www.egi.eu
@EGI_eInfra

Information Security at EGI Foundation

In big text blocks only to be even more boring...

May 2021

The work of the EGI Foundation
is partly funded by the European Commission under H2020 Framework Programme

Outline

- Overview of ISM and ICT at EGI Foundation
  - Security Coordination for the EGI Federation
  - High level requirements
  - Examples of Security Threats and incidents
  - Requirements and best practices
- Playing with Information Security

- Intro on GDPR

Overview of ISM and ICT

At the EGI Foundation

- Information Security: a process in our Information Management System (IMS)
  - IMS is certified against ISO 20000-1 and ISO 9001
    - All started with FitSM
  - No ISO 27001 certification for EGI itself, only for people
  - https://confluence.egi.eu/display/IMS/Information+Security+Management+ISM
  - Contacts
    - Baptiste Grenier (Process Manager)
    - Matthew Viljoen (Process Owner)
    - ism@mailman.egi.eu
  - Activities are focused on EGI Foundation but also linking with EGI Federation
  - Also covering data protection aspects

Overview of ISM and ICT

At the EGI Foundation

- Information Security Management: what do we manage?
  - Policies
    - Information Security, ICT, Classification, Federation-related policies...
  - Procedures
    - Managing Assets, BYOD, Security Risks, Security Controls, Security Events and Incidents, DPA, Federation-wide procedures...
  - Inventories
    - Information Assets and Supporting Assets
    - Security Events and Incidents
    - Security controls (mostly references to other documentation)
    - Access management for consultants
    - Required Access rights for new employees
  - Data Protection
    - DPO, Processing Directory, Data Processing Agreements, Privacy Policies, TOMs

Security Coordination for the EGI Federation

Via collaborative management

- EGI CSIRT: Computer Security Incident Response Team
  - Central team coordinating the security of the EGI Federation infrastructure
- EGI IRTF: subset of the EGI CSIRT, with only the individuals involved in the coordination of the Incident Response and active in the weekly rota
- EGI SPG: Security Policy Group
  - Group providing the policies defining the expected behaviour of sites and users to ensure a secure distributed computing infrastructure
- EGI SVG: Software Vulnerability Group
  - Group handling software vulnerabilities reported which are relevant to the EGI Federation infrastructure. Part of the process is assessing vulnerabilities and issuing advisories.

High level requirements

Applying to all employees

- Training and awareness
  - ISO 27001 Foundation training required for all employees
    - Enjoy! :)
  - Awareness campaigns: email, Slack, staff forums, documentation in confluence...
- Following the EGI Information Security and ICT policies
  - You should already have agreed to them when joining :)
- Reporting any Security Incident and potentially relevant Security Events
  - By creating an issue: https://jira.egi.eu/projects/IMSISM
  - By contacting the ISM team: ism@mailman.egi.eu
  - By direct mail or message via Keybase, Slack...

Examples of Security threats and Incidents

That may potentially have happen...

- Service takeover due to attack exploiting unmaintained/obsolete software
- Information disclosure
  - Information shared without realising it like via screen sharing or capture/photos
  - Information sent to the wrong or unintended people
  - Information accessible due to incorrect service configuration
- Phishing attempts
  - Attacks can be very targeted using public data and well elaborated
- Compromise of service providers (like websites)
  - Leaking of data, leaking of credentials
- Cryptocurrency mining on computing resources

Requirements and Best practices

Managing the OS and applications

- Devices registration, encryption, access control and automatic locking
- Keeping Operating System and applications updated is a hard requirement
  - Unpatched systems and applications are one of the main entry points for attackers
  - Manually check at least weekly if OS updates are available (especially on Windows)
  - Always deploy the latest browsers and email clients updates
  - Install and keep running BitDefender to protect from malware
- 2FA/2 steps authentication must be enabled wherever possible
  - Favouring authentication applications for One Time Passwords (OTP) over SMS
- BitWarden must be used to generate, store and manage passwords
  - Enabling 2 Step for Bitwarden
  - Disabling browser's password managers
  - Checking leaked, weak and reused passwords using BitWarden web interface

Requirements and Best practices

Separating work from personal data

- Using browsers and email client dedicated to a specific facet, ex:
  - Brave for work purpose, using EGI.eu Bitwarden account to manage passwords
  - Firefox for personal life, using free personal Bitwarden account to manage passwords

- Keeping data separated on the hard drive
  - Documents/Personal folder to keep personal documents together
  - All work data should go to Google Drive
    - MyDrive for personal documents (in a sub dir) or early drafts
    - Shared drives for all work-related documents

Requirements and Best practices

Protection for online activities

- Use uBlock Origin to protect from tracking and third parties' vulnerabilities
- Verify, verify, verify, verify:
  - Verify real email address behind a name
  - Verify domain names before clicking a link
  - Verify domain name before entering any credentials on a website
  - Verify what is sent to whom
  - Always double think, and avoid decisions and actions in a hurry
    - Think before clicking, acting and/or sharing information
- Register your email address to https://haveibeenpwned.com/
  - Update all passwords for accounts that have been compromised

Requirements and Best practices

Privacy

- Avoid granting access to your device or data to third parties
  - Uninstall all apps that are not used or not trustable
    - Often if a service is free it means you are the product
  - Refrain from installing every new hype app that is collecting your data to show you how you would look in 40 years
- Take care of your and other's privacy, see more at Protecting your privacy
  - Always refuse as much cookies as you can and opt out of treatment that is not required
  - Always grant the less access possible to the less data
  - It's not only about your data, but also contacts, colleagues, customers, suppliers and EGI Foundation's one

Requirements and Best practices

Working remotely or from home

- Organise your home office: Working Remotely
- Maintain a confidential work environment
  - Do not share access to the company laptop
  - Do not leave the laptop unattended and unlocked
  - Only used approved devices
- Find a proper location for working
- Connect to the internet securely via trusted connections or using eduVPN
- Backup you work in Google Drive

Playing with Information Security

Gamified learning, enjoy the fnu!

- For a fun way to learn about CyberSecurity look at https://tryhackme.com/
  - Great amount of free content
  - Including penetration testing aka Ethical Hacking
  - Other interesting resources:
    - https://hackthebox.eu (some free access and content)
    - https://vulnhub.com (only free content)
    - https://www.root-me.org/ (some free access and content)
    - https://yolospacehacker.com/ (Commercial game available on Steam)

About GDPR
Data Protection

- What is GDPR?
  - The EU General Data Protection Regulation
    - A protection legislation to protect and give more control to EU citizens over their data
      - Ratified in 2016, comes into force in 2018
      - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
      - https://gdpr.eu/: a human-friendly version of GDPR with various resources
    - ...and to facilitate the free flow of personal data within the Union
    - Significant change compared to previous directives
      - Consistent treatment of data protection across all EU states and for all citizens
      - Requiring organisations to put in place tools, processes and documentation to comply
- To whom does it apply?
  - To all EU citizens and to any organisation processing personal data of European citizens
    - Including non-EU-based organisations

GDPR: definitions

https://gdpr.eu/article-4-definitions/

- Data subject or natural Person
  - ***an identifiable natural person is one who can be identified, directly or indirectly****, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
- Personal Data
  - ***any information relating to an identified or identifiable natural person*** *('data subject');*
    - Can be name, gender, address, genetic or health information, ID card number, IP address,...
- Processing
  - ***any operation or set of operations which is performed on personal data or on sets of personal data****, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

GDPR: definitions

https://gdpr.eu/article-4-definitions/

- Profiling
  - ***any form of automated processing of personal data*** *consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular* ***to analyse or predict aspects concerning that natural person****'s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*
- Controller
  - *the natural or legal person, public authority, agency or other body which, alone or jointly with others,* ***determines the purposes and means of the processing of personal data;***
    - Entity responsible of and deciding why there is a collection, storage or sharing of personal data, how it's collected, stored and processed.
      - We can act as a controller with potential processors (service or resource providers)
- Processor
  - *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*
    - We can act as a processor, like when providing of a wiki to a project that can use it to store and manage personal data

GDPR: definitions

https://gdpr.eu/article-4-definitions/

- Supervisory Authority
  - *an independent public authority which is established by a Member State and responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons and to facilitate the free flow of personal data within the Union;*

GDPR: Data Protection Officer (DPO)

DPO to the rescue

- Data Protection Officer
  - *GDPR Recital 97: A person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation*
    - To assist data controllers and processor comply with GDPR and avoid risks when processing personal data. Can be internal or external to an organisation.
    - Linking with public and the organisation's employees
      - Point of contact for data protection-related requests
  - Not always required, but if not to be justified to the authorities if asked
    - Almost no processing of personal data, no breaking of data subject's rights
    - No processing of special categories of personal data (religion, sexual orientation,...)
    - Small group of data subjects
  - EGI Foundation is having an external data protection officer
    - Thomas Schaaf, to be contacted via dpo@egi.eu

GDPR: the 6 principles

https://gdpr.eu/article-5-how-to-process-personal-data/

- Data shall be
  - processed lawfully, fairly and in a transparent manner in relation to the data subject (‘*lawfulness, fairness and transparency*’);
  - collected for specified, explicit and legitimate purposes (‘*purpose limitation*’);
    - Cannot harvest/data without any specific goal, in case it could be useful later
  - Adequate, relevant and limited to what is necessary (‘*data minimisation*’);
  - accurate and, where necessary, kept up to date (‘*accuracy*’);
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘*storage limitation*’);
    - personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (as long as in accordance to other articles).
  - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘*integrity and confidentiality*’).

GDPR: rights of the data subject

https://gdpr.eu/tag/chapter-3/

- Transparent information, communication and modalities for the exercise of the rights
- Right of access
- Right of rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object to processing
- Right to not be subject to automated decision making and profiling which produces legal effects or may significantly affect them

GDPR: financial and trust impact

Fines and other reasons to comply

- Fines up to 20 Million Euros or 4% of global turnover (taking the highest)
  - Google (France): 50 million Euros for not complying with the right to be forgotten
  - H&M (Germany): 35 million Euros, due to technical error the data on the company's network was accessible to anyone and the company collected sensitive personal data of their employees using dubious methods
  - British Airways (UK): 20 millions Euros for a data breach impacting 400 000 customers due to poor security;
  - TIM (Italy): 27 million Euros for unlawful data processing (improper consent, excessive data retention, data breaches,...)
  - Austrian Post (Austria): 18 million Euros for processing the political affiliation of data subjects for direct marketing
- In addition to costs for legal defense and changing processes and procedures
- Loss of customers' trust and customers

GDPR: Impact on EGI Activities

What is the impact on our daily activities?

- Need to keep records, via a processing activities directory of
  - Information to be collected from service owners and service suppliers/providers
    - What personal data is processed;
    - Why we are processing that personal data;
    - To whom this personal data is shared;
    - How long its kept;
    - The measures put in place to protect it...
- Need to inform users, projects, partners
    - about the what/why/how/whom and for how long of the personal data processing
    - About their rights and how to exercise them
- Need to have documentation using agreements and policies
    - With users, projects: privacy policies, Data Processing Agreement (DPA) as processor
    - With providers: DPA as controller
- Need to find the proper way to make this work in our special contexts
  - EGI Foundation, EGI Federation with loosely coupled providers,...