UK e-Infrastructure Security and Access Management Working Group

The Research Councils' UK e-Infrastructure group has asked Janet to establish a working group to support those providing and using e-infrastructure services in achieving an approach that both protects services from threats and is usable by practitioners. The Group's approach is to identify security and access management requirements that are common to different e-infrastructures and to identify or develop and disseminate good practice – whether policy, procedural or technical – in those areas.

Activities

The Working Group has held its first two, quarterly, face to face meetings and established a closed mailing list for working group members. A collaborative website has been created where information about the working group, discussion documents and presentations, references, links and recommendations are being published.

[https://community.ja.net/groups/uk-e-infrastructure-security-access-management-wg]

Achievements

A list of organisations relevant to e-infrastructure access management and security has been made; details about each are being added to a wiki on the working group website.

Janet staff have met with a number of different e-infrastructures (including Diamond, DiRAC, Crick and GridPP) to discuss access management requirements and suggest how existing and planned Janet services might assist. A paper identifying what appears to be a common 'user journey' from application to use of an e-infrastructure was presented to the Project Directors' Group in February. Following their validation of this approach this paper is now informing the working group's activities in the access management area.

A discussion on e-infrastructure security has identified relevant good practice from other fields and suggested that the Top20 security controls suggested by UUK/BIS may also be an appropriate cybersecurity standard for e-infrastructures.

Planned Work Areas

In access management we plan to help e-infrastructures take advantage of their users' existing authentication relationships with their home universities. This will include comparing the requirements of e-infrastructures with the authentication and enforcement policies provided by the existing UK Access Management and eduroam federations. In cooperation with Janet's Moonshot pilot programme we will also work with e-infrastructures to determine how their existing systems for authorising access to resources and data can be linked to these federation technologies. Future plans include examining how to authenticate users from outside the UK education community (e.g. from other sectors and countries, and citizen scientists with no organisational affiliation), and whether there might be benefits in delegating group management services as well as authentication.

In security we will consider whether the CyberSecurityCouncil list of Top20 controls may provide an appropriate standard for e-infrastructures, as well as continuing to share existing good practice for e-infrastructure design and operation. Future plans include consideration of the risks to which e-infrastructures are exposed, to assist the choice of appropriate controls and help users choose the appropriate infrastructure for their task.