Threats, Attacks and Countermeasure

Introduced to: APTLD 69, Auckland

Yousef M. Sarairah

Director of Information Security and Network Incidents Directorate
Contents:

• NITC Overview
• NITC Services
• NITC – Information Security and Network Incidents Directorate
• Security Roles and Responsibilities
• Types of Attacks
• Security Controls and Measures
• Challenges
Overview:

NITC is the government technical arm for utilizing the national IT resources of the public sector and maximize its contribution to economic growth and welfare of Jordan.
National Information Technology Center

Team Certifications

- CISSP
- PMP
- PMI
- ITIL
- Microsoft Certified
- CCNP Security
- CCNP
- CEH Technology Specialist
- ISO 27001 Certified
- EMC² Certified
- Certified for IBM WebSphere software
- ISTQB International Software Testing Qualifications Board
- EC-Council Disaster Recovery Professional
- Fundamentals in Computer Forensics
NITC - Services

- Internet Service Provider for the Government
- e-Gov Operations Center: In charge of running, maintaining and administration of e-Gov Services such as:
  - Secure connectivity between Government entities through Secure Government Network (SGN)
  - Microsoft Services (Active Directory Root Domain, Exchange Server, DNS)
  - Jordan Portal and Payment Gateway
  - Enterprise Service Bus
  - Public Key Infrastructure “will be lunched in 2015”
Registry and Registrar for domain names under .jo and الاردن.

- We have 4744 domain names registered under .jo, and 142 domain names under الاردن.
- For more updated statistical information you can visit the following links:

  https://www.idn.jo/statistics.aspx
National Information Technology Center

NITC – Services

- Hosting Government Websites
- Data Center Collocation Service
- Security Assessment and policy compliance for entities
National Information Technology Center

Information Security and Network Incidents Directorate

- Network Security
- Information Security
- Researches and Awareness
- Incident Response Handling - CIRT
Roles and Responsibilities

- Establish Security Operations Center “SOC” which will provide full visibility and complete controls for ingress and egress traffic.
Current Phase

- Rely on legacy security appliances and open source tools to have visibility on the traffic and perform manual reports and analysis
- Upgrade the Network to add multi-layers of security and to Jump to Next Generation Security Solution
- To have a SIEM solution which can collect the logs from different appliances which will lead to have a full visibility, analysis and reporting for the whole traffic
Roles and Responsibilities

- Establish JOCIRT, which will be a focal point for Government Security Incidents, and will provide the following services:
  
  - Reactive Services: including Alerts and Warnings, Incident Handling, Attacks Mitigation, Service Recovery
  
JOCIRT Implementation Plan

- Legal framework
- Dedicated Team
- Training
- Tools and Software
- JOCIRT Website
- Promoting JOCIRT
- Extend the service to be available for Citizens and Enterprises
- Coordinate with other national CIRT
- Coordinate with international CIRT and organizations
- Secure Quality Management Services (Risk Analysis, Consultation, DR Planning)

Documentations: NIACSS, JOCIRT
Announcements, Alerts and Warning
Log Analysis
Incident Handling
Vulnerability Assessment

Current Phase
Roles and Responsibilities

- **Security Awareness**
  - Conduct Awareness Sessions to Government Employees
  - Create Broachers, Flyers and Guidance for awareness
  - Send hints, information and tips through e-mails, SMS
  - Onsite visit to perform surface security assessments
  - Conduct a professional training programs for IT staff
Type of Attacks

- Attacks are classified into three categories:
  - Internal Attacks
  - External Attacks
  - Unknown
Type of Attacks

1. Internal Attacks:

   - **Malware Attacks**: due to the careless of some employees of security rules, which lead them to download malicious contents or open infected email attachment or using infected USB drive that make their PCs as a dangerous backdoor.

   - **Data Leakage**: Many of end users used weak passwords that can be easily guessing which lead to get access to their machines and steal information.
Type of Attacks

2. External Attacks:

- **DDOS Attacks**: Government infrastructure exposed to two types:
  - Volumetric Attacks: which lead to fill the main links that cause interruption for the whole services
  - Services Attacks: which targeted specific system and exhaust its resources to be unavailable for a period of time

- **Applications attacks**: Since NITC is hosting many government applications, these applications exposed to different type of attacks (Injection, XSS, Tampering, Brute force, Defacements, Data Extraction). The most targeted attacks are (Web Servers, DB and DNS).
Type of Attacks

3. Unknown Attacks:

Since there is no any figures or any techniques to discover zero-day attacks / unknown attacks, they considered the most dangerous attacks.
Security Control and Measures

- Information Security Policy:
  - National Information Security Policy
  - NITC / IT Operations Security Policy

- Physical Security:
  - Tier-3 Data Center Design with the following measures:
    - Multi-layer Of Security to access the data center (4 Access Layers)
    - Isolated area for Public Key Infrastructure Project (PKI)
    - Surveillance system to monitor and record motions
    - Fire Fighting System
    - Suitable HVAC system
    - Redundant Power Sources (Electricity Co., UPS, Diesel Generators)
Security Control and Measures

Network Security:
- Access to end users’ network is only allowed through wired connectivity, security parameter are applied such as port security, VLANs
- Data Center network is separated to security zones (Internet, DMZ and Backbone) by dual firewall architecture
- Access to the appliances through secure protocols such as SSH
- The connectivity between entities are secured through Secure Government Network which is a fiber based network owned by the Government
- Logs from security appliance are reviewed periodically
- Internet provided by different vendors from different routes
- There is a plan to replace the legacy appliances to intelligent appliances and deploying layers approach (NGFW, NGIPS and Web Applications FW) to provide maximum protection and implement defend in depth strategy
Security Control and Measures

- Business Continuity and Security Operations
  - Backup solution are available and take backup for all critical information
  - Most of the critical component in the network are redundant.
  - Security team respond to many Government Security Incidents.
  - Vulnerability assessment conducted periodically.
  - There is a plan to have a DR in another location.
Challenges

1) Budget Limitation
2) Since SGN is connected as a chain, so it affected by its weakest link
3) Network Full Visibility
4) Application Controls
5) DDOS Protection
6) Policy Enforcement
7) Common Framework for the whole Government.
8) Resources Turnover
Thank you

Yousef M. Sarairah
Director of Information Security and Network Incidents Directorate