Eskan Bank

Core Access Case Study

Eskan Bank selected Core Security to help Eskan focus on its critical assets at headquarters to ensure that they could not be attacked from branch offices or external sources. Key results include:

- Strengthened and simplified its vulnerability management process
- Consolidation and prioritization of a large quantity of vulnerabilities from scanning efforts to an actionable number, leading to more frequent and effective remediation efforts
- A highly secure network with less administrative overhead

Background

Eskan Bank was established in 1979 with a unique social role to provide mortgages for citizens of the Kingdom of Bahrain on low-to-medium incomes, and also to engage in community-related property development activities. Eskan Bank is the Kingdom of Bahrain's leading provider of residential mortgages, and a significant player in the property development market. Since inception, the Bank has provided mortgages totaling BD 663 million benefiting 46,719 Bahraini families. Eskan Bank's property development and investment activities embrace real estate investment, construction and property management; as well as finance for the construction of social and affordable homes, Community Projects and commercial projects.

The Challenge

Eskan Bank performs scans with Tenable Nessus, which results in an overwhelmingly large set of potential vulnerabilities, making it extremely difficult to isolate the highest priority threats. They were reliant on IT operations to consistently apply security patches. Given their current process, focusing on and patching vulnerable systems was a challenge.

Vulnerability and risk assessments were outsourced to a consultancy. Analysis and testing was performed only once a year and the consultants conducted vulnerability assessments on a sample of 25 systems. This left Eskan Bank with an unnecessarily high risk profile. To stem their growing security concerns, the information security team needed a way to comprehensively review potential threats on a continuous basis to ensure that the bank's critical assets could not be attacked.

The Approach

Implementation was completed in less than thirty days, due to the local support of one of Core Security's solution partners Fakhro Electronics as well as support from Core's Master Distributor for the MEA region, Starlink. The Eskan Bank information security team feeds Nessus vulnerability scans into Core Insight for analysis to consolidate and prioritize what was an overwhelming amount of scan data. While there are three branch offices with important assets, the headquarters holds truly critical assets such as the main banking system database, human resources management system, active directory, bank cashier system, and the internal web application server. Eskan Bank needed to be sure that the branch offices couldn't be used as a launch point to compromise any critical assets at the headquarters.

The Nessus scan results were ultimately filtered down by Core Insight to highlight exploitable areas around the network that could lead to critical assets at their headquarters. Further validating these exploits, Core Insight identified potential breach points through attack path simulation. The attack paths generated by Core Insight highlighted the systems that attackers could leverage as pivot points to reach the bank's critical assets. After identifying these systems, the IT operations and information security teams were able to focus and prioritize their remediation efforts on the highest risk systems.

As a final test, Core Impact was deployed for targeted live testing to determine if the headquarter critical assets could be compromised from branch locations. Live testing established that the exploitable sections of their network were sufficiently remediated. This has given an improved sense of security, with the data and test results to support it.

Eskan Bank continuously runs Core Insight on all five VLANs to ensure their security posture is up to date while continuously simulating exploitable attack paths throughout their networks. This has validated Eskan Bank's vulnerability management efforts and helped to prove the low exposure of their IT assets.

As a result of this combination, the information security team now has more valuable and actionable information coming out of their scanner.

The Result

Core Security greatly reduced the administrative overhead and advanced Eskan Bank's vulnerability management program. This new approach to vulnerability management now covers all devices on the network and vulnerability assessments are run weekly on each IP address. The result is comprehensive visibility into vulnerabilities within Eskan Bank and efficient remediation without the burden of managing an overwhelming amount of scanner data.

ABOUT CORE SECURITY

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com