

SECURITY BASELINE

- Policy templates/examples
- "default" ISMS
- A common mechanism for evaluating security posture - useful for benchmarking
- Guide to apply the baseline for an NREN (e.g. where/how to start with ISMS)
- Standards/frameworks in easy terms (explanations)
- Developing an integrated European Standard considering IT Service management, Information Security-Standards like ISO20k, ISO27k, NIST, GDPR
- Benchmarking your NREN to others
- Few standards selection and analysis for Policies creations
- Consider baselining for our clients (Universities) also (not sure if this is scope or just NRENs) - it would be equally of interest to NREN

MANAGEMENT OF RISK

- templates for risk acceptance/temp authorized non-compliance
- It could be part of the Information Security Management but also on General risk Management -> ISO 31kIdentify and share best practices
- Establish collaboration mechanism

LEGAL COMPLIANCE

- Make dedicated workshop on our possibilities of influencing future legislation
- Look at influencing upcoming legislation
- we should investigate the GDPR and security laws and their consequences regarding our operational processes and IT-Services -> check laws

TRAINING AND AWARENESS

- Framework for spheres, divided into sub-spheres, and examples of each
- Developing the Secure Code Training and secure Code Audit to general Services for NRENs, universities etc.
- Having a range of basic security awareness training courses would be useful - also completion stats/reporting would be valuable.
- Collaboration with local (countries) CERT/CIRT agencies/teams doing join shared actions
- TRANSITS like training for management level (crisis management 101)
- common tool, where you can measure whether people read your policies

INCIDENT RESPONSE, BUSINESS CONTINUITY, CRISIS MANAGEMENT

- Working group on information sharing and tooling
 - discussions/collaboration on technical controls
- Developing an integrated, harmonized incident Management process, combining the current different approaches and considering GDPR

PRODUCTS AND SERVICES

- Tools to pull threat info out of / process netflow data to indicate malicious activity
- organizational and technical interop of NRENs and GEANTs DDoS analysis and mitigation platforms
- Generalized Multi-Domain FirewallOnDemand interface supporting further (non FlowSpec) DDoS mitigation technologies (washing machines, SDN/
- Evaluating pentesting as a service
- Communication with local law enforcement. What are the procedures?

- IoC detection and sharing at institutional level
- Information sharing platform
- foster use of PKI for client security (esp. E-Mail)
- EDU VPN: make VPN technology commonly available, by building better and more user-friendly tools (Secure and privacy preserving access fro
- A channel for realtime information / threat sharing
- Agreements for inter-country collaboration - trusted frameworks/standards
- RepShield (correlated security events and reputation score for e.g. IP addresses) further development and distribution in Multi-Domain manner
- Helping to design an NREN security strategy
- Working group on information sharing and tooling
 - discuss/collab on technical controls
 - wiki?
- Also: FirewallOnDemand as Multi-Domain interface for DDoS mitigation across multiple domains (GEANT, NRENs, institutions)
- General: Regional collaboration - particularly outside of EU
 - what NRENs do and how we approach security
 - link up to other groups
- Sensor development and aggregation platform (e.g. honeynet, IDS, etc.)