RÉPUBLIQUE TOGOLAISE

RAPPORT D'ACTIVITÉS 2022

ANCy
Agence Nationale de la Cybersécurité

AGENCE NATIONALE DE LA CYBERSECURITÉ

RAPPORT D'ACTIVITÉS 2022

SOMMAIRE

MOT DU DIRECTEUR GÉNÉRAL

Le Togo, à l'instar des autres Etats du monde a procédé au renforcement de ses capacités de défense et de sécurité de son cyberespace par la mise sur pied de dispositions juridiques, techniques, financières et techniques efficaces et performantes.

Ce nouveau dispositif institutionnel dédié aux administrations publiques aux entreprises et aux individus, vise à renforcer la résilience des systèmes d'information étatiques essentiels à la continuité des activités économiques et sociétales dans notre pays, face à la multiplication sans cesse croissante des cyberattaques, qui sont de plus en plus organisées et sophistiquées.

Le présent rapport annuel, qui fait le point des activités de l'ANCy au cours de l'année 2022, marque le véritable lancement de notre institution sur le chemin de la sécurité du numérique dans notre pays, avec la poursuite de son processus d'opérationnalisation entamé depuis sa création en février 2019.

Ainsi, l'ANCy, au cours de l'exercice 2022, a enregistré globalement des résultats encourageants dans les différents compartiments de ses activités et de sa gestion, notamment à travers :

- la poursuite du processus de recrutement du personnel ;
- la vulgarisation des textes en vigueur en matière de cybersécurité à travers des ateliers de sensibilisation et de formations ;
- la maîtrise de la gestion financière et budgétaire se traduisant par un solde excédentaire établi à un niveau appréciable ;
- l'organisation d'une série de sessions de sensibilisation et de formation visant le renforcement des capacités humaines, institutionnelles et opérationnelles des acteurs publics et privés de la chaîne de la sécurité des systèmes d'information ;

- le démarrage des actions de communication en direction des acteurs publics et privés du système ainsi que de l'opinion publique sur les enjeux et les défis de la cybersécurité.

Toutefois, il y a lieu de rappeler que l'ANCy n'étant qu'à ces débuts, beaucoup reste encore à faire. C'est pourquoi, je suis persuadé que les recommandations faites pour pallier les insuffisances relevées au cours de l'exécution des activités engagées durant l'exercice sous revu, permettront de mettre en œuvre les actions correctives appropriées dans le but d'accroître durablement la performance et le rôle de l'Agence dans l'accomplissement de ses missions pour la sécurisation des systèmes d'information au Togo.

Je saisis cette opportunité pour exprimer, à l'endroit du comité stratégique de l'ANCy, toute ma déférente reconnaissance et mes vifs remerciements pour sa permanente écoute, disponibilité et sollicitude, qui nous ont permis de faire sereinement face à de nombreux obstacles, qui, il faut le dire, étaient loin d'être franchis d'avance.

À tous les acteurs, notamment les administrations publiques et les opérateurs de services essentiels, je voudrais, aussi, exprimer toute ma gratitude pour les efforts déployés en vue de se mettre au diapason de la réforme et des exigences de l'ANCy, malgré les difficultés rencontrées.

Je voudrais, en outre, dire un grand merci à tous les partenaires techniques et financiers pour leur engagement aux côtés de notre jeune institution afin d'aider le Togo à poursuivre le respect des grands principes qui régissent la gestion de la cybersécurité.

Je voudrais rassurer les uns et les autres et leur rappeler que, comme un petit enfant qui fait ses premiers pas pour devenir adolescent, puis adulte, l'ANCy est déterminée à faire son petit bonhomme de chemin pour se hisser inéluctablement au rang des plus grandes, pour peu qu'on lui fasse confiance et qu'on croit aux hommes et femmes qui l'animent.

Enfin, je reste convaincu que la pour suite des efforts de réglementation, de régulation et de contrôle des systèmes d'information des opérateurs de service essentiels, de même que la poursuite de la dynamique de sensibilisation, de formation et de communication, nous permettront d'accomplir au cours des années à venir, l'ambition de notre pays de devenir, à l'horizon 2025, un hub logistique et un centre d'affaires par excellence, dans la sous-région ouest-africaine.

Commandant GWALIBA Gbota

1. PRÉSENTATION DE L'ANCY

L'ANCy est organisée selon les dispositions du décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité.

1.1 Les attributions

L'Agence Nationale de la Cybersécurité (ANCy) a été créée par le décret n° 2019-026/PR portant organisation, attributions et fonctionnement du 13 février 2019. Sous l'autorité, du Premier Ministre, Président de son comité stratégique, l'ANCy est placée sous la tutelle technique et administrative du ministère en charge de l'économie numérique et de la transformation digitale et du ministère de la sécurité et de la protection civile.

Autorité nationale en matière de sécurité des systèmes d'information au Togo, l'ANCy concourt de manière significative à la définition et à la mise en œuvre de la politique et des orientations stratégiques en matière de cybersécurité. Elle apporte son concours aux services de la République togolaise en matière de défense et de sécurité. Elle est chargée de la sensibilisation des utilisateurs des équipements, des services et installations informatiques, de la prévention des intrusions, de la sécurisation et de la défense de l'ensemble des systèmes d'information.

L'ANCy assure, en outre, la coordination et la riposte aux attaques informatiques. Elle instruit les demandes de qualification et qualifie les produits de sécurité et les prestataires de services de confiance pour les besoins de la sécurité des systèmes d'information au Togo.

La coordination et la riposte aux attaques informatiques sont assurées par Cyber Defense Africa (CDA). Bras technique et opérationnel de l'ANCy, CDA se charge de l'implémentation du Computer Emergency Response Team (CERT) et du Security Operation Center (SOC) à l'échelle nationale, en tant que services délégués par l'ANCy.

1.2 Missions de l'ANCy

Les missions assignées à l'Agence Nationale de la Cybersécurité sont les suivantes :

- Coordonner l'action gouvernementale en matière de sécurité et de défense des systèmes d'information ;
- Répondre aux crises affectant ou menaçant la sécurité informatique des infrastructures essentielles au Togo ;
- Fixer les règles de cybersécurité et veiller à leur application par les divers acteurs ;
- Certifier les dispositifs matériels ou logiciels de cybersécurité en République togolaise ;
- Contrôler le bon fonctionnement du CERT (Computer Emergency Response Team) et du SOC (Security Operation Center) national opérés par CDA ;
- Désigner et auditer les Opérateurs de Services Essentiels (OSE) ;
- Délivrer des agréments aux prestataires en cybersécurité ;
- Participer à la lutte contre la cybercriminalité ;
- Former et sensibiliser le public en cybersécurité.

1.3 Cadre de gouvernance de l'ANCy

Le cadre de gouvernance de l'ANCy est composé de deux organes :

- Le comité stratégique et,
- La direction générale.

1.3.1 Le Comité stratégique

Placé sous l'autorité du Premier Ministre, le comité stratégique est l'organe d'administration et de gestion de l'Agence. À ce titre, il définit, oriente la politique générale de l'ANCy et évalue sa gestion dans les limites de ses attributions.

Le comité stratégique est composé de :

- Le Premier Ministre, Présidente du comité stratégique ;
- Ministre de l'Economie numérique, membre ;
- Ministre de la sécurité, membre ;
- Ministre de la défense, membre ;
- Ministre de la Justice, membre ;
- Deux (2) représentants de la Présidence de la République, membres.

1.3.2 La Direction générale

Elle est assurée par un Directeur général nommé par décret du Président de la République, pour un mandat de trois (3) ans renouvelables une fois.

Sous le contrôle du Comité stratégique, le Directeur général est chargé, entre autres, de :

- Proposer des réformes juridiques et institutionnelles nécessaires à la mise à niveau de la législation nationale au regard du caractère évolutif des menaces technologiques ;
- Négocier et signer selon les directives du comité stratégique les accords et conventions nationaux et internationaux, dans le cadre des missions de l'ANCy ;
- Etablir le plan d'organisation et de fonctionnement et des services de l'Agence.

La Direction générale de l'ANCy comprend les directions suivantes :

- la direction du service administratif et financier ;
- la direction de la réglementation et du contrôle de conformité ;
- la direction de la formation et des appuis techniques.

Par ailleurs, le Directeur général est assisté dans ses fonctions par un conseiller technique, un conseiller en communication et une assistante de direction.

2. APERÇU DU CADRE JURIDIQUE

2.1 Les textes communautaires

L'Agence Nationale de la Cybersécurité (ANCy) a été créé

La directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

2.2 Les textes africains

Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel adoptée à Malabo en Guinée Équatoriale le 27 juin 2014.

2.3 Les textes nationaux

Il s'agit de la loi n°2018-026 du 07 décembre 2018 modifiée par la loi n°2022-009 du 22 juin 2022 sur la cybersécurité et la lutte contre la cybercriminalité.

En application de cette loi, le gouvernement a pris un certain nombre de décrets et un arrêté, notamment :

- le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité ;
- le décret n° 2019-095/PR du 8 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- le décret n° 2021-045/PR du 29 avril 2021 portant nomination du directeur général de l'agence nationale de la cybersécurité ;
- le décret n° 2022-090/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- l'arrêté N° 2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise.

- Rédiger un recueil des textes en cybersécurité


SYMBOLS

3. GESTION ADMINISTRATIVE DE L'ANCY

Le processus de recrutement lancé dans le cadre de l'opérationnalisation de l'ANCy a permis de recruter une (1) assistante de direction, un (1) Directeur Administratif et Financier et un (1) Directeur de la Réglementation et du Contrôle de Conformité. Le personnel recruté a pris fonction à la fin du mois de juillet 2022.

En dehors de ce recrutement, quatre (4) jeunes cadres ont été mis à la disposition de l'ANCy, dans le cadre du Programme présidentiel d'excellence, pour une durée de trois (3) ans.

Ainsi, au 31 décembre 2022, l'effectif global de l'ANCy est de huit (8) personnes.

4. LA MISE EN ŒUVRE DES MISSIONS

4.1 Les missions opérées par l'ANCy

4.1.1 Sommet de la cybersécurité Lomé 2022

Les 23 et 24 mars 2022, Lomé a accueilli le 1er sommet de la cybersécurité, placé sous le thème "Faire de la cybersécurité une priorité absolue pour les États africains". Ce sommet coorganisé par la République togolaise et la Commission Economique des Nations Unies pour l'Afrique (CEA) a abouti à l'adoption de la « Déclaration de Lomé » des chefs d'États et de gouvernement. Cette déclaration identifie les pistes de coopération et de coordination entre les parties prenantes, tout en marquant un engagement renouvelé en faveur de la lutte contre les cybermenaces.

Figure 1: Photo prise lors du sommet sur la cybersécurité

Le prix du Champion d'Afrique de la cybersécurité a été décerné au Président de la République togolaise, S.E.M. Faure Essozimna GNASSINGBE, par Mme Vera Songwe, Secrétaire générale adjointe de l'Organisation des Nations Unies (ONU) et secrétaire exécutive de la Commission économique des Nations Unies pour l'Afrique (CEA). Cette reconnaissance vise à récompenser les efforts réalisés par le Togo dans la lutte contre la cybercriminalité et la protection des données à caractère personnel.

Figure 2: Remise du prix du champion d'Afrique de la cybersécurité au Président de la République

Plusieurs sujets d'actualité ont été abordés au cours des panels de discussion. Les participants composés de spécialistes en cybersécurité et en développement numérique se sont penchés sur la conception d'approches innovantes pour répondre aux enjeux de cybersécurité en Afrique, les enjeux de cybersécurité dans les politiques publiques en Afrique, le financement et l'opérationnalisation des stratégies de cybersécurité sur le continent.

Partenaire de cette première édition et autorité nationale en matière de cybersécurité au Togo, l'ANCy a joué un rôle clé durant ces deux jours d'échange. L'agence a activement pris part aux différents panels de discussion avec des experts et professionnels en cybersécurité sur des problématiques actuelles. L'équipe de l'Agence et son bras opérationnel, CDA ont saisi cette opportunité pour sensibiliser et initier les participants aux bonnes pratiques en cybersécurité à travers des démonstrations en temps réel de cyberattaques.

Partenaire de cette première édition et autorité nationale en matière de cybersécurité au Togo, l'ANCy a joué un rôle clé durant ces deux jours d'échange. L'agence a activement pris part aux différents panels de discussion avec des experts et professionnels en cybersécurité sur des problématiques actuelles. L'équipe de l'Agence et son bras opérationnel, CDA ont saisi cette opportunité pour sensibiliser et initier les participants aux bonnes pratiques en cybersécurité à travers des démonstrations en temps réel de cyberattaques.

4.1.2 Réglementation

L'année 2022 a été marquée par la finalisation et la validation de deux (2) projets de textes. Il s'agit de :

- Arrêté n° 2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise;
- Vu le décret n° 2022-090/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;

Les équipes techniques de l'Agence sont à pied d'œuvre pour finaliser les référentiels et pour acquérir les outils et les méthodes techniques de qualification des prestataires de service de confiance, des produits de sécurité et d'agrément des centres d'évaluation.

4.1.3 Communication

La stratégie de communication de l'ANCy s'articule, entre autres, autour de l'information et de la sensibilisation de l'opinion publique, des administrations publiques et des OSE sur les enjeux de la cybersécurité et les bonnes pratiques à adopter aussi bien individuellement que collectivement.

Plusieurs activités ont été organisées par l'ANCy au cours de l'année 2022 pour poser les bases d'une communication en vue de favoriser, par l'information, l'adhésion des acteurs et des partenaires à la nouvelle dynamique.

Entre autres actions, on peut citer :

- la vulgarisation des textes légaux et réglementaires régissant la cybersécurité ;
- l'information et la sensibilisation organisées à l'intention des acteurs (hommes de média, société civile, secteur privé et administration et OSE);
- le lancement et l'animation du site Internet et des réseaux sociaux ;
- l'information du public sur les actualités à l'ANCy ;
- la couverture médiatique des activités (ateliers, formations et rencontres diverses) ;
- la publication de communiqués de presse ;
- la participation à plusieurs émissions audiovisuelles sur taxi FM, Canal FM et Zéphyr FM.
- les Publications sur les plateformes du CERT des 10 commandements pour une hygiène numérique sur la page Facebook du CERT.tg et Cyber-Quiz sur les pages Facebook et twitter du CERT.tg et de l'ANCy.
- l'organisation d'une réunion d'information et de sensibilisation aux ministres, autorités sectorielles des futurs OSE sous le haut patronage de Son Excellence Madame le Premier Ministre;
- l'organisation du cybersécurité challenge sur le thème : « cybercriminalité au Togo : protégez-vous des arnaques en ligne et renforcez vos mots de passe ».

4.1.4 Désignation des opérateurs de services essentiels (OSE)

Un opérateur de services essentiels (OSE) est un statut caractérisant une entité publique ou privée qui fournit un service essentiel et qui est tributaire de réseaux informatiques ou de systèmes d'information et dont l'arrêt aurait un impact significatif sur le fonctionnement de l'économie ou la société.

L'Agence Nationale de la cybersécurité fixe les règles de cybersécurité que les opérateurs de services essentiels doivent respecter.

Ces règles prévues dans l'arrêté portant adoption des règles de cybersécurité en date du 29 juin 2022 définissent les mesures appropriées dans les domaines de la gouvernance de la sécurité des réseaux et systèmes d'information, la protection des réseaux et systèmes d'information, la défense des réseaux et systèmes d'information et la résilience des activités.

Elles ont pour objet de garantir un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances et visent notamment à s'assurer que les opérateurs de services essentiels identifient les risques qui menacent la sécurité des réseaux et systèmes d'informations nécessaires à la fourniture des services essentiels et prennent les mesures techniques et organisationnelles appropriées pour gérer ces risques, pour prévenir les incidents qui compromettent la sécurité desdits réseaux et systèmes d'information ainsi que pour en limiter l'impact, de manière à garantir la continuité de leurs services.

4.1.5 Les ateliers de sensibilisation

Dérouler des sessions de sensibilisation sur les enjeux de la cybersécurité et les bonnes pratiques à adopter, font également partie intégrante des principales missions de l'Agence Nationale de la Cybersécurité ; l'objectif étant de transmettre aux togolais, des connaissances et outils nécessaires en cybersécurité pour qu'ils se protègent contre les attaques des cybercriminels, afin d'instaurer une véritable culture de la cybersécurité, nécessaire pour une effective résilience nationale en cybersécurité.

À ce titre, l'administration, les institutions publiques et les utilisateurs d'Internet ont été les principales cibles des activités de sensibilisation de l'ANCy au cours de l'année 2022 qui a organisé des tournées, ateliers, symposiums et jeux.

4.1.5.1 Atelier de présentation des règles de cybersécurité

Le 22 septembre 2022, l'Agence Nationale de la Cybersécurité (ANCy), en collaboration avec Cyber Defense Africa (CDA) a organisé un atelier de présentation des règles de cybersécurité.

L'objectif était de présenter les règles de cybersécurité aux Opérateurs de Services Essentiels (OSE) et aux équipes de l'administration publique. Elle a été présidée par le Ministre de la Sécurité et de la Protection Civile, le Général Damehame Yark.

En effet, adoptées par arrêté n° 2022-040/PMRT du 29 juin 2022, les règles de cybersécurité permettront aux OSE et à l'administration, de disposer des outils pour l'identification des risques qui menacent la sécurité de leurs réseaux et systèmes d'information puis de mettre en œuvre les actions techniques et organisationnelles appropriées pour gérer ces risques. Ces actions visent à prévenir les incidents et/ou limiter leurs impacts de sorte à garantir la continuité des services qu'ils fournissent.

Figure 3:Photo de famille lors de l'atelier de présentation des règles de cybersécurité

4.1.5.2 Ateliers de présentation et de pré validation de la stratégie nationale de la cybersécurité

L'ANCy, dans son rôle d'autorité de régulation et de contrôle de l'écosystème de la cybersécurité, a en charge l'élaboration de la stratégie nationale de la cybersécurité.

C'est dans cette logique que le projet de stratégie nationale de la cybersécurité a été présenté dans un premier temps, lors de l'atelier du 18 octobre 2022 à tous les acteurs et parties prenantes du cyberespace togolais de différents secteurs. L'implication des différents acteurs du cyberespace dans l'élaboration de la stratégie était très importante pour l'ANCy pour avoir une cohésion et une compréhension globale entre tous les acteurs de la cybersécurité.

Cet atelier a permis de présenter le draft de la stratégie nationale de la cybersécurité rédigée par l'ANCy, et d'avoir les avis et observations de tous les autres acteurs. Cette démarche a permis à l'ANCy d'affiner le projet de stratégie et de le rendre le plus inclusif possible.

Figure 4:Photo prise lors de l'atelier de validation de la stratégie nationale de la cybersécurité

Un mois après, un autre atelier a été à nouveau organisé par l'ANCy en vue d'échanger, en présence de tous les acteurs impliqués dans le processus, à propos de chacun des avis, amendements, propositions et pistes de réflexion proposées par les partenaires et parties prenantes sus-indiquées. La rencontre qui s'est tenue du 23 au 25 novembre 2022 a permis de s'accorder sur la dernière version du projet de stratégie aux différents acteurs du cyberespace togolais.

Cette stratégie quinquennale (2023-2028), une fois adoptée en conseil des ministres et promulguée par le Président de la République, permettra de mettre en œuvre la politique nationale de la cybersécurité qui assurera aux entreprises et aux citoyens togolais, la continuité des activités sociétales et économiques, dans la quiétude, la paix et la stabilité.

Figure 5: Photo prise lors de l'atelier de prévalidation de la stratégie nationale de la cybersécurité

4.1.5.3 Tournée nationale de sensibilisation sur les enjeux de la cybersécurité

Conformément à ses attributions, l'ANCy à la faveur du cyber/mois célébré chaque année en octobre à travers le monde, pour promouvoir la culture de la cybersécurité, a entamé du 24 octobre au 04 novembre 2022, une campagne nationale de sensibilisation dans les cinq (5) régions du Togo.

Dans le cadre de cette 1ère édition nationale, l'ANCy s'est fixée comme objectif, d'attirer l'attention des autorités locales, des responsables des services déconcentrés sur les enjeux de la cybersécurité et les efforts collectifs nécessaires à mener pour prévenir les cyber intrusions et les escroqueries

Cette tournée a permis à l'ANCy de présenter aux participants l'écosystème de la cybersécurité du Togo, les règles de cybersécurité du Togo, les bonnes pratiques et mesures pour se prémunir contre les actes de cybercriminalité.

En effet, en collaboration avec Cyber Defense Africa (CDA), les citoyens et organisations ont été entretenus sur les types de cybermenace et les modes opératoires utilisés par le système criminel pour l'atteinte de leur objectif. Les différents échanges leur ont permis de cerner l'écosystème de la cybersécurité, et plus spécifiquement comment est-ce qu'il a été réfléchi, pensé et mis en place. Ils ont été amenés à découvrir également l'outil de réponse et d'alerte aux incidents informatiques, le CERT.tg.

Figure 6: Photo prise lors de la tournée de sensibilisation de l'ANCy sur les enjeux de la cybersécurité

4.1.5.4 Participation à l'atelier national de sensibilisation des professionnels des médias sur les enjeux du numérique

Dans le cadre des ateliers nationaux de sensibilisation des professionnels des médias sur les enjeux du numérique et l'implication des nouvelles lois adoptées dans l'exercice de leur profession pour une bonne pratique démocratique, organisés respectivement les 25 et 26 ; 29 et 30 août 2022 ; 1er et 2 septembre 2022 à Lomé, Kara et à Atakpamé, par les ministères chargés des droits de l'homme et de la communication, sous le thème :

«Médias, démocratie numérique et participation citoyenne», l'ANCy a présenté des communications sous le thème « Rôle des médias dans la promotion d'un cyberspace sûr ».

Cette communication animée par le Commandant Gbota GWALIBA, Directeur général de l'Agence Nationale de la Cyber sécurité (ANCy), visait à présenter aux organisations professionnelles du secteur de la presse, les journalistes Radio et télé, les Web journalistes et la presse écrite, l'écosystème de la cybersécurité du Togo et surtout à leur expliquer leur importance stratégique dans acquisition d'une culture de la cybersécurité dans notre pays, la promotion des compétences nationales en la matière, le positionnement du Togo comme acteur majeur de la cyber sécurité en Afrique, la protection des infrastructures critiques et la collaboration avec les différents acteurs, dont les médias.

La contribution des médias est incontournable et elle doit se faire en passant par leur implication à travers les renforcements de capacités sur les termes techniques du phénomène, la visibilité de l'ANCy par des programmes d'émissions de sensibilisation surtout à l'égard des jeunes.

4.1.5.5 Participation au HackerLab 2022

Lancée officiellement le lundi 10 octobre 2022, la 5ème édition nationale et la 1ère élargie aux pays de la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) du HACKERLAB 2022 : ÉDITION CEDEAO (BÉNIN), dans le cadre de son projet « Criminalité organisée : Réponse de l'Afrique de l'Ouest sur la cybersécurité et la lutte contre la cybercriminalité (OCWAR-C) » financé par l'Union Européenne, co-organise avec le bjCSRIT, s'est déroulé du 10 au 12 octobre 2022 à Cotonou (Bénin).

Placée sous le thème : "Jeunesse CEDEAO engagée contre les Cybermenaces", le HackerLab est une compétition qui permet de détecter et de former à terme, des hackers éthiques, un maillon essentiel dans la lutte contre la cybercriminalité.

Il s'agissait d'un concours d'affrontement de 48 heures non-stop sur des épreuves d'exploitation système, d'exploitation web, de reverse engineering et de forensic. Au terme de ces épreuves farouchement disputées, c'est l'équipe « Warning du Bénin » qui surclasse finalement tous ses challengers dont le plus farouche aura été le Nigeria, suivi de la Mauritanie.

Pour la grande finale de ce concours, Cyber Défense Africa (CDA) le bras opérationnel de l'Agence Nationale de la Cybersécurité (ANCy), a su former l'équipe des trois (3) talents représentant le Togo dans cette compétition. À l'issue de la compétition, la délégation togolaise, pour une première participation, a honorablement défendu les couleurs nationales en se positionnant en milieu de classement face à des équipes qui ont l'habitude de ces rencontres.

En vue de renforcer leurs compétences dans la perspective des rencontres à venir, l'ANCy a offert des formations en sécurité informatique à ces jeunes talents.

Figure 7: Photo prise lors du lancement de la 5e édition nationale de HackerLab au Bénin

4.1.5.6 Jeu-concours Cyber Quiz

Du 25 novembre au 10 décembre 2022, l'ANCy a lancé le jeu Cyber Quiz en partenariat avec Cyber Defense Africa (CDA) et le Groupe Vivendi Africa (GVA) Togo. Piloté par l'ANCy, le Cyber Quiz est un jeu qui vise à sensibiliser les utilisateurs d'Internet sur les enjeux de la cybercriminalité à travers une série de questions à choix multiples liés à la cybersécurité.

Les lauréats de ce jeu ont bénéficié de : une (1) tablette smartphone, un forfait d'abonnement Canalbox valable pendant six (06) mois et des goodies.

Il faut rappeler que ce challenge a été possible grâce à la présence effective de l'ANCy sur les réseaux qui dans sa stratégie de communication en a fait un outil clé de sensibilisation ; ainsi qu'avec le constant accompagnement de, CDA et GVA Togo.

Figure 8: Remise de prix aux gagnants du Cyberquiz Challenge par les DG de GVA, ANCy et CDA

4.1.6 La lutte contre la cybercriminalité

La cybercriminalité est un phénomène qui touche de plus en plus de pays dans le monde, y compris le Togo. Il s'agit de l'ensemble des infractions commises sur les réseaux informatiques ou par le biais des technologies de l'information et de la communication. Ces attaques qui visent à compromettre la confidentialité, l'intégrité et la disponibilité de nos données et de nos systèmes d'information ont des conséquences graves sur notre sécurité nationale, notre économie et notre société.

De façon générale, ces attaques se répartissent en quatre catégories principales : les attaques par déni de service (DDoS), qui visent à saturer les ressources d'un serveur ou d'un réseau ; les attaques par rançongiciel (ransomware), qui chiffrent les données d'une victime et exigent une rançon pour les déchiffrer ; les attaques par hameçonnage (phishing), qui usurpent l'identité d'une personne ou d'une organisation pour obtenir des informations sensibles ; et les attaques par injection de code malveillant (malware), qui infectent un système avec un logiciel malveillant.

Selon les statistiques de la police et de la gendarmerie nationales, quatre-vingt-six (86) cybercriminels impliqués dans des incidents de sécurité informatique, tels que l'atteinte à un système informatique, la cyber escroquerie, l'arnaque, le faux et groupements de malfaiteurs, ont été déférés en 2022.

Comme le montrent les figures 12 et 13 du présent rapport d'activité relatif aux incidents de cybersécurité traités par le CERT national en 2022, le nombre relativement faible de cybercriminels appréhendés par les forces de défense et de sécurité de notre pays, se justifie par deux raisons :

D'une part, la plupart des victimes préfèrent ne pas porter plainte ou ne pas signaler les incidents informatiques dont elles ont connaissance, pour des raisons liées à nos mœurs et croyances.

D'autre part, il s'agit dans la plupart du temps, d'opérations réalisées dans un espace immatériel qui ignore les frontières des États et les législations propres à ceux-ci. En raison de ces particularités, Internet constitue en quelque sorte une « zone de non droit ».

Dans le cas de la cyber escroquerie, le mode opératoire consiste à envoyer diverses photos sous différentes identités notamment celles de riches hommes d'affaires, des militaires américains, des hautes personnalités ou des photos de jeunes filles, pour appâter leurs victimes qui, pour la plupart, sont des asiatiques, des américaines et australiennes à qui, de gros sous ont été spoliés.

Une autre pratique cybercriminelle bien ancrée dans le cyberspace togolais est le phishing ou « hameçonnage » en français. Le phishing est une technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de cartes de crédit au moyen de messages ou de sites qui usurpent l'identité d'institutions ou entreprises ou d'individus. La technique du phishing peut prendre plusieurs formes en passant par un site web, des mails, des SMS ou des appels vocaux. En envoyant un email à sa victime, le cybercriminel en profite pour lui demander de mettre à jour ses coordonnées bancaires ou personnelles en cliquant sur un lien qui dans la réalité redirige cette dernière vers un faux site Web.

En dehors du vol de données, la célèbre « arnaque nigériane », connue sous l'appellation de fraude 419, est largement répandue dans notre pays. La méthode nigériane consiste à envoyer des courriels en espérant que parmi les destinataires du message, certains mordront à l'appât. En règle générale, les adresses électroniques qui sont utilisées sont récupérées sur des listes de diffusions ou des forums sur internet. Pour ce type d'arnaque, les pratiques les plus habituelles s'articulent autour d'un héritage fictif bloqué dans une banque, un gain à la loterie inexistante, une demande d'aide venant d'une personne inconnue, le règlement d'un achat effectué en ligne, etc.

Les impacts de ces cyberattaques sont multiples et peuvent être très graves. Par exemple, une attaque contre le réseau électrique peut entraîner des coupures de courant, affectant la fourniture d'eau potable, les services de santé ou les transports. Une attaque contre le système d'information d'un ministère peut compromettre la sécurité des données sensibles ou la crédibilité du gouvernement. Une attaque contre une plateforme numérique peut nuire à l'accès à l'information ou à l'éducation.

Face à ce constat alarmant, le gouvernement a mis en place une politique nationale de cybersécurité, qui repose sur trois axes : la prévention, la protection et la réaction. La prévention vise à sensibiliser les acteurs publics et privés aux bonnes pratiques de sécurité informatique, à renforcer les compétences des professionnels du domaine et à promouvoir la recherche et l'innovation dans ce secteur. La protection vise à sécuriser les infrastructures critiques du pays, à mettre en place des normes et des standards de sécurité et à renforcer la coopération régionale et internationale en matière de cybersécurité. La réaction vise à détecter et à analyser les incidents de sécurité informatique, à y apporter une réponse adaptée et à poursuivre les auteurs de ces actes.

La prise de conscience de ces enjeux par les plus hautes autorités de notre pays s'est traduit par la mise en place d'un cadre juridique et institutionnel complet en matière de cybersécurité, à travers l' adoption dès 2018, de la loi sur la cybersécurité et la lutte contre la cybercriminalité, la mise en place des structures dédiées à la cybersécurité, telles que l'Agence nationale de cybersécurité (ANCy), qui est chargée de coordonner les actions de prévention, de protection et de réaction face aux incidents cybernétiques et un Centre national de réponse aux incidents de cybersécurité (CERT.tg) opéré par Cyber Defense Africa (CDA).

A cette mesure s'ajoute l'organisation du premier sommet international sur la lutte contre la cybercriminalité en Afrique en mars 2022, avec la participation de hauts responsables et d'experts du continent.

Toutes ces actions ont permis de ralentir considérablement les velléités de ces cybercriminels, recherchés pour la plupart au Benin, en Côte d'Ivoire et au Nigeria, qui pensaient trouver au Togo une terre d'accueil.

Voilà pourquoi, dans la perspective des années à venir, de nombreuses autres mesures, notamment le renforcement des capacités des forces de l'ordre et des magistrats, sera davantage accentué.

4.2 Les missions de l'ANCy opérées par Cyber Defense Africa (CDA)

4.2.1 Présentation de Cyber Defense Africa S.A.S (CDA)

Issu d'un partenariat stratégique entre la République togolaise et la société polonaise Asseco Data Systems S.A. (ADS), la société Cyber Defense Africa S.A.S. (CDA) est mandatée par la République togolaise pour assister les institutions, organisations et sociétés publiques et privées togolaises dans la sécurisation de leurs systèmes d'information. CDA porte la responsabilité opérationnelle de la cybersécurité nationale aux côtés de l'Agence Nationale de la Cybersécurité (ANCy) et fournit un service de Computer Emergency Response Team (CERT) national ainsi qu'un service de Security Operations Center (SOC) dédié à la surveillance de la sécurité des réseaux et des systèmes d'information des clients de la société.

CDA a été créée en septembre 2019, le SOC de CDA est devenu opérationnel en septembre 2020 et le service de CERT national (CERT.tg) a été lancé en février 2021. L'année 2022 marque par conséquent notre deuxième année complète d'opérations. Au fil de ces deux années, CDA a connu une croissance remarquable, notamment en termes d'effectifs, de partenariats internationaux et de base clientèle. Cela a permis de réaliser de grands projets et d'atteindre de nouveaux sommets. Dans ce présent rapport, nous passerons en revue les activités CERT et SOC réalisées en 2022 et explorerons comment notre croissance continue a permis d'atteindre ces objectifs.

Le modèle PPP est structuré de telle sorte que le CERT est offert comme un service principalement gratuit au public. Le CERT alerte la population des vulnérabilités et sensibilise le public sur les moyens de se protéger contre les attaques. Le CERT fournit également des informations clés sur la publication des correctifs pour les vulnérabilités identifiées. Le SOC, quant à lui, est un service payant qui fournit une cybersécurité en tant que service sur mesure destinée aux Opérateurs de Services Essentiels, aux entreprises, aux institutions publiques et à d'autres parties intéressées.

4.2.2 Répartition des rôles entre l'ANCy et CDA

L'ANCy en tant qu'autorité régalienne, régule le cyberespace togolais. L'ANCy coordonne les activités et les relations entre les différents acteurs du secteur, pilote les programmes nationaux de cybersécurité et contrôle l'application des lois et des différents textes du secteur.

L'ANCy surveille et contrôle les services qu'elle délègue à CDA par un contrat de délégation de service contenant les éléments de mesures de performances claires et mesurables.

CDA en tant que bras opérationnel de l'ANCy est en charge :

- D'opérer le CERT national (CERT.tg).
- D'opérer le SOC national pour le suivi et l'accompagnement de la sécurisation des Opérateurs de Services Essentiels.
- De la sensibilisation des usagers des équipements, des services et installations informatiques, de la prévention des intrusions, de la sécurisation et de la défense de l'ensemble des systèmes d'information.
- De la coordination de la riposte aux attaques informatiques.
- Du support technique pour le compte de l'ANCy.

4.2.3 Les services du CERT.tg et du SOC national

Le CERT national est responsable de la fonction générale de surveillance des risques au Togo associés au cyberespace, de la protection de la société civile contre les utilisations malveillantes des outils ou services Internet, ainsi que des réponses à apporter aux attaques qui peuvent se produire. L'équipe CERT fournit ces services gratuitement 24 heures sur 24 et 7 jours sur 7 au gouvernement togolais, au grand public et à toute organisation au Togo :

- Analyse des données sur la menace dans le cyberespace togolais selon les informations recueillies auprès de la population togolaise, des entreprises, administrations et autres organisations togolaises ainsi que de la communauté mondiale des CERT et CSIRT ;
- Traitement, réponse et coordination des incidents de cybersécurité nationaux ;
- Notification des menaces détectées et communiquées par les citoyens togolais au centre d'appel, par courrier électronique et sur le site web ;
- Annonce des intrusions, des vulnérabilités et des bulletins de sécurité;
- Analyse avancée des logiciels malveillants au niveau national et/ou international ;
- Rapports sur les tendances des cyberattaques et leur impact potentiel sur le pays ;
- Formation générale à la cybersécurité et campagnes de sensibilisation proposées au grand public, aux écoles, aux universités, etc. ;
- Réalisation d'audits de sécurité et délivrance de certificats de conformité sous la supervision de l'ANCy ;
- Participation et contribution à des études techniques spécifiques ou à des projets de recherches et développements sur la cybersécurité ;
- Participation à l'élaboration de normes de cybersécurité dans tout le pays.

L'équipe SOC fournit des services payants 24 heures sur 24 et 7 jours sur 7 aux opérateurs de services essentiels et à toutes organisations souhaitant bénéficier de services de protection proactive en cybersécurité. Elle se consacre à la sécurité des entreprises qu'elle protège et utilise le soutien et les services de l'équipe CERT lorsque cela est nécessaire. Le SOC fonctionne comme une société de services en cybersécurité avec des prestations de type services managés dits « SOC as a Service » :

- Administration et maintenance de l'infrastructure SIEM (Security Information & Event Management) national et/ou sur le site de chaque organisme bénéficiant des services SOC ;
- Surveillance sur mesure des événements de sécurité 24 heures sur 24 et 7 jours sur 7 ;
- Détection et identification des menaces et des attaques ciblées ;
- Réponse aux menaces et mesures correctives (en collaboration au besoin avec l'équipe CERT) ;
- Assistance dans le processus de correction et de rétablissement du système d'information (en collaboration avec l'équipe CERT) ;
- Analyse ciblée des logiciels malveillants (en collaboration avec l'équipe CERT) ;
- Analyse et gestion des vulnérabilités inhérentes à l'organisme protégé ;
- Rapports périodiques ;

L'équipe SOC délivre également d'autres prestations nécessaires à la sécurisation des systèmes d'information des organismes protégés :

- Conseil en cybersécurité (rédaction de politiques de sécurité des systèmes d'information, réalisation de cartographies des infrastructures essentielles, autres…) ;
- Formations avancées en cyber sécurité;
- Intégration de solutions de cybersécurité ;
- Audits et tests d'intrusions.

4.2.4 Les chiffres clés de 2022

4.2.4.1 Données collectées sur l'année 2022

Figure 9- Donnés collectées, événements par secondes et incidents traités

Sur l'année 2022, CDA a surveillé via son service SOC, le réseau E-Gouv, les équipements réseaux, serveurs et applications du MENTD et ceux de CDA. Au total, les systèmes ont analysé plus de 50 Téraoctets de données provenant des équipements réseau, des systèmes et aussi des applications surveillées telles que la plateforme Novissi, la plateforme voyage.gouv.tg ou encore la plateforme vaccin.gouv.tg.

Ces données analysées représentent 64 015 journaux d'événements (logs) reçus et traités chaque seconde.

Ces logs sont corrélés et analysés dans le but de rechercher des anomalies dues à une cyberattaque. Les analystes SOC de CDA ont ainsi traité 46 070 incidents de cybersécurité (ou anomalies) au cours de l'année 2022.

4.2.4.2 Evolution des données collectées

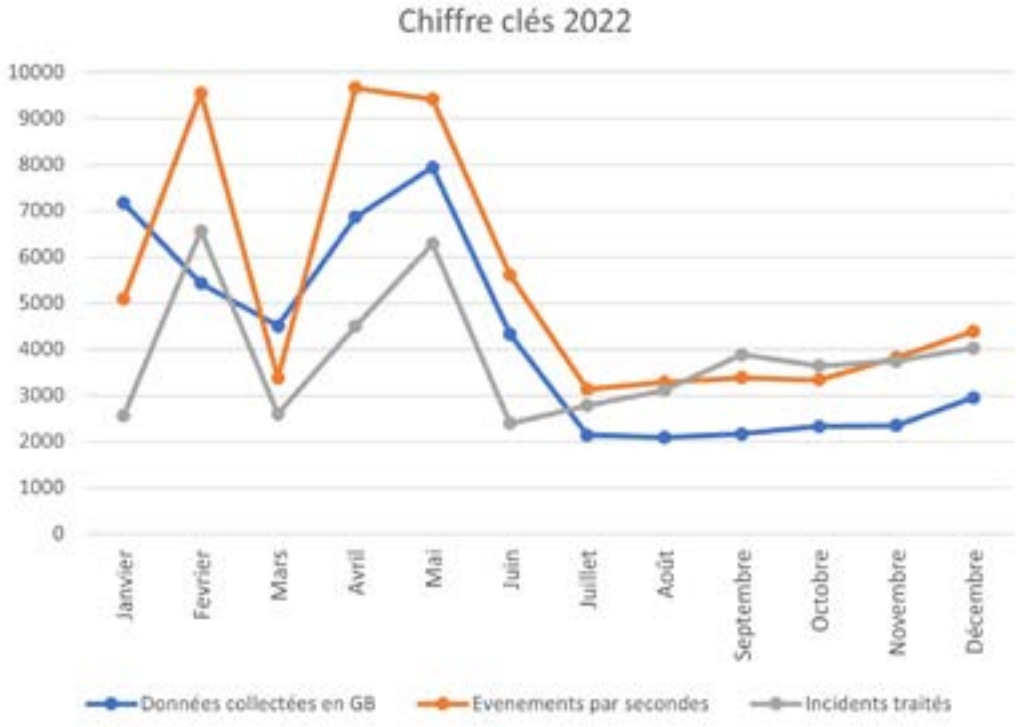

Figure 10 - Evolution des données collectées en 2022

L'évolution des données collectées

Les données et les Événements Par Seconde (EPS) collectés de janvier à décembre 2022 ont considérablement varié au cours de cette période avec un pic en février et avril, respectivement 9 547 et 9 661 EPS, et un creux en juillet avec seulement 3 134 EPS.

Après les cinq premiers mois, on a eu une diminution conséquente du nombre d'événements par seconde qui s'est plus ou moins maintenue jusqu'en décembre même si on note une légère hausse au dernier mois de l'année.

Cette diminution correspond à la période où certains équipements E-Gouv ont cessé d'envoyer les logs aux systèmes de surveillance du SOC CDA en raison de l'expiration de la licence d'un module du pare-feu HUAWEI. Cela a pour conséquence que le SOC de CDA est limité dans la détection des incidents de sécurité sur le réseau E-Gouv.

L'évolution des incidents

Les incidents de cybersécurité sont le résultat des règles de corrélations définies dans l'outil SIEM par les équipes CDA. Dans le cadre de l'amélioration continue du Service SOC, CDA affine régulièrement (fine tune) non seulement les règles de corrélation, mais aussi la sévérité des incidents. Ainsi, au cours de l'année 2022, nous avons connu une augmentation des incidents en février et mai avec un pic en février qui est dû à la communication récurrente autour du CERT.tg et de CDA et aux activités de remédiation de E-Gouv de la vulnérabilité critique Log4j que le monde a connu en fin 2021 et début 2022. En effet, plus de citoyens et d'entreprises ayant pris connaissance du CERT y déclarent plus d'incidents, mais surtout, plus d'attaquants tentent de pénétrer le réseau de CDA et attaquer le site Web du CERT. À partir de mai 2022, CDA a procédé à la sensibilisation de 25 ministères et administrations publiques dont la plupart sont des utilisateurs du réseau E-Gouv. Cela a permis de réduire significativement le nombre d'incidents détectés sur le réseau E-Gouv entre juin et décembre 2022.

4.2.5 Activités CERT.tg en 2022

4.2.5.1 Traitement des Incidents CERT

CDA a traité 308 incidents CERT au cours de l'année 2022 dont **131 vrais positifs**.

4.2.5.2 Evolution des incidents traités

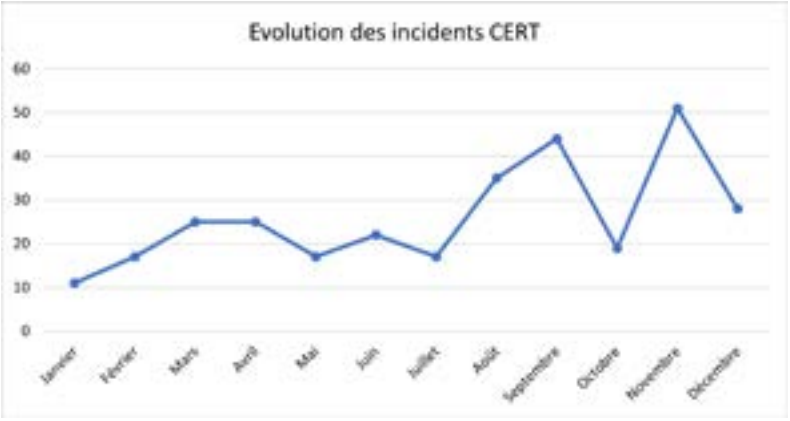

Figure 12 - Evolution des incidents CERT

Les services CERT sont principalement destinés aux citoyens. Nous constatons une évolution des incidents au fur et à mesure que la communication autour de l'ANCy, de CDA et du CERT évolue. En effet, d'août à décembre 2022, l'ANCy a organisé des ateliers de sensibilisation à l'endroit des professionnels de médias, des ateliers de présentation des règles de cybersécurité au Togo et une tournée nationale de sensibilisation sur les enjeux de la cybersécurité et cybercriminalité pour ne citer que ceux-là.

Ces événements ont été couverts par les médias et le Directeur général de l'ANCy a eu l'occasion d'expliquer aux médias présents, le rôle du CERT.tg.

Ainsi, des campagnes d'attaques qui passaient inaperçues du CERT, ont pu être déclarées par les citoyens. Entre autres, 23 incidents de phishing, 16 incidents de Ransomware, 20 incidents d'escroquerie en ligne ont été signalés.

4.2.5.3 Répartition des incidents traités

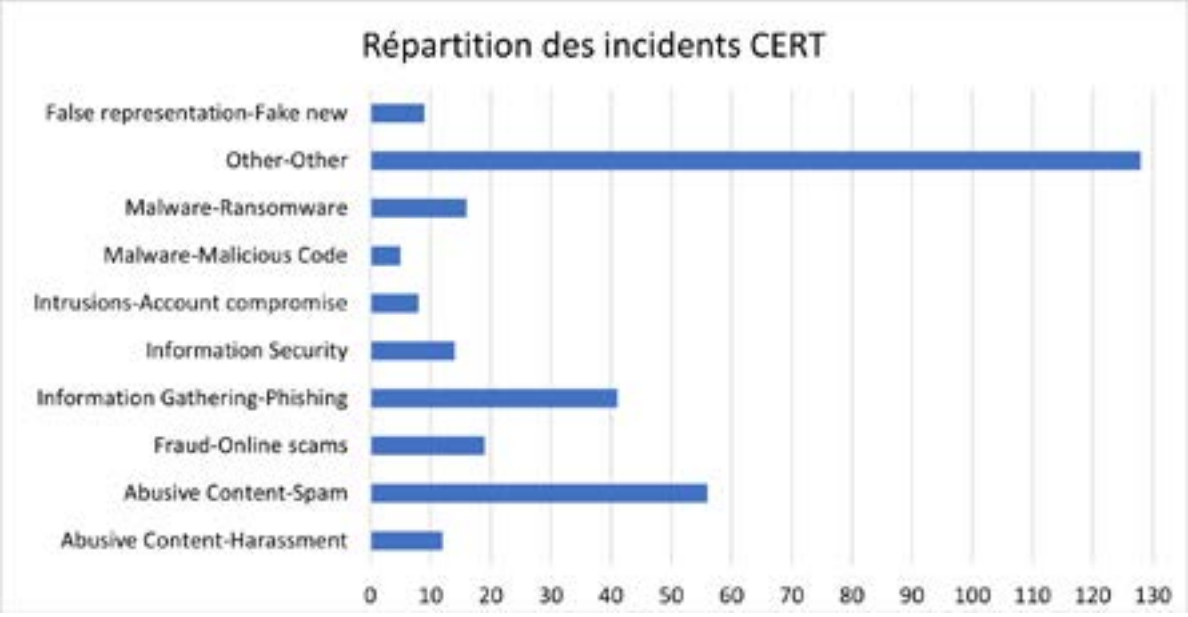

Figure 13 - Répartition des incidents CERT traités

Les incidents les plus traités par le CERT.tg sont les campagnes de Ransomware, de phishing, les fraudes en ligne et les spams. Les incidents les plus critiques sont les ransomwares de la SNB, de la CRRH-UEMOA et de la banque centrale de la GAMBIE, la campagne de phishing sur les domaines gouv.tg et sur le réseau Moov Africa Togo, la vulnérabilité sur un serveur de l'Office du BAC ainsi qu'une menace de publication de données sur le gouvernement congolais sur le darknet.

4.2.6 Audit de sécurité des applications portées par le gouvernement togolais

CDA a procédé à l'audit des applications web suivantes :

Entité gouvernementale	Application auditée
Ministère de l'économie maritime, de la pêche et de la protection côtière	Togo-Maritime
Ministère du commerce de l'industrie et de la consommation locale	Togognim
Ministère des enseignements primaire, secondaire, technique et de l'artisanat	Bac1 et BEPC
Ministère de l'économie numérique et de la transformation digitale	FaitEtatCivil – PRISE eVISA- Service Public

Tableau 1: Liste des applications auditées par CDA

4.2.7 Collaboration avec les forces de l'ordre

CDA a collaboré avec les forces de l'ordre lors d'une mission d'Interpol en septembre 2022, sur les points ci dessous :

1. Assistance sur les missions d'Interpol
    - Investigation sur les adresses IP et domaines malveillants détectés par Interpol afin d'ordonner leurs fermetures et/ou de trouver les personnes qui en sont responsables.
2. nvestigations OSINT (technique de renseignement) demandées par les forces de l'ordre
    - Recherche avancée de toute information à partir de noms, de numéros de téléphones, d'emails ou d'alias fournis par les forces de l'ordre.

4.2.8 Tests d'intrusions (Pentest) sur le réseau E-Gouv

CDA, dans le cadre de ses activités CERT, a effectué des tests d'intrusion sur 135 noms de domaines actifs dans gouv.tg en septembre 2022 et sur toutes les adresses IP publiques appartenant au réseau E-Gouv. Il s'agit d'une initiative visant à anticiper la découverte d'éventuelles failles et vulnérabilités et surtout à les corriger.

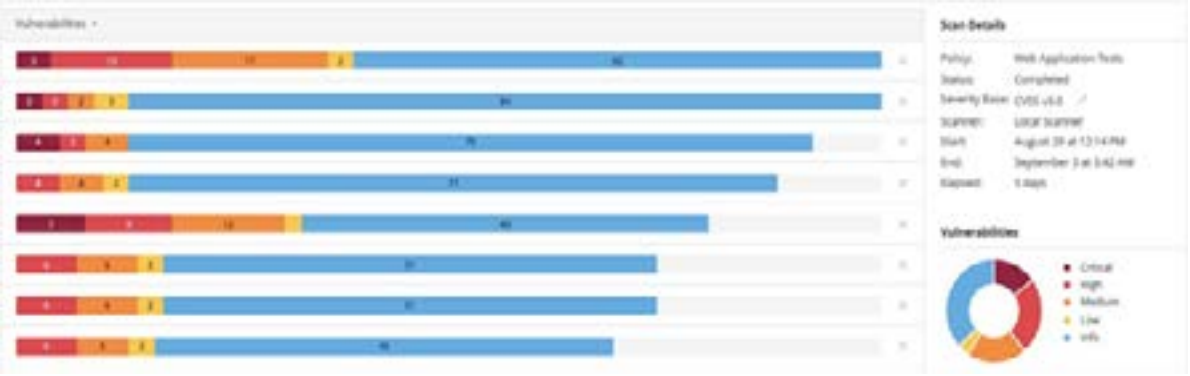

Figure 14 - Exemple de résultat des analyses de vulnérabilité

Le rapport complet des résultats de l'analyse de vulnérabilités et des tests d'intrusion a été partagé avec le responsable de réseau E-Gouv et l'ANCy.

4.2.9 Site web CERT.tg

4.2.9.1 Site Internet CERT.tg en bref

Le site CERT.tg, disponible en français et en anglais pour les particuliers et les entreprises s'est enrichi cette année de contenu avec la publication des vulnérabilités découvertes et de bulletins de sécurité.

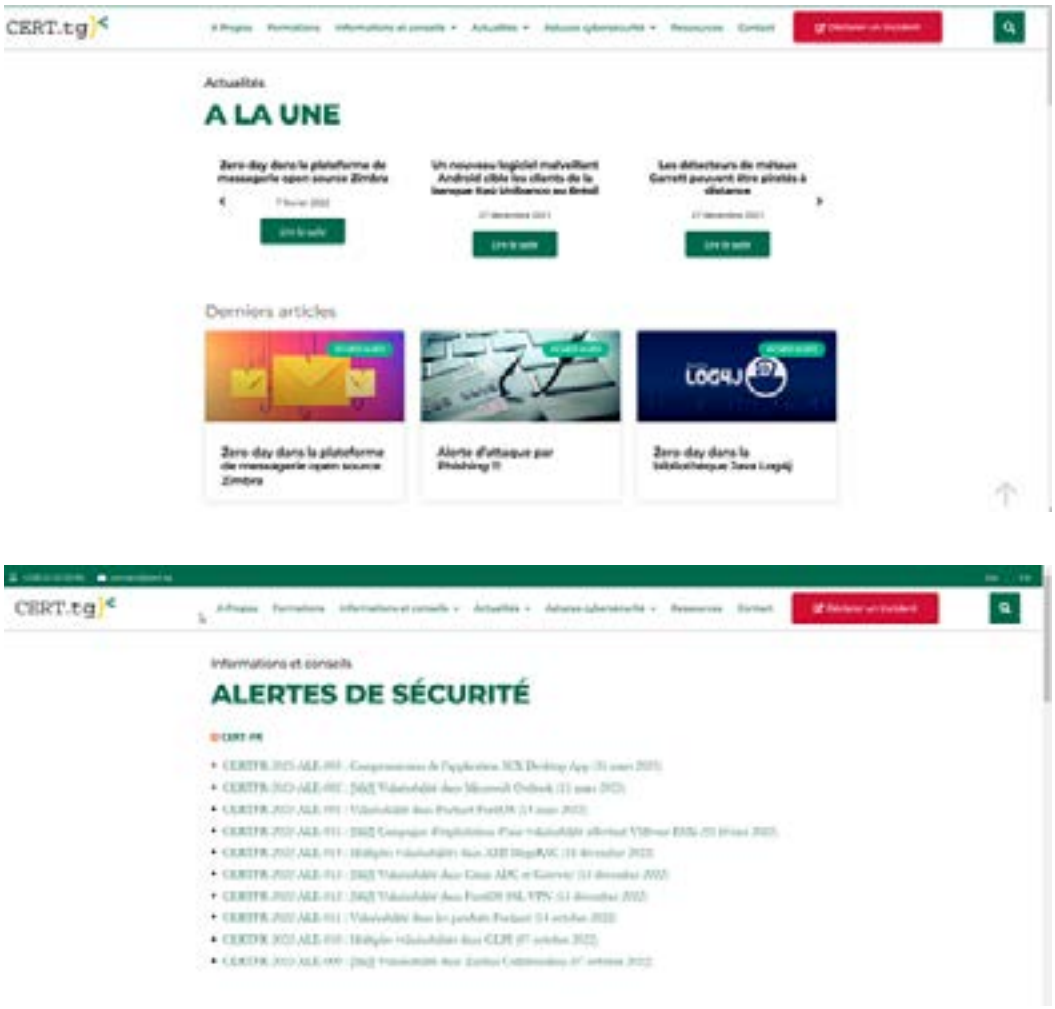

Figure 15 - Exemple de publication des bulletins de sécurité

4.2.9.2 Statistiques du site Internet CERT.tg en 2022

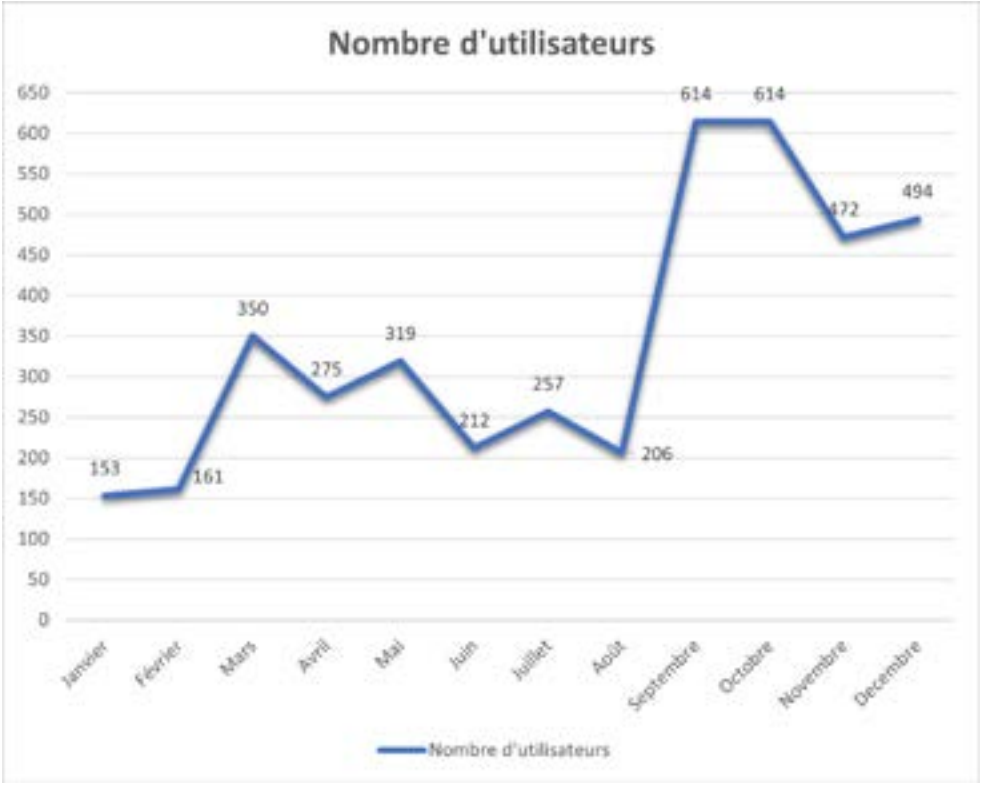

Figure 16 - Statistiques du site Internet CERT.tg

Conformément au graphique présentant l'évolution des incidents traités par le CERT.tg, les données collectées grâce au plugin Google Analytics configuré sur le site montrent une fluctuation du nombre de visites au cours de l'année avec une augmentation en Mars, mai septembre et octobre et une baisse en juin, juillet et août. La fréquence des visites est relativement stable sur le reste des mois.

La communication autour de la plateforme CERT.tg par CDA et l'ANCy lors de l'atelier de présentation des règles de cybersécurité applicables en République togolaise à l'hôtel Sarakawa a permis d'augmenter le nombre de visite sur le CERT.tg en septembre 2022 et octobre et d'atteindre le pic de l'année 2022.

4.2.10 Sensibilisations à la cybersécurité

4.2.10.1 Sensibilisation en présentiel

CDA surveille le réseau E-Gouv dans le cadre de ses activités SOC.

L'erreur humaine est la cause de plus de 90 % des incidents de sécurité (clic sur un lien de phishing, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées).

Dans le but de réduire les incidents de sécurité et protéger l'administration, il est indispensable que les fonctionnaires, principaux acteurs de l'administration togolaise, soient sensibilisés et outillés pour faire face aux enjeux croissants de la cybersécurité.

Le CERT.tg organise donc des campagnes de sensibilisation en fonction des incidents de sécurité observés sur le réseau E-Gouv en priorisant les entités générant le plus d'incidents. Ainsi, 92 sessions de sensibilisations pour un total de 5 059 participants ont été organisées dans les 25 ministères et Administrations publiques suivants :

#	Nom Ministère	Nombres de participants
1	Ministère de la Communication et des Médias	50
2	Ministère de la Santé	379
3	Ministère de l'Action Sociale, de la Promotion de la Femme, et de l'Alphabétisation	350
4	Ministère de l'Administration territoriale	52
5	Ministère de l'Agriculture, de l'Elevage et du Développement Rural	1070
6	Ministère de l'Economie et des Finances	1009
7	Ministère de l'Environnement et des ressources Forestières	218
8	Ministère des Enseignements Primaire, Secondaire, Technique et de l'Artisanat	583
9	Ministère du Commerce, de l'Industrie et de la Consommation Locale	150
10	Ministère des Sports et des Loisirs	100
11	Ministère du Désenclavement et des Pistes Rurales	52
12	Ministères des Affaires Etrangères, de l'Intégration Régionale et des Togolais de l'Extérieur	108
13	Ministère Chargée de l'Inclusion Financière et de l'Organisation du Secteur Informel et FNFI	46
14	Ministère des Transports Routiers, Aériens et Ferroviaires	30
15	Ministère des Mines et de l'Energie	60
16	Ministère des Droits de l'Homme, de la Formation à la Citoyenneté, des Relations avec les Institutions de la République, Porte-parole du Gouvernement	60
17	Ministère de la justice et de la Législation	50
18	ANID	16
19	Assemblée nationale du Togo	60
20	PAL	350
21	Primature	50
22	TVT	167
23	Mairie Ogou	30
24	Mairie Golfe 3	21
25	Mairie Golfe 4	18
	TOTAL	3059

Tableau 2: Sessions de sensibilisation organisées

4.2.10.2 Sensibilisation sur les médias

CDA, dans le cadre de ses activités CERT et soucieux d'atteindre le plus grand nombre de la population pour une sensibilisation accrue à la cybersécurité, a animé des débats sur différents sujets de cybersécurité dans les émissions de la Télévision nationale (TVT) et sur la radio Pyramide FM. Les principaux thèmes ci-dessous ont fait objet de sensibilisation dans 3 émissions radio et télévision en novembre et décembre 2022 :

- Débats sur le thème « Choix de bons mots de passe » dans l'émission Web Academy de GTT sur la radio Pyramide FM

- Débats sur le thème « Protection des comptes en ligne avec le 2FA » dans l'émission Nektar sur la TVT

- Débats sur le thème « 10 Règles de cybersécurité » dans l'émission Nektar sur la TVT.

https://www.youtube.com/watch?v=8owc5zwDsDc

4.2.10.3 Partenariats

Après les partenariats avec les entités africaines et internationales Africa-CERT, Trusted Introducer (TF-CSIRT), Fondation Shadowserver, Computer Incident Response Center Luxembourg (CIRCL) en 2021, CDA a intégré les réseaux internationaux comme FIRST et NationalCERT en 2022.

Forum of Incident Response and Security Teams (FIRST) est le Forum mondial des équipes de réponse aux incidents et de sécurité. Il est la première organisation et le leader mondial reconnu en matière de réponse aux incidents. Être membre de FIRST permet aux équipes de réponse aux incidents de répondre plus efficacement aux incidents de sécurité de manière réactive et proactive.

L'adhésion de CERT.tg à FIRST a permis à CDA de participer à la FIRSTCON2022 à Dublin en IRELAND qui est une conférence internationale pour promouvoir la coordination et la coopération entre les CSIRT/CERT à l'échelle mondiale.

Figure 17 - Conférence mondiale du FIRST -Edition 2022

4.2.11 Participation aux événements

4.2.11.1 OCWAR-C

Semaine des CSIRT

La Commission de la CEDEAO a convoqué la semaine des CSIRT pour réunir les CSIRT établis et émergents ainsi que les pays bénéficiaires du projet OCWAR-C sans CSIRT pour discuter et commencer l'élaboration d'une feuille de route vers la mise en place d'un MISP régional qui desservira toutes les entités impliquées dans les questions de cybersécurité et de cybercriminalité. Deux (2) analystes de CDA y ont participé en tant que participants au forum.

Cette semaine des CSIRT a eu lieu du 24 au 28 octobre 2022 en Guinée-Bissau.

Figure 18: Photos de la semaine des CSIRT- Edition 2022

4.2.11.2 AfricaCERT

Le CERT.tg a participé à la 2ème édition de l'Africa Cyber Drill (cyber exercice) organisé par AfricaCERT sous le thème «Stay on Alert» pour les CERTs/CSIRTs/CIRTs nationaux et sectoriels ainsi que leurs partenaires. Cet exercice est organisé afin de :

- Améliorer la communication et la collaboration entre les CERT/CSIRT régionales.
- Renforcer les capacités de réponse aux incidents des CERT/CSIRT régionales.
- Mesurer et améliorer la préparation à l'identification, la réponse, la prévention et la résolution des incidents informatiques.

L'événement s'est déroulé en ligne le 8 et le 9 septembre 2022 en ligne.

4.2.12 Développement de relations bilatérales

Le CERT.tg a établi une relation bilatérale avec les responsables ANSSI et CERT du Bénin, Burkina, Maurice, de la Guinée, du Sénégal et de la Côte d'Ivoire.

Plusieurs projets sont en cours de discussions entre ces CERTs. On peut par exemple citer, la définition d'un plan national de réponse à incident avec le CERT-MU, la collaboration pour établir les contacts sur les réseaux sociaux avec le bjCERT, les investigations sur des chantages en ligne provenant des numéros du Bénin et de la Côte d'Ivoire avec le CI-CERT.

4.2.13 Global Cybersecurity Index (GCI)

Depuis son lancement en 2015, le GCI est une référence de confiance, mesurant les engagements des pays à la cybersécurité et la sensibilisation à l'importance et aux différentes dimensions de la question. Comme la cybersécurité est une question vaste et complexe, transversale aux industries et aux secteurs, le développement ou l'engagement est évalué selon cinq piliers : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et coopération – puis agrégées en une note globale.

Les méthodes et techniques d'évaluation font souvent objet d'amélioration. Ainsi CDA depuis octobre 2022, fait partie du groupe de travail des experts de cette 5e édition du GCI (v5) qui a pour objectifs de :

1. Donner son avis sur les qualités clés à privilégier dans tout modèle de niveaux du GCI.
2. Proposer des modèles pour les niveaux, avec une méthodologie et un raisonnement.
3. Participer de manière productive aux discussions
4. Exprimer des préférences sur le modèle par paliers préféré.

Global Cybersecurity Index

4.2.14 Activités SOC de 2022

4.2.14.1 FOCUS E-GOUV et MENTD

4.2.14.1.1 Incidents par catégorie

Figure 19: Les incidents par catégorie

Au cours de l'année 2022, CDA a traité 17 669 incidents relatifs à l'environnement E-Gouv. 2 624 incidents, soit 15% sont des actions de scanning du réseau E-Gouv / MENTD. Les attaquants utilisent cette technique dans leur phase de reconnaissance. Il s'agit pour eux de pouvoir découvrir l'étendue des adresses IP du réseau, les noms de domaines, les ports ouverts sur le réseau ainsi que les services ouverts sur Internet.

CDA a également détecté 15 045 tentatives d'intrusions sur le réseau, soit 85%. Lorsque les scans sont terminés, les personnes malintentionnées essaient de pénétrer le réseau sur les ports disponibles sur Internet. Ils utilisent dans la majorité des cas, des dictionnaires de noms d'utilisateur et de mots de passe.

Dans le cas où CDA n'aurait pas détecté une intrusion dans le système d'information, nous surveillons également les actifs présents au sein du système. Cela permet de pouvoir détecter les tentatives d'accès suspects sur les actifs du MENTD ou E-Gouv.

4.2.14.1.2 Evolution des incidents détectés sur le réseau E-Gouv / MENTD

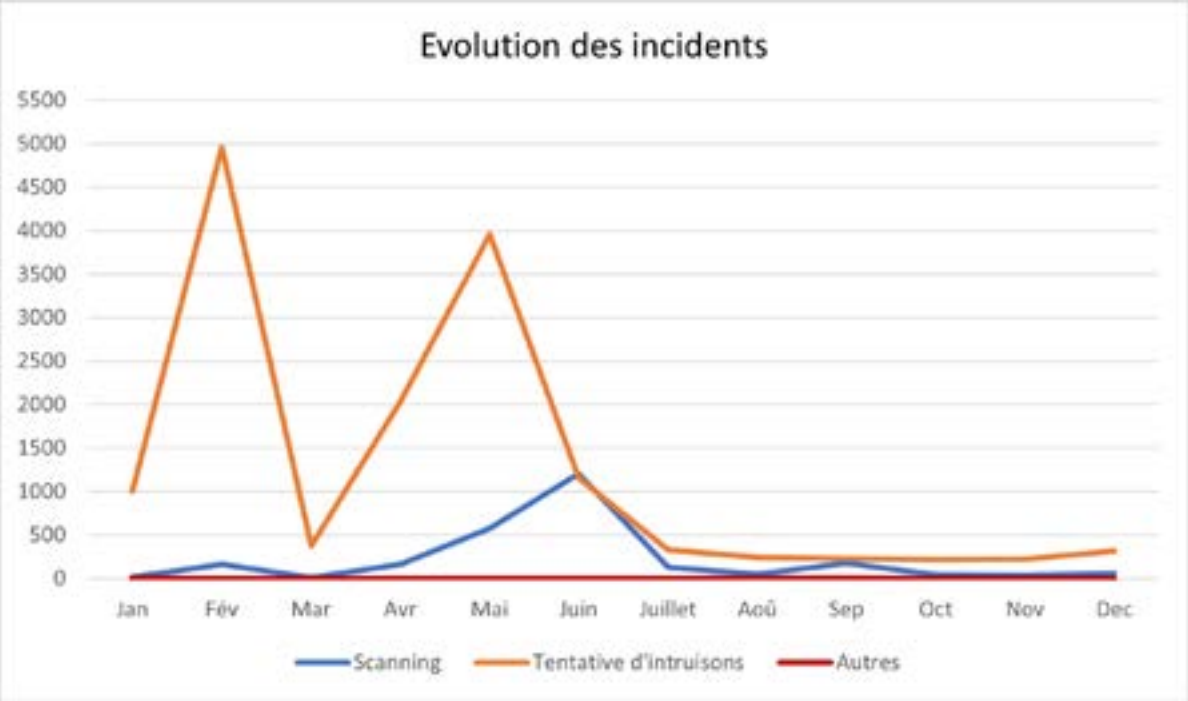

Figure 20: Evolution des incidents sur le réseau E-Gouv

4.2.14.1.3 Analyse de vulnérabilités sur le réseau E-Gouv/MENTD

A la fin de l'année 2022, le réseau E-Gouv/MENTD dispose de 552 vulnérabilités dont 32 sont susceptibles d'avoir un impact majeur sur le système d'information si elles sont exploitées et 87 sont susceptibles d'avoir un impact significatif sur le système d'information. Dans ces deux cas, elles peuvent être exploitées de manière à causer des dommages considérables, tels que l'incapacité à fournir les services, la perte ou le vol de données sensibles, l'accès non autorisé aux systèmes, ou l'exécution de code malveillant.

4.2.15 Références

Référence	URL
Site Web ANCy	https://ancy.gouv.tg
Site Web CDA	https://cda.tg
Site Web CERT.tg	https://cert.tg
ITU Global Cyber Index	https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
FIRST & FIRSTCON2022	https://www.first.org/conference/2022/
Africa CERT	https://www.africacert.org/about-us/
ANCy-CDA : Présentation des règles de cybersécurité au Togo	https://ancy.gouv.tg/les-regles-de-cybersecurite-ont-ete-presentees-ce-22-septembre-2022-aux-differents-acteurs-du-cyberespace-togolais-par-lancy-et-cyber-defense-africa-cda/
CEDEAO/OCWAR-C : Semaine du CSIRT	https://www.ocwarc.eu/ecowas-csirt-week-guinea-bissau/
ANCy-CDA : Validation de la stratégie nationale de la cybersécurité	https://ancy.gouv.tg/du-mercredi-23-au-vendredi-25-novembre-2022-se-tait-tenu-latelier-de-validation-de-la-strategie-nationale-de-la-cybersecurite-avec-la-participation-des-institutions-nationales/

5. DIFFICULTÉS RENCONTRÉES

Dans la mise en œuvre de ses activités, l'ANCy a été confrontée à certaines difficultés.

Au nombre de ces difficultés, on peut citer :

1. Les problèmes de dotation de l'ANCy d'un siège propre ;
2. Ressources humaines limitées ;
3. Réticence de certains opérateurs de services essentiels à répondre promptement aux obligations issues de leur statut ;
4. La non-opérationnalisation des services de la qualification des prestataires de services dd confiance en cybersécurité ;
5. La non-complétude des référentiels de qualification des prestataires de services de confiance en cybersécurité.

Cette situation a pour conséquences notamment le :

- Non-respect des délais légaux de mise en conformité avec leur statut d'OSE ;
- Non-démarrage des audits de conformité annuels visant à évaluer leur niveau de robustesse de leurs systèmes d'information ;
- Retard dans la mise en route des services de la qualification des prestataires de services de confiance, des produits de sécurité et de l'agrément des centres d'évaluation ;
- La difficulté à enclencher les sanctions contre les OSE qui ne respectent pas les obligations issues de leur évolution statutaire.

6. LES PERSPECTIVES

Ces activités réalisées par l'ANCy en 2022, ont permis d'ouvrir bon nombre de chantiers pour l'année 2023 dont la réalisation devra être accélérée.

En effet, tirant les leçons des activités réalisées et eu égard aux difficultés et contraintes rencontrées, l'ANCy s'engage à mettre un accent particulier sur la poursuite des chantiers entrepris afin de combler les attentes légitimes placées en elle. Dans cette perspective, les grandes orientations de 2023, sont les suivantes :

- la poursuite du processus de recrutement du personnel ;
- la réalisation des audits de conformité des OSE ;
- Le contrôle et l'encadrement des OSE dans le processus de leur mise en conformité avec leurs obligations statutaires.

Par rapport à la réglementation et à la régulation :

- Désignation de 38 nouveaux OSE,
- Poursuite des ateliers de sensibilisation visant à les familiariser avec les obligations de mise en conformité avec les règles de cybersécurité ;
- Contrôle effectif du respect de leurs obligations réglementaires.

En ce qui concerne la formation et les appuis techniques :

- renforcement du dispositif de formation par l'élaboration d'un plan de formation et des appuis techniques;
- mise en place d'un système de réponses aux demandes d'appuis techniques exprimées par les OSE ;
- mise en place d'un mécanisme de suivi régulier de la mise en œuvre des obligations statutaires des OSE;

Par rapport aux audits :

- démarrage effectif des audits annuels de conformité des OSE ;
- mise en place d'un mécanisme de suivi de la mise en œuvre des recommandations des audits de conformité ;

Par rapport aux ressources humaines et matérielles :

- poursuite du recrutement du personnel pour les directions techniques ;
- renforcement des capacités du personnel par les formations ;

Par rapport à la communication :

- Poursuite de la dynamisation du cadre de concertation entre l'ANCy et les OSE ;
- renforcement de la sensibilisation des OSE, des Autorités administratives, des autorités judiciaires, des autorités militaires, des médias sur les missions et les attributions de l'ANCy et sur la réglementation ;
- mise au point d'un journal sur les activités de l'ANCy ;
- organisation d'activités d'information à l'endroit du grand public sur les enjeux de la cybersécurité ainsi que les missions et les attributions de l'ANCy ;
- la vulgarisation des textes en vigueur en matière de cybersécurité à travers ;
- L'organisation d'une série de sessions de sensibilisation et de formation visant le renforcement des capacités humaines, institutionnelles et opérationnelles des acteurs publics et privés de la chaîne de la sécurité des systèmes d'information ;
- L'organisation d'une campagne nationale de sensibilisation de formation au profit des acteurs du secteur privé ainsi que de ceux des administrations décentralisées et déconcentrées.

Par rapport au partenariat :

- développement du partenariat avec les donateurs.
- rédiger un recueil des textes en cybersécurité.

CONCLUSION

La cybersécurité est un enjeu crucial pour les entreprises, les gouvernements et les particuliers. Il est indéniable que les attaques informatiques sont de plus en plus sophistiquées et que les mesures de sécurité doivent être constamment renforcées.

Voilà pourquoi, dès sa phrase d'opérationnalisation, l'équipe de l'Agence s'est courageusement investie à faire face à toutes les difficultés du débutant, convaincue que la mission d'intérêt général dont elle est investie, contribuera à garantir la continuité des activités sociétales et économiques de notre pays.

Il s'agit d'une problématique qui nous concerne tous et qui nécessite que nous fassions, collectivement front, car la menace en face se professionnalise et devient de plus en plus en plus sophistiquée.

Au demeurant, la détermination des plus hautes autorités nationales en vue d'assurer la sécurité et la stabilité de notre cyberespace reste constante. Cela représente d'ailleurs, la meilleure garantie pour chaque citoyen togolais, qui au-delà, de la réalité des menaces protéiformes qui nous environnent, que tout est mis en œuvre pour assurer la continuité des activités sociétales, sur la terre de nos aïeux, notre héritage commun.

ANCy
Agence Nationale de la Cybersécurité

63 Bd du 13 Janvier,
Nyékonakpoe, Lomé-TOGO
07 BP 7878
secretariat.ancy@ancy.gouv.tg
+228 22 21 25 28
+228 97 52 58 58
+228 70 60 60 83

ancy.gouv.tg