BRD-Groupe Société Générale

Reducing risk and strengthening customer satisfaction with advanced fraud protection

Overview

The need

BRD security staff evaluated the need to offer security protections to the customer endpoint, the weak link in banking security.

The solution

The bank deployed advanced fraud prevention solutions from IBM that help detect, block and remediate malware, and detect phishing threats on infected customer endpoints.

The benefit

Improved detection and protection against malware and phishing threats, and faster remediation, help save time, reduce risk and increase customer satisfaction.

BRD-Groupe Société Générale (BRD) is the second largest bank in Romania based on assets and is the leading bank in the Romanian syndicated loans market. BRD serves 2.2 million customers and operates a network of approximately 870 branches.

Addressing the weak link in online banking security

Several years ago, Mihai Andries, Chief Information Security Officer for BRD, sought to proactively expand security protections to the customer endpoint, the weak link in banking security. While the bank had not experienced fraud losses through its online banking channel, Andries and his team believed that it was worth proactively addressing this increasingly at-risk area.

"From the hacker's point of view, the client endpoint is more susceptible to attack than the bank's infrastructure," says Andries. "There are significant browser and operating system vulnerabilities that can be exploited by criminals to intercept traffic, inject fake pages and steal credentials. We wanted to offer our clients an efficient solution that could rapidly detect malware and phishing attacks, and remove any infections."

For BRD executives, prevention is an important focus in the battle against online fraud. "The impact of a loss on a bank's reputation can cost many times more than the loss itself," says Mihai Andries, Chief Information Security Officer, BRD.

Solution components

Software

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

Focusing on the root cause of fraud—malware and phishing attacks

BRD evaluated several solutions before selecting an advanced fraud protection solution from IBM. “We chose Trusteer software based on our comparative analysis, analyst reports and recommendations from colleagues at Groupe Société Générale,” says Andries.

Today, IBM® Security Trusteer Rapport® software is offered as a free download to all of the company’s business customers. The software helps protect users against phishing and malware attacks—including financial zero-day malware—and helps prevent the tampering of online banking transactions to create a safer online banking experience.

In cases where customers have not yet downloaded Trusteer Rapport software, the bank uses IBM Security Trusteer Pinpoint Malware Detection™ Advanced Edition software to help security staff automatically and accurately detect when malware-infected devices are accessing the bank’s website.

“We recommend Trusteer Rapport to our business banking customers to protect against potential fraud and we complement it with Trusteer Pinpoint Malware Detection so that we can deliver protections to all our business customers,” says Remus Oprea, Operational Security Coordinator, BRD.

"Customers who had downloaded Rapport were protected from Dyre malware early on. We were able to inform our executives of this fact and demonstrate how we could protect customers against this new threat as it emerged."

—Mihai Andries, Chief Information Security Officer, BRD

Protecting against emerging threats

Improved detection and protection against malware and phishing threats, along with faster remediation, is helping security staff to reduce risk while increasing customer satisfaction. For example, in mid-2014, when Dyre, an advanced financial trojan that targeted banks worldwide, appeared, Trusteer Rapport software was able to block threats.

"Customers who had downloaded Rapport were protected from Dyre malware early on," says Andries. "We were able to inform our executives of this fact and demonstrate how we could protect customers against this new threat as it emerged."

Additionally, Trusteer software has helped reduce the time required to track, investigate and report on threats—time that can now be redirected to other activities, including customer education programs.

Take the next step

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

For more information about BRD-Groupe Société Générale, visit: www.brd.ro

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
August 2015

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.

Please Recycle