NOPSEC

Financial Services - Vulnerability Prioritization

A Use Case to Manage Risk and the Sprawling Attack Surface

The Problem

The cybercrime onslaught of financial institutions is continual, relentless and costly.

$5.72M[1]
average cost of breach

The financial services sector has the second highest average total cost of a breach – behind only healthcare, according to the IBM Cost of Data Breach, 2021

520%[2]
increase in attacks

Banks experienced an increase in phishing and ransomware attacks between March and June 2020

>100[3]
organizations affected

Targeted ransomware attacks on financial institutions are gaining popularity with cybercriminals, 70% of such attacks come from the Kyptik Trojan malware and the Android-attacking LokiBot trojan

Of course, financial institutions make an attractive sector for cybercriminal activity because the nature of their products and services. But the rapid digital transformation and shift to remote work that the pandemic brought on has meant a far wider attack surface, one that is difficult for security teams to fully account for, let alone protect.

Additionally, the ever-growing list of common vulnerabilities and exposures – a record 18,378 tabulated in 2021[4] – puts greater pressure on SecOps and IT to keep pace, prioritize and remediate before damage is done.

Failing to respond in a timely and effective fashion by not equipping themselves with the right tools can cost financial institutions millions more on average than otherwise.

The Challenge

The new paradigm of remote workers and devices is likely to remain a near-permanent feature of financial institutions. With growth and possible mergers of organizations, the attack surface is likely to become even wider and potentially more vulnerable.

Cybersecurity professionals remain in short supply globally, so it is difficult to adequately respond to threats by relying primarily on human intervention.

Tool sprawl as well as siloed corporate infrastructures add complexity and lessen the visibility of risks, resulting in unduly complex threat-response processes.

The Solution

NopSec's Unified VRM gives financial institutions the critical functionality they need to manage their sprawling attack surfaces and vulnerabilities.

The Cost of Data Breach Report, 2021, from IBM Security notes that organizations that had 60% of their employees working remotely had a higher than average cost[5] of a data breach. They recommended products and services that would give security teams deeper visibility into endpoints so they can quickly investigate suspicious activity and isolate breaches before too much damage can be done.

NopSec's Unified VRM

Key Functions

1. **Monitoring**
   Continuously observes a variety of hybrid environments externally and distributed ecosystems (such as cloud services and external-facing on-premises infrastructures), including all those potential entry points posed by your remote workforce
2. **Asset discovery**
   Discovers and maps unknown external-facing assets and systems to the organization to include shadow IT, unmanaged assets, and internet-facing devices from outside the organization that may be connected to the corporate network
3. **Analysis**
   Evaluates and analyzes asset attributes to determine if an asset is risky, vulnerable, or behaving in an abnormal way outside of the normal baseline
4. **Prioritization**
   Prioritizes risks and vulnerabilities and provides alerts based on prioritization analytics
5. **Remediation**
   Provides automated action plans on the mitigation of prioritized threats with embedded native detection and response capabilities

Key Features

NopSec Unified VRM uses patented Machine Learning algorithms to precisely calculate the risk of vulnerability exploitation on your network. Go beyond standard scanner and CVSS scores to identify and rank the criticality of your vulnerabilities. Eliminate security vulnerability overload with a single risk score.

Correlates Scanner data with 30 threat, exploit and social media feeds

Patented Machine Learning predicts the likelihood of exploit

Uses Asset Criticality from your CMDB or UVRM calculates it for you

Configurable rules for SLA assignment

With Unified VRM, your team responds to the vulnerabilities that matter and ignores the ones that don't. Beyond that, it gives you the ability to proactively assess, manage and report any weaknesses before they're found by cybercriminals. With its powerful automated capabilities at your disposal, you dramatically reduce the burden on your security team, lessen potential damages and increase your overall effectiveness as a security team.

Contact NopSec for a demo today.

[1] Cost of a Data Breach Report, 2021, IBM Security, p. 15; [2]"5 ransomware trends that should alarm banks," Penny Crosman, Oct. 6, 2020, *American Banker*; [3]"Top Security Threats Facing Banks in 2021," Doron Gez, Feb. 2, 2021, HUB Security; [4]"With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers," Jonathan Greig, Dec. 8, 2021, ZDNet; [5]Cost of a Data Breach Report, ibid., page 59.