USING VIRTUAL DESKTOP AT-HOME AND IN-OFFICE

AUGUST 2020

ITSAP.70.011

Virtual desktop infrastructure (VDI) allows you to access an entire virtual computer (complete with operating system, storage, and memory) from your existing desktop computer. With VDI, your organization's employees can access organizational applications and data inside and outside the office. VDI is often implemented to reduce hardware costs, but, if not configured properly, VDI can introduce security vulnerabilities to your organization. This document covers the benefits and the risks of using VDI and introduces security practices that you can implement to mitigate the risks.

WHAT IS VDI?

VDI uses technology to host virtual desktop environments on organizationally-owned or personal devices. VDI allows you to access your workstation through a virtual session connected to your device. Your IT team creates a virtual desktop session that clones your organization's system and replicates the desktop session to all users (i.e. everyone accesses a common session to be used by multiple users in parallel).

PERSISTENT VDI AND NON-PERSISTENT VDI

VDI software supports two different approaches: persistent VDI and non-persistent VDI.

With **persistent VDI**, users can save files and customize their desktops. Your organization must configure and update persistent desktops individually to maintain users' personalized desktops. Persistent VDI requires more storage space and backups than non-persistent VDI.

Non-persistent VDI runs multiple users on the same desktop image by cloning a shared master desktop. Non-persistent VDI can be easier to manage because you configure and update only the master desktop. Users cannot personalize their desktops when using non-persistent VDI; when you update the master desktop, its previous images are deleted.

Desktop-as-a-Service (DaaS) is another approach to VDI in which desktop sessions live in the cloud. A third party handles storage, security, backups, and updates for your organization's VDI software and applications.

As the data owner, you are still legally responsible for the security of organizational information when using DaaS services.

WHAT ARE THE BENEFITS?

VDI offers benefits including the following examples:

- **Provide flexible work arrangements**. Employees can work from any location, using the same tools.
- **Manage information effectively**. Employees can use corporate networks, applications, and repositories instead of saving local copies on many devices.
- **Provide IT support from anywhere**. IT teams can connect virtually to devices to run software updates or fix configuration issues.
- **Separate environment from device:** IT teams can dispose of desktop sessions if compromised without affecting the device.
- **Reduce hardware costs**. For example, your organization may rely on fewer in-office servers or implement a mobile deployment model.

WHAT ARE THE RISKS?

One of the most common risks to consider when implementing VDI is software misconfiguration. These misconfigurations can be targeted and taken advantage of by threat actors.

For example, a threat actor can carry out man-in-the-middle (MitM) attacks by taking advantage of misconfigured VDI software to gain entry into your network and systems. In an MitM attack, a threat actor eavesdrops on communications sent between users, or a user and an application, or impersonates one of the parties. Threat actors use MitM attacks to steal sensitive information (e.g. VDI credentials).

Overall, software misconfigurations can weaken your security efforts and result in unauthorized access to systems, data, and unauthorized disclosure (e.g. data and privacy breaches).

Threat actors may also use different attack methods, such as phishing attacks or malware, to gain entry to your network and systems. For more details on phishing attacks and malware, read *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks* or *ITSAP.00.057 Protect Your Organization from Malware*.

AWARENESS SERIES

WHICH MOBILE DEVICES SHOULD BE USED?

You can install VDI software on your users' mobile devices to enable them to connect to your network and access their work desktops from any location.

However, before doing so, you should choose a mobile device deployment model that supports your business needs and meets your security requirements, such as the need to sufficiently handle data based its sensitivity.

For example, if you have remote workers who work with sensitive information, you should give them corporately owned devices to reduce the risk of data mishandling and breaches (e.g. locking-down the endpoint device for organizational use only). With corporately owned devices, your organization has more control over the security controls that are implemented on the devices (e.g. multi-factor authentication, encryption). You can also ensure that the devices are updated regularly.

For more details on mobile deployment models, refer to *ITSAP.70.002 Security Considerations for Mobile Deployment Models* on our website.

HOW DO I SELECT A PROVIDER?

Select a provider that can support your organization's data and security requirements. Look for a provider that provides the following security measures:

- Offers encryption for your organization's data when it is in transit and at rest.
- Offers a virtual private network (VPN).
- Monitors network for any suspicious activity.
- Enables automatic software updates.
- Controls administrator access.
- Uses privileged access management (PAM) to control who can access the servers data.
- Offers multi-factor authentication (MFA).
- Abides by Canadian privacy laws to ensure your data is protected from sharing.
- Supplies advice and guidance on the proper configuration, deployment, and hardening of VDI software.

HOW TO MITIGATE THE RISKS?

To mitigate the risks associated with using VDI, follow these suggested security practices:

- Enforce the principle of least privilege when dealing with sensitive data in business functions.
- Choose a mobile device deployment model suitable for your organization's security requirements (e.g. encrypted data).
- Ensure your IT team separates in-office and remote network zones to restrict the amount of access offered remotely.
- Use an anti-virus software that runs only on master desktops and tests the output before cloning to remote devices (e.g. disable anti-virus on non-persistent desktops).
- Use anti-phishing software that aligns with the Domain-based Message Authentication, Reporting, and Conformance (DMARC) standard.
- Patch and update software and devices frequently.
- Back up your systems regularly.

You should train your employees on security threats (e.g. phishing and social engineering). Encourage employees to follow these cyber security best practices:

- Use passphrases or strong passwords for accounts.
- Use MFA (e.g. a passphrase and a biometric such as a fingerprint) on devices.
- Run updates and patches on devices.
- Use a secure Wi-Fi network and avoid using public, unsecure networks.

WHAT IF I'VE BEEN HACKED?

If you suspect malicious activity is taking place through VDI software or mobile devices, your organization should take the following actions:

1. Restrict access to affected software or disconnect affected devices from your network to protect against continued exploitation.
2. Contact your provider immediately.
3. Restore VDI software through back-ups once exploitation has ended.
4. Use incident data to inform future preventative measures.
5. Report activity to the Cyber Centre: **contact@cyber.gc.ca**

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**