DATA SECURITY
SharePoint File Access Breach

CASE STUDY

A breach on an HR file caused a Software CEO to call into question access on all SharePoint files.

The Environment

The Software firm had an understaffed internal IT team that was pre-occupied by end-user support initiatives. The IT team did not have the bandwidth or resources to keep up with, or discover on their own, the network permissions within each folder or document or the access level of every employee - past and present. Verifying the security they had put in place on folders and the files within them was a daunting task. They knew that there were holes, just not certain where, and not sure how to prioritize this project into their already busy schedules.

> *73% of IT security teams are understaffed, and CISOs are turning to automation for help.* - *Tech Republic*

The Event

A routine SharePoint alert on a Human Resources file was sent to the CEO providing the name of the employee who had accessed the file. It was by chance the CEO even opened the alert as the volume of Sharepoint alerts can easily grow and be neglected. As suspected, this HR file contained sensitive employee information. The employee in question should not have been granted access to the HR file, much less the entire folder. The CEO did not treat it as an isolated event. Rather, he called into question the security on every folder and file within the company's Sharepoint instance, and called for a review of all employees' access levels.

Identifying Where the Problems Are

Fixing this critical problem with limited resources would be a challenge. The software firm knew fully that any environment with more than 10 users is going to struggle with effective permissions as there are so many variables that come into play - security groups in Active Directory, owner of the files themselves, global administrators in Office 365, domain policies, etc. All of these factors affect permission, and taking all those into account for every user and every file is virtually impossible to manage without an automated data security platform.

CLIENT PROFILE

Industry:
Software Development

Number of locations:
1 headquarters location

Number of employees:
<50

Multiple remote employees and contractors with system access

Data Security Case Study

Enter RSI

The client's technology partner suggested that they approach the problem with RSI's automated data security solution that would discover, monitor and report the data usage permissions and behaviors across the organization's entire IT environment, not just SharePoint. By doing this they would have a single report that would be generated on a scheduled basis that would provide the high level data points for the CEO so he knows remediation is being made. Additionally, reporting would provide drill down to details for the IT team to show where issues are and to prompt more remediation.

Data Security Implementation

From an IT perspective, installation of the RSI Data Security platform went quickly. It has minimal requirements that are achievable by even a small IT team because of "pre-packaged" functionality for virtual or physical deployments. RSI layered the support of a data security specialists to accelerate implementation and they were able to install and configure the application within a one-hour call with the IT team of the client. Once it was set up the IT team was able to re-asses after a few days of gathering data. The RSI data security specialist ushered the client through the entire process for report interpretation and remediation guidance.

After running data through RSI's Data Security platform for only a few days, initial results showed that their situation was actually worse than originally thought.

What Was Found

- Users with unauthorized admin rights to critical and sensitive applications
- Thousands of failed logon attempts
- Hundreds of passwords without expiration dates
- Numerous dead service accounts and unused system default accounts
- Various other high risk data points

Remediation

Because the report provided information across the entire environment, cloud and on premises, the client was able to start remediating immediately. By having RSI at their side to interpret the data and guide the client, prioritization of tasks happened immediately. The report provided recommendations regarding how to remediate each risk and sorted the risks into high, medium and low categories. The client IT team and RSI's data security specialist worked together to create a data security roadmap to remediation. A weekly high-level report was created to automatically generate so the CEO could monitor progress to reduce the highest risks.

Conclusion

RSI's Data Security platform helped our client identify and track sensitive and important data in real time. They can now detect potential data breaches and prevent them by monitoring, detecting and blocking sensitive data while in use, in motion, and at rest. With the support of RSI's data security specialists and Managed Security Services, remediation steps have been identified, prioritized and in implementation.

> ***RSI's Data Security platform and implementation services were delivered as sold - true, easy-to-use data security and auditable data classification.***
>
> ***- CEO***

About RSI: Since 1982, RSI has provided innovative technology solutions, advanced professional services and fully automated solutions for effective business workflow. With RSI, clients realize that relationships matter, and our quality is embedded into our culture. Through our proven Assess-Remediate-Maintain process, RSI helps clients manage complexity and drive a return on your IT investment. We serve the enterprise with proactive cyber security solutions, custom software development for business process improvement, and advanced IT operations to create greater efficiencies. RSI uniquely supports remote data collection through advanced drone flight services.

rsitex.com | 512-600-3200 | 24/7 Support: 512-334-3334 | 5426 Guadalupe St, Suite 100 | Austin, TX 78751