Devolutions

10 façons d'accroître la sécurité des réseaux privés virtuels

LES RPV UTILISENT LE CHIFFREMENT POUR CRÉER UNE CONNEXION SÉCURISÉE SUR UNE INFRASTRUCTURE INTERNET NON SÉCURISÉE

On me pose souvent la question suivante : « Les réseaux privés virtuels (RPV) sont-ils sécuritaires pour les entreprises? » La réponse courte : oui! Maintenant, voici la réponse longue :

Les RPV utilisent le chiffrement pour créer une connexion sécurisée sur une infrastructure internet non sécurisée. Si les RPV offrent une sécurité et un anonymat solides, ils ne sont pas à toute épreuve. Tout comme les mots de passe, ils peuvent être piratés. Cependant, il y a certaines choses que toutes les organisations devraient faire pour accroître leur protection. Voici 10 éléments à considérer :

1. Utilisez l'authentification à 2 facteurs/multifacteur

Il arrive qu'un mot de passe soit compromis ou que les certificats des clients du RPV et les témoins d'authentification soient utilisés pour contourner l'authentification. Dans ces cas, l'authentification à deux facteurs (A2F) ou multifacteur (MFA) sur votre RPV peut être votre dernière et meilleure ligne de défense. Bien sûr, il va sans dire (mais je le mentionne quand même juste au cas où) qu'il est essentiel de mettre en place une bonne politique de mots de passe dans votre organisation.

2. Utilisez le protocole OpenVPN

Les RPV prennent en charge différents protocoles qui offrent différents niveaux de sécurité. Les trois protocoles les plus courants sont PPTP, L2TP et OpenVPN :

- Le PPTP est le protocole le plus faible. Il utilise un chiffrement de 128 bits, et le processus d'authentification et de connexion peut être intercepté par des pirates informatiques - ce qui entraînerait le décryptage et la compromission des données. Le PPTP est cependant l'un des protocoles les plus rapides, justement parce qu'il est le moins chiffré.
- Le protocole L2TP est plus sûr que le PPTP, mais il est assez lent et peut augmenter considérablement les coûts d'exploitation.
- OpenVPN offre le plus haut niveau de sécurité et de confidentialité. Il est relativement rapide et la récupération après une perte de connexion se fait aussi rapidement. Nous recommandons fortement aux organisations d'utiliser uniquement une solution RPV qui prend en charge OpenVPN.

3. Bloquez les fuites de DNS

A DNS leak is a security flaw that enables DNS requests to be revealed to ISP DNS servers, even though the VPN service attempts to conceal them. If this happens in your organization, then contact your VPN vendor and see if they offer DNS leak protection. If not, it is probably necessary to start shopping for another solution.

4. Utilisez un bouton d'arrêt

Dans le cas peu probable où votre connexion RPV tomberait en panne, vous risqueriez d'utiliser une connexion

ordinaire non protégée gérée par votre fournisseur d'accès Internet. Un bouton d'arrêt virtuel (mieux connu sous le nom *Kill Switch*) permet d'éviter ça en fermant les applications et en empêchant l'accès aux sites Web dès que la connexion est perdue.

5. Utilisez le verrouillage du réseau

Si votre réseau Wi-Fi est interrompu, un verrou de réseau bloque automatiquement l'accès de votre ordinateur à l'Internet. Ça permet de sécuriser et de protéger les informations pendant la reconfiguration du RPV.

6. Bloquez les fuites d'IPv6

IPv6 est une version du protocole Internet qui vous permet d'accéder à plus d'adresses Internet qu'IPv4. Le problème avec l'IPv6 est qu'il fonctionne en dehors du territoire du RPV et qu'un pirate informatique pourrait l'utiliser pour voir qui vous êtes. Je vous recommande de faire un test rapide ici pour vérifier si vous êtes en sécurité. Sinon, vous pouvez désactiver IPv6 manuellement en exécutant la commande suivante sous Windows :

```
netsh interface teredo set state disabled
```

7. Bloquez les fuites de WebRTC

WebRTC (*Web Real-Time Communication*) est un projet à code source ouvert qui permet à deux appareils de communiquer entre eux en diffusant leurs adresses IP respectives. Il est utilisé par la plupart des navigateurs (par exemple Chrome, Firefox, Safari, Edge et les navigateurs mobiles pour Android et iOS) pour diverses applications d'appels vocaux et vidéo (comme Google Hangouts, Skype for Web, Discord, etc.).

Le problème? Chaque fois qu'un utilisateur se connecte à un site dont le WebRTC est activé, celui-ci peut transmettre des données en dehors du tunnel chiffré du RPV. Ça permet de connaître l'adresse IP réelle de l'utilisateur et sa localisation. Comment pouvez-vous savoir si ça se produit? Faites ce test : désactivez votre RPV et connectez-vous à un site qui utilise le WebRTC. Regardez vos informations de connexion et notez l'adresse IP. Ensuite, lancez votre RPV. Si votre adresse IP change pour celle du RPV ou disparaît, il n'y a pas de fuite de WebRTC. Si votre adresse IP reste la même, alors il y a une fuite.

Dans ce cas, la meilleure solution est de choisir un autre service RPV qui bloque le trafic WebRTC pour qu'il ne soit pas transmis en dehors du tunnel RPV chiffré. Si le changement de RPV n'est pas pratique ou financièrement faisable à l'heure actuelle, vous pouvez le bloquer manuellement dans votre navigateur. Pour les étapes et les captures d'écran sur la façon de procéder, je vous recommande cet excellent article sur Comparitech.com.

8. Limitez l'accès au RPV

Limiter l'accès au RPV à des utilisateurs autorisés spécifiques, et uniquement pour la durée requise. N'oubliez pas qu'une connexion RPV est une porte vers votre réseau local.

9. Utilisez un Intranet ou un Extranet au lieu d'un RPV

Il peut être prudent de permettre aux utilisateurs d'accéder à certains documents via un site web HTTPS sécurisé avec une authentification A2F ou MFA plutôt que via un RPV. Dans cette configuration, une violation n'exposera que des documents sélectionnés sur un seul serveur comparativement à l'ensemble du réseau.

10. Sécurisez les réseaux sans fil distants

Les routeurs sans fil sont étonnamment peu sûrs par défaut et ces vulnérabilités peuvent nuire à la sécurité des RPV. Il y a beaucoup de choses que les utilisateurs finaux peuvent faire (ou qui peuvent être faites en leur nom par l'équipe TI) pour corriger le tir. Plutôt que de toutes les énumérer ici, je vous encourage à lire et à partager notre article « 9 conseils pour rendre votre réseau sans fil domestique plus sécuritaire ». Et bien sûr, ces conseils s'appliquent également à la sécurisation des réseaux sans fil d'entreprise!

En bref

La mise en œuvre de tous les conseils ci-dessus rendra-t-elle votre RPV absolument, catégoriquement et sans équivoque impénétrable? Malheureusement, non. Cependant, ça améliorera considérablement la sécurité des données et réduira la probabilité et la gravité d'une faille. C'est pourquoi je vous invite fortement à en faire une priorité absolue.

Si vous n'êtes pas satisfait de votre RPV actuel ou si vous souhaitez explorer ce qui est disponible sur le marché, alors je vous invite à consulter notre comparaison de 8 RPV populaires. Et si vous avez d'autres conseils ou astuces pour sécuriser les RPV, commentez ci-dessous pour qu'on puisse tous bénéficier de vos connaissances et de votre expérience!