés de codes malveillants ;
- les versions « crackées » de logiciels contiennent souvent des codes malveillants.

Logiciels gratuits ?

- Certains logiciels gratuit comportent des malwares qui sont installés en même temps que le logiciel.

Mises à jour logicielles et systèmes

Rôle

Apporter des corrections à un(e) logiciel / application afin de corriger un dysfonctionnement ou une vulnérabilité.

En entreprise, les mises à jour s'*effectuent* de manière centralisée.

- Téléchargement sur des serveurs dédiés ;
- Déploiement et observation sur des machines de test ;
- Sauvegarde des machines de production ;
- Déploiement sur les machines de production.

Mises à jour logicielles et systèmes

Les mises à jour ne concernent pas que le système d'exploitation : tous les logiciels peuvent présenter des failles et doivent être mis à jour régulièrement également ;

- Flash, Shockwave, Javascript, les lecteurs PDF sont connus pour nécessiter des mises à jour régulières ;
- La plupart des logiciels ont une option qui permet une « mise à jour automatique », il est recommandé de l'activer.

En entreprise, c'est à l'administrateur de planifier et valider les mises à jour (cela inclut notamment des tests préalables de non régression).

Antivirus, Antimalware & Antispyware

Ils doivent être configuré de manière à :

- Télécharger automatiquement les nouvelles signatures (base antivirale) ;
- Être toujours actif (faire attention si votre antivirus est désactivé) ;
- Scanner tout l'ordinateur sans exception de répertoires / fichiers ;
- Effectuer des analyses complètes de manière périodique ;
- Analyser automatiquement de nouveaux périphériques tel que les clés USB ;
- Analyser les emails (entrants et sortants) et la messagerie instantanée.

Limites

- Les antivirus ne détectent que les virus dont les signatures sont « connues » ;
- De très nombreux codes malveillants sont créés chaque jour.

Symptômes de présence des codes malicieux

Ralentissement

- du terminal : exemple pendant l'arrêt et le redémarrage ;
- du débit : la bande passante semble partagée.

Ouvertures régulières de fenêtre de pop-up et publicités

Modification de la configuration du navigateur

Surconsommation des ressources

- réduction de l'espace disque
- surcharge du processeur

Symptômes de présence des codes malicieux

Désactivation des protections

- modification des configurations du pare-feu
- désactivation de l'anti-virus
- échec des mises à jour

Messagerie

- présence ou envoie de mails inconnus

Protéger les données

Lors des échanges par mail

- Chiffrer les pièces joints ou les données sensibles.
- Envoyer le mot de passe par un autre canal si possible (SMS)

Lors de l'usage du cloud

- Utiliser des logiciels spécialisés pour protéger/chiffrer vos données (DropBox, Box, SkyDrive, etc.)

En effectuant des sauvegardes

- Sur disque externe
- Dans le cloud

Protéger les données

Lors des échanges par mail

- Chiffrer les pièces joints ou les données sensibles.
- Envoyer le mot de passe par un autre canal si possible (SMS)

L

Chiffrer vos données sensibles avant de les stocker.

- Box, SkyDrive, etc.)

En effectuant des sauvegardes

- Sur disque externe
- Dans le cloud

Durcissement de configuration des équipements

Modifier les mots de passe des comptes par défaut ;

- admin/admin

Désinstaller les logiciels/services inutiles ;

Désactiver les ports/lecteurs non utilisés ;

- port série / port USB ;
- lecteur de disquette ;
- désactiver le « débogage USB » sur les téléphones.

Mettre un mot de passe BIOS lors de la phase de démarrage ;

Désactiver le boot sur des périphériques externes ;

Activer la journalisation.

Gérer les utilisateurs

Attribution de privilèges

Politique des « moindre privilèges » : n'attribuer aux utilisateurs que les droits dont ils ont besoin pour effectuer leurs tâches ;

- ne pas donner de droit important à tous les utilisateurs, mais uniquement à ceux qui en ont besoin ;
- pour les visiteurs, ne pas donner l'accès qu'à internet.

« Besoin d'en connaitre » : donner l'accès et les privilèges appropriés aux utilisateurs :

- donner accès seulement aux données nécessaires aux utilisateurs ;
- restreindre l'accès aux répertoires contenant les données sensibles.

Attribution de privilèges : recommandations

Attribuer les comptes aux utilisateurs de manière nominative ;

- Un utilisateur = un compte ;
- Tracer les actions effectuées par chaque utilisateur ;
- Éviter les comptes partagés entre plusieurs utilisateurs.

Attribution de privilèges : la charte S.I.

Faire signer une charte d'utilisation du S.I., informant sur :

- La conduite à tenir lors de l'usage du S.I. ;
  - Actions encouragées :
    - Utiliser son poste pour des recherches, pour le travail qui est confié ;
    - protéger ses moyens d'accès : badge, identifiant, etc.
  - Actions interdites :
    - Installer des logiciels malveillants / arrêter les outils de détection de codes malveillants ;
    - Porter atteinte à un autre utilisateur du S.I..
- Les conditions et les règles d'utilisation des ressources du S.I. ;
- Les responsabilités de l'utilisateur et ceux de l'entreprise/université ;
- Les sanctions internes, pénales, civiles encourues ;

Sous Windows, la commande `GPEDIT.msc` permet de configurer de manière fine les droits des utilisateurs.

Attribution de privilèges : attribution / retrait de privilèges

Définir une procédure d'attribution/retrait de privilèges.

- Tenir à jour une liste des droits attribués à chaque utilisateur ;
- Chaque nouveau compte utilisateur doit être créé en respectant les principes d'attribution de privilège ;
- Au besoin, chaque utilisateur doit avoir son répertoire personnel et sa boite aux lettres ;
- Lorsque qu'un utilisateur n'a plus besoin d'accéder au système (démission, changement de poste...), la procédure de retrait de droit doit :
  - Décrire la désactivation de son compte et la suppression de son compte ;
  - Décrire la procédure de retrait des accès aux locaux (badge, clés).

Rôles utilisateur

Administrateur

Privilèges les plus élevés sur le système. Il peut être de plusieurs types :

- Administrateur système : en charge de l'administration des systèmes, de la gestion des disques ;
- Administrateur réseau : en charge des équipements réseaux, des règles de filtrage ;
- Administrateur sécurité : en charge de la journalisation, de la supervision.

Utilisateur

Ayant le droit d'utiliser le système et d'accéder à des répertoires sensibles ;

Invité

Ayant peu de droits, et pas d'accès aux répertoires contenant les informations sensibles.

Mots de passe : politique de mots de passe

Définir une politique de mot de passe qui oblige à:

- Créer un mot de passe complexe
  - Différent d'un mot sorti du dictionnaire ;
  - Différent d'une date de naissance ;
  - Différent d'une partie du nom d'utilisateur, prénom, nom, etc.
- Avoir un mot de passe d'au moins 8 caractères (10 pour les administrateurs)
- Changer réglièrement les mots de passe (tous les 6 mois) ;
- Utiliser un mot de passe pour vérouiller l'écran de veille.

Recommandations : ANSSI

Mots de passe : mémorisation

Ne pas choisir le même mot de passe pour différents comptes.

- Même si ce principe devient difficile à respecter au vu du nombre de mots de passe que les utilisateurs doivent se rappeler ;
- A minima, ne jamais réutiliser son mot de passe de messagerie. Le compte email devient le pivot numérique de chacun.
  - En cas de perte de mot de passe, c'est souvent graĉe à la boite email que l'on est en mesure d'en régénérer un nouveau ;
  - L'email sert aux sites marchands pour nous identifier.

Mots de passe : aide-mémoire

Aide-mémoire pour construire des mots de passes complexes :

- Choisir une pharase comme mot de passe (« passphrase »).

« Je suis étudiant à ÉPITA »

- Ne garder que la première lettre de chaque mot puis un mot complet :

`JséàÉPITA`

- Remplacer les caractères qui ressemblent à des caractères spéciaux ou des chiffres :

`J$é@ÉP1T@`

Mots de passe : aide-mémoire

Le mot de passe est personnel et doit être mémorisé :

- ne pas écrire les mots de pasqse sur des post-it ;
- il existe des solutions pour stocker les mots de passe sous forme sécurisée.

Les outils pour deviner les mots de passes prennent parfois en compte les remplacements par caractères spéciaux.

Mots de passe : stockage des mots de passe

Toujours stocker les mots de passe sous forme chiffrée

- Exemple :

  Thousands Of Leaked Sony Passwords Were Reportedly Kept In A Folder Marked "Password"

Utiliser des « porte-feuilles » de mot de passe :

- Dashlane, KeyPass, 1Password

Ne pas enregistre les mots de passe sur les navigateurs Web.

Autres méthodes d'authentification

Biométrie

- permet l'authentification par la lecture d'attributs physiques, e.g. voix, rétine, emprunte digitale, etc.

Carte à puce & code pin

Single Sign On (SSO)

- Une seule méthode d'authentification pour accéder à différents services.

One Time Password (OTP)

- Générer à la demande et utilisable une seule fois. Sa durée de validité est très courte.

Sécuriser physiquement

Protection physique des locaux

Protéger physiquement les locaux contenant les biens sensibles :

- Contrôler l'accès aux locaux ;
- Utiliser des alarmes pour identifier les intrusions.

Les prises d'accès réseau doivent être protégées

- Elles ne doivent pas être accessibles aux visiteurs ;
- Si elles doivent être exposées, activer uniquement les prises lorsque nécessaire.

Protéger contre les incidents environnementaux :

- Incendies (OVH)
- Inondations
- Pannes életriques

Imprimantes & Photocopies

- Faire attention lors des photocopies à ne pas oublier les originaux ;
- Aller rapidement retirer les documents imprimés pour éviter que des informations sensibles soient révélées ;
- Ne pas oublier que les imprimantes disposent :
  - De disques durs ;
  - D'historique des impressions : dont les titres de documents pourraient être révélateurs ;
  - De configuration IP pouvant être usurpée.
- Les documents papiers sensibles doivent détruits à la déchiqueteuse ;
- Les imprimantes ne doivent être accessibles depuis Internet.

Sécuriser les équipements

- Attacher avec un câble de sécurité les équipements le permettant ;
- Protéger l'accès aux équipements :
  - Avoir un code/mot de passe pour restreindre l'accès à son équipement :
    - lecteur d'empreinte ou signe sur téléphone ;
    - code PIN ou mot de passe ;
  - Demander un code/mot de passe pour sortir de la veille.
- Verrouiller son écran en cas d'inactivité de quelques minutes ;
- Faire attention aux médias USB :
  - Des clés USB piégées sont parfois offertes ou abandonnées ;
  - Toujours scanner (anti-virus) une clé USB avant de l'utiliser.
- Utiliser les filtres de confidentialité d'écran ;
  - Écran d'ordinateur (fixe, portable) ;
  - Écran de téléphone.

Contrôler la sécurité du S.I.

Contrat, Maintenance & Professional Services

- Lors de l'achat de :
  - matériel : souscrire à des contrats de maintenance ou d'assurance pour vous garantir une assistance en cas de difficulté ;
  - application : souscrire à des contrats de support et d'assistance.
    - niveau 1 : description et enregistrement du problème rencontré. Conseil/information basique ;
    - niveau 2 : intervention de technicien ;
    - niveau 3 : intervention d'expert.
- *Service Level Agreement* (SLA) : indique le niveau de service garanti par le prestataire pour une prestation de service donnée.
  - Exemple : couverture 3G ou 4G.

Contrat, Maintenance & Professional Services

Cyber-assurance : est une assurance visant à indemniser et assister les victimes de cyber-attaque (fuite de données, attaque à la e- réputation…) :

- Exemple : AXA propose pour les particuliers « Protection Familiale Intégr@ale »
- Noter que la souscription d'une assurance est considérée comme une mesure de sécurité permettant de réduire les risques portant sur l'entreprise (au même titre qu'une assurance habitation n'empêchera pas un incendie, mais compensera/limitera les pertes financières de la victime).

Surveiller & Superviser

- Activer la journalisation d'évènements ;
  - Enregistrer les tentatives d'accès réussies ou pas ;
  - Enregistrer les tentatives de modifications d'informations sensibles ;
  - Etc.
- Consulter les journaux d'évènements ;
- Définir une politique de supervision :
  - définir les seuils : au-delà de tel taux d'occupation du disque, recevoir une alerte ;
  - définir le type d'alerte souhaité : SMS, mail, etc.

Incidents de sécurité: catégories d'incidents

- Divulgation d'information personnelle ;
  - carte de crédit, vol d'identité, numéro de sécurité sociale, etc.
- Déni de service ;
  - entrant ou sortant.
- Activité causée par un code malveillant ;
  - Vers, virus, keylogger, Rootkit.
- Enquête et activité criminelle ;
  - Vol de terminal, fraude, pornographie infantile.
- Non respect de la politique de sécurité ;
  - partage de mot de passe.
- Défacement Web ;
  - Redirection de site, défacement d'un site internet.
- Vulnérabilité non corrigée.
  - système/application vulnérable, non application d'un correctif important.

Incidents de sécurité: gestion des incidents de sécurité

- Un processus de gestion des incidents de sécurité permet de :
  - Réagir rapidement et de réduire l'impact en cas d'incident ;
  - Améliorer la prévention et la sensibilisation ;
  - Détecter et d'identifier les incidents ;
  - Améliorer le niveau de sécurité.
- Exemple de réaction en cas d'une infection virale :
  - déconnecter le poste du réseau ou d'Internet, sans l'éteindre ;
  - S'assurer que l'antivirus/antimalware est à jour avec les dernières signatures ;
  - Exécuter le scan complet (en « mode sans échec » par exemple) avec un antivirus ;
- Contacter un spécialiste au besoin ;
- Chercher à identifier la cause.

Plan de secours

- Avoir un plan de secours en cas de dysfonctionnement important (électrique, télécom...) :
  - Double alimentation :
    - pour un téléphone : batterie de secours ;
    - ordinateur/serveur : onduleur, batterie de secours, groupe électrogène.
  - Accès Internet :
    - utiliser son téléphone comme modem en cas de dysfonctionnement de sa Box ;
    - en entreprise, souscription à une offre Internet comme ligne de secours fournie par un opérateur différent.
  - Avoir une sauvegarde de ses données en cas de panne de son disque dur.
- En entreprise, il y a des :
  - *Plan de Reprise d'Activité* (PRA) qui permet de « reprendre » après une interruption inattendue comme la perte d'un site de travail ;
    - Exemple : utilisateur d'un site de secours « B » et déplacement du personnel en cas d'incendie dans le site principal « A »
  - *Plan de Continuité d'Activité* (PCA) qui permet de s'assurer que l'activité ne s'arrêtera pas ;
    - Exemple : usage d'une architecture réseau redondée en haute disponibilité.
  - Les PCA et les PRA doivent être testés et mis à jour régulièrement.

Audit : informations générales

- Un audit peut porter sur tout ou partie du S.I., une application, etc.
- Le but de l'audit est généralement :
  - d'évaluer le niveau de sécurité par rapport à un référentiel (interne ou à une norme) ;
  - obtenir un agrément ou une certification : (ASIP Santé, PCI-DSS, 27001, etc.)
  - trouver des faiblesses et les corriger : (site Web, application développée « in-house »)
- L'audit peut être réalisé par :
  - des experts appelés « auditeur sécurité », « pen-testeur »
  - des sociétés spécialisés.

Audit : informations générales

Un cadre légal et contractuel est requis pour les audits :

- Pour les audits de site Web, il faut l'accord du propriétaire du site (par exemple l'association étudiante), de l'hébergeur du site (OVH ou l'université) et parfois celui de l'opérateur ;
- L'auditeur doit indiquer à partir de quelles adresses IP publiques son audit sera effectué ;
- L'auditeur doit s'engager à ne pas provoquer d'incident de sécurité (déni de service par exemple) au cours de son audit.

Audit : types d'audit

- Audit de conformité pour déterminer les écarts par rapport à un référentiel :
  - Politique de sécurité interne ou exigences de sécurité d'un cahier de charge ;
  - Norme internationale : exemple 27001, PCI-DSS, ASIP Santé.
- Audit de certification :
  - Audit physique des datacenters pour obtention d'un agrément SAS 70 ;
  - Audit 27001 en vue de démontrer la bonne application des principes de la norme.

Audit : types d'audit

- Audit Technique :
  - « Boite noire » ou « Pentest » : sans aucun accès, on évalue le système (site web par exemple) du point de vue d'un attaquant quelconque ;
  - « Boite grise » ou « test du stagiaire » : on dispose de quelques informations et on essaye d'élever ses privilèges ;
  - « Boite blanche » pour faire des « audits de configuration » par exemple. On dispose d'accès, y compris administrateur et on évalue le système par rapport à un référentiel ;
  - « Forensic » ou « Post-mortem » : effectuer sur un système après une attaque.