Cybersecurity Case Study

RESULTS Technology

This small, home town bank in Texas experienced dramatic improvements to its cybersecurity environment within five months of installing RESULTS new cybersecurity tool, Invicta VPS.

Prior Environment & Challenges

This bank relied on annual external IT audits to conduct internal vulnerability assessments and IT security reviews. Although they had the usual security policies, logs, monthly reports and controls in place, they had no tools to actively monitor for changes in their network, user behavior and policies.

Each year brought a list of "new" vulnerabilities from the audit report that had to be reviewed, researched and remediated.

These vulnerabilities could have been resident on their network for up to the full year between assessments.

Then the bank added Invicta VPS to their cybersecurity program...

The Solution

RESULTS Invicta VPS is an enhanced Cyber Security Tool crafted for businesses that require optimal protection from threats to their IT systems, critical data and their clients' data. This Vulnerability Protection System is designed to meet a majority of regulatory compliance (HIPAA, FFIEC, PCI, NIST, and more) requirements for system hardening, intrusion detection, vulnerability analysis, and reporting.

Invicta VPS works in conjunction with RESULTS' RITA Solution with IDS and IPS, anti-malware, data backup, security awareness training, and patch management to provide the highest level of information security and regulatory compliance.

The Result

Once the Bank installed Invicta VPS, key monitoring components were installed immediately, internal scans initiated and vulnerabilities were remidiated. Over the next two months Invicta VPS "learned" what was normal and acceptable network behavior and then sent active alerts directly to designated bank officers. The full implementation includes these features:

1. Enhanced security hardening policies were applied to all servers and workstations, and required exceptions were clearly identified (eg: workstations where USB drives may need to be used).

   Invicta enforces over 55 hardening policies on workstations and servers to ensure that only legitimate changes and activities are permitted, and monitors every 5 minutes to verify compliance.

Invicta VPS detected encryption activity and immediately isolated the affected device, sparing the bank from potential disaster.

2. A Ransomware Monitor was installed on all workstations that instantly detected the beginning of encryption activity and isolated the affected device from the network before the damage could spread.

3. A network configuration baseline was established to allow Invicta to recognize changes to the network and generate alerts on unexpected changes or additions.

   Invicta established policies for "normal" network activity to identify unusual behavior that generate alerts. For instance, an alert may generate for a user that logs onto a workstation that they do not ordinarily use or at a time unusual for them.

4. Active Directory was monitored daily for changes to users, policies, and administrative access so officers in the bank could be alerted and confirm all changes.

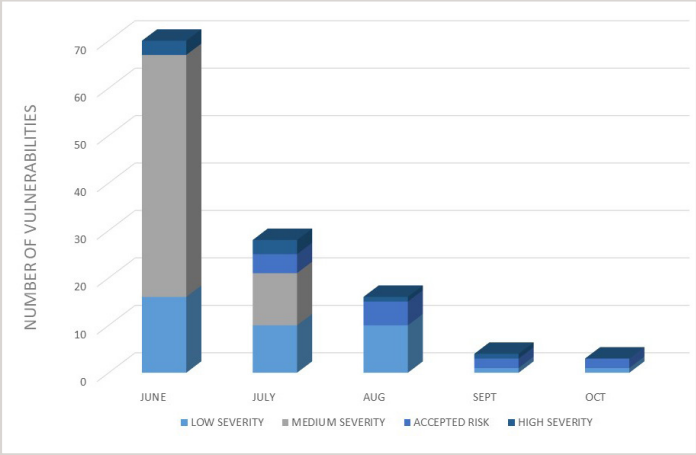
5. **An internal vulnerability scan ran weekly** on all network devices and the RESULTS security team immediately began remediation of identified issues to keep the network proactively safe.

6. **An advanced antimalware agent was added to all workstations and servers** that constantly monitored worldwide events to identify emerging threats requiring "zero day" responses.

   Invicta's advanced breach detection technology finds footholds that anti-virus can't. It detects keyloggers, trojans, spyware, unauthorized registry changes, or other malicious activity.

7. **Weekly and monthly summary reports were generated** for inclusion in IT Committee minutes and board reporting, guaranteeing that the right people in the bank know at all times their network is secure and actively monitored.

8. **External vulnerability scans were scheduled to be conducted quarterly** on all internet connections to verify that firewall settings using a hackers point of view. Any "holes" were immediately closed. This table illustrates the progression to a clean, safe network for the bank over time.



This graph illustrates the bank's progression to a clean, safe network over a five month period.

About RESULTS Technology:
RESULTS Technology is a leading provider of proactive IT solutions for small and midsized businesses. Founded in 1992, our full-service technology solutions provide proactive IT security and compliance for regulated industries across the Midwest. RESULTS Technology is consistently ranked as one of the best IT firms in both Kansas City and St. Louis.

877.435.8877
www.resultstechnology.com
RESULTS Technology