Sécurité et Réseaux
RSX 112

Sécurité et Réseaux

Introduction

Introduction

Depuis les années 1960 les ordinateurs sont devenus le cœur des systèmes d'information.

Avec l'arrivée des ordinateurs individuels et de l'internet, l'informatique s'est imposée partout :

- Entreprises,
- Particuliers,
- Objets connectés,
- …

→ Nous avons à faire à une véritable révolution économique, sociale et humaine.

Introduction

Quelques chiffres

•Le taux d'équipement en informatique continue à augmenter dans les foyers (+4,6%),
•81% des foyers sont connectés a internet .
•79% des français se connectent via le Wifi (+ 50% en 2 ans)
•50% des ordinateurs familiaux servent aussi à des activités professionnelles.
•Internet est de plus en plus utilisé sur les lieux de vacances, dans les hôtels, les cyber-cafés (+10% en 2 ans).
•Le stockage en ligne des données personnelles est utilisé par 38% des internautes.
•93% des internautes ont effectué des achats en ligne
•4 personnes sur 5 utilisent les réseaux sociaux.

Source Clusir .

Introduction

Les systèmes informatiques contiennent aujourd'hui de véritables trésors :

- Informations bancaires
- Information sur les personnes
- Projets industriels
- Travaux de recherche ou d'écoles
- Adresses E-mail
- Données relatives aux comptes (mot de passe E-mail, mots de passe de connexion, mots de passe de services Internet, mots de passe FTP, etc.)
- Etc...

Introduction

Problème : entreprises et individus évoluent dans un milieu « hostile » :

- concurrence économique
- gestion de ressources humaines
- pirates
- systèmes non-fiables
- catastrophes climatiques
- environnement politique
- …

Introduction

Tous ces facteurs sont sources d'insécurité :

→Fuite des données

→Modification/pertes des données

→Blocage des systèmes

Introduction

Cette insécurité est en constante progression …

Les types d'incidents rencontrés sont en hausse :

- pertes de services essentiels (26% → 39%),
- vols (19% → 37%),
- pannes d'origine interne (25% → 35%).

Incidents d'origines malveillantes sont toujours en hausse :

1 - « infections par virus » (+14,4%),

2 - « attaques logiques ciblées » (+10,5%)

3 - « vols » (+7,1 %).

Les principaux incidents de sécurité rencontrés par les entreprises (Source Clusif)

Cas d'école

Janvier 2008 : un adolescent polonais de 14 ans provoque le déraillement de 4 wagons d'un tramway après avoir pris le contrôle du système de signalisation et d'aiguillage.

Fin 2008 , 9 millions de dollars de retraits frauduleux avec des cartes clonées dans 2100 distributeurs de billets de 280 villes et 8 pays. 4 personnes sont a l'origine de cette fraude.

Le 24 février 2007: « Un hacker joue un mauvais tour aux automobilistes argentins », il pénètre le site internet du secrétariat à l'Energie et efface plusieurs milliers de stations à essence de la liste officielle de livraisons de carburant. Conséquence, privation de combustible de ces stations service en Argentine. L'information est relayée par les médias → énorme panique dans le pays.

Cas d'école

Espionnage aux Etats-Unis : «J'avais le pouvoir d'écouter n'importe qui»

LIBERATION 10 JUIN 2013 À 12:50

Réfugié à Hongkong, l'Américain Edward Snowden, la source qui a fait fuiter des informations sur le programme de surveillance des communications, est sorti de l'ombre face à une caméra du «Guardian».

Cybervandalisme, 25000 sites Web français attaqués

Sécurité : *L'offensive des activistes islamistes contre le Web français donne lieu à une réponse judiciaire commune, prévient le ministre de l'Intérieur.*

Par La rédaction de ZDNet.fr | Lundi 19 Janvier 2015

Suivre @zdnetfr

Cas d'école

SURVEILLANCE

Ecoutes : 25 ans de politique de l'autruche des gouvernements

29 JUIN 2015 | PAR JÉRÔME HOURDEAUX

C'est en 1988 qu'est paru le premier article révélant précisément le système d'écoute déployé dans le monde par les États-Unis. Depuis, malgré les rapports parlementaires et révélations de lanceurs d'alerte, les responsables politiques ont pris soin d'éviter toute confrontation avec leur allié.

Le contrôle de l'activité des salariés par l'outil informatique

Publié le 28/04/2014 à 06:00 par la rédaction des Éditions Tissot dans sanction et discipline

Ordinateur, disque dur, clé USB, messagerie électronique, site Internet… tout cela fait partie de notre quotidien. Reste que le développement des nouvelles technologies dans l'entreprise crée un nouveau mode de contrôle et de surveillance de l'activité des salariés. Comment adapter votre pouvoir disciplinaire et de direction ? Qu'avez-vous le droit de faire, que ne pouvez-vous pas faire ? Eléments de réponse…

01net ▸ Actualités ▸ Buzz, société

Des réparateurs informatiques beaucoup trop curieux

24/07/2009 à 16h20

Cas d'école

Les vols de matériels informatiques sur les lieux de travail prennent de l'ampleur,
D'après une étude réalisée par l'entreprise Kensington

Le 16 août 2016, par Miary, Expert éminent

Les pertes de données sont préjudiciables pour les entreprises. De ce fait, il est très important pour la DSI de mettre en place des stratégies de sécurité afin de protéger au maximum les données de l'entreprise. Cependant, il arrive souvent que les responsables de la sécurité informatique se concentrent davantage sur les moyens logiciels que matériels. Spécialisée dans les verrous de sécurité pour ordinateurs, l'entreprise Kensington a réalisé une étude basée sur l'utilisation des moyens matériels de sécurité auprès de 300 entreprises. Les résultats de son analyse ont montré que même si plus de la moitié des entreprises ont effectivement mis en place une politique sur la sécurité matérielle de leurs équipements informatiques, 23 % des vols d'ordinateurs se passent au sein même de l'entreprise.

Derrière une série d'attaques informatiques très puissantes, un réseau d'objets connectés piratés

Un réseau de caméras de surveillance piratées aurait permis à des pirates de mener des attaques informatiques d'une ampleur sans précédent.

LE MONDE | 26.09.2016 à 11h59 • Mis à jour le 26.09.2016 à 13h41

OVH visé

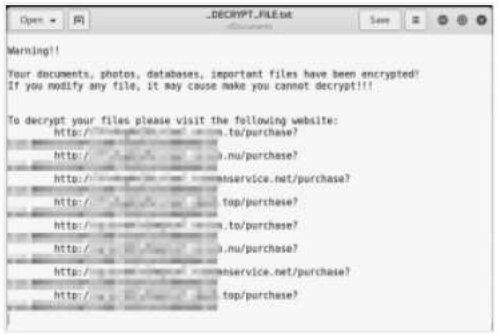
Coïncidence ? Le 22 septembre également, l'hébergeur et fournisseur d'accès français OVH était également victime d'une tentative de blocage massive – une série de 26 attaques simultanées de plus de 100 Gbps, affirme Octave Klaba, le PDG de l'entreprise sise à Roubaix. L'attaque a occasionné des dysfonctionnements temporaires sur le réseau d'OVH.

Cas d'école

LE 02 NOVEMBRE 2018 / MALWARE

L'Iran frappé par un malware plus violent que Stuxnet

Une variante du ver Stuxnet plus sophistiquée et dangereuse a ciblé l'infrastructure réseau de l'Iran. L'agence de la défense civile de ce pays ne s'est pas étendue sur...



LE 19 JUIN 2018 / MALWARE

Les systèmes Linux aussi terrorisés par les malwares

Les bots, backdoors, trojans et autres applications malveillantes qui attaquent le système d'exploitation Linux sont rares. Mais lorsqu'ils apparaissent, mieux vaut ne pas les...

TSMC contraint de fermer des usines à cause d'un virus

Sécurité : *Le fabricant de semiconducteurs, qui travaille notamment pc Nividia, a été obligé de stopper plusieurs usines dont les outils de product un virus informatique.*

Un ver mystérieux cible les machines à rayons X et les scanners IRM

Technologie : *Le groupe de hacker Orangeworm choisit soigneusement les victimes de ses attaques très ciblées.*

Introduction

Conséquences de ces sinistres

Toute panne ou perturbation devient préjudiciable pour l'entreprise :

- Arrêt de production
- Perturbation interne de l'entreprise
- Retard de la mise sur le marché d'un produit
- Fuite de technologie
- Diminution de la qualité de service
- Perte d'image
- …

Introduction

Principales causes

→ SYSTÈME (Installations par défaut, mauvaises configurations, erreurs de programmation, manque de protections,…)

→ RESEAU (**Manque de fiabilité** , virus, complexité, …)

→HUMAIN (**Absence de consignes, manque de formation**, négligence , erreur de manip, …)

→ORGANISATION (Manque de protections, pannes diverses, …)

Pourquoi les réseaux ne sont pas fiables ?

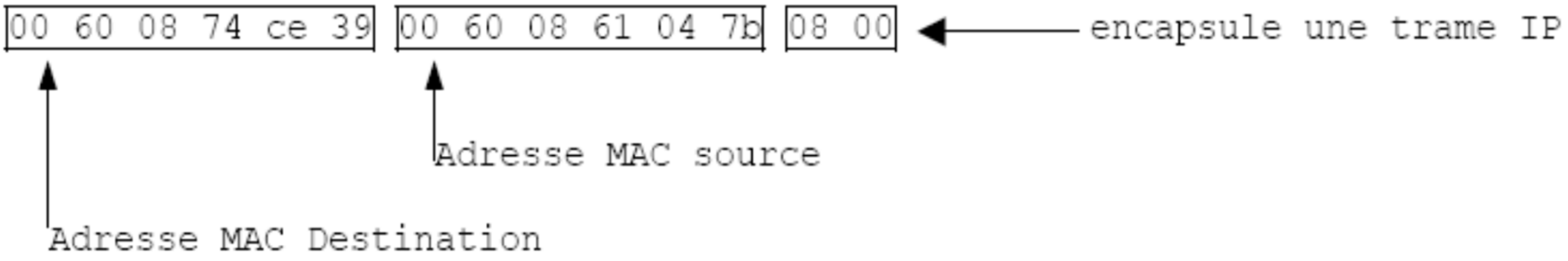
Exemple d’interception d’information

Une trame ethernet

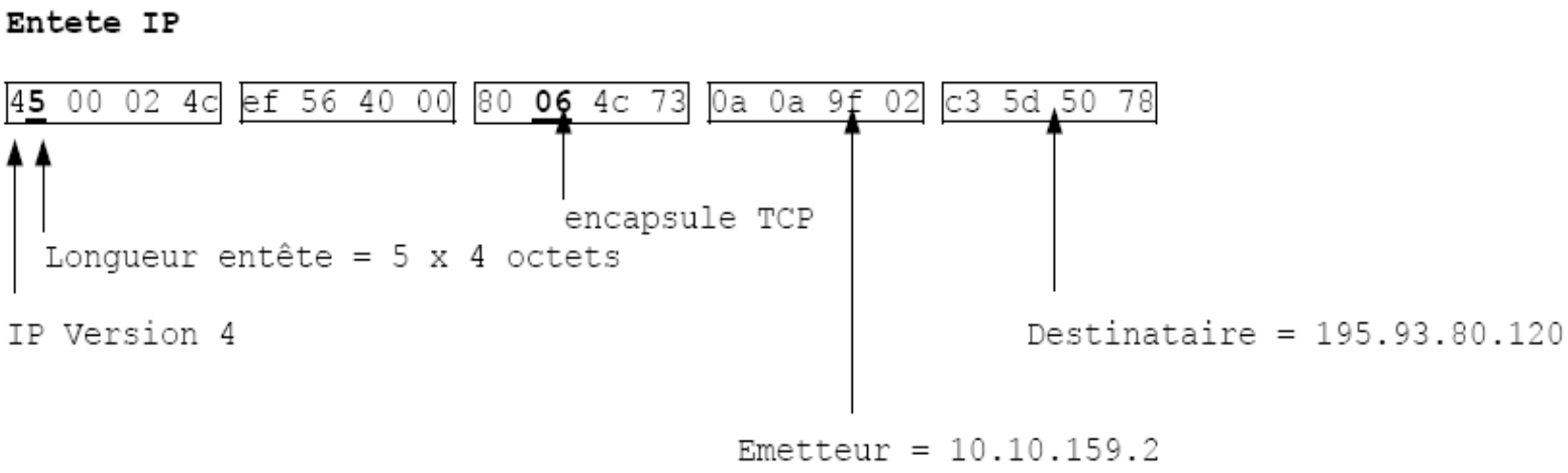
00 60 08 74 ce 39 00 60 08 61 04 7b 08 00 45 00 02 4c ef 56 40
00 80 06 4c 73 0a 0a 9f 02 c3 5d 50 78 0a 7b 00 50 15 35 05 44
4c 80 64 5f 50 18 22 38 b9 57 00 00 50 41 53 53 3a 54 4f 54 4f

Exemple d'interception d'information

Entête éthernet

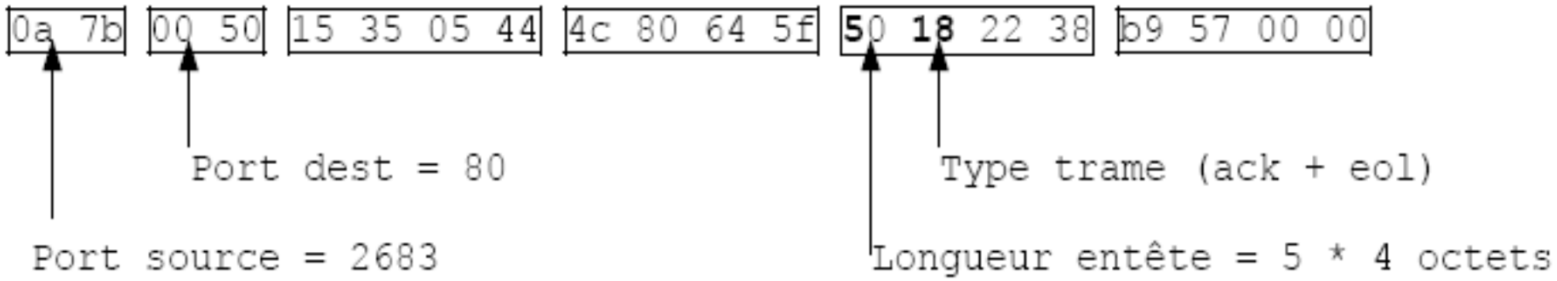


Exemple d'interception d'information



Exemple d'interception d'information

Entête TCP



Données TCP = Requête http (mais cela vous ne pouvez pas encore le deviner)

Exemple d'interception d'information

Les données transportées

00 60 08 74 ce 39 00 60 08 61 04 7b 08 00 45 00 02 4c ef 56 40 00 80 06 4c 73 0a 0a 9f 02 c3 5d 50 78 0a 7b 00 50 15 35 05 44 4c 80 64 5f 50 18 22 38 b9 57 00 00 50 41 53 53 3a 54 4f 54 4f

A l'aide une table ASCII on traduit les derniers caractères :

50	→	**P**
41	→	**A**
53	→	**S**
53	→	**S**
3a	→	**:**
54	→	**T**
4f	→	**O**
54	→	**T**
4f	→	**O**

Exemple d'interception d'information

Ce que l'on peut faire maintenant :

Localiser la machine d'adresse IP 195.93.80.120

Récupérer :
- les nom et version du serveur http
- les nom et version du système d'exploitation
- la liste des services ouverts

On pourra ensuite scanner les ports pour trouver les failles ou envoyer des mails avec des fichiers attachés.

Pourquoi « l'Humain » présente un risque ?

Fisching

LA BANQUE POSTALE

Désactivation de votre carte de crédit.

Bonjour .

Nous venons de désactiver votre carte de crédit.
Pour le réactiver, vous devez vous connecter sur le site de La Banque Postale et accéder à votre espace sécurisé de Banque en Ligne via le lien ci-dessous en saisissant vos identifiant et mot de passe ainsi que votre carte de crédit.

La procédure est trés simple :

1. Cliquez sur le lien ci-dessous pour ouvrir une fenétre de navigateur sécurisée.
2. Confirmez que vous étes bien le titulaire du compte et suivez les instructions.

accéder a votre compte

Ce Message est généré automatiquement, ne répondez pas à l'expéditeur.
Si vous n'étes pas destinataire(s) de ce message, merci de le détruire.

La Banque Postale, Société Anonyme à Directoire et Conseil de Surveillance, au capital de 2 342 454 090 euros
Siége social : 115, rue de Sévres - 75275 Paris Cedex 06 - RCS Paris 421 100 645 - Code A.P.E 6419Z.

Fisching

CHANGER L'ENERGIE ENSEMBLE

Chèr(e) Client(e),

Votre prélevement bancaire a été refusée par votre banque . Afin de regulariser votre situation veuillez vous refferez ci-dessous :

Cliquez ici pour résoudre ce problème.

Lors d'echec de regularisation de votre situation , nous procèderons à la suspension de votre fourniture d'energie. Cette intervention vous sera facturée.

Merci de votre confiance.

Dominique REMOND
Directeur Service Client

Comment lutter ?

Mettre en place des systèmes fiables en sécurisant tout ce qui concerne, de manière directe ou indirecte, le traitement de l'information.

→ La sécurité devient un enjeu stratégique et économique pour les entreprises et les particuliers.

Une prise de conscience, mais …

•La vision du risque encouru pour les données augmente ainsi de 29%→ 44% concernant les ordinateurs et de 30% → 42% concernant les smartphones ou tablettes.
•35% des internautes déclarent avoir subi au moins une perte de données durant ces 24 derniers mois sur leur ordinateur et 25% sur leur smartphone. La panne (27% et 25%, respectivement 'ordinateur' et 'smartphone'), l'erreur de manipulation (27% et 30%) et le virus ou piratage (21% et 15%) restent les trois raisons majeures invoquées lors de la perte de données sur un ordinateur.
•Au final , 43% (vs 32% il y a 2 ans) des internautes considèrent que les risques auxquels sont exposéés leurs données augmentent.

Source Clusir .

L’insécurité : les limites

En termes de comportements, les moyens de protection restent très ‘classiques’ : anti-virus (81%), pare-feu (80%), anti-spyware (77%) et anti-spam (76%).

La sécurisation des systèmes n’est pas une priorité :

- la sécurisation de la connexion wifi via une clé de chiffrement (77% inchangé en 2 ans),
- la sauvegarde des données sur divers supports (67% vs 69% 2 ans avant) .
- la mise en place de mots de passe au démarrage des sessions sur l’ordinateur personnel (59% inchangé en 2 ans).

Pourquoi ces limites

Mettre en place une sécurité efficace est complexe et couteux.

Plusieurs raisons :

- La sécurité concerne plusieurs aspects et/ou techniques,
- Il faut savoir ce que l'on veut sécuriser ,
- La sécurité a un coût,
- **Il faut sensibiliser et former les personnes,**
- …

Pourquoi il est difficile de sensibiliser les gens ?

Quelques chiffres à méditer

Avez-vous déjà été attaqué par un virus?

	UK	France	Allemagne	Espagne	Italie
Oui	70%	59%	69%	69%	69%
Non	24%	34%	25%	26%	29%
Ne sait pas	6%	7%	6%	5%	2%

Source: Yahoo mail global survey 24/05-9/06/2004

Quelques chiffres à méditer

comment votre PC est-il infecté par un virus

	UK	France	Allemagne	Espagne	Italie
en ouvrant un mail	14%	14%	17%	20%	20%
en ouvrant une pièce jointe	46%	30%	44%	39%	42%
avec les downloads	17%	15%	16%	15%	18%
directement via un site web	19%	2%	17%	12%	16%
par la proximité d'un autre pc infecté	1%	1%	0%	0%	0%
Ne sait pas	1%	17%	2%	6%	0%

Source: Yahoo mail global survey 24/05-9/06/2004

La sécurité à un coût, quelques chiffres …

Le spam

Un peu d'histoire (source Wikipédia)

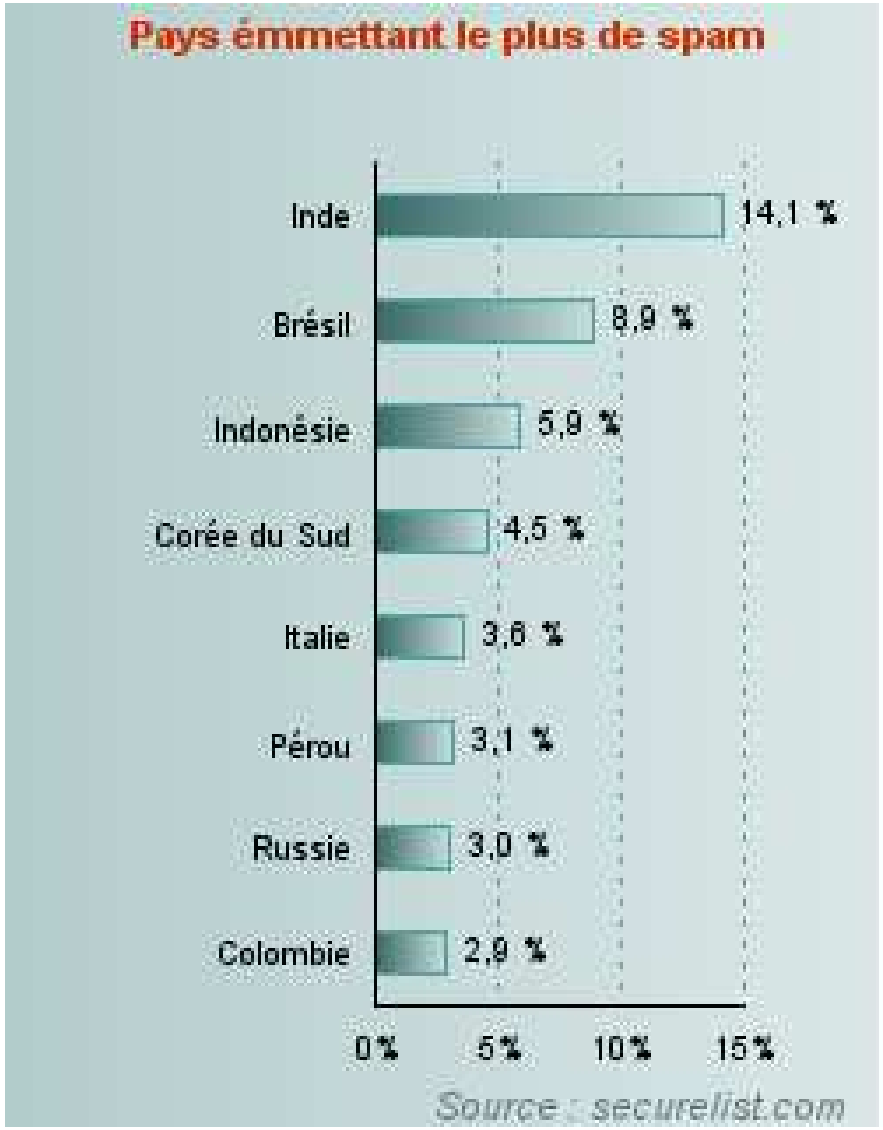
Le premier spam a été envoyé le 3 mai 1978 par Gary Thuerk2,3, marketeur travaillant chez DEC.

Il envoya son message à près de la totalité des utilisateurs d'ARPAnet (ancêtre d'Internet) vivant sur la côte ouest des États-Unis, soit environ 600 personnes.

Bill GATES à reçu jusqu'à 4 millions de mails par jour, pour 150 mails utiles.

Le spam

De 55% à 95% des mails reçus sont des spams



3,4 millions de spam par seconde
262 milliards de spams par jour
107 000 milliards de spams par an

Le spam

Combien vous coûte le spam ?

Nombre d'employés	100	employés
Salaire annuel moyen	40000	€
Nombre d'e-mails reçus / employé	50	messages / jour
% des spams sur les e-mails reçus	70	%

Calculer Réinitialiser

VADERETRO
E-MAIL SECURITY

Le spam

Voici le rapport des coûts cachés provoqués par le spam dans votre entreprise :

Perte de productivité

A force de faire le tri, chaque employé de votre entreprise perd annuellement (base de calcul : 5 secondes en moyenne par spam)	11.18 heures
Ajoutons l'effet de tentation par employé et par an (base de calcul : perte de temps de 20 minutes pour 1 spam sur 1000)	2.68 heures
Soit une perte de temps TOTAL par employé de	13.86 heures
Ce qui implique une charge cachée pour l'entreprise estimée à	30138.89 €

Le spam


Coût informatique
Le transfert et le stockage des spams impliquent une charge par employé de : (base de calcul : 1ct d'€ par spam)
80.50 €
Ce qui implique un coût informatique supplémentaire pour l'entreprise estimé à
8050.00 €
AU TOTAL, LE SPAM COUTE A VOTRE ENTREPRISE
38188.89 €

Le spam

SECURITE

Lutter contre les spams pour réduire ses coûts informatiques

Serveurs de messagerie saturés, dégradation des performances réseau, problèmes de stockage, pertes de productivité des employés : le spamming peut coûter très cher aux entreprises qui ne s'en protègent pas efficacement.

Partager :  Plus

Quelques chiffres - ddos

En 2018

2/3 des banques ont subis des DDoS

Les DDoS dans les banques américaines ont augmentés de 170 % ,

Entrainant des coûts de 32 560 dollars par minute de temps d’arrêt des systèmes.

Quelques chiffres

Evaluation des heures perdues à cause des attaques de virus

Heures perdues/semaine	%
0	48%
<1	31%
1-3	11%
3-12	6%
12+	3%
Moyenne par semaine	32 minutes
Moyenne annuelle	27,7 heures
Impact financier	3,3 Milliards $/an

Quelques chiffres

Sécurité informatique : des budgets en hausse

Les services en sécurité informatique à la hausse, selon Gartner

Plusieurs études se sont penchées sur les budgets informatiques en cette fin d'année 2017. C'est ainsi le cas d'une **étude Gartner**, qui pronostique **des dépenses informatiques en hausse de 7,6% pour atteindre 93 milliards de dollars en 2018**.

Cette même étude Gartner compare, au sein de ce budget sécurité, les différents segments de croissance. Selon elle, le segment qui disposera de la croissance la plus forte sera celui des **services de sécurité**, notamment englobant les dépenses liées **l'externalisation informatique**, au **conseil** et à la **mise en oeuvre**.

De plus, l'adoption de plus en plus importante des services délivrés en mode Cloud devrait entraîner une **baisse des dépenses liées aux équipements matériels**.

10,3% de croissance mondiale pour les dépenses sécurité informatique selon IDC

Source : ivision.fr

Plan du cours

Plan général du cours

1ère partie – Sécurité des systèmes

1 - Les risques et menaces

Failles des systèmes informatiques
Les menaces des systèmes
Les techniques d'attaques

2 - La protection

Protection de l'accès aux données
Protection dans les réseaux (Filtrages , pare feux,..)
Aspects juridiques

Plan général du cours

2eme partie – La cryptographie

1 – Introduction

- Techniques de base de la cryptographie
- Cryptographie à clés secrètes
- Cryptographie à clé publique
- Fonctions de hachage sécuritaire

2 - Protocoles de sécurité

- Méthodes de chiffrement par blocs, par flots
- Protocoles d'intégrité et d'authentification
- Protocoles d'authentification des usagers

3 – Mise en œuvre des protocoles de sécurité

- Infrastructures à clés publiques (PKI)
- Sécurité de la couche liaison (protection des réseaux WIFI)
- Sécurité au niveau transport : SSL, TLS.
- Sécurité des applications Web

Plan général du cours

3eme partie – Politique de sécurité

1 – Politique de sécurité

Notion de politique
Les étapes

2 – Analyse des risques

Objectifs
Méthodes d'analyse (Mehari, E-bios)
Tests d'intrusion