APSI-CI

LE MAGAZINE

Avril 2022

AVIS D'EXPERTS

Efficacité des normes en sécurité de l'information

- Faits marquants sur la cybersécurité
- Focus sur un membre

www.apsi.ci

SOMMAIRE

Faits marquants du mois

Alerte aux détenteurs de sites WordPress !

Rapporté par Gérard KONAN, CEO de Agilly

Une attaque massive a touchée près de 16500 sites WordPress en Février et en mars 2022. Les attaquants compromettent les sites, y injectent des malwares que les visiteurs téléchargent en pensant installer une mise à jour de leur navigateur. Le malware ainsi distribué est un outil d'accès à distance qui permet aux attaquants de contrôler la machine des victimes. Nous avons été témoins d'au moins 10 incidents similaires dans les deux dernières semaines.

Que faire pour protéger vos sites Web WordPress?

- installez un Pare-feu d'application Web
- CloudFlare est gratuit et fait l'affaire pour la plupart des sites
- Changez la page du login par défaut
- Mettez à jour la version de WordPress et les plugins

Comment faire pour éviter de télécharger un malware par erreur?

- Protégez votre ordinateur avec un Anti-Malware, capable de filtrer la navigation web en temps réel
- À défaut, installer un filtre DNS dans votre navigateur ***(Exemple Quad9)***

Source : https://thehackernews.com/2022/04/over-16500-sites-hacked-to-distribute.html

Conseils et recommandations

Les mots de passes sont utilisés comme éléments d'authentification des utilisateurs.

Avec la contribution de Nicaise KOUAMÉ, Baacit COULIBALY, Hyacinthe KAHO et Marius OUPOH.

Force est de constater la fâcheuse habitude des utilisateurs à utiliser des mots de passe faibles tels que ***Password123 ,Bonjour2020 ,Azerty123.*** D'autre part,pour plusieurs entreprises, les mots de passes sont formés de la façon suivante "nom de l'entreprise suivi @ l'année en cours".
Il est fortement recommandé de former les mots de passes de manière à les rendre difficiles à deviner.

En règle générale, Un mot de passe fort doit contenir au moins 8 caractères aléatoires. Un mot de passe fort associe lettres minuscules et majuscules, chiffres et caractères spéciaux pour former une chaîne de caractères qui ne ressemble à aucun mot ou nom propre.

Des logiciels de gestion de mots de passes tels que "KEEPASS Password Safe" peuvent être utilisés pour générer des mots de passes forts et les sauvegarder de façon sécurisée.

Avis d'experts

Un Programme de sécurité qui ne repose pas sur une norme internationale peut-il assurer la sécurité d'une entreprise ?

Les différents intervenants

Gérard KONAN
Co-Fondateur
et CEO d'AGILLY

Ignace YAO
Chargé de la Sécurité des Systèmes d'information chez Groupe PROSUMA

Hyacinthe KAHO
RSSI à la LONACI

Fabrice DJIREBO
Consultant en cybersécurité

Nicaise Kouamé
Responsable infrastructure et sécurité du BNETD / CEO & Founder NKTEK

Gérard KONAN

Co-Fondateur
et CEO d'AGILLY

Adosser un programme de sécurité sur une norme ou un standard est une bonne pratique qui améliore considérablement l'efficacité d'un programme de sécurité.

Il faut cependant préciser que la mise en application stricte et la certification à certaines normes peuvent s'avérer complexes et même hors budget pour les petites structures, en particulier quand il s'agit des normes les plus connues. Bien que la certification aux normes présente des avantages indiscutables vis à vis des partenaires externes, ils s'apparentent parfois à un empilement mécanique de solutions techniques, débouchant sur une sécurité cyclique, efficace au moment des audits. Ainsi, être conforme ou certifié ne signifie pas toujours que l'on est à l'abri des incidents.

D'un autre côté, certains standards basés sur de l'auto évaluation en continu, tels que CIS Framework, peuvent s'avérer plus accessibles et plus efficaces. Nous en avons fait l'expérience avec certaines structures de taille intermédiaire. Et les résultats sont plutôt satisfaisants.
Avec des moyens humains et financiers limités, les PME et les ETI, peuvent déployer un programme de sécurité efficace et démontrer le niveau de sécurité de leur SI, documents et résultats à l'appui.

Ignace YAO

Chargé de la Sécurité des Systèmes d'information chez Groupe PROSUMA

Chaque secteur d'activité s'appuie sur de bonnes pratiques, des référentiels et des normes pour aider les professionnels du secteur à améliorer ce qu'ils font.
C'est ainsi que quand on fait des appels à candidatures, c'est pour rechercher des compétences et des expériences en rapport avec ces normes, référentiels...

Par conséquent personne ne peut légitimement prétendre sécuriser un système d'information en se passant des normes et standards qui régissent la cybersecurité.

Le véritable problème réside dans la complexité de l'implémentation de ces normes dans un environnement de production que ce soit les normes ISO 27000, COBIT, NIST …
C'est pourquoi je pense les normes ISO 27001 et ISO 27002 qui ont connu d'énormes refontes dans leurs versions 2022 sont très en phase avec les nouvelles typologies de menaces, l'évolution des technologies ainsi qu'avec les nouvelles réglementations .
Ce qui est intéressant c'est que dans leurs nouvelles montures, les normes ISO 27001 & 27002 se mappent (s'arriment) harmonieusement avec de nombreux nouveaux référentiels comme NIST, CIS ... qui permettent une implémentation des exigences techniques de ces normes plus aisement.
C'est le cas du référentiel CIS que je connais très bien. En fait quand tu bases ton programme de Cybersécurité sur les mesures techniques de CIS, tu fais d'une pierre, deux coups :

D'une part, tu mets en place des mesures de sécurité très efficaces contre les cyberattaques les plus courantes de nos jours ;
D'autre part tu te mets en conformité avec plusieurs normes déjà reconnues.

C'est pourquoi je dis souvent que les mesures de sécurité de CIS doivent être vues comme l'ISO 27002 et la norme ISO 27001.

Hyacinthe KAHO

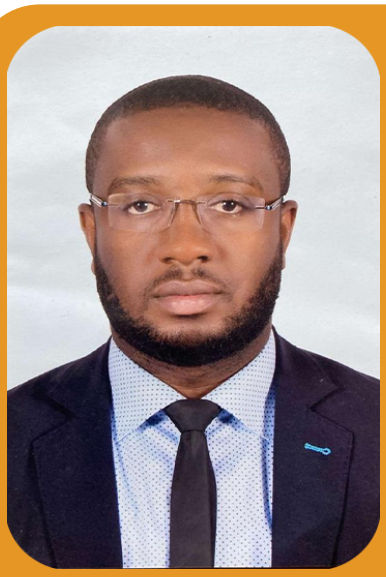
RSSI à la LONACI

Bâtir son programme de sécurité sur une norme reconnue de manière internationale offre plus d'assurance étant donné qu'il y a une démarche clairement définie à suivre.

Cependant selon le contexte, la mise en œuvre de certaines normes peut s'avérer difficile.

Dans ce cas d'autres outils se présentent aux professionnels de la sécurité notamment les directives nationales de Cybersécurité, le panorama des menaces, … sur lesquels il peut s'appuyer pour bâtir son programme et assurer une protection efficace du patrimoine informationnel de son organisation.

Un tel programme n'est pas moins fiable que celui bâti sur une norme.



Fabrice DJIREBO

Consultant en
cybersécurité

Un programme de sécurité repose toujours plus ou moins sur une norme ou un standard ajusté en fonction des besoins de l'entreprise. Et cela permet de rassurer les parties prenantes sur la méthodologie, les contrôles etc…surtout lorsque l'entreprise ne souhaite pas aller jusqu'à la certification.

La certification ne garantie pas forcément que nous avons le niveau de maturité et de sécurité de l'information adéquat pour garantir la pérennité de l'entreprise.

La certification constitue un avantage marketing et concurrentiel visant à rassurer les clients.

Nicaise Kouamé

Responsable infrastructure et sécurité du BNETD / CEO & Founder NKTEK

Le SMSI est considéré comme tel que si et seulement si l'on respecte les exigences normatives de la norme ISO 27001 et les objectifs et mesures de sécurité de son annexe A applicables à l'environnement dans lequel il est mis en œuvre.

La norme est juste la standardisation des best practices dans une industrie.

Un programme de sécurité ne reposant pas sur une norme est viable mais très fastidieux à mettre en place avec son corollaire de risques de biais, de double emploi, de mauvaise structuration de l'information, d'un manque d'informations documentées.
Cette approche est très souvent empirique.

Focus sur un membre

Constant Diby
Responsable informatique
chez KPMG

Titulaire d'un diplôme d'ingénieur en conception option réseaux et télécommunication, je suis certifié CCNA R&S pour ce qui concerne le réseau et ISO 27001 Lead Implémenter pour ce qui concerne la sécurité des systèmes d'informations. L'essentiel des formations auxquelles j'ai participé étant en activité se sont déroulées en Côte d'Ivoire (CISM, ISO27001, CCNA R&S), Afrique du Sud (sur les applications métier interne), France (cybersecurité).

Je commence mon parcours professionnel en 2010 en tant qu'ingénieur systèmes et réseaux.

L'essentiel de la seconde partie de mon parcours se déroule pour l'instant à KPMG Côte d'Ivoire, le bureau régional que j'ai intégré depuis 2013 en tant qu'assistant IT pour ensuite en devenir le responsable informatique en charge de la gestion du support, de la gestion des projets liés au système d'information et de la sécurisation du SI. Il faut signifier que c'est un poste à portée régionale.
De part ma position j'ai pu effectuer des missions d'audit IT notamment au Mali et au Burkina Faso.

Evénements à venir

Assemblée Générale Mixte de l'APSI-CI

Lieu

Abidjan, Côte d'ivoire

Date

28 Mai 2022

Webinar

Thème

Rôles et Responsabilités de la PLCC

Date

04 juin 2022

Lieu

En direct sur la chaine Youtube de l'APSI-CI

Heure

11h00

Webinar

Thème

Droit du citoyen ivoirien en matière de protection de ses données personnelles

Date

18 juin 2022

Lieu

En direct sur la chaine Youtube de l'APSI-CI

Heure

11h00

APSI-CI
LE MAGAZINE

www.apsi.ci

Contacts
+225 0759673513
contact@apsi.ci