Administrative and environmental security measures of windows

Law, Security

Based on the information provided in Part F ‘ EP IT Environment and Development Standards’, our response considers an European Parliament (EP) infrastructure consisting of Windows Server 2016 and covers security controls related to the same. We have also included a comparison table in the annexure between the security controls managed by Windows Server 2016 vs earlier versions (2012 and 2008). The following table shows an overview of typical organizational (such as the EP) security objectives and how Windows Server 2016 can help. EP needs to Example threat Windows Server 2016 helps Protect admin credentials Pass-the-Hash attack where an attacker can authenticate to a server (using NTLM) by using the hash of the password. . Credential Guard component helps in dealing with Pass-the-Hash and Pass-the-Ticket attacks. Remote Credential Guard delivers Single Sign On for Remote Desktop Protocol (RDP) sessions, eliminating the need to pass credentials to the host Protect servers, detect threats and respond in time Wannacry attack Device Guard technologies provide application whitelisting and code integrity policies to avoid malicious code to execute. Additionally, malware activity is stopped by means of Windows Defender. This takes place due to the protection of known vulnerabilities. Malicious code within the application (library downloaded from internet) Isolate containerized applications by using Hyper-V containers. This takes place without changing the container image. Additionally, Reducing of the attack surface with the just-enough OS deployment capabilities of Nano Server will help in application risk reduction. identification of malicious activities Malware activities trying to get user credentials. Enhanced Logging aids in threat detection including providing auditing access to kernel and other sensitive

processes. This information is consumed by Microsoft Operations Management Suite (OMS), which in turn provide intelligence on potential breaches through its Log Analytics feature.

Secure Virtualization

Hacker could compromise fabric admin credentials, allowing him to access to virtualized Active Directory Domain Controllers. Create Shielded Virtual Machines — Generation 2 VMs that have a virtual TPM. They are encrypted using BitLocker and can only run on approved hosts in the fabric. This can take place due to the host Guardian Service. It requires hosts to attest to its security health before Shielded Virtual Machines will boot or migrateю Windows Server 2016 gives EP the power to prevent attacks and detect suspicious activity with new features to control privileged access, protect virtual machines (VMs), and harden the platform against emerging threats.

Security Controls

While Microsoft Windows has continued to become more security through its inbuilt security features over the years, it requires multiple levels of security controls to be added to build a secure infrastructure. Below is a brief overview of security controls which are required to ensure greater degree of security.

Technical Controls

To secure machines (server or endpoints) is needed to apply patches and update antivirus signatures daily. Patch Management is a process to manage how the software is updated to prevent the exploitation of vulnerabilities.

This results in the reduction the time and money spent dealing with vulnerabilities and their exploitation. The Automated Patch Deployment options help EP allows to scan the systems should for virus definition updates frequently. Once the scanning has been completed successfully, EP can also specify the appropriate action to be performed based on the scan results.. Several benefits are provided, such as, Automation of the definition update; and streamlines the anti-virus definition update process.

Hardening of Operating System (OS)

Though Microsoft has been improving the default configuration in every server version, hardening activities are still needed to put the server in a production environment. Specific best practices differ depending on need but addressing these areas before subjecting a server to the internet will protect against the most common exploits. Some common areas of hardening listed below:

- User Configuration
- Network Configuration
- Features and Roles Configuration
- Update Installation
- NTP Configuration
- Firewall Configuration
- Remote Access Configuration
- Service Configuration
- Further Hardening
- Logging and Monitoring

Administrative and Environmental Security measures – Key Controls

The administrative and environmental security measures focus around key control activities like review, restriction, security, protection and authentication. Each of these are explained below in more detail.

Review of privilege access periodically: These reviews can highlight for a multitude of user access errors. User access reviews should be carried out on a periodic basis. The frequency of reviews should be aligned with the security policy of the EP, and aligned with the current best practices of the security industry.

Restricted internet access: Internet is one of the biggest entry points of cyber-attacks, therefore security measures should be applied to mitigate the risk. As happened in the WannaCry incident, an employee can trigger a serious incident by downloading malicious code. Company data must be protected from internet too, potential information leakage can take place through internet. The websites and protocols used by users must be controlled to avoid potential issues

IDS/IPS to secure perimeter: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are a family of security solutions that look for anomalous traffic on the network they are connected to. They employ signature-based scanning with behavioral heuristics to learn the network’s normal traffic patterns and to alert users when rules and thresholds have been broken.

Web Application Firewall (WAF) to protect external facing URLs: A Web application firewall (WAF) is a firewall that monitors, filters or blocks data packets as they travel to and from a Web application. A WAF can be either network-based, host-based or cloud-based and is often deployed through a proxy and placed in front of one or more Web applications. Running as a network appliance, server plug-in or cloud service, the WAF inspects each packet and uses a rule base to analyze Layer 7 web application logic and filter out potentially harmful traffic.

2 Factor authentications: Two-factor authentication (2FA) is based two different factors used during authentication. The possible types are ‘ inherence’ (something you are), ‘ possession’ (something you have), or knowledge (something you know) Using 2 factors (one of each type) improves a lot the security during authentication, due to the need of compromises two elements of different nature instead of one.

Our View of Windows Security

Security is a top priority for IT teams. New threats have made it harder than ever for IT to secure data and applications. Windows Server 2016 gives EP new capabilities to help prevent attacks and detect suspicious activity, with features to control privileged access, help protect virtual machines and harden the platform against emerging threats.

Here are some security feature description that introduced in 2016 (were not present in Windows server 2008 and 2012): Shielded virtual machines, host

guardian service, credential guard, remote credential guard, device guard, control flow guard.

Support developers in the race to create cloud-ready, business-changing apps and services, whether on-premises or in any cloud, using technologies such as containers and the lightweight Nano Server installation option. Windows Server 2016 can help you modernize your apps and innovate faster. Here is the list of features exclusive to 2016 for application platforms: Windows server containers, hyper-v containers, nano server installation option.