APSI-CI

LE MAGAZINE

Mars 2022

AVIS D'EXPERTS

Cybersecurité et Sensibilisation

Faits marquants sur la cybersécurité

Focus sur un membre

SOMMAIRE

Page 01 **01** | **Faits marquants du mois**

Toute l'actualité sur la cybersécurité en Afrique et partout dans le monde.
-CONSEILS ET RECOMMANDATIONS

Page 03 **02** | **Avis des experts**

Thème : À votre avis, quel serait le meilleur moyen pour faire de la sensibilisation au top management.

Page 08 **03** | **Focus sur un membre**

Découvrez la biographie et le parcours du membre de l'APSI-CI M.Marc saint clair Kouassi.

Page 09 **04** | **Evénements à venir**

Suivez APSI-CI pour ne rien rater de nos prochains rendez-vous.

Faits marquants du mois

Guerre en Ukraine : l'Anssi appelle à se méfier de l'éditeur russe Kaspersky

Rapporté par Alexis NDRI, RSSI COFINA

Dans une note publiée par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, l'Anssi préconise de trouver des alternatives aux logiciels russes. Kaspersky est la principale entreprise visée. Le gendarme français de la cybersécurité demande aux particuliers et aux entreprises de ne pas changer brutalement d'antivirus "***sans solution de substitution***". En l'absence de protection, la porte serait en effet grande ouverte pour les cybercriminels. Par conséquent, l'Anssi estime qu'à moyen terme "***une stratégie de diversification des solutions de cybersécurité doit par conséquent être envisagée***".

Sources : https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/
https://www-lesnumeriques-com.cdn.ampproject.org/c/s/www.lesnumeriques.com/pro/guerre-en-ukraine-l-anssi-appelle-a-se-mefier-de-l-editeur-russe-kaspersky-n178153.amp.html

le PCI SSC publie la norme de sécurité des données PCI v4.0

Rapporté par Laicana COULIBALY, Consultant Cybersecurité et DG de Diamond Security Consulting

Les mises à jour de la norme visent à répondre à l'évolution des besoins en matière de sécurité de l'industrie des paiements, à promouvoir la sécurité comme processus continu, à accroître la flexibilité des organisations qui utilisent différentes méthodes pour atteindre leurs objectifs de sécurité et à améliorer les méthodes et les procédures de validation.

Source : https://blog.pcisecuritystandards.org/pci-dss-v4-0-resource-hub

Conseils et recommandations

Rapporté par Moussa SIDIBE, Sous-Directeur Sécurité SI chez GS2E

1. Renforcer l'authentification sur les systèmes d'information : il s'agit ici de mettre en œuvre une authentification forte pour les comptes particulièrement exposés (administrateurs, personnel de direction, cadres dirigeants…), nécessitant 2 facteurs, soit « un mot de passe, un tracé de déverrouillage ou une signature», soit « un support matériel (carte à puce, jeton USB, carte magnétique, RFID) ou a minima un autre code reçu par un autre canal (SMS) ».

2. Accroître la supervision de sécurité : un système de supervision des événements journalisés devra être mis en place pour « détecter une éventuelle compromission et de réagir le plus tôt possible ».

3. Sauvegarder hors-ligne les données et les applications critiques : les sauvegardes effectuées doivent être réalisées en étant déconnectées du système d'information « pour prévenir leur chiffrement », et des solutions de stockage à froid (disques durs externes, bandes magnétiques) peuvent être utilisées afin de « protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité ».

4. Établir une liste priorisée des services numériques critiques de l'entité : l'ANSSI conseille de réaliser un inventaire des services numériques d'une organisation en les listant par type de sensibilité, et d'identifier les dépendances vis-à-vis des prestataires externes.

5. S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque : les entreprises doivent déterminer les contacts d'urgence et établir un plan de réponse adapté à la gestion des cyberattaques.

Avis d'experts

À votre avis, quel serait le meilleur moyen pour faire de la sensibilisation au top management : Simulations de ransomwares ou vidéos éducatives?

Les différents intervenants

Hyacinthe KAHO
RSSI de la LONACI

Saint Clair KOUASSI
Gestionnaire de risques informatiques chez GTBANK CI

Marc COULIBALY
RSSI chez BNI

Constant Diby
Responsable informatique chez KMPG

Idriss Kader Koné
Consultant en cybersécurité chez MANIKA CI

1

Hyacinthe KAHO

RSSI de LONACI

Généralement le top management comprend le langage business.

Pour une sensibilisation impactante, une approche montrant clairement les impacts business d'un ransomware serait idéale à mon avis.
Donc oui une simulation et / ou un retour d'expérience d'entreprises ayant déjà subient des préjudices suite à ce genres d'incidents serait l'idéal.

2

Saint Clair KOUASSI

Gestionnaire de risques informatiques chez GTBANK

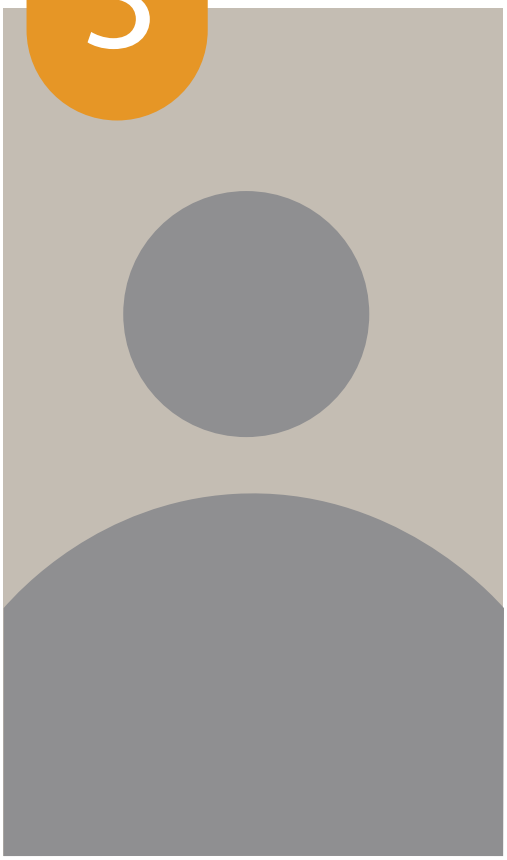
La sensibilisation contre tout type de cyberattaque reste un des moyens préventifs contre une quelconque compromission de l'écosystème informatique.

Notons que cette sensibilisation devrait s'appliquer à toutes les couches de l'entreprise.

En ce qui concerne le top management, qu'il soit technique ou pas,nul besoin de comprendre le language de la sécurité informatique.Mais de maîtriser les enjeux et défis fasse à une cybermenace. Clairement, le moyen de sensibilisation du top management doit se faire en fonction de la culture de l'entreprise.

Pour certaines, une simple présentation powerpoint pourrait suffire alors que pour d'autres, seule une simulation mettant clairement en lumière leurs vulnérabilités les ferait prendre conscience du danger.

3



Marc COULIBALY

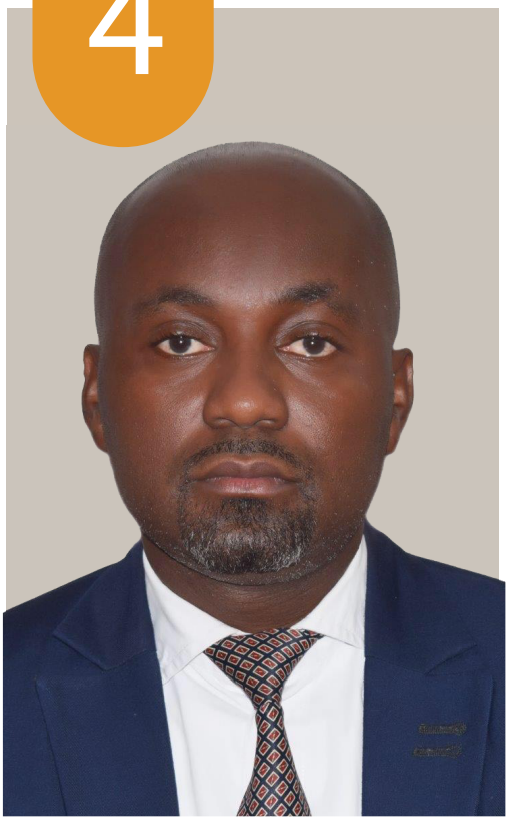
RSSI à BNI

Je dirais que cela dépend du secteur d'activité.

En teleco le top management comprend bien ses problématiques. Par rapport à ceux dont la technologie n'est pas leurs cœur de métier.

Et donc face à ce type de top management il faut avoir un autre langage .

4



Constant Diby

Responsable informatique
chez KMPG

Je pourrais dire que le top management ne comprend que tout ce qui est lié à la gouvernance corporate.

Pour s'y prendre un business case avec la démonstration de la perte des actifs en termes de chiffre d'affaires et d'image pourrait les alerter avec bien-sur des exemples d'entreprise dans le même secteur d 'activité ayant subit ce type d'attaque.

5

Idriss Kader Koné

Consultant en cybersécurité
chez MANIKA CI

Pour réaliser une bonne sensibilisation au top management, il est important de bien comprendre les enjeux stratégiques ou objectifs métiers de l'organisation et corréler les risques cyber pouvant les empêcher.

Généralement quand l'impact business d'une attaque est bien compris par le top management ceux ci deviennent plus sensibles aux risques.
Par exemple si la stratégie d'une banque repose essentiellement sur les clients entreprises, on pourrait facilement montrer qu'une crise ransomware permettrait de bloquer le cœur bancaire pendant une X durée. Ce qui aura pour impact le blocage du traitement des transactions des organisations comme La présidence, etc. D'où possibilité de perdre des gros clients, de sanctions, perte d'argent, etc.

Après le moyen utilisé pour réaliser la sensibilisation devra être adapté en fonction du management. Certains aiment le spectaculaire, d'autres non. Quoiqu'il en soit une présentation en présentiel est la meilleure pour ma part.

Saint Clair KOUASSI

Gestionnaire de risques informatiques

Entreprise : GTBANK

Titulaire d'un MBA en Nouvelles Technologies de la National Institute of Business Management de l'Inde, Marc Saint Clair est Ingénieur Système de Sécurité Informatique. Il est doté d'une certification ITIL V4 et prépare présentement un Doctorat.

Son parcours professionnel débute en 2012 après son obtention du BTS en Réseau Informatique et Telecom (RIT).

Il intègre en 2013 le groupe Orange pour un stage de 2 ans d'Agent Support Technique puis de Responsable Administrateur Système pour un grand cabinet d'avocat International.

En 2019, il intègre la compagnie TCS en qualité de Support Technique et depuis décembre 2022, est recruté en tant que Gestionnaire des Risques Informatiques chez GTBank CI, un poste qu'il a acquit grâce à ses connaissances du Hacking Ethique et de la Sécurité défensive au cabinet IvoireNode entre 2020 et 2022.

Evénements à venir

Les dates à retenir pour les prochains événements :

- ## CAF (Cyber Africa Forum)

  Date : 9 et 10 Mai 2022

  Lieu : Au Radisson Blu (Hotel)
  Abidjan , Côte d'ivoire

- ## Assemblée Générale Mixte de l'APSI-CI

  Lieu : Abidjan, Côte d'ivoire

  Date : 21 Mai 2022

SUIVEZ-NOUS WWW. APSI .CI POUR NE RIEN MANQUER DE NOS PROCHAINES ACTIVITÉS

APSI-CI

LE MAGAZINE

Contacts

+225 0759673513

contact@apsi.ci

www.apsi.ci