MXCuBE CyberSecurity Survey

Comparison and Summary

Purpose

- **Start discussion** intra/inter-facilities on cybersecurity
- Sharing insights on security strategies, tools, and experiences
- Identify common and divergent solutions
- Identify any gaps or weaknesses in current practices

Remote access

- **Methods**:
  - Remote desktop
    - VPN and clients sometimes required
    - Tools: NoMachine, FastX, TeamViewer
  - Proxies
  - Direct
- **Time fencing**:
  - Almost all the facilities implement time-limited user access policies
  - Applied to VPN, remote desktop or web application

Cyber protection

- **DNS**:
  DNS firewall and Protective DNS: query filtering, blocking malware and anti-phishing
  - Implemented by ESRF, ANSTO, ALBA
  - Providers: **N**ational **R**esearch and **E**ducation **N**etwork, Akamai, site implementation
- **(D)DoS:**
  Denial of service
  - ~ 50% of the facilities have DoS protection in place
  - Providers: **N**ational **R**esearch and **E**ducation **N**etwork, Akamai, site implementation (e.g. fail2ban)

Login

- **Methods**:
  - Facility login (User-office credentials)
  - Multi-factor authentication (MFA)
    - Implemented by ANSTO, HZB, ESRF but other facilities use it for other systems (e.g. e-mail, web portal)
  - Single sign-on (SSO):
    - Implemented by ANSTO, ESRF
    - Federated system Keycloak
  - OTP integrated in RD applications
- **Account expiration date**:
  - 50% of the facilities implemented it

Access to control system

- **User-side**:
  - Through MXCuBE
  - Dedicated control system tools installed on workstation, via web or remote desktop
  - Authenticated and authorized (during beamtime only)
- **MXCuBE machine-side**:
  - In most of the cases there are no restriction in connection/communications with the control system

Access to storage system

- **User-side**:
  - SFTP, web tools
  - Authenticated and authorized (proposal)
- **MXCuBE machine-side**:
  - The common solution is to mount the storage using NFS protocol

Networking

- All the facilities implement internal network segmentation
- In most of the cases MXCuBE, control system and storage system are in different subnetworks
- Few cases of fire-walling and filtering between internal networks

Others cybersecurity practices

- Only two facilities (ESRF, EMBL) perform penetration tests
- Almost all have a dedicated team for cybersecurity
- Software Bill Of Materials (SBOM) is exportable from GitHub, but we don’t perform security benchmarks
- Backups of MXCuBE installation are performed by almost all the partners, in these cases, the recovery plan involves restoring these backups.

Thoughts and open questions

- Many common solutions (e.g. Remote Desktop, NFS, etc..)
- Many facilities already have established cybersecurity teams, or they have plans to create one.
- Should we run automated checks on SBOM to look for potential vulnerabilities?
- Weakness in penetration testing and security benchmarks comes up. Should we take some action ?
- Cybersecurity guidelines (highlight best practices like MFA, DoS and DNS protection)