A PENETRATION TEST CASE STUDY

RETAIL

WHO

MID-SIZE RETAILER

e-Commerce
Brick & Mortar Stores
1200 customer accounts

Our client, a mid-sized retailer of discretionary consumer products, was originally founded as a traditional brick and mortar storefront with a single site in the Midwest. They have steadily grown over the last 30 years, expanding to multiple locations both through rollouts and acquisitions. In the mid-nineties, a strategic decision was made to embrace the emerging online retail community as a supplement to the storefront presence. Currently, the retailer operates facilities including data centers, shipping and distribution, and several thousand storefront locations throughout the United States. The online presence services customers both domestically and internationally.

WHY

PCI DSS Compliance Requirements

M&A - now Level 1 Service Provider
Former IT resource errors
Needed comprehensive review

Most retail organizations accept credit card as a form of payment and, as such, are subject to the Payment Card Data Security Standard (PCI DSS). The PCI DSS, maintained by the Payment Card Industry Security Standards Council (PCI SSC), is a global security standard consisting of a series of technical and operational security safeguards designed to prevent credit card theft and fraud. The PCI DSS applies to all organizations that store, process, or transmit card data, and additionally sets forth requirements for assessment activities to validate compliance, including penetration testing.

This retail organization accepts credit cards at all storefront locations and exclusively accepts credit card payment through the online presence. Classified as a Level 1 merchant, an annual penetration test is required as part of the broader onsite assessment. In addition, as a direct result of acquisition and mergers, this organization was also classified as a Level 1 Service Provider. This is due to the fact that the parent company is accepting credit card payments on behalf of franchise stores operating under their brand. This results in additional validation activities being required. After a particularly challenging compliance cycle with another provider, missed compliance dates, and resulting fines, the organization decided it was time to work with a QSA company that could handle their unique and complex needs.

WHAT

Successful Remediation

Comprehensive Testing & Compliance
Increased Efficiencies
Reduced Compliance Validation
Decreased Surface for Attacks
Significant Cost Savings
Lessened Overhead

The organization needed to have a penetration test conducted, but not just any penetration test. They needed to ensure the penetration test aligned with the scope and boundaries of the cardholder data environment, covered all the required tests defined within PCI DSS Requirement 11.3, including segmentation verification testing every six months, and ensure the e-commerce presence was compliant with PCI DSS Requirement 6.6.

They needed a team that not only understood how to safely plan and execute a complex penetration test, but also do so in a manner that was be acceptable under the PCI DSS.

A PENETRATION TEST CASE STUDY

RETAIL

Scope Definition

Scope definition is the critical step to developing the approach for any penetration test engagement. An initial consultation meeting was conducted to gather the business requirements, discuss compliance requirements, and determine the scope of review. This process is as much about requirements gathering as it is about education. As the retailer utilizes segmentation to reduce the scope and boundaries of their compliance requirements and validation, particular focus was paid to the network architecture and flow of card data throughout the environment. During this discussion with a HALOCK QSA, it was determined that the scope would include several components:

- EXTERNAL, NETWORK, and WEB APPLICATION PENETRATION TESTING which required a single production data center, fully isolated from all other environments, housed the e-commerce environment.
- Two call centers, connected to an isolated segment at a second operations data center, contained staff handling card data. Both call center sites and portions of the data center would also require internal network penetration testing. The call centers had no direct internet access as traffic was routed through the data center, therefore external network penetration testing of the latter would be required.
- Internal network penetration testing required for the retail storefront presence. As all the store locations was hub and spoke connected to the operations call center, a plan was developed to deploy centrally to reach each store utilizing the wide area network, reducing the cost of testing.
- Limited access was permitted to both data centers from corporate, however segmentation was implemented to minimize the scope of PCI compliance at the corporate location. Wireless was present at corporate, but also segmented to prevent wireless access into the cardholder data environment. Internal network penetration testing would be required within this isolated environment as well as segmentation verification testing to confirm segmentation was effective between the cardholder data environment and the remaining out of scope corporate networks. This segmentation verification testing would also have to be repeated every six months.
- REMEDIATION VERIFICATION TESTING would be needed to retest any identified vulnerabilities following remediation but prior to compliance validation submission, as required by the PCI DSS.

The complete scope of review, methodology, and related considerations are consolidated for the customer's review and approval.

Planning and Preparation

Following finalization of contracts, an initial planning call was conducted. The agenda for this initial call was to identify stakeholders, discuss general planning considerations, and make arrangements to conduct follow up meetings with various members of the organization. Several considerations emerged.

First, as the compliance validation data was fast approaching, a timeline was developed to ensure there would be adequate time for preparation, testing, reporting, remediation, and verification. Float was worked into the schedule to accommodate several upcoming change freezes that prohibited testing from being performed during those windows. Additionally, delays in preparation were anticipated and accounted for because one of the data centers was managed by a third-party provider with a history of missing committed deadlines. Second, due to a recent migration, it was determined that the target IP ranges would need to be reviewed and updated to reflect several changes to the assigned ranges.

All planning considerations, including technical details, planned upcoming meetings, fieldwork details, and related considerations were documented in a detailed project plan. This plan was updated as information requests were completed, and details were finalized. As the fieldwork testing dates approached, reminders, updates, and a final planning review meeting was conducted to ensure everything required for testing was in place and that no other open items remained. Everything was confirmed to be complete and accurate.

A PENETRATION TEST CASE STUDY

RETAIL

Penetration Test Fieldwork

On the first scheduled test shift, a notice was issued to all stakeholders that testing was beginning. HALOCK initially began reconnaissance activities, both internally and externally, originating from several points of origin. The team collaborated to ensure network discovery and segmentation verification covered each scenario and all target networks from each origin, responding hosts and services were located and documented, and that potential vulnerabilities affecting these hosts were enumerated. The team compiled the results of the discovery phase, finalized target lists within the sampling requirements defined, and developed an attack plan.

Testing progressed iteratively as the team moved through each target environment, pursued exploits, eliminated false positives, and confirmed the presence of exploitable vulnerabilities. Initially, very little opportunity to gain access was observed. Testing continued for several days, each beginning and ending with notices and status. By midweek, the team identified a portion of the environment that did not demonstrate the same level of security hardening as observed elsewhere. It was also observed that this portion of the environment was largely comprised of franchise stores.

Pursuing several vulnerabilities, an exploit was executed, resulting in access to several PC based point of sale terminals at two different franchise locations. Testing progressed through several phases of privilege escalation, lateral movement, data exfiltration, and related activities. This access resulted in the identification of several vulnerabilities that would materially affect PCI compliance validation. Using information obtained at this site, including configuration data, documents access, and password hashes obtained on the compromised hosts, HALOCK revisited networks that had (up to this point) been resilient against attack. The access achieved at the franchise store allowed HALOCK to gain an initial footprint within the data center environment that was expanded as testing progressed.

The customer was notified during testing due to the criticality of the vulnerabilities, however testing continued as scheduled. Testing of the application was also being conducted in parallel, with several vulnerabilities identified as a result.

Delivery of Results

At the conclusion of testing, the team gathered evidence, documented step by step walkthroughs of each exploit, developed remediation recommendations, and compiled the complete results into the formal PCI DSS penetration test report. This report was subjected to QA to ensure quality and completeness, then securely issued to the customer for advance review.

The HALOCK project manager also coordinated a follow up review meeting with stakeholders identified by the customer as involved in remediation planning. During these meetings, the findings, recommendations, and next steps were discussed. During these discussions, new information emerged. Namely, it was determined that the specific franchises compromised during the penetration test were all located in a region outside the coverage of corporate field support. As such, a third party had been contracted to manage the environment. This shed light on why these environments did not exhibit the same security protections as the rest of the target environment.

It was also determined that the e-commerce website had recently been updated by a different third party with all identified vulnerabilities being observed in the recently updated areas of the web application. While the technical recommendations were important and would be implemented by the customer, these additional insights established root cause that also influenced operational and procedural remediation activities to address third party oversight.

*Samples available.

A PENETRATION TEST CASE STUDY

RETAIL

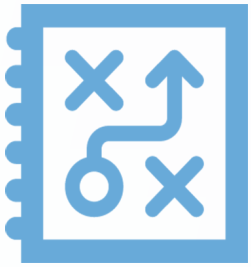
Post Assessment

Following remediation, HALOCK reengaged to conduct the remediation verification test. Each vulnerability was retested to independently confirm remediation was successful. The detailed report was updated to reflect successful remediation (as was the case). This report was retained on file as evidence in support of the broader compliance validation.

The follow up segmentation verification test was also scheduled to be performed six months later, as required of Service Providers. With testing complete, the compliance validation finalized, and the necessary attestation and reports filed, HALOCK and the customer took the opportunity to discuss some lessons learned. While the testing and compliance went very smoothly as planned, some opportunities to gain some efficiencies with compliance management and subsequent validation were identified.

Several minor enhancements to network segmentation were observed that would reduce the scope of compliance. Additionally, several legacy hosts were identified within the cardholder data environment, and therefore subject to the complete requirements of the PCI DSS, that were no longer required. These hosts would be decommissioned, further reducing the surface for attack as well as operational overhead in maintaining hosts no longer required. At the conclusion of the annual validation cycle, the customer determined that a significant cost savings had been realized.

This was attributed to several factors. Working with HALOCK, the project was efficient and well managed, reducing the duration of compliance validation by half. This allowed resources to return to business development and revenue generating projects quicker. Second, reductions in the scope of compliance validation with segmentation and scope reduction reduced both hard and soft costs associated with managing the cardholder data environment.



Finally, by implementing several key recommendations HALOCK provided, allowed the customer to not only reduce remediation activities, but also maintain the remediated state with reduced overhead.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

www.halock.com