Cyber Security Audit

The Evolvement Cyber Security Audit is an annual validation of your organisations that will improve your organisations IT systems by performing internal and external vulnerability checks to identify the IT security controls that your organisation needs to ensure you are managing cyber security effectively and that you are mitigating the risk from internet borne threats, such as phishing and hacking.

How it Works

The Audit will provide your organisation with concise information on how to maximise security for your data, and ensure that the data you hold is managed and protected in the best possible manner that shows your organisation takes cyber security seriously. The process:

- A member of the Evolvement team will go through the Cyber Security Questionnaire with your organisation, allowing us to gain clarity of your organisations infrastructure and current defence.
- An Evolvement engineer will conduct the necessary tests on the organisations internal and external systems, as appropriate.
- A full report of the major findings will be issued to your organisation along with reliable recommendations for maintaining a secure network.
- A follow up meeting to provide advice and planning for implementing a robust cyber security strategy for your organisation.

The 5 Key Areas of Mitigation

Mitigation is required to protect your organisation from a cyber-attack. The most common way in which your organisations systems are vulnerable to attack is through phishing and hacking The Evolvement Cyber Security Audit will implement the controls listed below in order to mitigate and control any threat.

Secure Configuration
We will run tests to confirm that computers and network devices are securely configured.

Boundary Firewalls & Internet Gateways
We will take measures to ensure that at least one firewall is installed on the boundary of your organisations internal network, that it is secured with a strong password and that any unauthorized services are blocked on the system.

Access Control & Administrative Management
User accounts will be reviewed to ensure that inactive accounts are removes from the system and that all users are updating their passwords (with suitably strong passwords) to protect the organisations data.

Patch Management
All software installed on your organisations systems will be reviewed to validate that they are supported and licensed by the official vendor, and, that the software is running the latest version of the program.

Malware Protection
Malware Protection will be installed on all computers that are able to connect to the internet, if they are not currently supporting enough protection. Malware that is already installed will be tested to ensure that it is up to date and functioning to the highest possible level.

Internal Vulnerability Checks

The internal systems will be tested to ensure internal devices are not able to intentionally or unintentionally impact the security of the network infrastructure or individual systems.

Weakness Detection
We will run tests to ensure that no significant weaknesses exist on the network infrastructure or on individual systems.

Database Testing
Testing will be conducted to determine if your data and resources are protected against potential attack. These tests will ensure that your database is exhibiting integrity and resilience for the protection of your organisations sensitive data.

Wi-Fi Testing
We will test your wireless network inside and out to check for any vulnerabilities or weaknesses that may exist. Our testing will include rogue access point detection, wireless LAN detection, frequency scanning and encryption analysis.

External Vulnerability Checks

Your organisations external systems will be audited to ensure maximum protection from unauthorised access or change.

Remote Devices Audit
We will run remote access tests to confirm that remote devices are functioning at maximum security, including mobiles, tablets and other electronic devices that regularly connect to your network**.**

Third Party Supplier Testing
We will audit third party supplier software to ensure that they are compliant with your organisations current security policies. Instilling confidence into the software you are using in your organisation. These tests are also beneficial for vendors who wish to validate the standards of their software.

Internet Testing
Internet testing will analyse your email servers, web servers, firewalls endpoints and much more to determine you're your organisation is using the internet in a secure manner.

Protect your Assets Today

Get in touch with our team today and find out how we can deliver you a realistic approach for achieving a robust cyber security strategy.

Evolvement Networks Ltd – www.evolvement.net – info@evolvement.net | Tel: 0800 819 9180

Evolvement, St Line House, Mount Stuart Square, Cardiff CF10 5LR | Tel: 02920 509 074

Evolvement, Mezzanine Level, Urban Village, 221 High St, Swansea SA1 1NW | Tel: 01792 439 150