SECURITY IS TOP OF MIND AT VAI

November 16, 2022 • IT Jungle • Alex Woodie

Kevin Beasley hasn't added "security" to his title yet at VAI, the Long Island-based IBM i ERP software and services provider. But the longtime CIO may just yet, considering all the security activities he's overseeing for VAI's on-prem and cloud customers alike.

"We're constantly looking at new things," Beasley tells IT Jungle. "Obviously, the security landscape out there is phenomenally dangerous. There was a local government attacked here, and we're constantly working on security."

The top threat at the moment is ransomware, which is typically perpetrated through email or text phishing schemes. Nearly a dozen VAI customers have been hit by ransomware in just the past 18 months, Beasley says. While none of the recent attacks breached the IBM i server at the heart of an S2K deployment, they did compromise some of the outer layers of the companies' security apparatus.

The message is getting out, Beasley says. Security is a big deal, and customers are taking notice. That's a good thing.

"As recently as a couple of years ago, during the big attacks like Colonial Pipeline, a lot of customers, especially SMBs [small the midsize businesses] said, 'Ah I don't have to worry about that type of problem. They're only going after the big guys,'" Beasley says. "Well, they go after everybody's nowadays. Big, small it doesn't matter. Lately, they've been targeting governments."

VAI has always taken security seriously. Some IBM i ERP software vendors are bit lackadaisical when it comes to IBM i configurations, but you won't find VAI users operating under powerful user profiles like QSECOFR or working with ALLOBJ security.

"Obviously we encourage people to move away from certain protocols, like SMB [Server Message Block], or at least have something that's going to do some inline scanning of things like that," Beasley says. "In our applications we offer a replacement option for customers who don't want to do mapped drives and file shares. It's an application we wrote that would replace it. It still can be launched from the IFS, but it's being launched through a Web browser and through security settings, with various different levels of authentication."

Having a good software architecture running atop IBM i – one of the most hardened operating systems around – can give IBM i shops piece of mind. When the security administrator locks down the rest of the platform – which is something that VAI does for its cloud customers and which it recommends that on-prem customers do for themselves – it can present a very resilient defense.

"IBM i stands up pretty good," Beasley says. "You still have to make sure you have your security set correctly. Many times in the IBM i world . . . if it's not completely public facing, you have to worry more about internal security, whether you're going to get hit with ransomware, and do you have everything in your authorities correctly set and so forth."

While the IBM i side of the house is mostly under control from a security perspective, it's the other components that worry Beasley. It's ensuring the network edge is sufficiently protected, that you're on top of new vulnerabilities, that you're applying patches, that the Web application firewalls are updated and functioning, that you're looking for spoofing and any traffic that could be impersonating you.

But it's been forced to up its game in response to the situation on the ground. Considering the threat that phishing poses to potential ransomware attacks, user training is a big deal. VAI conducts training sessions every couple of months to help educate its customers on how to avoid. Even so, ransomware attacks are still successful. "It happens all the time," Beasley says. "You just don't hear people talking about it."

VAI already conducts periodic system audits and has contracts with penetration testing provider to check the security of its systems. Those provide a good point-in-time reference for security, but Beasley wanted something that could work in a more real-time manner.

"It's like when you're doing a data backup. You're backing up. It's a point in time," he says. "We're looking at what's going on out in the security world that is the security equivalent of continuous data protection, or high availability."

To that end, VAI is now contracting with additional security professionals who can actively work to penetrate the system, in a "red team-blue team" type of configuration. The company has brought in some folks with high-level security experience, including former military, to help them take security to the next level. This gives Beasley and the VAI leadership team more confidence that they are doing everything they can to protect their clients' valuable data.

"We wanted to . . . ensure that we're secure [by] using red-team types tools that simulate what an attacker would really be looking for," he says. "Not just a simple weakness. You can patch this, and we do patching and everything else. But sometimes, what a blue team might think is what's being targeted might not be what our red team might be looking at."

VAI has also contacted the Cybersecurity & Infrastructure Security Agency, a federal agency in the Department of Homeland Security. According to Beasley, CISA will assign a security advisor to work with American companies free of charge.

"Obviously they're on top of everything," he says. "But being in contact with them obviously and having an advisor that we can reach out to when we need to" has been beneficial.

The majority of new sales for VAI today are occurring in the cloud. Part of the reason for that is doesn't require the customer to have as many technical skills, which for an IBM i software developer, is a good thing. But the other part of the cloud equation is that it actually provides a more secure environment, Beasley says.