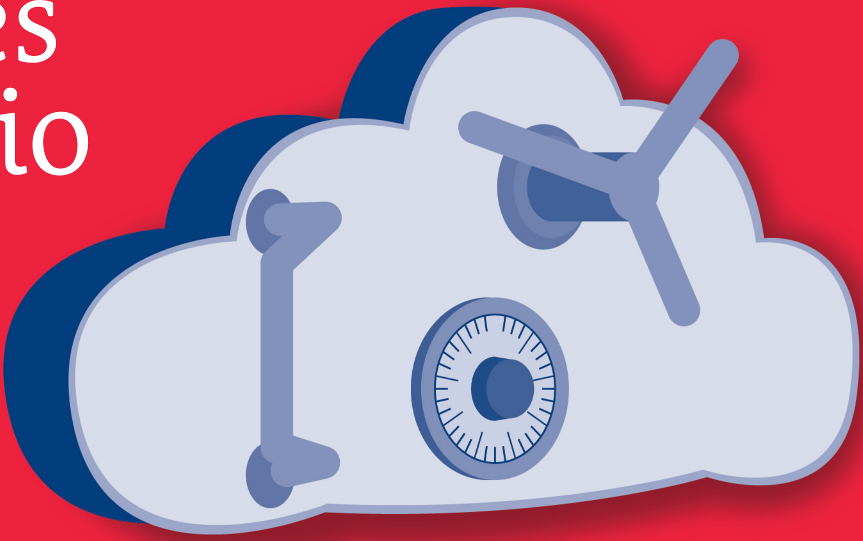
HEAnet
Ireland's National Education & Research Network

Security Services Portfolio



What are HEAnet's Security Services?

HEAnet offers a range of services to help limit the vulnerability of clients' systems to exploitation and attack.

These measures range from SSL website certification and anti-spam blacklisting services, to more pro-active website auditing and scanning engagements, which actively seek out and uncover potential weaknesses in client systems before they can be exploited.

HEAnet also offers services to assist client institutions in the event of an incursion (CERT) - helping to resist, recover and ultimately learn from an attack incident. All HEAnet security services are provided on a not-for-profit basis.

Specific Services

- **Security Auditing -** HEAnet's in-depth auditing service, this is a comprehensive examination of an institution's systems.
- **Vulnerability Scanning -** HEAnet's in-depth scanning service which will comprehensively "crawl" an institution's network in order to discover any vulnerabilities or flaws.
- **HEAnet-CERT -** HEAnet's active incident service, providing real-time advice and recommendations to any HEAnet client suffering an intrusion.
- **HEAnet TCS (Trusted Certificate Service) -** HEAnet's no-cost website SSL certificate service, essential for website traffic encryption and data protection.
- **Real-time Blacklisting Service -** This Blacklisting service acts as a powerful component to any active anti-spam strategy, providing a list of suspect IPs.

Client Needs

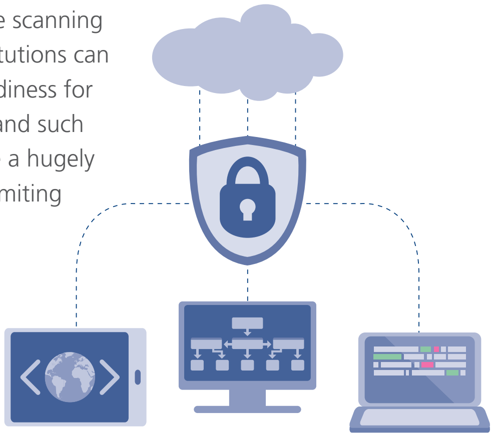
The worse-case security scenarios for HEAnet clients are a highly disruptive attacks, DDoS incidents, hijacking of client servers or systems, or any incident of data loss.

> **Such malicious attacks can cause major disruption to end-users and institution staff, resulting in extensive costs and a negative perception of an institution's IT security.**

Even minor intrusions can incur significant costs and consume staff time in dealing with the problem.

The proliferation of malware, and the range of "direct" online attacks has brought a need for institutions to continually patch, strengthen and assess their own online security.

Through pro-active scanning and auditing, institutions can ascertain their readiness for such an incident, and such actions could have a hugely positive effect in limiting potential damage.



SSL Certificate Service

SSL website certification is a service, which ensures HEAnet clients' websites are encrypted and have a base level of security.

The across-the-board roll-out of certification is being driven by an increased awareness of the need for encrypted channels, and the proliferation of authentication and authorisation middleware.

HEAnet's TCS (Trusted Certificate Service) is providing server certificates valid for three years to our clients at no cost. These certificates are essential for the security of everything from institutional websites, to sub-sites for research groups, student societies, etc.

The server certificates can be used for institution services, including web (HTTPS), email (IMAPS), server authentication and any number of SSL or TLS based services that require trusted certificates.

This service can be expanded to additional areas of certification including document certification, allowing an institution or department to digitally sign, and thus protect, written content.

This can also be expanded to certifying programmes and developed applications, ensuring that ownership and development rights are protected.

HEAnet Cert Service

CERT is HEAnet's single contact point for clients dealing with computer security incidents. In an instance where a client is concerned they may be experiencing an intrusion or attack, CERT rapidly provides support, advice and expertise.

To report an active security concern, please contact the HEAnet CERT service via cert@heanet.ie

If a security concern arises out-of-hours, please contact the Jisc service desk at: +44 3300 300 2212.

This CERT mailbox is monitored by HEAnet to promptly provide support, and is supported out of hours by the Janet Network CSIRT (UK), who will help and advise HEAnet clients in any security situation.

CERT provides the following to all HEAnet clients:

- Technical assistance on what to do in the case of an incident
- The collection, analysis and reporting of statistics on incidents.
- Notifications to sites that they may have been the source, intermediary or target of an attack, as they can often be unaware.

CERT is also ready to assist all HEAnet clients who wish to pro-actively seek support for any perceived security issues and vulnerabilities.

Real-time Blacklisting Service

This is a useful service for clients who wish to cut off email contact with servers that are associated with extensive spamming.

This is an especially useful service for clients who run their own mail servers, as it gives the server the power to shield itself against highly troublesome IP ranges.

To prevent these servers from interacting with a client's mail server, a range of IP addresses are supplied to client institutions, who can then block these ranges. This results in the refusal of incoming emails from this range of suspect IPs, ensuring no contact is possible.

This service is offered in partnership with **TrendMicro.com** and **SpamHaus.org**

HEAnet
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***

HEAnet
Ireland's National Education & Research Network

Vulnerability Scanning

A Risk-assessment Service for discovering Security Holes in IP Networks

Vulnerability Scanning - What is it?

The HEAnet Network Vulnerability Service is a no-cost, risk-assessment service for discovering security holes in a client's IP network.

It allows HEAnet clients to closely examine their networks for faults that, if not fixed, could become serious threats to their organisation's network security.

This powerful tool allows member institutions to probe their network's Internet-facing devices, identifying any aspects of it that may be vulnerable to attack or be compromised. It seeks out security holes and bugs in host operating systems and application software that could cause serious issues.

The HEAnet Network Scanning Service is provided as part of HEAnet's service to clients and is covered by existing Client Service Agreements.

Why do I Need Vulnerability Scanning?

The need for IT departments to have a thorough, dependable way to check their network for vulnerabilities is more pressing than ever.

This service, based on Tenable's powerful Nessus vulnerability scanner, allows IT departments to gain a detailed overview by conducting a complete network scan.

The service sequentially examines all aspects of the network in order to locate vulnerabilities, logs them, and delivers a detailed report upon completion.

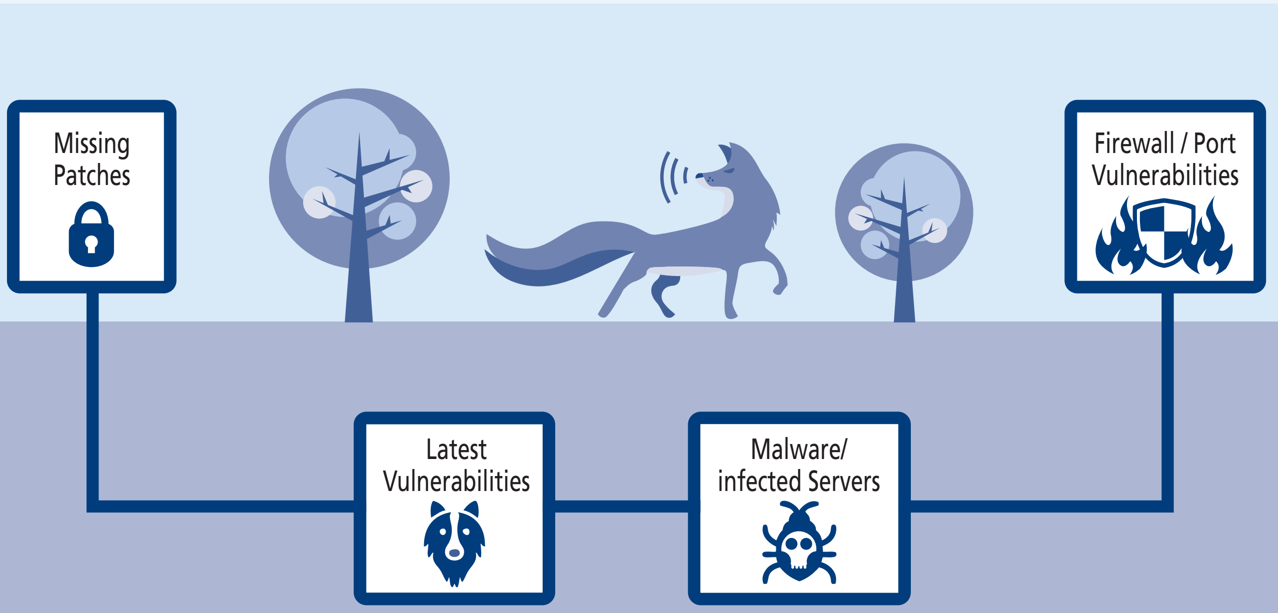
With an improved reporting process and the ability to specifically scan for the very latest vulnerabilities and security concerns (e.g. Heartbleed, POODLE vulnerabilities), this tool can highlight instances where the institution may be at risk.

Routine use of the vulnerability scanning tool forms part of an effective risk mitigation process. This is one of the most useful tools that can be deployed in a risk-minimisation plan. It could unearth vulnerabilities that standard "eyes-only" scanning misses.

Part of an Integrated Strategy

By using this service to gather detailed information in a structured manner, an IT department can stay fully informed as to the state and readiness of the network, via clearly defined risk levels.

Vulnerability Scanning - A Risk-assessment Service for discovering Security Holes in IP Networks



Missing Patches

Firewall / Port Vulnerabilities

Latest Vulnerabilities

Malware/ infected Servers

Vulnerability Scanning provides:

- Accurate "snapshot" of the security status of a client network
- Deep Scanning, ensuring all system aspects are inspected
- Improved reporting process, providing ready "to-do-list" for IT staff to act upon

Food for Thought

- 74% of web attacks still using simple exploits in executed code
- Low employee security awareness still ranked as # 1 security inhibitor
- 4 in 10 organisations now carrying out full system scans at least monthly

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)

HEAnet's Vulnerability Scanning service makes use of Nessus (Tenable) and Outpost24 deep scanning tools - leading solutions in the information security industry.

Nessus vulnerability scanner | Outpost24

Contact HEAnet

Vulnerability Scanning 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 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