GFCE Triple-I Workshop @AIS2018, 7 May 2018, Dakar

Summary

On Monday 7 May, during the Africa Internet Summit 2018, AfricaCERT hosted the GFCE Triple-I Internet Infrastructure Security Day. The Dutch Ministry of Economic Affairs and Climate as a member of the Global Forum on Cyber Expertise coordinated this initiative to look for ways forward towards more trusted use of Internet and email in the African region. Participants in this workshop were regional Internet stakeholder groups, including the government, business and technical community who all contributed in finding solutions to strengthen an open end-to-end Internet.

The workshop was opened by Mr. Nii Quaynor. Nii played an important role in the introduction and development of the Internet throughout Africa. He also established some of Africa's first Internet connections and was involved in setting up key organizations known as African Organizations for Internet Governance (AF*), including the African Network Operators Group (AfNOG), the Regional Registry for Internet Number Resources serving the African Internet Community (AfriNIC). With regards to this workshop he emphasized the importance of continued joint action across the African continent – and he encouraged the participants to work together on development and implementation of new actions to improve trust in the Internet in the region.

Block I: Better Use of Today's Open Internet Standards

Alain Aina (WACREN) and Olaf Kolkman (ISOC) moderated and discussed the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, DMARC, DKIM, SPF and IPv6, in interaction with the participants. A joint take-away is that much can be gained by implementing state-of-the-art Open Internet Standards, already available today.

Block II: Inspiration from Good Practice Actions

During this block several good practices on how to mitigate Internet- and email vulnerabilities were discussed.

Ms. Octavia de Weerdt from NBIP.NL explained that the NBIP offers on-demand DDoS security for both small Internet providers, and medium-sized and larger

businesses, as well as for VoIP providers that helps to put up a powerful resistance against DDoS attacks. This service has been set up at the initiative af a number of ISPs working together, and is now provided by the non-profit NBIP organization against a fee. Next o creating joint capacity to assist individual organization with "sinking" attacks, NIBP also builds up knowledge on how to deal with this up and beyond what the individual participants could do, thanks to the collaboration.

Marcus Adomey from AfricaCERT stressed the importance of Incident response since more devices are put online and more incidents are received. For incident response to scale up it is important that a coordinated approach is used that is built upon trust rather than competition. There is also need for greater collaboration among Computer Security Incident Response Teams (CSIRTS). He called for other CSIRTS to be set up and to join AfricaCERT for this purpose.

Michuki Mwangi from ISOC talked about Mutually Agreed Norms of Routing Security (MANRS) and the need for a culture of collective responsibility whereby best practices on routing security are shared among the stakeholders. For consumers it is wise to choose a reliable router supplier that agrees to the MANRS Principles. Aim is to involve more ISPs in the region as to enhance reliability of the routing.

Kevin G. Chege from ISOC spoke on the growing impact of the Internet of Things on the Internet. It is important that manufactures, suppliers and users all play a role to ensure adequate security in devices, and in systems consisting of multiple IoT devices working together to deliver specific services. ISOC recommends the adoption the OTA IoT Trust Framework as a guideline for safer IoT implementation.

Jesse Sowell stressed that the Transnational Anti-Abuse Working Group Development (M3AAWG) has much to offer in terms of good practice experiences in detecting and fighting abuse on the Internet. Currently, the core of activities is in the USA and western Europe, and Jesse called for volunteering ambassadors from other regions to help implement M3AAWG, locally, as well – both for the benefit of that specific region and to further grow the "global insights".

Yurie Ito explained that Cybergreen undertakes research on a country's Cyber Ecosystem. It also provides recommendations to improve cyber health by informing Computer Security Incident Response Teams (CSIRT) on the most important risks and helps them to adapt the right security measures. It does so by providing data based on measurements in the routing networks, and in that way Cybergreen is able to show comparable data that provide an excellent sedgway into action with a focus on those points that are recognized as "most vulnearable".

GFCE TRIPLE - I

Block III: Planning for a more Trusted Internet

Following the introductions about open internet standards that can help enhance justified trust in use of the Internet and email (Block I) and the examples of good practice provided (Block II) the brainstorm session focused on answering the question:

> *"What to do, together, to improve justified trust in using the Internet and email in the region"*

Using the Open Access method for organizing this slot, three main topics were selected and consequently discussed amongst delegates:

(1) MANRS (proposed by Michuki Mwangi)

Here, it was emphasized that there is a need to find ways to link Internet security incidents to MANRS. Next to national CERTS and IXs promoting this, local ambassadors that monitor and inform local operators of incidents would be a great addition. Governments can consider providing guidelines (and possibly regulations) to encourage adoption of Best Current Practices. Users and enterprises should require adoption of MANRS from their service providers. Sharing best practices (that will continue to evolve), including on regulatory recommendations and routine security should become ongoing practice.

Actions concluded by the group on promoting MANRS are:

- Setting up of MANRS training: This should be done by MANRS
- Setting up a MANRS mailing list: This should be done by MANRS
- Regulatory incentives: ISOC will (continue to) inform and stimulate governments for action in this.

(2) IoT (proposed by Kevin Chege)

The number of IoT devices continues to surge with estimates indicating that the devices will number 2.5 times the population of earth by the year 2020. For these devices to be trusted and used properly, users need to be educated early on what IoT devices are as well as on the risks and opportunities IoT devices present. Manufacturers need to ensure that IoT devices are secure by design from the beginning, following broadly recognized Principles and Guidelines on IoT design such as the OTA IoT Trust Framework Guidelines.

When looking at smart city applications, it becomes clear that standards for interoperability and security need to be set, and that privacy aspects of data collection, storage and sharing need to be considered. In order to ensure compliance, there may be a role for regulation (local or national), up and beyond broadly recognized principles and guidelines.

Actions concluded by the group on enhancing sustainability of IoT:

- Awareness and education on IoT: There is a role for educators to train developers on IoT design and security implementation around IoT .

- Creating a legal framework and setting up Standards: There is a role for Regulators, users, IoT manufacturers and consumer standards bodies to collaborate together to come up with regulation and policies on IoT devices to protect consumers from insecure devices. This should include policies of what type of IoT devices can be allowed into a country and ensure that the devices conform to security principles and technologies as well as how the data on IoT devices should be secured
- The Open Standards Organizations (like the IETF and IEEE) will play an important role in defining the standards that ensure interoperability of the IoT devices
-

(3) M3AAWG (proposed by Jesse Sowell)

Identification of Abuse and measures to fight abuse have been developed over the years, mainly in other areas than Africa. The proposal from Jesse to get an active chapter going in Africa was well received. In order to do this, participants agreed it would be useful to keep the dialogue going, and focus on identification of specific regional issues areas; champions to step forward in supporting this; and set up an exchange of threat warnings with the main M3AAWG center.

Next to this, participants agreed to contribute to the build-up of local capacity and further engage with M3AAWG.

Conclusions

Many of the good practices presented on subjects like IoT security, MANRS, M3AAWG, Cybergreen, CERT activities and the NIBP approach to fight DDoS attacks were "new" for at least a good part of the over 50 participants from the region that participated during the day. During this day delegates learned how much global resources are already there to help in taking local action, and expressed the intent to further local implementation of global good practices.

This was the first of a series of Triple I Workshops that will be organised in different regions of the world. Big thanks to all contributors to this workshop – co-organisers, presenters and participants. The results and outcomes will all be shared on the Triple-I event website.

For more information: maarten@gnksconsult.com .