APSI-CI
LE MAGAZINE

E-mag trimestriel

Juillet
Août
Septembre

- Faits marquants
- Avis d'experts
- Focus sur un membre
- Evénements à venir

www.apsi.ci

SOMMAIRE

Cisco victime d'une cyberattaque

Rapporté par Roger DABIRE

Au tour de Cisco d'être confronté à une cyberattaque. L'entreprise américaine spécialiste de l'IT et des réseaux a été victime d'un hacker en lien avec les groupes Lapsus$, UNC2447 et Yanluowang.
Cisco a découvert fin mai dernier avoir été victime d'une cyberattaque. L'entreprise américaine spécialiste de l'IT et des réseaux a détaillé ces informations dans un poste de blog le 10 août 2022, après que le hacker ai divulgué une liste de fichiers volés sur le dark web. *"Nous n'avons identifié aucune preuve suggérant que l'attaquant ait eu accès à des systèmes internes critiques, tels que ceux liés au développement de produits, à la signature de code, etc."*, tente de rassurer Cisco.

Source : https://www.usine-digitale.fr/article/cisco-victime-d-une-cyberattaque.N2033857

Google a bloqué la plus grande attaque DDoS de tous les temps

Rapporté par Roger DABIRE

L'un des clients du géant informatique a été confronté à une avalanche de 46 millions de requêtes

Du jamais vu dans l'histoire du web.
C'est un nouveau record, un de plus. Le premier juin dernier, Google a bloqué une attaque de déni de service distribuée (DDoS, Distributed Denial of Service) d'une puissance inégalée depuis que l'internet existe. À 10h18 (heure de San Francisco), l'un des clients du géant informatique est la cible d'une avalanche de données dont le débit a culminé à 46 millions de requêtes HTTPS par seconde !

Source:*https://www-01net-com.cdn.ampproject.org/c/s/www.01net.com/actualites/google-a-bloque-la-plus-grande-attaque-ddos-de-tous-les-temps.html?amp=1*

Conseils et recommandations

-Un site qui peut sauver la vie en cas de ransomwares

https://www.nomoreransom.org/fr/decryption-tools.html

Par Roger Dabire

-Outil de performance reseau

Zabbix, grafana, si environnement K8S alors Prometheus dont les métriques peuvent être transmis à grafana comme source de données.

Par Nicaise Kouamé

Avis d'experts

Question 1

Autoriseriez-vous les administrateurs à avoir la possibilité d'accéder en "remote protocol" (ssh, rdp..) sans traverser sous le prétexte d'anticiper d'éventuelles indisponibilités du bastion ?
Si non, comment anticipez-vous le cas d'urgence liée à l'indisponibilité du bastion d'administration ?

Réponses des intervenants

Fadiga Falikou
Architecte IT-Security
à KfW Bank

Les connections RDP et SSH aux différents systèmes à administrer seront seulement autorisées à partir des "Jump Serveurs".
Ces derniers seront placés dans une ou des zones sécurisées, suivant le modèle "Zero Trust". L'accès à ces Jump serveurs devra être uniquement autorisé aux comptes privilégiés, qui devront se soumettre à la MFA (l'authentification multifacteur) .
Il est conseillé de mettre en place une redondance au niveau des serveurs et des zones.

Hyacinthe KAHO
RSSI à la LONACI

L'objectif du bastion (WALLIX) par exemple étant de gérer les accès à forts privilèges, toutes les connexions SSH et RDP devront obligatoirement passer par ce réseau bastion.
Pour gérer l'indisponibilité il est important de mettre en place une redondance. Généralement pour le cas de Wallix, une machione virtuelle est offerte avec l'appliance.

Avis d'experts

Question 2

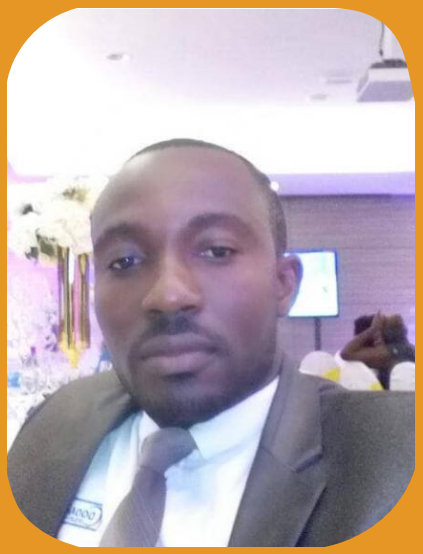
Doit-on sanctionner un collaborateur de la SSI qui se fait avoir par un mail de phishing ?

Réponses des intervenants

Olivier CLARK

Les circonstances du phishing permettent de savoir s'il y a preuve de négligence et si la personne récidive souvent.
Si les règles sont claires pour tous dès le départ, il n'y aura pas de confusion

---



DJINZOU Yanick

Associé et Directeur des Opérations de ACM-African Cybersecurity Market Group
Co-founder & CEO de Dooahoo Company

Une chose est de connaître les risques Cybersecurité et de sensibiliser mais une autre c'est de vivre des cas réels de phishing.
En plus de la bonne Culture Cybersecurité du personnel, il faudrait faire des simulations de Phishing via Email, Sms, USB et même Voice pour montrer que c'est pas un leurre mais une réalité.
La sanction est bonne mais il serait important de se poser la question de savoir:
Est-ce que l'entreprise a-t-elle cherché à anticiper les cas de phishing par les methodes de campagnes de Sensibilisation Cybersécurité et de Phishing?

Saint clair Marc Kouassi
Gestionnaire de risques informatiques chez GTBANK

Peut on être professionnel et perdre une compétition?
Les maîtres mots sont une formation continue et des séances pratiques soumettant le personnel à des tests.
Avec les prouesses observées ces dernières années dans le domaines des nouvelles technologies, les cyberattaques sont de plus en plus dissimulées et l'attaque par phishing en fait partie.

Hormis cet aspect, la sécurité des systèmes aussi se renforce avec les nouvelles technologies donc la compromission d'un système se fait de plus en plus difficile.
L'un des moyens d'atteindre les entreprises est le vecteur humain.

Le management doit comprendre les enjeux de mettre en place un dispositif (outils de campagne de phishing, training régulier, envoi de sensibilisation sur intranet au moins deux fois le mois) pour se prémunir de toute attaque du style.

Par ailleurs, ne voyons pas uniquement le côté attaque par phishing.

Un employé sous payé face à la dépression au travail dû au manque de leadership du management est une véritable vulnérabilité à découvert pour l'entreprise.

Un peu de OSINT et nous avons la porte d'entrée aux infra du système...

J'invite le Management à une prise de conscience et de decision pour un investissement dans la formation des employés tout en appelant l'opérationnel à doubler encore plus de vigilance.

Avis d'experts

Question 3

La PSSI peut elle servir de refentiel pour un audit interne? Un référentiel externe est-il obligatoire ?

Réponse de l'intervenant

Nicaise Kouamé

Responsable infrastructure et sécurité du BNETD / CEO & Founder NKTEK

L'application des dispositions de la PSSI entraînent des mesures organisationnelles et techniques ainsi que des indicateurs de performance et de surveillance.

C'est donc la PSSI qui est audité que soit interne ou externe. Les résultats de ces audits permettent en partie de faire la revue de la PSSI donc de s'inscrire dans un processus d'amélioration continue.
Cette revue doit se faire au moins une fois par an et doit être documentée.

Avis d'experts

Question 4

Que pensez-vous du changement régulier des mots de passes. Est-ce vraiment pertinent de nos jours ?

Réponses des intervenants

Olivier Nkuissi
Founder and CEO
iCONNEKT TECHNOLOGIES

Je préciserai que les mots de passe complexes changés régulièrement ne suffisent malheureusement plus.... il est nécessaire, voir indispensable de songer à intégrer un mécanisme d'authentification à facteur multiples (MFA) pour renforcer le niveau de protection des comptes et des identités.

La limitation de la validité du mot de passe est toujours recommandée dans tous les cas de figure....

Par ailleurs, le SMS est un moyen de livrai - son et de transport fortement déconseillé... on peut aujourd'hui dupliquer un numero sim et dans ce cas de figure le problème demeure entier... il faudrait plutot s'orienter vers de l'OTP délivré par des soft (google, microsoft ou autre) ou token physiques (le must)...

Les soft génèrent les OTP de façon totalement autonomes sans recourir à une connexion Internet ni aux SMS.

Dans des environnements critiques ce sont les tokens physiques qui sont fortement recommandés.

Il faudrait d'autre part définir une politique ou une stratégie de mot de passe capable de refuser des mots de passe itératifs... en outre je persiste à dire que une stratégie de changement périodique de mot de passe n'est pas suffisante, il faut la coupler avec une stratégie d'authentification à facteurs multiples pour disposer d'un niveau de protection des comptes et des identités qui soit pertinente.

Assaud P. Arnaud
Chef de projet confiance numérique chez Chronoservices

L'une des meilleures stratégies d'authentification forte est de coupler une identité numérique délivrée par une infrastructure à clé publique PKI avec des tokens physiques.

Pour ceux qui utilisent Windows Server vous avez Microsoft ADCS qui est déjà disponible comme rôle intégré. Sinon vous pouvez allez sur certaines autres solutions PKI complètes.

Avis d'experts

Question 5

Un contrat contenant des clauses de sécurité et un Plan d'assurance Sécurité sont-ils suffisants pour une organisation qui sous-traite un pan de son activité avec un partenaire ?

Réponse de l'intervenant

Marius OUPOH
CyberSecurity and
IT Risk Specialist

Le PAS (Plan d'assurance Sécurité) est un document qui décrit l'ensemble des exigences que le prestataire doit pouvoir garantir pour assurer la sécurité de l'activité externalisée de son client.

En effet, une entreprise peut choisir de confier à un tiers un pan de son activité. Cela s'appelle de l'infogerance.

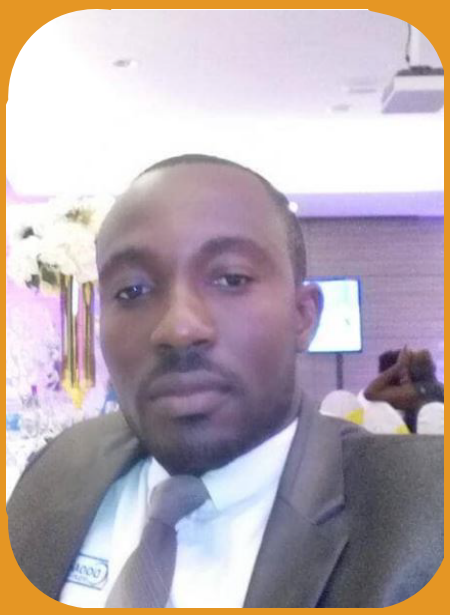
Mais cette infogérance induit généralement des risques parmi lesquels on peut citer :

- Risque de perte de maîtrise du système d'information par le client ;
- Risques liés aux interventions à distance par le prestataire ;
- Risques liés à la mutualisation de l'hébergement (dans le cadre d'un hebergement).

L'entreprise doit donc apprécier les risques liés à l'infogerance selon la nature de celle-ci et identifier les objectifs/mesures de sécurité adaptés pour le traitement de ces risques.
Ce sont ces mesures de sécurité qui seront intégrés dans le PAS sous forme de réponse du prestataire.

Ce PAS (réponse du prestataire) sera par la suite approuvé ou non par le client. Est-ce que le PAS suffit ? non. Le PAS reste du déclaratif.
Le client doit par la suite tenir avec le prestataire un Comités de Suivi de la prestation à fréquence régulière, pour s'assurer que ses exigences sont bien respectées. Il pourrait également réaliser des audits du prestataire dans le même but.

Focus sur un membre



Yanick DJINZOU

Associé & Directeur des Operations

Entreprise : Groupe Africain Cybersecurity Market

Diplômes : Ingénieur de Conception Option Réseau Informatique

Certifications : CCNA R&S, CCNA Security, CND,CheckPoint, Barracuda

Il débute comme Technico-Commercial en 2006 à Logical technology, il embrasse le monde de la Cybersécurité avec la démocratisation des formations Certifiantes en CI avec le Cabinet SION SYSTEMES en 2012 dans lequel il occupe le poste de Responsable Technique & de la Formation.

En 2015, il est Co-Fondateur et IT Manager de Dooahoo Company et s'en suivra une belle expérience d'années entrepreneuriale, d'appui et de Consultance pour des entreprises Ivoiriennes et Sous Régionales qui portait sur de vastes projets en Réseau, Système, VoIP, Cloud, Formations et surtout sur la Cybersécurité en Côte d'Ivoire et dans la Sous-région.

Depuis 2022, il est Associé et Directeur des Opérations du Groupe Africain Cybersecurity Market présent dans 3 pays.

Evénements à venir

Les prochains webinars de l'APSI-CI

- Initiation à l'investigation Numérique
- Lab : Comment pénétrer les téléphones mobiles ?
- Quelle architecture minimale de sécurité pour les PME ?

APSI-CI
LE MAGAZINE

www.apsi.ci

Contacts
+225 0759673513
contact@apsi.ci