VIACODE Azure Security Assessment

for

Customer X

XX/XX/202X

Contents

Executive summary

The VIAcode Azure Security Assessment provides an in-depth analysis of the Azure infrastructure security posture. Our analysis delivers actionable recommendations to dramatically improve security, efficiency, and effectiveness of your Azure environment to reduce risks and improve strategies to maintain an optimized and secured Azure environment. The recommendations in this assessment can be used to plan necessary improvements in your Azure environment. VIAcode can help you implement these security improvements.

Using data collected from your Azure environment VIAcode experts analyzed possible infrastructure and data vulnerabilities to deliver the following:

- Prioritized, actionable and specific recommendations for improving your Azure environment.
- Interactive analytical report to help identify infrastructure affected by recommended improvements.
- Estimated value for each proposed recommendation.

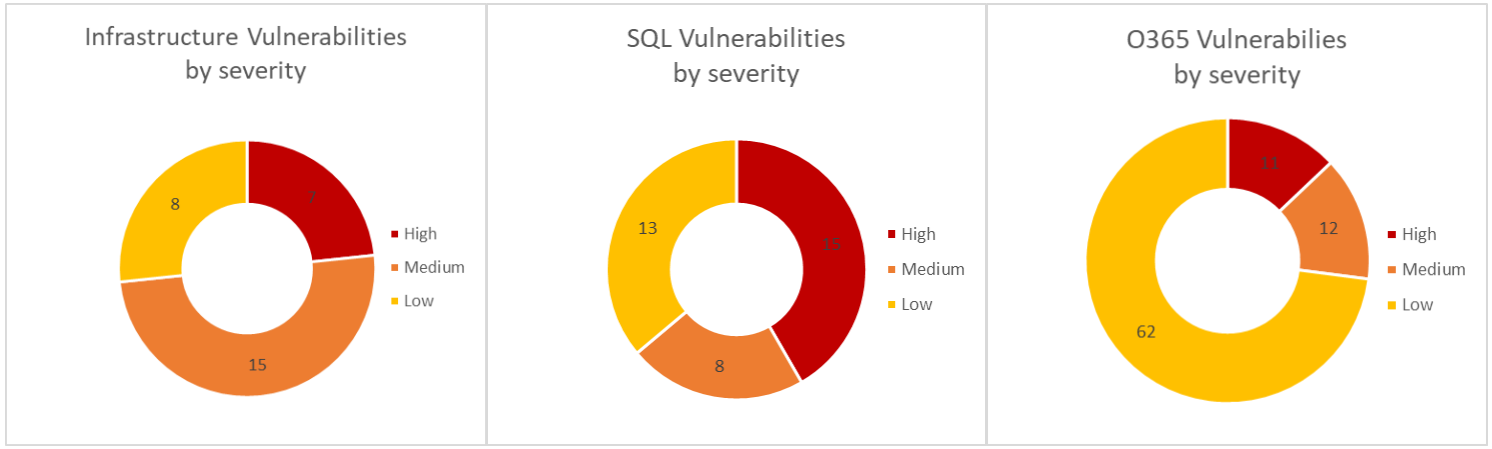
The VIAcode Azure Security Assessment provides a thorough review of your Azure infrastructure to identify key improvement areas and understand the health of the environment. The recommendations in the Assessment can be used to drive security and governance improvements.

The infrastructure security analysis has revealed several high severity vulnerabilities. These issues may potentially put your data at risk. The highest potential threat is a Linux VM that is deployed to the same vnet as your DB server and that has a public IP and open 22 port with unrestricted access. Moreover, the VM authentication method is username-password which may be vulnerable to brute force attacks. This and other high severity issues need to be fixed to make sure your data is safe.

On the SQL server level, a set of high severity vulnerabilities are found. The most critical unequivocal issues need to fixed. Other findings need to be carefully reviewed and fixed or, if the current state is intended, they should be added to the baseline. We recommend not to disable Defender after the trial period so that it keeps checking your DB server and alarm you if the security state changes. New issues may appear or the state may differ from the baseline.

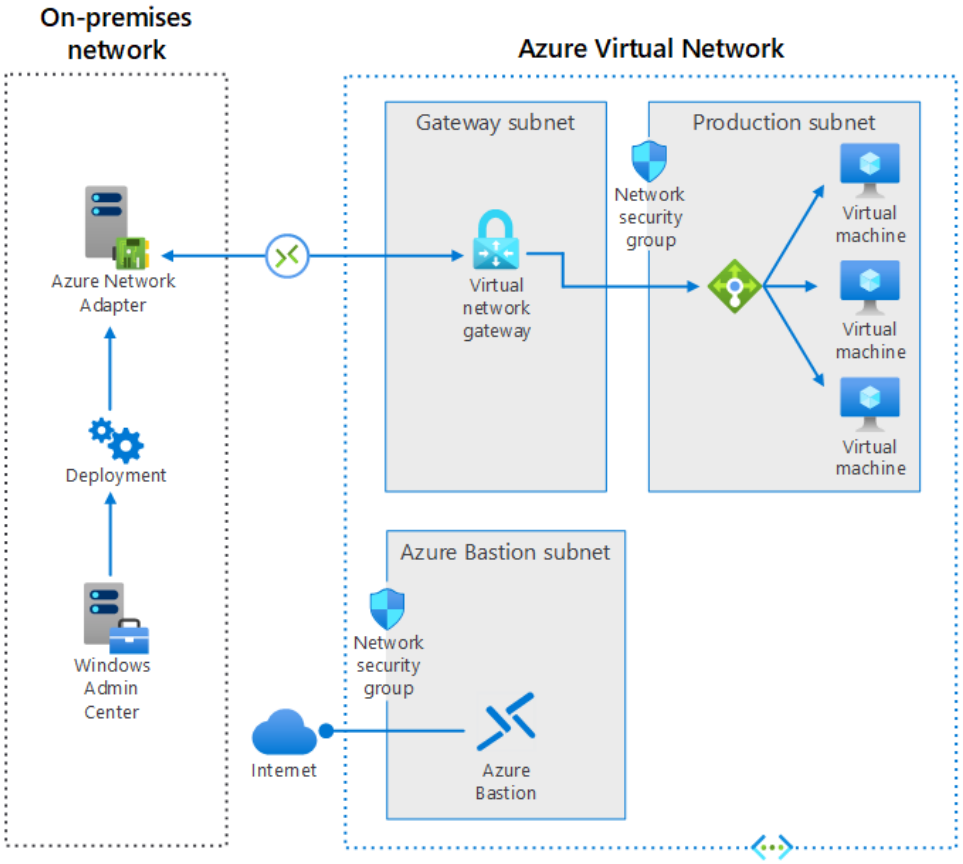
Our analysis of Office 365 vulnerabilities has detected several actions that need to be taken in order to secure your account. The MFA recommendations should be addressed at the first step.

We performed penetration testing of your environment. The testing revealed only one severe vulnerability – we attempted a brute force attack on the Linux server and it did not trigger any alert or blocking. We recommend taking actions to secure the VM to make sure that the brute force attack never succeeds.

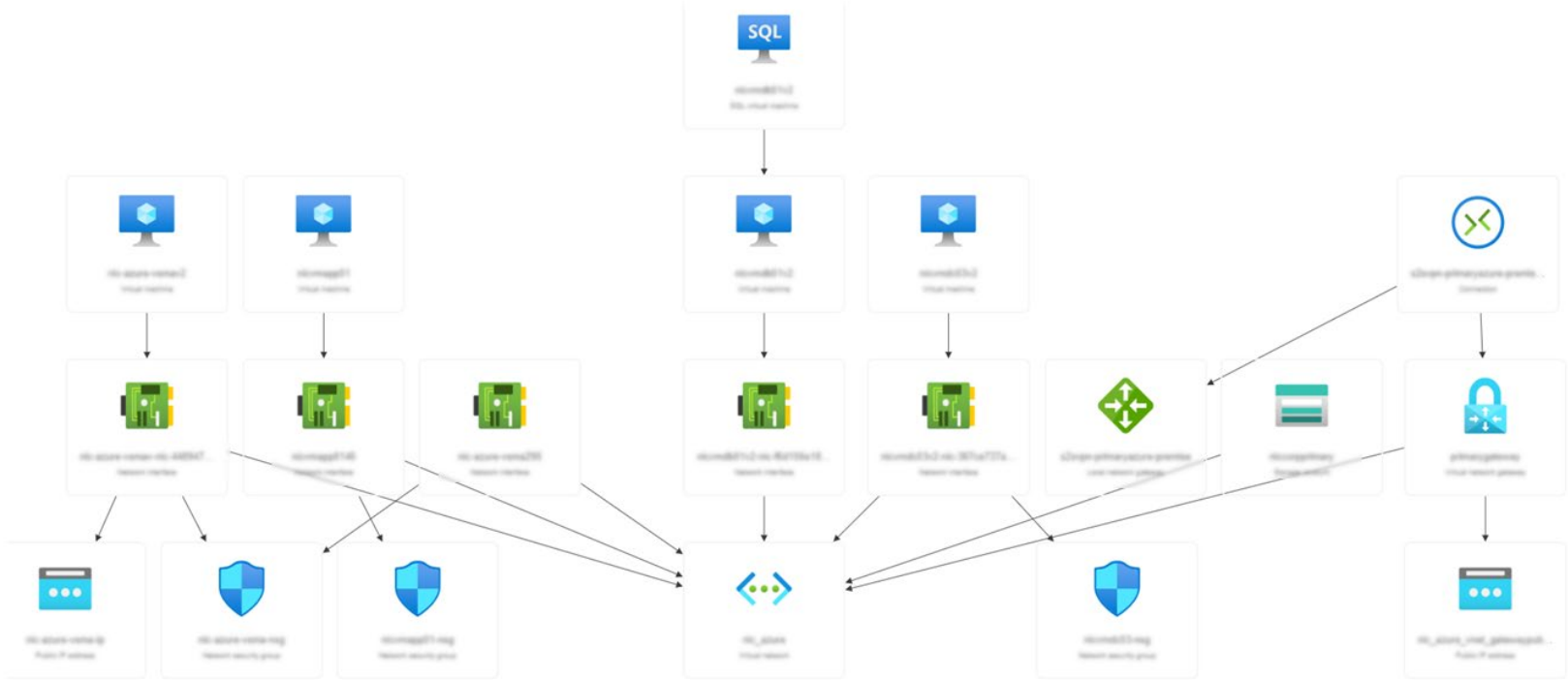


Description of service provided

Infrastructure and network diagram



Azure resources diagram



The DB server environment contains 4 virtual machines:

1. SQL Server VM (SQL-VM1)
2. Domain Controller VM (DC-1)
3. App VM – **Deallocated (App-VM1)**
4. Third-party appliance VM (TPA-VM1)

All machines are in the same network. All machines but the SQL server VM are protected with NSGs.

The virtual network has a VPN gateway. The gateway is not connected to the onprem environment (site-to -site connection is set up but not connected). Point-to-site connection is available.

There are several orphaned resources – network interfaces, public IPs, disks.

Action Items

Infrastructure

1. Secure TPA-VM1
    a. Restrict access to the SSH port (22) of the TPA-VM1 VM doing one of the following
        i. Close the 22 port access in the NSG
        ii. Allow access to only a few IP addresses if the access needs to preserve
    b. Secure SSH authentication of the TPA-VM1 VM. Change the authentication method from username-password to SSH-keys.
    c. Protect the SSH connection with just-in-time network access control.
2. Secure SQL-VM1
    a. Protect the SQL-VM1 VM with a network security group
3. Secure RBAC
    a. Remove external accounts with owner permissions from your subscription, or revoke owner permissions.
    b. Enable Multi-Factor Authentication (MFA) for all subscription accounts with owner permissions.

SQL Server

1. Accounts
    a. Disable the well-known sysadmin account 'sa' on Instance1 and Instance2 SQL instances. Instead use Windows-based groups to grant permissions to DBA and other administrative roles (see VA1058).
    b. The database owner information in the database should match the respective database owner information in the master database. Use ALTER AUTHORIZATION ON DATABASE DDL-command against the database to specify a new server principal that should be the owner of the database (see VA1245)
2. Encryption
    a. Enable ForceEncryption setting on SQL Server Control Manager for Instance1 and Instance2 instances (see VA1220, VA1279)
    b. Enable TDE on the affected databases (see VA1219)
3. Exploit vulnerabilities
    a. Disable the trustworthy bit (TWbit) from all affected databases (see VA1102). If you need to use functionality that is controlled by the TWbit, it is recommended to use digital signatures to enable the functionality instead of enabling the TWbit on the database
    b. Drop CLR assemblies from the affected databases (see VA1256)
    c. Disable the 'xp_cmdshell' feature on the Instance1 instance (see VA1059)
4. Baseline

a. Review other, not mentioned above, vulnerabilities, apply the suggested remediation or add the current state to a baseline.

O365

1. Device protection
    a. Block executable content from email client and webmail
    b. Use advanced protection against ransomware
    c. Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM'
    d. Encrypt all BitLocker-supported drives
2. Identity protection
    a. Require MFA for administrative roles
    b. Ensure all users can complete multi-factor authentication for secure access
    c. Turn on sign-in risk policy
    d. Turn on user risk policy
    e. Set 'Maximum password age' to '60 or fewer days, but not 0'
3. Application protection
    a. Block outdated ActiveX controls for Internet Explorer
    b. Remove TLS 1.0/1.1 and 3DES dependencies

Penetration testing

1. Virtual network
    a. Secure the Linux VM (see recommendations above)
2. Domain controller
   N/A – need internal network access
3. SQL server
   N/A – need internal network access

Security Monitoring

Azure fired one security alert that needs to be resolved.

ALERT TITLE	SEVERITY	FIRST ALERT DATE (UTC)	LAST ALERT DATE(UTC)	REMEDIATION
Traffic detected from IP addresses recommended for blocking	Low	02/15/22, 00:00 AM	03/03/22, 00:00 AM	1. Review the IP addresses and determine if they should be communicating with the virtual machine

				2. Enforce the hardening rule recommended by Defender for Cloud which will allow access only to recommended IP addresses. You can edit the rule's properties and change the IP addresses to be allowed, or alternatively edit the Network Security Group's rules directly

APPENDIX A. Infrastructure vulnerabilities details

ID	SEVERITY	NAME	UNHEALTHY	DESCRIPTION
NS-3.1	High	Management ports should be closed on your virtual machines	1 of 4	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.
NS-1.4	High	All network ports should be restricted on network security groups associated to your virtual machine	1 of 4	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.
NS-3.PA-2.1	High	Management ports of virtual machines should be protected with just-in-time network access control	1 of 4	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations
PA-1.PA-4.2	High	External accounts with owner permissions	1 of 1	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.

		should be removed from your subscription		
IM-6.1	High	MFA should be enabled on accounts with owner permissions on your subscription	1 of 1	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.
IM-6.4	High	Authentication to Linux machines should require SSH keys	1 of 1	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed.
NS-1.2	High	Internet-facing virtual machines should be protected with network security groups	0 of 4	Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at https://aka.ms/nsg-doc
PA-1.PA-4.1	High	Deprecated accounts with owner permissions should be removed from your subscription	0 of 1	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.
IM-6.2	High	MFA should be enabled accounts with write permissions on your subscription	0 of 1	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.
PV-6.6	Medium	SQL servers on machines should have vulnerability findings resolved	4 of 4	SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive