

INFORMATION SECURITY AUDIT

How secure is your Network?

It is not a surprise the Information security policy is still not widely practiced in most of the organizations today's. In fact, most of them do not have a security policy. How secure is the network? Are the passwords difficult to crack? Are there audit logs to track who accesses data? These are the questions normally asked among us!



An information security audit (ISA) is one of the best ways to determine how effectively the network security of an organization without incurring high cost and other associated damages of a security incident.

Ofisgate emphasizes the importance of Information Security Audit. We insist Information Security Audit is the essential network audit for government, private sector or non-profit organization. We offer comprehensive Information Security Audit plans, consisting of vulnerability assessment and penetration testing. It gives a vital security health check on client network and recommends the appropriate security methodology.

Our Vulnerability assessment runs scan tests on client's network and identifies entry points that might cause risks, attacks and damages of a security incident. Penetration testing is where numbers of attacking software applications are being tested on a computer system, network or web application to find vulnerabilities that an attacker could exploit. Auditing reports will be generated afterward based on all the findings and information gathered.

Information Security Audit Program

Network Security Audit identifying...

- Network Mis-configuration
- Open Port In Client Network
- Unknown Port
- Weird Connections
- Firewall Configurations & etc...

Database Security Audit identifying...

- SQL/MySQL/Oracle/MS Access/postgress
- Default configuration (setting & setup)
- Connection settings
- Database settings
- User Account settings & etc.

Remote Security Audit including ...

- External and internal Pen-test for Backdoors
- Unsecured Open Port
- Unknown Open Port
- Old/Unused Services that at risk of exploit
- Weak security configuration
- Domain Name Server
- Trojan, Daemons
- Brute Force attack
- SMTP & etc...

Web/Application Security Audit identifying...

- Common Holes in Web
- Bad Password
- Directory Traversal
- Old Directory/Folder
- SQL/MySQL injection
- Blind SQL/MySQL injection
- Cross site scripting
- Cross site forgery
- Bad Configuration
- CGI-BIN Exploit & etc...

Server Security Audit identifying....

- Weak Server Configuration
- Weak Password Implementation
- Unpatched services
- Old Account
- Unused account
- Possible Denial of Service(DOS/DDOS) & etc..

OFISGATE SDN BHD (610820-A)

Malaysia
Tel: +603 8994 0778
Fax: +603 8994 0779

Singapore
Tel: +65 6296 5563
Fax: +65 6294 7339
www.ofisgate.com



tm

ofisgate

changing the climate