Financial Services: Protect customer data from cyber-attacks

Financial Services Industry

A customer's financial information is precious to both consumers and the organizations that handle them – and an appealing target for cyber criminals. Financial services institutions must defend against attacks that are becoming increasingly frequent, sophisticated, and widespread.

98%

According to the 2016 Verizon Data Breach Investigations Report (DBIR), financial sector systems were compromised in minutes or less in 98% of cases.

Security challenges faced by financial institutions

- Complex and distributed IT infrastructure with legacy and difficult to patch systems.
- Reliance on third-party vendors for critical banking functions and inability to verify their security.
- Overwhelming number of alerts resulting in failure to spot genuine indicators of compromise.
- Constantly evolving industry, state, federal and international regulatory compliance requirements.

Reduce threat exposure

Financial institutions need to understand their weak points across servers, endpoints, mobile devices and web assets in order to reduce risk of a breach. Web application attacks made up 48% of all security incidents in financial services (Verizon 2016 DBIR).

Rapid7 Threat Exposure Management solutions can help you:

- Identify threats as they emerge including vulnerabilities, controls gaps and configuration issues.
- Prioritize risks based on business criticality, the threat landscape, and real-world attack exposure.
- Dynamically assess modern web applications for vulnerabilities and continuously monitor for changes.
- Conduct a penetration test to uncover weaknesses and verify security controls effectiveness.

Keep financial data safe

In the financial services industry, 15% of security incidents remain undiscovered for months or more (2016 Verizon DBIR). During this time, attackers are stealthily moving across the network to identify and access valuable targets. It's not enough to simply prevent attacks and identify malware; financial institutions need to detect and contain threats that use multiple attack vectors before critical assets are breached.

Rapid7 Incident Detection and Response solutions can help you:

- Detect attacks earlier in the attack chain, including top attack vectors like compromised credentials, malware, and phishing.
- Investigate and respond to incidents quickly to stop attackers before damage is done.

"Rapid7 Nexpose is simple to use and still meets the bank's security needs even after the organization doubled in size. Today Bridgehampton National Bank receives stellar audits and relies upon Nexpose to scan hundreds of workstations and a virtualized server environment."

Thomas Simson
Chief Information Officer, Bridgehampton National Bank

- Integrate with existing network and security solutions for endpoint to cloud visibility, log search, and compliance use cases.

Increase confidence in your security program

Financial institutions need a flexible and comprehensive security program to protect against emerging threats and meet regulatory requirements. A good security program needs to align to business goals, industry standards and compliances, and mitigate threats specific to each organization.

Rapid7 Security Advisory Services can help you:

- Perform a gap analysis of your program against a security maturity model and industry best practices.
- Develop strategic and tactical road maps, including a prioritized set of security initiatives.
- Create executive scorecards to measure security improvement and drive risk reduction over time.

Simplify compliance efforts

Regulatory compliance is a continuing challenge for the financial services industry, and the number 1 factor driving security spend (New York State Department of Financial Services). In the face of growing cyber threats, compliance requirements are continuing to evolve and audits are becoming increasingly rigorous.

Rapid7 solutions can help you:

- Automatically audit the network against requirements for risk, vulnerabilities and configurations.
- Demonstrate compliance with standards such as PCI DSS, FFIEC, NIST 800-53, and ISO 27001.
- Perform web application scanning and generate reports as required by PCI DSS, SOX, GLBA, and more.
- Achieve PCI DSS compliance with quarterly vulnerability scans by an Approved Scanning Vendor (ASV).
- Perform internal and external penetration tests with detailed remediation advice and reporting.
- Monitor user access to systems containing personal information regulated by data privacy laws.
- Deliver customizable user security training to increase awareness of security risks and responsibilities.
- Identify gaps in security policies and controls against various compliance standards.