esiea

Laboratoire de cybersécurité CNS

Confiance Numérique & Sécurité

Intervention au profit du coTer numérique

Les villes « cyber-responsable »

07/06/2021

Richard REY (Rexy)

richard.rey@esiea.fr

Sensibilisation à l'hygiène informatique

esiea

Confiance Numérique & Sécurité

Les risques actuels

Vos comptes et vos mots de passe

La sauvegarde de vos données sensibles

Le télétravail

- Software Engineering
- Intelligence Artificielle & Data Science
- Réalité Virtuelle et Systèmes Immersifs
- Systèmes Embarqués et Autonomes
- Cybersécurité

SecNumedu ANSSI

- Association labellisée EESPIG (Établissement d'Enseignement Supérieur Privé d'Intérêt Général)
- Formation **initiale** (de la 1re à la 5e année) labellisée **CTI** (Commission des Titres d'Ingénieur)
- Formation par la voie de l'**apprentissage** (cycle ingénieur)
- Formations **spécialisées cyber** labellisées CGE (Master Spécialisé et Badges)

MSc Mastère spécialisé

Laboratoire CNS (Confiance Numérique et Sécurité)

- **Genèse :** Il est l'héritier d'un laboratoire militaire de l'École des Transmissions de Rennes (COMSIC/ETRS)
- **Thèmes privilégiés :** Éthique et droit en SSI, audits et tests d'intrusion (pentest), cybersurveillance, sécurité des objets connectés, investigation numérique (forensic), sécurité physique, cryptologie et stéganographie.
- **Production :**
  - Ingénierie pédagogique et production de cours ;
  - Contrats opérationnels intégrant nos étudiants : audits , tests d'intrusion, cybersurveillance, sensibilisations, campagnes de phishing, etc.
  - R&D et projets opérationnels : ALCASAR, checkmyhttps, OpenSOC, calculateur cryptographique, station blanche, iotrust (analyse d'objets connectés), etc.
  - Communication : publications, conférences, reportages et articles.

Interventionau profit du coTer numérique

- 05/2021 : Plan de relance cyber 136M€ (https://www.senat.fr/presse/cp20210511a.html) 60M€ pour la mise en place de « centres de réponse cyber (csirt*) » régionaux destinés à soutenir localement les acteurs de taille intermédiaire victimes de cyberattaques (PME, ETI, collectivités et établissements publics).

- Accompagnement national : cybermalveillance.gouv.fr (250 demandes d'assistance par mois depuis 6 mois)

- Accompagnement régional :
  - Délégué cyber : Philippe Loudenot (philippe.loudenot@paysdelaloire.fr)
  - Correspondant ANSSI : Régis DUBRULLE (regis.dubrulle@ssi.gouv.fr)
    - analyse de votre A.D + audit de l'exposition de votre S.I. sur Internet

Région PAYS DE LA LOIRE

CSIRT = Computer Security Incident Response Team

Interventionau profit du coTer numérique

label "Ville cyber-responsable"

Souligner les efforts des mairies engagées dans une démarche **d'amélioration** de leur cybersécurité (quelque soit le point de départ).

→ Désignez un "cyber champion" (ni le maire, ni le responsable informatique ;

→ Questionnaire "Immunité cyber" (neuf questions relatives aux points critiques de la sécurité informatique d'une commune) ;

→ Formalisez un plan d'action cyber (sensibilisation, audit et actions correctives).

Pour aller plus loin

- Les guides des bonnes pratiques de l'ANSSI. Ils sont **pragmatiques, réalistes et lisibles.** Exemples :
  - Sécurité numérique des collectivités territoriales (réglementation) ;
  - Bonnes pratique à l'usage des pro en déplacement ;
  - Attaque par Rançongiciels : comment réagir.

- Poursuivez la sensibilisation (séances, campagne de phishing, affiches) : Témoignages d'élus sur cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

- Le guide de sécurité numérique pour les petites et moyennes collectivités territoriales du PEC (Pole d'Excellence Cyber)

PÔLE D'EXCELLENCE CYBER

Pour aller plus loin

Vidéos AFP :

- La cybercriminalité : http://www.dailymotion.com/video/x2srjfl_la-cybercriminalite_news
- Les outils du pirate : http://www.dailymotion.com/video/x340z37_la-boite-a-outils-du-hacker_news
- Les ransomwares : http://www.dailymotion.com/video/x4w49i8_ransomware-la-prise-d-otage-informatique_news

- Les analyses de sécurité : audits de sécurité, tests de pénétration (pentest), analyse de serveurs, etc.

- Cybersurveillance de son S.I. par un Security Operation Center (S.O.C)

Interventionau profit du coTer numérique

MINISTÈRE
DE L'ÉCONOMIE
DES FINANCES
ET DE LA RELANCE
Liberté
Égalité
Fraternité

COMMUNIQUE DE PRESSE

Paris, le 21 mai 2021
N°1031

Bruno Le Maire et Olivier Dussopt félicitent les douaniers enquêteurs de la DNRED qui viennent de démanteler la plateforme « le monde parallèle » et ses activités illégales sur le Darknet.

Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance et Olivier Dussopt, ministre délégué chargé des Comptes publics, félicitent les douaniers enquêteurs de la Direction Nationale du Renseignement et des enquêtes Douanières (DNRED), qui viennent de démanteler la plateforme « le monde parallèle » et ses activités illégales sur le Darknet.

Quelques opérations médiatisées :

- 2018 : Forum « Black Hand »
- 2019 : Plateforme « French Deep Web Market »
- 2020 : Arrestation d'un groupe de 106 mafieux italiens
- 2021
  - Plateforme LMP (Le Monde Parallèle)
  - Double VPN + Sky ECC + Encrochat
  - 2 opérateurs ukrainiens de ransomwares (500K€ + 1M$ en bitcoin)

Ces opérations mobilisent des dizaines d'opérationnels, d'analystes et de spécialistes pendant plusieurs mois.

Interventionau profit du coTer numérique

EUROPOL

Les risques actuels

Vos comptes et vos mots de passe

La sauvegarde de vos données sensibles

Le télétravail

FEEDBACK - IT (technical)

Systems

- **Deprecated systems** (no more updates) or **Systems without their updates**
- **AD** analyzes:
  - **Passswords management (too simple/small, old, anti brute-force attack, etc.)**
  - **Too powerful users** (too many rights) and a lot of **unused users**
  - Nobody looks the audit system (authentication failures)
- **Laptop/PC analyze**
  - **BIOS restriction**
  - **Non-ciphered data zone (internal folders or external disk) → Bitlocker / veracrypt / 7zip / ...**
  - **Too powerful users** - Local admin account → LAPS (Local Admin Password Solution)
  - Whitelist/blacklist applications restriction with GPO → "SRP - Software Restricted Policies" (Vista and before), Applocker (>= W7 enterprise)
  - **Non managed network connection (3G/4G)**