LIGNES DIRECTRICES POUR LA MISE EN PLACE D'UN VPN

MAI 2020

DROITS D'UTILISATION

APPROBATION, HOMOLOGATION DE PRODUITS

Les produits, fabricants et constructeurs de produits qui sont cités dans le présent document sont présentés exclusivement à des fins d'information et ne constituent en aucune façon une approbation, homologation ou promotion desdits produits ou constructeurs par le CI-CERT.

AVERTISSEMENT, LIMITATION DE RESPONSABILITE

Tous les efforts ont été déployés par les auteurs pour rendre le présent document le plus complet, exhaustif et précis possible. Cependant, aucune garantie n'est apportée sur la complétude et la précision des informations qui y sont contenues. En effet, les informations sont fournies "en l'état" et ne renferment nullement le caractère de résultats d'évaluation, comparaison, etc. Par conséquent, le CI-CERT décline toute responsabilité en ce qui concerne les pertes ou dommages résultant de la dépendance ou de l'usage des informations contenues dans le présent document.

Les produits, fabricants et constructeurs de produits qui sont cités dans le présent document sont présentés exclusivement à des fins d'information et ne constituent en aucune façon une approbation, homologation ou promotion desdits produits ou constructeurs par le CI-CERT.

TABLE DES MATIÈRES

INTRODUCTION

Dans un monde numérique hyper connecté où les échanges sont ultra dynamiques et quasi instantanés, les entreprises doivent assurer en permanence leur présence sur le marché, afin de garder leurs services et offres commerciales compétitives. La disponibilité et l'accessibilité des systèmes d'information et des données sont devenues essentielles, voire vitales pour les entreprises. Il est impératif que les utilisateurs en général (clients, partenaires, etc.) et les employés en particulier aient accès aux systèmes chaque fois que le besoin se manifeste. Notamment, en voiture, en réunion, lorsqu'ils sont chezeux ou même lorsqu'ils voyagent à l'étranger. En effet, les organisations doivent mettre au point des mécanismes sécurisés spécifiques viables, afin de rendre les systèmes accessibles à leurs employés de manière sûre. Une des solutions les plus utilisées consiste à utiliser les services VPN pour se connecter aux systèmes d'entreprise à partir de sites distants. Un VPN (Virtual Private Network) ou réseau privé virtuel est un mécanisme qui consiste à relier directement des ordinateurs distants entre eux, de sorte à isoler les échanges de données qui y sont effectués, du reste du trafic se déroulant sur des réseaux publics. Ce document examine certains des risques posés par l'utilisation des technologies VPN ; et comment les atténuer afin de fournir un accès sécurisé à ses employés lorsqu'ils accèdent aux systèmes d'entreprise à partir de réseaux non fiables.

L'objectif de ces lignes directrices est d'aider les organisations, de comprendre les risques potentiels de sécurité de l'information associés à l'utilisation des services VPN et d'identifier les contrôles appropriés pour atténuer ou éviter ces risques.

COMPRENDRE LES RISQUES

Les VPN vous permettent de connecter un système distant à votre système d'entreprise. Le système distant peut être un appareil appartenant à une entreprise et géré par elle ou un appareil domestique géré par un employé ou pire un terminal public dans un cybercafé, un salon d'affaires ou un aéroport. Ces appareils peuvent se connecter par une connexion internet à large bande domestique, par les services de données des FAI, par le wi-fi public ou par les réseaux sans fil invités, dans tous les cas des réseaux non fiables pour ainsi dire.

En tant que tel, vous augmentez la surface d'attaque de vos systèmes à moins que ces menaces ne soient correctement contrôlées et que les risques soient atténués.

Accéder à distance aux services et ressources informatiques d'une entreprise l'expose à des risques, dont les plus importants sont :

1) **Perte de données personnelles et confidentielles ;**
2) **Attaques de déni de service et prévention de l'utilisation de systèmes opérationnels ;**
3) **Corruption des données entraînant une perte d'intégrité ;**
4) **Fraude financière ;**
5) **Dommages répressifs causés par l'un ou l'autre de ces risques.**

DES MENACES EVOLUTIVES

Quelques-unes des principales menaces auxquelles sont confrontés les services VPN mal configurés ou mal sécurisés incluent sans s'y limiter :

Attaques basées sur le Wi-Fi : A moins d'être correctement sécurisés, les systèmes Wi-Fi traditionnels sont vulnérables et les acteurs malveillants (il pourrait s'agir d'initiés tels que les clients utilisant le Wi-Fi ou les pirates informatiques, les cybercriminels, etc.) pourraient les utiliser pour pénétrer les systèmes d'entreprise ou d'autres utilisateurs.

Attaques DDoS et botnet : Les attaques par déni de service distribué ont gagné en popularité pour mener à bien une gamme d'activités d'injection de logiciels malveillants. Dans le cadre de telles attaques, les pirates utilisent des réseaux de machines compromises pour inonder les systèmes critiques de trafic, ce qui entraîne un crash de la plate-forme. Les attaquants peuvent aussi demander aux propriétaires de verser une rançon pour éviter que de tels systèmes ne soient perturbés.

Fuites de données : Il s'agit d'attaques où des acteurs malveillants ont accès à vos systèmes et y restent autant que possible et essaient d'identifier et d'extraire des données critiques en dehors de l'organisation. Les données comprennent des informations sensibles liées aux plans stratégiques d'affaires, ainsi que des informations sur les données à caractère personnel de clients (nom, prénoms, numéros de carte de crédit, numéro de compte bancaire, informations sur l'état de santé, etc.

Hameçonnage : Il s'agit d'attaques au cours desquelles l'attaquant agit comme une institution légitime ou un individu pour inciter la cible à fournir des données sensibles telles que des informations personnelles d'identification, des données bancaires et de carte de crédit, et des mots de passe, etc.

RECOMMANDATIONS

Veiller à ce que les systèmes d'information soient disponibles et accessibles en tout temps est devenue une nécessité vitale et plus un luxe. Cependant, il est très important de veiller à ce qu'il n'y ait pas de failles susceptibles de faciliter l'accès illicite aux données ou systèmes ou d'en modifier le fonctionnement ou l'intégrité. À cet effet, les organisations devraient s'assurer que l'accès à distance fourni à leurs employés et/ou à la chaîne d'approvisionnement est sécurisée et respecte les meilleures pratiques.

Les organisations devraient assurer la sécurité par une approche de conception en toute sécurité dans leurs systèmes d'entreprise. Au minimum, il faut tenir compte des facteurs et principes de sécurité suivants :

1

SURFACE D'ACCES

L'accès aux ressources devrait être limité uniquement aux systèmes restreints et dument contrôlés. De plus, il faut s'assurer de ne fournir que les renseignements requis, en masquant toutes les autres informations autant que possible (concept de "sécurité par l'obscurité").

2

DEFENSE EN PROFONDEUR

Protéger les actifs informationnels à plusieurs niveaux et points à l'aide de techniques et de technologies multiples. La sécurité du système devrait être évaluée en fonction du bien le moins sécurisé du système (lien le plus faible).

3

PROTECTION ADEQUATE

Les contrôles de sécurité choisis devraient être adéquats et appropriés en fonction du profil de risque de l'organisation, du risque pour le bien lui-même ainsi que sa valeur intrinsèque.

Authentification

1) Utilisez l'authentification multi-facteur (MFA) pour vous protéger contre toute violation de mot de passe ;
2) Mettre en œuvre des DMZ (Demilitarized Zone) ou zone démilitarisée ;
3) Dans le cas où il ne serait pas possible de mettre en œuvre la DMZ, les organisations devraient utiliser le nom d'utilisateur et les mots de passe avec des mesures supplémentaires telles que la liste d'autorisation de la source IP, le filtrage des adresses MAC, etc. ;
4) Les mots de passe doivent être conformes à la politique de mot de passe de l'entreprise. Utilisez des mots de passe faciles à mémoriser et difficiles à deviner et prenez le soin de les changer à intervalles réguliers ;
5) Une attention particulière devrait être accordée aux comptes administratifs ou privilégiés.

Autorisation

1) L'accès aux systèmes d'entreprise devrait être assuré en fonction des privilèges et du besoin de savoir et de la nécessité d'avoir accès ;
2) Limitez le nombre de systèmes ou d'hôtes ciblés qui seront accessibles aux utilisateurs distants ;
3) Limitez le nombre de protocoles et de services utilisés par les utilisateurs distants. Par exemple, n'autorisez que les protocoles sécurisés tels que Https ;
4) Restreignez l'utilisation du Bureau à distance pour accéder aux dossiers de partage, à moins qu'il n'y ait une nécessité commerciale manifeste ;
5) Pour les ordinateurs de bureau distants, les organisations devraient explorer des options telles que :
    a. Utilisation de passerelles Bureau à distance : Toutes les demandes d'ordinateurs de bureau distants doivent être traitées par un serveur central.
    b. Tunnelisation du bureau distant : Si l'utilisation d'une passerelle Bureau à distance n'est pas possible, vous pouvez ajouter une couche supplémentaire d'authentification et de chiffrement de vos sessions Bureau à distance via IPSec ou SSH.
    c. Modification du port d'écoute pour le Bureau à distance : La sécurité par l'obscurcissement, le changement du port d'écoute peut protéger contre les pirates qui analysent votre réseau.

Disponibilité

1) Prémunissez-vous contre les arrêts de fonctionnement dus à des pannes, en utilisant des éléments redondants en haute disponibilité ;
2) Veillez à ce qu'une bande passante suffisante soit disponible pour assurer que les utilisateurs d'accès à distance puissent accéder aux services clés sans aucune latence ;
3) Mettez en place des contrôles pour protéger contre les attaques par déni de service (DOS/DDOS) ;
4) Utilisez judicieusement des applications telles que la vidéoconférence (selon le besoin) pour conserver la bande passante ;
5) Assurez et surveillez les accords de niveau de service avec votre fournisseur de services Internet.

Intégrité

1) Assurez l'intégrité de la solution VPN déployée en veillant à ce que le logiciel et le matériel soient mis à jour avec les correctifs les plus récents ;
2) Assurez-vous que l'ordinateur de l'utilisateur distant soit géré et restreint conformément à la politique de sécurité de l'information de l'entreprise, notamment mis à jour avec les derniers correctifs, renforcé conformément à la stratégie de l'entreprise et configuré avec un système de protection Endpoint ;
3) Si vous autorisez les utilisateurs distants à utiliser leurs appareils personnels, tels que des ordinateurs portables et des tablettes, assurez-vous qu'ils respectent une configuration minimale acceptable. Cela devrait inclure un système d'exploitation acceptable (avec un niveau de patch minimum) et un système de protection des points de terminaison avec les derniers correctifs et mises à jour ;
4) L'accès aux systèmes d'entreprise devrait être interdit depuis des réseaux Wi-Fi publics ;
5) N'autorisez pas le tunneling fractionné à moins que des contrôles appropriés ne soient en place et n'autorisent qu'une seule connexion à la fois ;
6) Déconnectez les VPN du réseau après une période d'inactivité prédéfinie et exigez que l'utilisateur se reconnecte au réseau.

Confidentialité

1) Assurez –vous que toutes les demandes de service Internet provenant de la navigation Internet et des services DNS (Domain Name Services) sont acheminées via la connexion Internet de l'entreprise et journalisées ;
2) Sécurisez la configuration des serveurs VPN ;
3) Une copie de la configuration mise à jour et testée doit être stockée dans un endroit sécurisé à utiliser en cas de sinistre ;
4) Implémentez et utilisez 6PE (IPv6 Provider) et 6VPE (IPv6 VPN Provider Edge) ;
5) Il est recommandé de traiter l'espace, l'itinéraire et la séparation du trafic avec l'aide de la VRF (applicable uniquement à 6VPE) ;
6) Masquer le cœur IPv4, ce qui permet de supprimer toutes les attaques contre les routeurs ;
7) Sécurisez le protocole de routage entre le bord client (CE) et le bord fournisseur (PE). Dans le cas de 6PE et 6VPE, les adresses à lien local qui ne peuvent être atteintes de l'extérieur, peuvent être utilisées.

Journalisation et surveillance

1) Définissez et mettez en œuvre un processus de journalisation et de surveillance conforme à la politique sur les NIA ;
2) Assurez-vous que tous les utilisateurs distants de la connexion VPN qui accèdent aux applications internes et externes sont enregistrés ;
3) Assurez-vous que les événements appropriés sont journalisés. Le système de journalisation doit pouvoir retracer la date, l'heure, les noms d'utilisateurs, les adresses IP, les services et les applications utilisés par les utilisateurs distants ;
4) Conservez les journaux pendant au moins pendant la durée légale et/ou réglementaire, conformément aux lois et règlements auxquels vous êtes assujettis ;
5) Surveillez les journaux de sécurité 24h/24 et 7j/7, du moins pour les systèmes critiques ;
6) Il est recommandé de corréler les journaux de divers systèmes, afin d'obtenir une vision globale des opérations ;
7) Assurez-vous que les systèmes distants et VPN sont synchronisés avec le serveur NTP d'entreprise.

Références documentaires

- https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel
- https://www.futura-sciences.com/tech/definitions/connection-vpn-1819/
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration_guide/mpls/b_166_mpls_9500_cg/b_166_mpls_9500_cg_chapter_0101.pdf

Découvrez et téléchargez gratuitement plus de ressources informatives utiles sur la cybersécurité, en visitant le lien suivant :

https://www.cicert.ci/index.php/ressources/cybersecurite-tics/guides

Abidjan - Marcory Anoumanbo -

Adresse Postale : 18 BP 2203 Abidjan 18 - Côte d'Ivoire

Téléphone : +225 20 34 43 73 / +225 20 34 43 74 ---

Fax : +225 20 34 43 75

E-mail : info[@]cicert.ci

Site web: www.cicert.ci