RAPID7

CASE STUDY

INDUSTRY:
Banking

SIZE:
1,000 employees

SOLUTIONS:
Penetration Testing
Nexpose

Air-gapped Network? No Problem. Building Stronger Vulnerability Management at a California Bank

CHALLENGE

- Vulnerability scanning on an air-gapped network.
- Pen testing reports can often be either too complex for the board or too simplistic for IT teams.

SOLUTION

- Rapid7's Nexpose tool has flexible deployment and update options, making offline scans easy.
- The Rapid7 penetration testing approach offers a high-level view for executives and more granular detail perfect for IT teams to dig into.

The financial services sector is no stranger to cyber threats. Banks are consistently targeted by malicious third parties due to the amount of customer PII and sensitive corporate information they hold. Security professionals working in this sector face these challenges against a backdrop of increasingly complex and wide-ranging compliance requirements.

The information security officer (ISO) at one Northern California bank is keenly aware of such challenges. The bank is a $5 billion revenue community lender first chartered back in 1884. With more than 80 branches in the Golden State, it claims to have grown into one of the "most stable" community banks in the country.

Plugging the gap

To maintain that reputation, the ISO knows it's vital to ensure systems are as resilient as possible to outside threats.

"We're a bank, so security here is mainly to protect customer and bank sensitive data against breaching," he says. "We don't want to be another data breach statistic. We want to safeguard our customers' information."

To do this successfully meant building a comprehensive vulnerability management program, but there was one problem: none of the solutions the ISO short-listed would work on the bank's air-gapped production network.

The risks associated with this environment were less acute than those on the internet-connected network because threat vectors are largely restricted to removable media. However, it was still important for him to gain detailed insight into the extent and type of vulnerabilities residing there.

Nexpose, Rapid7's vulnerability management solution, was the only tool shortlisted by the bank that could function without an internet connection. This industry-leading, on-premise vulnerability management software monitors a variety of sources in real-time to provide an up-to-date view of risk, prioritized with a highly granular Real Risk Score for each issue discovered. From there, remediation is a cinch thanks to reporting, which can be tailored to individual IT teams to make the whole process more efficient.

The ISO particularly praised the ability of Nexpose to "go deep" with highly granular scanning and its customization capabilities. In this regard, the product's exception-handling capabilities have been a great help.

The ISO was so pleased with the results that he expanded the scope of Nexpose to cover the bank's internet-facing network, where vulnerabilities are monitored more closely and need to be remediated expeditiously each month before the next scan.

"The [pen test] report was really well done; I presented it to the board and it was well received."

A magical pen test

Buoyed by these successes, the ISO also brought Rapid7 on board to pen test a device the team had set up to send out SIEM alerts straight to their phones, in the event of a serious outage or issue. In the end, the pen tester was unable to hack into the device, but the bank was impressed by the level of detail Rapid7 provided, their suggestions on how to improve security, and the quality of the reporting.

"Everything was good," he says. "You guys brought someone here who was a wizard, and he was frustrated that he couldn't get in, which was cool. The report was really well done; I presented it to the board and it was well received."

Specifically, the report struck a perfect balance in terms of the granularity of detail provided: enough for the board to understand what was going on at a high level, but also with enough detail there for IT to dig into.

A better program

There's still some configuration to do before the bank can reap the full benefits of Nexpose on its production and internet-facing networks, but the ISO is excited to try some of the more advanced features—including dashboards, agents, and remediation projects—as well as hooking it up to the bank's SIEM solution.

However, Rapid7 and Nexpose has already helped his team of seven take a more rigorous approach to vulnerability management.

"Before, we had one scanner and it would come up with certain vulnerabilities. There wasn't a lot on the internet side, and we would fix them and go with it," he explains. "Then we got Nexpose on the production network and thought 'Wow, there are a lot of vulnerabilities here.' Maybe it's because they're not on the internet and the patching is done a little differently."

"Putting that other instance on the internet side and seeing the difference between the scans has really made us think," he concluded. "It's helped us start to build a better vulnerability management program."