Feel free to challenge

PENETRATION TESTING

With the constant change in technology, organizations are required to ensure that their existing IT infrastructure evolves to protect confidential information.

KPMG can help better protect your business's critical and confidential information by regularly assessing and addressing security threats and system vulnerabilities before they are discovered by a digital intruder.

KPMG's penetration testing team has the skills to thoroughly assess your level of information security through simulated attacks on your network and web based applications such as eCommerce sites. Using hacker techniques, we identify targets that exploit existing security weaknesses. Common targets include the Internet perimeter, internal and external network infrastructure, online databases and applications.

The objective of performing proactive penetration testing is to provide you with substantive proof of vulnerabilities and recommend effective countermeasures, allowing you to take appropriate actions before your network falls victim to a security incident.

Affordable piece of mind

KPMG strives to offer you value, reasonable professional fees and an objective assessment of your network security controls. Our team offers an impressive track record and network of knowledge at your service.

We have executed penetration tests for both small and large organizations with a wide range of network designs and information systems. Our clients operate in a number of industries such as financial services, insurance, telecommunications, government, utilities, education, consumer goods, retail, wholesale, hospitality and oil and gas.

Potential benefits to you

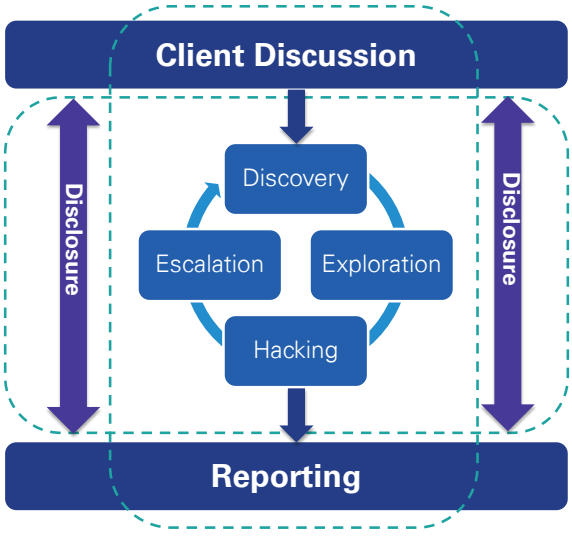
- Identification of risks surrounding how the confidentiality of data may be compromised.
- Identification of poorly implemented security controls which may lead to performance and/or security issues.
- Overview of deficiencies that could be exploited by an internal or external threat.

Our approach

KPMG's approach is based on the risks facing your organization. Cyber attackers can target your network and eCommerce applications from the other side of the globe. Employees may also be attempting to compromise your confidential information. Thus, three types of penetration tests are available:

1. **External penetration tests** assess and quantify threats and vulnerabilities associated with specific target environments, such as Web servers, eCommerce sites, electronic mail servers and other publicly visible servers which could be targeted by cyber attackers.
2. **Internal penetration tests** help focus on the protection of critical data and resources, intranet servers and databases and administrative level accounts. This type of test can identify risks which could be exploited by a disgruntled employee.
3. **Web application penetration tests** assess the security of the authentication process and security of a user's session. Further, data validation tests are also performed to identify areas that allow a user to insert and run their own code e.g. XSS (Cross-site scripting) and SQL injection.

We have developed a methodology that addresses the requirements of penetration testing. The approach is shown in the diagram below.



Rules of engagement

The rules of engagement will be signed by both parties involved. These rules outline the terms that we will follow during the penetration tests. KPMG's professionals work to take every precaution to protect your online and network operations during the tests as well as any information that may be collected during the tests.

Reporting

Our reports reflect the work we do: quality, accuracy and objectivity. They help to offer all intended audiences the information needed to appropriately manage security requirements.

- Management can gain an overall understanding of the work performed and the results obtained.
- Technical personnel can immediately use our report to correct the vulnerabilities or weaknesses identified. The recommendations are of a technical nature so that IT personnel can leverage the report without loss of time.
- For recurring clients, we analyze the progression of your information security level. We review your previous system deficiencies, weaknesses and vulnerabilities to assess the level of corrective action. We also perform additional tests to identify potential new deficiencies.

WE BELIEVE CYBER SECURITY SHOULD BE ABOUT WHAT YOU CAN DO – NOT WHAT YOU CAN'T

WHY KPMG?

INDEPENDENT

KPMG is not tied to any technology or software vendor. Our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

COLLABORATIVE

We facilitate and work with collaborative forums with the aim of bringing together the best minds in the industry to collectively solve shared challenges.

TRUSTED

KPMG member firms have a long list of certifications to work on engagements for the world's leading organizations.

GLOBAL, LOCAL

KPMG is a global network of member firms with over 174,000 people working in 155 countries. We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide. KPMG's regional practices can service your local needs from information security strategy and change programmes, to low level technical assessments, forensic investigations, incident response, training and ISO27001 certification.

Contact us:

Diveane Bowe
Partner
Audit and IT Advisory Services

T: +1 (242) 393-2007
E: dbowe@kpmg.com.bs

Shavonne Thompson
Senior Manager
IT Advisory Services

T: +1 (242) 393-2007
E: slthompson@kpmg.com.bs

kpmg.com.bs **kpmg.com/app**

Download on the App Store