Protect Retail Operations with Security Threat Risk Assessment

Our client, a large mobility telecommunications service provider, needed to assess the security risks associated with their retail outlets including their Point of Sale (POS) systems and physical infrastructure. These systems and locations contained confidential customer information that are critical to driving new revenue, providing an excellent customer experience and preserving the integrity of the service provider's brand.

CHALLENGES

- As with any business, the retail outlet provides one of the most visible 'faces' of the organization that not only needs to be open to the general public , but also needs to be highly secure - thereby introducing other uncontrollable variables into the mix
- The security framework and recommendations for improvement needed to balance the requirement for an open environment with the preservation of sensitive information

Client / Telecommunications Service Provider

Security Threat Risk Assessment (TRA)

MARINER

APPROACH

Mariner security team provided a full security assessment of IT operations, procedures, and processes including penetration and vulnerability testing of the existing IT infrastructure at several retail locations. Physical security testing was conducted. This included reviewing doors, cameras and location of network infrastructure and server rooms.

The analysis was broken down into four key areas:

- Documentation & Configuration Review of IT systems
- Store Lab Penetration and Vulnerability Tests
- Retail Store Visits to review physical security and conduct tests
- POS system source code review

BENEFITS ACHIEVED

Security plan outlining governance level and tactical level security recommendations

The overall report included a prioritized list of recommendations to minimize risk, while maintaining functionality and openness of the IT network and infrastructure in a retail environment.

Practical approach for implementation of the recommendations

Each area to be addressed was given a high/medium/low level of risk and an associated timeline to implement the recommended changes. For example, items listed as High Risk were put on a schedule to be remediated within 14 days with longer deadlines for medium and lower risk items.

Ongoing plan for updating security documentation to follow best practices

Several opportunities for improvement were discovered in various areas of the assessment and these are all being addressed by the client. They engaged in the remediation process and intend to implement periodic TRAs to ensure a consistent secure environment.

© 2021 Mariner Partners Inc. All rights reserved.