THE AfricaCERT Project

presented for public comment by AfNOG / AfriNIC

Secretariat: Jean Robert Hountomey

Email: project (at) africacert.org

1. Executive Summary

The Internet penetration is improving in Africa with so many submarine cables landing into the continent. Businesses in Africa are being more successful and more connected by enabling a range of services. African governments are building their infrastructure and enabling "services to citizen" solutions by putting critical infrastructure on the media. At the same time few African countries have in place teams to deal with incidents and problems that may or more probably will happen from the cyberspace. That goes from having trusted point of contacts to highly trained teams who can deal with incidents that can happen. Is the continent prepared ? Considering the degree of sophistication that cyberattacks take, Africa is potentially vulnerable to variety of contingencies which could have serious implications. For example a highly distributed attack could harm African Infrastructure on the Internet and cause severe damage.

The creation of an African Computer Emergency Response Team (AfricaCERT) as an African international team of trusted computer incident response teams devoted to cooperate to handle computer security incidents and promote incident prevention programs would provide a powerful basis to strengthen defenses and help reduce the impact of future attacks against African assets and critical infrastructure that dwell and operate on the internet. The AfricaCERT team is willing to support and encourage all the individual efforts, to empower the existing achievement, to outline the success stories, to be a forum of collaboration and to promote international cooperation within the African community but also outside of the continent.

1.1. Vision: United in promoting cyber security in Africa.

Because the African Continent is more and more connected, AfricaCERT facilitates incident response capabilities among African countries and provides capacity building, access to best practices, tools and trusted communication at the continent level.

1.2. Identity

AfricaCERT has opted for an identity system represented by its logo.

The ring symbolizes the unity of a whole continent standing together.

Gold color symbolizes the noble ambitions of AfricaCERT.

Brown and Black symbolize the roots in the African continent.

1.3. Mission Statement

AfricaCERT is the African forum of computer incident response teams who cooperatively handles computer security incidents and promotes incident prevention programs.

 a. AfricaCERT provides security incident response coordination

 - coordinates incident response activity (in Africa and with other continents)

- coordinates with other African Internet organizations

- Members create and share technical information, tools and best practices.

b. AfricaCERT promotes education efforts and human resource development

- training material development

- offer training courses

c. AfricaCERT organizes events

 - organize conference, workshop, meeting,...

- facilitate dialogue, discussion,...

1.4. Milestone

2011.6   First BoF on AfricaCERT (during AfNOG Meeting)

2011.11 AfricaCERT Workshop (during AfriNIC Meeting)

2012   Inauguration of AfricaCERT

2. Background

The African Internet community has formed over the years several entities to respond to specific needs. The first of these entities; the Africa Network Operators Group (AfNOG) was formed as a response to the need for cooperation and held its first meeting from April 30 to May 5, 2000 in Cape Town, South Africa. AfNOG is a forum for the exchange of technical information, and aims to promote discussion of implementation issues that require community cooperation through coordination and cooperation among network service providers to ensure the stability of service to end users.

The Africa Network Operators Group has empowered several sisters organization at the continental level on dedicated issues. Since the beginning Prof Nii Quaynor, Co Convenor of AfNOG has made clear the recognition from the African community of the need to deliver their services in a secure environment. The African Network Operators has tackled several issues from securing the core, delivering secure services to providing awareness raising and capacity building for all the stakeholders and are now moving forward by enabling Computer Emergency Response Teams among different countries.

2.1. Awareness raising

The African community has raised awareness and capacity building issues at different AfNOG conferences.

AfNOG-1 meeting in Cape Town, South Africa from April, 30 to May 5, 2000.

Topic 1: "Denial of Service ((DOS), What they are and how to defend against them" presented by Alain Aina

Topic 2: "How not to be a spam relay" presented by Adiel Akplogan

AfNOG-4 meeting in Kampala, Uganda from June 08th to June 15, 2003.

Topic 1: "Content Security Panel" Chairperson: Sunday Folayan

Topic 2: " Web security" presented by Joel Jaeggli

Topic 3: "SPAM" presented by Noah Sematimba

Topic 4: Network and Services Security" presented by Jean Jacques B

AfNOG-5 / AfriNIC-1 meetings in Dakar, Senegal from May 16th to May 21, 2004.

Topic: "We all need CSIRTs in Africa" presented by David Crochemore - Member of the FIRST

Steering Committee

AfNOG-9 / AfriNIC-8 meetings in Rabat, Morocco from May 24 to June 6, 2008.

Topic: "Why DNS-SEC?" presented by Olaf Kolkman

Topic:"Introducing CSIRT" presented by Yurie Ito (JPCERT)

AfNOG-10 / AfriNIC-10 meetings in Cairo, Egypt from May 10 to May 22, 2009.

Topic:"CSIRTs and FIRST Activities" presented by Chris Gibson

Topic: "Network Level Spam Defenses" presented by Nick Feamster

AfNOG-11 / AfriNIC-12 meetings in Kigali, Rwanda from 23 May to 4 June, 2010

Topic: "Is privacy on the Internet still possible" presented by Jean Robert Hountomey

AfNOG-12 / AfriNIC-14 meetings in Dar Es Salaam, Tanzania from 30th May to 10 June 2011.

Confronting the Threat Profile for Africa - Security for $1-day presented by Cecil Goldstein.

Understanding and meeting the new challenges of cybersecurity presented by Prof Benoit Morel.

2.2. Tutorials

The African community has hosted several tutorials around information systems security to raise awareness on the need to have incident handling capabilities in the continent.

AfNOG-6 / AfriNIC-2 in Maputo, Mozambique from April 17 to April 22, 2005.

Topic: A half day workshop done by Liliana Velásquez Solha (CAIS/RNP) with the TRANSITS materials - Training of Network Security Incident Teams Staff - operational and organizational modules as the basis. [2]

AfNOG-9 / AfriNIC-8 Meetings in Rabat, Morocco from May 24 to June 6, 2008

Topic 1: "Setting up CSIRTs in the Africa Region" by Yurie Ito JPCERT/Coordination Center. (Half Day)

Topic 2: "DNSSEC: Why, how, why now?" by Olaf Kolkman and Alain Aina (Half Day)

AfNOG-11 / AfriNIC-12: Meetings in Kigali, Rwanda from May 23 to June 4 2010

Topic 3: "DNS SEC Tutorials" by Alain Aina

AfriNIC-13 meeting in Johannesburg, South Africa from Nov 20 to Nov 26 2010

Tutorial: Understanding and Identifying network attacks By Cecil Goldstein - Team Cymru

[2] Final Report - TRANSITS - http:// www.ist-transits.org/d12_transits.pdf

AfNOG-12 / AfriNIC-14 meetings in Dar Es Salaam, Tanzania from May 29 to June 10, 2011

Two days training on Network Forensics & Malware Analysis By Cecil Goldstein Team Cymru

2.3. Workshop

2.3.1. Af-Cyersec2008 - Cybersecurity event in Cote d'Ivoire from Nov 18 to 20, 2008.[3]

An international conference on cybersecurity organized by Didier Kla was hosted in by the governement of Cote d'Ivoire in Yamoussoukro, on the theme: "Building a digital space of trust in Africa". Organized with the support of Francophonie, the conference raised the need for collaboration between African countries in cybersecurity.

2.3.2. Cybersecurity Workshop in Kigali – Rwanda on May 30, 2011

A Cyber Security Workshop was organized jointly with AfNOG/AfriNIC/AfREN.[4]

2.4. Secure Registry Operation by AfTLD.

The African Top Level Domains Organization (AfTLD), the association of African country code top level domains (ccTLDs)code top level domains (ccTLDs), held at its 5th Annual African ccTLD Event in Ghana from April 17 to 23 2011 hosted by the National Information Technology Agency (NITA) of Ghana with the support of the Ministry of Communications Ghana and other local sponsors a five five-day technical training workshop on Secure Registry Operation Course (SROC) , an initiative of ICANN, ISOC and NSRC.[5]

[3]. Af-Cyersec2008 (http://www.afcybersec.org/fr/)

[4]. Cyber Security Workshop (http://africaasia.net/2010-5-Security.html)

[5]. AfTLD Technical WG report (www.aftld.org/tz2009/docs/presentations/Day5/Technical_WG_Report.pdf)

2.5. The AfriNIC Government Working Group (AfGWG) - Law Enforcement initiative.

The African Network Information Center (AfriNIC) has formed the AfriNIC - Government Working Group (AfGWG) & Law Enforcement collaboration framework to strengthen the collaboration between AfriNIC and African Governments and Regulators; to create a dynamic framework to address (i) General Internet Governance challenges faced within the region (ii) Specifically those internet governance issues related to Internet Number Resources. AfGWG had its first meeting in Mauritius from January 25 - 26 2010. The AfGWG meeting has discussed several challenges with Internet-related crimes; discuss about steps being taken by law enforcement agencies, exchange ideas about the formation of a Internet Law Enforcement Working Group that will promote security by facilitating global cooperation and coordination. Presentations at AfGWG meetings tackled several issues:

- CERT Update and Reports

- Role of CERT for government

- FBI Cyber Crime Initiatives

- USDOJ Cyber Security

- European Convention on Cybercrime

- Cyber Security in Africa – Law Enforcement (Initiatives, Challenges, Accomplishments)

- Protecting Critical Infrastructure

- AfricaCERT report

2.6. Cert training courses

AfNOG and AfriNIC has funded Cert dedicated courses through the Africa Asia Forum on Network Research & Engineering under the coordination of Prof Kilman Chon, with the support of the Government of Japan and the JPCERT. The Team from Japan is coordinated by Prof Suguru Yamagushi. [6]

2.6.1. CERT Introduction(CERT Training Course for Manager and Policy Maker)

- May 31, 2010 at AfNOG-11 / AfriNIC-12 meetings in Kigali, Rwanda

- Nov 23, 2010 at AfriNIC AfriNIC-13 meeting in Johannesburg, South Africa

- May 30, 2011 at AfNOG-12 / AfriNIC-14 meetings in Dar Es Salaam, Tanzania

2.6.2. CERT Training Course for Technical Staff

- Nov 23, 2010 at AfriNIC AfriNIC-13 meeting in Johannesburg, South Africa

- May 31 to June 02, 2011 at AfNOG-12 / AfriNIC-14 meetings in Dar Es Salaam, Tanzania

2.6.3. Advanced CERT Training Course on Web Server Security Management

- June 3 to June 4 , 2011 at AfNOG-12 / AfriNIC-14 meetings in Dar Es Salaam, Tanzania.

[6] . Africa Asia Forum on Network Research & Engineering (http://africaasia.net)

3. The Premises of AfricaCERT

- Declaration of the AfricaCERT project

The AfNOG / AfriNIC Community has organized the first Security Workshop on May 30 2010 in Kigali, Rwanda. At the workshop the representatives of the countries presents updated the community on their local ongoing initiatives. The major outcome was the declaration of Kigali to create a Computer Emergency Response Team for the Africa Region.- Dar Es Salaam Bof.

On June 5th, 2011; African delegates present in Dar Es Salaam have organized a BOF on the creation of a Computer Emergency Response team for the African Continent. The Bof was chaired by Adiel Akplogan, CEO of AfriNIC.

Because we use the internet to conducted our day to day activities, the issue of cyber security is more and more a concern to people from different sectors: government, education, industry, banks, etc...

The community has recognized that AfNOG / AfriNIC as well as sisters organization like them has been promoting security in the cyberspace. To move further, AfNOG/AfriNIC have provided the room, starting at Kigali for the emergence of an African organization around cybersecurity by introducing training of trainers courses for manager and policy makers as well as technical staff. A direct result was the declaration at Kigali of the need to create a Computer Emergency Response team at the continent level.

The need to move forward has been clearly pointed by the delegates. The African organization

will leverage all the previous and existing efforts, which can lead to the creation of CERTs in different countries. The proposed name of the organization is AfricaCERT. As pointed during the meeting, countries are in different stages and the goal is not to tell Governments what to do but to build a central repository of experiences, a group of trusted contacted and a group of highly skilled professionals who can drive local initiatives in their community what Prof Nii Quaynor, called the African Leadership. One of the primary task of this team will be to get countries ready and to figure out what to do to see countries emerge.

The commitment has been strong to support LEA and Governments in their fight against cybercrime, by providing assistance in all the areas they need but also training.

On the training aspect, The help of our friends from Asia; the JPCERT team leaded by Prof Suguru Yamaguchi and coordinated by Prof Kilnam Chon is highly appreciated.

Funding and support issues have been raised. AfriNIC has expressed its will to help (what the organization is already doing). It is also expected to see more people involved in the process after the incorporation of the company and the presentation to the community.

Different steps have been identified to move forward and an interim committee has been setup to think about the following issues: incorporation, bylaws, stakeholders. The committee is expected to produce a report at the AfNOG/AfriNIC meeting in Gambia.

In the midtime, at the AfriNIC meeting in Cameroon, AfricaCERT is expected to have its first event after the "CERT training for Managers and Policy makers." The coordination team will at

the same time start working on the business plan as well as making sure that the community and government are aware of such an initiative and are willing to provide support.

The project was presented to the Government and LEA working group meeting on June 10, 2011.

Project Leadership

Adiel A. Aklplogan

Nii N. Quaynor

Pierre Dandjinou

Jean Robert Hountomey

Advisory Committee

Alain Aina

Anne Rachel Inne

Pierre Ouedraogo

Kilman Chon,

Suguru Yamaguchi

About AfNOG

AfNOG (See <http://www.afnog.org/>) is a forum for cooperation and the exchange of technical information between operators of Internet-connected networks in Africa. AfNOG has organized an event like this one every year since 2000.

About AfriNIC

AfriNIC (See <http://www.afrinic.net/>) is a Regional Internet Registry (RIR), responsible for Internet Number resources Mangement in the Africa region. AfriNIC organizes two Public Policy meetings every year (see < http://www.afrinic.net/meeting/>).

About AfGWG

The African Government Working Group (see - http://meeting.afrinic.net/afgwg/) was set up at the initiative of AfriNIC "with the aim of strengthening the collaboration between AfriNIC and African Governments and Regulators in order to create a dynamic framework to address general Internet Governance challenges faced within the region and specifically those related to Internet Number Resources.

About AfTLD

AfTLD – www.aftld.org - was established in 2002 to act as a focal point for African Country Code Top Level Domain (ccTLD) managers in coordinating, formulating, developing and presenting a unified approach to issues related to the Domain Name System. AfTLD also

presents a forum for sharing ideas between the regions Internet community with an aim of promoting the utilization of national country's Top Level Domains.

About AAF

 AAF – www.africaasia.net - is the Africa Asia Forum on Network Research & Engineering.