Summary Insights: Continuous Monitoring with NIST & Zero Trust

RFG Perspective: Hackers will always find a way to penetrate one or more flaws in an organization's security barriers; therefore, it is imperative organizations have in place containment, mitigation, and remediation strategies. Business and IT executives should be incorporating approaches like the National Institute of Standards and Technology (NIST) standards and Zero Trust methodologies so that they can minimize and mitigate their organization's security risks.

Regardless of how many physical and software-based solutions are installed to prevent breaches, hackers will find ways to breach the cybersecurity walls through unknown zero-day attack factors or known, existing code vulnerabilities.

These breaches are becoming more complex and sophisticated and, in many cases, breaches are now caused by rouge groups and state actors. Simply put: security breaches are going to happen, whether they are the result of internal code, external code third-party vendor code, or imported open-source code. Therefore, the issue becomes an exercise in accurately detecting, containing, and preventing attacks – and doing so as close to real-time as possible.

RFG 100 Panelists and Insights from Participating RFG 100 Executives

On Mar. 10, 2021, RFG facilitated an RFG 100 video conference entitled *"Continuous Monitoring with NIST and Zero Trust."*
The panelists on the call were:

- Ron Ross, Fellow, NIST
- Ben Agner, Director, Aflac
- Keyaan Williams, Managing Director, CLASS LLC
- Anthony Cruz, Principal Architect, BNY Mellon

These RFG 100 executives and panelists discussed the challenges of continuous monitoring networks and systems to stop or minimize the damage caused by hacking attempts.

RFG Analysis

POLL RESULTS

RFG 100 executives were polled about their existing security capabilities. We found the following results:

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

- 69% of the poll respondents said they believe their organization still has some serious security exposures, due to technical debt related to aging and legacy systems and software.
- The same percentage of respondents reported that they are very satisfied with their security risks even though they presumed there were potential inconsistencies in their hybrid cloud environment.
- About 50% of the respondents rated the security risk from their work from home environments as acceptable. A similar percentage rated their DevSecOps environment as problematic. However, 62% of respondents still believe that they must be mindful of serious security risk exposures due to ever-changing configuration management.
- Slightly more than half of the respondents rated their cloud service provider (CSP) security efforts as meeting all of their organization's security requirements. Another 31% disagreed with that statement, with the remaining feeling that most of their requirements are satisfied.

Analysis of the Discussion

The overall consensus from within and beyond the RFG 100 Membership community is that the NIST standards are valuable in setting security policies whereas zero trust and continuous monitoring are excellent concepts for protecting assets. However, zero trust is not viewed as a silver bullet, which is why Zero Trust currently remains an aspirational goal for most organizations.

Most large enterprises see significant efforts ahead of them, as they seek to ensure their networks and systems cannot be penetrated – and to ensure that any security-related damage would be minimized in case of any failure, large or small.

NIST Below the Waterline

Cybersecurity today faces two major challenges: complexity and transparency. In large enterprises there are millions of lines of code – internally developed, open sourced, and acquired from third parties – and thousands of devices employed by a corporation (millions if you include all the customers and prospects that might visit corporate websites).

This ubiquitous connectivity creates a massive attack surface, which for all intent and purposes has the appearance of a black box. As a result, companies often lack the details about how individual applications and products were engineered and about what kind of security engineering was employed at that time. Yet,

corporations typically use a wide variety of components as core elements of a corporation's foundation for mission-critical applications.

Building a Cybersecurity Framework

NIST has been creating cybersecurity frameworks and standards since 2013, when Executive Order (EO) 13636 was issued. The EO tasked NIST with the development of a cybersecurity framework. As part of the framework, NIST was always committed to continuous monitoring as one of the key elements for ensuring end-to-end security. However, up until recently, the order's focus was on above-the-waterline workloads (i.e., production). It has just begun to address the below-the-waterline issues, which is where the real action will be in the future.

Today's cybersecurity adversaries live below the waterline. In many cases, the attackers understand corporate systems better than do the staffers within the enterprise that could become a target of security attacks. These corporate and nation-state invaders are good at discovering known vulnerabilities that have not been fixed – or finding and attacking security flaws that were not known, thereby creating zero-day exploits. Because of the extensive complexity of systems and the reuse of acquired code, zero-day exploits are growing at an alarming rate. This is why NIST has done a significant amount of work on above-the-waterline issues.

Today, NIST is moving toward the engineering side, as security has to be engineered in throughout the software life cycle – and not just applied at the time of production. In that regard, companies have to do a better job of managing and reducing the complexity. These tasks can be done in a variety of ways: by eliminating unnecessary applications, by reducing the number of components, by creating more transparency, or by moving things to the cloud, where other specialists can manage some of the cybersecurity efforts.

Now, IT has to get below the waterline, too – and to fix things at the architectural level. Organizations must become more resilient to be able to absorb an attack and to limit the damage the attacker can do. Once the enemy is inside the corporate firewall, methodologies must be employed to slow them down and to kick them out. This can be accomplished through zero trust architecture or micro virtualization, micro-segmentation, impediment of lateral movement, increasing their work factor, or other techniques.

Zero Trust – and How It Works

Zero trust, an aspirational principle for corporate security, is aimed at minimizing the "splash" – or the extent – of any damage created. It is about detecting a problem

as quickly as possible and then preventing the attacker from moving laterally within the organization's networks or systems.

The term "zero trust" also applies to an enterprise's supply chain because these types of attacks can be just as damaging as other types of cyberattacks. This was revealed by the far-reaching SolarWinds breach, which impacted at least 18,000 companies worldwide. The Solar Winds attack came in "under the radar," so to speak, because it was embedded in management software for distributed network devices. Overall, enterprises have to be able to confirm that their supply chain is good.

Five Fundamental Principles

There are five major fundamental principles of trust and zero trust. First is to **identify** and **protect** the IT surface from internal and external dangers – applications, data, devices, services, and users. Here are the five principles:

1) **Having authority.** One must know who has been granted what authority. What are they trying to access? From what devices?

2) **Understanding cybersecurity controls.** Then, one needs to understand the cybersecurity controls that are already in place. Usually what exists within an organization is insufficient to provide a complete, end-to-end zero trust model.

3) **Leveraging new tools.** Thus, the next principle calls for incorporating new tools and a modern architecture to provide the missing layers of protection.

4) **Write a detailed security policy.** After new software tools are installed, one needs to apply a detailed policy. Zero-trust policies are rules that permit access to various resources based on a strict set of standards to only allow access when absolutely necessary. These policies should identify which users, devices and applications should have access to what data and services and when. Only after the high-level policies are built can administrators then configure the security devices to adhere to the permission rules, while denying access to everything else.
5) The last principle calls for continuous monitoring and alerts. Without taking this important step, all the preventative steps fall short.

It is important to note that each one of the five principles has its own maturity curve. One has to create a trust engine that takes into account all of the five factors and makes risk scoring decisions in real time. The engine has to permit immediate revocation, if and where it is required. *If the trust engine is not intelligent enough to*

do that, there needs to be a SOC in place that can quickly execute the revocation manually.

And here's the proof: If hackers can get past your corporate firewalls by coming in off-network, they may be able to attack third-party software packages – or an acquisition's applications that are not fully integrated into the overall zero trust environment.

Even worse, if the acquired packages are no longer on a trusted network and the attacker pulls down the package, they may be able to poison a public repository with a package that is named the same way as your enterprise package is named.

Protection requires the establishment of authority certificates, the signing of the package and the signing of the repositories. IT organizations must also ensure that their software developers are only working with the trusted code repositories that they have been authorized to work with – whether those repos house open-source or vendor-specific software.

Developers and operations need to build resiliency into their systems. If a user is accessing an application and something negative occurs, then there needs to be the ability to pull the application or, in some cases, to shut down the network – or one or more devices. This will require an AI or ML trust engine that can make real-time decisions in a minimal timeframe. This consideration is of major importance because in many large enterprises, the biggest risk is inside the internal IT organization, which requires human intervention and is not sufficiently automated. These gaps in overall security can result in significant risk exposures unless one has a highly intelligent real-time trust engine.

The Cloud Security Swiss-Cheese Problem

Many participants felt the move to the cloud is not driving towards zero trust but causing a Swiss cheese environmental problem. Large enterprises have a backlog of $0.5 billion to $1.0 billion dollars of technical debt – most of which has been accruing over the last 30 years. This debt is sitting in systems on-premises, using antiquated technology. The good news is that people feel this provides them a level of acceptable risk.

The Swiss cheese environment occurs when the software that holds the debt is not being fixed but is being moved to the cloud. This increases the organization's risk profile by "Swiss cheesing" the security trust boundaries. Most clouds are designed to be open, in contrast to business-critical and mission-critical applications that operate in a very closed, protected environment. This means that companies must employ a multi-layered security approach to ensure they are still fully covered.

The model has to be designed to function in a hybrid multi-cloud world and needs to address detection incident response, containment, mitigation, and remediation components. Basically, a multifaceted model has to reduce the blast radius from any type of intrusion that inevitably will happen or any other type of corruption. This is true for applications, data, devices, and networks. Therefore, it is suggested that the responsibility for developing this model should rest with the various enterprise architecture groups, because they need to work collaboratively to address all the security components and how they are knitted together into a cohesive protection layer – up, down and across the stack.

API and Steganography Security Threats

Another security threat is the actual APIs that are embedded in the code that is being used. The threat resides inside the functionality of the API itself, after authentication. Once authentication is given, then it is possible for the API to be executed with an incorrect operational scope, allowing that API to be utilized to escalate privileges, or to masquerade as a different user. IT needs to ensure that the API calls are logged and monitored – and that a backup plan is in place in case problems arise from the API calls.

Steganography – the practice of hiding a message within another message – like malware that is hidden within a picture – is another serious threat that tends to be taken too lightly. It needs to be on the security checklist.

Continuous Monitoring and Vulnerability Testing

Zero trust does not work without continuous monitoring. Trust engines today have gaps in them and truly are not mature yet. Therefore, it is necessary to continually monitor activities. Additionally, a zero trust methodology provides the ability to utilize legacy technology and to secure it with a trust wrapper without having to break the old logic or address the existing technical debt.

When moving into new environments, it is reasonable to assume not all of the required controls will have been put into place. To use an analogy: It is a bit like the Wild West. That is why it is necessary to do penetration testing and vulnerability assessments as often as possible, until everyone is satisfied with the maturity of the new environment. Without real-time visibility, one cannot identify simple bad code or systemic problems in one's coding practices or configurations. Once the root causes have been corrected, then the frequency of assessments can be reduced.

Another area of concern is the introduction of implementation bugs. These flaws can create openings for attack vectors. Thus, new code must be flagged for continuous

monitoring until one is satisfied that the new code is not creating new risk exposures.

SUMMARY

NIST has produced cloud and cybersecurity standards and zero trust methodologies that have been around a while. However, at most companies, a full implementation of these proven NIST methods remains, today, more of an aspirational goal than an achieved goal.

The challenge for IT executives and IT staffers in today's environments is that the complexity and ability to obscure the cyber-attack vulnerabilities increase daily. To succeed in this war against cybersecurity attacks, IT organizations must approach security strategically, not tactically. Rather than addressing the penetration points, they must ensure that the containment, mitigation, and remediation strategies are addressed simultaneously, in order to reduce vulnerability to cyberattacks.

RFG POV: No perimeter is impenetrable – hackers will always find a flaw through which they can gain access. Continuous monitoring through use of NIST standards and zero trust methods is intended to minimize the risks caused by these attacks. Business and IT executives must remember that the business objective is to attain a continuous acceptable risk exposure level, so that a future cyberattack would not harm the entire business. Accordingly, they must implement an architecture that ensures that no attack can result in a major data loss, an extended outage, corporate embarrassment, or a loss of customer loyalty. Without customer loyalty, the organization would face the prospect of diminished revenue and greater losses in a challenging, and competitive, world economy.

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.
