**Virtual Machine Configuration**

As computing power and technology kept on developing, the 1990s saw the rise of server virtualization. Innovations like VMware introduced the capacity to run multiple operating systems on a single physical server, allowing for the optimization of resource utilization as well as the ability to streamline IT infrastructure. This new advancement revolutionized data center management and paved the way for a widespread adoption of virtual machines in various computing environments. The configuration of these machines would include specifying the OS (operating system), allocating resources such as memory and storage, as well as a mirage of other things. Each VM operates as a unique entity with its own set of applications and functionalities. The securing of these VM configurations is generally regarded as being highly important. It has proven to be crucial in preventing vulnerabilities and optimizing resource utilization in virtualized infrastructures amongst other things.

The National Institute of Standards and Technology released a bulletin in 2016 regarding network security in Virtualized Infrastructure. In it the highlighted the importance of the heightened security needs of VMs within the era of cloud computing. It underscores the criticality of providing VMs, supporting vital business processes, with security levels equivalent to traditional physical devices. It also discussed key configurations such as network segmentation, network path redundancy, traffic control through firewalls and traffic monitoring. It also provides detailed analyses, advantages, disadvantages, and security recommendations for each of these configuration areas, emphasizing the significance of securing VMs through a combination of host-level and network-level measures.

**Access Control**

With regard to access control in these computing systems, the historical trajectory can be traced back to the days of multi-user systems. At the time administrators would grant permission to a user based on their role. The rise of networking and distributed computing would call for and necessitate a more sophisticated level of access control mechanisms. This coupled with the rise of the internet and the focus was shifted in order to protect digital assets from external threats. This was the birth of modern access control frameworks.

One could think of access control as a digital bouncer. A determination is made about who is allowed into specific areas within a virtual space. The defining and enforcing of rules that in practice dictate which users or systems are allowed to access certain resources or perform particular actions. The principle of least privilege emphasizes restricting access rights for users to the bare minimum necessary to complete the duties of their job. By using this approach, a company minimizes the potential impact of security breaches through limiting exposure to critical resources. In essence, it's akin to assigning digital permissions, ensuring that individuals have access only to what is essential for their roles and responsibilities. A Zero-Trust model could and should be employed as well. It is a security model that by default trusts no device or user and authenticates every transaction. The CISA Zero Trust Maturity Model v1.0 refers to the definition of Zero Trust in NIST SP 800-207: “a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.”

Another one of the governing cybersecurity bodies NIST has also provided the following security recommendations. Security Recommendation HY-SR-13: The access control solution for VM administration should have the granular capability both at the permission assignment level as well as at the object level (i.e., the specification of the target of the permission can be a single VM or any logical grouping of VMs - based on function or location). In addition, another desired capability for the access control solution is the ability to specify deny permission to some specific objects within a VM group (e.g., VMs running workloads of a particular sensitivity level) in spite of having access permission to the VM group.

**Password Management & Authentication**

The use of passwords as a security practice is deeply intermixed with the evolution of computing. As one could assume, as computing power grew and interconnected systems became more prevalent, the need for more robust and strong password practices became more evident. No longer could the simple password schemes of the early days of computing be relied on.

Effective password management and authentication revolves around the implementation of different strategies to create and maintain secure passwords in order to gain access to virtualized environment. Policies surrounding passwords should be sure to make clear that passwords should be complex and frequently changed. Should there be a higher security need, password-based authentication may nor even cut it. As threats grow, stronger forms of authentication like personal identity verification (PIV) cards should be used. Authentication is the actual process of verifying the identity of users or systems attempting to access VMs and their applications. There are several authentication methods such as Kerberos, Certificate Based, Biometric and Multi-Factor. With a method such as Multi-Factor Authentication (MFA), an extra security layer is added my requiring multiple forms of verification such as a temporary code being sent to one’s phone. These extra layers of security checks aids in making unauthorized access more challenging and protecting against different types of cyber threats.

The hosts of these virtual machines should also ensure that user accounts, both privileged and regular should be connected to the main directory infrastructure of the entire organization. In doing this authentication methods such as Kerberos can be used. It would also ensure that security rules are enforced and changes to user’s accounts can be done smoothly. NIST details this in the following security recommendation. Security Recommendation HY-SR-15: The user accounts (including privileged accounts) on the hypervisor host must be integrated with the enterprise directory infrastructure in order to enable authentication through robust authentication protocols (e.g., Kerberos), enable enforcement of some corporate security policies (e.g., password policies) as well as handle changes to user account list (addition and deletion of user accounts).