

Introduction

IMAGINE!!!!

Your customers' vital financial information is stolen by an attacker!

Your customers' day to day operations are monitored by an outsider from a remote location!

All correspondence like e-mails are viewed by a competitor!

ARE YOU RESPONSIBLE FOR THIS????

You'd surely be dragged into the ensuing legal quagmire that might cause unnecessary costs owing to legal hassles and can also result in

- Loss of goodwill
- Loss of brand value and
- Loss of invaluable customers.

Need

Customer trust: IT vendors are heavily losing on customer trust as their products are becoming more and more vulnerable to newer attacks thereby bringing the customer businesses to stand still.

Market share: Most of the IT vendors are seeing a plunge in their market share due to high customer attrition rates.

Legal Implications: A vendor is directly responsible for product he manufactures. Therefore, in case of a security breach in the product, the vendor is made to cough up huge sums of money as compensation by the affected end users.

Risks Involved

Legal hassles.

Loss due to compensation paid.

Direct impact on brand value

Loss of time & credibility.

Mental strain and pressure.

Erosion of goodwill and brand value.

Customer/client attrition.

The company's revenue and in turn, the bottomline can take a serious hit in the event of a security breach as confidential information gets leaked to unauthorized sources.

Our Solution

At COE Security, we strive to provide solutions for combating threats which plague an Enterprise.

Solutions are provided through a complete assessment of the software product wherein we apply various innovative techniques in finding the threats existing in the product. This assessment delivers a complete picture of the security competence of the product thus enabling you to protect your organization from any unforeseen legal implications.

Benefits

- Mitigation of threats
- Improved product quality.
- Customer satisfaction.
- Avoid legal hassles.
- Protection of goodwill and brand value.
- Credibility (for both product and organization).
- Business advantage over competitor's product.

PRE-RELEASE PRODUCT SECURITY TESTING LIFE-CYCLE



Possible Threats by a Software Product

Category	Attack	Description
Malicious Software	Virus	Malicious software that causes damage to a computer system. The damage can range from repeatedly displaying a pop-message to crashing of the system and loss of important data. It duplicates itself within a computer system, potentially attaching itself to every software application.
	Spyware	It is a broad category of malicious software which intercepts or takes partial control of a computer's operation without the informed consent of that machine's owner or legitimate user.
	Worm	Propagates through a network thus hogging the bandwidth and slowing down the network considerably.
	Trojan Horse	Same as Virus or Worm, but also sometimes used to send confidential information like username and passwords, back to the perpetrator.
	Reverse Trojan (Server-to-Client)	Same as virus or worm where the server is active and the client passive. This kind of attack can bypass firewalls, IDS, anti-virus softwares, spyware removal tools, etc.
	Time Bomb	Same as Virus or Worm, but get activated only on a certain predetermined date and time.
	Logic Bomb	Virus or Worm designed to activate under certain conditions.
	Key loggers	Malicious programs that secretly capture or log all the keyboard inputs and transfer or mail them to the attackers located outside the trusted the local network.
	Backdoors / Trapdoors	Developers usually put some access points in the software they develop for easy navigation during development and testing. Backdoors / trapdoors are such system access points that are inadvertently left available even after software release.
	Rootkits	They are a set of tools that enable the intruder to maintain his stealth after gaining access to the system. In other words, the intruder uses rootkits in order to maintain access to the remote system without the owner's knowledge.
Malfunction	Software Malfunction	Malfunction in the operation of the software due to a faulty code or data.
	Hardware Malfunction	Faulty hardware.

For Further Details visit: www.coesecurity.com or Email sales@coesecurity.com