Komerční banka

Reducing logins from malware-infected endpoints by 90 percent in just three months

Overview

The need

With its existing security solutions unable to stop malware-based attacks, KB executives sought a specialized solution that would protect its clients from this dangerous threat.

The solution

The bank uses advanced fraud and malware protection solutions from IBM that help detect, block and remediate malware infections, and detect phishing threats before online financial fraud can occur.

The benefit

The solution surpassed the company's expectations, reducing the number of online banking logins from infected endpoints by 90 percent and preventing 200 potential fraud attempts in just three months.

Komerční banka, a.s. (KB) is a leading bank in the Czech Republic and in Central and Eastern Europe, serving more than 1.6 million clients. The bank, which is a member of the Société Générale Group, offers a wide range of retail, corporate and investment banking services.

Combating a surge in financial malware attacks

In the autumn of 2013, banks in the Czech Republic, like many banks worldwide, saw a surge in malware-based attacks. As KB executives assessed the threat landscape and bank security, they saw that their existing security solutions would not protect their clients from these threats. “We needed specialized tools focused on online financial fraud and malware to resist these malware-based attacks,” says the lead business architect, Channels & Customer Intelligence, Marketing and Communication, KB.

Following deployment of IBM Security Trusteer solutions, KB saw a 90 percent reduction in online banking logins from infected endpoints in just three months. Word of the team's success spread quickly across Société Générale. “We received many calls from colleagues asking how we achieved the success we did,” says the lead business architect from the bank's Channels & Customer Intelligence department.

Solution components

Software

- IBM® Security Trusteer Pinpoint Malware Detection™ Advanced Edition
- IBM Security Trusteer Rapport®

Gaining real-time actionable alerts

KB staff turned to its peers at Société Générale to learn what tools they used to help prevent financial fraud. It was through these conversations that KB decided to implement IBM® Security Trusteer® solutions.

“The Trusteer solutions were proven and operated within Société Générale and they addressed one of the main pillars of our security strategy—client security and fraud prevention,” says the lead business architect on the project.

Using the Trusteer solutions, KB can protect its clients against phishing and malware-driven attacks. The IBM Security Trusteer Pinpoint Malware Detection™ Advanced Edition solution provides KB security staff with real-time actionable alerts when malware-infected devices access the bank’s website. The solution interacts with more than 1.3 million KB online banking users.

The IBM Security Trusteer Rapport® solution can be downloaded by clients to assist with malware removal, as well as to help prevent future malware infections.

“If a client logs in to our online banking system using an infected PC, our call center is immediately alerted by the Trusteer Pinpoint solution and they can alert the client,” explains the project manager, Information Technology, KB. “They can re-credential the clients and they can offer Trusteer Rapport to remove the malware and provide further protection of the client’s desktop. It allows us to act proactively with clients and communicate rapidly when threats are present. We also monitor the information we receive about threats continuously and use this information to further improve the client’s security.”

> *“We needed specialized tools focused on online financial fraud and malware to resist these malware-based attacks.”*
>
> —Lead Business Architect, Channels & Customer Intelligence, Marketing and Communication, Komerční banka

Increasing adoption of Trusteer Rapport solution with comprehensive communications

KB developed a comprehensive communications plan that would help increase client adoption of the Trusteer Rapport solution, which offers frontline protection to help prevent malware infections at the outset.

The communications was delivered in a phased approach to KB clients, employees and media outlets, beginning early in project planning, continuing through development and testing, and even following deployment.

For example, the bank launched an extensive public awareness campaign to clients and media outlets across the Czech Republic that helped increase consumer understanding about online banking security issues, threats, and frauds, and that promoted the bank’s use of Trusteer solutions.

The bank also conducted external communications research through targeted focus groups with nearly 500 of its clients across client segments. According to the team, key findings included the following:

- 9 out of 10 online banking users in the focus group paid attention to communications about keeping their finances safe
- 8 out of 10 of focus group users installed the Trusteer solution if they had all the information they needed

These findings demonstrated the importance of a strong communications program and helped shape the content included in the bank’s security messages.

> *"Clients who have downloaded Rapport have been protected from very dangerous forms of malware."*
>
> —Project Manager, Information Technology, Komerční banka

"In our first communications, we stressed the risks in the digital world, and the point that the end user must protect themselves; the bank is a partner in this effort following KB's brand claim: 'Partnership matters,'" says the bank's lead business architect on the project. "Once we launched the solution, we became more specific and talked about the solutions we offer to help protect our clients."

Preventing fraud before clients are affected

The value of the new solution was seen very quickly following the launch. "In three months, we saw about a 90 percent decrease in logins from infected endpoints to our online banking system, and 200 potential fraud attempts from infected PCs were prevented," says the lead business architect. "This is a major achievement."

Adoption of the Trusteer Rapport solution by KB clients has been very strong, with over 40,000 KB online banking clients downloading the solution in the first three months. For KB executives this was a significant achievement. "We surpassed our original goal for the year very quickly," says the project manager. "Clients who have downloaded Rapport have been protected from very dangerous forms of malware."

Identifying best practices to achieve success

What best practices did the bank use to achieve its success? The team cites three strategies that helped ensure the successful rollout of the solution and strong client adoption.

First, engage senior management personally and build broad organizational support. "We promote client security as one of our strategic values, which is why we look to our CEO and others to be involved and be ambassadors for us," explains the lead business architect. "Our Chief Operating Officer sponsored the solutions' delivery and our CEO and executive director of Marketing and Communication participated in decisions and communications."

The project manager adds, “Our main clients were our Channels and Customer Intelligence, Communication, Transaction and Payment Processing, Call Center, and IT Security departments. We worked in tight cooperation to deliver the solution, and we closely involved a number of other organizations, including Operational Risk, Card Protection, Information Management, and Information Security.”

Second, prepare, test and pilot communications before the solution is rolled out publicly. “We did many focus groups and prepared our communications based upon the feedback,” says the lead business architect. “We also piloted communications with small groups of clients and employees in each of our banking segments. We were concerned with the point of views of both internal and external audiences because both are very important to be successful.”

Finally, monitor direct client feedback along with online posts and media articles, and fine-tune communications on an ongoing basis. “Actively acting on feedback contributed greatly to our success,” says the lead business architect. “And continuous security education and communication will bring continuous success.”

Take the next step

To learn more about IBM Security solutions and services, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

For more information about Komerční banka, visit: http://www.kb.cz/en

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.