ESA1124: COURS BONUS

Sécurité informatique : une étude de cas à travers les mesures prises par l'ANTIM face à l'attaque mondiale par le ransommalware WannaCry au Mali

Ousmane LY, MD, MsC
Expert en Santé Numérique

Plan

- Définition
- Objectifs de la sécurité informatique
- Le cas WannaCry en 2017 au ministère de la santé du Mali
- La réaction de l'ANTIM
- L'organisation de la sécurité informatique des entités institutionnelles et des entreprises
- Solutions aux problèmes d'organisation de la sécurité informatique au Mali : Centre d'alerte et de réaction aux attaques informatiques (CERT)
- Conclusion

Définition

La sécurité informatique est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique. D'une manière générale, elle consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Objectifs -SI

Il y’en a cinq, qui sont:

- L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ;
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée ;
- L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

WannaCry en 2017-MS

- Un ransomware qui attaque massivement les systèmes informatiques le 12 mai 2017
- Exploite les failles SMB () de windows
- Encrypte les données sur la cible
- Demande un rançon pour le déverrouillage des fichiers
- Paiement exclusif en bitcoin

Infection mondiale

Réaction de l'ANTIM

- Cellule de veille technologique identifie le risque
- Analyse situationnelle
- Proposition de solution
- Rédaction d'une note d'information critique a l'attention de l'autorité
- Applications des mesures correctives sur les systèmes en production a l'ANTIM
- Conseil et supports des autres usagers du MSHP

Note d'information

Elle a été produite immédiatement et contenait les informations suivantes:

- L'équipe technique de l'ANTIM passera au cabinet et au secrétariat pour un contrôle de vulnérabilité et mise à jour de tous les équipements informatiques sous windows le lundi 15 mai 2017 dans la matinée, conformément aux missions de l'agence
- Contrôle systématique de tous les systèmes d'information avant leur connexion à l'internet et usage le lundi 15 mai 2017 par les équipes informatiques des différents services du ministère
- Mise à jour des systèmes d'exploitation Windows avec le patch MS17-010 disponible en téléchargement gratuit sur le site de microsoft
- Information des hôpitaux sur le risque accru par rapport à leur activité
- Information de la réunion de cabinet sur ce type de risque et les mesures à prendre
- Instructions aux usagers de ne pas ouvrir sur leur ordinateur les fichiers joints provenant de sources non identifiées (pièces jointes, Word et PDF)
- Mise à disposition d'une hotline par l'ANTIM pour soutenir les services qui auront des difficultés, au 72 29 56 43/72 29 56 44/79 88 06 84 (sans frais pour la flotte du ministère) et le 20 22 38 44
- Institution de séances d'informations, de communications et de formations continues sur les questions de cybersécurité auprès des responsables.

http://www.sante.gov.ml/index.php/actualites/item/2953-regles-de-securite-contre-les-ransonwares

Organisation: fonctions

Les fonctions de la Sécurité Informatique sont:

- Analyse de risques
- Sensibilisation et formation aux enjeux de la sécurité
- Étude des moyens et préconisations
- Audit et contrôle
- Veille technologique et prospective
- Suivi de la sécurité opérationnelle
- Autorisation et gestion des habilitations

Organisation: composantes

Les composantes organisationnelles de la Sécurité Informatique sont:

- Un « responsable » (RSSI)
- Comité de sécurité informatique
- Groupes de travail
- Projet X
- Gestion de crise

En résumé on peut dire que:

- Le risque zéro n'existe pas, mais il faut travailler à minimiser le risque
- La sécurité est une chaîne dont la force est celle du maillon le plus faible

Solutions: CERT

Un computer emergency response team (CERT) ou computer security incident response team (CSIRT) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

Certains pays africains comme la Tunisie l’ont déjà mis en place et leurs systèmes de veille cyber sécuritaire fonctionne bien.

CERT ROLES

- Centralisation des demandes d'assistance à la suite des incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
- Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERT, contribution à des études techniques spécifiques ;
- Établissement et maintenance d'une base de données des vulnérabilités ;
- Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet CERT nationaux et internationaux.

CERT AFRIQUE

Etat de lieu du continent Africain

Operational	Implemenation	Plannig	Brainstorming
Tunisia	Morocco	Rwanda	Angola
South Africa		Côte d'Ivoire	Benin
Egypt		Nigeria	Burkina Faso
Mauritius		Senegal	Republic of Congo
Kenya		Algeria	Libya
Sudan		Cameroon	Madagascar
		Ghana	Mali
			Mozambique
			Niger
			Togo
			Tanzania
			Zambia
			Uganda

CERT TUNISIE

Janvier | Février | Mars | Avril | May | Juin | Juillet | Août | Septembre

Résultats

Risque	Référence	Date découverte	Titre
	tunCERT/Vuln.2018-325	12/09/2018	Noyau des systèmes Microsoft Windows
	tunCERT/Vuln.2018-324	12/09/2018	Microsoft: Outils de développement
	tunCERT/Vuln.2018-323	12/09/2018	Microsoft Office
	tunCERT/Vuln.2018-322	12/09/2018	Navigateurs web de Microsoft
	tunCERT/Vuln.2018-321	12/09/2018	Google Chrome
	tunCERT/Vuln.2018-320	12/09/2018	Adobe ColdFusion
	tunCERT/Vuln.2018-319	12/09/2018	Adobe Flash Player
	tunCERT/Vuln.2018-317	06/09/2018	Mozilla Firefox
	tunCERT/Vuln.2018-316	06/09/2018	Cisco Webex Teams
	tunCERT/Vuln.2018-315	06/09/2018	Cisco Webex Meetings Client pour Windows
	tunCERT/Vuln.2018-313	06/09/2018	Cisco SD-WAN Solution
	tunCERT/Vuln.2018-312	06/09/2018	Cisco RV110W, RV130W et RV215W Routers
	tunCERT/Vuln.2018-311	06/09/2018	Cisco Umbrella Enterprise
	tunCERT/Vuln.2018-310	06/09/2018	Google Android
	tunCERT/Vuln.2018-309	05/09/2018	Google Chrome
	tunCERT/Vuln.2018-308	31/08/2018	Smart phones Huawei
	tunCERT/Vuln.2018-305	29/08/2018	FortiManager
	tunCERT/Vuln.2018-304	29/08/2018	Joomla!
	tunCERT/Vuln.2018-303	29/08/2018	Cisco Data Center Network Manager
	tunCERT/Vuln.2018-302	28/08/2018	Apache Struts2

Première Précédente [1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 de 259] Suivante Dernière

CONCLUSION

La création d'un centre national d'alerte et de réaction aux attaques informatiques (CERT), n'est pas surement la panacée même si elle procède à la résolution des problèmes de **coordination** et de **leadership** entre différentes **entités publiques**.

L'enjeux de la question est la sensibilisation aux questions de sécurité informatique des **USAGERS** et des **DECIDEURS**.

Nous devons tous prendre conscience que la cybersécurité devient une question de sécurité nationale et voir d'existence nationale tout simplement.

MERCI !