UNETP LAB

JEUDI 14 MARS 2024

17.00 – 18.30

ANIMATEURS

- Emmanuel Ferron, Aline Gaté et Eric Hans, Administrateurs

NOMBRE DE PARTICIPANTS

- 23

RAPPEL DES PRINCIPES DE NOTRE TEMPS DE TRAVAIL

- Un temps et un espace partagés où la parole est libre
- Approche coopérative et mutualiste
- Des apports spécifiques aux différents points abordés sont faits
- Chacun fait l'effort d'apporter une expérience ou une idée

THÈME NUMERO 21 :

La cybersécurité

- Risques encourus par un établissement scolaire
- Comment travailler sur la cybersécurité dans le cadre d'un établissement scolaire ?
- Les règlements intérieurs des élèves et des personnels sont-ils adaptés à la cybersécurité ?
- Le RGPD
- La e-réputation
- Qui sont les partenaires internes et externes de ce travail ?
- ...

AXES TRAITÉS :

Introduction

La cybersécurité ou sécurité informatique fait référence à l'ensemble des mesures, des pratiques et des technologies mises en place pour protéger les systèmes informatiques, les réseaux, les données et les dispositifs contre les menaces, les attaques et les intrusions potentielles. Ces menaces peuvent provenir de diverses sources telles que des pirates informatiques, des logiciels malveillants, des attaques par déni de service (DDoS), des tentatives de phishing et d'autres formes d'activités malveillantes en ligne.

L'objectif de la cybersécurité est de garantir la confidentialité, l'intégrité et la disponibilité des données et des ressources informatiques essentielles. Pour y parvenir, les professionnels de la cybersécurité mettent en œuvre une gamme de stratégies et de technologies.

Les experts présents

- Bruno Bonnat (Responsable Informatique Saint Dominique à Pau)
- Matthieu Collet (responsable informatique La Croix Rouge à Brest)
- Vincent Douchet (responsable informatique Saint Croix Saint Euverte à Orléans)
- Simon Nadot (Praeventia – accompagnement du risque cyber auprès de la MSC)

A travers les interventions et échanges techniques mais néanmoins passionnants autour de la cybersécurité, plusieurs points sont revenus régulièrement, dont un primordial : le risque est le plus souvent dans l'humain. Une étape clé de la cybersécurité : **la sensibilisation de tous les acteurs de nos communautés éducatives** (élèves, enseignants, personnels administratifs).

Nous avons tenté de synthétiser les bonnes pratiques qui ont été présentées tout au long de ce lab :

- Existence du **pare feu** : filtrer. Ouvrir le moins possible de flux entrants.
- **Maintenance** des postes de travail : antivirus, mises à jour systèmes d'exploitation + équipement réseau à jour : bcp de failles sur le matériel.
- **Sensibilisation très forte au niveau des utilisateurs.**
- Changements des mots de passe tous les 3 mois en fonction des différents comptes. Mots de passe forts et renouvellement régulier.
- Mettre en place un système de **sauvegarde** et **plan de sauvegarde**. Sauvegarde des postes serveurs et données sensibles que ce soit sur cloud ou serveurs locaux.
- Outils de surveillance des flux internes sur réseau local.
- Consultation du site de **l'ANSSI** : mises à jour, problématiques, inscription sur leur page linkedin.
- Vérouillage systématique des sessions
- Arrêt programmé de l'ensemble du système.
- Eviter les post-it avec les mots de passe collés sur le bureau.
- Attention aux élèves qui filment les enseignants lors de la saisie des mdp.

Les mots de passe

- On relève le problème des mots de passe, constatant que beaucoup d'entre nous avons les mêmes mauvaises habitudes, liées à la complexité à gérer tous les mdp différents.
- L'ANSSI revient sur l'utilisation des mdp et sur la politique de renouvellement. Aujourd'hui la bonne pratique de sécurisation est la multiplicité des mdp et l'utilisation d'un coffre-fort de mdp. Par exemple : Keepass qui est gratuit et fiable. C'est un bon outil qui crée identifiants et mdp. Il existe des tutoriels.

✓ ***Le + UNETP Lab' : Nos experts travaillent à une rapide procédure pour nous guider dans l'utilisation de ce type de coffre-fort.***

Attention à la sécurisation des connexions : authentification multi-facteurs (MFA) va devenir la norme : premier facteur : mdp + confirmation par un code.

- **Partage d'expérience** : Saint Ambroise à Chambéry. La solution d'un gestionnaire de mdp comme Keepass reste compliquée quand il faut gérer différents profils sur un même matériel. A Saint Ambroise : utilisation du gestionnaire intégré de google chrome. 1000 utilisateurs prof + élèves : 1 ordi – 1000 personnes dessus potentiellement : problématique pour ces logiciels de mdp. Changements de mdp compliqué y compris pour les élèves.

- **Partage d'expérience :** La Croix Rouge à Brest pour lutter contre le phishing : mise en place de campagnes de sensibilisation des utilisateurs avec des tests campagnes fictives de faux mails. Efficacité prouvée.

Présentation de Simon Nadot,
Praeventia – accompagnement du risque cyber auprès de la MSC (cf. diaporama]

Tout le monde est concerné par le risque.

En cyber la plus grande vulnérabilité est entre l'ordinateur et la chaise. La faille c'est l'humain.

- 1er prérequis demandé par les assureurs :
  la sensibilisation de l'ensemble des collaborateurs

Panorama des attaques présenté par l'ANSSI :

- Cyber : information manipulée.
- Outils informatiques ne sont que des outils.
- Le Ransomware est l'attaque majeure : pour rendre les données inaccessibles. Blocage sous rançon.
- Attaque cyber = attaque d'opportunisme.
  Activisme / petits malins / malveillance.
  En majorité : opportunisme : exploitation de l'intrusion qui fonctionne.

Objectif des assurances : redémarrer l'activité sans payer la rançon.

60% des entreprises non assurées ferment 18 mois après une attaque cyber.
Pour remédier à l'attaque : refaire le cheminement.

Pré requis pour être assuré :

- Sensibilisation des utilisateurs : tests de phishing. Identification des serial clickers. Scans de vulnérabilité.
- Généralisation de la MFA : tous les comptes en mobilités, qui se connectent depuis l'extérieur. Tous ceux qui ont des privilèges.
- Antivirus dépassés bloque ce qui est indiqué. L'EDR bloque tout ce qui semble louche.
- Sauvegardes offlines, non exploitables.

Les réactions :

- Difficulté de mettre en œuvre cette protection assurancielle qui a un coût important.
- Beaux principes pas de miracle ; il faut mettre en place un véritable plan d'action investissements.
- Il ne faut pas qu'une intention, cela nécessite de réels efforts, et avoir du personnel dédié.

- Mise en place d'un SIEM efficace mais coûteux (les SIEM sont des systèmes centralisés qui offrent une visibilité totale sur l'activité de votre réseau et vous permettent ainsi de réagir aux menaces en temps réel).

➢ **Partage d'expérience** : cyber attaque : concrètement ransomware sur un cadre haut placé qui avait les droits d'administrateur, suite à l'ouverture d'une pièce jointe. Introduction d'un virus qui crypte les données, notamment données comptables – paie. Présence d'une sauvegarde externalisée avec prestataire. Remise en place avec les sauvegardes du dimanche soir**. Importance du système de sauvegarde.**

✓ ***Le + UNETP Lab' : Le lab permet de faire remonter les demandes et les besoins, d'identifier des objets de formation afin que l'UNETP puisse monter une formation, possiblement en interne.***

Pour compléter votre information,
consultez le diaporama mis à disposition par
Simon Nadot,
Praeventia – accompagnement du risque cyber auprès de la MSC

MERCI À TOUS LES COLLÈGUES QUI ONT PARTICIPÉ À CET UNETP LAB.

RENDEZ-VOUS LE JEUDI 4 AVRIL PROCHAIN POUR TRAVAILLER ENSEMBLE SUR

L'INTELLIGENCE ARTIFICIELLE : LE GRAND REMPLACEMENT ?