Auditing IBM i Back Door User Access:

BNC National Bank solves new audit requirement with SafeNet/i

A New Audit Requirement

Like most IBM i shops, BNC National Bank in Bismarck, North Dakota had its IBM i green-screen access securely locked down.

"Menu security was in place; the users didn't have command line access; and we had archived audit journal reports in cold storage. Our auditors were happy with our native IBM i controls," said Bryon Oja, VP, AS/400 Administration at BNC.

What BNC didn't have was audit information and control on back door user access, which is what the auditors asked for in their most recent audit.

In 2013, BNC's auditors introduced a new requirement for the company's annual audit: the auditors wanted BNC to report on and control who was accessing and updating IBM i data using middleware and client server technologies, such as .NET, ODBC, FTP, SQL, OLE, and Microsoft Excel. This request never came up in any previous audits. It was a totally new need, and BNC didn't have any audit journals to record and report on outside system access.

> *"With SafeNet/i, BNC answered a potentially significant audit finding before it became a big issue"*
> - Bryon Oja, VP, AS/400 Administration, BNC

"We needed to get the problem fixed, and we needed to get it fixed quickly," said Oja.

If BNC couldn't find a solution for back door auditing and control, the company would receive a significant audit finding on this year's audit.

The Auditors Agree!!! SafeNet/i Solves the Need

BNC went to IBM for auditing and control advice, and they suggested that the company write its own program for monitoring and securing exit points for back door access. But BNC didn't have time to write a custom program to solve this need.

So BNC looked for a third-party solution for outside access security auditing and control. BNC researched various IBM i security packages, and contacted Rich Loeber, owner of Kisco Information Systems. Rich suggested Kisco's SafeNet/i product, which performs the following functions for tracking and controlling outside access to IBM i systems.

- Request logging for tracking each request coming from a client connecting to an IBM i system

- Audit reports for analyzing which client/server and middleware clients are connecting to a server

- The ability to limit client back door access to server functions, IBM i objects, and remote commands

- Shutting down user access to server functions during off-hours, holidays, or specific days of the week

With SafeNet/i, customers can at any time, go back and specifically see who accessed the system and what they did…and then make changes to prevent any unauthorized access from occurring again.

For these reasons, BNC decided that SafeNet/i was the auditing answer they needed to satisfy the new back-door auditing requirements.

And the auditors agreed!

BNC shared their research with their auditors and the auditors agreed that SafeNet/i would help BNC resolve the audit issue. The auditors particularly liked SafeNet/i's audit reports and said that would answer the new requirements. They accepted SafeNet/i as part of BNC's remediation plan to audit and control IBM i back door access, even before BNC had fully implemented SafeNet/i on their system.

The auditors are happy that BNC will have an outside access audit solution in 2013. With SafeNet/i, BNC is answering a potentially significant audit finding before it becomes a big issue

"SafeNet/i paid for itself in getting the auditors off our back," said Oja.

> *"SafeNet/i paid for itself in getting the auditors off our back"* - Bryon Oja, VP, AS/400 Administration, BNC National Bank

SafeNet/i is Easy to Use and Install

BNC also discovered there was a lot more to SafeNet/i than just producing audit reports.

It was incredibly easy to get SafeNet/i up and running on the system. BNC was able to get the product installed in about 15-20 minutes. BNC was also pleased that it didn't take any special assistance, training, or consultants to start using the product on their system.

"We installed and configured SafeNet/i on our own with just a little help from Kisco. We didn't need to hire anyone to get outside access auditing going," said Oja.

BNC was also pleased with SafeNet/i's product cost and Kisco's technical support. SafeNet/i was significantly less expensive than buying other IBM i exit point security programs, and Kisco support was top notch.

"The manuals are really good. Kisco always researches and gets back to you with an answer," said Oja. "They are patient with our questions, and Kisco rolls up their sleeves and gets right in there with you to get your problems solved."

SafeNet/i sits on top of and works with the IBM i operating system. It doesn't try to take over operating system security. It's tightly integrated with the operating system and works together with IBM i exit point security, rather than trying to insert another layer on top of IBM's world-class security features.

SafeNet/i's approach to security is intuitive with the way that IBM i security works. It mimics the way the operating system security works, using library and object level access and read only-read/write access to objects. The product doesn't contain a lot of new terminology or different security models to learn, which enhances SafeNet/i's ease of use.

SafeNet/i Institutes Control Without Disruption

One of the most valuable things about using SafeNet/i is that BNC can set up auditing and outside access control without disruption.

"We're taking the first 4-6 six weeks to gather information without restricting access," says Oja. "We don't want to stop valid system access by going live with restrictions too soon."

BNC particularly likes SafeNet/i's on-line monitoring feature, which allows them to see when and where access exceptions are occurring. They can set up pre-approved situations for outside access and then use on-line monitoring to identify and deal with non-approved exceptions on a case-by-case basis.
"When we go live with exit point security, the pre-approved people won't be affected," said Oja.

Kisco also reports that the on-line monitoring helps customers like BNC understand all the different points and methods of connection that outside users employ to access an IBM i system.

"So many people say that they have no idea how many outside clients are accessing the system until they start using SafeNet/i," said Rich Loeber. "It's a real eye-opener."

BNC is also using SafeNet/i's modeling feature to configure future settings and understand what's going to happen before they go live with their exit point security. BNC also likes being able to set up security on an exit point by exit point basis. This enables them to set up their auditing restrictions slowly without affecting production in a major way.

> *"So many people say that they have no idea how many outside clients are accessing the system until they start using SafeNet/i. It's a real eye-opener."* - Rich Loeber, Owner, Kisco Information Systems

Results They Can Live With

BNC is happy with what SafeNet/i delivers for access control and auditing for a number of reasons.

- SafeNet/i effectively allows BNC to pinpoint and prevent unapproved outside access

- SafeNet/i provides tracking reports and functions, that can satisfy hard-to-please auditors

- SafeNet/i can send out alerts when there is an intrusion or a broken access rule. Alerts can be sent via text messages, emails, or tweets.

- SafeNet/i is reasonably priced. It's much less expensive than other products

- SafeNet/i is easy to install and configure. It doesn't require expensive consultants to implement a security system

- SafeNet/i provides great technical support that always provides answers to the toughest technical issues

SafeNet/i is an excellent match for BNC's audit and security needs in tracking and controlling outside user access. Even the auditors agree that it can do the job for BNC.

About Kisco Information Systems: Kisco Information Systems provides high quality products and services at a reasonable price to IBM i customers running IBM i, i5/OS, and the OS/400 operating systems. With over 6000 software installation in over 40 countries, Kisco offers solutions for IBM i network security; communications and monitoring; and operating system utilities.

Contact Information: