Security Planning from the Start

PCaPAC 2002

Frascati

14 October 2002

Hans Frese, DESY Hamburg

Background

The concepts underlying this presentation are based on personal experience and security related studies in the context of

- DESY's information security organization
- The Information Security Assessment of the Comprehensive Nuclear Test Ban Treaty Organization (CTBTO)

Overview of this presentation

- Information Security Issues
- GAN Security Action Items
- Questions and Conclusions

Information Security Issues

- Security Leadership
- Security Program
- Security Policy
- Security Management
- User Management
- Information Asset Security
- Technology Protection and Continuity

Information Security Issues: Security Leadership

- Security Ownership contains the activities that show executive level commitment and establishes the executive level commitment to support GAN security initiatives.
- Security Strategy contains the activities that produce the overall security vision and strategy that shape and direct security improvements within GAN operations.

Information Security Issues: Security Program (1)

- Security Organization covers the activities that build up and maintain the information security organization design, composition, and reporting structures, as well as the roles and responsibilities, skills and experience, and resource levels committed to the GAN security capability.

Information Security Issues: Security Program (2)

- Security Audits cover the audit related activities that ensure that, periodically, all relevant objects are to be assessed against security requirements. This will also ensure independent monitoring of the security management process.

Information Security Issues: Security Policy (1)

- Security Policies and Requirements cover the activities that establish the formal and prescriptive directives, policies, standards, guidelines, and procedures for implementing security requirements at various levels of the GAN organization. It also includes the process of managing the lifecycle of policies.

Information Security Issues
Security Policy (2)

- Security Agreements cover the activities that establish formal agreements with parties concerning compliance with requirements, to ensure secure GAN operation.

Information Security Issues: Security Management (1)

- Ownership of information covers the activities that establish an overview of assets and the security properties of these assets.

Information Security Issues: Security Management (2)

- Operations and Monitoring covers the processes and procedures for management and administration of the security architecture, as well as the monitoring and incident response efforts to ensure continuous compliance to security requirements.

Information Security Issues
User Management

- Access security covers the activities that implement user privileges and the necessary organizational segregation of duties within the GAN IT infrastructure, e.g. at network, host and application level.
- Personnel related security requirements covers the activities that establish the envisioned level of awareness and education of staff across the GAN.

Information Security Issues: Information Asset Security

- System and network management covers the activities that embed security in the GAN IT management processes, e.g. service level management, problem management, change management, and operations management.
- System development and maintenance covers the activities that integrate secure design principles and implementation of functionality into information systems.

Information Security Issues: Technology Protection and Continuity

- Physical security and security of the environment covers the activities that ensure the mitigation of physical threats to the GAN facilities and related environments which support the GAN information systems.
- Contingency Planning covers the activities that manage the necessary plans and procedures for restoration and continuity efforts that will enable the GAN to recover from major disruptions.

GAN Security Action Items

- Lessons learned from the DESY experience
  - Differentiate from the start
    Policy making organs vs.
    Operations and monitoring organs

GAN Security Action Items

- Define *Security Ownership*
  - Needs GAN Organization Concept
  - Initially, defaults to Site Lab
- Define *Security Strategy*
  - Needs committee representing relevant parties
- Create *Security Organization*
  - Default = Start with Site Lab's?

GAN Security Action Items

- Execute *Security Audits*
  - Must be separate from Site Lab
- Define *Security Policies and Requirements*
  - Must be separate from implementation and enforcement
- Conclude *Security agreements*
  - Intrinsic part of GAN collaboration agreements

GAN Security Action Items

- Establish *Ownership of Information*
  - Needs to be simple and safe
- Perform *Operations and Monitoring*
  - Needs to be done across lab boundaries

GAN Security Action Items

- Implement *Access Security*
  - Remember segregation of duties
- *Personnel related security requirements*
  - Keep personnel aware and educated
- *System and network management*
  - Keep aware of security concerns

GAN Security Action Items

- *System development and maintenance*
  - Keep personnel aware of secure design principles and implementation of functionality into information systems.
- Maintain *Physical Security*
  - at all GAN related sites
- Keep *Contingency Planning* up-to-date.

Questions and Conclusions

- How long can we continue GAN activities with the Workshop Series as the Policy Making Organ?
- Lacking an official GAN Information Security Board, can we lean on a existing one in the TTF2 GAN prototype context?

Questions and Conclusions

- We will liase with ADHOCSEC, the implementation and enforcement level information security committee of the HEP labs (18 Oct 2002 @ FNAL) to discuss technical steps such as cross-lab VPN usage.
- While a GAN wide information security structure does not exist, the Site Lab structure rules.

Outlook

- In the context of TTF2 as a GAN prototype, DESY will act as the site lab
- VPN access from various labs will be implemented according to agreements reached in the ADHOCSEC context
- GRID style access will be investigated