Computer Security Incident Response Team (CSIRT)

SAIGF-18
29 November 2018

Noma-Efese Mnqeta
Deputy Director: Cybersecurity Operations
Department of Telecommunications & Postal Services
Making South Africa a Global Leader in Harnessing ICTs for Socio-economic Development

1. Cyber Trends in Africa
2. RSA Cybersecurity Regulations
3. RSA CSIRT: Cybersecurity Hub
4. Conclusion
Cyber Trends in Africa

https://www.serianu.com/resources.html
Cyber Trends in Africa

**Cybersecurity Training**

64% of organisations do not train their employees at all or only do so when an incident occurs.

**Cyber Exposure Value**

83% of parents do not understand what measures to take to protect their children against cyber bullying.

https://www.serianu.com/resources.html
Cyber Trends in Africa

The cost of cyber-attacks is $3.5B annually.

Fake News has hit Africa's media streams as we increasingly see unverified and often conjured up news being circulated through various mediums.

Banking Sector is still the most targeted industry in Africa.

Most organisations' Cyber security programs are Tool Oriented.

96% Cyber security incidents either go unreported or unsolved.

97% Skill Shortage

There is a huge Cybersecurity skill shortage within the Saccos particularly for mid and senior level hires.

83% Cybersecurity Management

Manage their Cyber security in-house. This is particularly worrying considering that the skill shortage is highest in Sacco as an industry.

https://www.serianu.com/resources.html
Cyber Attack

Ransomware: I don’t WannaCry

Worldwide attack map

Key:
- Countries affected by WannaCry attack
- Countries not affected by WannaCry attack

https://www.serianu.com/resources.html
Top Cybersecurity Related Threats in RSA

Information security
- Unauthorised access to information
- Unauthorised modification of information

Abusive Content
- Spam
- Cyberbullying
- Cyber stalking
- Child Pornography
- Violence

Malicious Code
- Viruses
- Worms
- Trojans
- Spyware
- Dialler

Information Gathering
- Scanning
- Sniffing
- Phising
- Spoofing
- Pharming

Fraud
- Unauthorised use of resources
- Copyright infringement
- Masquerade

Availability
- Denial of service
- Distributed Denial of service
- Sabotage

Intrusions
- Privileged account compromise
- Unprivileged account compromise
- Application compromise

Intrusion attempts
- Exploitation of known vulnerabilities
- Login attempts
- New attack Signature

Making South Africa a Global Leader in Harnessing ICTs for Socio-economic Development
Cybersecurity Regulations in RSA

- **Policy**
  - National Cybersecurity Policy Framework (NCPF)

- **Legislation**
  - Cybercrimes and Cybersecurity Bill: Currently tabled before Parliament
  - Critical Infrastructure Bill: Out for public comment

- **Regulation**
  - Will be drafted on promulgation of the Bill
To set out an aligned and coherent approach to Cybersecurity, in March 2012, the South African government approved the National Cybersecurity Policy Framework (NCPF).

The NCPF outlines broad policy guidelines on Cybersecurity in the Republic and requires Government to develop detailed Cybersecurity policies and strategies.

Problem Statement

01 Uncoordinated and silo approach to Cybersecurity

02 Inadequate regulatory framework to support Cybersecurity

03 Lack of general public awareness about Cybersecurity

04 Inadequate capacity, skills and resources.

Objectives

Articulate overall aim and objectives of the South African Government

Centralize coordination of Cybersecurity activities;

Foster cooperation and coordination between Government, the Private Sector and Civil society

Promote international cooperation

Promote a culture of Cybersecurity

Develop requisite skills and R&D capacity

Promote compliance with appropriate technical and operational Cybersecurity standards

Making South Africa a Global Leader in Harnessing ICTs for Socio-economic Development
DTPS Mandate:

- To establish a Cybersecurity Hub to serve as a central nodal point for consultation and coordination on cybersecurity matters with stakeholder (public, private, civil society including any other interest groups etc.);
- To promote cybersecurity awareness

To report a cybersecurity incident:
- Email: incident@cybersecurityhub.gov.za
# Cybersecurity Hub Functions

## Coordination
- Sector CSIRT Establishment
- Increase collaboration through public-private partnerships
- Coordinate Responses to threats at a national level

## Information Dissemination
- Information Dissemination
- Best practice Guidelines
- Standardisation

## Awareness
- Initiate cybersecurity Awareness campaigns

## Strategic Initiatives
- Readiness Assessment
- Skills Development
Making South Africa a Global Leader in Harnessing ICTs for Socio-economic Development

**Sector CSI RT Establishment – Current Initiatives**

- SSA Cyber Response Committee
- Cybersecurity Hub
  - SECTOR-CSIRT
  - SECTOR-CSIRT
  - SECTOR-CSIRT
  - SECTOR-CSIRT
  - SECTOR-CSIRT
  - Financial Sector

**Institutions and Initiatives:**
- SABRIC: South African Banking Risk Information Centre
- ASISA: Association of Savings and Investments South Africa
- PASA: Payments Association of South Africa
- SAIA: South African Insurance Association
- FMI: Financial Markets Institutions (JSE, Reserve Bank, Bankserv, STRATE)
- Other CSIRTS
The Hub has established a War Room:

- To enable constituents and law enforcement agencies to communicate with each other in a secure manner from remote locations.
Cybersecurity Incident Response ‘War Room’

- Stakeholders
  - Imperative to be able to engage with all stakeholders when responding to Threats and Incidents at a National level

- Real Time Response
  - The ‘War Room’ will give the Hub the ability to respond in real-time and to coordinate responses to Cybersecurity threats and incidents

- Tools
  - A set of secure collaborative communications tools
  - A Business Intelligence (BI) capability that allows stakeholders to take decisions to resolve threats

- Proof of Concept
  - ‘Proof of Concept’ are being undertaken by various vendors
  - The processes and workflow that support the ‘War Room’ are being developed in conjunction with Law Enforcement Agencies and other constituents
Making South Africa a Global Leader in Harnessing ICTs for Socio-economic Development

The Cybersecurity Hub’s Incident Handling Process

- Report and Registration
- Verification and Classification
- Prioritization and Assignment
- Notification
- Resolution
- Closure
Example 1: 419 Scam- Advance Fee by Domain

The name and surname of the Minister of Telecommunications & Postal Services (MTPS) was used in an email scam with a fake email account: siyabongacwele@secretary.net

The email indicated that the recipient had been nominated to be a beneficiary of a BRICS international funding grant. However, the email indicated that in order for the recipient to receive the grant, he had to obtain a compulsory form costing him about R 5 613.46.

The recipient fortunately decided to contact the Minister’s office and reported the incident to the Cybersecurity Hub.
Example 1: Scam - Advance Fee by Domain

01

- After an initial investigation by the Cybersecurity Hub the incident was escalated to SAPS for further investigation, and to decrease the number of future victims for the same scam.

02

- The lessons learnt from all reported incidents are documented for future purposes.

03

- The lessons learnt from all reported incidents are also used to inform the public during the Cybersecurity awareness Month – October in various provinces.
Example 2: Fraudulent Purchase Orders

We have been contacted via email from the dept of human settlements to supply them with gas cylinders. They sent an “official” and advised me as to where I can purchase from. I suspect this is a scam, they will issue me a purchase order on which I then pay for the goods, etc etc...

Attached is the rft, And the quotation 4d details are below.

Cylinders 45 kg gas cylinder case Capacity: 58 liters Diameter: 375mm Height: 1250mm

Dennis at Cylinder warehouse
Example 2: Fraudulent Purchase Orders

01

• The incident was referred to SITA for resolution and engagement with relevant Government departments

02

• The lessons learnt from all reported incidents are documented for future purposes

03

• The lessons learnt from all reported incidents are also used to inform the public during the Cybersecurity awareness Month – October in various provinces.
Example 3: Jobs Scam

Good Day Colleagues,

1. Kindly note the story titled “Online jobs scam exposed” covered in The Times was discussed at Government Communication and Information System Rapid Response meeting. According to the story:
   - Fraudsters masquerading as government employment agents have conned thousands of desperate job seekers into divulging their personal details, which they use to commit crimes.
   - Since last August more than 200 000 people have subscribed to the “Government Jobs Application Page” on Facebook offering jobs in the SA Police Service, departments of home affairs, health and education, the SA Soc Sec Agency, Transnet and the Treasury, among others.
   - Desperate job seekers have been posting their personal details on the bogus page and sending their CVs to the fraudulent e-mail address provided on the page.

Recommendation:
was therefore, recommended that the GCIS social media unit to report the alleged “Government Jobs Application Page”, and look at the possibilities of blocking the page.

our reason in this regard would be highly appreciated.

Deputy Director:
Government Communication and Information System
Tshedimoseto House
1035 Frances Baard & Festival Street
Hatfield, Pretoria
Call:
Tel:
Email:
Website: www.gcis.gov.za
Example 3: Jobs Scam

01

- The incident was referred to SITA and relevant Government departments for resolution

02

- The lessons learnt from all reported incidents are documented for future purposes

03

- The lessons learnt from all reported incidents are also used to inform the public during the Cybersecurity awareness Month – October in various provinces.
Cybersecurity incidents reported at Hub

- Identity theft
- Phishing
- SMiShing
- Credit card fraud
- Lost and stolen credit card fraud
- Card not present fraud
- Account takeover card fraud
- Cheque fraud
Conclusion

To report an incident:

- Visit: https://www.cybersecurityhub.gov.za
- Email: incident@cybersecurityhub.gov.za
Thank You!