**3GPP TSG-SA3 Meeting #102-e-bis *S3-210829***

**e-meeting, 1-5 March 20201**

**Source: NCSC**

**Title: Administration of the virtualisation fabric**

**Document for: Approval**

**Agenda Item: 2.4**

# 1 Decision/action requested

***It is requested that SA3 approves this new solution for administration of the virtualisation fabric.***

# 2 References

[1] 3GPP TR 33.848, Study on security impacts of Virtualisation, v0.6.0

# 3 Rationale

Attacks on the administration of a virtualized network have the potential to be catastrophic given the high level of privilege and access involved, so some stringent steps must be taken to secure it.

# 4 Detailed proposal

START OF CHANGE 1

6.x Solution #<x>: Administration of the virtualisation fabric

6.x.1 Introduction

This solution addresses Key Issue #10, Single Administrator Domain.

Administration of a network takes place in the management plane. A compromise in this part of the network infrastructure could impact the whole network, making it the primary target for any malicious attack intending to disrupt or otherwise compromise the operation of a network. Exploitation of the management plane could have a long-term impact on the availability and confidentiality of the operator’s services, including critical services.

Historic management of telecoms networks has relied heavily upon standard corporate devices doubling up as administrative workstations. Consequently, machines that perform standard ‘office’ type functionality such as email, and web access are also defining the operation of the network. This is often referred to as a browse up architecture, and brings significant risk. Where it is used, several commodity classes of attack can be performed with relative ease upon administrative users, and these can achieve a significant impact. Several attack vectors exist, the most notable being the possibilities afforded to an attacker via phishing of administrative users, targeted or otherwise, which can result in credential loss, remote code execution, and further exploitation of networks or users.

Attacks of this type tend not to be noisy, meaning that there is no overt impact on the network, and they may be maintained for years, growing in scale and complexity over time. These attacks are likely to have a significant impact on the operator and hence securing the management plane should be treated as a priority. Given the risks, it is not appropriate for operators to be using a browse up architecture. Instead, operators should architect, and operate, their management plane infrastructure to inhibit network compromise through administrative access. Operators should treat virtualisation administration as a management plane.

NOTE: A host compromise will compromise all workloads running on that host, and as such the administration of the underlying hardware is as critical as the administration of the virtualisation fabric.

6.x.2 Solution Details

Access to the management plane needs to be temporary and time-bounded. The operator needs to constrain the number of administrator accounts able to modify the Virtualisation Fabric, and the number of administrators, to a minimal manageable number to meet their needs. Administrators need to be prevented from being able to grant themselves privileged access to the network, and should not have access to the host’s hardware or the virtualised workloads running within the environment.

All administrative access needs to be logged, and the activity of the session recorded. Manual administration of the Virtualisation Fabric (e.g. access to a command line on host infrastructure) should raise a security incident. The devices and locations from which the fabric can be modified should be limited.

All new deployments of equipment need to be administered via authenticated and encrypted channels. Insecure or proprietary security protocols need to be disabled. Administrative access needs to be via secure, encrypted, and authenticated protocols whenever technically practical. Functions that support the administration and security of the Virtualisation Fabric should not be run on the fabric itself, and should be considered as Security Critical functions running on separate dedicated hardware.

6.x.3 Evaluation

Editor's Note: To be added.

END OF CHANGE 1