Deloitte.

Ethical Hacking

Defend against Cyber Attacks

Operating in an increasingly connected world and placing greater reliance on information technology have one inevitable consequence: cyber attacks. An organisation will need appropriate defences if it wants to avoid finding its perimeter, website or data breached sooner or later.

Security technology may have progressed considerably; a "silver bullet" solution is still a long way off. As the sophistication and frequency of cyber attacks rises, securing perimeters and externally accessible systems is becoming more time consuming, resource intensive and expensive. Organisations need to continually assess their environments to identify weaknesses and vulnerabilities within their systems before taking the appropriate action to remediate and defend against cyber-attacks.

Understanding the threats

Ethical Hacks are becoming the cornerstone of a proactive cyber threat defence strategy. Understanding their cyber attack profile requires organisations to consider this:

"Companies need to make major changes in the way they use computer networks to avoid further damage to national security and the economy. Too many companies, from major multinationals to small start-ups, fail to recognize the financial and legal risks they are taking - or the costs they may have already suffered unknowingly - by operating vulnerable networks"

Shawn Henry, FBI

- How will a cyber hacker probe our environment and would we detect it?
- Do we patch systems for known vulnerabilities?
- Are online services we offer to clients, employees and business partners secure?
- How do we test our defences to determine their effectiveness or how they can be improved?
- Are employees sufficiently aware, so they can recognize attacks?
- Do we have enough measures in place to restrict access to physical locations?

In answering these questions organisations can begin to focus their cyber threat defence strategies on the areas of greatest risk, thus reducing their cyber-attack profile.

Deloitte.

Types of Ethical Hacks

Organisations need to conduct periodic Ethical Hacks to continuously assess weaknesses and vulnerabilities to prevent cyber attackers from potentially breaching defences. Ethical Hacks may include assessments of:

Infrastructure: perform network-based testing that simulates a hacker attack on your IT infrastructure. This may involve your VPN solution for employees or the infrastructure supporting your critical web portals.

Application: perform network-based testing that simulates a hacker attack on your web applications or mobile apps. This may involve testing the resilience of your customer portal against unauthorized access or malicious behaviour of valid customers.

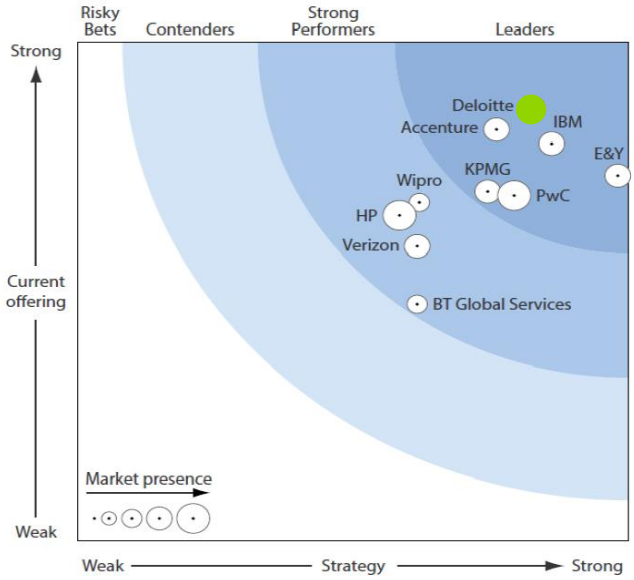
Employee: perform social engineering based testing to simulate a hacker attack on the human element: your staff. This may involve testing how your employees respond to phishing emails.

Physical: perform physical testing to simulate an attack aimed at gaining unauthorized access to your premises. This may involve testing measures in place to prevent unauthorized access to office buildings or critical data centres.

All Ethical Hacks can be performed with or without prior knowledge of your environment. This will enable us to perform an Ethical Hack that closely simulates an actual attack on your environment.

World class services

- Our security experts have the same skills and methods hackers use, but can also translate technical issues into business risks.
- Deloitte has a global reach, with a presence in over 150 countries worldwide.
- We can support you in solving security issues as a trusted advisor in a vendor-agnostic, but knowledgeable way.
- Deloitte has been named a leader by Forrester Research, Inc. in Information Security Consulting in a new report, The Forrester Wave™: Information Security Consulting Services, Q1 2013.



Cybercrime.
Be ready.

Deloitte.

Contact

Do you want your cyber readiness and user awareness tested by our team of ethical hackers? Contact us:

Panicos Papamichael
Partner – Risk Advisory
(+357) 22 360 805
ppapamichael@deloitte.com

Yiannis Ioannides
Senior Manager- Hacking services
(+357) 25 868 849
ymioannides@deloitte.com