AfricaCERT
United Teams promoting Cybersecurity in Africa

COMMUNIQUÉ DE PRESSE

01 July 2021
POUR DIFFUSION IMMEDIATE

1st AfricaCERT CYBER DRILL
"Testing The Waters"

Le Forum des Centres de veille, d'alerte et de réponse aux attaques informatiques en Afrique (AfricaCERT) a terminé son premier exercice annuel pour tester la capacité des équipes dans les économies africaines du 30 juin au 1er juillet 2021.

Une équipe de coordination composée d'AfricaCERT, bjCSIRT (Bénin), CERT-MU (Maurice), EGCERT (Egypte), KE-CIRT (Kenya), KEYSTONE (Tunisie), tunCERT (Tunisie) a organisé l'exercice. Le CERT-MU a présidé cette édition 2021 ; les scénarios ont été fournis par CERT-MU et EGCERT et ont été supportés par la plateforme SILENSEC CYBER RANGE.

Le 30 juin 2021, lors de la cérémonie d'ouverture, plusieurs orateurs principaux ont présenté l'importance d'être préparé et divers programmes soutenant le renforcement des capacités des CSIRT en Afrique. M. Chris Gibson, Directeur Exécutif, Forum of Incident Response and Security Teams, a souligné l'importance de « l'exercice, l'exercice et l'exercice ». M. Moctar Yedaly a parlé du Forum mondial sur la cyber-expertise et des initiatives de renforcement des capacités en Afrique. Mme Joanne Esmyot, Directrice Exécutive du National Computer Board Mauritius, représentant l'honorable Deepak Balgobin, Ministre des technologies de l'information, de l'Innovation en communication, République de Maurice, a prononcé le discours d'ouverture.

L'exercice visait à tester la capacité de réponse des équipes participantes face aux scénarios suivants : hameçonnage, défiguration de site internet, REM, reponse en cas de ransomwares. Ces exercices ont été conçus pour mettre les participants dans des conditions réelles et tester leurs capacités de réponse, de communication et leurs capacités techniques. Le scénario de défiguration de site internet a simulé la réponse d'une banque qui a subi un vol de données après que des acteurs malveillants ont illégalement accédé à ses informations via l'une des vulnérabilités de son système d'information. L'attaque de phishing a simulé divers scénarios pour tester la capacité de réponse des participants en cas d'attaques de phishing à la fois au niveau du pays et au delà de leur frontière. L'exercice d'analyse des logiciels malveillants a fourni un scénario d'analyse des logiciels malveillants avec divers outils. Le scénario d'attaque de ransomware a fourni un cas de réponse à un incident de ransomware.

Les pays africains participant à l'exercice sont le Bénin, le Botswana, la Côte d'Ivoire, Djibouti, l'Égypte, la Gambie, le Kenya, le Lesotho, le Mozambique, le Nigéria, les Seychelles, la Tanzanie, la Tunisie et la Zambie, en plus de l'équipe du secrétariat de la SADC. Des collègues de l'OIC-CERT et de l'APCERT (Brunéi, Inde, Indonésie, Malaisie, Japon, Pakistan, Philippines, Sri-Lanka, Ouzbékistan, Turquie et Syrie) ont rejoint les équipes africaines. 32 équipes de réponse aux incidents de sécurité informatique de 25 pays ont participé à l'exercice, y compris les équipes organisatrices. Des observateurs de Cyber4Dev et du ministère de l'Intérieur britannique ont participé à l'exercice et ont fourni des conseils.

~ Fin ~

Publié par le **Secretatiat d'AfricaCERT**.
Pour plus d'informations sur ce document, n'hésitez pas à contacter : secretariat (at) africacert.org