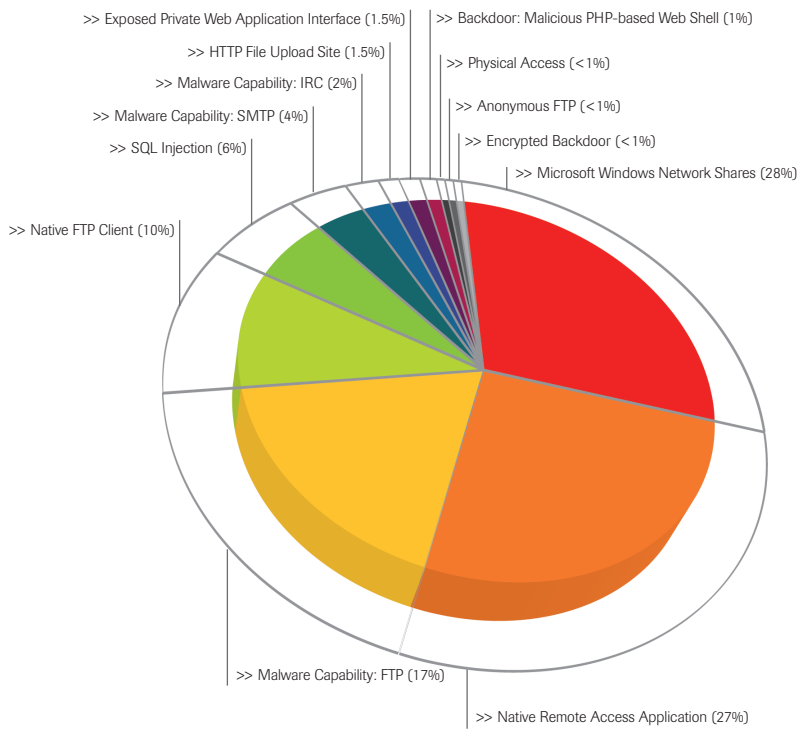
Global Security Report 2010
Overview

Trustwave's Global Security Report 2010 analyzes data gathered from nearly 1900 penetration tests and more than 200 security incident and compromise investigations conducted in 2009. Providing business and technical impact analysis, the report was compiled by SpiderLabs, the advanced security team at Trustwave responsible for delivery of incident response and forensics, penetration testing, application security and security research services.

Report Highlights

- More than 60 percent of incident investigations were carried out for companies with less than 500 employees.
- Criminals most frequently used a remote access application, such as Windows Remote Desktop Protocol, to carry out an attack.
- Software Point-Of-Sale (POS) systems were the most frequently breached, making up 83 percent of assets targeted.
- 81 percent of compromised systems were managed by a third-party vendor.
- Hospitality and food and beverage clients accounted for only 7.6 percent of the proactive penetration tests performed, yet this sector made up over 50% of incident investigations, indicating a defense-in-depth strategy deters cyber criminals.

Attack Methods Used to Extract Data



10 Strategic Initiatives for Every Organization

1. Perform and Maintain a Complete Asset Inventory– Commit to decommissioning older systems
2. Monitor Third-Party Relationships– Choose a platform and vendor with a solid security history
3. Perform Internal Segmentation– Segment network into as many security "zones" as possible
4. Rethink Wireless– Never place wireless access points within the corporate core network
5. Encrypt Your Data– Understand where data is located, purge what is not needed and encrypt the rest
6. Investigate Anomalies– Investigate unexpected behavior such as suspicious server outages or crashes
7. Educate Your Staff– Education can lead to earlier notification and detection of a potential incident
8. Implement a Software Development Life Cycle (SDLC)– Process should include security planning up front
9. Lock Down User Access– Most persons do not require all access rights they have been granted
10. Use Multifactor Authentication Everywhere Possible– Cost to implement is far less than a breach's impact

Top 3 Attack Methods

- Remote Access Application– Leveraged, for example, to take advantage of an improperly configured firewall that allows this type of access.
- Third-party connectivity– Any telecommunications line connecting two or more physically dispersed networks; an example being multiprotocol label switching (MPLS).
- SQL Injection– Exploits flaws in Web-based applications that result in exposure of data and information within a database.

Top 4 Industries that Experienced Breaches*

Hospitality	Financial Services	Retail	Food and Beverage
38%	19%	14%	13%

(*% of all Incident Response Investigations)

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave®
Information Security & Compliance