Sécurité informatique

Bruno Martin

Université Côte d'Azur

M1 Informatique

Contenu

Présentation générale

Intervenant : B. Martin

8 séances cours/TD ou TP.
But : comprendre le fonctionnement, les usages d'outils de sécurité pour :

- une machine
- un réseau local
- l'accès à un réseau externe
- la vie privée

Avec les notions pour comprendre les outils :

- introduction à la sécurité
- principes de cryptologie

Vu dans la presse

Vu dans la presse

Selon un rapport gouvernemental britannique, élaboré avec le concours de la société de conseil PricewaterhouseCoopers (PwC) et publié à l'occasion de l'édition européenne du salon spécialisé Infosecurity, les entreprises d'outre-Manche ont – en moyenne – multiplié par trois les sommes consacrées à la sécurité informatique en l'espace de six ans. Une société britannique emploie désormais 7 % de son budget informatique pour la sécurité, contre 2 % en 2002.

De fait, 90 % des entreprises disent effectuer une copie de sauvegarde de leurs systèmes, avoir mis en place des filtres antispam, des pare-feu, des antivirus et des antispywares. 55 % ont une politique de sécurité documentée, contre 27 % en 2002. Et 40 % forment leurs salariés à de bonnes pratiques de sécurité, un chiffre qui a doublé. Résultat : le coût total des failles de sécurité a chuté de 35 %.

Cependant tout est encore loin d'être parfait. Un quart des sociétés britanniques a, malgré tous ces efforts, constaté de sérieuses failles de sécurité au cours des deux dernières années. 21 % d'entre elles consacrent moins de 1 % de leur budget à se protéger du piratage. Et persistent des pratiques informatiques dignes de l'ère pré-Internet. Ainsi, 35 % des entreprises britanniques ne contrôlent pas l'usage de la messagerie instantanée. Et 84 % ne vérifient jamais si les courriels sortants contiennent des informations confidentielles.

Vu au cinéma

Motivation

- Augmentation des échanges sur Internet :
  - d'information
  - commerciaux
- Modification des habitudes de travail :
  - plus de communications
  - plus de mobilité
  - plus de sous-traitants
  - recours aux clouds

Donc moins de contrôle de l'information

Environnement «réseau»

- Hier :
  - centralisé
  - échanges papier
  - pas d'accès distants
- aujourd'hui :
  - distribué, soit sur plusieurs sites, soit localement
  - externalisé (cloud de stockage ou de service)
  - accès distants
  - multiplication du partenariat

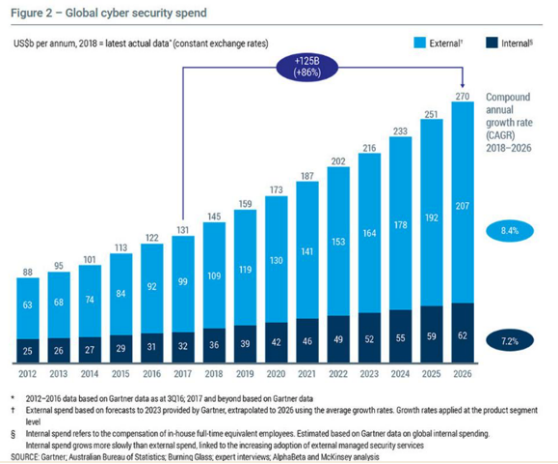
De + en + de dépendance à l'informatique : SI devient l'épine dorsale des entreprises ; 98% des ents. avouent une dépendance modérée ou forte.

Conséquences :

- Augmentation des communications, donc des risques :
  - fraudes diverses
  - piratage

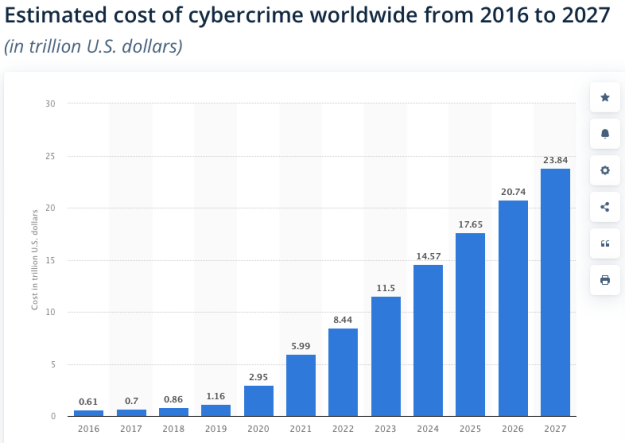
Dépenses cybersécurité

Dépenses cybersécurité :



Quelques autres chiffres : Gartner et McKinsey.

Coût cybercrime



327 milliards d'euros en 2014. 445 milliards de dollars en 2015 (budget de la France 2021 390 milliards €). (2023 trillion : mille milliards)

Quelques chiffres

2 à 10$ prix moyen de la vente de numéros de cartes bancaires selon les payes et les plafonds

5$ tarif de location d'1h de botnet pour saturer un site Internet

2399 $ le tarif du malware *Citadel* permettant d'intercepter des numéros de cartes bancaires (et un abonnement mensuel de 125 $)

Source : Cyberedu

Deux grands types de sécurité

- **Sécurité des données :** celles contenues au sein d'un système ; (traité par la crypto et la théorie des codes)
- **Sécurité des réseaux :** pour les données qui transitent entre des systèmes, dans un environnement distribué ou par un réseau.

On peut y ajouter la sécurité des infrastructures, des applications, des réseaux, du cloud et de l'IoT.

Contenu

Panorama des menaces

Classification par le CLUSIF [http://www.clusif.fr/] basées sur les déclarations de sinistres des entreprises :

- accidents naturels : incendie, dégâts des eaux, etc.
- perte des services essentiels : coupure courant, réseau, rupture de stocks
- erreurs : tous les stades de l'activité : analyse, conception, réalisation, mise en œuvre, utilisation
- malveillance : vol, vandalisme, fuite d'informations

Voir le le rapport des menaces du CERT-FR et sur le rapport d'accenture, les menaces les plus importantes en 2021 sont : *increased ransomware demands, abuse of penetration testing frameworks, commodity malware and Dark Web enablement of newcomer challenges to IT and OT networks.*

Top 5 des menaces en 2020

- DNS hijacking ($\rightarrow$ MiTM)
- Rançongiciels
- Remote Access Trojan
- Office 365 Phishing
- Digital Extorsion Scams

Hi, your account has been infected! Renew the pswd right this moment!
You do not heard about me and you obviously are certainly wondering for what reason you are getting this email, is it right?
I'm ahacker who openedyour emailand devicesnot so long ago.
Don't attempt to contact me or try to find me, it is impossible, since I directed you an email from YOUR own hacked account.
I've created virus to the adult videos (porno) site and guess that you have watched this site to have fun (think you understand what I really mean).
During the time you have been keeping an eye on vids, your browser started out operating like a RDP (Remote Control) with a keylogger which provided me the ability to access your display and webcam.
Consequently, my softobtainedall information.
You wrote passcodes on the web services you visited, I already caught them.
Surely, you could possibly modify each of them, or have already changed them.
However it doesn't matter, my program updates needed data every 5 minutes.
And what did I do?
I generated a backup of every your device. Of all the files and personal contacts.
I formed a dual-screen record. The 1st part displays the film you had been watching (you have got the perfect preferences, huh...), the 2nd screen demonstrates the video from your own web camera.
What do you have to do?
Great, in my opinion, 1000 USD is a fair price for our very little riddle. You'll make the payment by bitcoins (if you do not recognize this, search "how to purchase bitcoin" in Google).
My bitcoin wallet address:

13cas4mnDPoNBDS3YJsthyfpfmEShDxMSD

(It is cAsE sensitive, so copy and paste it).
Attention:
You will have only 48 hours to make the payment. (I have an unique pixel in this e-mail, and at this time I understand that you've read this email).
To tracethe reading of a letterand the actionsin it, I installeda Facebook pixel. Thanks to them.
(Everything thatis usedfor the authorities may also helpus.)
In case I do not get bitcoins, I shall undoubtedly send your video to each of your contacts, along with relatives, co-workers, and so forth?

Tant en interne qu'en externe (voir Cisco Threat Report)

Incidents

58% erreurs de conceptions logicielle ou procédures
47% perte services essentiels (EDF, comms...)
46% erreurs utilisation
44% vols ou disparitions
37% pannes internes (indisponibilité système)
36% infection virale
8% catastrophes naturelles

dans une moindre mesure : divulgation d'informations, attaques logiques, actes d'atteinte à l'image, sabotages, intrusion, fraudes, chantage, intrusion par wifi.
Voir le secure access threat report.

Risque de sécurité

Définition (Risque)

La probabilité qu'une menace donnée tire parti des vulnérabilités d'un actif ou d'un groupe d'actifs et cause dès lors du tort à l'organisation.

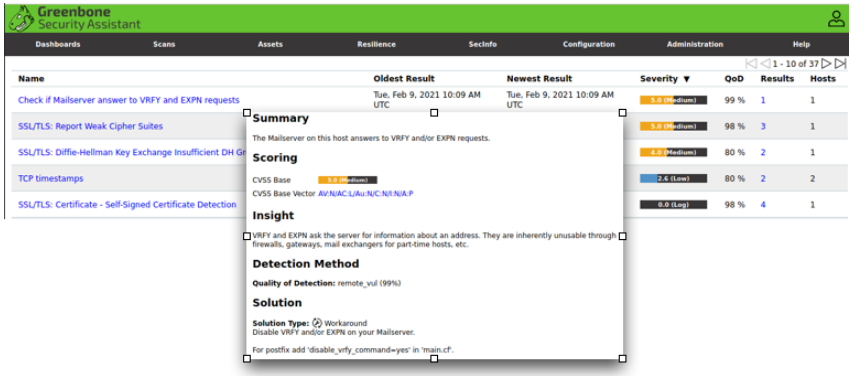
Une équation simple :

$$\text{Risque} = \text{Menace} \times \text{Vulnérablité} \; [\times \text{Coût}]$$

- **Menace** : ce contre quoi on veut se défendre (DoS,...)
- **Vulnérabilité :** faiblesse connue de l'architecture de sécurité (trop de points d'accès, faible authentification,...)
- **Coût :** impact financier

Voir également là.

Test de vulnérabilité



Connaitre les vulnérabilités permet de déterminer la surface d'attaque

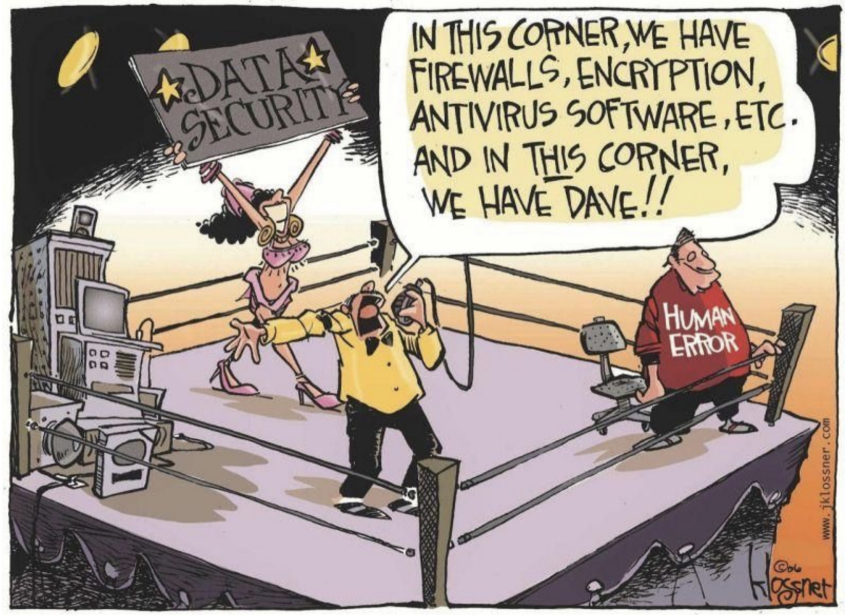
Coût des incidents

CLUSIF-APSAD (France) : statistiques des erreurs sur 16 ans.

	Pertes en M€		
Origine	1984	1994	2000
Facteur humain	309	280	177
Erreurs	269	426	338
Fraude	335	998	???

35% des incidents dus à des fraudes des employés.

IBM (web) : Cybersécurité: 5 chiffres à connaître et voir la sécurité en quelques chiffres



Coût d'une cyberattaque

- 800k€ : coût moyen d'une violation de sécurité
  - 330 k€ pour une entreprise de taille intermédiaire
  - 1,3 M€ pour une grande entreprise
- 9 semaines pour réparer les dégâts
- Préconisation : 5% du budget pour la cybersécurité
- Essayer de chiffrer au mieux l'impact financier de chaque couple (menace, vulnérabilité) –voir plus loin, coût des actifs–

Méthodes d'estimation du risque

qualitative : utilise une échelle d'attributs qualitatifs pour décrire l'amplitude des conséquences et la proba de l'événement. Facile à comprendre mais subjectif sur le choix de l'échelle.

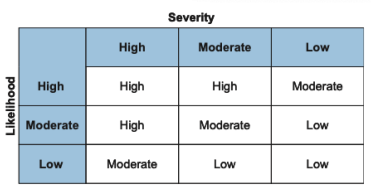
quantitative : utilise une échelle de valeurs numériques. Dépend de l'exactitude des valeurs et des modèles.

Classification des risques

On estime la gravité (ou sévérité) sur une échelle de 3 ou de 5 :

1. **Nul :** risque jugé non significatif
2. **Faible :** événement génèrant une nuisance organisationnelle, des pertes financières faibles, peu gênant pour l'utilisateur
3. **Sensible :** événement occasionnant des pertes financières significatives, nuisible à l'image, gênante pour l'utilisateur
4. **Critique :** événement occasionnant des pertes financières innacceptables, une perte de clientèle
5. **Stratégique :** événement susceptible d'entraîner un arrêt immédiat d'une activité de l'entreprise

Matrice des risques



Likelihood \ Severity	High	Moderate	Low
High	High	High	Moderate
Moderate	High	Moderate	Low
Low	Moderate	Low	Low

- **Elevé :** apporter des corrections au plus vite
- **Modéré :** appliquer des mesures dans un délai raisonnable
- **Faible :** accepter le risque ou le réduire

Exemple : phishing

Etude: 14% des cibles donnent leurs identifiants.
probabilité : faible
gravité : élévée
Décision : risque modéré

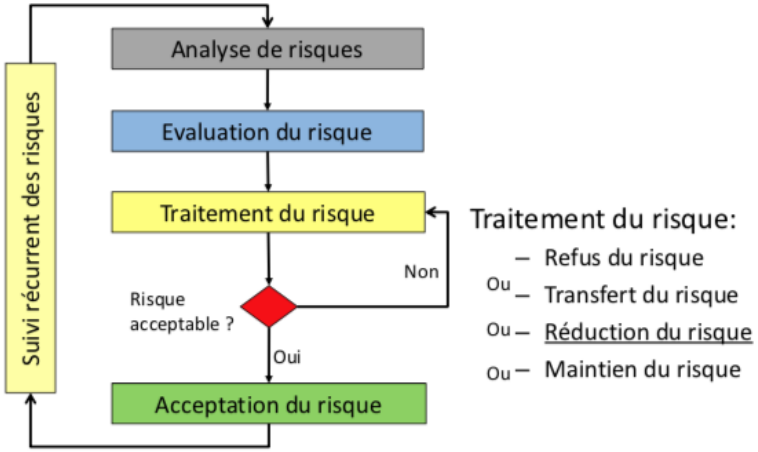
Gestion des risques

Consiste en la réalisation et le maintien à jour :

- de l'**inventaire** des **actifs**
- de l'expression des **besoins de sécurité** de ces actifs
- de l'analyse des risques pesant sur les actifs
- du traitement de ces risques pour les réduire

Des méthodes (MEHARI, EBIOS, OCTAVE) guident la gestion du risque.
Informer et la sensibiliser les personnels (chartes, lettre de sécurité, RSS RSSI...)

Processus de traitement des risques



Actifs/Assets ?

Regroupent les biens et les RH ; 2 types :

- **primordiaux :** processus métiers et informations, gérés par le SI
- **de support :**
  - actifs techniques constituant le SI (logiciels, matériels, moyens de communication)
  - actifs relatifs à l'environnement (personnes et bâtiments)

Actifs généralement inventoriés :

96% actifs physiques (matériel info/comm)
93% logiciels
82% informations
57% services info/comm
41% personnels et leurs compétences
20% valeurs immatérielles (réputation, image)

Coût des actifs

- coût d'achat
- coût de remplacement
- valeur de la propriété intellectuelle
- coût de maintenance
- coût des responsabilités si des données personnelles sont compromises

A noter qu'il existe maintenant des assurances contre les risques de cybersécurité

Types d'attaques

- **passives :**
  - observation non autorisée
  - accès non autorisé à de l'information
- **actives :**
  - contrôle non autorisé d'un système
  - modification de l'information
  - accès à des services
  - *refus de service* aux utilisateurs légaux

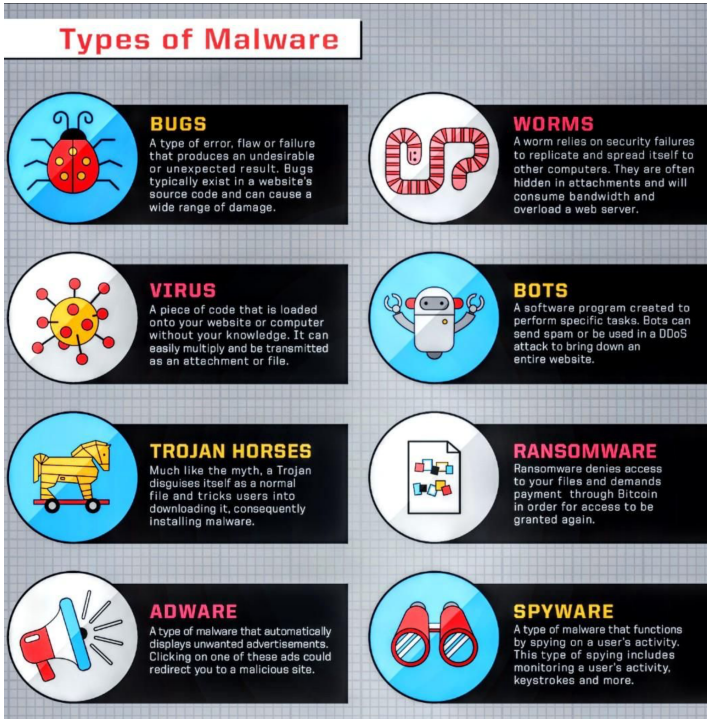
Types d'attaques & menaces

- **l'intrusion :** quelle que soit sa provenance (par le réseau, par un terminal local ou par programme)
- **le refus de service :** DoS. Conséquence des virus ou des attaques du type *ping of death*
- **le vol d'informations :** il n'est pas nécessaire de pénétrer un système pour obtenir de l'information. Une attaque passive peut suffire (exemple du login).
- **rançonnage :** maliciel conçu pour interdire l'accès à un système en attendant le paiement d'une rançon.

Attaques physiques

Nécessitent un accès physique aux installations.

- **interception :** récupération du signal électromagnétique de l'écran de l'ordinateur, des émissions satellites, radio.
- **brouillage :** permet de rendre le système inopérant.
- **écoute :** sur le réseau conduit l'attaquant à analyser les informations qui transitent.
- **balayage :** on envoie au système un ensemble d'informations de nature diverse qui suscitent un retour d'information positif.
- **piégeage :** l'attaquant tentera d'intruire des fonctions cachées, notamment en phase de conception.



Qui écoute ou falsifie ?

- les gouvernements :
  - NSA aux états unis cf. Le Monde et, en plus technique
  - les groupes APT
  - DGSE/DGSI en france
- le crime organisé
- les concurrents
- les pirates (hackers) ; typologie :
  - **hacker “canal historique” :** par prestige, améliorer la qualité des logiciels (espèce en voie de disparition)
  - **hacktiviste :** passer un message politique (anonymous)
  - **cyber-délinquant :** pour gagner de l’argent (espèce en forte croissance, jusqu’aux organisations mafieuses)
  - **cyber terroriste :** pour marquer les esprits et déstabiliser avec des attaques importantes.
  - **cyber-mercenaire :** cf. cyber-terroristes mais agissant seul

(a)

(b)

(c)

Et que fait la police ?

Plusieurs services spécialisés traitent les intrusions en France :

- *Sous direction de lutte contre la cybercriminalité* à compétence nationale
- *service d’enquêtes aux fraudes aux techniques de l’information* sur Paris et la région parisienne
- *brigades spécialisées de gendarmerie*
- DGSI
  - saisie pour les piratages à connotation d’espionnage industriel ou scientifique
  - enquêtes
    - de sécurité, traitement du cadre judiciaire
    - enquêtes informelles à la demande et en collaboration avec les victimes, en dehors du dépot de la plainte
  - objectif : comprendre le plus rapidement possible les causes et l’orientation vers un autre service compétent.

Voir la page actualisée

Contenu

Que veut-on protéger ?

- **les données :** informations conservées dans un système
- **les ressources :** systèmes (généralement les ordinateurs)
- **la réputation de votre site**

Caractéristiques essentielles de la protection des données :

- **Confidentialité :** l'information doit rester secrète
- **Intégrité :** l'information ne doit être ni altérée ni détruite par un utilisateur non autorisé
- **Authentification :** déterminer si un individu ou un système est réellement qui il prétend être.
- **Disponibilité :** l'information doit être disponible aux utilisateurs autorisés.
- **Preuve :** traçabilité de l'information

Protéger

- **Ses ressources**
  Coût des ressources (disque, imprimantes, CPU) à ne pas laisser à disposition d'un intrus.

  On ne souhaite ni réinstaller le système de chaque hôte si les configurations ont été altérées ni laisser à un intrus le loisir de se servir de ses propres ressources comme d'un tremplin pour s'introduire dans un autre système (pivoter).
- **Sa réputation**
  Cas où un indiscret usurpe votre identité et commet des actions illicites en votre nom (problèmes légaux . . .)
  Même sans usurper votre identité, une faille dans votre site conduit à une méfiance envers votre organisme.

Comment protéger ?

- **pas de protection :** ne rien ajouter à l'installation de base
- **sécurité par l'obscurité :** masquer l'existence du système en espérant que le serveur d'une PME ou d'une machine domestique ne présente pas d'intérêt.
- **sécuriser l'hôte :** sécuriser chaque hôte séparément. Cela marche bien pour des machines individuelles mais pas pour un grand nombre de machines du fait de leur diversité. Demande beaucoup de temps par machine.
- **sécuriser le réseau :** contrôler les accès réseau aux différents hôtes et services proposés plutôt que sécuriser hôte par hôte. Cette approche utilise les coupe-feux, l'authentification et le chiffrement des données

Où se porte la protection ?

La sécurité informatique recouvre à la fois :

- **l'aspect physique :** vols inondations incendie, accidents électriques etc. . .
- **l'aspect logique :** intrusions, bombes logiques, virus, sabotage, utilisation frauduleuse des ressources

Il faut éviter tout ce qui nuit à la disponibilité des systèmes et aux services qui y résident.

La sécurité du système est celle de son plus faible maillon

Politique de sécurité

Ensemble de règles qui définissent ce sur quoi porte la sécurité

- définir l'importance de l'information enregistrée, sa protection et l'accessibilité des ressources identifiées.
- une politique de sécurité par organisme
- elle peut couvrir le secret et/ou l'intégrité
- elle est mise en place par une autorité

Politique de sécurité

But : informer les utilisateurs, personnels et responsables des conditions à satisfaire pour protéger les avantages technologiques et en information.

Définit les mécanismes de protection et sert de fil conducteur pour la configuration et l'audit des systèmes d'information.

Elle commence généralement par la phrase :

Tout ce qui n'est pas autorisé est interdit

Pour plus de détails, se reporter à la RFC2196

Politique de sécurité : mise en œuvre

1. identifier les besoins en terme de sécurité, les risques et les conséquences
2. trouver les règles et procédures à mettre en œuvre pour les risques identifiés
3. surveiller et détecter les vulnérabilités du SI et effectuer une veille technique
4. définir les actions à entreprendre et qui contacter en cas de détection d'une menace.

Qui la définit ?

Tous les membres d'une même organisation doivent être d'accord avec la politique de sécurité pour qu'elle devienne effective. Elle est plus spécifiquement définie par

- l'administrateur de sécurité du site (RSSI)
- le personnel technique
- les chefs de service
- le groupe d'audit de sécurité
- des représentants des utilisateurs
- le directeur général
- un conseiller juridique le cas échéant

Politique de sécurité : caractéristiques

1. implémentable par l'administrateur
2. améliorable par des mesures de sécurité et le cas échéant par des sanctions
3. définit les domaines de responsabilité de chacun

Politique de sécurité : contenu

- politique d'achat de matériel de sécurité
- une politique de respect des droits des individus (lecture d'e-mails)
- définir une politique d'accès et de droits sur les données avec des messages d'alerte adéquats
- une politique de gestion des comptes qui définit les responsabilités et les mesures d'audit
- définir une politique d'authentification des utilisateurs
- définir la disponibilité des ressources pour gérer les pannes et les mises à jour logicielles et matérielles
- définir une charte de maintenance du système et des ressources
- tenir à jour un cahier des intrusions et de leur type

Politique de sécurité : flexibilité

Il faut assurer la viabilité de la politique de sécurité. Celle-ci doit être basée sur un concept d'architecture de la sécurité. Elle doit être la plus indépendante possible de matériels et de logiciels spécifiques qui peuvent être facilement remplacés.

Ne pas oublier qu'il y a des exceptions à chaque règle. Il faut essayer de tenir à jour une liste des exceptions de sécurité. P.e. dans quel type de situation un administrateur a le droit d'explorer le contenu d'un compte utilisateur.

Exemple : classification des documents sensibles

- toute information possède un niveau de sécurité
- toute personne dispose d'un niveau d'habilitation
- niveau de sécurité et le niveau d'habilitation consistent en
  - un degré de confidentialité (non-classifié, confidentiel, secret, secret-défense)
  - un ensemble de domaines (chiffre, OTAN, nucléaire,...)
  - des relations d'ordre :
    non-classifié $<$ confidentiel $<$ secret $<$ secret-défense
    ensemble de domaine A **domine** ensemble de domaine B si $B \subset A$.
- la personne X a le droit de lire le document D si
  habilitation(X) $\geq$ confidentialité(D) et
  ensemble de domaine(X)$\supseteq$ ensemble de domaine(D)

Cette politique ne couvre pas l'intégrité de l'information.
Il faut adapter la politique de sécurité.

Exemple « léger »

- Matériel, périphériques et équipements
  - utiliser un onduleur
  - supprimer les données des vieux équipements et contrôler l'infrastructure réseau
  - verrouiller chaque poste de travail
- travail à distance
  - définir le cadre de travail d'un collaborateur extérieur
  - sensibiliser le personnel aux risques de l'utilisation d'un ordinateur portable et du travail à distance
- contrôle de l'accès au SI et à ses contenus
  - avoir une authentification uniforme et centralisée
  - classifier l'information ; l'associer à des profils d'utilisateurs
  - bien définir les rôles des utilisateurs
  - avoir une politique de sélection des mots de passe
  - placer les serveurs et équipements réseau dans des locaux à accès restreint

Exemple « léger »

- traitement de l'information
  - faire installer et gérer le réseau par des personnels qualifiés
  - limiter les actions d'administration à du personnel qualifié
- email et accès Internet/Intranet/Extranet
  - utiliser des détecteurs de virus
  - utiliser des outils de confidentialité
  - mettre en place un firewall
  - traiter avec précaution tout mail non sollicité
  - vérifier `from` et `to` de tout email
  - limiter la taille d'expédition des messages

Modèles de sécurité

Expression formelle (mathématique) de la politique de sécurité
Un modèle de sécurité comprend :

- des variables d'état (p.e. sujets, objets, droits)
- des fonctions de transition

But : prouver que chaque état possible d'un système est cohérent avec un ensemble de propriétés souhaitées

Exemple

Modèles de sécurité pour le secret :

- *modèles de contrôle d'accès de sujets à des objets.*
- *modèles de flux d'information : contrôlent le transfert d'informations*

Très peu de modèles traitent l'intégrité ; aucun la disponibilité.

Principes généraux

- identité : est-ce que chaque utilisateur, programme, objet et ressource peut être identifié de manière unique ?
- responsabilité : les utilisateurs peuvent-ils être tenus responsables de leurs actions ?
- audit : les actions des utilisateurs sont-elles enregistrées ?
- autorisations : gèrer qui a le droit de faire quoi.
- moindre privilège : quel est le minimum nécessaire pour mener à bien le travail demandé ?
- étanchéité : non interférence d'actions différentes
- redondance : gestion des sauvegardes et de la redondance, gestion des pannes

Modèle par matrice d'accès (Bell-Lapaluda)

Modèle de contrôle d'accès

- **objets** : entités passives du système
- **sujets** : entités actives qui peuvent accéder aux objets
- **droits d'accès** : {propriétaire, lire, écrire, exécuter, fusionner}
- **primitives de base** :
  - accorder/refuser un droit
  - créer/supprimer un sujet/objet
- **règles de transition** : si S_i a le droit D_j sur O_k alors primitive$_l$

Généralisation BSD/WIN/OSX

UNIX standard : Bob veut donner à Alice l'accès à UN fichier.
Généraliser méthode user/group/others d'UNIX par ACL ; contrôle + fin des accès aux fichiers.
ACL définit actions d'un **rôle** sur une **ressource**.
Rôle : utilisateur ou groupe
Ressource : fichier ou répertoire
Permissions : action comme lire ou écrire

- sur SGF : delete, readattr, writeattr, readextattr, writeextattr, readsecurity, chown
- sur fichiers : read, write, append, execute
- sur répertoires : list, search, add_file, add_subdirectory, delete_child

```
chmod +a ‘‘alice:allow:read’’ ./ressource.txt
```

un + est ajouté en sortie d'un `ls` et détaillé par un `ls -le`
ACL exécutées avant les permissions UNIX comme suite ordonnée de règles

Contenu

Services et mécanismes

- Politique de sécurité implémentée par les services de sécurité.
  Certains services inutiles pour une politique donnée.
  Exemple : action de communication ne requiert pas l'intégrité.
- Chaque service traite un ensemble particulier de menaces
  Exemple : le service de confidentialité prémunit contre l'accès non-autorisé à l'information.
- Les services de sécurité sont implémentés par les mécanismes de sécurité
  certains services peuvent utiliser le même mécanisme
  Exemple : chiffrement utilisé par confidentialité et authentification.

Services de sécurité

Définis dans la norme ISO 7498-2 comme :

1	authentification d'entités
2	contrôle d'accès
3	confidentialité avec/sans connexion
4	intégrité de connexion avec/sans récupération
5	non répudiation avec preuve d'origine
	non répudiation avec preuve de dépot

Service d'authentification

Vérifier que la partie distante est bien qui elle prétend être

- intégrité de l'information d'identification
- fonctionnalité particulière pour les réseaux.

Service de contrôle d'accès

Empêcher l'utilisation non-autorisée de ressources

- information
- entités (utilisateurs, terminaux, nœuds intermédiaires)
- liens, connexions, routes
- services (réseau ou application)

Dépend fortement de la politique de sécurité.

Service de confidentialité

Empêcher la divulgation non-autorisée

- *de l'information*
- *du trafic*

1. confidentialité orientée connexion : protection des PDU (*Protocol Data Units* ou *paquets*)
2. confidentialité sans connexion : protection des SDU (*Service Data Units* ou *messages*).
3. confidentialité sélective : protection de champs sélectionnés d'un PDU ou d'un SDU.
4. confidentialité d'un flux de données : protéger contre le contrôle du trafic

Service d'intégrité des données

Empêcher la modification accidentelle ou maligne des données

1. intégrité orientée connexion : protection des PDU avec ou sans récupération.
2. integrité sans connexion : protection des SDU.
3. integrité sélective : concerne un ou plusieurs champs choisis.

Observons que l'integrité n'assure pas la confidentialité.

Service de non-répudiation

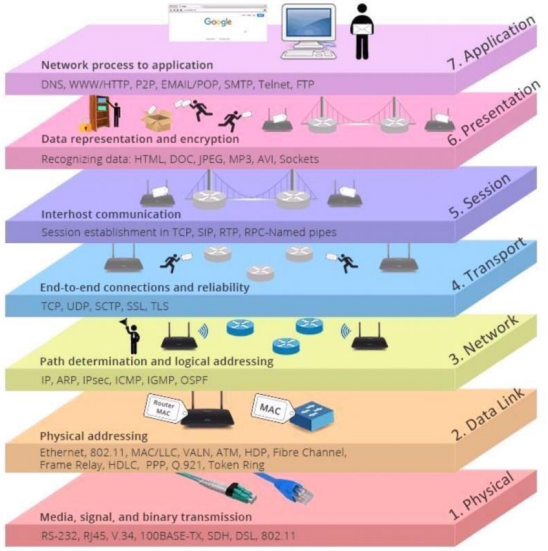
Confirme le fait qu'un sujet a accompli une opération malgré une possibilité de démenti.

1. non-répudiation avec preuve d'origine : fournit la preuve de l'origine au destinataire : empêche l'expéditeur de démentir l'envoi.
2. non-répudiation avec preuve de dépot : fournit la preuve de dépot du message à l'expéditeur : empêche le destinataire de démentir la réception.

Indispensable pour les paiements électroniques EDI, EFT.

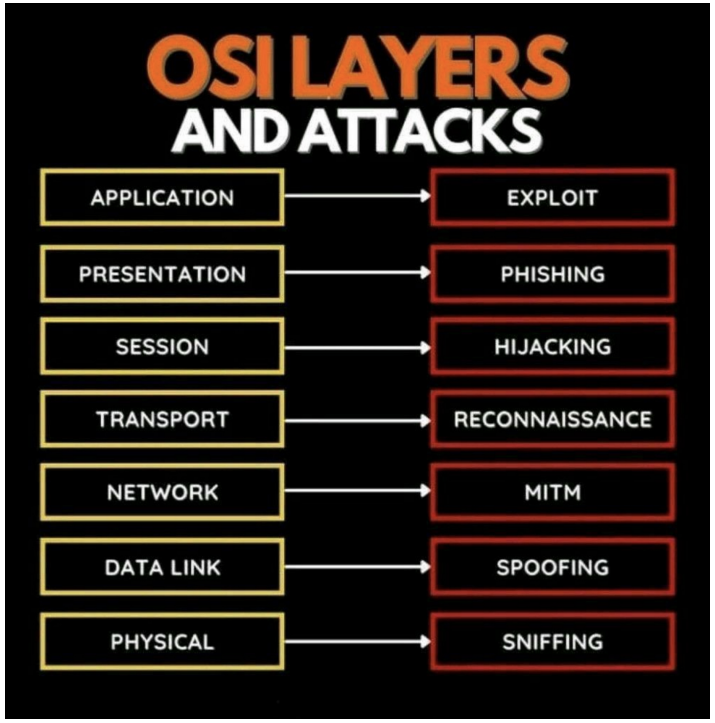
Standard OSI (rappel)

Définit des standards d'échanges de données.



Services de sécurité par couche

	1	2	3	4	5	6	7
Authentification		x	x	x			x
Contrôle d'accès		x	x	x			x
Confidentialité	x	x	x	x		x	x
Confidentialité sélective						x	x
Secret du trafic	x		x				x
Intégrité		x	x	x			x
Non-répudiation							x



Services vs Couches

- Sécurité de la couche application
  - granularité fine (vérification utilisateur et programme)
  - sécurité point à point
  - non-transparent pour les application
- Couche de transport
  - granularité moyenne (utilisateurs finaux non visibles)
  - sécurité point à point
  - transparent pour les application
- Couche réseau
  - granularité grosse
  - pas de sécurité point à point (sécurité hop par hop repose sur les systèmes intermédiaires)
  - transparent pour les application
- Couche physique
  - comme pour la couche réseau, plus de facilité d'intégration
  - fonctionnalité limitée (seulement matérielle)

Mécanismes de sécurité

Implémentent les services de sécurité

- chiffrement
- signatures numériques
- mécanismes de contrôle d'accès
- mécanismes d'integrité des données
- mécanismes d'authentification
- empaquetage pour le trafic
- contrôle de routage
- tiers de confiance (notariat électronique)
- gestionnaire de sécurité (gestion des clés)
- audit
- détection d'intrusion

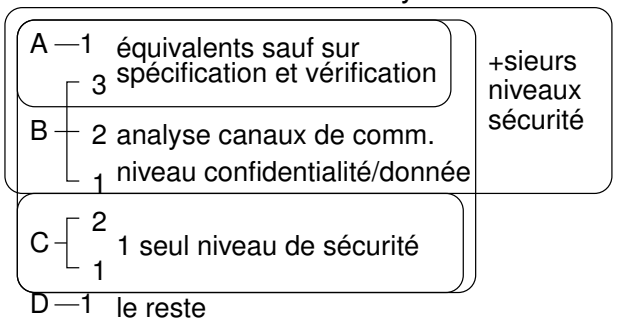
Contenu

Différents critères

- *National Computer Security Center* (NCSC) ; 2 livres :
  - Orange 1985 : Trusted computer system evaluation criteria
  - Rouge 1987 : Trusted network Interpretation of the TCSEC
- *Communauté Européenne*
  - Information Technology System Evaluation, 1991
  - provient de travaux sur les modèles de sécurité
  - important pour le marché gouvernemental et de la défense
- *Bundesamt für Sicherheit in der Informationstechnik*
  - cahier des charges pour la sécurité des coupe-feux
  - centres de certification
- En France, l'ANSSI : héritier du service du chiffre, créé pendant la guerre. Evalue les procédés de chiffrement, les produits et systèmes relevant des technologies de l'information et les procédés de protection contre les signaux électronique compromettants.

Livre Orange

Origine : commande DoD US
Utilité : évaluation de la sécurité des systèmes informatiques.



	Description
A1	fonctionnellement équivalent à B3 mais meilleure analyse de la sécurité
B3	B2+ robustesse aux attaques
B2	B1+ politique de sécurité, gestion niveaux de sécurité, bonne auth.
B1	C2+ gestion niveaux sécurité, classification des données
C2	C1+ amélioration du login, audit, isolement des ressources (mémoire)
C1	protection des données sur le besoin d'en connaitre. Sépare util/données
D	le reste

Livre Orange

Au centre, modèle de sécurité de Bell & Lapadula
Systèmes (matériel et logiciel) doivent satisfaire aux conditions requises en matière de politique de sécurité, gestion des comptes, assurance et documentation

- gestion des comptes : identification, authentification, audit
- assurance que le système vérifie bien ses specs en matière de sécurité avec tests, protection des mécanismes de sécurité et sauvegarde/ restauration des mécanismes de sécurité
- documentation sur les fonctionnalités de sécurité, les tests et la conception

Livre Orange

Propose différents niveaux de sécurité pour les OS selon une sécurité croissante C1-C2-B1-B2-B3-A1
À titre d'exemple :

- A1 : SCOMP Honeywell
- B3 : Multics Honeywell, AIX IBM
- B2 : SunOS, AIX-IBM
- B1 : Solaris CMW, AIX IBM
- C2 : Solaris BSM, Solaris 2.3, IBM, DEC..

Et initiatives type SELinux (security enhanced) fait par NSA qui ajoute des règles de sécurité aux distribs standard.

Standardisation (ISO 27001-2) ?

ISO 17999 en 2000 maintenant 27002 pour la sécurité des SI. Destinée aux dirigeants, aux directeurs de système d'information et aux responsables sécurité (Chief Security Officer, RSSI). Code de bonnes pratiques pour la gestion de la sécurité de l'information.
ISO 27001 : norme de gestion de la sécurité de l'information : Technologies de l'information- techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences.
Tout comme la norme ISO9000 pour la qualité, la norme ISO17999 a pour objectif d'établir un label de confiance reconnu de tous en ce qui concerne la sécurisation de l'information sous un aspect global.

Vers une standardisation

ISO 17999 : importance particulière à des aspects de la sécurité :

- le support des dirigeants quant à la mise en œuvre d'une politique de sécurité et la détermination des moyens humains
- l'identification des menaces propres à l'organisation et l'évaluation des risques associés
- la classification des informations afin de ne déployer les moyens que sur celles qui le nécessitent
- les dispositions prendre pour instaurer une "culture sécurité".

En conjonction avec des guides techniques :

- ISO13335 : concepts et modèles pour la gestion de la sécurité
- ISO14516 : gestion et utilisation des services de certification
- ISO15408 : critères d'évaluation de la sécurité
- ISO18044 : gestion des incidents de sécurité

ISO 27002

Découpée en 15 articles (chapitres) ; 200 CHF ; aux US : NIST handbook : Introduction to computer security

- 4 qui définissent le cadre de la norme
- 11 articles qui proposent 133 mesures définissant les objectifs de sécurité et les mesures à prendre :

- politique de sécurité
- organisation de la SI
- gestion des biens
- sécurité et RH
- gestion télécom
- contrôle accès
- acquisition, dév. maint. SI
- gestion des incidents
- continuité de l'activité
- conformité

ISO 27002 – critères de succès

- pointe et évalue les risques encourus
- mise en œuvre compatible avec culture entreprise
- soutien et engagement visible de la Dir.
- compétence et moyens pour mettre en place une politique de sécurité
- formation appropriée à tous les échelons de l'entreprise
- accès pour tous aux normes et directives de sécurité

Contenu

Data Protection Officer

1. Data protection officer

Previous Next

A data protection officer (DPO) is a relatively new job role that is gaining in popularity following the implementation of the GDPR, the Europe-wide regulation that threatens businesses with tough fines if they fail to meet data compliance and reporting standards.

DPOs are most likely to be responsible for overseeing data protection strategies and ensuring on an ongoing basis that an organisation complies with all GDPR requirements.

According to Article 37 of the GDPR, the role is mandatory for all companies that collect or process EU citizens' personal data, hence the high demand since GDPR came into effect in May 2018.

Some of the responsibilities of a DPO may include training staff involved in data processing, being the point of contact between the company and GDPR supervisory authorities and interfacing with data subjects.

The average annual salary advertised for a DPO in the UK is £55,000.

Chief Security Officer

2. Chief Security Officer

Previous Next

Many CIOs know now that they cannot go at it alone when it comes to security, and so the demand for a chief security officer/chief information security officer (CSO/CISO) is increasing - especially with the explosion in data with IoT and ever-more sophisticated threats from attackers.

A CSO can be responsible for information security, corporate security or both. This may include the physical security of the organisation and its technologies, as well as its IT systems, people and processes.

CSO's are also expected to oversee all standards for hardware and data. They are expected to have knowledge of protecting the internal corporate systems as well as cloud services and managing third parties too.

The average annual salary advertised in the UK is £50,000.

Security Analyst

…l reporting by Hannah Williams.

…well as

…ity analysts

Previous Next

A security analyst will prepare, plan and carry out tests to ensure an organisation's network and system are able to protect itself against malicious attacks.

Security analysts are expected to protect the organisation the best they can either through consulting or carrying out system testing or combing over code.

They will be responsible for a range of activities including keeping up to date with the latest security and technology developments and planning disaster recovery in case of a data breach.

The average annual rate of pay advertised in the UK is £49,000.

Security Consultant

4. Security consultants

Previous Next

Security consultants aim to design security solutions depending on particular business needs.

Security consultants will have to think of every eventuality, ensuring that the best security software is in place.

Under the 'security consultant' umbrella, information security consultant was the most sought after role by UK businesses.

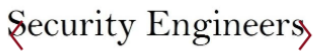
According to figures from Dice job market report 2017, consulting was one of the highest job areas amongst IT professionals with 16 percent working as a consultant.

In addition, there were 90 advertised job openings for network security consultants resulting in a growth of 120 percent over the past five years.

The average annual rate of pay advertised in the UK is £65,000.

Security Engineer

5. Security engineers Previous Next



5/9

Security engineers focus on the design of security systems, ensuring that they are designed to block or react quickly to disruption such as cyber attacks or other malicious activities.

The security engineer title houses numerous job roles, including one of the most sought after by UK employers. Infrastructure engineers have undergone a massive growth period with demand for this role increasing by 617 percent over the past five years.

Network (security) engineers also received a boost in job openings with 590 job listings in each quarter over the last year with demand increasing by 139 percent in five years.

The average annual rate of pay advertised in the UK is £55,000.

See also: **How to get a job as a security engineer.**

Security Manager

6. Security managers Previous Next

6/9

Security managers aim to provide secure procedures, from policy-led best practised to supervising security tests and software installations.

Over the past six years, security management positions have increased by 138 percent, with project management roles within the security management bracket increasing by 231 percent since 2011.

In terms of actual job advertisements, the role of information (security) manager was the most advertised, with 330 job openings during each quarter over the past year.

The average annual rate of pay advertised in the UK is £65,000.

Security Architect

7. Security architects Previous Next

7/9

A security architect is responsible for updating and maintaining an organisation's security programs and/or infrastructure, as well as anticipating potential threats by keeping up to date with current trends.

The role of information security architect has increased by 269 percent over the past five years, with enterprise architect following a similar path with a reported growth of 137 percent since 2011.

The annual rate of pay advertised in the UK is £77,500.

Security Officer and Administrator

8. Security officers and administrators Previous Next

8/9

An entry-level security officer will provide support for the security procedures and software in place and tackle its day to day running.

Over the past year, 150 information security officer jobs were advertised in each quarter.

The average annual rate of pay advertised in the UK is £45,000.

Security Tester and Pentester

9. Security tester and penetration tester

Previous Next

Penetration testers are responsible for locating flaws in code and security software through robust testing, usually mimicking the tools actual hackers would use to breach a perimeter. Exposing these vulnerabilities will help organisation future-proof their businesses and patch up any security holes.

Since 2011, penetration tester job openings have increased 123 percent in five years with the general security tester role has grown by 120 percent since 2011.

The annual rate of pay advertised in the UK is £60,000.