AfricaCERT Workshop on CSIRTs in NRENs

AfricaCERT
United in promoting cyber security in Africa

3rd WACREN regional workshop
Ouagadougou, Burkina Faso
10 – 15 October 2016

Perpetus Jacques Houngbo
Head of Projects

Contents

- Introduction:
  - Participant introductions, backgrounds and expectations
  - Overview of common Internet security threats
  - Complexity of information security problems
  - CSIRTs, global response to globalization of threats
- CSIRTs in NRENs
  - CSIRT Functions, Services and Benefits
  - Steps for creating NREN CSIRTs
  - Activity: Role play - CSIRT development working groups
  - CSIRT presentations from group representatives
  - Role for CSIRTs in Trust and Identity Management
- Wrap up and next steps
  - Critical success factors
  - Law enforcement
  - Practical information
  - Evaluation
- Conclusion

Objectives

- Better understanding of Internet threats and the need for an effective way to balance academic research and educational missions with the need for computer security
- Answers to questions about network situational awareness and incident handling in campus networks and the relationship with NREN and national CSIRTs
- Design and implementation plans for campus and NREN security teams
- Connections among Research and Education network security communities towards establishment of a secure communication platform

We are AfricaCERT …

- Vision
- One Continent, One Vision, One Team United in Promoting Cybersecurity in Africa.

- Mission
- The African forum of computer incident response teams, aims to propose solutions to Challenges for Internet Health in Af* Internet Ecosystem.

AfricaCERT

United in promoting cyber security in Africa

AfricaCERT and FIRST representatives greeting Deputy Minister of Communications of Ghana at the AfricaCERT and FIRST Regional Symposium, Accra (Ghana) September, 2015

Global Threat Landscape, Africa Threat Landscape

- A pile of reports ...
  - Hewlett Packard Enterprise, Cyber Risk Report 2016
  - NYA International, Cyber Extortion Risk Report, October 2015
  - Ponemon Institute LLC, 2015 Global Megatrends in Cybersecurity
  - PricewaterhouseCoopers LLP, Key findings from The Global State of Information Security® Survey 2016
  - McAfee, McAfee Labs Threats Report August 2015
  - Verizon, 2015 Data Breach Investigations
  - Symantec, 2015 Internet Security Threat
  - Arbor Networks, Worldwide Infrastructure Security Report
  - Etc.

and an avalanche of bad news!

- Storm of not so good news:
  - Data breaches increase in number, size and impact
  - Sophisticated data breaches go beyond just credit card numbers
  - Most attackers are still driven primarily by financial interests, but it’s a relatively good bet that some amount of stolen data are not meant for the hands of criminal gangs or identity thieves
  - Vulnerability market continue to evolve as more and more vendors announce their own programs to incentivize research
  - As more and more data migrates online, the scenario of data breaches is likely to repeat itself unless data protections—namely privacy safeguards—are held firmly in place
  - Despite the advancement of defensive strategies, malware cont pervasive piece of life online
  - The threat of cyber-attack is unlikely to go away.

Security breaches on [African] campus?

- May 2016: University of Calgary
  - Victim of ransomware attacks, the school paid CND$20,000 in Bitcoin to get rid of the malware. Despite paying the fee, not all systems are back online, as the provided decryption keys do not restore all systems automatically.
- June 2015: University of Cape Coast (UCC)
  - There have been instances where people's mobile phones, laptops and handbags have been snatched from them by criminal elements who mingle with students, the UCC has installed Closed Circuit Television cameras at vantage points on campus to monitor and check criminal activities
- March 2015: Auburn University
  - Student information — including Social Security numbers — was leaked from a server in the university’s business school
- March 2015: University of Chicago
  - Social Security numbers, employee IDs, names and the e-mail and residential addresses of students (both former and current), employees and contractors in the Department of Medicine were exposed

But …

- Defenders now look to secure their enterprise
- Vulnerability white market has a tremendous positive effect in securing the landscape by bringing researchers and vendors together
- Creating better protection solutions becomes harder and takes more time
- Regulations and legislation are evolving in ways to affect the nature of disclosure
- Decoupling security and privacy is more and more matter of debate
- World instability has also brought the topic of surveillance and encryption into the minds of many
- **<u>Through thoughtful planning, defenders can continue to increase both the physical and intellectual price an attacker must pay to successfully exploit an enterprise</u>**

So, what to do ? (Complexity of information security problems)

- Objective is
  - thoughtful planning
  - increase both the <u>physical</u> and <u>intellectual</u> price an attacker must pay to successfully exploit an enterprise
- This encompasses many activities that must focus on five work areas:
  - Legal Measures

    Criminal legislation / Regulation and compliance
  - Technical Measures (first line of defense against cyberthreats and malicious online agents)

    CERT / Standards / Certifications
  - Organizational Measures

    Policy / Roadmap for governance / Responsible agency / National benchmarking
  - Capacity Building

    Standardization development / Manpower development / Professional Certification / Agency certification
  - Cooperation

    Intra-state cooperation / Intra-agency cooperation / Public-Private Partnerships / International cooperation

Needs for a global response 1 / 4

- Crime: an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. http://www.merriam-webster.com/dictionary/crime
- Cybercrime is 'crime' with some sort of 'computer' or 'cyber' aspect. http://us.norton.com/cybercrime/definition.jsp
- Dealing with any crime:
  - Prevention is better than cure: education
  - Expertise for investigation on wrong doing, prosecution, trial, punishment, etc.
- Dealing with cybercrime: Key experts and personnel from diverse area (law enforcement, regulators, country focal, cybersecurity experts, etc)

Needs for a global response 2 / 4

- Number and diversity of actors involved
- Threats are coming from all directions
- Global Response Centre at local and national level, cooperation at all levels
  - Local: Top management, Staff, HR, Unions, IT staff
  - National, experts from diverse area: Economy, Politics, IT, Security, Law enforcement
- International cooperation
  - Cybercrimes easily (and usually) ignore geographical boundaries
  - The problem is global, it needs a global solution

Needs for a global response 3 / 4

- Framework for national and international cooperation
  - Legal aspects
  - Technical measures
  - Organizational structures (including policies and strategies)
  - Capacity building
- Global partnerships (unavoidable)
  - Understanding the level of vulnerability of the system at the base of the global economy and individual well-being
  - Identifying and protecting the vulnerable targets
  - Learning from other experiences

Needs for a global response 4 / 4

- The response is a Computer Security Incident Response Team (CSIRT)
  - *A service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client. http://www.cert.org/csirts/csirt_faq.html*

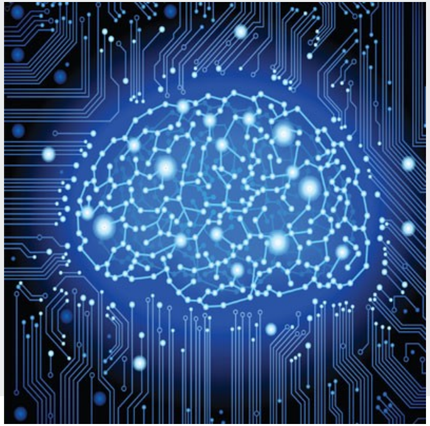
CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

CSIRT functions

- Single point of contact to report security incidents
- Assistance to the Constituency in preventing and handling computer security incidents
- Sharing information and experience with other response teams
- Collaboration with Law enforcement & Local authority bodies
- International cooperation with
  - global structure of responses, FIRST
  - inter-governmental organizations (ICPO, UNODC, IWWN, Meridian etc.)
  - regional bodies AfricaCERT, APCERT, TF-CSIRT, etc.

CSIRT benefits

- Dialogue and info sharing among public and privates
- Centralized coordination for IT security issues
- Centralized and specialized handling of and response to IT incidents: systematic respond to incidents with appropriate steps
- Expertise to support users for quick and efficient recovery from incidents, minimum loss or theft of information and disruption of services
- Learning from experience, better preparation for handling future incidents
- Expertise with legal issues, evidence handling
- Up to date with developments in security fields
- Stimulation of cooperation within constituency



CSIRT services 1 / 3

- CSIRT services defined during creation process
- CSIRT services, but also sometimes covered by “security team”
- Great care while choosing services, impact on:
  - resources
  - skills sets
  - partnerships
- Quality / Quantity
- Think big, start small and …scale fast

CSIRT services 2 / 3

- Reactive services
  - services are triggered by an event or request
  - services aim at cure of compromised system
- Proactive services
  - prepare, protect, and secure
  - reduce the number of incidents
- Security quality management services
  - improve the overall security
  - reduce the number of incidents

CSIRT services 3 / 3

- Many cross links of services
- Services offered must be tailored to the specific needs and prospective evolution of the constituency
- Services offered must be tailored to resources available: financial, organizational, human
- Dissemination of information is very important
- Prevention is better than cure

Steps for creating CSIRT

- Clarification of constituency: stakeholders and prospective clients
- Choosing the right services
- Making an analysis of the constituency and the appropriate communication channels
- Elaborating the Mission Statement
- Defining the Business Plan: Financial model, Revenue model, Organizational model, Staff, Office and furniture, Information security policy, Cooperation partners
- Promoting the Business Plan: Validation of the business case, Designing the project plan, Estimation of the set-up costs and the cost of operation
- Making the CSIRT operational: Creating workflows, Implementing CSIRT tooling
- Training the staff
- Exercising and go-live

ENISA, A step-by-step approach on how to setup a CSIRT, December 2006,
http://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide

Role play in working groups: creating CSIRTs

- Constituency
- Services
- Appropriate communication channels
- Mission Statement

Critical success factors

- Country’s commitment at the highest level
- Relevant Agency involvement supported by the highest level of the country
- Communication about the strategic value to the Country’s Cybersecurity Programme
- Design and communication of a relevant National CSIRT vision and operational plan to fit the country’s security objectives
- Implementation of CSIRT tools and processes in line with the above vision and operational plan
- Announcement of the CSIRT Operations to the country
- Periodic and systematic assessment of CSIRT activities and its effectiveness
- Periodic reviews and adjustments to the National CSIRT Development Roadmap
- Permanent improvement of network of trust with the constituency

CSIRTs and Law Enforcement Agencies (LEAs)

- Responsibilities of CSIRTs vis-a-vis law enforcement and intelligence agencies
  - Democracy
  - Security vs privacy
  - Freedom, open access vs regulation
- Cooperation
  - which information can be shared
  - how is information shared
    - common vocabulary
    - sharing mechanism for the exchange of information

Practical information

- AfricaCERT
- FIRST
- ENISA
- Minimum staffing
- CERTification-Certified Computer Security Incident Handler (CSIH)
- Equipment should have when starting
- Equipment better have later on
- Learning what other CSIRT do: http://first.org/members/teams/

Thank you !

AfricaCERT

United in promoting cyber security in Africa

Perpetus Jacques Houngbo
Head of Projects
jacques.houngbo@africacert.org