BANCO POPULAR DE PUERTO RICO (BPPR)

Security technology combats phishing attacks and provides strong authentication

AT-A-GLANCE

Key Requirements

- Required by Federal Financial Institutions Examination Council (FFIEC) to introduce multi-factor authentication (MFA) for user access into online banking services
- Risk assessment showed that its existing in-house security system was not adequate to meet these new demands

Solution

- Deployed RSA® Adaptive Authentication MFA for online banking access
- RSA FraudAction™ anti-phishing rolled out to combat an increase in phishing attacks
- RSA SecurID® authentication deployed to secure employee remote access to the corporate intranet

Results

- A dramatic reduction in the number of phishing attacks, with customers now benefitting from peace of mind, knowing that their assets are fully protected
- Time and costs associated with shutting down fraudulent sites have been reduced, meaning BPPR can take a more proactive approach to combating phishing scams

CUSTOMER PROFILE

"Multi-factor authentication and anti-fraud technologies have enabled us to accelerate the speed at which we can identify and prevent phishing attacks in the online channel. Rather than a reactive approach, we are now able to proactively identify fraudsters and shut down fraudulent sites."

CAMILLE BURCKHART, SENIOR VICE-PRESIDENT, TECHNOLOGY MANAGEMENT DIVISION AT BPPR

"We have implemented a risk-based authentication process for our Internet service channel. The system has proved to be very effective. Anti-fraud technology has provided us with a more efficient and proactive way to detect and monitor potential phishing attacks or fraudulent websites which might have a direct impact on our brand and services."

MIGUEL MERCADO TORRES, CISO, VICE-PRESIDENT, OPERATIONAL RISK MANAGEMENT AT BPPR

Banco Popular de Puerto Rico is Popular, Inc.'s main subsidiary and the largest commercial bank in Puerto Rico. It provides the most extensive and complete distribution network in Puerto Rico, with 196 branches, over 620 ATMs, more than 27,162 point-of-sale terminals, a 24/7 call center, and an advanced Internet banking service. To find out more, visit www.popular.com.

KEY REQUIREMENTS

As Puerto Rico's largest commercial bank, Banco Popular de Puerto Rico (BPPR) takes the security of its customers' assets extremely seriously. To authenticate users of its online banking services, BPPR had in place a three-step password system based on its own in-house technology. Customers were asked to answer one of three rotating questions (all previously chosen by them), as well as one set question, before finally being asked to enter a PIN.

While this existing system was effective in preventing phishing attacks on BPPR's existing customers, it was required by FFIEC to introduce MFA. An extensive risk assessment carried out by the bank showed that its existing in-house system was not sufficient to meet these latest compliance demands.

RSA

As a result, BPPR searched for a brand new alternative, an MFA solution that would enable it to meet FFIEC requirements. What's more, it had to find this solution quickly as the FFIEC deadline was looming.

SOLUTION

RSA Adaptive Authentication

Initially BPPR decided to deploy an MFA solution from one of its existing vendors, but found this vendor to be extremely unresponsive. BPPR then reached out to RSA – The Security Division of EMC, and was immediately impressed by RSA's MFA solution, as well as RSA's responsiveness.

RSA Adaptive Authentication leverages risk-based authentication (RBA) technology to identify fraud and high-risk transactions. The system is supported by the RSA Risk Engine, which tracks more than 100 fraud indicators in order to detect suspicious activity. The Risk Engine assigns a unique risk score to each transaction: The higher the score, the greater the likelihood that a transaction is fraudulent.

RSA Professional Services

RSA Professional Services helped with what was a very customized implementation, providing ongoing consultation around how the solution could be adapted to fit the bank's requirements. During the implementation of RSA Adaptive Authentication, BPPR saw a dramatic increase in phishing attacks so BPPR decided to bolster security further by signing up to RSA FraudAction anti-phishing.

RSA FraudAction & Anti-Fraud Command Center (AFCC)

RSA FraudAction anti-phishing is a proven service geared toward stopping and preventing phishing attacks that occur in the online channel. It includes 24x7 monitoring and detection, real-time alerts and reporting, forensics and countermeasures, and site blocking and shutdown.

At the core of the FraudAction service is RSA's exclusive Anti-Fraud Command Center (AFCC). RSA's experienced team of fraud analysts work to shut down fraudulent sites, deploy countermeasures, and conduct extensive forensic work to stop online criminals and prevent future attacks.

RSA SecurID

BPPR has also deployed RSA SecurID two-factor authentication to secure employee remote access into the corporate intranet; approximately 500 RSA SecurID hardware tokens are in use.

RSA SecurID two-factor authentication is based on something the user knows (a password or PIN) and something the user has (an authenticator). It provides a much more reliable level of user authentication than a user name and password, which is what the bank had previously relied on.

Miguel Mercado Torres, CISO, Vice President, Operational Risk Management at BPPR, said: "We were keen to upgrade our solution in light of the increase in cyber threats and cyber fraud activity. By adding in an extra layer of security for access into the corporate intranet, RSA SecurID authentication enables us to increase the number of people who are able to work from home, and also enables the sales team to complete more transactions while out in the field."

RESULTS

Since deploying RSA Adaptive Authentication, BPPR has seen a dramatic reduction in the number of phishing attacks. As a result, customers benefit from peace of mind, knowing that their assets are fully protected.

RSA FraudAction has greatly simplified the process of detecting, blocking, and shutting down fraudulent sites. Previously BPPR's internal staff handled this in-house and found it to be a very time-consuming and costly process. What's more, their approach was reactive, relying on customers to inform them about issues. RSA FraudAction allows BPPR to be more proactive, by enabling them to identify and shut down fraudulent sites before they become a problem.

To further bolster security in the online channel, BPPR is also planning to roll out RSA Transaction Monitoring. RSA Transaction Monitoring is typically integrated at various points within online banking applications in order to monitor high-risk activities such as money transfers, user profile changes, account modifications, and more.

To prevent fraudsters from setting up new customer accounts, in order to commit fraud, BPPR is also looking to roll out RSA Identity Verification to verify the identity of callers into its call center.

"We were keen to upgrade our solution in light of the increase in cyber threats and fraud activity. By adding in an extra layer of security for access into the corporate intranet, RSA SecurID authentication enables us to increase the number of people who are able to work from home, and also enables the sales team to complete more transactions while out in the field."

MIGUEL MERCADO TORRES, CISO, VICE-PRESIDENT, OPERATIONAL RISK MANAGEMENT AT BPPR

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.RSA.com

www.rsa.com

RSA