

Inattentiveness to security, new infrastructure changes, altered firewall rules and new security threats all impact businesses in critical ways. COMPUTERLINKS' Testing and Auditing Services ensure that you highlight these issues to your customers, so that they are kept updated about potential weaknesses in their systems. This also alleviates the aggravation of them or you having to purchase, install and train staff on off-the-shelf solutions.

Our Network Health Check service reviews the state of an organisation's perimeter security. Whether it be for main IT systems, satellite offices or remote workers, if there are any doubts about how secure systems are, our entry-level assessment will determine exposure to attack or information theft.

Whatever the requirement, this service is an excellent top-level method of detecting security holes in your clients' networks and e-commerce/web applications and will uncover essential information about perimeter security, such as: security status and defense mechanisms, incident response handling, employee security awareness, security policy guidelines and adherence.

SERVICE DESCRIPTION

Network Health Check

The Health Check provides a bird's eye view of an organisation's security status, that can be broken down into the following:

1. **Network Surveying**
2. **System Fingerprinting**
3. **Port Scanning**
4. **Services Probing**

Network Surveying is primarily a non-invasive data collection and information analysis stage. The aim is to find the number of reachable systems to be tested. Expected results can be:

- Domain names
- Server names
- IP addresses
- Network map
- ISP / ASP information
- Possible test limitations

System Fingerprinting is the active exploration of a system for responses that allow us to distinguish between unique systems to OS and version level. If successful, this can reveal further information on OS type, patch levels and system types.

Port Scanning is the invasive probing of system ports to enumerate live or accessible Internet services as well as examining, and penetrating firewalls to find additional live systems. Expected results include:

- Open, closed or filtered ports
- IP addresses of live systems
- Active services

Services Probing aims to provide further information about applications and services running behind open ports. Information that may be acquired are details such as web server/database versions, patch level, server modules and misconfigurations in setup and security.

Internal Health Checks

COMPUTERLINKS also offer a more thorough review by duplicating the test above on the internal network, providing analysis of an organisations security risk from both an internal and external network perspective. A consultant will visit the customer's premises to perform the additional assessments and will include all findings in the final report.

In addition to this Health Check Service, COMPUTERLINKS also offers a wider range of enhanced security testing services. For more information, please contact us.

DELIVERABLES

On completion of the work, COMPUTERLINKS will present documentation with our findings and where appropriate, recommendations, along with a debrief of the results over the phone with the consultant who performed the scan.

Documentation information is as follows:

- Executive Summary
- Findings and analysis
- Potential security holes and vulnerabilities broken down into levels of priority
- Recommendations and improvements to be made to overall security
- Any assumptions made by COMPUTERLINKS over the course of the audit
- Next steps beyond the Vulnerability Scan snapshot
- Appendix of material acquired over the course of the audit

REGULAR VULNERABILITY SCANS

As time progresses, new vulnerabilities are discovered, new trojans are written and occasionally misconfigured software can be installed, all of which can render a system vulnerable to attack.

COMPUTERLINKS is able to offer monthly or quarterly Network Health Checks at increased discounts, which will identify any potential weaknesses in a network or systems connected to the Internet. Our experienced consultants will use their specialised knowledge of network security and the latest vulnerabilities to examine network perimeters.

Each scan will result in extensive documentation, which will be suitable for both technical and non-technical audiences and will highlight any potential issues relating to their Internet presence.

In addition to this Network Health Check, and for more extensive testing, COMPUTERLINKS have a wide range of testing and auditing services.

SECURITY SERVICES

External Infrastructure Penetration Test
DMZ Testing
Internet Application Testing
Gateway security review
wLAN testing
VoIP penetration testing

INFORMATION SECURITY MANAGEMENT SYSTEMS

Gap Analysis
Internal Audit
Firewall Policy Review
Policy & Build Reviews
Policy/procedure review

BUSINESS CONTINUITY

Business Continuity Planning
Business Continuity Testing
Incident response and forensics
Telecoms services

 **SERVICE LEVEL AGREEMENTS**

 **PRICING & DISCOUNTS**

 **BESPOKE CONTRACTS**