



CyberEdu

La sécurité par l'enseignement supérieur des NTIC

IUT de Cergy, 4/4/2019

julien.breyault@cyberedu.fr

Vice Président de CyberÉdu

Responsable de formation LP ASSR

IUT de Sénart

Présentation

- Enseignant et administrateur systèmes et réseaux
- Responsable de formation LP en administration et sécurité des systèmes et réseaux
- Spécialisation dans la gestion des compétences, la FTLV (FC, FA, VAE, VAPP..) et l'enseignement à distance



- Vice-président de



On est tous concernés

- pro et particuliers
- 2 foyers sur 5 ont des périphériques connectés non sécurisés
- 3/4 à cause d'identifiants faibles
- 1/3 à cause de mises à jour tardives
- Mot d'ordre de l'ANSSI au FIC 2019 :
*« tous connectés,
tous impliqués,
tous responsables »*

ANSSI/Talents du numérique, FIC 2019: constat

"L'enjeu formation est décisif dans un domaine en croissance à 17%, avec des objets connectés qui se multiplient et des recrutements difficiles"

- En 2018 :
 - une hausse des effectifs de 6%
 - 1 400 créations nettes d'emplois
(dans un domaine qui en compte déjà 24 000, dont 7/10 en IDF)
- Plusieurs dizaines de milliers d'emplois en France d'ici 2022.
- Seulement 1200 postes pourvus sur les 6000 ouverts en 2017 en France

<https://talentsdunumerique.com/communiqués-presse/competences-et-cybersecurite-2019>

- **Compétences techniques :**
 - sécurisation des applications,
 - gestion des accès et des identités / protection des informations
 - audit de sécurité / supervision/ gestion de la continuité d'activité
 - infrastructure et réseaux
 - programmation et cryptographie,
- **Les compétences transversales (« softskills ») jouent également un rôle important :**
 - adaptabilité/flexibilité et réactivité,
 - respect des règles de confidentialité,
 - curiosité (veille),
 - capacité d'analyse, d'anticipation,
 - communication orale/écrite fluide,
 - pratique de l'anglais (pro.),
 - culture générale en matière de géopolitique et d'intelligence économique,
 - maîtrise des enjeux juridiques (non limités au RGPD) – une matière dans laquelle des lacunes sont souvent identifiées chez les étudiants.

ANSSI/Talents du numérique, FIC 2019 + OPIIEC: évolutions

- Intégrer le sujet « cybersécurité » à tous les cursus supérieurs, même généralistes
- Accompagner la mobilité professionnelle et la montée en compétences des salariés

La commission recommande aux établissements de formation de s'intéresser
- au programme CyberÉdu (pour les étudiants du numérique non spécialistes) et
à la labellisation pour les responsables de formation,
- et de demander le label SecNumedu (pour les formations de spécialistes)

- Une alerte néanmoins : le secteur souffre d'un déficit d'attractivité...
Des actions de communication d'envergure, notamment vers les jeunes et le grand public, sont indispensables.

Trop souvent réduite à son aspect technique, la cybersécurité ne séduit pas.

- **Catégorie 1 : Hygiène numérique**
 - BTS, IUT, licences ou diplômes d'informatique non spécialisés en cybersécurité,
 - personnels des administrations et des entreprises,
 - plus largement tous ceux qui utilisent des moyens numériques dans leur emploi.
- **Catégorie 2 : Formation complémentaire**
 - Personnels des systèmes d'informations et des communications,
 - acquérir ou de mettre à jour des connaissances et compétences nécessaires à leurs métiers.
- **Catégorie 3 : Formation à la cybersécurité**
 - Formations pour les spécialistes des systèmes d'information à la cyber-protection, à la cyberdéfense et à la cyber-résilience .
- **Catégorie 4 : Experts techniques**
 - ... et responsables spécialisés de haut niveau dans les disciplines de pointe, telles par exemple la cryptologie, le forensic (investigation numérique) ou le pentest (test d'intrusion),...
 - pouvant aller jusqu'à des certifications.
- **Catégorie 5 : Conduite des opérations cyber**
 - Formations pratiques, pour des généralistes de la conduite des opérations « cyber »
 - pouvant aller jusqu'à la gestion des crises : le Mastère spécialisé Gestion des crises cyber que propose Saint-Cyr Coëtquidan, ou le diplôme d'ingénieur Cyberdéfense de l'ENSIBS par exemple.

Quelques Dates

- Depuis 2006 : de nombreux rapports :
 - La France n'est pas préparée face aux Cyber attaques
- Livre Blanc Défense & Sécurité Nationale 2013
 - La cyber défense devient un enjeu national
 - La cyber sécurité dans l'enseignement supérieur
 - ANSSI lance son appel d'offre
- Stratégie Nationale de la Sécurité du Numérique
 - Présentée par M. Manuel Valls le 16 Octobre 2015
 - Portée depuis 2016 par la CPU et la CGE

Les atouts de CyberÉdu

Pour les étudiants :

- une vision transversale du système d'information,
- des mesures d'hygiène minimales,
- les bases pratiques en systèmes et réseaux,
- l'aspect légal de la cybersécurité.

Pour les formations :

- un accompagnement dans l'élaboration des parcours,
- des ressources libres disponibles,
- une associations d'échange autour des pratiques,
- une visibilité/labellisation.

CyberÉdu – Missions

- Accompagner les enseignants (utilisation et production)
- Enrichissement du fond de supports pédagogiques
 - GT-Supports (Creative Commons BY), GT-Labelisation (ANSSI)
- Attribuer le label CyberEdu aux formations (valorisant)
- Adhésion des établissements → amplifier la dynamique
- Colloques sur le territoire
- Communication et événementiel (FIC, ...)
- Tisser des relations avec les autres associations
 - ARCSI – Réservistes du Chiffre et de la Sécurité de l'Information
 - ADIUT et CRI-IUT en lien avec les IUTs
 - SupDPO– DPD de l'Enseignement Supérieur
 - CEFCYS – Association des Femmes de la Cyber sécurité
 - AFCDP – Informatique et Libertés dans les entreprises

CyberÉdu – Mallette Pédagogique

- Guide pédagogique d'intégration dans les formations
 - Enseignement basé sur la protection principalement
- Modules de sensibilisation (bac+2/3)
 - Syllabus (introduction) et Quizz (conclusion)
 - Module 1 → Cyber sécurité : notions de base 5h
 - Module 2 → Les règles d'hygiène informatique 6h
 - Module 3 → Les aspects réseaux et applicatifs 4h
 - Module 4 → La gestion de la cybersécurité 3h
- Ensemble de supports pédagogiques de cours (M1/2)
 - Fiches sécurité des OS
 - Fiches sécurité des réseaux
 - Fiches sécurité des logiciels
 - Fiches sécurité des composants
 - Fiches sécurité authentification

CyberÉdu – mise en œuvre

- Parcourir l'ensemble des enseignements pour voir lesquels sont les « bons » candidats (réfèrent interne nécessaire):
 - L'informatique
 - Le droit
 - La communication/expression
 - Gestion des entreprises
 - L'anglais
 - Les projets tutorés
- Et/ou, moins contraignant :
 - Créer un module spécifique faisant le point en fin de formation
 - > Dans tous les cas : il faut faire pratiquer les outils

Phishing, vol d'identités, ransomwares...

- Messages infectés
- Clés USB/cartes SD infectées
- Logiciels compromis
- Sessions laissées ouvertes
- Saisies clavier non discrètes
- Écrans visibles de tous dans des lieux publics
- Compromission de mails perso pour toucher la partie pro
- Mots de passe faibles
- ...

Hack académie

- <https://www.hack-academy.fr>
- On va voir aujourd'hui comment y faire face et mettre en place des outils ensemble

- Qu'est-ce qu'il est le plus important de protéger au niveau informatique ?

- Dans TIC, NTIC, SI, ... il y a information (et communication)

→ Le plus important est l'information et comment on la diffuse/protège

- Comment évalue-t-on la sécurité globale d'un système ?

- Comment évalue-t-on la sécurité globale d'un système ?

→ La sécurité globale d'un système et celle de son maillon le plus faible...



GUIDE D'HYGIÈNE INFORMATIQUE

RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

- Il faut protéger en profondeur car :
 - La sécurité à 100 % n'existe pas
 - Et le risque 0 donc non plus

et aussi :

<https://www.ssi.gouv.fr/guide/guide-des-bonne-s-pratiques-de-linformatique/>

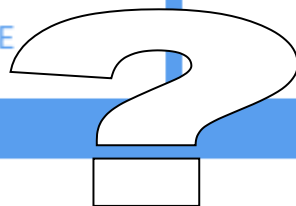


';-- have I been pwned ?

- <https://haveibeenpwned.com/>
- Check if you have an account that has been compromised in a data breach
- Alors ?
- Essayez aussi <https://www.shodan.io/>

HAMEÇONNAGE

LÉGITIME



Luke Johnson <luke.json8000@gmail.com>

à moi

11:02

Adresse connue
mais pas tout à
fait identique ?

Luke Johnson a partagé un lien vers le document suivant :

 Budget département 2019.docx



Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

Ouvrir dans Docs

Liens non officiels/fichier non attendu

<http://drive-google.com/luke.johnson>

Ne pas s'identifier !

<https://phishingquiz.withgoogle.com/>

Mots de passe

- Le problème/dilemme en pratique :
- Les mots de passe peuvent être complexes

c a q u a i) w # a e 3 U p 3 A

ou

- modifiés régulièrement
- t o t o 2 , t o t o 3 ...
- Pourtant les deux sont nécessaires ;-)

Trousseau de mots de passe



C'est LA solution !

- Coffre-fort numérique
- Chiffré par mot de passe maître
- Mdp générés de 12 à 16 caractères aléatoires (min./maj., chiffres, caractères spéciaux)
- Ne pas enregistrer les mdp sur le navigateur (copier-collé sécurisé)
- Keepass est certifié par l'ANSSI
- Atelier de prise en main accompagné par les LP Sécurité des données en fin de conférence

Trousseau de mots de passe, sécurisation

- Possibilité d'utiliser un outil contre le vol de mdp maître (second facteur d'authentification):
 - Carte à puce, clé USB/NFC,
 - empreinte biométrique,
 - mot de passe à usage unique (OTP), éventuellement via SMS



Dear User,
Your OTP is
176359

- ne pas donner d'informations permettant, par ingénierie sociale de déduire mots de passe, identifiants...
- ne pas donner d'informations de localisation

<http://pleaserobme.com/>

Réseau

- mdp wifi complexe et modifié régulièrement (utiliser keepass)
- attention à la portée/débordement
- éviter les réseaux wifi publics (ou alors avec VPN),
- éviter les VPN publics également (préférer ceux fournis par des prestataires de confiance, nationaux de préférence, et avec authentification forte)



Systemes

- compte utilisateur non administrateur (pas root/jailbreak), 1 compte par personne
- pare-feu/antivirus intégrés au système d'exploitation (à rajouter pour les Mac)
- mises à jour quotidiennes du matériel, système, des pilotes (en changer si elles ne sont plus fournies ou pas assez souvent)
- filtre de confidentialité dans les lieux publics
- activer le blocage de session lors d'inactivité (courte)
- éteindre l'ordinateur lors d'inactivité prolongée
- ne pas utiliser un ordinateur public ou partagé pour accéder à des comptes critiques de type mail/cloud/banques..

Applications

- Les limiter au **strict nécessaire** (attention aux plugins navigateur)
- **fournisseur officiel** (store ou site du développeur/éditeur)
- **mises à jour quotidiennes** si intégrées à l'application (par ex navigateur)
- vérifier le « **degré de confiance** » : les droits qui sont demandés, l'éditeur, la dernière mise à jour, les commentaires,...
- attentions aux applications "gratuites" (mais pas libres) qui sont souvent des pièges, au mieux pour de la pub, au pire pour prendre le contrôle de l'ordinateur

→ <http://references.modernisation.gouv.fr/socle-logiciels-libres>

Données

- chiffrement des disques
 - tout ce qui est mis dans le cloud doit être chiffré (au moins par mot de passe) si ce sont des données personnelles et/ou confidentielles
 - idem pour ce qui est mis sur des supports portables/perdables/volables...
 - ne pas copier/connecter de données pro sur des supports perso et inversement
 - sauvegarde+archivage planifiés et automatiques
 - + test de restaurations réguliers (si tout le monde appliquait cette recommandation les ransomwares disparaîtraient)
- appliquer en priorité aux informations sensibles/de valeur

En cas d'incident :

<https://www.ssi.gouv.fr/en-cas-dincident/>

- Spam: <https://www.signal-spam.fr/>
- Contenu illicite:
<https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>
- Assistance aux victimes: <https://www.cybermalveillance.gouv.fr/>
- Bons réflexes en cas d'intrusion (admins sys):
<https://www.cert.ssi.gouv.fr/information/CERTA-2002-INF-002/>
- Ne pas payer de rançon !
<https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001/>
- déconnecter du réseau filaire/radio/cablé (3g, wifi, bluetooth, USB,...)

Après l'incident :

- réinstallez complètement le système d'exploitation à partir d'une version saine
- +BIOS/UEFI,
- restaurez les données d'après une copie de sauvegarde non compromise,
- changez tous les mots de passe

Secnumacadémie... pour aller plus loin

- MOOC de sensibilisation de l'ANSSI :
<https://www.secnumacademie.gouv.fr/>

Sources/liens

<https://talentsdunumerique.com/sites/default/files/public/2019-01-note-tdn-competences-cybersecurite.pdf>

<https://www.fafiec.fr/85-L-observatoire-opiiec/etudes-transversales/459-formations-competences-france-cybersecurite.html>

<http://cigref.hr-ingenium.com/accueil.aspx>

<https://www.imt.fr/formation/debouches-et-metiers/barometre-metiers-numerique/>

<https://business.lesechos.fr/directions-numeriques/metier-et-carriere/parcours/0301348177395-les-femmes-boudent-toujours-la-cybersecurite-319154.php>

<https://theconversation.com/les-metiers-de-la-securite-du-numerique-sont-ils-reserves-aux-hommes-100696>

<https://www.capdigital.com/notre-vision/nos-ressources/>

<http://www.onisep.fr>

<http://www.enseignementsup-recherche.gouv.fr/cid20181/la-licence-professionnelle.html>

<https://www.trouvermonmaster.gouv.fr/>

<http://www.cti-commission.fr/>

<http://www.cge.asso.fr/>

<http://www.cncp.gouv.fr/>

<https://www.ssi.gouv.fr/entreprise/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/>

<http://www.data.gouv.fr/fr/datasets/referentiel-des-metiers-et-competences-des-systemes-dinformation-et-de-communication-sic/#resource-f933e725-e031-4f7b-ab41-be6e0fb9ac1d>

<https://infos.emploipublic.fr>

<https://www.ssi.gouv.fr/recrutement/>

<https://www.cyberjobs.fr>

<https://www.ssi.gouv.fr/actualite/decouvrez-la-diversite-des-metiers-de-la-securite-numerique-avec-le-panorama-de-lanssi/>

<https://www.ssi.gouv.fr/uploads/2018/10/kit-presse-panorama-des-metiers-de-la-securite-du-numerique.pdf>

<https://www.ssi.gouv.fr/entreprise/formations/secnumedu/>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-181.pdf>

<https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

<https://www.cyberedu.fr>

<https://www.secnumacademie.gouv.fr/>

<https://www.cnil.fr>

<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

<https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/>

<http://references.modernisation.gouv.fr/socle-logiciels-libres>

<https://www.qwant.com/>

Merci !

Julien BREYAULT

<julien.breyault@cyberedu.fr>

Vice-président de CyberÉdu

IUT de Sénart-Fontainebleau / UPEC

contact@cyberedu.fr

information, adhésion, groupes de
travail

www.cyberedu.fr

colloques, communications,
supports pédagogiques,
labellisation