KEY RESOURCES
The Key to zSystems Integrity

CASE STUDY

After Suffering a Breach, an Insurer Automates Mainframe Security Checks

CHALLENGE

- Curb excessive access on the mainframe.
- Reduce drifting from internal security policy guidelines.
- Comply with the requirements of a third-party audit.

SOLUTIONS

- Implemented z/Assure® CAM to automate tailored security checks.
- Used custom parameters to identify and correct drifting and misconfigurations.

BENEFITS

- An automated, process that scans for drifting, excessive access and other configuration issues.
- Realigning mainframe security settings with company security policies.
- A no-frills solution tailored to the company's specific needs that can be learned quickly.

Global insurance companies collect millions of pieces of sensitive information from their policyholders, including names, addresses, social security numbers and employment data. This information is often stored within the mainframe because of its security and reliability. Even so, a number of insurers have seen sensitive data exposed after being compromised in a data breach, resulting in both public embarrassment and hefty financial penalties, as high as $115 million in one prominent case.

After suffering a data breach, one national private insurer turned to Key Resources, Inc. to close a critical mainframe security gap and shore up its data security estate.

An Inside Threat Exposes a Gap

This insurance company, which has offices in North America and Europe, suffered a data breach. The company enlisted a third-party consultant to audit the situation and determine how to make sure it wouldn't happen again.

The insurer had long followed mainframe security policy guidelines which, among other things, specify who in the organization is authorized to view or make changes to secure data sets. At some point, its mainframe configuration settings had deviated from the security policy's guidelines. This drifting opened up an excessive access vulnerability for a rogue employee to exploit.

To close this gap, the auditor recommended an ongoing excessive access checking process, to ensure that unnecessary access is not granted to sensitive data sets and to limit drifting in the future. This process would need to check access privileges based on the company's security policy, which at the time of the breach was only written on paper. Time was a priority – the company needed to plug this significant security gap quickly.

"What we wanted was something simple: none of the bells and whistles, just a solution that was straightforward and our team could pick up and run with," said the insurer's CIO.

Improving the Security Check Process

Having collaborated on security scans in the past, the CIO knew he could trust Key Resources to help. He asked for a customized tool that could focus on only the most relevant configuration and access data, rather than every configuration setting across the system.

> "Key Resources understands the mainframe inside and out, and the potential problems it can pose. They knew exactly what kind of problem we were dealing with, and knew exactly what they had and what we needed to resolve that problem, with the level of specificity it required."
>
> CIO

Key Resources recommended customizing its z/Assure® Compliance Assessment Manager (CAM), a mainframe security configuration and compliance management solution, to align the insurer's configuration settings with its internal security policy.

The first step was to digitize the company's security policy, inputting key security parameters directly into z/Assure CAM. These parameters formed a baseline, against which z/Assure CAM could automatically check for signs of drifting. A report tells the insurer exactly how far they've drifted from the security policy, allowing its IT staff to find and close security gaps.

"We've found the product very easy to use and are very pleased with the specificity that the report provides us for meeting our compliance requirements," the CIO said.

From there, the insurer was able to automate additional access checks. With its scheduling function, z/Assure CAM can be set up to operate on a predetermined schedule, to more proactively weed out excessive access and curb potential future breaches.

Laying the Foundation for Better Security

In the end, Key Resources was able to provide the insurance company with a customized version of z/Assure CAM that was up quickly, and allowed the company to both meet its compliance deadline and follow through on next steps. The automated access checking process also means that the insurer will be able to protect against future incidents of unauthorized access on the mainframe, limiting exposure to costly data breaches.

"We're planning to expand our usage just as soon as we've reviewed our procedures and our personnel are all completely comfortable on the new processes," the CIO said. "We are now more adept at identifying, classifying and fixing misconfigurations, thereby reducing breach risks."

Key Resources Inc. has decades of expertise providing software, services and consulting to enterprises running critical apps on IBM® z/OS. We help CIOs, CISOs and programmers take control of mainframe security so they can protect their data, avoid costly breaches and maintain regulatory compliance.

Contact Key Resources

Call 1-800-574-1339 ext 701

Visit www.krisecurity.com/contact