Demystifying the Key Benefits of Network Security Automation

What if security protection of assets could be automated? As networks are dynamic and evolve, network security automation with policy-based and intelligent solutions can help communications service providers minimize business risks.

NEWS RELEASE BY **ERICSSON**

Northampton, MA | March 07, 2022 02:46 PM Eastern Standard Time

By: **Keijo Mononen**, General Manager, Security Solutions at Ericsson

Communications service providers (CSPs) and mission-critical service providers face increasing security challenges and a rapidly evolving threat landscape. To provide trustworthy 5G services, CSPs need increased capabilities to continuously protect these services and detect and respond to threats. In addition, these capabilities need to be well integrated and life-cycle managed with the network infrastructure.

To minimize business risks in their operations, CSPs need to shift how they manage security and move towards automated, policy-based, and intelligent security solutions fit-for-purpose supporting the emerging dynamic networks. The earlier this transition is done, the better. With decades of experience in the telecom security industry, here is my

take on how CSPs can protect their assets and gain a better understanding of network security automation.

Facing the security reality for CSPs

The network evolution introduces dynamic, distributed, and open networks to support various services including industry-specific use cases. These networks open endless opportunities for society and accelerate digitalization. However, while the networks are becoming dynamic, distributed, and more intelligent, security needs to be on par.

Increased pressure on the network

New and advanced industry use cases put pressure on network requirements. With 5G, networks will serve as critical infrastructures to facilitate the digitalization, automation, and connectivity to machines, robots, transport solutions, etc. Thus, there is a significant value at stake and, so too, a significantly different tolerance for risk. 5G marks the beginning of a new era of network security.

The telecom industry and 5G are their own domains with mission-critical assets and specific protocols. This requires both skills, an understanding of relevant security risks, and ensuring solutions are well integrated with the telecom and 5G environment.

Dealing with dynamic and evolving networks

Furthermore, an additional challenge from a security point of view is the dynamic nature of the networks. It happens in two dimensions; first, the networks are dynamic and distributed to scale with business needs and support different industry use cases. As a result, security must follow these dynamic networks in real-time. Second, the networks need to evolve continuously with new features and add value to businesses. This puts requirements on continuous integration and continuous deployment (CI/CD). Security monitoring and management must be tightly integrated with the network products to reduce the time to market for the new features. Because networks are becoming the foundation of society, there are also increased network security regulations driving the need for visibility and control of security – this is efficiently achieved by automation.

How prepared are CSPs?

When trying to understand the level of readiness among CSPs, my conversations with them and research indicates a major shift. This is no surprise, and many trends point in the same direction. According to Ernst & Young, CSPs face these shifting sentiments amid rising cyberattacks, with 75% reporting an increase in cyberattacks in the last twelve months. Responding effectively is a crucial concern: 47% say they've never been more concerned about their own ability to manage cyber threats.

Input from IBM shows that in 2019, 16% of businesses reported having a fully automated network security solution, 36% said having a partially automated solution. Another 36% reported not having automated security but plan to implement it during the next 24 months. Finally, 12% did not have an automated security solution and had no plan to deploy it. These figures relate to businesses in general and are not specific to CSPs. The degree of automation is likely even lower in telecom networks; however, it is evident that telecom networks will follow the same route towards automation. ENISA's Telecom Security Incident report from 2020, points out that incidents caused by human errors in 2020 reached 26% of the total number of incidents. Yet another reason for increasing the level of automation.

Armed with 3 security pillars: protect, detect, and respond – managed by automation

Protection

I see a strong trend to increase automation for threat detection and incident response in the security market; this is for very good reasons. One area that should always be top of mind is protection; the better you are protected at all times, the better off you are when you are under attack.

One of the main challenges is the introduction of dynamic and distributed networks and cloud-native environments – protection needs to follow. This challenge is solved with automation and security orchestration, where fit-for-purpose security policies are automatically set in the network infrastructure. Security policies ensure that the infrastructure has the desired and consistent security level across domains. This means policies enabling holistic security, e.g. identity and access security, data and traffic protection, and valid certificates. Furthermore, the automation ensures solid configurations of the network across domains making intrusion or lateral movement for an attacker difficult. It also serves as a solid baseline of "what is normal in the complex system" – this enables effective detections of breaches as well. This is one of the reasons why automated security management solutions combining protect and detect capabilities becomes so effective.

The value of security automation is already evident with traditional networks up to 4G. With 5G, network security automation is becoming mandatory and gives advantages in scaling the security, not in the least with the introduction of network slicing. With security automation, you also have support to slice specific security policy sets. This enables tailored security for different network slices targeting different industries, including mission-critical enterprises or government functions.

Detection

Once the actual protection of the network is established, and under control, the focus will be on detection of threats and vulnerabilities. One obvious vulnerability that must be monitored is the lack of compliance with security policies. Compliance must be continually detected and corrected. It is also good practice to analyze the root cause of a policy change. For example, it could be a legitimate temporary change of a policy configuration or an attacker tampering with the security to gain increased access in the system or turning off security logging. This can be effectively managed with automation.

In addition, CSPs must detect threats in their domains such as RAN (Radio Access Network), Core, and OSS/BSS infrastructure, considering the transformation to cloud native architecture.

Response

What can we learn? Leveraging lessons learned is such a fundamental force for humanity, and likewise, it is required within the network security domain. A successful security strategy must start with solid protection, always including detecting domain-specific threats and vulnerabilities and then responding. Some threats are so significant that they should be assigned to incident response teams. Resources who have the right domain knowledge to analyze threats at a deeper level based on data and insights from security tools fit-for-purpose understand what is going on and what actions need to be taken. Breaches and incidents are also feedback to the security solution for continuous improvements, e.g. leading to new or enhanced security policies.

What often is discovered is that responses are often very manual, even for quite basic needs such as non-compliance of policies. These have a clear action that can be automated. To respond quickly, security automation needs to be integrated closely with other software involved in managing and orchestrating the network, such as telecom orchestrators.

Benefitting from network security automation

In my opinion, the end goal is that security is always adapting with the dynamic network and constantly evolving with the threat landscape. To achieve this, automated processes are the answer providing security assurance to CSPs for their continuous network deployment and operations. This will save a lot of manual, error-prone work, address the lack of staff for security operations, and be a key enabler for managing security for the evolved networks. Furthermore, CSPs will benefit from automation to protect, detect and respond through security automation fully integrated with networks; the sooner that journey starts, the better.

With an automated constantly evolving fit-for-purpose security orchestration solution well integrated with a multivendor telecommunications infrastructure, CSPs meet the end goal by constantly monitoring security compliance, detecting and responding to new threats, and supporting cost-efficient security operations.

Learn more about how we can protect your assets.

References:

How can risk foresight lead to fresh insight? | EY - Global

2019 Cost of a Data Breach Report (ibm.com)

ENISA's Telecom Security Incident report

View additional multimedia and more ESG storytelling from Ericsson on 3blmedia.com