Cyber Security Threats: Are you prepared?

- Vulnerability testing service -

Although security threats are a well-known fact in the IT security industry, most organizations are not taking steps to secure their systems. Recent reports show that most organizations are not adequately prepared to handle cyber threats and major security incidents. So how can Teamlink help you to prepare for the changing cyber threats?

The NTT Group's 2015 Global Threat Intelligence Report demonstrated that most organizations are not prepared to handle cyber- threats and -attacks with adequate procedures.

"76 % of all detected vulnerabilities are more than 2 years old"

Today the amount of security threats are increasing. Anyone can become, even for a non IT or security expert, an attacker using widely available user-friendly malicious toolkit (e.g Exploit kits).

"Over 80% of vulnerabilities in 2014 exploit kits were published in 2013 and 2014"

These toolkits are created with the focus of delivering an up to date and effective way to achieve successful attacks on targeted systems.

For an organization it is important to know how prepared they are to confront ever changing external threats. TeamLink offers security and vulnerability audit services to protect small/mid-sized companies.

Why is recurrent vulnerability testing important?

In today's complex security landscape new threats keeps emerging on a regular basis and there are more vulnerabilities than ever before.

The goal of penetration testing is to find vulnerabilities in networks, servers, applications, and operating platforms that could potentially be exploited by attackers or cause business disruption.

While many organizations today have some type of penetration/vulnerability tests performed annually (usually for compliance reasons), vulnerability tests should ideally be done more often to determine with higher certainty that flaws do exist.

Important for your clients

Data protection has always been a business requirement in the security industry, but the last several years this has become more acute and important in all business sectors which handle sensitive data or business critical IT infrastructure.

This is due to several reasons; Security breaches are more frequent and severe than ever before; large scale breaches are now widely publicized in media; and an increasing ratio of consumers that want to know what information is stored about them, where the data is stored and how it is used (e.g personal and credit card info).

The last is especially important for organizations that store customer and/or process credit card info.

Compliance requirements

Besides being a security best practice overall, many compliance mandates specify penetration testing as a

Powered by:

Audea
Seguridad de la Información

requirement or recommendation. The most well-known that explicitly requires penetration testing is the Payment Card Industry Data Security Standard (PCI DSS), which requires pen testing at least once a year.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies that **process, store or **transmit** credit card information maintain a secure environment.*

Cyber threat intelligence

Vulnerability testing is a good way to know how an organization is prepared to meet external threats. However to make these test results valuable and lead to actionable solutions, the resulting test report needs to include risk level assessment together with recommended actions.

Combining these test results with a periodic cyber-intelligence alerts report will allow you to move to a more proactive approach and to take actions and plan better for future threats.

The service offering

TeamLink and its partners have been focused on delivering IT services for the modern company. Along with Offshore Mobile and Web Development, TeamLink has now added a state of the art Security Audit / Penetration Test Information Security Service.

The audit service provided simulates the actions of an external attacker who intends to bypass the security of an organization. Just as an attacker would do the auditor tries to exploit security vulnerabilities to gain access to critical systems and sensitive information.

Powered by:

Audea
Seguridad de la Información

Our Security Audit is ISO/IEC 27001 compliant and its objective is to conduct regular vulnerability audits and / or perform penetration tests on customer owned IP addresses and applications. Our service will also provide information on your systems security risks and vulnerabilities in a threat intelligence report. There are three levels to our recurrent service:

***Bronze Level Service**:*

- *Quarterly analysis report of vulnerabilities on up to 3 IP addresses.*
- *A monthly threat intelligence report of alerts relevant to the type of IT system.*

***Silver Level Service**:*

- *Monthly analysis report of vulnerabilities on up 10 IP addresses.*
- *A monthly threat intelligence of alerts related to the type of IT system.*
- *4h Remote support by email/Skype about the conducted audits or any other issue related to the SGSI-ISO/IEC 27001.*

***Gold Level Service**:*

- *Monthly analysis report of vulnerabilities on up 20 IP addresses.*
- *A monthly threat intelligence report of alerts related to the type of IT system.*
- *A penetration test on an IP or web application during the course of the year.*
- *8h Remote support by email/Skype about the conducted audits or any other issue related to the SGSI-ISO/IEC 27001.*

Contact Us

For more information about the service or partnership enquires:

TeamLink International AB
Gjuterigatan 9
55318 Jönköping
Sweden
Tel: +46 76 015 50 44

Powered by: