Accra, 13 novembre 2023.

COMMUNIQUÉ DE PRESSE : TROISIÈME CYBERDRILL AFRIQUE : COMBLER LES LACUNES.

Le Forum des équipes africaines d'intervention d'urgence (également connu sous le nom d' AfricaCERT) a achevé le troisième cyberexercice annuel (également connu sous le nom d'Africa Cyber Drill) sous le thème : « Combler les lacunes » à Maputo, au Mozambique, du 7 au 10 Novembre 2023. Le troisième cyberexercice fait suite à la deuxième édition réussie : « Restez en alerte » et à la première édition : « Tester le terrain ».

L'événement hybride a été organisée en collaboration avec l'Institut national des TIC (INTIC), qui est l'organise hôte de l'équipe nationale de réponse aux incidents de sécurité informatique du Mozambique (nCSIRT.Mz) , la Communauté de développement de l'Afrique australe (SADC), l'Institut de génie logiciel (SEI) avec le soutien du Bureau of Cyberspace and Digital Policy (CDP) – Département d'État des États-Unis. L'objectif principal du cyber-exercice était d'améliorer la préparation des équipes africaines contre les cybermenaces. L'événement conjoint avec le Secrétariat de la SADC était le premier du genre.

Les Cybedrills sont devenus à la fois pour la Communauté SADC et pour l'AfricaCERT une plate-forme essentielle de renforcement des capacités pour améliorer les mécanismes de communication existants, pour connecter et renforcer les approches de coopération innovantes entre les équipes de réponse aux incidents de sécurité informatique et, surtout, pour améliorer la préparation, et les capacités de réponse aux incidents en matière de cybersécurité de la région (augmenter leur cybersécurité maturité) et de protection à travers des exercices pratiques et pratiques.

L'exercice était structuré comme suit :

Protocole:

Le 7 novembre , suite au discours de bienvenue de M. Jean-Robert Hountomey, Co-Fondateur d' AfricaCERT , les représentants du pays hôte et des institutions organisatrices ont prononcé des discours d'ouverture :

- Dr Angel L. Hueca, Représentant du CERT/CC, Software Engineering Institute, Carnegie Mellon University
- Dr. _ George Ah- Thew – Chargé de programme principal (SPO) TIC, Communauté de développement de l'Afrique australe (SADC),

- Mme Kathrine Fitrell Représentante du Département d'État américain, Bureau du cyberespace et de la politique numérique,
- M. Hecdiantro Wilson da Costa Mena, Directeur national des politiques de cybersécurité et des services numériques du ministère des télécommunications, des technologies de l'information et des communications sociales (MINTTICS) de l'Angola, le représentant du président de la SADC et Président de ce Cyber Drill continental ;
- Professeur Lourino Chemane, Président de l'Institut national des TIC (INTIC), qui héberge l'équipe nationale de réponse aux incidents de sécurité informatique du Mozambique (nCSIRT.Mz).

Ing. Nilsa Miquidade, Secrétaire Permanent du ministère de la Science, de la Technologie et de l'Enseignement supérieur du Mozambique, notre hôte et invité d'honneur; a prononcé le discours ministériel au nom de l'honorable Ministre Daniel Nivagara .

Formation

L'exercice comprenait deux jours de sessions de renforcement des capacités sur site en parallèle sur la criminalistique numérique, la création et la gestion de CSIRT et le cyber-risque et la résilience, les 7 et 8 novembre 2023. Les (2) autres jours se sont concentrés sur les exercices d'exercice qui ont été livré en mode hybride.

Cyberexercice.

Au cours de l'exercice, plusieurs présentations ont été réalisées comme suit :

- Développement d'exercices de cyber-simulation par le Dr Kaleem Ousmani . CERT MU
- Rendre la réponse aux incidents efficace en Afrique et favoriser les relations avec les communautés mondiales par AfricaCERT
- Présentation de l'adhésion à FIRST par Mme Tracy Bills, Présidente du Conseil d'Administration de FIRST,
- Études de cas et partage d'expériences de représentants du Bénin, du Bostwana , du Malawi, du Mozambique, d'Eswatini et de la Zambie.

L'exercice visait à tester la capacité de réponse des équipes participantes face aux scénarios suivants : compromission de la messagerie électronique professionnelle, vulnérabilités de la chaîne

d'approvisionnement et dégradation du site Web. Les scénarios ont été conçus pour refléter l'environnement en temps réel par MaCERT , CERT MU et le « National KE-CIRT/CC », ainsi que par les organisateurs en plus de bjCSIRT et AfricaCERT .

Les pays africains qui ont participé à l'exercice étaient l'Angola, le Bénin, le Burkina Faso, le Botswana, les Comores, la Côte d'Ivoire, la RDC, la Gambie, le Ghana, le Royaume d' Eswatini , l'Éthiopie, le Royaume du Lesotho, le Niger, le Nigeria, le Malawi, Madagascar et Maurice. , Maroc , Mozambique, Namibie, Rwanda, Seychelles, Sénégal, Afrique du Sud, Tanzanie, Tunisie, Togo, Zambie et Zimbabwe

Des collègues de l'OIC-CERT et de l'APCERT (Inde, Indonésie, Malaisie et Pakistan), ainsi que de Trinidad et des Bahamas, ont rejoint leurs collègues d'Afrique.

Des équipes de réponse aux incidents de sécurité informatique de 35 pays, dont 29 pays africains, ont participé à l'exercice, y compris les équipes organisatrices.
L'équipe organisatrice remercie les sponsors dont Cyber Range et Iservices Systems.

Rendez-vous à l'automne 2024 pour le Cyberdrill annuel 2024.