Summary Insights: Identifying and Closing Cloud Security Gaps

RFG Perspective: The SolarWinds security breaches, which reached thousands of enterprises around the world, point up the continuing issue of ensuring security in an increasingly uncertain world. Clearly, the scope of security breaches is changing – and IT organizations are finding that they must become far more proactive in protecting their systems, their storage and their networks.

What set the SolarWinds breaches apart was the breadth of the attack – affecting at least 18,000 organizations worldwide – and the method of attack, through third-party periodic software updates. Intruders gained access to corporate networks, then maintained low-visibility for weeks on-end, before finally attacking vast repositories of information – and gaining access to corporate data.

This incident proves that CxOs and IT executives can never let their guard down, and that they must closely monitor any anomalous activities on the network. Many organizations are finding that the remedy to the SolarWinds breach will be replacing entire systems found to have a snippet of malware code, or using IAC, (infrastructure as code) configuration files that can be quickly replaced, if needed.

IT executives must assume that no matter how much they spend on prevention, hackers will find and exploit vulnerabilities. Therefore, IT executives must ensure that they have deployed solutions that detect breaches early, contain the attack surface -- and minimize exposures.

INTRODUCTION

The SolarWinds intrusion was effective for the hackers—and it was especially shocking for IT professionals, because it was a severe and widespread threat, whose full impact is not yet known. The intrusion occurred via malicious code that was embedded in an update of the SolarWinds monitoring software, called Orion. As is standard industry practice, the software was assumed to be safe to install and it was propagated across all of the vendor's customers. That means that the malware was applied widely – and that it was "lurking" in the update software for weeks and months before being detected.

Because it had such a low profile before becoming active, it was a jarring surprise when the security attacks began to be detected– affecting more than 18,000 organizations worldwide, including enterprise data centers, federal agencies, and a number of high-tech companies, including Microsoft, Intel, Cisco and NVIDIA.

SolarWinds' Orion control plane provides a single pane of glass for monitoring network operations, gathering data regarding security product performance

monitoring and configuration throughout an enterprise or organization. Installed as a security protector, its failure to protect sensitive enterprise assets was shocking, precisely due to the degree of damage.

This report summarizes a thoughtful discussion among CxOs and senior IT executives, facilitated by the Robert Frances Group, that sheds light on the nature of the attack itself – and methods of identifying and correcting future security attacks.

Lurking In Plain Sight

As the late New York Senator Daniel Patrick Moynihan observed in a 1985 congressional hearing – we shouldn't worry only about the ICBM flying high over the North Pole, where it can be seen and easily detected – but also about the cruise missile that is flying low over the East River of Manhattan, where we may not be looking for it at all. That is a great example of flying under the radar. And that is what happened in the SolarWinds incident, where malicious code hitched a ride in a software update intended for a network management product.

For many cybersecurity incidents, delayed detection – months after a cycle of security breaches begins, is typical. Customers don't realize they have been attacked until a number of companies find the malware, and news of the breaches begins to bubble up in news accounts, webcasts and TV broadcasts.

It's only when we see anomalous results, or outages, that we notice the presence of security intrusions. And, often that later detection is by-design, so that intruders can get their software tendrils installed first before beginning to access production data. Otherwise, the offended software could have been "backed out" and removed as soon as it was installed or updated. In this case, organizations are saying it will take many months to find all the compromised systems – and to root out the malware.

Given the SolarWinds intrusions, it's clear that organizations need to re-evaluate their approach to software security, looking at everything from their trust in open source and vendors' software to their own deployment, configuration, quality assessment monitoring, audit intervention, and remediation processes of mission-critical systems. During their audits, they must leave no stone unturned in the task of assessing how much damage can be done through the use of externally developed code. Furthermore, IT executives must also extend these concepts to the new low-code and no-code software providers.

The RFG100 Panel Discussion

On Jan. 13, 2021, RFG facilitated an RFG100 video-conference entitled *"Identifying and Closing Cloud Security Gaps."* This conference examined security impacts, requirements, and the re-mediations that are needed to address the upgrades necessary in today's high-risk and evolving business and technology climate.

The panelists on the call were:

- Keyaan Williams, Managing Director, Cyber Leadership and Strategy Solutions, LLC
- Warren Gedge, CTO, ScriptString
- David Giambruno, founder & CEO, Nucleaus
- Matthew Shriner, global SIOC partner, IBM

Closing the Security Gaps, Minimizing Cyber-Attack Damage

In this research report, we include the panelists' reflections on the challenges they are experiencing, the lessons learned – and their approaches to improving monitoring and remediation of security breaches like the SolarWinds incident.

The discussion turned up key issues associated with identifying, and addressing, security gaps. Panelists agreed that IT organizations need to do far more to discover and address this type of cybersecurity attack – including replacement of infected hardware throughout their large networks round the world.

These include:

- **Finding better ways to detect potential security threats**, especially as a follow-on effect following the installation or update of third-party software
- **Improving detection software** in the Security Operations Centers (SOCs) – creating greater visibility for warning alerts about any security breaches.
- **Including mobile devices and smartphones in the alerting process**, to reduce reaction time in the event of a security breach.
- **Becoming more pro-active** about closing an array of potential security gaps in our networks – an activity that has become more challenging because of work-from-home (WFH) support of remote employees.
- **Implementing on-going risk assessments** – preferably more than once a year, if at all possible.
- **Determining Best Practices for identifying potential security threats** – and shutting them down before too much harm is done. One example is detecting malicious code – and then replacing software updates that might have had a role in spreading the malware, using pre-tested code.

- **Improving protection of high-value assets** within the network
- **Adopting important industry standards for security**, including the FedRAMP and NIST (National Institute of Standards and Technology) standards for federal work with the U.S. government. Track updates from CISA, the U.S. Cybersecurity and Infrastructure Security Agency.
- **Ensuring a consistent supply-chain for application code, and a chain of custody for sensitive data;** both will protect end-to-end security within a large enterprise or cloud deployment.
- **Adjusting contracts with third-party software vendors** to protect against damages caused by flaws that are found in the software products
- **Updating a risk-mitigation strategy** for the company, to make it more defensible from a software security perspective.
- **Ensuring that SMB firms have an appropriate detection and response system** in place, even though they have fewer IT staffers to monitor their networks and systems than large organizations do.

RFG Analysis

RFG100 executives were polled about their usage of security software, which turned up the following results:

- Fully 33% of respondents said they had an assessment program in place.
- An equal percentage of respondents, 33%, said they did not have a robust assessment program in place.
- Respondents used a variety of methods to assess the quality of security software from ISV (independent software vendors) – Note: multiple answers were permitted for this question:
    - Security questionnaire (62%)
    - Documentation review (52%);
    - Remote assessment (57%);
    - Cyber rating (38%)
    - Onsite assessment: 29%)
    - Code-testing (48%)
- Regarding their Security Operations Centers (SOCs), respondents said:
    - 43% said they have full confidence in their ability to respond quickly to any breach
    - 33% said they have discovery tools they run daily
    - 29% said they have detection tools they run daily
    - 33% said they have an incident response and remediation process

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

ANALYSIS

Having a single dashboard for security is a sign of a smart, and stable, security operations center (SOC). But what we're seeing is an accumulation— a gathering point – for many dozens of point products shown with a "single-pane-of-glass" view of the individual security-monitoring results. Normally, this is a reasonable solution, given that it is a convenience for the IT staffers to quickly "check in" regarding the status of all of the firm's installed security software products. Now, organizations must also consider the possibility that the control planes themselves could present an incomplete picture of some looming security threats.

Another dimension is emerging, as well. Could an organization's cloud providers discover a security issue before enterprise data centers do? The large cloud service providers leverage powerful AI/ML software to hunt for security anomalies faster than manual processes – allowing organizations to respond to far-reaching security breaches sooner. These AI/ML software tools could be applied to a company's on-premises private cloud, if one is used for processing data in highly regulated industries (e.g., financial services; healthcare; pharmaceuticals and government).

Often, CxOs and IT managers only find that there is a security issue when log entries of timestamps look unusual, RFG 100 panelists noted. And that activity takes time to "bubble up" into IT oversight awareness. Something has to be obviously wrong in order to notice it – and the question now is how AI can be applied to find these anomalies sooner – allowing IT organizations to remove the offending software.

Sometimes, organizations experience an outage that is obvious – usually when the "dormant" security intrusion is activated in the network, allowing customers to identify the breach. At other times, they must look to adopt new and better "best practices" that will guide their corporate reviews of security flaws in ISV software they install and update periodically.

The best way to do that, RFG100 panelists said, is to automate the overnight process by setting operational parameters that would "trip" the warning alerts in what otherwise seem to be routine production for business services.

SUMMARY

The SolarWinds incidents, triggered by malware installed during third-party software updates, is a jarring wake-up call for IT organizations. It demonstrates the need for IT organizations to be proactive, rather than reactive, in closing the security gaps they detect in their networks. It cast a bright light on the potential to disrupt businesses and governments through the use of malware imported into any of the organization's systems.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

All of this is framing an urgent "call to action" for IT organizations: They must hunt down and address anomalous security issues in a comprehensive and more effective way. And they must work with federal and government agencies to protect and extend current security standards (e.g., FedRAMP, NIST) to counter future intrusions. Cybersecurity training and increased automation may also improve an organization's operational defense against future security breaches.

Business and IT executives must formulate new security policies that envision the potential for broad-based cybersecurity attacks. They must find ways to identify them when they occur, to limit their attack surface and to close those security gaps quickly to limit damages if similar incidents occur in the future.

RFG POV: In the wake of the SolarWinds security breach, enterprise organizations need to re-evaluate their approach to relying on third-party security software. IT organizations need to implement a better process for attestation and acceptance of all third-party software that enables them to acknowledge and evaluate the common vulnerabilities and exposures (CVEs) of new or patched software before issuing a go/no-go for implementation. Additionally, IT must implement tools that can alert the SOC and other appropriate parties to any unusual exfiltration of data. Moreover, IT executives and architects need to perform an extensive review of all their applications, datasets and systems to determine how they can construct smaller security domains so that when security breaches occur, their organization's exposure is minimized.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research. Jean S. Bozman, President of Cloud Architects Advisors LLC, co-authored this report.

---

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*