APSI-CI

ASSOCIATION DES PROFESSIONNELS DE LA SÉCURITÉ DE L'INFORMATION DE CÔTE D'IVOIRE

E-mag trimestriel

Année 2023

Juillet Août Septembre

- Actualités
- Avis des experts
- Focus sur un membre

www.apsi.ci

SOMMAIRE

• Faits Marquants

Alerte : Campagne de Malspam en cours.

Nous avons observé une attaque massique en cours de spam combinée à une distribution de lien vers des sites malveillants.
Au début, les emails parvenaient à contourner les protections anti-spam par défaut de Microsoft 365 et même la protection avancées avec Defender for Microsoft 365. Cela, pour une raison toute simple : les emails sont envoyé via des adresses emails qui varient et qui proviennent de compte "légitimes" Microsoft 365, en utilisant le domaine par défaut fourni par Microsoft 365 ("adresse@compagnie.onmicrosoft.com") l'ensemble des membres officiels.

Une faille dans Kubernetes élève les privilèges sur les terminaux Windows

Une faille dans les fichiers configuration YAML des clusters Kubernetes est capable d'accorder des privilèges systèmes sur les hôtes Windows. La brèche a été réparée dans la dernière version de l'orchestrateur de cluster de conteneurs.
La dernière version de Kubernetes publiée le mois dernier corrige toute une classe de vulnérabilités à partir desquelles des attaquants pouvaient abuser de la propriété subPath des fichiers de configuration YAML pour exécuter des commandes malveillantes sur les hôtes Windows.

Source : Lucian Constantin, IDG NS (adaptation Jean Elyan)

• Web conférences

Webinar : La méthode EBIOS RM (les fondamentaux)

Le 10 Juin dernier s'est tenu la Première partie de la conférence publique en direct de la chaine Youtube de l'Association, sur le thème La méthode EBIOS RM avec pour invité Rachid El ALAOUI.

Webinar : La méthode EBIOS RM (Notions avancées)

La première partie du webinar avait pour objectif de fournir une vue d'ensemble de la méthode EBIOS RM et de présenter ses notions fondamentales. La deuxième session a consisté à approfondir l'une des briques de base de la méthode, qui est le socle de sécurité.

Webinar : Comment bien gérer les vulnérabilités

La gestion des vulnérabilités est un processus essentiel dans la Sécurité de l'Information qui consiste à réduire la surface d'attaque des Systèmes d'information.

Quels sont les bonnes pratiques qui permettent de bien gérer ce processus ?

Pour traiter ce sujet, nous avons bénéficié du

retour d'expérience de 3 membres officiels de l'APSI-CI, experts du sujet :

– Hyactinhe KAHO, RSSI de la LONACI
– Martial AHUI, RSSI de SNEDAI Groupe
– Fahd MOHAMED, Consultant GRC chez LUTESSA

Webinar : Management de la protection des données à caractère personnel en zone UEMOA (Cas des banques et des assurances en Côte d'Ivoire)

La question de la sécurité des données à caractère personnel se pose dans nos organisations africaines en général et particulièrement au niveau du secteur bancaire et assurantiel . La sécurité des données à caractère personnel est-elle réellement prise en considération par le management dans les banques et assurances en Côte d'Ivoire ?

Le samedi 5 août 2023 à 10H GMT en direct de notre chaîne youtube le Docteur Hyacinthe KOFFI, membre officiel de l'APSI-CI nous a fait une restitution de son etude sur le sujet .

Webinar : Quelle cybersécurité pour une PME ?

Une cyberattaque sur une entreprise de type TPE et PMU pourrait avoir des impacts directs sur sa survie.
Ces risques sont parfois sont souvent sous-estimés par ce type d'entreprises qui restent pourtant des cibles de choix pour les cybercriminels.

Pour traiter ce sujet, nous avons reçu 2 experts chevronnés, membres de l'APSI-CI qui sont Koné HENRI, Directeur des Opérations à AFRICAN SECURITY MARKET et Gérard KONAN, CEO de AGILLY.

Avis des experts

Thème : Quelle est la mesure de sécurité la plus importante à mettre en oeuvre dans une entreprise ?

Réponses des intervenants

GUY-KEVIN POTE

Secrétaire Général de l'APSI-CI
Chef de service Contrôle de la Sécurité du Système d'Information à BRIDGE BANK GROUP CÔTE D'IVOIRE

Les systèmes d'information sont devenus de plus en plus complexes avec des besoins métiers qui évoluent (Connexion aux logiciels depuis différents endroits, interconnexion des SI avec ceux des partenaires, Systèmes Cloud, etc). Ces évolutions présentent des risques (fuite de données suite à un accès non autorisé, indisponibilité des systèmes) auxquels les organisations doivent répondre.

La mesure de sécurité la plus importante à mettre en œuvre dans une entreprise est la définition d'une Gouvernance par l'élaboration d'une stratégie de sécurité du système d'information qui sera validée par le Top management afin de donner les orientations en termes de sécurité du système d'information qui s'alignera à la vision de l'entreprise et également qui intégra la réglementation et loi en vigueur ainsi que les standards internationaux auxquels elle pourra être soumise.

Dr KOURAOGO Yacouba

Maître-Assistant
Enseignant - Chercheur
Université Virtuelle de Côte d'Ivoire (UVCI)

Le firewall (pare-feu) est un programme, ou un matériel chargé de protéger du monde extérieur en contrôlant tout ce qui se passe et surtout ce qui ne doit pas circuler entre internet et le réseau local privé.

Cependant, dans un système d'information, il est situé techniquement à l'intersection des postes de travail, de la zone démilitarisée (DMZ) et du routeur internet.
De ce fait, sa bonne configuration technique est à mon humble avis la mesure de sécurité la plus importante à mettre en œuvre dans une entreprise.
Celle-ci permettra le contrôle,la sécurité ,la vigilance entre le réseau local et Internet.

OUATTARA LANZENI

RSSI à IVOIRE
CARTES SYSTÈMES

C'est un sujet sur lequel on peut disserter pendant longtemps.

Chaque entreprise a sa réalité en fonction de son activité, de ce qui la fait vivre.
La mesure la plus pertinente serait celle qui pérennise l'activité.

Et pour savoir cela, il faut absolument transiter par une analyse de risque.

DOUMBIA Alassane

Directeur des
Opérations
Adjoint chez
SUD CONTRACTORS

L'essentiel est de fournir une formation constante sur la détection d'attaques, la gestion des mots de passe et la protection des données sensibles.

De plus, il est impératif d'adopter des politiques de sécurité transparentes, de déployer des pare-feu robustes, d'installer des systèmes de détection d'intrusion et de réaliser régulièrement des sauvegardes de données.

Cependant, il est important de souligner que la sécurité doit être un processus en cours, et une approche à plusieurs niveaux se révèle souvent la plus efficace pour défendre l'entreprise contre les menaces qui évoluent constamment…

Focus sur un membre

Martial AHUI

Biographie

Martial AHUI amoureux des nouvelles technologies, est dans le domaine de la cybersécurité depuis plus de 10 ans en tant que consultant et formateur.

Il débute sa carrière en tant qu'administrateur réseau pour être aujourd'hui responsable de la sécurité du Système d'Information du Groupe Snedai.

L'avis de Martial AHUI sur le paysage de la cybercriminalité

Les menaces cyber continuent à prendre de plus en plus de l'ampleur dans nos environnements SI; nos entreprises sont de plus en plus ciblés par des hackers ou réseau de cybercriminel.

Danger qui s'est accru avec la crise COVID et le télétravail. La pandémie de Covid-19 a démultiplié les risques. Dans une étude réalisée auprès de 211 grandes entreprises basées dans onze pays d'Afrique francophone et dévoilée, 40 % d'entre elles ont connu une augmentation du nombre d 'incidents depuis 2020.
En cause, les surfaces d'attaques encore plus importantes, conséquence du télétravail. Sans oublié les budgets faibles dédiés à la DSI et dont l'essentiel est alloué aux infrastructures, sans réel investissement dans le domaine crucial de la sécurisation des données. Pour minimiser les risques sachant que la multiplication et la sophistication des attaques nécessitent tout d'abord le développement d'une culture de la cybersécurité.

APSI-CI
LE MAGAZINE

www.apsi.ci

Contacts
+225 0759673513
contact@apsi.ci