Fidelis Cybersecurity

CASE STUDY

First Midwest Bank Uses Fidelis Deception* to Detect and Respond to Security Anomalies

About First Midwest Bank

Operating through more than 110 branches in the suburban metropolitan Chicago market, NW Indiana, Central Illinois, and the quad cities, First Midwest Bank is a community bank that attracts deposits, makes loans and provides wealth management, investment, and retirement-plan services. The bank's clientele includes a diversified mix of industry groups, including manufacturing, health care, pharmaceutical, higher education, wholesale and retail trade, service, and agriculture.

Regulations and Information Security

First Midwest Bank operates in an environment of growing industry and information security regulation. For example, the bank is subject to the Federal Financial Institution Examination Council's uniform principles and standards for financial institutions and its processes are periodically tested for compliance with a litany of laws and regulations. As an issuer of credit and debit cards, First Midwest must comply with the Payment Card Industry Data Security Standard (PCI DSS), a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. First Midwest must also comply with other standards, including HIPAA (Health Insurance Portability and Accountability).

"First and foremost, we have to protect client information, the bank's proprietary information, and employee information," states Weston Nicolls, SVP, Information Security Manager. "Personal and financial data are considered Personal Identity Information (PII) and are subject to privacy law."

Beyond the risk and damage from potential financial information leakage, security breaches could place the bank in a highly undesirable noncompliance condition that could jeopardize its long-term health.

Benefits

- Compliance with information security regulations
- Superior real-time visibility and insight into potential risks
- Quick and easy deployment
- Automatic and transparent to users, networks, and applications
- Detailed forensics covering the entire progress of the attack

Information Security as We Grow

First Midwest's operating environment is expanding and multiplying in complexity. As a growing bank, it continues to add lines of business and incorporate new 3rd- party applications, making the environment increasingly complicated. At the same time, the accelerating US regulatory environment continues to place higher information security demands on banking institutions.

As the person in charge of information security, Nicolls clearly understands the challenges facing the banking industry in general and First Midwest in particular.

"Keeping on top of everything, especially new technologies, changes in the business, and making sure that security controls are addressed as we grow are my consistent challenges," he declares.

Good visibility of the use of information across the bank's myriad operations is becoming more difficult, requiring extra time and effort and better tools. Nicolls notes, "We need tools that give the team timely, preemptive intelligence across our operations. We can't be surprised."

*formerly Topspin DECOYnet

"We found Fidelis Deception* to be very efficient. Its decoy aspect provided an excellent way to detect anomalies without having to sort through so much data as with other approaches"

~ Weston Nicolls, SVP, Information Security Manager

To achieve its security goals, First Midwest implements many levels of information security measures to prevent the escape of personal and other critical data. And, like so many other financial institutions, First Midwest cannot rest on its laurels as the environment continues to get more complex.

A New Type of Solution

Upon witnessing it in operation, First Midwest determined that Fidelis Deception would provide several necessary security enhancements to its already formidable arsenal of information security tools. "Right away, we really liked the real-time visibility," enthused Nicolls.

After a quick and easy deployment in the First Midwest network, Fidelis Deception began to map data activity throughout the bank's sophisticated communication channels, endpoints, and applications. Automatically identifying complex behavioral patterns throughout the network, Fidelis Deception quickly assembled a real-time view of all communication channels and network activities.

"Fidelis Deception provides a novel approach to viewing our data traffic, all the activity going in and out," asserted Nicolls. "We learned new essential specifics like where we have potential leakage problems that we didn't know about before."

Fidelis Deception provides a clear and accurate view of attackers' movements and activities. Not based on black and white lists, it goes beyond other tools, protecting against malware that has not yet been identified anywhere.

Efficient Use of Resources

The First Midwest Bank security architecture includes firewalls, IPS, and gateway/proxy technology. The bank deploys many layers of control in its data-center perimeter and maintains aggressive internal controls. Despite all that, perfect security is an ongoing battle. First Midwest's information security team does not have unlimited resources. They require tools that promote information security without wasting a lot of time.

"We found Fidelis Deception to be very efficient," declares Nicolls. "Its decoy aspect provided an excellent way to detect anomalies without having to sort through so much data as with other approaches. As soon as you see some activity chase after the decoys, you know that's an activity worth monitoring. This is much more efficient than other types of solutions — like having a SIEM and collecting loads of logs from various systems and spending tons of time looking for something unusual."

Fidelis Deception focuses on the security problems that are vital to information security teams. It identifies and mitigates highly complex attacks while practically eliminating false alarms. The solution provides invaluable risk-assessment data, anticipating attacker intentions based on actions, lateral movements, and access attempts. The accumulated information can be viewed via the user-friendly dashboard, and can be sent to or incorporated into any existing Security Information and Event Management (SIEM) software.

*formerly Topspin DECOYnet