Deloitte.

Řízení zranitelností a penetrační testování
Vulnerability Management and Penetration Testing

Dostupnost informací a přístupová oprávnění představují dvojsečnou zbraň. Mohou usnadnit přístup na nové trhy, spojit Vás s klienty a obchodními partnery a pomoci zvýšit produktivitu a výkonnost. Zároveň Vás však, často ve spojení se zranitelnostmi systémů, na kterých jsou informace zpracovávány, vystavují novým rizikům, k nimž patří neautorizovaný přístup k informacím, porušení mlčenlivosti, ztráta duševního vlastnictví, odepření služby či zavirování.

Silné a slabé stránky infrastruktury, aplikací a dat mohou přímo ovlivnit úspěch společnosti v podnikání. V prostředí rychle se měnících technologií a neustále se zvyšující potřeby spojení se světem potřebujete vysoce kvalitního, nezávislého partnera v oblasti bezpečnosti služeb, který s Vámi bude spolupracovat s cílem efektivně plnit Vaše obchodní požadavky.

Kompetence Deloitte

- Pracovníci s rozsáhlými zkušenostmi z oblastí výroby, financí a IT.
- Kontinuální vzdělávání konzultantů v oblasti penetračního testování a řízení zranitelností.
- Certifikace konzultantů v oblasti řízení zranitelností.
- Znalosti z mezinárodních a velkých českých organizací.

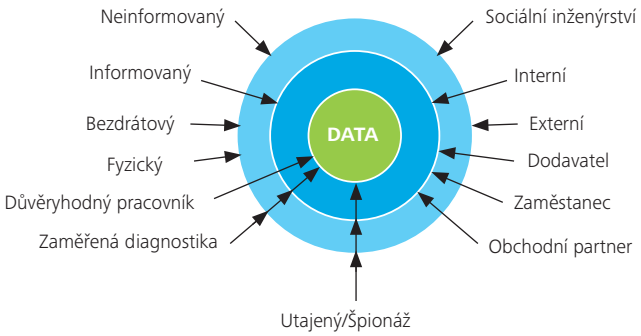
Externí penetrační testy…

…se používají pro hodnocení bezpečnostních rizik. Testy jsou navrženy tak, aby simulovaly reálné útoky s použitím nástrojů a technik využívaných opravdovými hackery. Primárním účelem těchto testů je odhalení a odstranění zranitelností před jejich zneužití útočníkem. Testy napodobují akce skutečného útočníka bez obvyklých rizik. Testy zkoumají slabiny IT systémů, které by mohly být zneužity externím útočníkem k narušení důvěrnosti, dostupnosti nebo integrity počítačové sítě, čímž umožní společnosti tyto slabiny řešit.

Interní penetrační testy…

…napodobují akce skutečného útočníka, např. záškodnického zaměstnance zneužívajícího slabin v bezpečnosti zevnitř počítačové sítě. Tento test zkoumá slabiny, které by mohly být zneužity k narušení důvěrnosti, dostupnosti nebo integrity počítačové sítě, čímž umožní společnosti tyto slabiny řešit.

Perspektivy hrozeb útoků



Úroveň simulovaného útoku

Testování na aplikační úrovni…

…zahrnuje testovaní prezentační vrstvy, vrstvy obchodní logiky, databázové vrstvy a jednotlivých rozhraní. Testy hledají problémy v autorizačních a autentizačních mechanismech, chyby validace vstupu či špatné bezpečnostní prostředí. Testy mohou probíhat anonymně či na úrovni autorizovaného uživatele.

Přínosy penetračního testování a řízení zranitelností

- Zabezpečení infrastruktury proti neoprávněnému vniknutí, zneužití systémů nebo zcizení dat.
- Zvýšení povědomí o zabezpečení provozovaných systémů.
- Ochrana reputace a dobrého jména společnosti.

Kontaktní informace: ***Vlastimil Červený*** – Senior Manager, +420 737 210 667, vcerveny@deloittece.com

Deloitte.

Vulnerability Management and Penetration Testing

The accessibility of information and access authorisations are a double-edged sword. They can simplify the access to new markets, connect you with clients and business partners and help increase productivity and efficiency. However, at the same time they expose you to new risks, including unauthorised access to information, breach of confidentiality, loss of intellectual property, denial of service or a computer virus infection, often in connection with the vulnerability of the systems in which the information is processed.

The strengths and weaknesses of the infrastructure, applications and data can directly influence the company's business success. In an environment of fast-changing technologies and a continuously-increasing need to connect with the world, you need a high-quality, independent partner in service security who will cooperate with you with the aim of fulfilling your business requirements effectively.

Deloitte's key competencies

- Employees with extensive experience in manufacturing, finance and IT;
- Ongoing education of consultants in the area of penetration testing and vulnerability management;
- Certification of consultants in vulnerability management; and
- Knowledge gained in international and large Czech organisations.

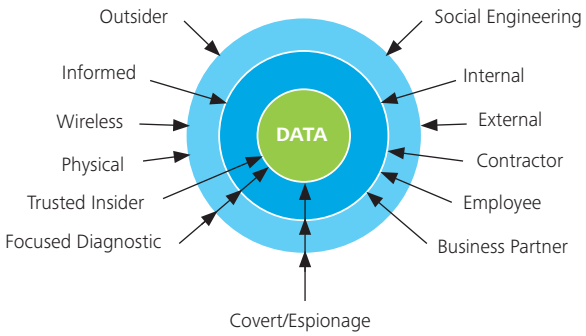
External penetration tests...

...are used to evaluate security risks. The tests are designed so as to simulate real attacks using tools and techniques used by real hackers. The primary purpose of these tests is the detection and elimination of vulnerabilities before they are abused by an attacker. The tests imitate the actions of a real attacker without the usual risks. They scrutinise the weaknesses of external IT systems that could be abused by an external attacker to breach the confidentiality, accessibility or integrity of the computer network, thus enabling the company to solve these weaknesses.

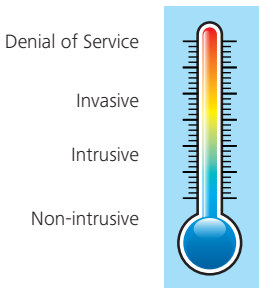
Internal penetration tests...

...imitate the actions of a real attacker, eg a saboteur (employee) using weak spots in the security inside the computer network. This test examines the weaknesses that could be used to breach the confidentiality, accessibility or integrity of the computer network, thus enabling the company to solve these weaknesses.

Attack Threat Perspectives



Simulated Hostility Rating



Testing at an application level...

...includes testing the presentation layer, business logic layer, database layer and individual interfaces. The tests are looking for problems in authorisation and authentication mechanisms, mistakes in the entry validation or bad security environment. They can be performed anonymously or at the level of an authorised user.

Benefits of penetration testing and vulnerability management

- Infrastructure security against unauthorised penetration, system abuse or data alienation;
- Increase in the awareness of security of the operated systems; and
- Protection of the company's reputation and good name.

Contact information: ***Vlastimil Červený*** – Senior Manager, +420 737 210 667, vcerveny@deloittece.com