Introduction à la Cybersécurité

Université Claude Bernard – Lyon 1
Jean-Patrick Gelas

Sources

- Découvrez l'univers de la cybersécurité, Openclassrooms
- Effectuez votre veille en cybersécurité, Openclassrooms
-

Introduction

- Les incidents de cybersécurité font régulièrement les grands titres
  - Mots de passe volés
  - Données personnelles stockées en ligne volées
  - Sociétés qui se font voler les données de leur clients
  - Hôpitaux paralysés
- On recense des milliers d’attaques chaque année.

- Objectifs :
  - Comprendre pourquoi entreprises, gouvernements et particuliers doivent se préoccuper de cybersécurité.
  - Identifier les risques liés à la cybersécurité.

La cybersécurité avant (90-2000)

- Un antivirus (et un *firewall)* suffisaient
- Acte d’individus isolés
- Vecteur principal : échanges de disquettes
- Risque majeur : effacer tous les fichiers

La cybersécurité aujourd'hui

- Un monde hyperconnecté
- Plus de données stockées en ligne
- Plus d'usage de l'informatique pour des applications critiques (électricité, hôpitaux,...)
- On observe :
  - ***Data breaches*** : accès aux BdD confidentielles
  - ***Ransomwares*** : nouveau type de virus, chiffre les données, clé de déchiffrement payante.
  - **Mise en péril d'infrastructure** : impact sur le monde réel.

L'impact n'est plus théorique mais bien réel !

Wannacry


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Qui et pourquoi ?

- Rarement le fait d'individu isolés
- Réalisé par des groupes coordonnés avec divers motivations :
  - Cybercriminalité : pour s'enrichir
  - Atteinte à l'image : pour décrédibiliser un individu
  - Espionnage : pour récupérer des informations secrètes
  - Sabotage : déclencher une panne
- Tout le monde est concerné : Personne n'est à l'abri.

Quelques attaques célèbres

- Sony pictures (info privées, email, films, serveurs effacés), 2014
- Equifax (credit checker), 2017
- Hopitaux (UK, FR) : Wannacry
- …

Ce qu'il faut retenir…

- Si une information est confidentielle ne l'enregistrez pas
- Si vous devez l'enregistrer utilisez un système de chiffrement puissant (GPG pour vos emails)
- Mettre à jour les logiciels (corrections de failles)
- Faire des sauvegardes régulières sur un système de stockage entièrement séparé.
- Le délai que vous mettrez a communiquer sur un piratage sera analysé
- La façon dont vous réagirez également
- L'ANSSI (Agence National de Sécurité des SI) recommande de ne pas payer

Les moyens d'attaques

- Certaines attaques sont sophistiquées, mais beaucoup ne le sont pas tant que ça.
- On peut les classer en 4 catégories :
  - **Failles logicielles** : bug -> mise à jour
  - **Failles réseaux** : échanges non chiffrés, connexion à un serveur (vol de *cookie*, mot de passe faible ou par défaut)
  - **Droits d'accès** : donner des droits d'accès nécessaire à chaque personne et pas plus.
  - **Ingénierie sociale** : **...** (cf. diapo suivante)

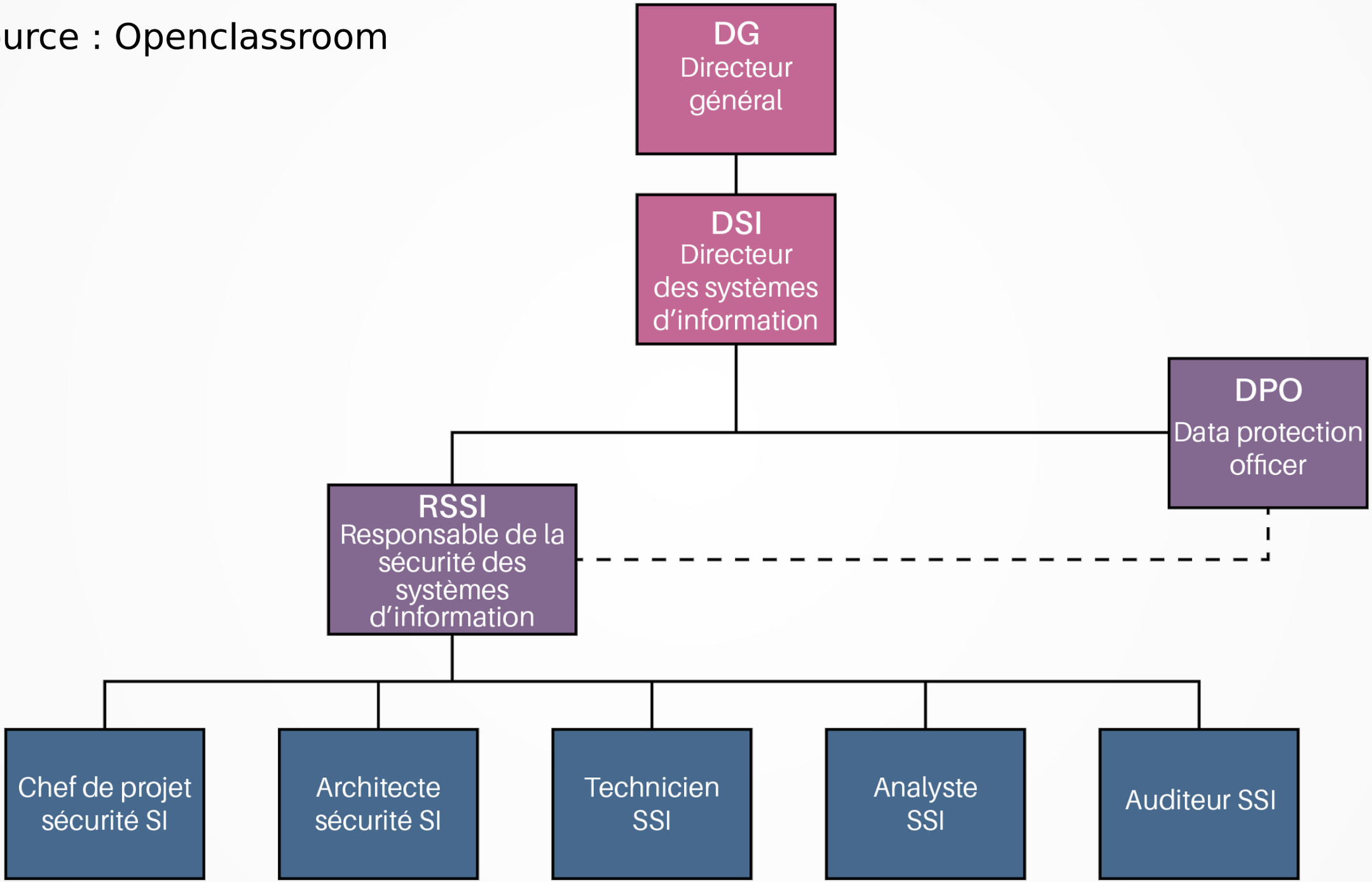
Ingénierie sociale

- Vecteur d’attaque le plus populaire → exploiter la faille humaine.
- Astuces :
  - Se faire passer pour un supérieur (au téléphone)
  - En jouant sur les sentiments
  - En jouant sur l’urgence
  - En utilisant une copie d’un site (*phishing*)
  - … (les pirates ne manquent pas d’imagination…)

Les métiers de la cybersécurité

- Le domaine de la cybersécurité embauche
- Le budget des entreprises en matière de cybersécurité est estimé à 96 milliards de $ (2018)

Source : Openclassroom



Veille en cybersécurité

- Chaque jour de nouveaux **risques** et de nouvelles **failles de sécurité** sont découverts → Danger pour vos données et systèmes !
- Nécessité de mettre en place une veille efficace pour :
  - Collecter les informations
  - Assurer une connaissances des vulnérabilités
  - Communiquer/Sensibiliser ses interlocuteurs (équipes, manager, direction)

Le référencement des vulnérabilités

- Les vulnérabilités sont référencées et classées au niveau mondial.
- Le système CVE (*Common Vulnerabilities and Exposures*)
- Le CVE est un dictionnaire qui référence toute vulnérabilité sous la forme **CVE-AAAA-NNNN**
  AAAA est l'année de publication et NNNN le numéro d'identifiant.

Vulnerability Details : CVE-2018-17197

A carefully crafted or corrupt sqlite file can cause an infinite loop in Apache Tika's SQLite3Parser in versions 1.8-1.19.1 of Apache Tika.

Publish Date : 2018-12-24 Last Update Date : 2019-01-10

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

- CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	400

- Products Affected By CVE-2018-17197

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Apache	Tika	1.8				Version Details Vulnerabilities
2	Application	Apache	Tika	1.9				Version Details Vulnerabilities
3	Application	Apache	Tika	1.10				Version Details Vulnerabilities
4	Application	Apache	Tika	1.11				Version Details Vulnerabilities
5	Application	Apache	Tika	1.12				Version Details Vulnerabilities
6	Application	Apache	Tika	1.13				Version Details Vulnerabilities
7	Application	Apache	Tika	1.14				Version Details Vulnerabilities
8	Application	Apache	Tika	1.15				Version Details Vulnerabilities
9	Application	Apache	Tika	1.16				Version Details Vulnerabilities

Score CVSS

- Le score CVSS est un indicateur de la gravité de la faille, basé sur des critères objectifs et mesurables.
- Les métriques **d'exploitation** recouvrent :
  - le vecteur d’accès (local, réseau local, réseau) ;
  - la complexité d’accès (basse, moyenne, haute) ;
  - l'authentification (multiple, simple, inexistante).
- Les métriques **d’impact** incluent :
  - la confidentialité ;
  - L'intégrité ;
  - la disponibilité.

Comment s'informer ?

- Les CERT (*Computer Emergency Response Team)*, sont des centres d'alerte pour les attaques informatiques.
- Les trois CERT français :
  - le CERT-FR, centre gouvernemental de veille, d'alertes et de réponses aux attaques informatiques pour l'administration (https://www.cert.ssi.gouv.fr/);
  - le CERT RENATER pour le secteur universitaire ;
  - le CERT-IST pour l'industrie, les services et le tertiaire.

Rappels

- emails
  - On vérifie l'adresse email de l'expéditeur entre chevrons.
    Ex : **`LinkedIn <er@vh310.timeweb.ru>`**
  - On ne clique pas sur les liens
  - On n'ouvre pas un fichier en pièce jointe
  - On décline l'affichage des images
- Web
  - Avant de s'authentifier on vérifie : **`https`** (cadenas) et le nom de domaine.
  - Lire le lien en bas à gauche avant de cliquer.
- Mots de passe
  - On ne communique pas son mot de passe
  - On active la 2FA quand c'est possible
- Autres
  - Utiliser des mots de passe solide (longs) et un gestionnaire de mot de passe
  - Chiffrer son disque dur

Liste de vidéos

- Hack célèbres
  - Sony picture : https://www.youtube.com/watch?v=EAQxElHsySw
  - Equifax (credit checker):
    - https://www.youtube.com/watch?v=_6Qbslgpw8U
    - https://www.youtube.com/watch?v=Y1BwWYVYS2E
  - Jeff Bezos phone hacked : https://www.youtube.com/watch?v=hZbVW04Ohjk
  - Twitch : https://www.youtube.com/watch?v=VDwHUrZrT0U
- Social engineering :
  - Vishing (voice phishing): https://www.youtube.com/watch?v=lc7scxvKQOo
  - Web page : https://www.youtube.com/watch?v=PWVN3Rq4gzw
- Physical access
  - Lockpicking : https://www.youtube.com/watch?v=TjRj69P5rKM
  - Tailgating : https://www.youtube.com/watch?v=1fmLds7EZXs