Referente cybersecurity per la rete GARR: quale nuova figura?

Laura Biagiotti
European University Institute
Referente cybersecurity per la rete GARR

Appointment of Data Security Officer

- Formal appointment made by Secretary General’s Decision N. 03/2021 (following the first appointment in 2018 by President’s Decision N. 08/2018).
- The role is indicated in the Establishment plan
- The mandate is detailed in the President’s Decision 12-2021 regarding the administrative organisation of the European University Institute (detailed in Article 14 par 2)
- The close cooperation with DPO is stated in the EUI Data Protection Policy, Article 13 point 7

Mandate

The DSO ensures the security of the information systems by establishing security policies and controls, and taking appropriate measures for their implementation in consultation with the Data Protection Officer.

(Extract from DSO’s appointment, SG’s Decision 03/2021)
The role of Data Security Officer includes:
- Advising Data Controller(s), DPO, Project manager(s) and Research projects
- Ensuring prevention and security monitoring
- Performing Information security incident management
- Selecting and managing security technologies
- Ensuring Identity governance and privileged access management
- Conducting Vulnerability assessment and ensuring vulnerability management
- Partnering with CERT-EU for monitoring and detection of security events

Reporting lines
• Advising Chief Risk Officer to reducing cyber risks to the appropriate risk-appetite level of EUI and to leverage cyber security investment;
• Reporting to ICT Director, as detailed in in PD 12/2021
• Reporting data breaches to Data Controller(s) and Data Protection Officer within 72 hours according to EUI DP Policy
• Reporting to CERT-EU on security incidents communicated by SOC’s teams
Cybersecurity risks

Sources: BBC and Reuters websites
The 9 top threats
1. Ransomware;
2. Malware;
3. Crypto jacking;
4. E-mail related threats;
5. Threats against data;
6. Threats against availability and integrity;
7. Disinformation – misinformation;
8. Non-malicious threats;
9. Supply-chain attacks
Referente cybersecurity per la rete GARR

Cybersecurity risks
- Il superamento del perimetro fisico
- L’Incremento della superficie d’attacco
- L’adozione massiva del cloud
- L’incremento del numero di attacchi e la combinazione delle tecniche utilizzate
- Crypto-locker e Ransomware che possono comportare l’interruzione parziale o totale delle attività

Compliance
Privacy policy (e.g. EUI Data Protection policy, GDPR)
- Misure di sicurezza (Security of processing)
- Notifica delle violazioni di dati personali (Data breach notification)
Standard de-facto per la sicurezza delle informazioni
- ISO/IEC 27001:2013 Information security
- NIST Cyber security framework
Referente cybersecurity per la rete GARR

Richiesta di istituire la figura del Referente GARR per la sicurezza informatica

Obiettivi

- Tempestiva comunicazione degli incidenti di sicurezza agli incaricati dall’istituzione accademica (i.e. CISO, Information security Officer, o CERT interni)

- Condivisione degli Indicatori di Compromissione (IoC) tra referenti per attuare le necessarie misure di prevenzione e mitigazione del rischio

- Creare una rete di referenti di sicurezza per condividere esperienze ed aumentare la consapevolezza sugli attacchi mirati verso la comunità Accademica
Referente cybersecurity per la rete GARR

Data Security Officer

Contacts
Data Security Officer (data_security_officer@eui.eu mail account)
Report phishing to phishing@eui.eu
Report abuse and malware to reports@eui.eu

For more details, visit the Information Security page at the following link:
https://www.eui.eu/ServicesAndAdmin/ComputingService/Security

Grazie per la vostra attenzione

Laura Biagiotti
laura.biagiotti@eui.eu