SERVICE DESCRIPTION

SpiderLabs Physical Security Assessment

Service Scope

The Trustwave SpiderLabs Physical Security Assessment service results in a collaborative assessment of the physical security controls protecting the target building, facility or campus. Trustwave Physical Assessment is a collaborative effort to review, assess, and test physical security controls.

The process begins by gaining an understanding of the primary physical security control objectives. Once Trustwave SpiderLabs has gained this understanding a review of the facility takes place, which includes: a site survey, identification and assessment of physical security controls weaknesses and failures; Networked physical access control system review.

The service assesses the effectiveness of the physical security systems against resilience to attack from an intelligent adversary, and the subsequent potential impacts of that adversary exploiting the identified control weaknesses and failures.

The deliverable will capture all key data points for the assessment and will provide recommendations for improvements and upgrades to the physical security systems in order to reduce the risk of unauthorized physical access to the target building, facility or campus.

Scope and Project Phases

Site Survey

Trustwave SpiderLabs will arrive on site at the facility to be tested. An initial discussion with the authorized site contact will determine the general building layout, sensitive areas, and the nature of the security controls in place. A perimeter survey (escorted) takes place to identify and assess the physical security controls such as exterior doors and locks, fences, waste disposal areas, security camera placement, etc.

Following the perimeter walk, a facility walk-through (escorted) takes place to assess interior physical security controls. At all stages findings and photographic evidence of potentially physical security weaknesses will be captured.

Physical Controls Testing and Review

After the walkthrough is completed, the Trustwave consultant will iteratively test physical security controls in place to ensure that either technical or non-technical bypass is not possible. Testing will include 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

As an additional step for organizations that have networked / computerized physical security and building access control systems, the consultant can launch a technical attack against these systems to determine vulnerabilities which may give an attacker control over these systems. The consultant may find issues such as authentication bypass, Man in the Middle attacks, attacks against Windows Domain joined systems or other attack vectors in which one could gain unauthorized access to these physical security control systems.

Deliverables

Following the conclusion of the engagement, findings will be made available. The deliverables will be both strategic and tactical in nature, presented in a format that is highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.