NSA and CISA release "Security Guidance for 5G Cloud Infrastructure" series. The first article focuses on preventing and detecting lateral movement from cybersecurity attacks

The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) published the first of their four-part series, "Security Guidance for 5G Cloud Infrastructure" at the end of October. The series outlines specific threats to the 5G infrastructure and provides guidance on how to build and harden the 5G cloud infrastructure against those threats. 5G's cloud infrastructure and multitenancy (i.e. the use of a shared physical infrastructure by multiple cloud infrastructure customers) create unique challenges and vulnerabilities compared to its predecessors, including more opportunities for lateral movement.

The whitepaper comes on the heels of several federal laws focused on improving cybersecurity. Former President Trump first laid out the nation's National Cyber Strategy and established the CISA in 2018. In March of 2020, the "Secure 5G and Beyond Act", requiring the President to develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure in the United States was signed into law. Out of that Act, the National Strategy to Secure 5G was developed and the Enduring Security Framework (ESF), a cross-sector working group comprised of both government and industry professionals, establishing working panels to review threats and paths forward for 5G. The NSA and CIA's white paper is an outcome of those working groups. It also supports the Executive Order on Improving the Nationals Cyber Security that President Biden signed in May 2021, which specifically called for the CISA to provide guidance on infrastructure and security structure as well as governance for cloud-based technologies.

The first article in the series, "Part 1: Prevent and Detect Lateral Movement," provides specific guidance to "detect malicious cyber actor activity in 5G clouds and prevent actors from leveraging the compromise of a single cloud resource to compromise the entire network." It is based in Zero-Trust, assuming that an attacker will inevitably gain access to the network. Thus, monitoring and securing the internal network is as critical an activity as building a strong perimeter. The graphic on the next page summarizes specific steps that can be taken in each of 5 threat areas.

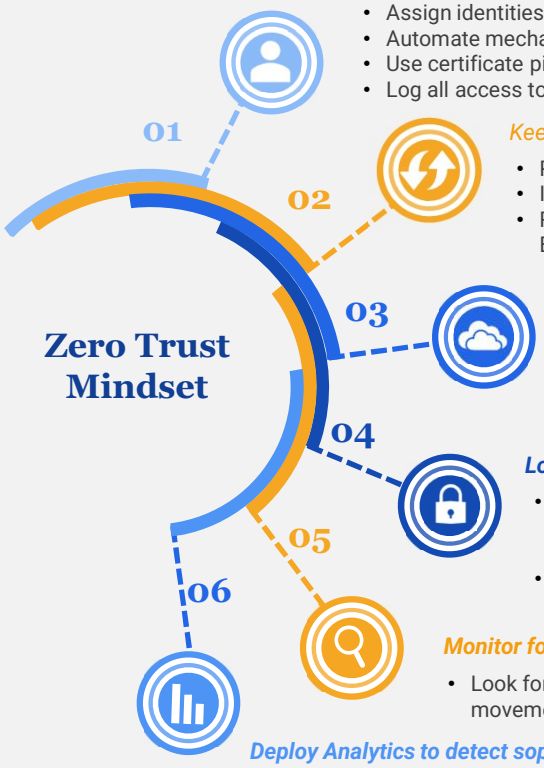
The remainder of the series will focus on securely isolating network resources, protecting data, and ensuring integrity of the infrastructure.

DAYBLINK

Mitigating threats associated with 5G Cloud Infrastructure

Threat	Mitigation
Increased external vulnerability points More element-to-element communications utilizing physical appliances and point-to-point interfaces require authentication	***Implement security identify and access management*** Reduce risk both at the network-function layer as well as the underlying cloud infrastructure layer
Vulnerabilities in any of the software applications Many software applications support virtual network functionality – basic services, open source, and specialized services, including third party applications	***Keep 5G software up to date and free from known vulnerabilities*** All organizations that deploy software have the responsibility to maintain it, including cloud/virtual networking software, management and orchestration code for deploying virtual networks, and integrated applications
Maintaining security in complex architecture Network functions or microservices may sit in the same logical network segment but two completely different security groups	***Securely configure networking within the 5G cloud*** Use networking functions (subnetting and stateful firewall/ACL) to control which nodes can communicate would add an additional layer of security
Increased internal vulnerability points Significantly more communication sessions between network elements than in 4G LTE	***Lock down communications among isolated network functions*** Provide mechanisms to ensure that all communication sessions are authorized, and policy is enforced over network resources in the same security group
Attackers gaining access undetected Attackers may steal legitimate authorized user credentials	***Monitor for notification of adversarial lateral movement*** Continuously monitor the evidence left by an attacker who is moving laterally
Difficulty in detecting an attacker Massive amounts of network traffic and IM events occurring regularly within the 5G native cloud deployment	***Deploy Analytics to detect sophisticated adversarial presence*** Analytics should be capable of detecting known and anticipated threat, but also be designed to identify anomalies in the data that could indicate unanticipated threat

Solutions drilldown: Guide to implementing mitigations



Implement security identify and access management

- Assign unique identities to all elements and each interface that will communicate to other elements in the network
- Authenticate and authorize resource entities requesting access at each network element
- Assign identities using Public Key Infrastructure X.509 certificates (preferred) or multi-factor authentication (MFA)
- Automate mechanisms for credential management (e.g., certificate rotation via a Service Mesh)
- Use certificate pinning or public key pinning when authentication is dependent upon multiple certificate authorities
- Log all access to resources; Regularly deploy and run analytics for detecting malicious resource access attempts

Keep 5G software up to date and free from known vulnerabilities

- Patch publicly known vulnerabilities as quickly as possible
- Integrate source code scanning and patching into the software development and deployment process
- Reference and implement measures as listed in NIST Special Publication (SP) 800-40, Guide to Enterprise Patch Management Technologies

Securely configure networking within the 5G cloud

- Create security groups per K8s Pod
- Use private networking for connecting microservices/network functions
- Configure default firewall rules or default ACLs to block inbound and outbound connections at the Pod and worker node level
- Use Service Meshes to protect node-to-node traffic

Lock down communications among isolated network functions

- Ensure that all communication sessions on a network function's control plane, user plane, management plane, and through the cloud infrastructure are authenticated using the identities provisioned from the Identity and Authorization session
- Create and deploy policies that enforce the separation of network resources in the same security group based on secure authentication and authorization

Monitor for notification of adversarial lateral movement

- Look for evidence of lateral moves; continuously monitor for evidence of exploitation and adversarial lateral movement within 5G cloud

Deploy Analytics to detect sophisticated adversarial presence

- Use sophisticated analytics, based on machine learning and artificial intelligence to detect adversarial activity and data anomalies

DAYBLINK