Security challenges within an Information System Directorate

Works of the RWG’s 5th meeting on Computer Development
Security challenges within an Information System Directorate

Direction Générale des Douanes
Direction des Systèmes Informatiques Douaniers

Modou MBOW

Responsable du Pôle Sécurité des systèmes d’information
Spécialiste en cybersécurité

ISO 27005 LRM®, ISO 27 001 LI®

Bloc des Madeleines, Boulevard de la République x Avenue André Peytavin - Dakar

(+221) 77 333 27 47
mmbow@douanes.sn
table of content

- CONTEXT
- VULNERABILITIES IS
- THREAT VECTORS
- HACKERS PROFILES
- CYBERATTACKS EXAMPLE
- CYBERSECURITY GOUVERNANCE
Context (1/2)

- Strong IT dependency
- Partnership outreach
- Digitalization
- Protection of the economy
- Contribution to the State budget
- Trade security
- Business facilitation
Context (2/2)

**COMPLIANCE**

**RESPECT OF INTERNATIONAL AGREEMENTS AND TREATIES**

Legislation (Customs Code, cyber criminality, personal data protection, Code of Telecoms, e-transactions, etc)

Standards (ISO 270XX, 900X, PCI-DSS, SANS, OWASP, NIST, CC, Bale II-III)
### Technical Vulnerabilities
- Contremesures non adaptés aux menaces
- Obsolescence des technologies utilisées
- défaut ou mauvaise configuration
- Défaut Conceptuel
- Etc. cf base vuln Mehari, Ebios, 27005

### Organizational Vulnerabilities
- Lack of procedure (PSSI, GIS, audit, etc )
- Lack of task separation
- Lack of rôle definition and responsabilities
- No organization of the security
- cf base vulnérabilité Mehari vulnerabilities database, Ebios, 27005

### Human ressources Vulnerabilities
- Lack of human ressources of unqualified human ressources
- Lack of staff awareness on cybersecurity
- Misunderstanding of procedures
- Etc.cf Mehari vulnerabilities database, Ebios, 27005
**Threat vectors (1/2)**

<table>
<thead>
<tr>
<th>SOCIAL ENGINEERING</th>
<th>• The art to persuade someone to give away a confidential information une personne de révéler une information confidentielle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Networks</td>
<td>• Social Networks can contribute and facilitate the loss of control on strategic information</td>
</tr>
</tbody>
</table>
| PHISHING            | • Mail  
  • Links  
  • Attachments |
| WEB APPLICATION     | • Injection: remote code execution  
  • Cross-Site Scripting: attacks on the client’s side  
  • Violation de Gestion d’Authentification et de Session: authorisation and authentification |
| REMOVABLE DRIVES    | • USB,  
  • keyboard,  
  • CD, etc |
| Shadow IT           | • Technology implementation (applications, services, storage function and information sharing) within collaborators without the need of the CIO |
| Physical intrusion  | • The hacker accesses the location of its victim so he directly connects. |
### Threat vectors 2/2

#### Who's behind the breaches?

- **73%** perpetrated by outsiders
- **28%** involved internal actors
- **2%** involved partners
- **2%** featured multiple parties
- **50%** of breaches were carried out by organized criminal groups
- **12%** of breaches involved actors identified as nation-state or state-affiliated

#### What tactics are utilized?

- **48%** of breaches featured hacking
- **30%** included malware
- **17%** of breaches had errors as causal events
- **17%** were social attacks
- **12%** involved privilege misuse
- **11%** of breaches involved physical actions
# Hacker Profiles 1/2

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Motivations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expert commissioned</td>
<td>Financial, Sabotage</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Ideology</td>
</tr>
<tr>
<td>Cyber-soldiers</td>
<td>State interests</td>
</tr>
<tr>
<td>Malicious user</td>
<td>Financial</td>
</tr>
<tr>
<td>Malicious staff</td>
<td>None (nuisance by mistake), Sabotage, Financial</td>
</tr>
<tr>
<td>Furniture Provider</td>
<td>Financial</td>
</tr>
<tr>
<td>Service provider</td>
<td>Financial</td>
</tr>
<tr>
<td>partners</td>
<td>Espionnage</td>
</tr>
<tr>
<td>Cybercriminals</td>
<td>Renommée, Financières</td>
</tr>
</tbody>
</table>
**Hackers Profiles 2/2**

**Figure 1.** Threat actors within breaches over time

**Figure 2.** Threat actor motives within breaches over time
## Examples of cyber-attacks in the international transit sector

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Military Sealift Command</strong></td>
<td>The attack targeted a sailing shuttle of the Military Sealift Command: many systems would have been compromised by the Chinese army according to a report from the American Senate.</td>
</tr>
<tr>
<td><strong>Anvers’ Port</strong></td>
<td>The attack was detected in June 2011 and was commissioned by a drug squad trying to high-jack containers and to circulate drug coming from Latin America by stealing agents’ passcodes.</td>
</tr>
<tr>
<td><strong>IRISL (Islamic Republic of Iran Shipping Lines)</strong></td>
<td>The attack occurred in August 2011 and all the date the company had on its cargos were deleted. The commissioner remains unknown.</td>
</tr>
<tr>
<td><strong>MAERSK</strong></td>
<td>The attack was detected by the end of June 2017 and was done by a group of hackers. MAERSK lost nearly 300 million dollars because of this attack.</td>
</tr>
</tbody>
</table>
Cybersecurity Governance (1/2)

• Engagement from the Top Management
• Organization (rôles and responsibility, institutions)
• Ressources
• Tools
## Cybersecurity Governance (2/2)

### Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

### Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

### Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

[cisecurity.org/controls](http://cisecurity.org/controls)
Thank you - Jerejef