Lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique

Une initiative conjointe de l'Internet Society et de la Commission de l'Union africaine

30 May 2017

Internet Society

Union Africaine

À propos de l'Internet Society

Fondée par des pionniers de l'Internet, l'Internet Society (ISOC) est un organisme à but non lucratif dévoué au développement ouvert, à l'évolution et à l'utilisation de l'Internet. Grâce à une communauté mondiale de chapitres et de membres, l'Internet Society collabore avec un large éventail de groupes pour promouvoir les technologies qui sécurisent l'Internet et protègent les politiques qui permettent un accès universel. L'Internet Society est également le siège organisationnel du Groupe de travail en ingénierie Internet (IETF).

À propos de la Commission de l'Union africaine

L'Union africaine (UA) a été officiellement lancée en juillet 2002 à Durban, en Afrique du Sud, suite à une décision prise en septembre 1999 par son prédécesseur, l'Organisation de l'unité africaine (OUA), formée en 1963, afin de créer une nouvelle organisation continentale s'appuyant sur le travail déjà accompli.

Un total de 54 pays sont membres de cette nouvelle organisation, dont le siège est resté à Addis Abeba, en Éthiopie.

La Commission de l'Union africaine (CUA) est le secrétariat de l'UA, chargée des fonctions exécutives, et composée de dix hauts fonctionnaires, dont le président, le vice-président et huit commissaires.

Cette structure représente l'UA et protège ses intérêts sous les auspices de la Conférence des chefs d'État et de gouvernement ainsi que du Conseil exécutif. La CUA est composée des portefeuilles suivants : Paix et sécurité, Affaires politiques, Commerce et industrie, Infrastructure et énergie, Affaires sociales, Économie rurale et agriculture, Ressources humaines, sciences et technologie et Affaires économiques.

La vision directrice de l'Agenda 2063 est la vision de l'UA : « Une Afrique intégrée, prospère et pacifique, dirigée par ses propres citoyens et représentant une force dynamique dans l'arène internationale ». La mission de la Commission de l'UA est « de devenir une institution efficace et porteuse de valeur ajoutée, qui mène le processus d'intégration et de développement de l'Afrique en étroite collaboration avec les États membres de l'Union africaine, les communautés économiques régionales et les citoyens africains ».

Remerciements

Nous tenons à remercier Ahmed Hussein (HiLCoE Computer Systems Engineering) et Mulugeta Libsie (Université d'Addis-Abeba), qui ont travaillé sur le premier projet de Lignes directrices et ont examiné les projets successifs basés sur l'apport des experts contributeurs, y compris : Souhila Amazouz (AUC), Dawit Bekele (ISOC), Abdoullah Cisse (Carapace), Niel Harper (ISOC), Jean-Robert Hountomey (AfricaCERT), Olaf Kolkman (ISOC), Ben Maddison (Workonline), Choolwe Nalubamba (ZICTA), Steve Olshansky (ISOC), Barrack Otieno (AFTLD), Ryan Polk (ISOC), Nii Quaynor (AfNOG), Andrei Robachevsky (ISOC), Bob Rotsted (NSRC), Christine Runnegar (ISOC), Joe St Sauver (Farsight Security, Inc.), et Moctar Yedaly (AUC).

Table des matières

Résumé analytique

En 2014, les membres de l'Union africaine (UA) ont adopté la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (« la Convention »).[1]

Pour faciliter la mise en œuvre de la Convention, la Commission de l'Union africaine (CUA) a demandé à l'Internet Society (ISOC) d'élaborer conjointement des Lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique (« les Lignes directrices »). Les Lignes directrices ont été élaborées grâce aux contributions d'experts régionaux et mondiaux de la sécurité de l'infrastructure Internet, des représentants gouvernementaux et des CERT et des opérateurs de réseau et de ccTLD DNS.

Les Lignes directrices soulignent l'importance du modèle multipartite et d'une approche collective de la sécurité dans la protection de l'infrastructure Internet. Les Lignes directrices proposent quatre principes essentiels de la sécurité de l'infrastructure Internet : sensibilisation, responsabilité, coopération et respect des droits fondamentaux et des propriétés de l'Internet.

Les Lignes directrices préconisent aux diverses parties prenantes de prendre des mesures extrêmement critiques en matière de sécurité de l'infrastructure Internet. Ces mesures importantes sont adaptées aux caractéristiques uniques de l'environnement de la cybersécurité africaine : un déficit en ressources humaines qualifiées ; des ressources limitées (y compris financières) que les gouvernements et organisations peuvent consacrer pour la cybersécurité ; des connaissances limitées en matière de cybersécurité parmi les parties prenantes ; et un manque général de connaissance des risques liés à l'utilisation des technologies de l'information et de la communication (TIC).

Étant donné l'étendue de la sécurité de l'infrastructure Internet, un seul document ne suffit pas et des travaux supplémentaires sont nécessaires pour compléter les Lignes directrices avec des recommandations spécifiques traitant des problèmes particuliers. Cette série de recommandations est une première étape, pourtant significative, pour amener un changement visible et positif dans le paysage africain de la sécurité de l'infrastructure Internet.

Au niveau régional (à l'échelle de l'Union africaine)

- Mettre en place un Comité africain de coordination et de collaboration en matière de cybersécurité (ACS3C)
    - Le Comité serait un groupe multipartite qui conseillerait les décideurs de la CUA sur les stratégies régionales et le renforcement des capacités et faciliterait le partage de l'information dans toute la région.

- S'engager dans le renforcement des capacités et le partage des connaissances au niveau panafricain
    - La CUA devrait développer des programmes de renforcement des capacités, comme le conseille l'ACS3C, dans tous les domaines de la sécurité de l'infrastructure Internet.

1 Pour consulter la Convention, cliquez sur le lien http://www.au.int/en/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_ security_and_personal_data_protection_e.pdf

Au niveau national

- Identifier et protéger l'infrastructure critique de l'Internet
  - Les gouvernements nationaux devraient adopter une approche basée sur les services pour identifier et protéger l'infrastructure critique de l'Internet.

- Faciliter l'échange d'informations par l'intermédiaire d'une structure nationale multipartite
  - Les gouvernements nationaux devraient élaborer des structures multipartites pour apporter conseil sur la stratégie et la politique de cybersécurité et pour faciliter le partage d'informations.

- Établir et renforcer au niveau national, les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT)
  - Les gouvernements nationaux qui collaborent avec d'autres parties prenantes devraient établir ou appuyer les CSIRT nationales existantes afin de coordonner les interventions menées avant et durant les incidents de sécurité.

- Promouvoir la résilience de l'infrastructure Internet par le biais des points d'échange Internet (IXP)
  - Les gouvernements nationaux devraient promouvoir l'utilisation des IXP et une plus grande coopération et connectivité entre les différents réseaux africains afin d'accroître la résilience de l'infrastructure Internet.

- Utiliser les institutions publiques pour donner l'exemple en matière de cybersécurité.
  - Les gouvernements devraient adopter et suivre les meilleures pratiques de cybersécurité dans leurs propres infrastructures et institutions, en encourageant leur utilisation auprès d'autres parties prenantes et d'autres secteurs.

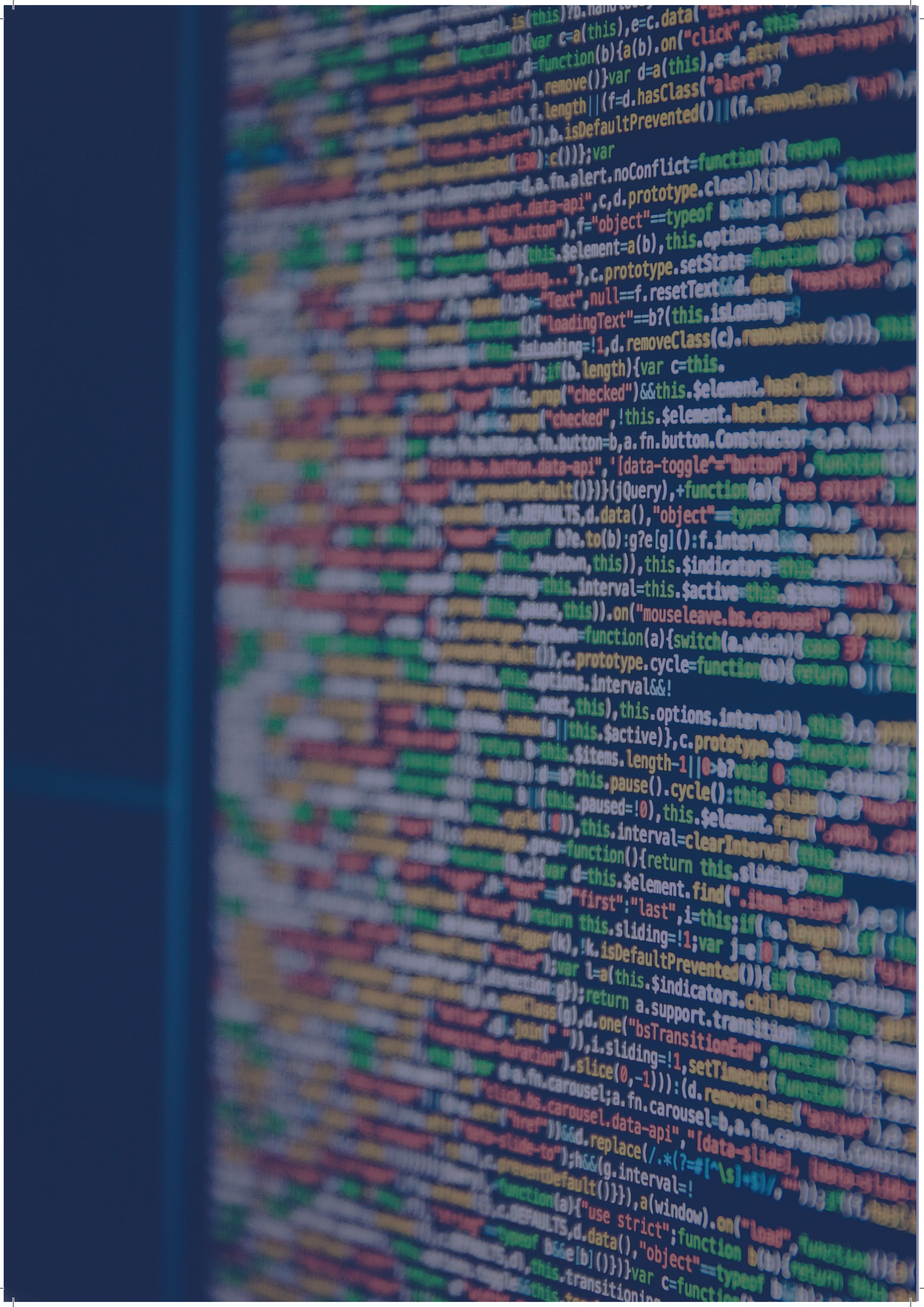
Au niveau des FAI et des opérateurs

- Établir la sécurité de base
  - Les opérateurs de réseau et les fournisseurs d'accès devraient mettre en place des mesures de sécurité essentielles pour le routage et les systèmes d'adressage par domaines, la sécurité du réseau et d'autres pratiques de sécurité essentielles pour entraîner un changement visible et positif dans le paysage africain de la sécurité de l'infrastructure Internet.

- Établir et maintenir une coopération et une collaboration
  - Les opérateurs de réseaux et les fournisseurs d'accès devraient établir et maintenir la coopération et la collaboration en tant que composante essentielle des solutions de sécurité.

Au niveau organisationnel

- Les organisations devraient mettre en œuvre les meilleures pratiques en vigueur et s'efforcer de développer une culture de cybersécurité à tous les niveaux de l'organisation.



1. Introduction

L'importance de l'Internet et des TIC comme outils efficaces pour réaliser le développement socio-économique dans les pays en voie de développement est largement reconnue par les gouvernements, les institutions financières et les partenaires au développement. L'Internet et les TIC constituent une infrastructure vitale pour le développement. Ce sont de nouvelles sources de croissance et des moteurs de l'innovation et du bien-être social. À mesure que l'économie de l'Internet se développe, les parties prenantes et le reste de l'économie dépendent de plus en plus des infrastructures numériques pour remplir leurs fonctions essentielles.

Chacun sait bien le rôle de l'Internet dans le soutien de l'économie, la diffusion de l'information et de l'éducation et la créativité. L'économie de l'Internet est un environnement dynamique où les technologies, les applications, les utilisations et les marchés évoluent constamment, souvent d'une manière imprévisible. Si l'Internet profite à la croissance économique et à l'innovation, les attaques contre l'infrastructure Internet représentent un risque majeur pour la croissance économique et l'innovation.

Le rapport conjoint CUA-Symantec Cyber Crime & Cyber Security Trends in Africa, publié en novembre 2016, révèle que 24 millions d'incidents malveillants visant l'Afrique ont été observés en 2016.[2] Un rapport de McAfee de 2017 révèle qu'au quatrième trimestre de 2016, près de 12 % de leurs clients mobiles africains ont signalé des infections malveillantes.[3] Les vulnérabilités ou les faiblesses exploitables constituent une menace pour les appareils, les réseaux et les systèmes, ainsi que pour ceux qui en dépendent. Ces vulnérabilités sont exploitées par des pirates pour attaquer une gamme de plus en plus diversifiée d'industries, d'organisations et de cibles.[4]

Compte tenu la menace que constituent les attaques sur l'infrastructure Internet pour le développement socio-économique, il incombe à toutes les parties prenantes, y compris les gouvernements et les fournisseurs d'accès Internet de s'entendre sur des solutions qui permettent de garantir la sûreté, la sécurité et la résilience de l'Internet dans chaque pays. Un aspect clé dans le choix des solutions de sécurité est de préserver la nature ouverte de l'Internet et de renforcer la confiance.

Étant donné que l'Internet est d'une importance cruciale pour l'économie et pour toutes les parties prenantes, les conséquences des défaillances en matière de sécurité peuvent avoir un effet direct sur la société dans son ensemble. Par conséquent, toutes les parties prenantes doivent s'engager à sécuriser les cyber-opérations.

Ces menaces peuvent être de différentes natures telles que le vol (d'identité, de données personnelles et de secrets de toutes sortes), les infractions aux droits de propriété intellectuelle, les attaques de déni de service, la dégradation et d'autres sources de perturbation. Cependant, les attaques à grande échelle de déni de service distribué (DDoS), l'utilisation abusive ou la violation des données à caractère personnelle et la perturbation des infrastructures critiques seraient les principales sources de préoccupation pour l'Afrique.

L'Afrique est de plus en plus connectée à l'Internet. Les entreprises, les infrastructures, les gouvernements, les citoyens et les industries clés sont de plus en plus liés à l'Internet. À mesure que le continent s'appuie de plus en plus sur l'Internet, la protection de ses éléments critiques

2 Voir https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa/documents/publications/2017/03/10/report-cyber- trends-in-africa

3 Voir https://www.mcafee.com/ca/security-awareness/articles/mcafee-labs-threats-report-mar-2017.aspx

4 Pour plus d'informations concernant les menaces, les agents de menace, les vulnérabilités et les attaques, voir Annexe I : La terminologie lié à l'Internet et à la sécurité

devient vitale. Les acteurs africains de l'écosystème Internet doivent travailler ensemble pour protéger l'infrastructure Internet interconnectée tout en préservant les propriétés fondamentales de l'Internet[5] et en défendant les droits fondamentaux.

La sécurité de l'infrastructure Internet est d'une importance et d'une ampleur primordiales. Les Lignes directrices traitent des domaines pertinents et spécifiques relatifs aux besoins actuels essentiels en Afrique.

Bien que les Lignes directrices mettent l'accent sur les problèmes de sécurité de l'infrastructure Internet, il est difficile de les distinguer des problèmes plus généraux d'Internet ou de sécurité de réseau. Par conséquent, certains aspects de la sécurité générale du réseau sont également couverts dans ce document ou abordés dans l'annexe.[6]

Les Lignes directrices visent à fournir des recommandations et à promouvoir des principes et des solutions pour s'assurer que la sécurité de l'infrastructure Internet en Afrique répond aux exigences des utilisateurs en général et que toutes les parties prenantes ont des lignes directrices claires pour atteindre les résultats escomptés. En assurant une sécurité et une résilience accrues, les recommandations contribueront à accroître la confiance et l'utilisation de l'Internet par la communauté africaine. Bien que les recommandations ne couvrent pas tous les problèmes liés à la sécurité de l'infrastructure Internet, elles constituent une première étape importante vers une infrastructure Internet africaine résiliente et sécurisée.

1.1 Méthodologie

La méthodologie utilisée dans l'élaboration des Lignes directrices comprend une recherche documentaire et un processus de collecte des points de vue des experts africains et internationaux.

La recherche documentaire a utilisé plusieurs sources différentes, y compris les recommandations et les meilleures pratiques publiées par les principales institutions, organisations et entreprises liées à Internet. Il s'agit notamment de la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), le Groupe de travail en ingénierie Internet (IETF), l'Union internationale des télécommunications (UIT), l'ISOC, l'Institut national des normes et de la technologie des États-Unis (NIST), l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et l'Organisation de coopération et de développement économiques (OCDE).

La table ronde d'experts sur la sécurité de l'infrastructure Internet organisée dans le cadre du sommet Africa Internet (AIS) tenu à Gaborone, au Botswana, du 29 mai au 10 juin 2016 a apporté de précieuses contributions.

Des professionnels sélectionnés dans le domaine de l'infrastructure Internet ont également été interviewés. Enfin, un projet de Lignes directrices a été présenté lors d'une réunion d'experts à Nairobi les 28 et 29 novembre 2016. Au cours de la réunion, les avis des participants ont été sollicités en vue d'améliorer la version finale de ce document.

5 Voir https://www.internetsociety.org/internet-invariants-what-really-matters et http://www.internetsociety.org/policybriefs/internetinvariants

6 Voir l'annexe II : Principes fondamentaux de sécurité

1.2 Le champ d'application des Lignes directrices

Le champ d'application des Lignes directrices est le suivant :

- Bien que l'accent soit mis sur la sécurité de l'infrastructure Internet, il est difficile de distinguer clairement la sécurité de l'infrastructure Internet, et la sécurité du réseau et les pratiques traditionnelles de sûreté de l'information.[7] Ce sont des domaines connexes, dont les problèmes et les solutions se chevauchent très souvent.

- Les solutions en matière de sécurité de l'infrastructure Internet englobent de nombreux domaines et de nombreuses parties prenantes, y compris la formulation de politiques, la promulgation et l'application de lois pertinentes et appropriées en matière de l'Internet, la collecte et l'analyse d'informations sur les menaces, le partage d'informations et la collaboration, et l'utilisation de solutions techniques, économiques et autres.

- Les méthodes et les pratiques en matière de sécurité physique sont maintenant assez matures. Par conséquent, elles ne font pas l'objet de ce document. Cependant, les Lignes directrices reconnaissent également l'importance de la protection des actifs physiques ainsi que des actifs numériques. Les recommandations mettent en évidence un certain nombre d'aspects de la sécurité physique pour les actifs tels que les câbles et autres infrastructures physiques, mais ces aspects ne sont pas abordés de manière exhaustive dans ce document.

- Comme indiqué précédemment, les Lignes directrices ne comprennent pas tous les aspects de la sécurité de l'infrastructure Internet. Cependant, elles constituent une première étape importante. D'autres travaux seront nécessaires pour établir des lignes directrices supplémentaires traitant des problèmes particuliers. Celles-ci doivent être considérées comme document de référence.

- En outre, les travaux de recherche ont révélé un manque de capacité en matière de sécurité de l'infrastructure Internet dans la plupart des pays d'Afrique. En conséquence, bon nombre des recommandations portent sur le renforcement des capacités aux niveaux régional, national, institutionnel ou organisationnel. Elles cherchent à développer les ressources humaines par l'éducation et la formation, la coopération à tous les niveaux, le renforcement des capacités et le partage de l'information, etc.

7 La sûreté de l'information est une action pour protéger et défendre l'information et les systèmes d'information en garantissant leur intégrité, leur disponibilité, leur authentification, leur non-répudiation et la confidentialité

2. Analyse de la sécurité de l'infrastructure Internet

2.1 Résultat des débats d'experts et des entretiens

Le 10 juin 2016, dans le cadre de l'AIS à Gaborone, l'ISOC et la CUA ont tenu un débat d'experts sur la « Sécurité de l'infrastructure Internet en Afrique ». Des entretiens ont également été réalisés avec des experts sélectionnés. Les débats d'experts et les entretiens ont porté sur les cinq principaux sujets suivants :

- **Les actifs constitutifs de l'infrastructure Internet et ses actifs critiques**
  La connectivité Internet est identifiée comme la fonction la plus importante de l'infrastructure Internet. Les actifs physiques qui rendent possible la connectivité Internet comprennent les périphériques réseau tels que les routeurs, les commutateurs, les pare-feu, les systèmes de détection d'intrusion, les serveurs proxy et les IXP. Divers composants virtuels intangibles ou abstraits sont également nécessaires pour que l'Internet fonctionne, comme l'adressage, le routage, les protocoles et services d'application, les protocoles de sécurité et le Système d'adressage par domaines (DNS).

- **Le paysage de la menace à la sécurité en Afrique**
  Fondamentalement, la nature des cybermenaces en Afrique est largement similaire au reste du monde. Cependant, la connectivité intermittente est un problème grave, qui distingue l'Afrique de la plus grande partie du reste du monde. La connectivité intermittente est le résultat d'un certain nombre de facteurs tels que l'insuffisance des ressources en termes de bande passante, le coût de la connectivité Internet, les coupures de courant et les pannes d'électricité fréquentes, le manque de maintenance efficace et de correctifs planifiés, le manque de personnel qualifié, les facteurs naturels (le mauvais temps), et les facteurs humains (fraude, sabotage, vol, pénurie de carburant, etc.). La connectivité intermittente limite la capacité des parties prenantes à collaborer pour se préparer ou réagir à une attaque.

- **Les composants de l'infrastructure Internet qui sont des cibles faciles des cyberattaques**
  De nombreux systèmes commerciaux et industriels ont des logiciels embarqués qui sont périmés et/ou non corrigés, et sont donc particulièrement vulnérables. Par exemple, de nombreux systèmes financiers et réseaux du secteur public dépendent de machines exécutant un logiciel qui n'est plus pris en charge par ses développeurs et pour lesquels les mises à niveau de sécurité ne sont plus disponibles. Le secteur des communications mobiles fait face également à des préoccupations similaires. Dans certains cas, les appareils mobiles sont vendus avec des logiciels périmés ou non corrigés. Parallèlement aux logiciels périmés ou non pris en charge, une incapacité ou une réticence à mettre à niveau ou à réparer les serveurs et les applications de manière régulière rend les systèmes vulnérables aux attaques.

  Les attaques physiques sur l'infrastructure constituent également une menace. Les attaques peuvent être motivées par des raisons financières, un activisme politique ou même le terrorisme. Les dommages physiques à l'infrastructure peuvent également être involontaires, en raison de facteurs tels que le manque d'entretien régulier de la part des opérateurs, ou de la négligence due à de mauvaises pratiques opérationnelles et de gestion.

Les coupures de fibres ont été citées comme un exemple d'attaques physiques. Il est difficile d'éviter totalement ce problème, mais des solutions pour identifier et localiser les coupures peuvent contribuer à atténuer l'impact. Le partage d'informations entre les opérateurs est essentiel à cet égard.

Un autre problème est le manque de transparence concernant les cyberattaques. Certaines organisations ne signalent pas d'incidents de sécurité. Il devient donc difficile de connaître l'ampleur des attaques en Afrique et de trouver des solutions. Par conséquent, un écosystème de confiance devrait être favorisé afin que tout le monde (y compris les opérateurs et les utilisateurs finaux) puisse tirer des enseignements des cyberincidents. Les pratiques établies en matière de divulgation responsable et de coordination de la divulgation des vulnérabilités sont également importantes, car elles permettent de recueillir des informations de manière à ne pas exposer l'infrastructure à d'autres risques.

- **Mesures visant à prévenir et à atténuer le risque de cyberattaques**
  Le partage de l'information, la législation et l'application efficace, et les meilleures pratiques reconnues ont été identifiés comme des mesures importantes pour prévenir et atténuer les risques de cyberattaques.

  Le partage de l'information est essentiel dans le renforcement des capacités, l'identification des menaces et l'élaboration des meilleures pratiques (techniques, politiques, juridiques, économiques, etc.). S'assurer que les bonnes pratiques sont en place pour permettre aux acteurs concernés de partager l'information de manière responsable est tout aussi important. Il existe de nombreux moyens efficaces de partage de l'expertise, y compris le Groupe des opérateurs de réseau africains (AfNOG) et le Forum africain sur le peering et l'interconnexion (AfPIF). L'atelier est un des moyens efficaces pour atteindre la communauté des opérateurs dans son ensemble.

  Une législation et une mise en application robustes contribuent à dissuader la cybercriminalité, tant au niveau local qu'international. Les cadres juridiques et réglementaires d'autres continents fournissent des points de départ utiles pour améliorer les meilleures pratiques dans le contexte africain. Des lignes directrices nationales devraient être élaborées pour mesurer l'efficacité des politiques de sécurité, ainsi que les conséquences imprévues.

  Les meilleures pratiques fournissent aux parties prenantes, des informations pertinentes et actuelles sur les méthodes de sécurité et les menaces à la sécurité. Les meilleures pratiques peuvent promouvoir des activités efficaces de surveillance de la sécurité des réseaux et encourager les opérateurs et les fournisseurs de services à effectuer et à partager des analyses régulières des risques.

- **Les principales parties prenantes doivent améliorer la sécurité de l'infrastructure Internet en Afrique**
  Toutes les parties prenantes en Afrique doivent renforcer leurs capacités dans le domaine de la cybersécurité. Il s'agit entre autres des gouvernements, du secteur privé, de la société civile, des universités et de la communauté technique.

2.2 Éléments de base de l'infrastructure Internet

Les résultats du débat d'experts, des entretiens avec des professionnels et de la recherche documentaire nous permettent de répartir les principaux éléments de l'infrastructure Internet dans six catégories : les protocoles et services, les logiciels et le matériel, l'interconnexion de réseau, l'infrastructure de communication, l'information et les ressources humaines.

a. **Protocoles et services**
   Un protocole est une norme pour les systèmes informatiques. Le protocole permet une communication effective entre les différents systèmes informatiques, ce qui en fait un actif précieux dans l'infrastructure Internet. Les protocoles peuvent être divisés en couches Datalink, Internet, Transport et Application.

Un service, dans le contexte de l'infrastructure Internet, se réfère à une combinaison abstraite de fonctionnalités utilisant d'autres actifs pour remplir une tâche définie. Sans les services, l'Internet serait peu utile. Les services peuvent être catégorisés comme suit : l'adressage essentiel (divisé en adressage de couche de liaison, adressage IP, adressage de protocole de transport et DNS), le routage, les applications (comme le courrier électronique ou le transfert de fichiers) et les services de sécurité. Les pirates exploitent les vulnérabilités des services et des protocoles, il est donc important de mettre en place les dernières versions des normes correspondantes afin d'assurer une sécurité maximale.

b. Logiciels et matériels

Dans le cadre de l'infrastructure de base de l'Internet, les logiciels peuvent être globalement répartis dans quatre catégories : celle des systèmes d'exploitation, celle des pilotes de périphériques, celle des microprogrammes et celle des programmes exécutables. Les produits logiciels présentent plusieurs vulnérabilités de sécurité qui nécessitent des correctifs réguliers et d'autres méthodes.

Le matériel est une composante physique des systèmes informatiques tels que les machines ou le câblage. Dans le cadre de l'infrastructure Internet, ils sont regroupés en trois catégories : les périphériques réseau (tels que les commutateurs, les routeurs, les pare-feu et les passerelles), les serveurs et les périphériques utilisateurs finaux (tels que les ordinateurs personnels ou les appareils mobiles).

c. Interconnexion de réseau

Puisque l'Internet est un réseau de plusieurs réseaux, les actifs fournissant l'interconnexion sont essentiels. Deux exemples qui facilitent l'interconnexion sont les fournisseurs d'accès Internet (FAI) et les IXP. Un fournisseur d'accès Internet fournit aux clients un accès Internet à l'aide de différentes technologies de transmission de données. Un IXP est l'emplacement physique où différents réseaux IP se rencontrent pour échanger du trafic local entre eux via un commutateur.

d. Infrastructure de communication

Les infrastructures de communication sont les structures physiques de base et les installations (par exemple, les bâtiments et les câbles) nécessaires au fonctionnement de l'Internet. Pour construire l'Internet, l'infrastructure de soutien est cruciale. L'infrastructure peut être divisée en plusieurs catégories : le câblage et l'interconnexion (sans fil, par onde hyperfréquence, radiofréquence et satellite, et filaire comme la fibre, le cuivre, le haut débit), les bâtiments (installations spéciales comme les points d'ancrage pour les câbles sous-marins ou les centres de données polyvalents utilisés pour abriter tous types de matériel et d'infrastructure), l'alimentation électrique, les systèmes de refroidissement et la sécurité physique (clôtures, murs, portes, etc.).

e. Information

L'information provient de la collecte de données. Les systèmes (par exemple, les logiciels, le matériel, les services) et les humains sont tributaires des informations fournies pour prendre des décisions raisonnables. Dans le contexte de l'infrastructure Internet, les actifs d'information sont regroupés en quatre domaines : l'inventaire (des matériels, des logiciels, de l'infrastructure, des informations), la topologie du réseau, la configuration du système et les informations opérationnelles.

f. Ressources humaines

Les ressources humaines sont les employés considérés comme actifs de l'infrastructure Internet. Ce sont les administrateurs, les opérateurs, les membres de l'équipe de soutien, les développeurs, les gestionnaires, les commissaires aux comptes et les utilisateurs finaux.

Peu importe la sécurité technique qu'une partie prenante peut avoir, les ressources humaines non formées et inefficaces sont des vulnérabilités potentielles pour leurs systèmes. Au contraire, des ressources humaines bien formées et efficaces renforcent la sécurité des systèmes. Les caractéristiques importantes des ressources humaines sont : la compétence, la compréhension et le soutien de la direction, la discipline des membres du personnel à respecter les procédures et la fiabilité des membres du personnel.

2.3 Principes nationaux de sécurité de l'infrastructure Internet

Lors de l'élaboration de stratégies nationales pour la sécurité de l'infrastructure Internet, les décideurs africains doivent s'orienter grâce aux quatre principes essentiels[8] qui sont la sensibilisation ; la responsabilité ; la coopération ; et les droits fondamentaux et les propriétés de l'Internet.

a. **Sensibilisation :** une compréhension des risques de sécurité et de l'impact qu'ils peuvent avoir sur les autres éléments de l'écosystème de l'infrastructure Internet. Les membres de l'écosystème d'infrastructure Internet africain doivent être capables d'identifier les risques et de les gérer, et d'évaluer l'impact des actions sur soi-même et sur les autres membres.

b. **Responsabilité :** Assumer la responsabilité de la gestion des risques de sécurité. En raison de la nature fondamentale de l'Internet, il faut prendre en compte des impacts potentiels de ses actions, ou de ses inactions, sur d'autres parties prenantes avant d'agir.

c. **Coopération :** participer à un dialogue continu sur la cyber-sécurité avec tous les acteurs transfrontaliers afin de contrer efficacement les menaces nouvelles et persistantes. La sécurité de l'infrastructure critique de l'Internet ne peut être établie isolément. Il existe un besoin de coopération et de responsabilité collective entre toutes les parties prenantes, sans se limiter au gouvernement et à un certain nombre de parties prenantes.

d. **Droits fondamentaux et propriétés de l'Internet :** les mesures de gestion des risques de sécurité doivent respecter les droits fondamentaux et les propriétés fondamentales de l'Internet et doivent être transparentes, y compris la collaboration volontaire, les normes ouvertes, les composantes technologiques réutilisables, l'intégrité, l'innovation sans autorisation et la présence mondiale.[9]

Une approche efficace de la sécurité de l'infrastructure Internet doit non seulement utiliser ces principes, mais habiliter toutes les autres parties prenantes à les utiliser. L'approche doit soutenir les conditions de la sécurité collaborative[10] et favoriser un dialogue continu sur la sécurité, encourager la transparence et habiliter les autres à préserver les propriétés fondamentales de l'Internet. L'approche doit améliorer l'accès et contribuer à un écosystème Internet plus ouvert, sans censure et respectueux de la vie privée.

8 Voir l'annexe II au sujet des principes fondamentaux de sécurité.

9 Pour plus d'informations sur les propriétés fondamentales de l'Internet, consultez la publication d'ISOC « Internet Invariants : What Really Matters » https://www.internetsociety.org/internet-invariants-what-really-matters

10 Pour plus d'informations sur la sécurité collaborative, voir la publication d'ISOC Collaborative « Security: An Approach to Tackling Internet Security Issues » http://www.internetsociety.org/collaborativesecurity

3. Recommandations

La cybersécurité est la responsabilité de toutes les parties prenantes, y compris les gouvernements, le secteur privé, la société civile, les universités et la communauté technique. Étant donné que l'Internet est un réseau mondial de réseaux interconnectés, aucune partie prenante ne peut agir seule pour assurer avec succès la sécurité de l'Internet. Même les gouvernements et les opérateurs puissants de réseaux ne peuvent sécuriser l'Internet, comme le montrent clairement certains incidents majeurs survenus l'année dernière.[11]11 L'Internet couvre tous les pays et se compose de milliers de réseaux individuels, composés chacun d'un grand nombre d'utilisateurs et d'appareils. Un écosystème fiable d'infrastructure Internet ne peut être réalisé que par des efforts de coopération entre toutes les parties prenantes.

Chaque partie prenante doit appliquer les principes essentiels de la sensibilisation, de la responsabilité, de la coopération et de la défense des droits fondamentaux et des propriétés de l'Internet lorsqu'elle prend des mesures spécifiques pour protéger ses systèmes et l'ensemble de l'écosystème Internet. Sinon, les mesures destinées à protéger l'Internet pourraient finir par le nuire.

À la lumière des débats d'experts, des entretiens menés avec des professionnels, de la recherche documentaire et, conformément aux principes essentiels, cette section présente des recommandations spécifiques.

Bien que de nombreuses solutions de cyber-sécurité développées ailleurs puissent fonctionner pour l'Afrique, certaines caractéristiques rendent l'Afrique différente. La plupart des pays africains diffèrent du reste du monde (à l'exception de certains pays en voie de développement dans d'autres continents) de la manière suivante :

- Une pénurie de ressources humaines qualifiées dans le domaine de la cybersécurité
- Les ressources (y compris les ressources financières) disponibles qui sont allouées pour la cybersécurité par les gouvernements, les organisations et d'autres parties prenantes sont limitées
- Des niveaux limités de sensibilisation aux problématiques de la cyber-sécurité parmi les principaux acteurs, tels que les régulateurs des TIC, les organismes chargés de faire respecter la loi, le système judiciaire, les professionnels de la technologie de l'information et les utilisateurs
- Un manque de sensibilisation aux risques liés à l'utilisation des TIC

Ces différences sont prises en compte dans ces recommandations.

Les Lignes directrices présentent les cinq volets suivants pour les solutions de cybersécurité :

- Les mesures juridiques et réglementaires, y compris la législation et l'application de la loi
- Le renforcement des capacités stratégiques pour améliorer les connaissances, l'expertise et les compétences afin de renforcer la cybersécurité
- Des solutions techniques et procédurales comme moyen de remédier aux vulnérabilités des logiciels et du matériel
- Les structures institutionnelles et organisationnelles qui visent à créer un environnement de collaboration propice à la prévention, à la détection et à l'intervention en cas d'attaques contre l'infrastructure critique de l'Internet.

11 Par exemple, l'attaque Dyn DDoS, le piratage du Comité National Démocratique des États-Unis, et l'attaque du Département américain de la justice.

- Une coopération efficace à l'échelle mondiale, qui met l'accent sur les stratégies de collaboration, de coordination et de partage d'informations continues et inclusives entre toutes les parties prenantes afin de renforcer la confiance accordée à l'Internet.

Cependant, d'autres solutions, comme les incitations économiques, peuvent également être utilisées pour améliorer la sécurité.

Les recommandations de cette section couvrent les cinq volets.[12] Il convient de noter que certaines de ces recommandations pourraient déjà être mises en œuvre dans certains pays, mais pas dans d'autres. Bien que l'accent soit mis sur la sécurité de l'infrastructure Internet, il est parfois difficile de séparer cet objectif de l'objectif général de la sécurité de l'information et du réseau. Par conséquent, certaines recommandations peuvent être plus proches du domaine de la sécurité de l'information.

3.1 Au niveau régional (à l'échelle de l'UA)

Comme l'Internet est conçu comme un ensemble de réseaux interconnectés, la responsabilité de la sécurité est partagée. Chaque participant doit être conscient que sa propre sécurité dépend aussi de la sécurité des réseaux voisins et que les décisions de sécurité ont un impact sur les autres. Il existe donc une responsabilité collective de mettre en œuvre les meilleures pratiques en matière de cybersécurité. Nous recommandons d'établir une structure de coordination au niveau continental et de lancer de nouvelles initiatives de renforcement des capacités. Il convient de noter que nous avons examiné les institutions africaines existantes qui participent à des activités liées à l'Internet afin d'éviter tout double emploi.

3.1.1 Établissement d'un Comité africain de coordination et de collaboration en matière de cybersécurité (ACS3C)

L'établissement d'un Comité africain de coordination et de collaboration en matière de cybersécurité (ACS3C) facilitera la coordination et le partage d'informations entre les parties prenantes. Il permettra d'identifier les domaines de la cybersécurité qui nécessitent des ressources et de conseiller les décideurs de l'Union africaine sur les stratégies régionales et le renforcement des capacités.

Le Comité que la CUA, en collaboration avec la communauté Internet africaine, sera un réseau d'experts restreint, fiable et en évolution. Le leadership du Comité sera multipartite. Il sera composé, entre autres, d'experts issues d'organisations et d'institutions panafricaines et nationales compétentes telles que AfricaCERT, des représentants des universités, de la communauté technique, de la société civile, des organismes régionaux chargés de l'application de la loi et de certaines structures nationales multisectorielles chargées de la cybersécurité. Grâce à sa structure de réseau multipartite, le Comité peut s'adapter plus facilement aux nouveaux problèmes liés à la sécurité auxquels l'Afrique est confrontée. Le Comité sera chargé de conseiller et de soutenir la CUA dans ses activités de cybersécurité en assumant les responsabilités suivantes :

- Conseiller la CUA sur les questions et politiques de cybersécurité, telles que les initiatives de renforcement des capacités ;
- Proposer des solutions afin de faciliter la mise en œuvre de la Convention ;
- Partager les recommandations sur les meilleures pratiques en matière de sécurité de l'infrastructure Internet ;
- Identifier les domaines de recherche nécessaires à la formulation de politiques, de lignes directrices, etc. qui peuvent être d'ordre général ou spécifique à des secteurs particuliers, par exemple, la cybersécurité pour les technologies de réseau intelligent dans le domaine de l'industrie de l'énergie électrique, pour les systèmes financiers et pour les outils de surveillance des équipements ;

12 Pour des recommandations élargies concernant les mesures juridiques, voir, par exemple la note d'orientation de la CEA, « Relever les défis de la cybersécurité en Afrique », Numéro NTIS/002/2014.

- Identifier les moyens de soutenir les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), y compris AfricaCERT, dans le domaine du renforcement des capacités et du partage d'informations au niveau régional et de l'Union africaine ;
- Encourager la collaboration étroite entre les parties prenantes, y compris en matière de divulgation responsable et coordonnée ;
- Proposer les moyens d'accroître les compétences des professionnels de sécurité en Afrique (par exemple en favorisant des programmes de certification digne de confiance) ;
- Soutenir la CUA dans la formulation de stratégies en matière de cyber-sécurité et de renforcement des capacités ;
- Soutenir la CUA et les États membres dans le domaine de la coopération internationale en matière de cybersécurité.

Le Comité doit travailler en étroite collaboration avec le Comité technique spécialisé de l'UA sur la communication et les TIC.

Des détails concernant son appellation, sa mission, sa vision, ses objectifs et ses activités détaillées pourraient être établis par la CUA en collaboration avec la communauté Internet africaine.

3.1.2 Engagement dans le renforcement des capacités et le partage des connaissances au niveau panafricain

Le renforcement des capacités et le partage des connaissances sont essentiels pour sécuriser l'infrastructure Internet en Afrique. Les parties prenantes, qu'il s'agisse des individus, des gouvernements, des organisations ou autres, doivent être équipées des outils nécessaires pour assurer la sécurité de l'infrastructure Internet tout en préservant la prospérité économique et sociale. Cela comprend des informations actuelles et utilisables sur les menaces et les techniques de sécurité, ainsi que sur les moyens de mise en œuvre. La recherche et le développement de la cybersécurité en Afrique doivent être améliorés afin de créer pour les acteurs africains des outils utilisables et actuels. En raison de la nature internationale de l'Internet, les informations doivent être mises à la disposition de toutes les parties prenantes, non pas seulement pour celles qui se trouvent dans les limites d'une frontière nationale.

Pour atteindre ces objectifs, la CUA doit mettre en place des programmes de renforcement des capacités, sur la base d'une évaluation des besoins, pour doter les parties prenantes des compétences nécessaires leur permettant de sécuriser l'infrastructure Internet. Ces programmes assureront la diffusion des outils, des techniques et des pratiques les plus modernes à d'autres parties prenantes grâce à des initiatives de sensibilisation. Les initiatives peuvent prendre différentes formes, comme des ateliers, des cours de formation et des conférences. Toutes les parties prenantes doivent participer à l'évaluation des besoins.

Les initiatives seront établies dans le cadre d'un processus en plusieurs étapes. Premièrement, l'ACS3C identifie les lacunes de capacité en matière de cybersécurité et conseille la CUA sur la manière d'agir. Ensuite, l'UA élabore des programmes en fonction des besoins identifiés par l'ACS3C et les met en œuvre en collaboration avec des organisations partenaires. Les possibles organisations ou institutions partenaires sont les CSIRT, les établissements universitaires et de recherche, la communauté technique de l'Internet, le secteur privé et la société civile.

En utilisant une approche axée sur l'initiative pour le renforcement des capacités, l'UA peut adapter ses efforts aux besoins et aux environnements spécifiques des différents pays africains. Il est important de noter que les initiatives ne seront pas uniquement techniques. Elles permettront plutôt de renforcer les capacités dans tous les domaines de la sécurité de l'infrastructure Internet, y compris les dimensions économiques et politiques. Surtout, ces initiatives favorisent le renforcement des capacités des parties prenantes qui ne disposent pas de ressources à affecter pour ces mêmes activités. Ces programmes encouragent également les organisations spécialisées à soutenir le renforcement des capacités sur des thèmes particuliers, même après que les initiatives initiales soient parachevées.

3.2 Au niveau national

Parallèlement au rôle que jouent les gouvernements nationaux pour faciliter le partage de l'information et promouvoir les meilleures pratiques, les gouvernements détiennent la position unique de législateur dans l'écosystème de l'infrastructure Internet. Par conséquent, les gouvernements doivent être les maîtres d'œuvre de la sensibilisation et de la responsabilité.

Les gouvernements peuvent adopter des lois sur la sécurité de l'infrastructure Internet. Il est important que les lois adoptées par les gouvernements respectent les quatre principes essentiels de la sensibilisation, de la responsabilité, de la coopération et des droits fondamentaux et des propriétés de l'Internet. Il importe également que l'application et l'impact potentiel des nouvelles lois soient soigneusement pris en considération avant promulgation. La ratification et la mise en application de la Convention sont la première étape importante vers la création d'un contexte juridique africain qui permet le développement d'un écosystème sain pour la sécurité de l'infrastructure Internet.

De plus, les gouvernements doivent envisager l'utilisation d'autres outils dont ils disposent, tels que les incitations économiques, la promotion du changement par les pratiques d'achat, la promotion de l'autorégulation de l'industrie et l'habilitation des citoyens à exiger de meilleures solutions de sécurité. Parfois, ces solutions peuvent être plus efficaces que la législation.

3.2.1 Identification et protection de l'infrastructure critique de l'Internet

L'identification de l'infrastructure critique de l'Internet est aussi importante que la promotion des actions à mener pour assurer leur sécurité. Une mauvaise classification des infrastructures critiques de l'Internet peut nuire à d'autres aspects de la protection des infrastructures critiques de l'Internet (CIIP). Les infrastructures critiques de l'Internet qui sont mal répertoriées ne bénéficient pas

des politiques conçues pour la protection des infrastructures critiques de l'Internet (CIIP). Cela peut se traduire par des problèmes de sécurité au niveau des actifs et des services. De même, les infrastructures non critiques de l'Internet qui sont répertoriées comme « critiques » seront affectées par les politiques élaborées pour la protection des infrastructures critiques de l'Internet (CIIP), ce qui risque de nuire à leur efficacité.

Les gouvernements africains et d'autres parties prenantes doivent adopter une approche basée sur les services pour identifier les infrastructures critiques de l'Internet. Cela signifie que les services tels que ceux qui sont essentiels « à la sécurité publique, à la stabilité économique, à la sécurité nationale, à la stabilité internationale et à la durabilité et à la restauration du cyberespace » [13] doivent être analysés pour identifier les infrastructures de l'Internet qui sont indispensables à la prestation de ces services essentiels. Ces infrastructures sont ensuite répertoriées comme « infrastructures critiques de l'Internet ». Parallèlement à l'analyse des services, les infrastructures critiques de l'Internet identifiées doivent également être examinées afin de vérifier les dépendances. Les parties prenantes incontournables liées aux infrastructures critiques de l'Internet doivent également être identifiées.

Il faudrait prioriser en fonction de leur importance, entreprendre des évaluations des risques et mettre en place des mécanismes de défense appropriés pour la sécurité, tout en conservant les fonctionnalités. Les évaluations des risques sont particulièrement importantes dans ce contexte pour évaluer l'adéquation des solutions de sécurité aux actifs spécifiques. Compte tenu des ressources limitées, il est essentiel que les mesures prises soient appropriées au risque, qu'elles soient ni de trop ni de trop peu.

En plus des évaluations des risques et une approche basée sur les services, la modélisation des menaces peut être une méthode utile pour identifier et protéger les infrastructures critiques de l'Internet. La modélisation des menaces permet d'identifier et de répertorier les menaces potentielles par ordre de priorité en se plaçant du point de vue du pirate. Cette méthode permet aux défenseurs de la sécurité de l'Internet de déterminer les vecteurs de menace susceptibles d'être utilisés par les pirates et leurs cibles probables.

13 Voir la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel à l'adresse https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

3.2.2 Facilitation de l'échange d'informations par l'intermédiaire d'une structure nationale multipartite

La promotion du partage d'informations au niveau national est importante pour développer un écosystème sain pour la sécurité de l'infrastructure Internet. Des structures nationales multipartites devraient être créées pour apporter des conseils aux gouvernements nationaux sur la stratégie et la politique de cybersécurité et faciliter le partage d'informations entre les parties prenantes.

Ces structures devraient être de nature multipartite et inclure des parties prenantes telles que les CSIRT nationaux, le gouvernement national, la société civile, les universités, la communauté technique et le secteur privé. S'appuyant sur l'expertise de ses groupes de parties prenantes, le réseau identifie les domaines dans lesquels des mesures doivent être prises au niveau national. Parmi les actions nationales conseillées, on peut citer de nouvelles formations visant à remédier le déficit de capacité dans un domaine spécifique de la sécurité ou à adopter de nouvelles pratiques de sécurité au sein des organismes gouvernementaux.

3.2.3 Établissement et renforcement, au niveau national, des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT)

Les CSIRT sont essentielles pour faire face aux problèmes de sécurité de l'infrastructure Internet. Elles assurent une fonction importante dans l'identification des incidents de sécurité, en aidant les organisations à se protéger contre les cyberattaques et à restaurer leurs systèmes. La fréquence et la gravité des cyber-menaces nécessitent des moyens efficaces de surveillance, d'alerte et de réaction aux incidents. Même une organisation qui dispose d'un mécanisme de défense performant peut faire face à un cyberincident à tout moment.

Toutes les parties prenantes, y compris l'UA, les gouvernements nationaux et la communauté technique doivent œuvrer pour l'établissement de CSIRT quand il n'en existe aucun et soutenir les CSIRT qui favorisent les principes de sensibilisation, de responsabilité, de coopération et de droits fondamentaux et des propriétés de l'Internet, ainsi qu'un Internet libre et ouvert.

3.2.4 Promotion de la résilience de l'infrastructure Internet par le biais des points d'échange Internet (IXP)

Les gouvernements doivent promouvoir l'utilisation des IXP ainsi qu'une coopération et une connectivité accrues entre les différents réseaux africains. Les IXP peuvent limiter la portée des cyberattaques. De faibles charges de trafic sur les connexions internationales rendent les attaques DDoS plus difficiles à mener sur ces

infrastructures. Si une attaque rend inaccessible un lien international, le trafic local passant par un IXP n'est pas affecté. Les IXP sont essentiels pour développer une infrastructure Internet solide et résiliente.

Il est nécessaire d'accroître la collaboration transfrontalière entre les IXP. Par conséquent, au niveau régional, l'Association africaine des IXP (AFIX), qui a été créée pour coordonner et échanger des connaissances entre les IXP, devrait être soutenue pour qu'elle contribue davantage dans ce domaine. L'AFIX est une plateforme facilitant le partage d'expériences et l'apprentissage entre les IXP et les opérateurs.

3.2.5 Utilisation des institutions publiques pour donner l'exemple en matière de cybersécurité

Les gouvernements, en tant que propriétaires et opérateurs des systèmes et des réseaux d'information, pourraient donner l'exemple en adoptant les meilleures pratiques, en utilisant les technologies de sécurité, en satisfaisant les exigences législatives et par le biais de leurs processus des achats.

Il est essentiel que les gouvernements comprennent l'importance d'intégrer la cybersécurité dans leurs plans stratégiques en matière de TIC, en gardant à l'esprit que l'objectif global est la prospérité sociale et économique et la confiance sur l'Internet en Afrique. Les gouvernements doivent promouvoir activement l'utilisation des normes de sécurité et des meilleures pratiques

dans leurs propres infrastructures, par leurs agences et par les prestataires externes de services gouvernementaux.

Les gouvernements peuvent également utiliser leurs budgets pour s'assurer que les ressources appropriées, y compris le budget et le personnel, sont attribuées aux ministères et organismes gouvernementaux pour faire fonctionner et sécuriser leurs systèmes.

3.3 Au niveau des FAI et des opérateurs

Les opérateurs de réseau ont un rôle direct dans la sécurisation de l'infrastructure Internet, car ils gèrent les réseaux en Afrique. Une faille de sécurité dans le réseau d'un opérateur affecte non seulement ce réseau, mais potentiellement d'autres réseaux en Afrique et dans le reste du monde.

3.3.1 Établir un niveau de sécurité minimal

Pour établir un niveau de sécurité minimal afin de répondre aux défis de sécurité de l'infrastructure Internet, il faut une collaboration et un engagement de toutes les parties prenantes. Dans un monde interconnecté avec des interdépendances entre de multiples réseaux, des nations et des continents, il est très important que tous les participants respectent au moins un niveau de sécurité minimal. Beaucoup de ces participants vont rapidement dépasser ce niveau minimum et d'autres devront travailler pour atteindre ce seuil.

3.3.1.1 Sécurité du routage et du système d'adressage par domaines

Les opérateurs de réseau doivent empêcher la propagation d'informations de routage incorrectes ; empêcher le trafic avec des adresses IP source usurpées ; faciliter la communication opérationnelle globale et la coordination entre les opérateurs de réseau ; et faciliter la validation des informations de routage à l'échelle mondiale. L'usurpation d'IP ou la falsification d'adresse source est souvent utilisée dans les attaques de déni de service pour rendre le filtrage défensif plus difficile.

Les opérateurs de réseau devraient activer la validation DNSSEC sur leurs résolveurs DNS (serveurs DNS) pour assurer la sécurité du DNS. Les opérateurs de réseau devraient également intégrer d'autres meilleures pratiques en vigueur en matière de sécurité de routage et de résilience dans leurs processus de gestion de réseau.[14] L'une des initiatives mondiales, Commun Accord pour la Sécurité de Routage (Mutually Agreed Norms for Routing Security) soit MANRS,[15] définit un ensemble concis de mesures minimales mais critiques pour répondre aux exigences ci-dessus. Il décrit également un certain nombre de principes et de mesures que les opérateurs de réseau doivent mettre en œuvre pour assurer la résilience et la sécurité du système de routage global. L'initiative MANRS a été mise en place par des membres de la communauté des opérateurs de réseau avec le soutien d'ISOC.

3.3.1.2 Sécurité des réseaux

La sécurisation d'un réseau est nécessaire pour protéger le réseau et d'autres réseaux de l'écosystème Internet. Cela inclut le filtrage du trafic usurpé et du trafic d'attaque volumétrique, à la fois entrants et sortants, à partir de leurs réseaux. Le trafic sortant usurpé et le trafic d'attaque peuvent entraîner des problèmes de e-réputation d'adresse IP pour le réseau d'origine, mais entraîneront souvent des impacts négatifs plus directs sur d'autres réseaux de l'écosystème Internet.

La boîte à outils Anti-Spam Toolkit d'ISOC[16] fournit les meilleures pratiques aux décideurs, aux opérateurs de réseau et aux utilisateurs pour mieux sécuriser leurs réseaux contre la menace des courriers indésirables. Elle fournit également des liens vers des ressources externes sur

14 Deploy 360 est une bonne source d'information sur la sécurité des routages et la sécurisation du DNS pour les fournisseurs de services Internet (http://www.internetsociety.org/ deploy360/).
15 Voir https://www.routingmanifesto.org/manrs/
16 Voir http://www.internetsociety.org/spamtoolkit

les courriers indésirables et la lutte contre le trafic indésirable. Le code de conduite anti-bot M3AAWG17[17] à l'intention des prestataires de services Internet conseille aux FAI de s'engager dans l'éducation, la détection, la notification, la réhabilitation et la collaboration. Le code de conduite favorise les principes essentiels de sensibilisation, de responsabilité, de coopération et du respect des droits fondamentaux et des propriétés de l'Internet.

3.3.1.3 Pratiques essentielles de sécurité

Des protocoles sécurisés doivent être utilisés dans les produits et les services qui supportent l'infrastructure Internet. Par exemple, le TLS (transport layer security) est un protocole cryptographique qui devrait être utilisé pour protéger les services Web. Le protocole TLS crypte les données échangées dans une transaction HTTP et identifie cryptographiquement une ou plusieurs des parties engagées dans une transaction. La confidentialité et l'identité sont des éléments fondamentaux de l'infrastructure Internet sécurisée.

Les opérateurs doivent également veiller à ce que les logiciels indispensables à l'infrastructure Internet soient efficacement sécurisés contre les vulnérabilités de sécurité. Il ne faut déployer dans l'infrastructure Internet que des logiciels qui sont entretenus par un fournisseur ou une communauté des logiciels libres. Les opérateurs doivent appliquer une politique de correctifs qui accorde la priorité à l'atténuation des vulnérabilités des logiciels, malgré les risques inhérents à la disponibilité (up-time). Les opérateurs peuvent également développer un programme de gestion des vulnérabilités logicielles qui confie la responsabilité de l'atténuation continue des vulnérabilités logicielles à un individu ou à une institution. De nombreuses organisations n'assurent pas de manière adéquate la gestion des correctifs du fait de l'absence d'une responsabilité institutionnelle relative à la gestion des vulnérabilités logicielles.

3.3.2 Établir et entretenir une coopération et une collaboration

Au-delà de leur participation aux structures multipartites nationales décrites dans la section 3.2.2, les FAI et les opérateurs de réseau ont la responsabilité de la coordination et de la coopération entre elles, avec les organisations clientes et d'autres parties prenantes. Les FAI et les opérateurs de réseaux doivent :

- Encourager la coopération et la collaboration avec les organisations clientes, les gouvernements locaux et régionaux et les organismes de réglementation dans la prévention, la détection et l'atténuation des incidents de routage ;
- Faciliter la communication et la coordination opérationnelles globales entre les opérateurs de réseau ;
- Participer activement dans les associations des FAI telles que les groupes et forums d'opérateurs de réseaux nationaux et régionaux ;
- Créer des mécanismes de partage d'informations avec d'autres fournisseurs concernant les coupures de fibres, afin de réparer rapidement et d'accélérer l'entretien ;
- Coopérer avec les organismes de réglementation et d'application de la loi durant les enquêtes et les poursuites liées à la cybercriminalité ou à d'autres activités illégales.

3.4 Au niveau institutionnel et organisationnel

La direction doit assumer le leadership et la responsabilité face aux problèmes liés à l'Internet. Dans chaque organisation, un cadre supérieur doit être responsable de la sécurité de l'information de l'organisation. Dans ce rôle, le cadre supérieur doit allouer des ressources pour promouvoir une culture organisationnelle de la cybersécurité. Les pratiques de sécurité des organisations qui utilisent les TIC ont non seulement un impact important sur elles-mêmes, mais également sur l'ensemble de l'écosystème Internet. Il est donc important que ces organisations soient conscientes des répercussions de leurs actions (ou de leurs inactions) sur la sécurité des autres. Une politique de sécurité claire, correctement mise en œuvre, s'appuyant sur une évaluation récurrente des risques et défendue par l'organisation doit contenir, au minimum, plusieurs éléments d'action spécifiques. Il s'agit, notamment, d'appliquer des mesures de base essentielles pour le maintien d'un réseau sain ; de mettre en place un système adéquat

17 Voir https://www.m3aawg.org/abcs-for-ISP-code

de contrôles ; d'avoir un processus formalisé et une capacité permettant de répondre aux cyberincidents ; d'effectuer des exercices réguliers ; d'établir un processus de divulgation ; et d'établir des relations de confiance avec d'autres parties prenantes, telles que les responsables gouvernementaux et les équipes CSIRT.

Les gouvernements nationaux et d'autres parties prenantes doivent habiliter les organisations et les institutions pour qu'ils créent une culture de cybersécurité pour la prospérité économique et sociale grâce au partage d'informations, à la promotion des meilleures pratiques et en montrant l'exemple. Il faut mettre en place une structure organisationnelle au sein des institutions qui sont responsables des initiatives et des activités de cybersécurité.

Les organisations et les institutions doivent mettre en œuvre les meilleures pratiques actuelles et développer une culture de la cybersécurité au niveau opérationnel et exécutif.

3.5 Coopération mondiale

Les menaces de cybersécurité sont, par nature, mondiales et en croissance continue. L'adoption de solutions techniques pour la prévention, la détection, l'atténuation et la restauration est une façon de répondre à l'évolution des menaces. Cependant, ces mesures technologiques doivent être accompagnées d'une collaboration transfrontalière efficace. Les limites numériques ne coïncident pas avec les frontières nationales, faisant de la collaboration mondiale une partie essentielle du mécanisme d'intervention. En outre, la propagation et les implications des menaces telles que les logiciels malveillants illustrent qu'il ne s'agit plus de problèmes qu'une organisation peut traiter seule. La responsabilité repose plus que jamais sur l'ensemble des parties prenantes.

Par conséquent, le caractère transfrontalier des menaces rend indispensable la mise en place d'une coopération internationale étroite. Cela nécessite d'importants efforts au niveau national, continental et international. Il faut une coopération étroite avec les partenaires mondiaux pour prévenir et intervenir en cas de cyberincidents. Bien que la communication formelle puisse être utile, les méthodes informelles de communication fiables permettent une réaction plus rapide aux menaces, l'établissement de liens plus étroits entre les parties prenantes et une coopération et une collaboration plus solides.

Le développement de multiples canaux fiables pour la communication assure une meilleure coopération et un meilleur partage d'informations. Les organisations, telles que les CSIRT ou les groupes d'opérateurs de réseau (NOG), dégagent des pistes intéressantes de collaboration. Les organisations ou les réseaux peuvent être formés géographiquement ou autour d'une thématique ou d'un secteur spécifique. Les relations entre les opérateurs de réseau, souvent développés dans les NOG, permettent une meilleure sécurité. Par exemple, lorsqu'un opérateur de réseau reçoit un courrier indésirable provenant d'un autre réseau relié, l'opérateur de réseau affecté peut informer l'opérateur de réseau émetteur du courrier indésirable. Comme cet opérateur est plus proche de la source du courrier indésirable, il est plus à même de résoudre le problème.

L'importance de la dimension internationale de la cybersécurité et la nécessité d'établir de meilleures alliances et partenariats avec des pays ou des alliés partageant les mêmes principes, y compris le renforcement des capacités, ne doivent pas être négligées.

4. Conclusion

L'Internet est devenu de plus en plus important pour le développement économique et social du continent. C'est une nouvelle source de croissance et un moteur d'innovation, de bien-être social, de sécurité nationale, de gouvernance, de communication médiatique et de citoyenneté. À mesure que l'économie de l'Internet se développe, toute l'économie et la société, y compris les gouvernements, dépendent de plus en plus de l'infrastructure numérique pour exercer leurs fonctions essentielles.

Avec une plus grande exposition technologique et une dépendance à l'Internet, l'Afrique est confrontée à de nombreux nouveaux défis liés aux cybermenaces. Comme ailleurs dans le monde, les cybermenaces sont de plus en plus nombreuses.

De plus en plus de pirates avec des motivations diverses sont attirés par les nouvelles opportunités qu'offre Internet à l'Afrique. Leurs impacts directs et indirects ne sont plus limités aux organisations cibles individuelles. Ils représentent aujourd'hui une menace à la sécurité nationale des États. Le faible niveau de sensibilisation en matière de cybersécurité, le manque de financement, l'absence de volonté des gouvernements et des autres parties prenantes à lutter contre la cybercriminalité et, surtout, les compétences limitées en matière de cybersécurité rendent l'Afrique particulièrement vulnérable.

La protection des infrastructures critiques de l'Internet en Afrique doit être à la fois une priorité nationale et une priorité transfrontalière. Grâce à une approche multipartite aux niveaux régional et national, les pays africains peuvent intensifier leurs efforts pour atténuer les risques liés à la cybersécurité. Cependant, les responsabilités doivent être partagées par toutes les parties prenantes, y compris les gouvernements, le secteur privé, la société civile, les universités et la communauté technique.

Cet ensemble de recommandations est une première étape, mais significative, pour la création d'un changement visible positif dans le paysage africain de la cybersécurité. L'Internet est une opportunité pour l'Afrique. Contrairement aux révolutions technologiques du passé, la révolution numérique est à la portée du continent. Avec un taux d'adoption élevé de l'Internet et une population jeune, l'Afrique pourrait devenir le leader mondial de l'Internet et d'autres domaines des TIC. En prenant les mesures recommandées et en mettant en œuvre les principes essentiels de la protection de l'infrastructure Internet, les parties prenantes peuvent aider le continent à tirer profit de cette opportunité et à progresser vers l'adoption de la révolution numérique pour y jouer un rôle moteur.

5. Postface

Dans le domaine de l'Internet et ses industries connexes, l'Afrique a l'opportunité d'être concurrentielle et réussir à l'échelle internationale. Avec une population jeune et des taux d'adoption d'Internet élevés, l'Afrique devrait rattraper le reste du monde assez rapidement. L'Afrique déploie les infrastructures de manière novatrice, s'appuyant sur des technologies plus récentes, comme les appareils mobiles, la 3G et la 4G pour stimuler l'adoption de l'Internet.

Alors que les opportunités de l'Afrique sont excellentes, elle est également confrontée à des défis lorsqu'il s'agit de la sécurisation de l'infrastructure Internet. Beaucoup de personnes utilisent du vieux matériel qui ne supporte pas les logiciels récents, mettant ainsi leurs systèmes en danger. Beaucoup de personnes utilisent des logiciels piratés, qui présentent également des risques de sécurité majeurs puisqu'ils ne peuvent pas être corrigés pour réparer les vulnérabilités et risquent de contenir des programmes malveillants. De nombreux gouvernements africains n'ont pas également des cadres juridiques et réglementaires efficaces pour soutenir la sécurité de l'infrastructure Internet. Certains gouvernements ont un impact négatif sur l'infrastructure Internet, car ils bloquent ou limitent l'accès à l'Internet pour leurs citoyens ou les parties prenantes. Le blocage ou la restriction de l'Internet limite les capacités des parties prenantes à intervenir et à collaborer pour atténuer les menaces qui pèsent sur la sécurité.

Les Lignes directrices fournissent les recommandations clés pour protéger la sécurité de l'infrastructure Internet. Les recommandations présentent les actions les plus importantes à prendre et les principes essentiels devant guider les parties prenantes afin de créer une référence en matière de sécurité de l'infrastructure Internet en Afrique. Afin de sécuriser de manière plus conséquente l'infrastructure Internet, d'autres organisations africaines telles que les CSIRT et le Comité proposé (ACS3C) devraient créer des recommandations et des pratiques exemplaires plus spécifiques. Ce n'est qu'avec les efforts multipartites continus de la communauté Internet africaine que l'Afrique peut surmonter ses défis, saisir ses opportunités et devenir un leader mondial de l'Internet.


10/100/1000 PCI-E
eth0
eth1
eth2
LAN

Références

Union africaine. (2014, 27 juin). Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel. Extrait de l'adresse https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_f.pdf

African Union, Symantec Corporation. (2017, novembre). Cyber Crime et Cyber Security Trends in Africa. (Rep.) Extrait de l'adresse https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa

Arbor Networks, Google Ideas, & Big Picture Group. (2013). What is a DDoS Attack? (Qu'est-ce qu'une attaque DDoS ?) Extrait de l'adressehttp://www. digitalattackmap.com/understanding-ddos/

Chatzis, N., Smaragdakis, G., & Feldmann, A. (2013, July 19). On the Importance of Internet eXchange Points for today's Internet Ecosystem [Scholarly project]. In Cornell University Library.. Extrait de l'adresse https://arxiv.org/abs/1307.5264v2

Crucial Research. (2014, septembre). People's Role in Cyber Security: Academics » Perspective.. [White Paper]. Extrait du site de Crucial Research : https://www.crucial.com.au/pdf/Peoples_Role_in_Cyber_Security.pdf

Conrad, D. (2012, January). Towards Improving DNS Security, Stability, and Resiliency (Rep.). Extrait de l'adresse https://www. internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

European Network and Information Security Agency. (2012, novembre). Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime. (Publication). Extrait de l'adresse https://www.enisa.europa.eu/ publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime/at_ download/fullReport

European Network and Information Security Agency. (2013, octobre). Cybersecurity cooperation: Defending the digital frontline. (Publication). Extrait de l'adresse https://www.enisa.europa.eu/publications/cybersecurity-cooperation- defending-the-digital-frontline

European Network and Information Security Agency. (2016, janvier 27). ENISA Threat Landscape 2015. (Représentant.). Extrait de l'adresse https://www.enisa.europa.eu/publications/etl2015

European Network and Information Security Agency. (2015, janvier). Threat Landscape and Good Practice Guide for Internet Infrastructure. (Publication). Extrait de l'adresse https://www.enisa.europa.eu/publications/iitl/at_download/ fullReport

The European Union Agency for Network and Information Security. (2015, décembre). Information sharing and common taxonomies between CSIRTs and Law Enforcement. (Rep.) Extrait de l'adresse https://www.enisa.europa.eu/ publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

France, Agence Nacionale de la Sécurité des Systèmes d'Information. (2013, janvier). 40 essential measures for a healthy network. Extrait de l'adresse https://www.ssi.gouv.fr/en/actualite/40-essential-measures-for-a-healthy-network/

Information Commissioner's Office, UK. Security Breaches Licensed under the Open Government Licence. Extrait de l'adresse https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

Internet Corporation for Assigned Names and Numbers. (2009, août). SAC 40 - Measures to Protect Domain Registration Services Against Exploitation or Misuse. (Rep.) Extrait de l'adresse https://www.icann.org/en/system/files/ files/sac-040-en.pdf

International Organization for Standardization/International Electrotechnical Commission. (2012, juillet). Information technology - Security techniques - Guidelines for cyber security. (ISO/IEC 27032:2012). Extrait de l'adresse https://www. iso.org/standard/44375.html

Internet Society. (2015, avril). Collaborative Security: An approach to tackling Internet Security issues (Publication). Extrait de l'adresse http://www.internetsociety.org/collaborativesecurity

Internet Society. (2016, juin). Un cadre politique pour un Internet ouvert et de confiance. (Publication). Extrait de l'adresse http://www.internetsociety.org/doc/policy-framework-open-and-trusted-internet

Internet Society. (2016, février). The Internet Society and African Union Commission Survey on African ICT Policy Makers. (Publication). Extrait de l'adresse https://www.internetsociety.org/doc/internet-society-and-african-union-commission-survey-african-ict-policy-makers

Internet Society. (2012, février). Internet Invariants : What Really Matters (Publication). Extrait de l'adresse https://www.internetsociety.org/internet-invariants-what-really-matters

Internet Society. (2016, octobre). Policy Brief : Internet Invariants. (Brief). Extrait de l'adresse http://www.internetsociety. org/policybriefs/internetinvariants

Internet Society. (2011). Deploy 360. Extrait de l'adresse http://www.internetsociety.org/deploy360/

Internet Society. (2015). Anti-Spam Toolkit. Extrait de l'adresse https://www.internetsociety.org/spamtoolkit
International Telecommunications Union. (2011, septembre). The ITU National Cybersecurity

Strategy Guide (Publication). Extrait de l'adresse http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

International Telecommunications Union, World Telecommunication Standards Assembly. Resolution 58, Encourage the creation of national Computer Incident Response Teams, particularly for developing countries (20-29, November, 2012) Retrieved from https://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2058.pdf

International Telecommunications Union, Plenipotentiary Conference of the International Telecommunication Union. Resolution 130, Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. (2014). Extrait de l'adresse https://www.itu.int/en/action/cybersecurity/Documents/ Resolutions/pp-14_Res.%20130.pdf

International Telecommunications Union Development Sector. (2009, April). Understanding Cybercrime: A Guide for Developing Countries, ICT Applications and Cybersecurity Division, Policies and Strategies Department. (Rep.) Extrait de l'adresse https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

Krebs, B. (2016, October). Hacked Cameras, DVRs Powered Today's Massive Internet Outage. Extrait de l'adresse https:// krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

MANRS. (2014). Mutually Agreed Norms for Routing Security https://www.routingmanifesto.org/

McAfee. (2017, avril). McAfee Labs Threat Report: April 2017 (Rep.) Retrieved from https://www.mcafee.com/ca/security-awareness/articles/mcafee-labs-threats-report-mar-2017.aspx

Messaging, Malware and Mobile Anti-Abuse Working Group. (2012, mars). The Anti-Bot Code of Conduct for Internet Service Providers: A Voluntary Industry Code to Help Reduce End-User Bots. (Publication). Extrait de l'adresse https://www.m3aawg.org/abcs-for-ISP-code

Michael, C. (2009, August). Computer Viruses Slow African Expansion.. Guardian. Extrait de l'adresse https://www.theguardian.com/technology/2009/aug/12/ethiopia-computer-virus

Nakashima, E. (2016, October), US government officially accuses Russia of hacking campaign to interfere with elections. Washington Post. Extrait de l'adresse https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.9961e9ff4fb3

Wilson, M., & Hash, J. (2003, October). Building an Information Technology Security Awareness and Training Program (United States, National Institute of Standards and Technology). Extrait de l'adresse http://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-50.pdf

Organisation for Economic Co-operation and Development. Ministerial Meeting on the Future of the Internet Economy (2008, June). OECD Recommendation of the Council on the Protection of Critical Information Infrastructures OECD Ministerial Meeting on the Future of the Internet Economy.

Schumann, R., & Kende, M. (2013, May). Lifting barriers to Internet development in Africa: Suggestions for improving connectivity. (Rep.) Extrait de l'adresse http://www.internetsociety.org/doc/lifting-barriers-internet-development-africa-suggestions-improving-connectivity

SANS Institute. (2015, décembre). Infrastructure Security Architecture for Effective Security Monitoring. (Publication) Extrait de l'adresse https://www.sans.org/reading-room/whitepapers/bestprac/infrastructure-security-architecture- effective-security-monitoring-36512

SSAC (ICANN Security and Stability Advisory Committee). (2009). SAC 40 : Measures to Protect Domain Registration Services Against Exploitation or Misuse. (Publication) Extrait de l'adresse https://www.icann.org/en/system/files/files/ sac-040-en.pdf

Storm, D. (2016 February). Hackers Breach DOJ, dump details of 9,000 DHS employees, plan to leak 20,000 from FBI. Computerworld. Extrait de l'adresse http://www.computerworld.com/article/3030983/security/hackers-breach-doj-dump-details-of-9-000-dhs-employees-plan-to-leak-20-000-from-fbi.html

Symantec. (2016). Internet Security Report (21 vol.). Symantec. Extrait de l'adresse https://www.symantec.com/content/ dam/symantec/docs/reports/istr-21-2016-en.pdf

Symantec. (2013, avril). Internet Security Threat Report (18 vol.). Symantec. Extrait de l'adresse http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18

Commission économique des Nations Unies pour l'Afrique (2014), Relever les défis de la cybersécurité en Afrique. (Publication) Extrait de l'adresse https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1_fr.pdf

United States National Institute of Standards and Technology. (2014, février, 12). Framework for Improving Critical Infrastructure Cybersecurity. (United States, National Institute of Standards and Technology). Extrait de l'adresse https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Annexes

Les annexes suivantes comprennent des définitions pour aider à expliquer les concepts et la terminologie trouvés dans les Lignes directrices aux besoins des lecteurs qui ne connaissent pas les termes. Les définitions ne constituent pas un glossaire complet, et ne sont pas des définitions faisant autorité sur ces sujets. Ils sont destinés à fournir une introduction simple aux termes.

Annexe I : La terminologie liée à l'Internet et à la sécurité

a. Les attaques et les vecteurs d'attaques

- Les pirates peuvent utiliser une variété d'outils, de scripts et de programmes pour lancer des attaques contre des réseaux et des périphériques de réseau, et pour tromper ou compromettre le personnel ou les fournisseurs qui ont accès au réseau, que ce soit sur le site ou à distance. En règle générale, les périphériques réseau attaqués sont les points d'extrémité, tels que les serveurs et les ordinateurs. Une cyberattaque se produit si un attaquant déjoue les contrôles de sécurité.

- Un vecteur d'attaque est un moyen par lequel un attaquant peut accéder à un réseau afin de fournir une charge utile (payload) avec un logiciel malveillant (malware). Les vecteurs d'attaque permettent aux pirates d'exploiter les failles des systèmes Les vecteurs d'attaque majeurs sont les botnets, les attaques DNS, le phishing (y compris les attaques ciblées ou le « phishing de lance ») et les attaques d'empoisonnement de table de routage.

b. Les meilleures pratiques

- Une méthode ou une pratique qui est généralement acceptée comme le moyen préféré pour atteindre le résultat souhaité.

c. Les violations de données à caractère personnel

- Dans le contexte des réseaux, « une violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, la modification, la divulgation ou l'accès non autorisé aux données à caractère personnel transmises, stockées ou autrement traitées dans le cadre de la fourniture »[18] d'un service de communications électroniques.

d. Approche de sécurité collaborative

- L'approche de sécurité collaborative en matière de sécurité de l'Internet reconnaît que ce sont les personnes qui finalement assurent l'équilibre et l'unité de l'Internet. Le développement de l'Internet repose sur une coopération et une collaboration volontaires. La coopération et la collaboration restent les facteurs essentiels pour sa prospérité et son potentiel. L'approche met l'accent sur cinq principes : préserver les opportunités et renforcer la confiance ; la responsabilité collective ; les solutions de sécurité entièrement intégrées aux droits et à l'Internet ouvert ; les solutions de sécurité fondées sur l'expérience, développées par consensus et évolutives dans les perspectives ; et en ciblant le point d'impact maximal - pensez globalement, agissez localement.[19]

18 Voir https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/
19 Voir http://www.internetsociety.org/collaborativesecurity

e. L'équipe d'intervention en cas d'incident de sécurité informatique (CSIRT)

- Une organisation ou une communauté d'experts qui reçoit, examine et répond à des incidents de sécurité informatique. Ils peuvent être spécifiques à différents secteurs ou à différentes régions, et dirigés par le secteur public et/ou privé. Les CSIRT fournissent une fonction critique de partage des connaissances pour assurer la sécurité.

f. Les infrastructures critiques de l'Internet

- Les systèmes et réseaux interconnectés, dont la perturbation ou la destruction aurait un impact important sur la santé, la sécurité, le bien-être économique des citoyens, la fourniture de services essentiels ou le fonctionnement efficace du gouvernement ou de l'économie.

g. Les attaques de Déni de Service Distribué (DDoS)

- Une attaque DDoS « est une tentative de rendre un service en ligne indisponible en surchargeant le trafic provenant de plusieurs sources »[20].

h. Système d'adressage par domaines (domain name system, DNS)

- Système de bases de données et de serveurs assurant la correspondance entre les noms de domaine ou de site utilisés par les internautes et les adresses numériques utilisables par les ordinateurs ou les systèmes connectés à l'Internet. Ce système permet aux internautes d'utiliser, dans la rédaction des adresses, des noms faciles à retenir au lieu de la suite de chiffres du protocole IP. Une requête d'un serveur DNS correspondra à un nom de domaine à l'adresse IP requise par l'ordinateur pour acheminer le trafic vers sa destination prévue.

i. Propriétés fondamentales d'Internet (ou Invariants Internet)

- « Les caractéristiques qui ont permis à l'Internet de servir de plateforme pour une innovation apparemment illimitée mettent en valeur non seulement sa technologie, mais aussi sa forme en termes d'impact global et de structures sociales »[21]. Ces caractéristiques identifiées sont : la collaboration volontaire, les normes ouvertes, les composantes technologiques réutilisables, l'intégrité, l'innovation sans autorisation et la portée mondiale.

j. Point d'échange Internet (IXP)

- Un système qui permet à de nombreux réseaux Internet d'échanger du trafic entre eux à un point de rencontre commun, éliminant ainsi la nécessité de créer des liens bilatéraux distincts avec chaque réseau local.

k. Infrastructure Internet

- Les éléments qui constituent et permettent le mouvement des données utilisables sur un réseau interconnecté de réseaux. Ces éléments incluent des protocoles et des services, des logiciels et du matériel, l'interconnexion de réseau, l'infrastructure de communication, l'information et les ressources humaines.

l. Fournisseurs d'accès Internet (FAI)

- Une entreprise ou une organisation qui offrent aux particuliers, aux organisations, aux entreprises et à d'autres personnes un accès à l'Internet. Mis à part la connexion des utilisateurs, les fournisseurs d'accès Internet fournissent souvent pour leurs clients d'autres services tels que le courrier électronique et l'hébergement de sites Web.

m. Routage

- Le routage détermine comment le trafic se déplacera d'un point du réseau vers un autre. Les nœuds de réseau qui prennent les décisions de routage s'appellent des routeurs. Les informations sur les possibilités d'accès (c'est-à-dire si un réseau particulier peut être atteint via un nœud) sont échangées entre les routeurs Internet. Les deux types de protocoles utilisés pour échanger ces informations sont le protocole de routage interne (Interior Gateway Protocol) qui échange des informations de routage à l'intérieur d'un réseau (tel que OSPF, IS-IS ou RIP) et le protocole de routage

20 Voir http://www.digitalattackmap.com/understanding-ddos/

21 Voir https://www.internetsociety.org/internet-invariants-what-really-matters

externe (Border Gateway Protocol, BGP) qui est utilisé entre les réseaux ou les systèmes autonomes (AS). L'une des vulnérabilités du protocole BGP est qu'il ne fournit pas les moyens de vérifier la validité des informations échangées. Une telle validation nécessite l'utilisation d'outils et de pratiques supplémentaires.

n. Les parties prenantes

- Les individus, les groupes, les organisations, les entités ou les communautés qui ont un intérêt ou une participation dans l'Internet. Les parties prenantes comprennent les gouvernements, le secteur privé, la société civile, les universités et la communauté technique.

o. Les menaces

- Une menace est un événement potentiel qui peut exploiter une vulnérabilité (les faiblesses dans les systèmes, les réseaux et les périphériques) et causer un impact négatif sur le réseau, le système ou l'organisation. Une menace est l'événement possible, alors qu'une attaque est l'incidence d'un tel événement. Les menaces peuvent être accidentelles ou intentionnelles. Les menaces accidentelles n'ont pas d'intention préméditée. Un dysfonctionnement potentiel du système ou du logiciel, une mauvaise configuration ou une divulgation accidentelle d'informations sensibles ou privées sont des exemples de menaces accidentelles. Des menaces intentionnelles sont des actes délibérés éventuels contre la sécurité d'un actif. Les menaces intentionnelles vont de l'examen occasionnel potentiel d'un réseau informatique utilisant des outils de surveillance facilement accessibles, aux attaques délibérées sophistiquées utilisant des connaissances spécifiques du système.

- Les menaces au réseau doivent être identifiées et les vulnérabilités connexes doivent être adressées afin de minimiser le risque de menaces. Les principales cybermenaces sont les logiciels malveillants, les attaques sur le Web, les attaques dirigées contre les applications Web, le déni de service, le phishing et le vol d'identité. Les menaces internes sont tout aussi dangereuses que celles provenant de l'extérieur du réseau.

p. Les agents de menace

- Il est habituel d'utiliser le terme pirate (attaquant) pour désigner une personne qui attaque un système informatique. « L'agent de menace » est un terme plus inclusif, se référant aux personnes qui attaquent ou ont attaqué un réseau, un système ou une organisation, aux côtés de ceux qui capitalisent sur une vulnérabilité (intentionnellement ou accidentellement) et causent un impact négatif sur le réseau, le système ou l'organisation.

- Les techniques d'évaluation des risques exigent une évaluation de la menace pour identifier les menaces auxquelles un système est confronté, et les acteurs ou les sources derrière eux. Bien qu'il soit possible d'identifier une menace et les vecteurs d'attaque correspondants utilisés, l'identification de l'agent de menace n'est pas simple. La collecte et l'analyse des journaux d'événements par le biais de systèmes spécialisés tels que le système de détection d'intrusion (IDS) ou même les systèmes de gestion d'information et d'événements de sécurité (SIEM) pourraient facilement révéler les menaces tentées ou réussies qui ont eu lieu, mais l'identification des agents de menace et l'analyse de leurs attributs nécessitent une enquête plus approfondie et l'expertise au-delà de la portée du domaine de la cybersécurité pure. L'identification des agents de menace devrait également englober des attributs tels que la motivation, la capacité, les opportunités exploitées et l'impact potentiel sur le système cible. L'analyse du journal est une approche utile et nécessaire, mais il peut être difficile de trouver l'information importante cachée dans de très grandes quantités de données collectées. Les journaux eux-mêmes peuvent également être utilisés par les attaquants pour obtenir des informations importantes sur le réseau et ses défenses, ce qui signifie que les journaux doivent également être protégés.

- Les principaux agents de menace sont des menaces d'initiés, des attaquants malveillants et des hacktivistes, des cybercriminels, des cyber-espions et des cyber-terroristes. Tous peuvent agir seuls, pour le compte ou au nom d'un État (par exemple, un organisme de sécurité nationale, un organisme militaire ou les autorités policières) ou des entités commerciales (dans le cas d'un espionnage industriel ou d'attaques).

q. Vulnérabilités

- Les vulnérabilités sont les faiblesses des systèmes, des réseaux et des dispositifs susceptibles d'être exploités par des agents de menace pour effectuer une attaque. Des vulnérabilités peuvent être présentes dans les protocoles de communication, les systèmes d'exploitation et les logiciels d'application fonctionnant sur des périphériques qui se connectent aux réseaux, y compris les routeurs, les commutateurs, les serveurs, les périphériques utilisateurs et même les périphériques de sécurité eux-mêmes. Les vulnérabilités peuvent être introduites par une mauvaise configuration et subsister en raison du manque de correctifs de logiciels.

- En général, les systèmes de réseau peuvent avoir une ou plusieurs des vulnérabilités ou faiblesses suivantes :
    - Faiblesses technologiques inhérentes ou bugs
    - Faiblesses de la configuration
    - Faiblesses de la politique de sécurité
    - Formation insuffisante des utilisateurs finaux, négligence des utilisateurs et actes intentionnels des utilisateurs finaux.

Annexe II : Principes fondamentaux de sécurité

Toutes les parties prenantes doivent comprendre les procédures de protection des actifs de l'infrastructure Internet et gérer les différents types de menaces et de faiblesses susceptibles d'avoir une incidence sur la sécurité d'une organisation ou d'un pays en général.

a. Principes fondamentaux de protection

Une fois les atouts identifiés et leurs vulnérabilités évaluées, la protection comporte quatre étapes : défense/prévention, détection, réaction et dissuasion.

- La prévention consiste à prendre des mesures pour prévenir l'attaque.
- La détection nécessite l'élaboration et la mise en place de mécanismes appropriés pour identifier rapidement l'apparition d'un événement de sécurité.
- L'intervention signifie développer et mettre en œuvre les actions appropriées nécessaires pour contrecarrer et éventuellement contenir un événement de sécurité détecté.
- La dissuasion augmente et signale les coûts de piratage d'un système, empêchant les intrus potentiels même d'essayer en raison de la très faible probabilité de franchir le système par rapport aux coûts très élevés de le faire.

b. Le principe de privilège minimal

Le principe de privilège minimal exige qu'un utilisateur particulier n'ait pas plus de privilèges que nécessaires pour exécuter ses fonctions ou son travail pour effectuer des actions ou accéder à l'information. En outre, le principe stipule également que les utilisateurs utilisent le plus bas niveau de leurs privilèges chaque fois que possible.

c. Le principe de défense en profondeur

Aucun contrôle de sécurité ne peut protéger seul une organisation. La défense en profondeur est une approche en couches pour se protéger contre les menaces, ou pour réduire la vulnérabilité. Par exemple, les contrôles de sécurité périmétrique tels que les pare-feu, les systèmes de détection/prévention d'intrusion ou les contrôles d'accès au réseau devraient être complétés par des contrôles de sécurité de points d'extrémité tels que les systèmes anti-programmes malveillants et de détection d'intrusion au niveau de l'hôte. L'utilisation des contrôles en couches et des contrôles complémentaires augmentera l'effort qu'un attaquant doit faire pour attaquer avec succès le système, ce qui en fait un moyen de dissuasion.