The use of web applications and web services has become an integral part of virtually every aspect in the business process cycle. Besides promoting products and services online, businesses are interacting with customers over the internet and employees are using a growing number of web-based tools for every-day tasks.

Web applications have become the most common platform for new software solutions. However, these efficient and cost-effective tools introduce new risks and a need for better or different security measures to compensate for the open, rapid development style that makes the technology increasingly common.

Can malicious attackers obtain access to sensitive company information through your web application?

Can you guarantee that the private data of your customers or employees is safe?

Can malicious attackers perhaps impair the availability of your application and negatively impact your revenue?

Can malicious attackers deface your website and cause you embarrassment and loss of reputation with your clients?

Awareness of the security vulnerabilities and possible weaknesses within the web applications is the first step towards adequate security.

Many organisations only fight these threats by preventing intrusion over the network layer; making use of network firewalls and intrusion detection and prevention systems. However, these controls do not secure the application layer, as they cannot differentiate between traffic of one web application from another web application.

Even though a company may have minimal online presence (e.g. static website with a simple form submission), considering the surge in web-related incidents (e.g. website defacement) and the resultant risks (e.g. reputational risk), web application security on every online presence should not be overlooked.

Given the inherent limitations in any system of control, and the continuous enhancements and changes in systems, new vulnerabilities may be introduced. In addition, the system may be vulnerable to new security loopholes in the underlying platform due to version upgrades or newly discovered flaws. Therefore, constant monitoring and change controls that address security are needed to ensure that system controls - remain effective over time.

The risk of malicious attack comes with any venture onto the web - no matter how small.

Are you sure that you are prepared?
Why do I need this?

It has become much easier to simply attack a web application, rather than spending hours hacking the network perimeter. In addition, a web application provides a much-larger canvas for an attacker to work on. These attacks can easily be automated and failing to protect your system against them can have serious consequences on the business – not just on the technology. Not only could attackers access confidential information but they could also attain some of the company’s intellectual property. A loss of information could lead to customer distrust; undermining a reputation and tarnishing the corporate image.

Typical Test Process

The Web Application Security Assessment is a penetration test targeted at the top-most layer in your IT services stack - efficiently and systematically. Our methodology is as follows:

Assess/Model Threats: Establish and acquire the information required to successfully define the scope of the web application security assessment.

Survey: Review the web application to identify points of entry, key processes, key controls and other required information to identify the type of tests that need to be carried out and define the respective tool set.

Automated Testing: Automated tests are designed to seek out potential weak points in web application and website security to allow the testing to be concentrated effectively.

Advanced Testing: Certain tests cannot be automated and must be executed by a security professional and the results must be analysed in detail. In addition, the results from automated tests allow the security professional to focus the effort on any identified weaknesses and carry out detailed tests during this stage.

Analyse Results and Prepare Report: Upon completion of testing, results are analysed and detailed technical recommendations are prepared. Results of manual tests, automated tests, advanced tests, and selected evidence collected throughout the assessment are provided.

Our Approach

At PwC, we aim to find the security vulnerabilities in the web application before others do. A structured and methodical approach is used such that the results of the assessment assist the company in taking informed decisions on how to apply better security measures. We assess the likelihood associated with each threat agent, security weakness and attack vector to determine the overall risk to your organisation. Focus is placed on the Top Ten application risks, compiled by OWASP, to be able to project an accurate report, depicting the weak points of the system.

We use a mix of commercially available tools and open-source tools to identify vulnerabilities at the infrastructure level and we use different test platforms to minimise the risk of false positives.

Our Experience

Globally, PwC has performed this service for our clients for a number of years, and has developed a mature and robust methodology that ensures all client risk is adequately managed.

We have secure laboratory environments to ensure that all testing activity is controlled and contained, and that your data is adequately secured. Locally, we have experience in successfully performing penetration testing on online banking services, online retail shops and online workflow systems for our clients.

The company needs a web presence that is secure.

Web-based technologies are efficient and practical to deploy, maintain and use but come with inherent vulnerabilities.

Have all the risks been assessed and addressed?

Contacts

George Sammut
george.sammut@mt.pwc.com
+356 2564 7608

Gordon Micallef
gordon.micallef@mt.pwc.com
+356 2564 7014

Nathan Gatt
nathan.gatt@mt.pwc.com
+356 2564 7035

Follow us on:

www.pwc.com/mt