UTILISER UN POSTE DE TRAVAIL VIRTUEL À LA MAISON ET AU BUREAU

AOÛT 2020 **ITSAP.70.111**

L'infrastructure de postes de travail virtuels (VDI pour *Virtual Desktop Infrastructure*) vous permet d'accéder à un ordinateur virtuel complet (ayant un système d'exploitation, un espace de stockage et une mémoire) à partir de votre ordinateur existant. Par l'entremise d'une VDI, vos employés peuvent accéder aux applications et aux données de votre organisation à partir du bureau ou d'un autre emplacement. La VDI est souvent mise en place pour réduire le coût du matériel. Cependant, si elle n'est pas bien configurée, elle pourrait exposer votre organisation à des vulnérabilités de sécurité. Nous présentons ici les avantages et les risques liés à l'utilisation d'une VDI ainsi que les mesures de sécurité que vous pouvez prendre afin d'atténuer les risques.

QU'EST-CE QU'UNE VDI?

La VDI utilise des solutions technologiques pour héberger des environnements de bureaux virtuels sur des dispositifs appartenant à l'organisation ou à l'employé. Elle vous permet d'accéder à votre poste de travail en ouvrant une session virtuelle sur votre dispositif. Pour ce faire, l'équipe des TI crée une session de bureau virtuel qui clone le système de votre organisation et la déploie à tous les utilisateurs (il s'agit d'une session commune à laquelle de multiples utilisateurs accèdent en parallèle).

VDI PERSISTANTE ET NON PERSISTANTE

Les logiciels VDI prennent en charge deux approches différentes : la VDI persistante et la VDI non persistante.

La **VDI persistante** permet aux utilisateurs d'enregistrer des fichiers et de personnaliser leur poste de travail. Votre organisation devra configurer et mettre à jour les postes de travail persistants individuellement pour maintenir les options personnalisées des utilisateurs. Les VDI persistantes nécessitent plus d'espace de stockage et de sauvegardes que les VDI non persistantes.

La **VDI non persistante** permet de connecter de multiples utilisateurs à la même image de poste de travail en clonant un ordinateur principal partagé. La VDI non persistante peut être plus facile à gérer, car il suffit de configurer et de mettre à jour un seul ordinateur principal. Cependant, elle ne permet pas aux utilisateurs de personnaliser leur poste de travail; dès l'ordinateur principal mis à jour, l'image précédente est supprimée.

Les **services de bureau virtuel** (DaaS pour *Desktop-as-a-Service*) sont une autre approche de la VDI dans le cadre de laquelle les sessions de poste de travail sont hébergées dans le nuage. Un tiers s'occupe du stockage, de la sécurité, des sauvegardes et des mises à jour du logiciel VDI et des applications de votre organisation.

En tant que propriétaire des données, vous êtes toujours légalement responsable de la sécurité des renseignements organisationnels quand vous utilisez les services DaaS.

QUELS SONT LES AVANTAGES?

La VDI offre nombre d'avantages, dont les exemples suivants :

- **Elle offre des conditions de travail flexibles.** Les employés peuvent travailler n'importe où, tout en utilisant les mêmes outils.
- **Elle permet de gérer l'information efficacement.** Les employés peuvent utiliser les réseaux, les applications et les répertoires de l'organisation au lieu d'enregistrer des copies locales sur plusieurs dispositifs.
- **Elle permet d'offrir un soutien TI n'importe où**. Les équipes des TI peuvent se connecter virtuellement aux dispositifs pour exécuter les mises à jour logicielles ou pour régler des problèmes liés à la configuration.
- **Elle constitue un environnement indépendant du dispositif.** Les équipes des TI peuvent supprimer toute session compromise sans avoir d'effet sur le dispositif.
- **Elle permet de réduire les dépenses liées au matériel**. Par exemple, votre organisation pourrait avoir besoin de moins de serveurs sur place ou choisir de mettre en œuvre un modèle de déploiement de dispositifs mobiles.

QUELS SONT LES RISQUES?

Les erreurs de configuration logicielle sont l'un des risques les plus communs associés à la mise en œuvre d'une VDI. Des auteurs de menace pourraient exploiter de telles erreurs et en tirer parti.

Par exemple, un auteur de menace pourrait profiter d'un logiciel VDI mal configuré pour lancer des attaques de l'intercepteur afin d'accéder à votre réseau et à vos systèmes. Lors d'une attaque de l'intercepteur, un auteur de menace intercepte les communications entre des utilisateurs, ou entre un utilisateur et une application, ou encore se fait passer pour l'une de ces parties. Les auteurs de menace utilisent les attaques de l'intercepteur pour voler de l'information sensible (p. ex., des justificatifs d'identité de la VDI).

Les erreurs de configuration logicielle peuvent affaiblir vos mesures de sécurité et mener à un accès non autorisé aux systèmes et aux données, ainsi qu'à la divulgation non autorisée (p. ex., fuites de données et atteinte à la vie privée).

Les auteurs de menace peuvent aussi utiliser différentes méthodes d'attaque, notamment en ayant recours à l'hameçonnage ou à des maliciels, dans le but d'obtenir un point d'accès à votre réseau et à vos systèmes. Pour plus de détails sur les attaques par hameçonnage et par maliciel, consultez le document *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage* (ITSAP.00.101) ou le document *Protéger l'organisme contre les maliciels* (ITSAP.00.057).

SÉRIE SENSIBILISATION

QUELS DISPOSITIFS MOBILES CONVIENT-IL D'UTILISER?

Vous pouvez installer un logiciel VDI sur les dispositifs mobiles de vos utilisateurs pour leur permettre de se connecter à votre réseau et d'accéder à leur poste de travail n'importe où.

Cependant, avant de procéder, vous devez choisir un modèle de déploiement de dispositifs mobiles qui répond à vos besoins organisationnels et à vos exigences de sécurité, comme la nécessité de bien gérer les données selon la sensibilité de celles-ci.

Par exemple, si des employés travaillant à distance sont appelés à traiter de l'information sensible, vous devrez leur fournir un dispositif appartenant à votre organisation pour réduire les risques liés à une mauvaise gestion ou à une fuite de données (p. ex., verrouiller le dispositif afin d'en permettre l'utilisation seulement à des fins opérationnelles). Votre organisation sera également mieux à même d'appliquer des contrôles de sécurité sur les dispositifs qui lui appartiennent (p. ex., l'authentification multifacteur et le chiffrement). De plus, vous pourrez ainsi veiller à ce que les dispositifs soient mis à jour régulièrement.

Pour plus de détails sur les modèles de déploiement de dispositifs mobiles, consultez les *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles* (*ITSAP.70.002*) qui se trouvent sur notre site Web.

COMMENT CHOISIR UN FOURNISSEUR

Choisissez un fournisseur qui peut répondre aux exigences de votre organisation sur le plan de la sécurité et des données. Assurez-vous que le fournisseur offre les mesures de sécurité suivantes :

- le chiffrement des données en transit et au repos de votre organisation;
- un réseau privé virtuel (RPV);
- la surveillance du réseau pour détecter toute activité suspecte;
- l'activation des mises à jour logicielles automatiques;
- le contrôle de l'accès administrateur;
- la gestion des accès privilégiés (PAM pour *Privileged Access Management*) permettant de contrôler qui peut accéder aux données des serveurs;
- l'authentification multifacteur;
- le respect des lois canadiennes relatives à la protection de la vie privée afin de veiller à ce que vos données ne soient pas divulguées à d'autres parties;
- la prestation de conseils et d'avis sur la façon de bien configurer, déployer et renforcer le logiciel VDI.

COMMENT ATTÉNUER LES RISQUES

Pour atténuer les risques liés à l'utilisation d'une VDI, suivez les pratiques de sécurité ci-dessous :

- respecter le principe du droit d'accès minimal lorsque vous gérez des données sensibles dans le cadre d'activités opérationnelles;
- choisir un modèle de déploiement de dispositifs mobiles répondant aux exigences de sécurité de votre organisation (p. ex., données chiffrées);
- veiller à ce que votre équipe des TI sépare la zone du réseau local de celle du réseau à distance pour restreindre l'étendue de l'accès offert à distance;
- utiliser un logiciel antivirus qui s'exécute uniquement sur les ordinateurs principaux et qui teste la sortie avant d'effectuer le clonage sur les dispositifs à distance (p. ex., désactiver l'antivirus sur les postes de travail non persistants);
- utiliser un logiciel antihameçonnage conforme à la norme du protocole DMARC (*Domain-based Message Authentication, Reporting and Conformance*);
- appliquer fréquemment les correctifs et les mises à jour aux logiciels et aux dispositifs;
- effectuer régulièrement des sauvegardes de vos systèmes;

Offrir à vos employés de la formation sur les menaces liées à la sécurité (p. ex., hameçonnage et piratage psychologique), et encourager vos employés à suivre les pratiques de cybersécurité présentées ici;

- utiliser des phrases de passe ou des mots de passe robustes pour les comptes;
- utiliser l'authentification multifacteur sur les dispositifs (p. ex., une phrase de passe et une donnée biométrique comme une empreinte digitale);
- effectuer les mises à jour et appliquer les correctifs sur les dispositifs;
- utiliser un réseau Wi-Fi sécurisé et éviter d'utiliser des réseaux publics non sécurisés.

QUE FAIRE EN CAS DE PIRATAGE?

Si votre organisation croit que des activités malveillantes sont menées par l'entremise du logiciel VDI ou de dispositifs mobiles, il conviendra de prendre les mesures suivantes :

1. Restreindre l'accès aux logiciels touchés ou déconnecter les dispositifs touchés de votre réseau pour éviter que les activités malveillantes se poursuivent;
2. Communiquer immédiatement avec votre fournisseur;
3. Restaurer le logiciel VDI au moyen des sauvegardes, une fois les activités malveillantes neutralisées;
4. Utiliser les données de l'incident pour établir des mesures de prévention;
5. Signaler les activités malveillantes au Centre canadien pour la cybersécurité : contact@cyber.gc.ca.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.