Ireland's National Education & Research Network

Security Auditing

A Comprehensive and Integrated up-to-date Security Strategy

Security Auditing - What is it?

HEAnet's Security Auditing service covers systems, networks, equipment, staff action, and the institution's IT activity as a whole.

Security Auditing is offered by HEAnet as a comprehensive, holistic review of an institution's security readiness, which could involve on-site visits.

Why do I Need Security Auditing?

IT administrators gain a commanding overview of their system's readiness against threats through a Security Audit. This is essential in developing an integrated and up-to-date IT security strategy.

This process requires experienced members of the HEAnet team working on-site at an institution, and allows HEAnet to assess all aspects of the institution's operations. It combines a rigorous, physical examination of a client's system and associated equipment, with detailed scanning and assessment of existing e-infrastructure.

The process involves a dedicated scoping exercise. This allows for a lining-up of the organisation's resources, and to centre the environment in which the audit will be applied.

Key Asset Identification

Engagement with members of staff is essential as information on resources and practices are gathered by the HEAnet audit team. This is followed-up by identifying key assets of the institution and how to best protect them.

Through deep network scanning, probing for vulnerabilities through the entire network ranges, the assessment of a client's whole network is possible.

With security tools like NESSUS and others, the vulnerability of client networks to the very latest security hazards can be properly assessed.

Security Auditing - A Comprehensive and Integrated up-to-date Security Strategy

1 Scoping exercise to establish audit aims

2 Engagement with key staff

3 Examination of key systems and assets on-site

4 Network/IP scanning using the latest tools

5 Detailed report and findings delivered

6 Provide follow-up support

Outcomes of Security Auditing

✓ Positive security behaviours encouraged

Highly comprehensive and complete image of security situation provided

Reduced institution risks as recommended security practices are implemented

Food for Thought

48% of surveyed organisations reported staff-related cyber security incidents

82% of surveyed organisations carried out risk assessments

42% spike in security incidents reported by organisations in 2015

Infographic Sources

BIS Cyber Security Breaches Survery 2014 (PWC)

Global State of Information Security Survey 2015 (PWC)

Verizon 2014 Data Breach Investigations Report

2015 Cyberthreat Defense Report (Tenable)

Contact HEAnet

Security Auditing support is provided by the HEAnet NOC.
Email: **noc@heanet.ie** or call 01-660-9040, Monday to Friday, 09:00 - 17:30.

The HEAnet NOC is committed to ensuring every HEAnet client receives a consistent, responsive service with an emphasis on minimising client disruption.

HEAnet
Ireland's National Education & Research Network

HEAnet Limited, 5 George's Dock, I.F.S.C., Dublin D01 X8N7, Ireland.
Tel: 01 660 9040. Fax: 01 660 3666.

www.heanet.ie | ***@heanet and #heanet***