Physical Security Testing

PT

Penetration Testing

Identify and remediate physical weaknesses with Trustwave's physical security and social engineering assessment.

For businesses that need to assess the physical security of a building, facility, campus or other physical location

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure—from the network to the application layer—to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

A Analyze | P Protect | V Validate

For more information about Trustwave's Elements of Compliance and Data Security please visit: www.trustwave.com

Keep the Intruders Out

At your place of business, is valuable intellectual property protected by two screws and a faceplate, leaving the latch accessible through a gap in the door? Physical security controls have technical weaknesses, such as this one which is easily exploited with a stiff card or needle nose pliers.

A company's physical security controls may also suffer due to poor security awareness and the natural human tendency to accept people at their word, leading to social engineering attacks where a malicious individual persuades well-meaning employees to volunteer information.

Trustwave's SpiderLabs is one of the leading, advanced security teams in the world, helping businesses identify vulnerabilities in their facilities, both externally and internally, through:

- Physical penetration tests
- Business intelligence tests
- Social engineering exercises

Our experts review, assess and test physical security controls to ensure these controls are serving their intended purpose—keeping the intruders out.

Physical Security Assessment and Testing

Trustwave's SpiderLabs work collaboratively with clients to assess the physical security of a building, facility or campus. Our proprietary methodology calculates the risk a business faces, and then our experts identify and evaluate security system upgrades in order to reduce that risk.

While the physical assessment and test are tailored to the specific requirements of an organization, we typically conduct the following tasks:

Site Survey: A SpiderLabs expert will visit the target facility, working on location to understand and review the general building layout, sensitive areas and the nature of the security controls in place, including:

- Exterior doors and locks
- Fences
- Dumpsters
- Camera placement
- Other external controls
- Interior physical security controls

All potential vulnerable spots and other findings are thoroughly documented.

Controls Testing: After the site survey, an expert will test physical security controls to ensure that both technical and non-technical bypass are not possible. This testing includes the attempted bypass of door locks, motion sensors or other controls, spotting weaknesses with camera placement, and the ability to access sensitive areas through security control bypass.

Networked Physical Security Access Control Systems (Optional): Clients may enlist the SpiderLabs team to launch a technical attack against networked or computerized physical security and building access control systems to determine vulnerabilities. This optional testing may include attempts at authentication bypass, "man in the middle" attacks, attacks against Windows Domain joined systems and other attack vectors to better identify how attackers may be able to gain unauthorized access to physical security control systems.

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

Why SpiderLabs is the Best Choice

Trustwave's SpiderLabs' services and delivery are backed by a full portfolio of information security resources:

Expertise

The SpiderLabs team consists of some of the top information security professionals in the world. With career experience ranging from corporate information security to security research and federal and local law enforcement, our staff possesses the background and dedication necessary to stay ahead of the technical, legal and management issues affecting your organization's information security.

Experience

SpiderLabs has performed hundreds of forensic investigations and application security tests and thousands of ethical hacking exercises for a client list that includes Fortune 500 companies, small to mid-sized businesses, government security agencies and law enforcement agencies.

Certification

Trustwave is certified by the National Security Agency (NSA), the agency responsible for assessing the US government's information security posture. We are also authorized by all major credit card brands to conduct investigations of compromised merchants and processors.

Facilities

SpiderLabs maintains the most advanced application and hardware testing facility in the industry.

Safety

SpiderLabs works closely with clients to ensure that all of its services are performed with strict confidentiality and rigorous legal oversight.

SpiderLabs®

Client-side Penetration Testing

Organizations that are already increasing security at their perimeter and adding systems to keep intruders out may still be vulnerable to external attacks. An attacker may instead attempt to get individuals to unknowingly run a malicious program on their work computers (e.g., phishing attacks) to bypass perimeter security and create a channel from inside the network.

In executing this test, our experts use social engineering and other methods to bypass perimeter security, validating that:

- Staff are adhering to acceptable use policy
- General security awareness exists across an organization
- Ideal performance of key systems such as SMTP/HTTP filtering and proxy services, and any endpoint security present in the environment

The test typically includes the methods below, but can be tailored to the needs of any organization:

Organization Intelligence: Through extensive research using various public databases and other resources, Trustwave experts compile a target list of users and contacts at the organization. Such lists are frequently used by attackers to target specific individuals within the organization.

Attack Delivery: Experts will attempt to exploit an organization's staff through e-mailed links, forged Web sites, browser hijacks through Cross Site Scripting (XSS), and other delivery methods. This phase simulates the methods an attacker might use, but safely, with the use of code developed specifically for this purpose by SpiderLabs.

Data Extraction: During this phase of testing, the SpiderLabs expert will attempt unauthorized access to sensitive information such as personally identifiable information (PII) or cardholder data (CHD). This allows organizations to learn more about the actual impact and risk they face.

Business Intelligence Testing

Social networking, location aware services, mobile blogging and other technologies make it easy for people to exchange information. Unbeknownst to the employee, some of this information can be sensitive to a business, putting its reputation or finances at risk.

To find out what data exists publically and online, one of our expert researchers examines public resources and uses data mining tools, potentially answering such questions as:

- Is a business' intellectual property the subject of someone's Facebook status?
- Has an employee used location adware software while posting something about their company?
- Do employees place confidential information or activities on Twitter?
- Is an employee blogging about an upcoming product release that has not been publicly announced?

After examining the overall risk of data loss, the researcher will deliver a strategic and tactical report to address these issues in keeping with the overall business model.

Social Engineering, or Red Team, Testing

A red team is a group of subject matter experts (SMEs) of various physical security disciplinary backgrounds who provide an independent review of plans and processes. Businesses, civilian government agencies and the military all use red teams to test concepts, hypotheses and operational plans or defense strategies in a controlled manner, using predetermined tactics, techniques, and procedures (TTPs) or situations.

The red team at SpiderLabs can act as both the adversary's advocate as well as knowledgeably role-play the client, using a controlled, realistic, interactive process. The SpiderLabs red team:

- Surveys and collects information on the physical perimeter and security controls
- Derives methods of attack and penetration methods for facility
- Carries out predetermined (approved) attacks on facility such as:
  - Lock picking
  - Forcing open magnetic doors
  - Avoiding alarm systems
  - Entering by ventilation systems
  - Tailgating
  - Procuring a badge to gain access
  - Soliciting
  - Redirecting video camera systems
- Gathers onsite sensitive information by physical collection, shoulder surfing and photographs.
- Gains access to protected areas such as a server facility or data center
- Records all possible penetration points as well as catalogs all information collected