Les concepts de la sécurité informatique

Licence Pro SEICOM – Module 37

Damien VERON

SOMMAIRE

QU’EST-CE QUE LA SÉCURITÉ INFORMATIQUE ?

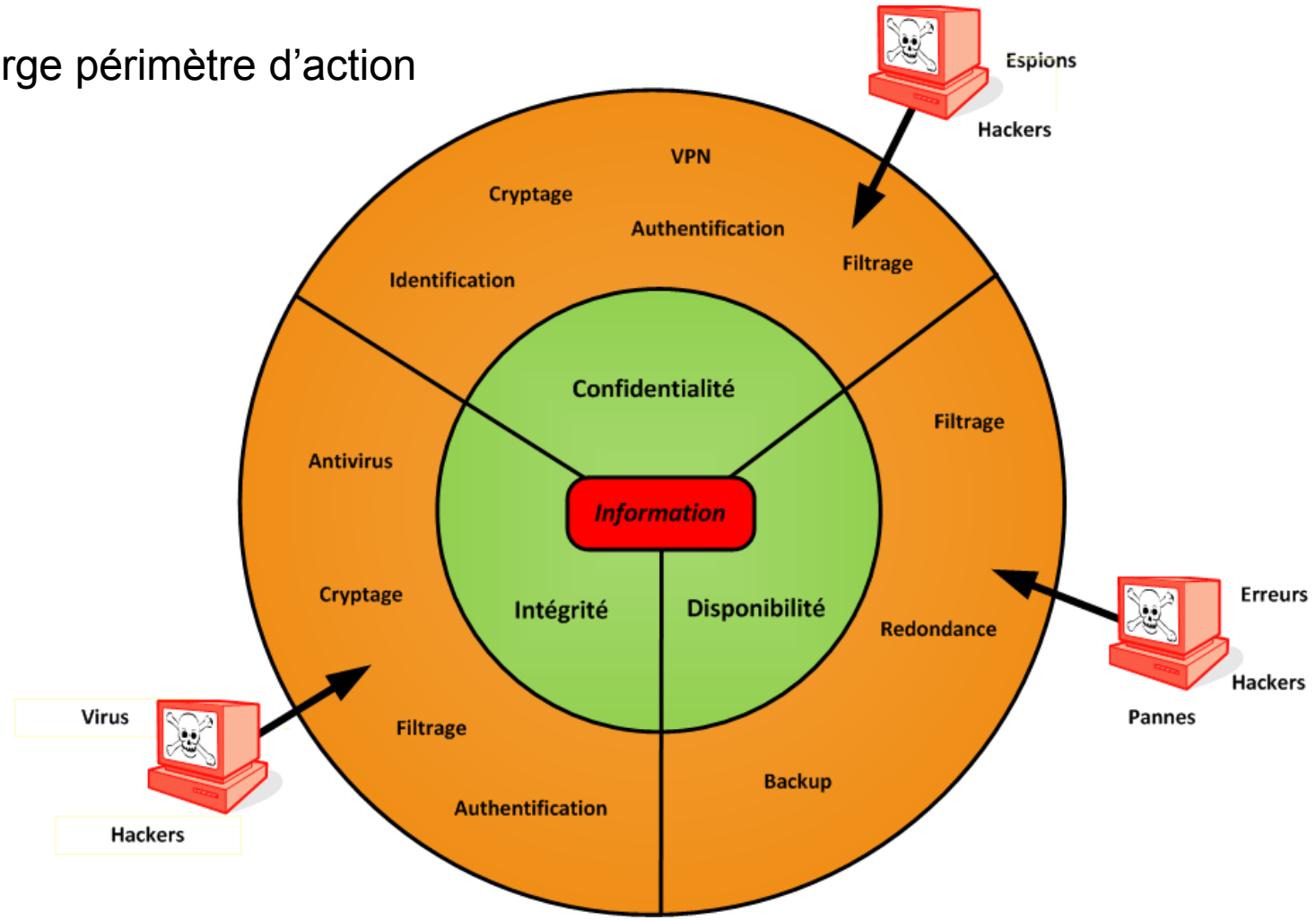
Qu’est-ce que la sécurité informatique ?

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques.

- Interdire les intrusions malveillantes (physiques et/ou logicielles)
- Protéger le réseau des utilisateurs
- Permettre de se connecter à Internet
- Définir les accès des utilisateurs aux différentes applications
- Permettre l’ouverture de son réseau à ses partenaires ainsi qu’à ses employés itinérants

Vue générale

Un large périmètre d'action



Propriétés de base

- **Disponibilité :** La disponibilité des accès aux ressources informatiques consiste à maintenir le système opérationnel, par la mise en place de plans de secours et de restauration.
  - Ces actions étant à prévoir suite à :
    - la panne du système
    - l'erreur de manipulation
    - la pénétration et à la destruction
    - l'attaque par refus d'accès.
- **Intégrité :** L'intégrité existe quand les personnes autorisées à modifier l'information sont réellement les seules à pouvoir le faire.
- **Confidentialité :** La confidentialité sur les systèmes et réseaux consiste à autoriser les accès aux ressources en respectant des règles strictes limitant l'accès aux ayants droit.

En France, une prise de conscience progressive

- Juin 2008 : Livre blanc sur la défense et la sécurité nationale
- Mai 2011 : Conseil des ministres du 25 mai 2011 dédié à « La politique de sécurité des systèmes d'information »
- Juillet 2012 : Rapport d'information du Sénat sur la cyberdéfense
- Avril 2013 : Nouveau livre blanc sur la défense et la sécurité nationale

- En France, l'ANSSI (Agence nationale de la sécurité des systèmes d'information), créée en 2009, est organisée en 4 sous-directions qui reflètent ses principales missions :

  - le centre opérationnel de la sécurité des systèmes d'information (COSSI) ;
  - la sous-direction Expertise (SDE) ;
  - la sous-direction systèmes d'information sécurisés (SIS) ;
  - la sous-direction Relations extérieures et coordination (RELEC).

LES MÉTHODES UTILISÉES EN SÉCURITÉ INFORMATIQUE

Le contrôle des accès

- Le contrôle des accès est ouvert si les accès non explicitement définis sont autorisés.
  - Cette méthode permissive est donc moins sécurisée mais facilite et diminue les opérations d'administrations.

- Le contrôle des accès est restrictif si les accès non explicitement définis sont systématiquement interdits.
  - Dans cette optique la mise en place d'une hiérarchie des droits d'accès et de l'assignation de niveaux d'accès pour chaque utilisateur est retenue. Chaque objet (serveur, répertoire, fichier etc.) se voit attribuer une étiquette classant son niveau de confidentialité « public, confidentiel, top secret ... ».

Identification et authentification

- L'identification est le processus de reconnaissance de l'identité des personnes cherchant à accéder au réseau et aux ressources des systèmes.
  - C'est typiquement le nom de l'utilisateur.

- L'authentification est le processus de vérification de l'identité de l'utilisateur.
  - mot de passe
  - analyse biométrique, ...

La non-répudiation

- La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu
- A cette notion sont associées
  - L'imputabilité: une action a eu lieu et automatiquement un enregistrement, preuve de l'action, est effectué
  - La traçabilité: mémorisation de l'origine du message
  - L'auditabilité: capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement.
- L'existence de fichiers journaux permet de garantir l'imputation et l'auditabilité

L’audit

- L’audit est un point important dans la sécurité. Il enregistre
  - les tentatives d’accès rejetées
  - les actions des utilisateurs de confiance
  - la pénétration par un trou de sécurité
  - la pénétration par vol d’identité

- Les fichiers d’audit et de log doivent être particulièrement bien protégés pour éviter leur destruction effaçant ainsi toutes traces de passage des personnes malveillantes.

LES MENACES

Les menaces

"Avant, pour faire la guerre il fallait une armée, …

… aujourd'hui tout ce dont vous avez besoin est une connexion internet"

http://tomnichols.net/blog/2011/11/16/meeting-cyber-attacks-with-military-force/

Identifier les « ennemis »

- **N'importe qui avec l'évolution et la vulgarisation des connaissances**
- **Beaucoup d'outils sont disponibles « facilement » sur internet**
- **Quelques populations :**
  - **Script kiddies, Lamers, Pyjamas, :** les néophytes
  - **Les hacktivistes :** défendre une cause (paralyser ou récupérer des informations)
  - **Les crackers :** s'attaquent aux libertés des programmes, anti-copyright et cartes de crédits.
  - **Les hackers**
    - White hat : professionnels de la sécurité informatique qui prennent en compte la législation
    - Black hat : nuire, faire du profit ou obtenir des informations (virus, espions, escrocs, etc.)
    - Grey hat : pénétrer les systèmes informatiques sans nuire. Recherchent l'exploit.
    - Crashers (black hat) : effacer des données. Excepté les pertes d'exploitation, les dégâts sont réparables par restauration des données.
  - **Les espions (industriels ou autres)** : Ce sont les plus difficiles à détecter car ils essayent de passer inaperçus. Ils utilisent toutes les méthodes d'espionnage connues pour pénétrer les réseaux et systèmes. La parade requiert une politique de sécurité draconienne.
  - **Les anciens employés :** souvent des comptes utilisateurs non-désactivés
  - **Les maladroits :** Ils ont malencontreusement ou normalement accès au réseau et vont sans le savoir détruire ou endommager des données. Considérant la difficulté de se protéger contre les erreurs de manipulation, il faut posséder des sauvegardes fréquentes, former et sensibiliser les individus.

Identifier les menaces

- Un contexte technique
  - Explosion des technologies de transferts de données (Cloud Computing, Réseaux Sociaux)
  - Complexité souvent croissante des architectures (matérielles, logicielles)
  - Ouverture plus ou moins maitrisée des réseaux de communications

- Un contexte organisationnel
  - Besoin de plus en plus d'informations
  - Grande diversité des informations (financières, R&D, médicales, techniques, etc.)
  - Ces données prennent de plus en plus de valeur et sont donc convoitées.

- Quels sont les objectifs des menaces ?
  - Désinformer
  - Bloquer l'accès
  - Récupérer de l'information
  - Utiliser un système pour rebondir
  - Constituer un réseau botnet pour mettre en commun des machines distinctes et rendre l'activité plus efficace
  - Etc.

Force de frappe d'un botnet

Top 10 des botnets en 2009

Nom du botnet	Nombre de machines	Capacité en mails par minute
Rustock	540 000 à 810 000	14 000 000
Cutwail	1 100 000 à 1 600 000	12 800 000
Bagle	520 000 à 780 000	12 000 000
Bobax	110 000 à 160 000	10 000 000
Grum	580 000 à 860 000	6 800 000
Maazben	240 000 à 360 000	1 500 000
Festi	140 000 à 220 000	900 000
Mega-D	50 000 à 70 000	690 000
Xarvester	20 000 à 36 000	615 000
Gheg	50 000 à 70 000	300 000

Quelques attaques significatives

Juin 2010 : Natanz, IRAN (site d'enrichissement d'uranium)

- Ce que nous savons de Stuxnet (Mikko … F-Secure) :
  - Stuxnet est un gros ver infectant les systèmes windows (1,5 Mo), se propage via ports USB
  - Stuxnet s'exécute même si Autorun et Autoplay sont désactivés
  - Stuxnet utilise 5 vulnérabilités (dont 4 zero-days) et 2 certificats électroniques volés
  - Stuxnet se cache à l'aide d'un rootkit
  - Stuxnet se met à jour via 2 serveurs (Malaisie, Danemark) ou quand il rencontre un autre ver Stuxnet avec une version plus récente
  - Stuxnet vérifie si l'ordinateur infecté est relié à un automate de type Simatic de Siemens
  - Stuxnet prend le contrôle de l'automate, modifie la vitesse de rotation des centrifugeuses
  - Stuxnet envoie des mesures de capteurs OK au module de contrôle-commande
- Des centaines de milliers de machines infectées, 15 usines touchées (d'après Siemens)
- La version de Stuxnet utilisée s'est autodétruite le 24 juin 2012
- http://www.f-secure.com/weblog/archives/00002040.html

Quelques attaques significatives

2012: Flame

- En mai 2012, un nouveau malware « Flame » infecte les systèmes d'exploitation Windows. Il semble qu'il ait été créé par les États-Unis et/ou Israël pour servir à des fins de cyber-espionnage. Flame est volumineux pour un logiciel malveillant (plus de 20 Mo une fois installé). Il inclut plusieurs bibliothèques de compression de données : zlib, libbz2 et PPMd, mais aussi un serveur SQLite 3 et une machine virtuelle en langage de script Lua3. Ce logiciel permet d'intercepter des e-mails, des données PDF, Office, des graphiques, et d'enregistrer des conversations en ligne.

- Cibles identifiées : Iran, Cisjordanie, Soudan, Syrie, Liban, Arabie saoudite et Égypte.
- Objectif pressenti : recueillir des données en préparation d'une autre attaque informatique visant à ralentir la capacité de l'Iran à développer une arme nucléaire

Une tendance croissante : Ransonware

Quelques attaques significatives

- FRANCE - Un logiciel espion pour iPhone : un groupe d'étudiants français propose en ligne une application capable d'enregistrer les conversations, de localiser le téléphone portable et d'en activer le micro à distance. Le logiciel fonctionne sur toute version d'iPhone dont les protections logicielles ont été débridées. (Communiqueo du 02/11 et SpyTic)

[En France, l'utilisation ou la mise à disposition d'une telle application est réprimée par l'article 323-3-1 du Code pénal. L'atteinte au secret des correspondances est sanctionnée par l'article 226-15 du Code pénal.]

Quelques attaques significatives

- Social Engineering

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC) W721460021

NAME: ..... MITNICK, KEVIN DAVID

AKS (S): ..... MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: ..... MALE
Race: ..... WHITE
Place of Birth: ..... SAN RUFO, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ..... 5'11"
Weight: 190
Eyes: ..... BLUE
Hair: ..... BROWN
Skintone: ..... LIGHT
Scars, Marks, Tattoos: ..... NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: 20POSSPIC181PM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSING UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia, Telephone: (800)336-0102 (24 hour telephone contact) NLETS access code is VAUSMOOOO.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132 (Rev. 5/1/85)

November 1992

Kevin Mitnick (Le Condor)

- 3 livres, 1 film (Cybertraque).
- Piratage des réseaux téléphoniques.
- Accès illégal aux bases de données des clients de Pacific Bell, ainsi qu'aux systèmes de Fujitsu, Motorola, Nokia, Sun Microsystems et du Pentagone. Il est le premier hacker à figurer sur la liste des dix fugitifs les plus recherchés du FBI.
- 5 ans de prison et sous interdiction d'utiliser des ordinateurs.

Les faux gentils

- FRANCE/ÉTATS-UNIS - La CNIL condamne Google à 100000 euros d'amende pour la collecte massive de données techniques sur les réseaux Wi-Fi français : lors de contrôles en 2009 et 2010, la CNIL a constaté que les véhicules Google Cars, utilisés pour la prise de vue de rues destinée à alimenter le service Street View, collectaient des données échangées sur des réseaux Wi-Fi non sécurisés. Selon la CNIL, ces données comportent des informations sensibles telles que des mots de passe et des courriels.

Les faux gentils

- DROPBOX, extraits des conditions d'utilisation

  - ***Fichiers journaux.*** Lorsque vous utilisez le Service, nous enregistrons automatiquement des informations sur votre Appareil, ses logiciels et vos activités. Ces informations peuvent inclure l'adresse IP (Internet Protocol) de l'Appareil, le type de navigateur utilisé, la page Web visitée avant que vous n'accédiez à notre site, les informations que vous recherchez sur notre site, vos paramètres régionaux, les numéros d'identification associés à vos Appareils, votre opérateur mobile, la date et l'heure des transactions, les informations de configuration du système, les métadonnées relatives à vos fichiers et d'autres interactions avec le Service.

  - ***Données personnelles.*** Pendant l'utilisation du Service, nous pouvons collecter des données personnelles qui peuvent être utilisées pour vous contacter ou vous identifier (les "**Données personnelles**"). Les Données personnelles sont ou peuvent être utilisées : (i) pour fournir et améliorer notre Service, (ii) pour gérer votre utilisation du Service, (iii) pour mieux comprendre vos besoins et intérêts, (iv) pour personnaliser et améliorer votre utilisation du Service

Identifier les menaces

- Prévision de sécurité par Symantec

1. Une explosion des ransomwares et des menaces sur mobiles et les réseaux sociaux de plus en plus pointuesRansonware : intimidation ou harcèlement pour effectuer des paiements en ligne
2. Menace sur l'intégrité des données : modifier les données donc les actions (ex : Stuxnet ou Narilam)
3. Usurpation d'identités (certificats, DNS)
4. De fausses pages sur les réseaux sociaux (renseignements généraux ou données bancaires)
5. Fuite d'informations via les réseaux sociaux professionnels (Viadeo, Linkedin, etc)
6. Nouvelles cibles : le Cloud et les mobiles

Enjeux juridique

- Art 121-2 Code pénal : " Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement (….) des infractions commises, pour leur compte, par les organes dirigeants ou représentants »

- Art 1384 Code Civil : «On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre (…) les maîtres et les commettants du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés »

- Art 1383 Code Civil : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence »

Quelques exemples de vulnérabilité

- Absence de politique de sécurité et de programme de sensibilisation
- Mauvaise gestion des mots de passe
- Absence de suivi des évolutions des problèmes et des solutions, de test et de relation entre les concepteurs d'une application et les administrateurs de sécurité
- Utilisation du profil administrateur pour les activités normales
- Absence ou manque de contrôles réguliers de l’état des sauvegardes
- Installations anarchiques
- Présence d'utilisateurs fantômes
- Stations de travail abandonnées non protégées
- Portables sans surveillance
- Firewalls et serveurs internes mal configurés
- Mauvaise gestion des autorisations
- Identifiants de session interprétables
- Informations échangées ou stockées en clair
- Absence de contrôle des canaux d’émission et de réception de courriels

Les logiciels malveillants

- Virus : Portion de code inoffensive ou destructrice capable de se reproduire et de se propager
- Vers : proches des virus mais capables de se propager sur d'autres ordinateurs à travers le réseau
- Chevaux de troie
- Spywares (adware, malware) : logiciel qui collecte des informations d'une machine et les envoie à l'insu de l'utilisateur sans son consentement
- Spam : Envoi massif et parfois répété de courriers électroniques non sollicités
- Phishing : Technique d'ingénierie sociale utilisée par des arnaqueurs (scammers)
- Scam : Pratique frauduleuse ("ruse") pour extorquer des fonds à des internautes
- Botnet : réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches

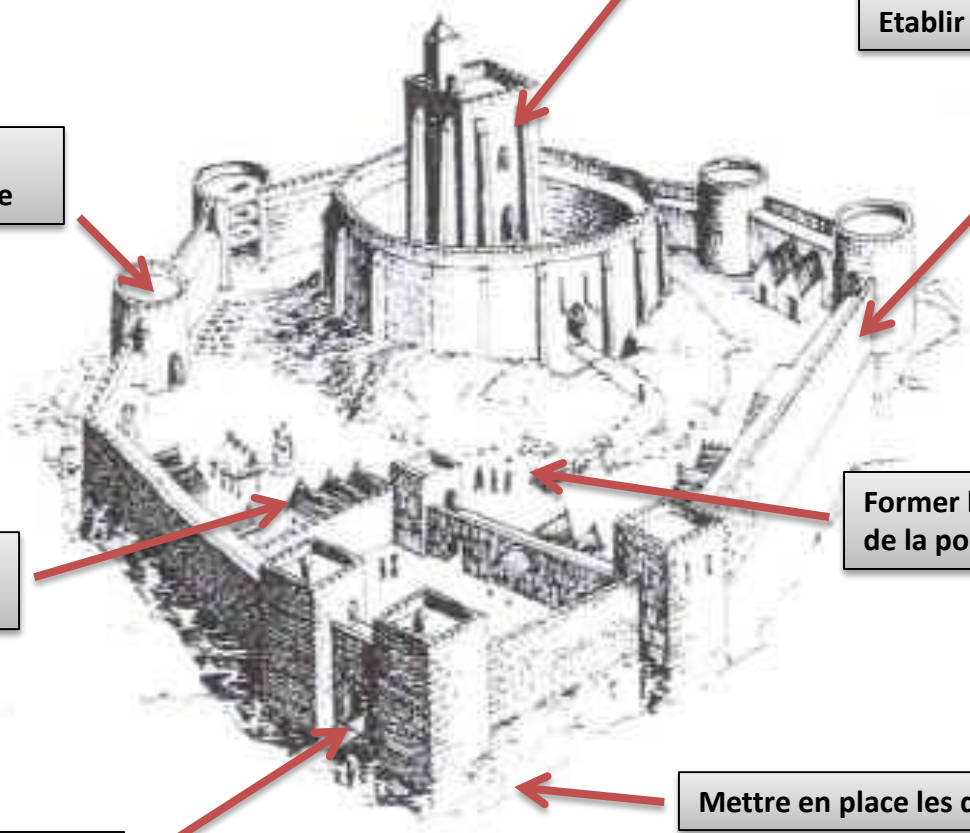
A retenir…

- La responsabilité des acteurs (responsable sécurité, ...) est de plus en plus invoquée lors de sinistre où les ressources informatiques qu'ils gèrent sont l'objet ou le moyen d'une fraude
- Il est donc nécessaire de pouvoir prouver que des mesures sont pourtant prise pour sécuriser le système afin de se protéger contre un délit de manquement à la sécurité
  - A défaut d'une obligation de résultat, les responsables de systèmes informatiques ou sécurité ont une obligation de moyens
- Les responsables d'entreprises doivent également être extrêmement attentifs à l'égard du droit des nouvelles technologies

DÉFINITION D'UNE POLITIQUE DE SÉCURITÉ

Eviter ceci…

La politique de sécurité



Protéger les ressources sensibles

Etablir les périmètres de sécurité

Assurer une surveillance permanente interne et externe

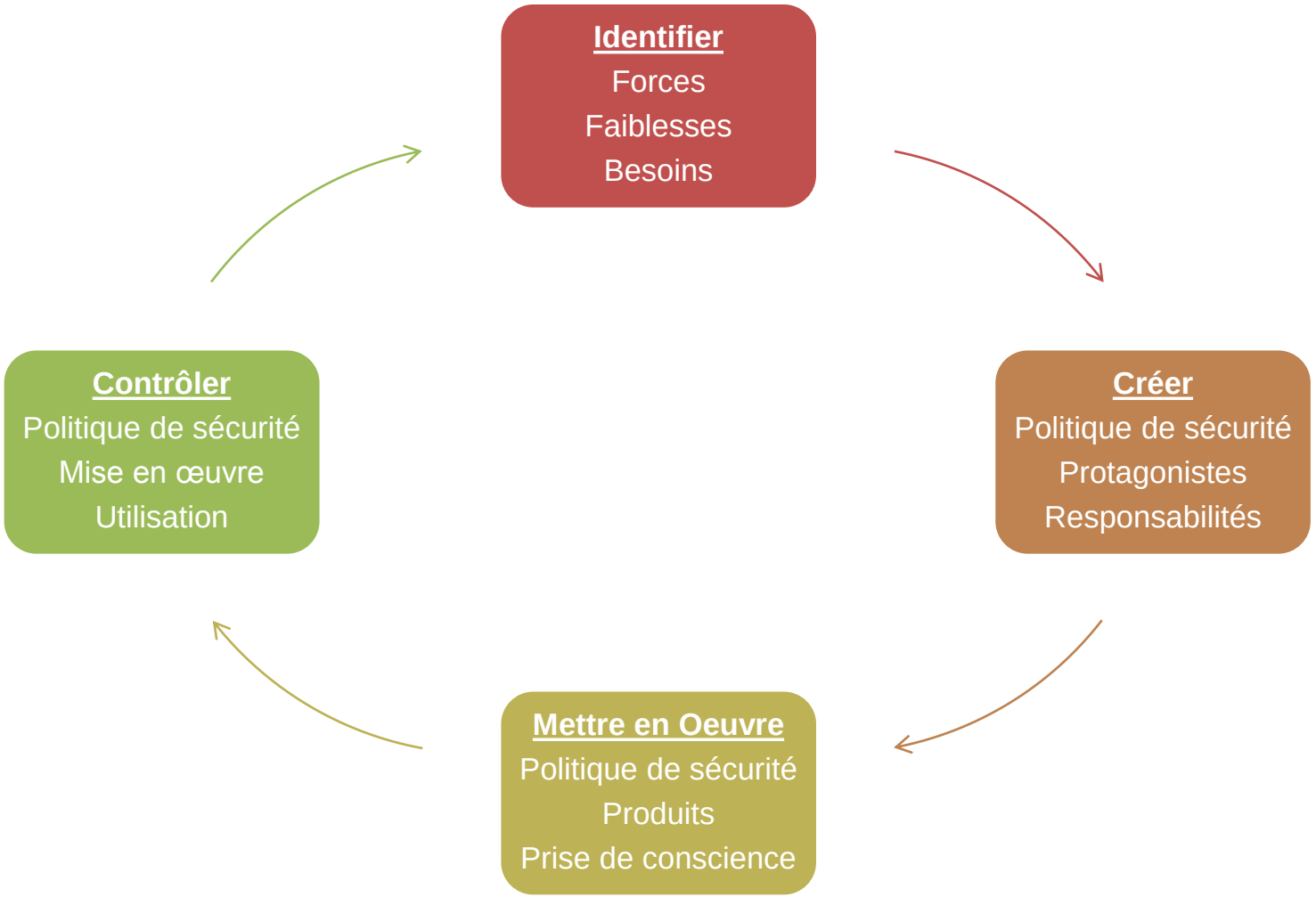
Former les hommes à l'application de la politique de sécurité

Préparer les méthodes de représailles

Mettre en place les défenses passives

Définir les points d'accès aux ressources et filtrer les entrées

La sécurité est un processus



Quelques notions

- Exprime la volonté managériale de protéger les valeurs informationnelles et le ressources informatiques de l'organisation
- Spécifie les moyens (ressources, procédures, outils, ...)
- Evite que le système d'information ne devienne une cible et qu'il ne se transforme pas en un acteur d'attaques par prise de contrôle à distance
- Cette protection est assuré par exemple par :
  - Des règles: classification de l'information
  - Des outils: réseaux, matériels, logiciels
  - Des contrats: clauses, obligations
  - La législation: dépôt de marques, brevets et protection de droit d'auteur

Propriétés d'une politique de sécurité

- La définition de la politique de sécurité doit être
  - Simple et compréhensible
  - Adoptable par un personnel préalablement sensibilisé voire formé
  - Aisément réalisable
  - De maintenance facile
  - Vérifiable et contrôlable
- Elle ne doit pas être statique mais périodiquement évaluée et adaptée
- Elle doit pouvoir être configurable et personnalisable
  - « Accès aux jours ouvrés entre 7h et 20h » mais occasionnellement, accès le week-end

Classification des ressources

- Réaliser un inventaire complet de tous les acteurs de la chaîne de sécurité :
  - Contribue à une meilleur connaissance et donc à la maitrise de l'environnement à protéger
- Analyser de l'existant et cet inventaire
  - Permet de déterminer le degré de criticité de chacune des ressources et d'en faire une classification
    - C'est à dire son importance en cas de perte, d'altération ou de divulgation des données
- Pour chaque classe, il faut identifier
  - les risques possibles (erreur d'utilisation, de paramétrage, accidents, malveillance, sabotage, ...)
  - les mécanismes de sécurité applicables
  - Les contraintes techniques et organisationnelles afin de déterminer la faisabilité de la politique de sécurité pour chaque classe de ressources

Mesures de sécurité

- Après identification des risques, des mesures de sécurité peuvent être mises en place
- Plusieurs types génériques de mesures de sécurité sont identifiés
  - Avant sinistre
    - Mesures préventives: détecteur d'intrusion, anti-virus, contrôle d'accès
    - Mesures structurelles: occultation des ressources, fragmentation de l'information afin de réduire la vulnérabilité des ressources
    - Mesures de dissuasion: peut être des protections juridiques ou administratives
  - Après sinistre
    - Mesures palliatives et correctives: les sauvegardes, plan de continuité, redondances
    - Mesures de récupération: limitent les pertes et réduisent les préjudices, utilisation d'assurance ou attribution de dommages et intérêts par des actions en justice

- Certaines de ces mesures sont décrites dans un plan de continuité.

DEFINITION D’UN PLAN DE CONTINUITE

C’est quoi ?

- Les Plans de Reprise d’Activités et les Plans de Continuité d’Activité (PCA) sont composés de documents et de procédures destinés à permettre le fonctionnement en cas d’incident/sinistre.
  - Le PRA est destiné à reprendre l’activité, éventuellement en mode dégradé, après un certain temps.
  - Le PCA est destiné à assurer la continuité du service, éventuellement en mode dégradé.
- Ramener au système informatique, on peut aussi parler de Plan de Secours Informatique (PSI) et de Plan de Continuité Informatique (PCI).
- Un plan de continuité doit être suivi comme un vrai projet et suivre une vrai méthodologie qui pourrait être en 4 phases

C’est quoi ?

- Quelques questions à se poser:
  - Quels sont les services prioritaires ?
  - Quelles sont les ressources (locaux, équipement, personne) ?
  - Quelle est la durée maximale d’interruption admissible (Recovery Time Objective) ?
  - Quelle est la perte de données maximale admissible (Recovery Point Objective) ?

RTO

- Le délai d'interruption est composé:
  - Délai de détection de l'incident (t1)
  - Délai de décision du passage en mode secours (t2)
  - Délai de mise en œuvre des procédures de secours (t3)
  - Délai de contrôle et relance des services et applications (t4)

- $t1 + t2 + t3 + t4 < RTO$

- La valeur du RTO impacte l'infrastructure:
  - Pour un RTO de 24h, un contrat de maintenance sur site peut suffire
  - UN RTO proche de zéro peut nécessiter du clustering, une salle serveur géographiquement distante,…

RPO

- Le RPO quantifie les données que l'on peut être amené à perdre suite à un incident.
- Le RPO exprime une durée entre le moment de l'incident et la date la plus récente des données qui pourront être restaurées.
- Le RPO est conditionné par le type et la fréquence des sauvegardes effectuées.
- Les données perdues pourront être récupérées à partir d'une sauvegarde, d'une réplication, d'un journal de transaction, …
- Des sauvegardes régulières peuvent suffire dans le cas d'un RPO élevé. Pour un RPO faible, des mécanismes tels que la réplication synchrone doivent être mis en place.

Méthodologie

- **Analyse stratégique**
  - Organisation et conduite de projet
  - Cahier des charges (fonctions prioritaires, niveau de service, ..)
  - Analyse (état de l'existant, criticité des services)
  - Phase d'orientation (hiérarchisation de la criticité des systèmes, sauvegarde des données critiques, …)

- **Analyse des solutions**
  - Proposition de solutions et d'architectures
  - Conventions avec les prestataires (assistance, spare, copie des documents/programmes)

Méthodologie

- **Mise en œuvre opérationnelle**
  - Maquettage et tests, puis mise en œuvre des mécanismes les plus simples possibles
    - La défense doit être à la hauteur du risque de l'attaque.
    - La défense doit aussi être uniforme. La sécurité de l'ensemble du système dépend du maillon le plus faible de l'architecture.
  - Attribution des responsabilités, la sensibilisation et la formation des personnes responsables de l'exécution des procédures de reprise
  - Une documentation complète du plan de secours
- **Validation et suivi**
  - Exercices réguliers et programmés
    - Permet de tester le plan de secours, son efficacité
    - Permet de documenter et analyser les résultats
    - Permet de mettre à jour le plan et éventuellement de réorganiser la répartition des tâches aux membres de l'équipe
  - Audit
    - Permet de déterminer la qualité du plan établi et d'élaborer des recommandations

DOMAINES DE LA SÉCURITÉ

Les domaines de la sécurité informatique

- Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information

- En fonction de son domaine d'application, la sécurité informatique se décline en
  - Sécurité physique
  - Sécurité de l'exploitation
  - Sécurité logique
  - Sécurité applicative
  - Sécurité des télécommunications

1/ Sécurité physique

- Concerne tous les aspects liés de l'environnement dans lequel les systèmes se trouvent
- La sécurité physique passe donc par
  - Des normes de sécurité
  - Protection de l'environnement (incendie, température, humidité, ...)
  - Protection des accès
  - Redondance physique
  - Plan de maintenance préventive (test, ...) et corrective (pièce de rechange, ...)
  - …

2/ Sécurité de l'exploitation

- Rapport à tous ce qui touche au bon fonctionnement des systèmes
- Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour
- La sécurité de l'exploitation dépend fortement de son degré d'industrialisation qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches
- Quelques points clés de cette sécurité
  - Plan de sauvegarde, de secours, de continuité, de tests
  - Inventaire réguliers et si possible dynamique
  - Gestion du parc informatique, des configurations et des mises à jour
  - Contrôle et suivi de l'exploitation
  - ...

3/ Sécurité logique

- La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel
- Elle repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation
- Elle repose également sur
  - Les dispositifs mis en place pour garantir la confidentialité dont la cryptographie
  - Une gestion efficace des mots de passe et des procédures d'authentification
  - Des mesures antivirus et de sauvegarde des informations sensibles
- Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier leur degré de sensibilité (normale, confidentielle, top secrète, ...)

4/ Sécurité applicative

- Faire un développement pertinent et l'intégrer harmonieusement dans les applications existantes
- Cette sécurité repose essentiellement sur
  - Une méthodologie de développement
  - La robustesse des applications
  - Des contrôles programmés
  - Des jeux de tests
  - Un plan de migration des applications critiques
  - La validation et l'audit des programmes
  - Un plan d'assurance sécurité
  - ...

5/ Sécurité des télécommunications

- Offrir à l'utilisateur final une connectivité fiable et de qualité de « bout en bout »
- Il faut donc mettre un canal de communication fiable entre les correspondants, quels que soient le nombre et la nature des éléments intermédiaires
- Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements

PROTECTION UTILISÉES DANS LA PRATIQUE

Un panel d'outils techniques

- **FIREWALL ou PARES-FEUX**
  - Application de règles d'accès (filtrage) entre les différents réseaux.
  - Tout ce qui n'est pas expressément permis est interdit
  - Firewall de type appliance ou logiciel

- **PROXY - Pour les utilisateurs « internes » :**
  - Cache : permet de sauvegarder les informations les + demandées (gain de performances / temps)
  - Mandataire : permet de ne pas exposer les utilisateurs à internet.
  - Centraliser et contrôler les accès à internet

- **REVERSE-PROXY - Pour les utilisateurs externes**
  - Permet de ne pas exposer directement le serveur public (www/ftp/….) à l 'Internet

Un panel d'outils techniques

- **CRYPTAGE (fichiers, disques, communications)**
  - La **cryptographie** est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de *secrets* ou *clés*.

- **AUTHENTIFICATION (simple et forte)**
  - Une **authentification simple** est une procédure d'authentification qui requiert un seul élément ou « facteur » d'authentification valide pour permettre l'accès à une ressource (ex : mot de passe)
  - Une **authentification forte** est une procédure d'identification qui requiert concaténation d'au moins deux éléments ou « facteurs » d'authentification qui sont :
    - Ce que l'entité connaît (Exemples : un mot de passe, un code PIN)
    - Ce que l'entité détient (Exemples : une clé USB, une carte à Puce)
    - Ce que l'entité est, soit une personne physique (Exemples : empreinte digitale),
    - Ce que l'entité sait faire, soit une personne physique (Exemples : signature, reconnaissance vocal)

Un panel d'outils techniques

- **ANTIVIRUS**
  - La protection antivirus doit être considérée à trois niveaux : Passerelle + Poste de travail + Serveurs
- **ANTISPAM**
  - Beaucoup de techniques antispam existent, mais il n'y a pas de recettes miracles…
  - Protection de base : anti-relay
- **FILTRAGE DE CONTENU**
  - Contrôler la navigation Internet (urls, flux, antivirus) des employés de l'entreprise, que ce soit par souci de productivité, de préservation de la bande passante, de sécurité ou de protection de l'image de marque de l'entreprise.

Un panel d'outils techniques

- **Contrôler les accès au réseau (NAC, NAP, SNA etc.)**
  - Objectifs
    - Minimiser l'impact des programmes malveillants sur un réseau de production
    - Empêcher les connexions aux ressources de personnes non-autorisées
    - Répondre à des exigences de conformité
  - Exemples de contrôle
    - Un logiciel anti-virus mis à jour
    - Un pare-feu activé
    - Utilisation de réseaux privés virtuels (VPN)
    - Présence de serveurs mandataires (proxy)
  - Sinon… QUARANTAINE

Un panel d'outils techniques

- **DETECTION et PREVENTION D'INTRUSIONS**
  - Complémentaire au firewall, permet de réagir en temps réel aux tentatives d'intrusions par :
    - Surveillance active du trafic réseau ou d'un système d'exploitation
    - Déclenchement automatiquement des actions en fonction des attaques détectées
  - La détection se fait suivant une base de signatures d'attaques connues.
  - En fonction des attaques ou vulnérabilités que l'on veut détecter, on identifie les actions associées qui peuvent être du type :
    - Informations (log, envoi de mail vers les administrateurs…)
    - Fermeture de la connexion en cours
    - Reconfiguration d'un produit (firewall)

Un panel d'outils techniques

- **PROTECTIONS DES POSTES DE TRAVAIL**
  - Firewall personnel
  - Antivirus
  - Host IPS
  - Contrôle des périphériques USB, des connexions réseaux
  - Cryptage du contenu
  - Contrôle des applications
  - Renforcement de l'OS

Un panel d'outils techniques

- **VIRTUALISATION**
  - Quelques avantages:
    - Optimiser l'usage des ressources d'une machine tout en isolant les services entre eux.
    - Optimisation du taux d'utilisation des ressources informatiques
    - Economie d'énergie (« green computing »)
    - Gain économique et d'encombrement
    - Possibilité de cloner et/ou de déplacer des machines
  - Quelques risques
    - Une panne ou une indisponibilité d'une ressource commune peut bloquer tous les services hébergés.
    - En fonction de la solution virtualisation, un manque de cloisonnement peut engendrer une fuite d'informations.
    - Risque de copie non souhaitée de machine virtuelle

Un panel d'outils techniques

- **SAUVEGARDE**
  - Types de sauvegardes:
    - Sauvegarde complète
      - Tout est sauvegardé
    - Sauvegarde différentielle
      - Sauvegarde des fichiers modifiés depuis la dernière sauvegarde complète. La restauration devra récupérer la sauvegarde complète et la dernière sauvegarde différentielle.
    - Sauvegarde incrémentale
      - Sauvegarde des fichiers depuis la dernière sauvegarde. La restauration devra récupérer la dernière sauvegarde complète et toutes les sauvegardes incrémentales.
  - Définir
    - La périodicité des sauvegardes
    - La durée de rétention des sauvegardes
    - Un lieu de stockage des sauvegardes

Un panel d'outils techniques

- Par exemple, pour tester son réseau, le LiveCD Backtrack contient douze catégories d'outils :
  - Rassemblement d'informations (Information Gathering)
  - Estimation des vulnérabilité (Vulnerability Assessment)
  - Outils d'utilisation des failles (Exploitation Tools)
  - Élévation des privilèges (Privilege Escalation)
  - Maintient d'accès (Maintaining Access)
  - Ingénierie inverse (Reverse Engineering)
  - Outils RFID (RFID Tools)
  - Test de résistance(Stress testing)
  - Recherche forensique (Forensics) = anticiper les failles
  - Outils d'obtention de rapports (Reporting Tools)

QUELQUES RÈGLES

Que faire en cas d'intrusion ?

- Pas de réponse unique:
  - Débrancher ou non la machine (souhaite t'on découvrir les méthodes utilisées par l'intrus ?)
  - Sauvegarder la machine en l'état afin de pouvoir l'analyser à posteriori.
  - Reformater et réinstaller le système à partir d'une sauvegarde saine.
  - Modifier les mots de passe utilisateurs et les éventuelles clés de chiffrement.
  - Ne pas donner d'informations sur l'incident à des tiers non directement concernés.
  - Être vigilant, l'intrus reviendra probablement.

Installation/Administration

- Prudence dans l'installation par défaut des logiciels
- Protection physique des équipements.
- Intégration des objectifs "sécurité" dans les choix de réseaux et des systèmes d'exploitation.
- Localiser et ne laisser ouvert que les services indispensables.
- Fermer les comptes inutilisés
- Se tenir informer des vulnérabilités.
- Passer régulièrement les correctifs.
- Installer les outils nécessaires (contrôle d'authentification, audits, …)
- Consulter régulièrement le journal généré par ces outils.
- Informer ses utilisateurs.
- Chiffrement des informations
- etc

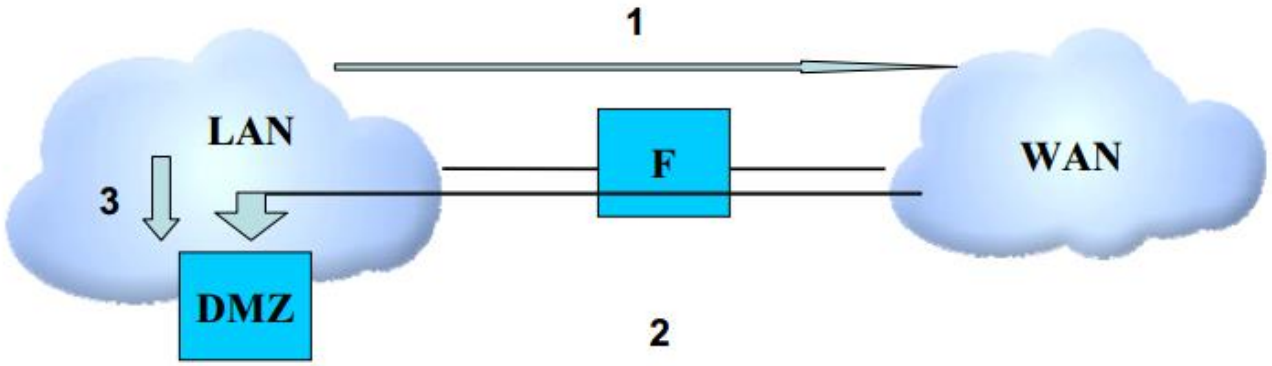
Conseils aux utilisateurs

- Responsabilité d'un compte informatique (personnel et incessible).
- Mot de passe sûr et protégé.
- Prudence avec les fichiers attachés des courriers électroniques, avec les logiciels « gadgets », …

EXEMPLES D'ARCHITECTURE

Architecture basique

- L'architecture la plus simple que l'on puisse proposer. L'interconnexion se résume ici à un simple pare-feu. Les serveurs applicatifs (y compris les serveurs web accessibles depuis internet) sont directement connectés au LAN. Les flux applicatifs considérés ici sont représentés par les schémas. Il s'agit ici:
  1. des flux de consultation internet depuis le LAN ;
  2. des flux de consultation du serveur Web par les internautes depuis internet ;
  3. des flux de mise à disposition de contenu sur le serveur Web depuis le LAN.

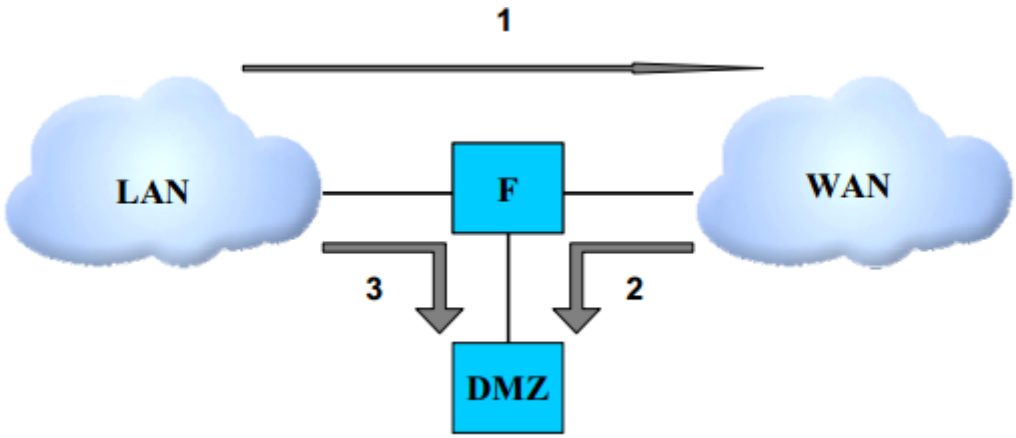


Architecture basique

- Problèmes :
  - Problème 1: les flux depuis Internet vers le serveur web traversent systématiquement le LAN.
  - Problème 2: le pare-feu est un point névralgique de l'architecture.
  - Problème 3: l'architecture ne propose aucune mesure de protection contre la défiguration du site web

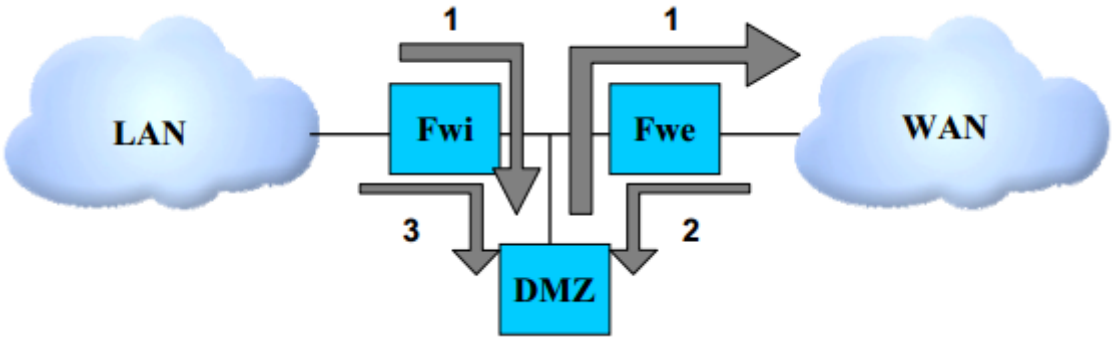
Architecture avec DMZ

- Le premier problème peut être aisément corrigé en connectant directement le serveur web de l'entreprise sur une des interfaces réseau du pare-feu



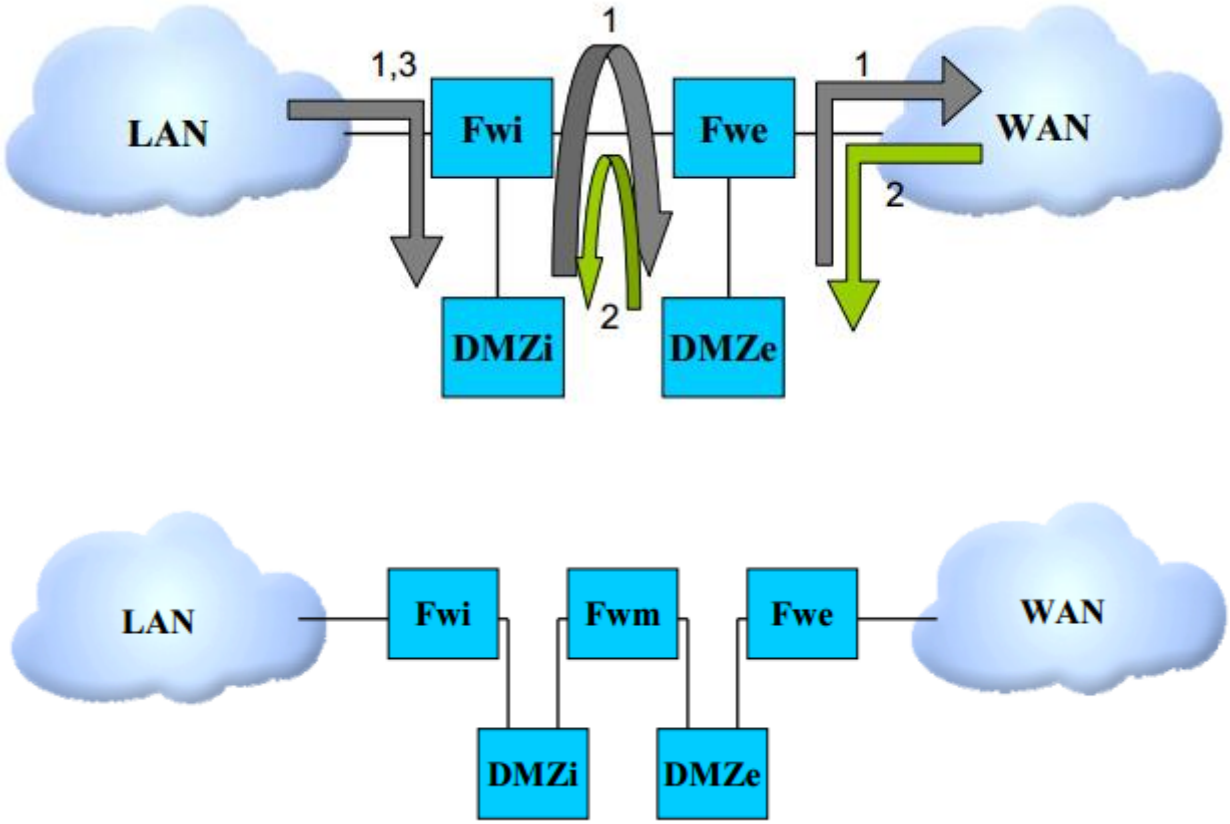
Architecture avec deux parefeux

- Afin de prendre en compte le second problème, il convient de mettre en place deux pare-feux comme indiqué ci-dessous.
  - Un pare-feu interne (FWi) en entrée de LAN
  - Un pare-feu externe, FWe à la frontière du WAN
  - Le nœud entre DMZ, FWi et FWe est par exemple assuré par un commutateur réseau.

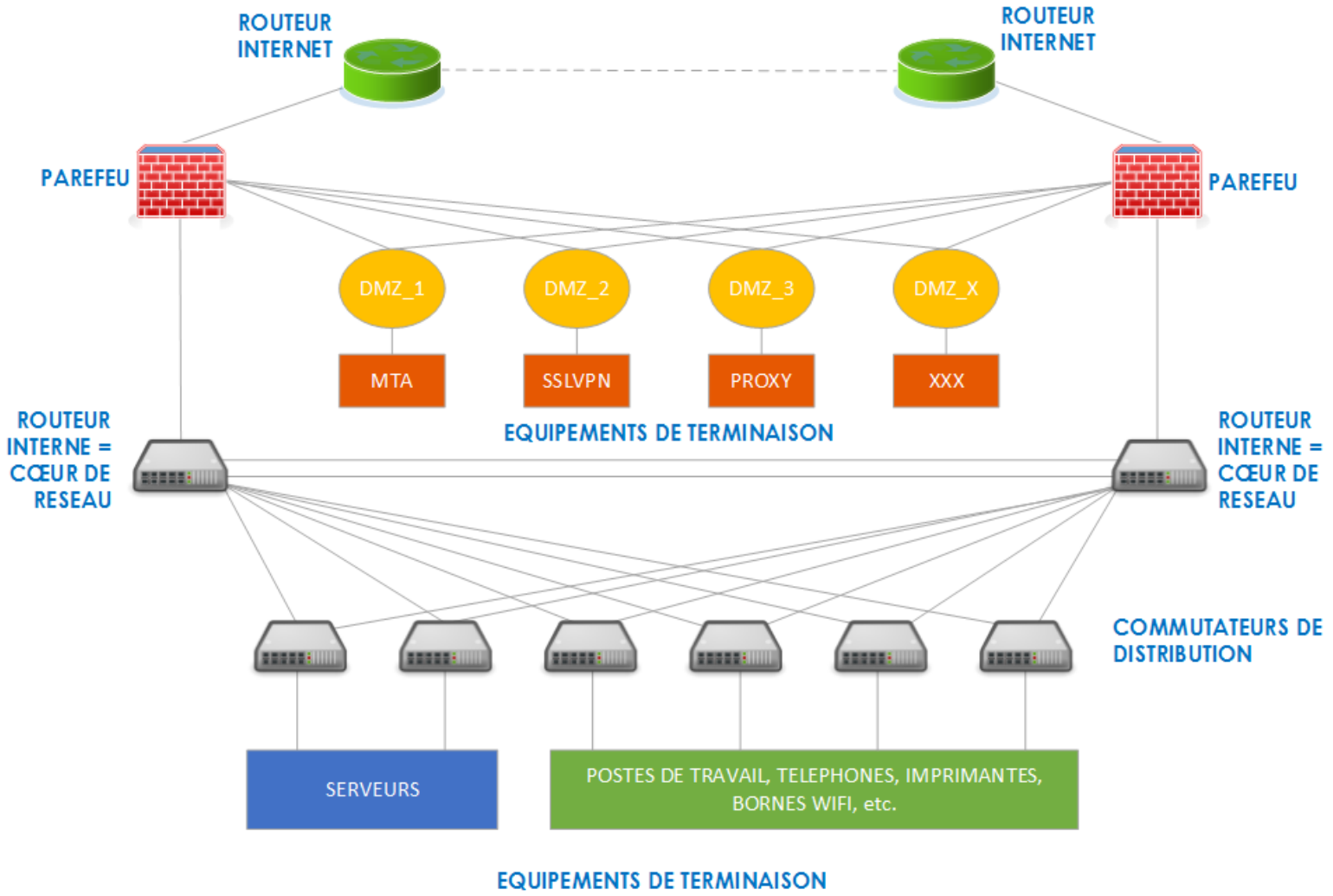


  - Diversifié les constructeurs de parefeux
  - On placera en DMZ les serveurs web + un serveur proxy web

Variantes



Exemple


ROUTEUR INTERNET
ROUTEUR INTERNET
PAREFEU
PAREFEU
DMZ_1
DMZ_2
DMZ_3
DMZ_X
MTA
SSLVPN
PROXY
XXX
EQUIPEMENTS DE TERMINAISON
ROUTEUR INTERNE = CŒUR DE RESEAU
ROUTEUR INTERNE = CŒUR DE RESEAU
COMMUTATEURS DE DISTRIBUTION
SERVEURS
POSTES DE TRAVAIL, TELEPHONES, IMPRIMANTES, BORNES WIFI, etc.
EQUIPEMENTS DE TERMINAISON