CASE STUDY: REMOTE WORKFORCE SECURITY ASSESSMENT SECURES KEY REMOTE OPERATIONS

As companies transition to remote work, new security risks emerge

Overview

Our client is a chemical, safety and hygiene company headquartered in the United States, but with operations worldwide. Like many North American companies of all sizes, the business had to rapidly shift to a work-from-home strategy as the COVID-19 pandemic became a significant concern in March 2020.

Background

While the company takes security very seriously and implemented several significant internal investments to protect against threats in its internal environment, the remote workforce presents a new challenge with a much larger target and new potential weaknesses. The unprecedented pandemic is uncharted territory, and the company had not planned for something few could have anticipated.

Once the new remote framework was implemented, the company's internal audit department became concerned about how data was accessed, what devices employees were using, how cloud access was governed and what locations the users were coming from. As a global organization, the company had different levels of security depending on the geographic location of the employee. But now that almost everyone is working from home, how does the company know that assets remain secure? Did IT make the necessary changes to accommodate all of the people working from home?

Project

The company selected RSM to perform a remote workforce security assessment to better understand its vulnerabilities and shape ongoing remote security planning efforts. The client needed quick, comprehensive analysis beyond typical security testing, with more insight into key areas of the new remote work structure.

The assessment began with a series of interviews with leaders from IT and security to understand and review all of the ways the organization's network and data is accessed. We learned that people use various methods to access information, depending on their job and task—some use the VPN, and others use virtual desktops on their personal devices, while some don't interact with the security perimeter at all through the SaaS cloud infrastructure.

With access controls as a top-of-mind concern in a remote environment, the RSM team evaluated how users accessed data and whether it was truly secure. We found that multifactor authentication was not utilized everywhere; it was only in what the company deemed as critical applications. If those systems with basic credentials are compromised, they can be used to access sensitive data as data loss prevention was not enabled. That is a risk regardless of the remote workforce; the new, larger target just amplifies it.

Like many companies, this organization had developed a strong on-premises network perimeter over the years. However, with the scale of the shift to remote work, it now has thousands of network perimeters to protect—the endpoints in each employee's home environment. With the rapid transition, the company did not have the same level of security configured on remote endpoints, because it always relied on on-premises perimeter controls. Luckily, the company's security stance was prepared to monitor and patch endpoints without devices needing to be connected to the VPN.

However, we discovered that when an endpoint is not connected to the VPN, web filtering capabilities were not activated. Even though they did have antivirus software in place, machines could still access potentially malicious websites and bring harmful malware back to the network without it being detected or quarantined.

In addition, the assessment discovered that endpoints are not automatically isolated on the network if they are compromised. While the company is proficient and follows established processes for detecting security events, a manual process is required to remove the endpoint from the network. Depending on the severity of an incident, infected devices may be able to infect other devices on the network before the security team can remove the device from the network. Our team suggested strategies to eliminate that manual process, including implementing security orchestration processes and automation platforms to remove problematic machines based on specific use cases such as ransomware to minimize interrupting an employee's work day.

How data travels is also a key consideration for any company, especially in a remote framework. The assessment found that the company allows USB devices to transfer data between machines, with all employees receiving access initially and revoking access if necessary. Contractors and business partners could not write to removable drives, but internal users could. We suggested a change in policy, denying everyone access to removable drives, and adding read or write permissions as necessary. It's much easier for a company to grant and then manage access than to take it away.

The company had a similar stance with its virtual desktop infrastructure. Employees could copy and paste data to personal devices—everyone was allowed this level of access except for contractors and third parties. Once again, we recommended a zero-trust approach, granting access only to employees that require it. In this scenario, data is easier to control, trace and ultimately secure.

Large companies use a wide variety of software and operating systems; within this organization, we uncovered that some were out of date and no longer supported by vendors. If devices with these systems are removed from the network, they are subject to being compromised. While the company did have an upgrade plan in place, unsupported applications inherently present security vulnerabilities, and these are amplified in such an active threat environment.

The assessment found that the company did a good job of ensuring intellectual property is encrypted prior to sending data to a third party. However, it found a process flaw where a particular set of employees could transmit data without it being encrypted. The company was in the progress of rolling out a new data encryption system and was integrating a fix for that vulnerability into that process.

Outcome

When navigating an unknown business landscape during a pandemic and balancing continuity with employee safety, new vulnerabilities are understandable—but they must be diagnosed and addressed in a timely manner. After the remote workforce security assessment, the company better understood its security posture in the new work-from-home environment, with critical insights into what was working and what areas needed immediate attention.

A more remote-focused workforce is a reality for many companies moving forward, and the assessment gave the company the knowledge to successfully adjust security measures to protect company networks and data, and meet new processes and ongoing demands.

+1 800 274 3978
rsmus.com

CS-NT-RC-ALL-0720