The Hague University of Applied Sciences
Lectureship Cybersecurity in SMEs
Analysis-Advice report

KOMP U TER HULP
Opleiding computerhersteller voor voortijdige schoolverlaters (VSV)

Name of assignor:	**Komp u ter hulp**	**Students/Consultants**
Name of Contractor:	**HHS**	**Halit Cankara**
Date:	**17 jul. 21**	**Randy Vos**
Version:	**1.0**	

[A DDoS attack: what is it and what are the consequences?](#)
[Benefits of using best practice](#)

1.1 Recommendation 1: IT Asset Management

IT Asset Management system is an important part of overall systems, which are needed to manage IT infrastructure. Without proper IT Asset Management, the organization will waste time and resources managing inventory, buying unnecessary equipment and software, and maintaining license compliance for software. With a well-functioning IT Asset Management system, the organization can expect to reduce the total cost of ownership for IT infrastructure and provide a solid foundation to keep your IT infrastructure operating efficiently. Managing IT assets is about more than just choosing the best software and devices.

When you deploy ITAM purposefully, you reap benefits such as:

- Improved communication between business units (such as sales, marketing, administration, store personnel);
- Improved software compliance;
- Cost savings in IT resources
- Enhanced data security;
- Improved service delivery through improved data availability;
- Better use of budgets and easy decisions through better understanding of IT resources and their function in the organization

1.2 Recommendation 2: ITIL Certification

ITIL (Information Technology Infrastructure Library) is a framework designed to better manage IT management processes. It provides concrete tools to set up and manage an IT organization.

ITIL certification is an absolute must in order to reduce the high costs associated with IT investments and to provide a solid foundation for total cost of ownership.
In addition, obtaining an ITIL certification is a great addition to the curriculum and demonstrates the student's ability to manage and set up IT management processes.

Recently, the latest version of the ITIL framework was released: ITIL 4. This includes 34 guidelines, defined as means and activities to perform work or achieve an objective. These practices are divided into three categories:

- General management practices, including projects and portfolios, business risk, information security, continuous improvement.
- Management in the area of service management, such as business analysis, service design and continuity, service desk, monitoring and incident management, change processes, and management of IT resources
- Management in the area of technical management, including software development, implementation, infrastructure and platform.

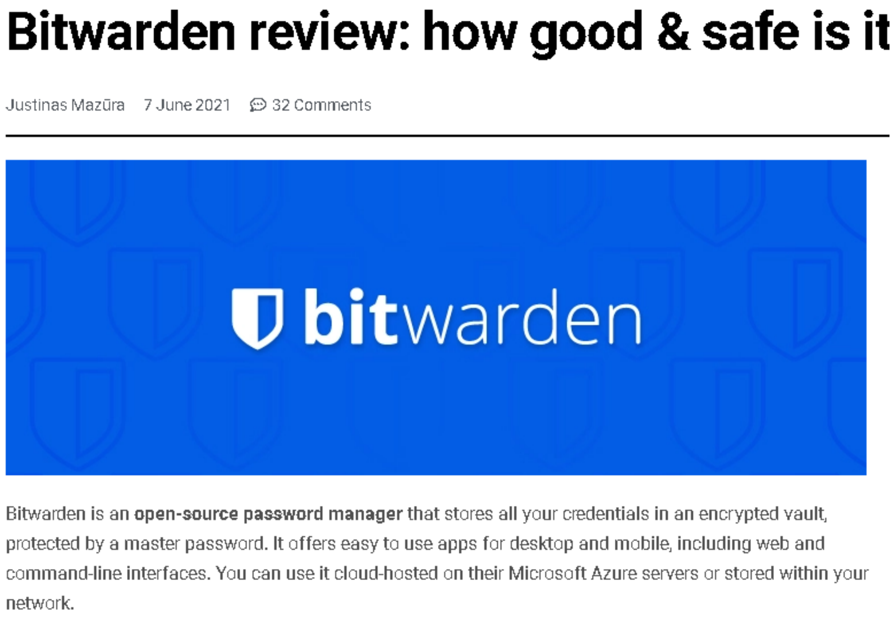
What is IT Asset Management?
ITIL explained (in Jip and Janneke language)

1.3 Recommendation 3: Use malware detection

Malware detection is critical now that malware is so rampant on the Internet, in part because it functions as an early warning system for computer security regarding malware and cyberattacks. It keeps hackers out and prevents information from being intercepted. Antimalware such as the free software Malwarebytes sets an antihacking lock, or runs regular scans to detect the presence of a hacker or malware in the computer network. This software can be used for the systems running virtual machines, and also on students' laptops. Real-time protection should be applied
to computers with name and address information.
This is a paid version of Malwarebytes, but it prevents, among other things, that malicious people secretly look into the computer by means of a RAT.

1.4 Recommendation 4: Use a password manager.

Within the organization, strong passwords, numbers, special characters and capital letters are used. Such as 096#Zaandam
The use of weak passwords can lead to cybercriminals gaining access to the company network and personal data.
This can cause viruses and malware to be installed and a data breach to occur. To prevent this, a password manager is recommended.
With a password manager, passwords can be managed securely and centrally. Also, the password manager itself generates strong passwords so that it does not have to be invented and remembered. In addition, some password managers also offer the ability to safely store other data such as notes, address information and software licenses. The password manager that is recommended is Bitwarden. This is an excellent password manager and is also free. An added value of Bitwarden is that it is open source and therefore cannot hide anything except of course the carefully encrypted passwords.



Bitwarden review: how good & safe is it

Justinas Mazūra 7 June 2021 32 Comments

Bitwarden is an **open-source password manager** that stores all your credentials in an encrypted vault, protected by a master password. It offers easy to use apps for desktop and mobile, including web and command-line interfaces. You can use it cloud-hosted on their Microsoft Azure servers or stored within your network.

Bitwire - GitHub

1.5 Recommendation 5: ISO 27001 certification.

Companies are advised to certify to the ISO 27001 standard. This is a globally recognized standard in the field of information security. This certification demonstrates that the company meets all requirements around information security. It is also true that with the introduction of the General Data Protection Regulation (AVG) the rules in Europe around data protection have been tightened considerably. As an organization this means that the management system for information security must be in order.

ISO 27001 helps you establish an information security management system. Establishing such a system and obtaining the ISO 27001 certification provides the organization with several benefits:

- With ISO 27001, the company shows that it meets the strict norm requirements around information security. More and more customers are demanding that the partners they work with have their information security in order. ISO 27001 certification demonstrates that the company meets all requirements around information security. In this way, the certificate can create commercial opportunities for the organization.
- The ISO 27001 certification helps reduce information security risks and prevent incidents. This protects the reputation of the organization.
- With the ISO 27001 certificate in your pocket, it can be assumed that enough has been done to comply with laws and regulations concerning information security.

1.6 Recommendation 6 Best practice for PXE and Pre-boot OS security.

Security problems begin with network access. The following recommendations should be followed to minimize risk from further potential network breaches via thePXE server.

During the creation of the automation environment, a username and password is used to grant access to shared network folders and locations, including access to the share point and network location of stored image files. It is strongly recommended that this never be a domain account. Create one local user account at each shared network location and grant this user account minimal user privileges (usually only read/write privileges) and only access to specific folders within the sub location (usually the PXE folder named "images" and any required folders).

Note: Special attention should be paid to securing location and protecting saved files to prevent unauthorized tampering with the PXE boot files.

- Limit the availability of PXE services by using MAC address filtering through the PXE configuration utility.
- Limit the availability of ports for network communication to UDP ports 67, 68, 69, and 4011, which are used in the PXE server boot process.

1.7 Recommendation 7: Security setup Azure according to best practice

Trainees are expected to set up an Azure virtual machine according to security guidelines. There are default settings for this that rely on the best-practice from the Microsoft handbook. Azure Virtual Desktop has many built-in security measures. This section provides information on security controls you can use to keep users and data safe.

1) Multi-Factor Authentication

Authentication for users and administrators in Azure Virtual Desktop improves security across the deployment. See Enabling Azure AD Multi-Factor Authentication for Azure Virtual Desktop for more information.

2) Enable conditional access

If conditional access is enabled, risks can be managed before users are granted access to the Azure Virtual Desktop environment. When determining which users will be granted access, it is recommended that we consider who the user is, how they log in, and what device they are using.

3) Collecting Audit Logs

If audit log collection is enabled, user and administrator activity is viewable. Some examples of important audit logs are:

- Azure Activity Log
- Azure Active Directory activity log
- Azure Active Directory
- Session Hosts
- Azure Virtual Desktop diagnostic log
- Key Vault logs

4) Using RemoteApps

When choosing a deployment model, remote users are granted access to entire virtual desktops or specific applications. Remote applications, or RemoteApps, provide a smooth experience when users interact with applications on their virtual desktop. RemoteApps mitigate risk because the user only interacts with a subset of the remote computer made available by the application.

5) Monitor usage with Azure Monitor

Monitor the usage and availability of your Azure Virtual Desktop service with Azure Monitor. Consider creating service health alerts for the Azure Virtual Desktop service to receive notifications when there is an event affecting the service.

Recommended procedures for security

6) Enable Azure Security Center

It is recommended to set up Azure Security Center Standard for subscriptions, virtual machines, key vaults and storage accounts.

Azure Security Center Standard can do the following:

- Managing security issues.
- Evaluate compliance with general frameworks such as PCI.
- Improve the overall security of your environment.

See Your Azure subscription to Security Center Standard for more information.

7) Improve the safety score

Security Score provides recommendations and best practices to improve overall security. These recommendations are prioritized to help choose which ones are most important, and the quick fixes help resolve potential security issues quickly. These recommendations are also updated after a certain period of time to keep one informed of the best ways to maintain security in that environment. For more Azure Security Center, see Improve your Secure Score in Azure Security Center.

8) Monitor usage with Azure Monitor

Monitor the usage and availability of the Azure Virtual Desktop service with Azure Monitor. Consider creating service health alerts for the Azure Virtual Desktop service to receive notifications when there is an event affecting the service.

1.8 Recommendation 8: Best practices for Azure security of session hosts

Session hosts are virtual machines that run within an Azure subscription and virtual network. The overall security of the Azure Virtual Desktop deployment depends on the security controls you implement on the session hosts. This section describes the best practices for securing session hosts.

1) Enable Endpoint Protection

To protect the implementation from known malware, it is recommended to set up endpoint protection on all session hosts. A third-party Windows Defender Antivirus program can be used. See Implementation Guide for Windows Defender Antivirus in a VDI Environment for more information.

For profile solutions such as FSLogix or other solutions that attach VHD files, it is recommended to exclude the VHD file extensions.

2) Install an endpoint detection and response product

It is recommended that an endpoint detection and response (EDR) product be installed to provide advanced detection and response capabilities. For server operating systems Azure Security Center enabled, Defender ATP is implemented by installing an EDR product. For client operating systems, you can implement Defender ATP or a third-party product on these endpoints.

3)Enable threat and vulnerability management.

Identifying software security issues that occur in operating systems and applications is essential to keeping the environment safe. Azure Security Center can identify problems through evaluations of security leeds for server operating systems. Also by using Defender ATP. This provides threat and vulnerability management for desktop operating systems. Third-party products can also be used, but it is recommended to use Azure Security Center Defender ATP.
What is ATP?

English
https://www.techzine.eu/news/security/47703/microsoft-defender-atp-gets-built-in-firmware-protection/

4)Patch security problems with software in the environment

Once a security problem is found, you need to start patching it. This also applies to virtual environments, including the operating systems running, the applications implemented in them, and the images from which new machines are created. Follow vendor notifications and apply patches in a timely manner. We recommend patching base images monthly to ensure that newly deployed machines are as secure as possible.

Best practices for securing session hosts

6) Set maximum idle time and disconnection policy

Logging users out when they are inactive preserves resources and prevents access by unauthorized users. We recommend that timeouts provide a good balance between user productivity and resource utilization. For users working with stateless applications, consider a more aggressive policy to disable machines and preserve resources. Disconnecting long-running applications that are still running when a user is idle, such as simulation or CAD rendering, can interrupt the user's work and may even require restarting the computer.

7) Setting screen locks for inactive sessions

You can prevent unwanted system access by configuring Azure Virtual Desktop to lock a machine's screen during idle time and require authentication to unlock it.

8) Layered administrator access to establish

It is recommended that users not be granted administrator access to virtual desktops. If you need software packages, you can make them available through configuration management utilities, such as Microsoft Endpoint Manager. In a multi-session environment, it is recommended that users not be allowed to install software directly.

9) Consider which users should have access to which resources

Consider session hosts as an extension of the existing desktop implementation. It is recommended that access to network resources be managed in the same way as for other desktops in that environment, such as using network segmentation and filtering.
Session hosts can connect to any resource on the Internet by default. There are several ways you can restrict traffic, Azure Firewall, virtual network devices or perxies. If you want to restrict traffic, you need to make sure the right rules are added so that Azure Virtual Desktop works properly.

10) Manage Office Pro Plus security

In addition to securing session hosts, it is important that you also secure the applications that run in them. Office Pro Plus is one of the most common applications implemented in session hosts. To improve the security of the Office deployment, it is recommended to use security policy advisor for Microsoft 365 apps for business. This utility identifies policies that you can apply to the deployment for greater security. Security Policy Advisor also recommends policies based on their impact on your security and productivity.

11) Other security tips for session hosts

By limiting the capabilities of the operating system, you can improve the security of those session hosts. Here are some things you can do:

- Manage device redirection by redirecting drives, printers, and USB devices to a user's local device in a remote desktop session. it is recommended that you evaluate security requirements and check whether or not these features should be disabled.
- Restrict Windows Explorer access by hiding allocations of local and remote drive. This prevents users from detecting unwanted information about system configuration and users.
- Avoid direct RDP access to session hosts in that environment. If you need direct RDP access for management or troubleshooting purposes, you should enable Just-In-Time access to limit potential attack opportunities on a session host.
- Grant users limited permissions when accessing local and remote file systems. You can limit permissions by ensuring that the local and remote file systems use access management lists with the fewest permissions. This way, users can access only what they need and cannot modify or delete critical resources.
- Prevent unwanted software from running on session hosts. You can enable App Locker for additional security on session hosts, so that only the apps you allow on the host can be run.

11) Support for Azure Virtual Desktop for trusted startup

Trusted launch are Virtual Gen2 VMs from Azure with enhanced security features aimed at protecting against threats on "the bottom of the stack" via attack vectors such as rootkits, boot kits and kernel-level malware. Here are the enhanced security features of trusted start, all of which are supported in Azure Virtual Desktop. Go to Trusted Start for Azure Virtual Machines (preview)for more information on trusted start.

12) Secure Boot

Secure boot is a mode supported by platform firmware that protects your firmware from rootkits and malware-based boot kits. This mode allows only signed BESe's and drivers to boot the machine.

13) Monitor Startup Integrity with Remote Attestation

External attestation is an excellent way to check the status of VMs. External attestation verifies that Measured Boot records are present, legitimate, and originating from the virtual Trusted Platform Module (vTPM). As a status check, it provides cryptographic assurance that a platform has booted properly.

14) vTPM

A vTPM is a virtualized version of a hardware Trusted Platform Module (TPM), with a virtual instance of a TPM per VM. vTPM enables external attestation by performing integrity measurement of the VM's entire boot chain (UEFI, operating system, system, and drivers).

It is recommended to enable vTPM for using external attestation on the VMs. If vTPM is enabled, you can also enable BitLocker functionality, which provides encryption on entire volumes to secure data-at-rest. All features that use vTPM result in secrets that are bound to the specific VM. When users connect to the Azure Virtual Desktop service in a pool scenario, users can be redirected to any virtual machine in the host group. Depending on how the feature is designed, this may have an impact.

15) Note

BitLocker should not be used to encrypt the specific disk on which you store the FSLogix profile data.

16) Security based on virtualization

Virtualization-based security (VBS) uses the hypervisor to create and isolate a protected memory region that is inaccessible to the operating system. Hypervisor-Protected code integrity (HVCI) and Windows Defender Credential Guard both use VBS to provide better protection against security problems.

17) Hypervisor-Protected Code Integrity

HVCI is a powerful system mitigation that uses VBS to protect processes in Windows kernel mode from injection and execution of malicious or unauthenticated code.

18) Windows Defender Credential Guard

Windows Defender Credential Guard uses VBS to isolate and secure secrets so that only authorized system software can access them. This prevents unauthorized access to these secrets and credential theft, such as Pass-the-Hash attacks.

19) Deploy trusted startup in your Azure Virtual Desktop environment

Azure Virtual Desktop does not currently support automatically configuring Trusted Start during the host group installation process. If you want to use Trusted Start in your Azure Virtual Desktop environment, you must implement Trusted Start normally and then manually add the virtual machine to the desired host group.