RAPPORT

ATELIER DE FORMATION SUR LES TECHNIQUE DE PROTECTIONS DIGITAL

Douala du 02 au 03 mars 2020

Formation sur les techniques de protection digital

Rapporteur : TJADE UM Natacha stagiaire au service de communication à ADISI

Rappel des objectifs de cette formation:

Objectifs de la formation

- Renforcer la sécurité numérique du système d'ADISI-Cameroun.

Objectifs principal:

- Permettre de sécuriser le système numérique

Objectifs spécifiques

- Permettre une formation complete de l'équipe de travail
- Permettre une collaboration pour l'amélioration des capacités du champion de l'organisation
- Assurer la sécurité numérique dans les années avenirs
- Faire bénéficier des connaissances sur la sécurité digital aux organization partenaires

ADISI-CAMEROUN à organiser une formation sur les techniques de protections digital animé par MR LOKWA Narcisse, qui s'est tenue sur une période de deux jours allant du 02 au 03 mars 2020 dans leur locaux si à feu rouge bessengue immeuble AZICUL au 4ème étage. formation portant sur les modules suivants:

MODULE 1: LE SYSTÈME D'INFORMATION

Module 2: DISCUSSIONS ET IDENTIFICATIONS DES MENACES

MODULE 3: L'EVALUATION DES RISQUES (AUDIT DE SECURITE INFORMATION)

MODULE 4 POURQUOI FAIRE UN AUDIT DE SECURITE INFORMATIQUE?

MODULE 5: TYPES D'ATTAQUES

MODULE 6: LES RISQUES

MODULE 7: LES CONTRES- MESURES

MODULE 8: POUR MIEUX SECURISER UN SI IL FAUT

MODULE 9: UNE APPROCHE GLOBALE DE SECURITE

MODULE 10: LES APPLICATIONS ET MATERIELSDE SECURITE

MODULE 11: AVANTAGES DES MESSAGERIES EN OPEN SOURCE

MODULE 12: LOGICIEL DE CHIFFREMENT

MODULE 13: ALGORITHME RSA

MODULE 14: RECOMMENDATIONS ET BONNES PRATIQUES

Etaient present à cette formation:

Formation sur les techniques de protection digital

Rapporteur : TJADE UM Natacha stagiaire au service de communication à ADISI

- L'equipe d'Adisi-Cameroun
- L'animateur de la formation MR LOKWA NDUMZAMA Narcisse (expert)
- Les differents invités

Cf: liste de présence

RAPPORT JOUR 1:

Lundi 02 Mars 2020 de 10 h 00 - 17 h 00 s'est tenue un atelier de formation sur les techniques de protections digital, dans les locaux d'ADISI. séance portant sur 14 modules à savoir:

- L'introduction

MODULE 1: LE SYSTÈME D'INFORMATION

LES 05 objectifs

1- l'integrité
2- la confidentialité
3- la disponibilité
4- l'authenticité
5- la non repudiation

MODULE 2: DISCUSSIONS ET IDENTIFICATIONS DES MENACES

1- identifier les menaces
2- les auteurs des menaces
3- les raisons pour lesquelles vous pouvez subir attaques
4- les flux d'information
5- comment souhaiterez vous limiter ces menaces

(20 minutes)

MODULE 3: L'EVALUATION DES RISQUES (AUDIT DE SECURITE INFORMATION)

1- Qui?
2- pourquoi?
3- quand?
4- comment?

MODULE 4 POURQUOI FAIRE UN AUDIT DE SECURITE INFORMATIQUE?

Pour permettre d'obtenir une analyse des risques et d'identifier les informations sensibles à proteger et les objectifs de sécurité.

MODULE 5: TYPES D'ATTAQUES

- **DDOS**: une attaquepar déni de service pour rendre impossible un service
- **Intrusion**: s'introduire dans un SI sans droit.
- **Spams**
- **Le phishing**: le but ici est d'obtenir des données sensibles par l'envoi d'un mail
- **Malware**: un programme développé dans le but de nuire à un SI
- **Le spoofing**: attaque d'usurpation d'identité

- **Les ransomwares**: prise en otage des données personnelles.
- **Cross-site scripting**: faille de sécurité des sites webs permettant d'injecter du contenu dans une page

MODULE 6: LES RISQUES

Risques = menaces X vulnérabilté

Contre -mesure

- **Menace**: représente le type d'action succeptible de nuire dans l'absolu
- **Vulnérabilté ou faille**: représente le niveau d'exposition face à la menace
- **Contre-mesure**: l'ensemble des actions mises en oeuvres en prevention de la menace

MODULE 7: LES CONTRES- MESURES

Les contre-mesures à mettre en oeuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un enselmble de règle clairement définies.

MODULE 8: POUR MIEUX SECURISER UN SI IL FAUT:

- Identifier les menaces potentielles, et donc de connaitre et de prévoir la façon de procéder de l'ennemi
- Connaitre les motivations des pirates de catégoriser ces derniers et enfin de donner une idée de leur façon de procéder pour mieux comprendre comment limiter les risques d'instrusions

MODULE 9: UNE APPROCHE GLOBALE DE SECURITE

- **La sensibilisation des utilisateurs aux problèmes de sécurité**
- **La sécurité logique**: la sécurité au niveau des données, les applications où encore le SI
- **La sécurité des télécommunications**: technologies réseaux, serveurs, reseaux d'accès, etc.

Formation sur les techniques de protection digital

Rapporteur : TJADE UM Natacha stagiaire au service de communication à ADISI

- **La sécurité physique**: la sécurité au niveau des infrastructures matérielles: salles sécurisées, lieux ouverts au public, etc.

MODULE 10: LES APPLICATIONS ET MATERIELSDE SECURITE

- Des USB cryptés
- Des anti-virus mise à jour
- Firewall
- VPN
- PGP KEYS
- Telephone cryptés
- Messagerie crytés

MODULE 11: AVANTAGES DES MESSAGERIES EN OPEN SOURCE

- Wire
- Signal
- Telegram
  Accès de code source aux multiples développeur / hackers qui peuvent verifier les failles.

MODULE 12: LOGICIEL DE CHIFFREMENT

- FlowCrypt
- Open PGP
- ProtonMail
- BestCrypt
- AxCrypt

MODULE 13: ALGORITHME RSA

- Rivest, Shamir et Adleman (1977)
- Nombre premier (divisible par lui et par 1)
- Le produit de deux facteurs identiques.
- Crytographie à clé publique/privée

MODULE 14: RECOMMENDATIONS ET BONNES PRATIQUES

- Installer des bons anti-virus
- Mise à jour régulière des anti-virus
- Bonne connaissance de votre SI
- Utiliser des applications de chiffrements
- Toujours chiffré des communications/messages/documents, etc.
- Avoir des mots de passes qui combine des lettres, chiffres, symboles t changer fréquemment .

RAPPORT 2

Formation sur les techniques de protection digital

Rapporteur : TJADE UM Natacha stagiaire au service de communication à ADISI

Mardi 03 mars 2020 s'est conduit la seconde journée de formation qui à débuter à 10 heures et s'est achevé à 16 heures. Séance portant sur quatres principaux points à savoir:

- Le récappitulatif des enseignements de la journée précédente
- Les préoccupations des participants
- Un excercice d'application
- L installation des logiciels (**signal et FlowCrypt**) sur téléphones et ordinateur et différentes thecniques d'itulisations.

La fin de cette formation s'est suivie d'une réunion entre MR LOKWA MBUNZAMA Narcisse et l'équipe d'ADISI pour une mise au point.

Formation sur les techniques de protection digital

Rapporteur : TJADE UM Natacha stagiaire au service de communication à ADISI