UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

DMZ - Réseau

Revue Générale

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIERES

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

PRÉFACE

La lecture de ce document est destinée redécouvrir la notion de DMZ dans un environnement actuel marqué par la transformation numérique avec les enjeux sécuritaire important en découlant. Ce document devrait permettre également d'initier une réflexion autocritique sur notre application des notions de DMZ et de segmentation réseau.

Nous allons revisiter les DMZ, clarifier leur rôle, leur fonctionnement, les avantages et enjeux éventuels d'implémenter une DMZ et les meilleurs pratiques d'implémentation.

RÉSUMÉ

Aujourd'hui, les réseaux informatiques sont un élément essentiel de tout environnement d'entreprise et, en termes de sécurité, il doit être le plus efficace possible si nous voulons que la sécurité règne dans l'environnement de travail. L'une des fonctions du routeur est d'aiguiller le trafic et de matérialiser les ports d'entrée du réseau pour aussi le protéger des connexions externes. Ici, nous parlons de la DMZ.

Avant d'expliquer ce qu'est la DMZ et à quoi elle sert, nous voulons souligner un facteur très important. Dans tout type d'action qui implique les mots sécurité et informatique, Nous devons être très prudents et toujours effectuer ces configurations si nous avons les connaissances nécessaires ou un soutien professionnel. Cela dit, voyons ce qu'est la DMZ.

RÉFÉRENCES

https://www.cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones

https://www.cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones

https://www.ssi.gouv.fr/uploads/2020/06/anssi-guide-passerelle_internet_securisee-v3.pdf

https://www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/

https://www.techtarget.com/searchsecurity/definition/DMZ

https://ipwithease.com/cisco-asa-configuration-for-dmz-to-inside-zone-and-dmz-to-internet-zone-communication/

https://www.ciscopress.com/articles/article.asp?p=1823359&seqNum=5

https://community.spiceworks.com/topic/2298909-design-config-dmz-on-cisco-asa

CONCEPT DE ZONE DÉMATÉRIALISÉE - DMZ

Le terme « DMZ » vient du concept militaire de zone démilitarisée, une zone neutre qui sépare les parties belligérantes. Au lieu de séparer les armées, un réseau DMZ est conçu pour séparer le grand public - et les pirates - d'un réseau interne. Dans le scénario DMZ le plus courant, un pare-feu sépare le réseau en trois segments : le réseau interne hébergeant les ressources critiques, la DMZ et Internet. Toute communication entre serveurs situés dans des zones différentes doit passer par le pare-feu et est soumise aux politiques de sécurité du réseau.

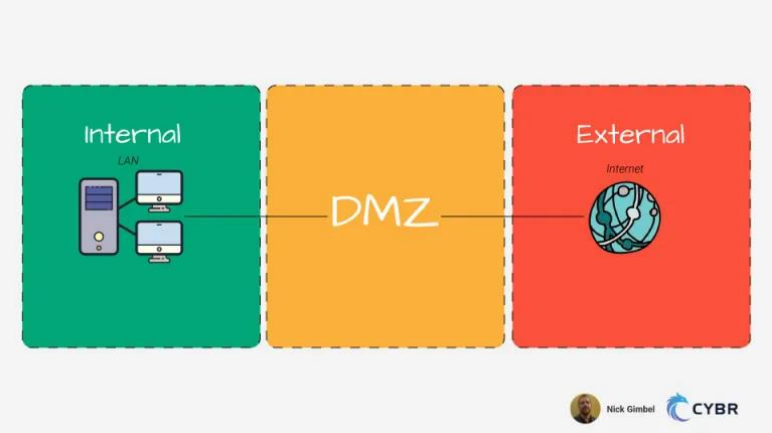

Figure 1. Vue simplifiée DMZ

La DMZ est donc un mécanisme couramment utilisé dans l'environnement des entreprises pour protéger les connexions réseaux. Il s'agit d'un réseau local (IP privé) qui se situe entre le réseau interne de toute entreprise et le réseau externe à celle-ci (Internet). Elle (la DMZ) agit comme un filtre entre la connexion Internet et le réseau d'ordinateurs et serveurs privés où elle fonctionne. Ainsi, l'objectif principal est de vérifier que les connexions entre les deux réseaux sont autorisées.

La DMZ typique abrite des serveurs Web, des serveurs de messagerie, des serveurs DNS et d'autres systèmes qui doivent avoir un certain niveau d'accessibilité depuis le monde extérieur. La DMZ est configurée de manière à ce qu'un attaquant capable de compromettre l'un de ces serveurs puisse exploiter ce serveur pour accéder uniquement aux autres systèmes de la DMZ, isolant le réseau interne de l'attaque. Pour cette raison, il est essentiel de concevoir des couches supplémentaires de contrôle de sécurité autour de la DMZ.

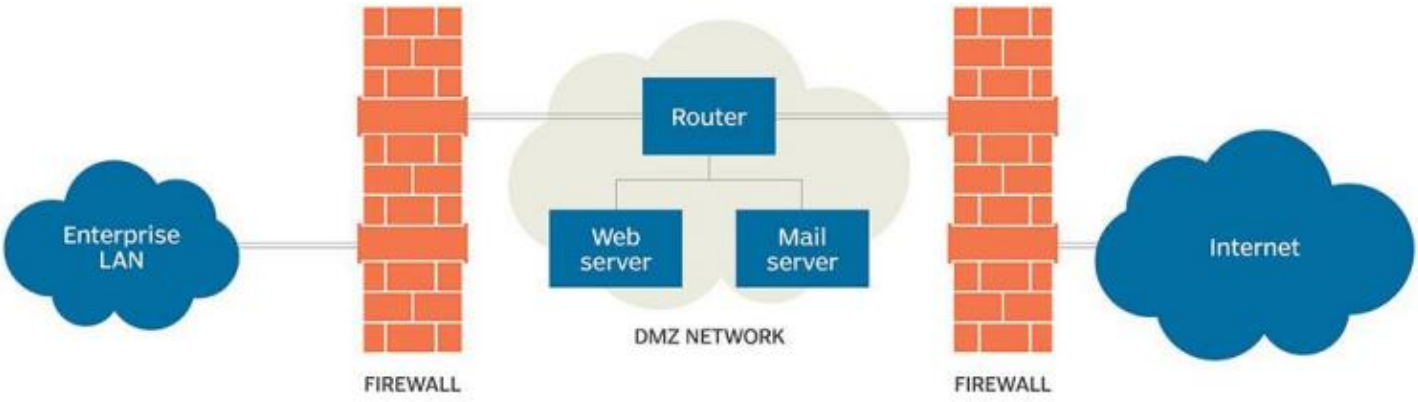

Figure 2. Vue globale DMZ

RÔLE D'UNE DMZ

Les réseaux DMZ sont une partie importante de la sécurité des réseaux d'entreprise depuis presque aussi longtemps que les pare-feu sont utilisés. Ils sont déployés pour des raisons similaires : pour protéger les systèmes et ressources organisationnels sensibles. Les réseaux DMZ sont souvent utilisés pour les éléments suivants :

1. Isoler et maintenir les systèmes cibles potentiels séparés des réseaux internes ;
2. Réduire et contrôler l'accès à ces systèmes par des utilisateurs externes ; et
3. Héberger les ressources de l'entreprise pour en rendre certaines accessibles aux utilisateurs externes autorisés.

Plus récemment, les entreprises ont choisi d'utiliser des machines virtuelles ou des conteneurs pour isoler des parties du réseau ou des applications spécifiques du reste de l'environnement de l'entreprise. Les technologies cloud ont largement éliminé la nécessité pour de nombreuses organisations d'avoir des serveurs Web internes. Une grande partie de l'infrastructure externe autrefois située dans la DMZ de l'entreprise a migré vers le cloud, comme les applications de logiciel en tant que service.

Le réseau DMZ existe pour protéger les hôtes les plus vulnérables aux attaques. Ces hôtes impliquent généralement des services qui s'étendent aux utilisateurs en dehors du réseau local, les exemples les plus courants étant la messagerie électronique, les serveurs Web et les serveurs DNS. En raison du potentiel accru d'attaque, ils sont placés dans le sous-réseau surveillé pour aider à protéger le reste du réseau s'ils sont compromis.

Les hôtes de la DMZ ont des autorisations d'accès étroitement contrôlées aux autres services du réseau interne, car les données transmises par la DMZ ne sont pas aussi sécurisées. De plus, les communications entre les hôtes de la DMZ et le réseau externe sont également limitées pour aider à augmenter la zone frontalière protégée. Cela permet aux hôtes du réseau protégé d'interagir avec le réseau interne et externe, tandis que le pare-feu sépare et gère tout le trafic partagé entre la DMZ et le réseau interne. En règle générale, un pare-feu supplémentaire sera chargé de protéger la DMZ de l'exposition à tout ce qui se trouve sur le réseau externe.

Tous les services accessibles aux utilisateurs en communiquant depuis un réseau externe peuvent et doivent être placés dans la DMZ, si celle-ci est utilisée. Les prestations les plus courantes sont :

1. **Serveurs Web** : les serveurs Web chargés de maintenir la communication avec un serveur de base de données interne peuvent devoir être placés dans une DMZ. Cela permet de garantir la sécurité de la base de données interne, qui stocke souvent des informations sensibles. Les serveurs Web peuvent alors interagir avec le serveur de base de données interne via un pare-feu applicatif ou directement, tout en restant sous l'égide des protections DMZ.
2. **Serveurs de messagerie** : les messages électroniques individuels, ainsi que la base de données des utilisateurs conçue pour stocker les identifiants de connexion et les messages personnels, sont généralement stockés sur des serveurs sans accès direct à Internet. Par conséquent, un serveur de messagerie sera construit ou placé à l'intérieur de la DMZ afin d'interagir avec et d'accéder à la base de données de messagerie sans l'exposer directement à un trafic potentiellement dangereux.
3. **Serveurs FTP** : ils peuvent héberger du contenu critique sur le site d'une organisation et permettre une interaction directe avec les fichiers. Par conséquent, un serveur FTP doit toujours être partiellement isolé des systèmes internes critiques.

Une configuration DMZ offre une sécurité supplémentaire contre les attaques externes, mais elle n'a généralement aucune incidence sur les attaques internes telles que le reniflement des communications via un analyseur de paquets ou l'usurpation d'identité par e-mail ou par d'autres moyens.

ARCHITECTURE D'UNE DMZ

Une DMZ est un « réseau largement ouvert », mais il existe plusieurs approches de conception et d'architecture qui la protègent. Une DMZ peut être conçue de plusieurs manières, d'une approche à pare-feu unique à des pare-feu doubles et multiples. La majorité des DMZ modernes, les architectures utilisent des pare-feux doubles qui peuvent être étendus pour développer des systèmes plus complexes.

1. **Pare-feu unique** : Une DMZ avec une conception à pare-feu unique nécessite trois interfaces réseau ou plus. Le premier est le réseau externe, qui relie la connexion Internet publique au pare-feu. Le second forme le réseau interne, tandis que le troisième est connecté à la DMZ. Diverses règles surveillent et contrôlent le trafic autorisé à accéder à la DMZ et limitent la connectivité au réseau interne.
2. **Double pare-feu** : le déploiement de deux pare-feu avec une DMZ entre eux est généralement une option plus sécurisée. Le premier pare-feu n'autorise que le trafic externe vers la DMZ, et le second n'autorise que le trafic qui va de la DMZ vers le réseau interne. Un attaquant devrait compromettre les deux pare-feu pour accéder au réseau local d'une organisation.

Les organisations peuvent également affiner les contrôles de sécurité pour divers **segments de réseau**. Cela signifie qu'un système de détection d'intrusion (IDS) ou un système de prévention d'intrusion (IPS) dans une DMZ pourrait être configuré pour bloquer tout trafic autre que les demandes HTTPS (Hypertext Transfer Protocol Secure) vers le port 443 du protocole TCP (Transmission Control Protocol).

Comment sont-elles utilisées ?

Les réseaux DMZ ont joué un rôle central dans la sécurisation des réseaux d'entreprise mondiaux depuis l'introduction des pare-feu. Ils protègent les données, les systèmes et les ressources sensibles des organisations en séparant les réseaux internes des systèmes

qui pourraient être ciblés par des attaquants. **Les DMZ permettent également aux organisations de contrôler et de réduire les niveaux d'accès aux systèmes sensibles.**

Des entreprises utilisent de plus en plus des conteneurs et des machines virtuelles (VM) pour isoler leurs réseaux ou des applications particulières du reste de leurs systèmes. La croissance du cloud signifie que de nombreuses entreprises n'ont plus besoin de serveurs Web internes. Ils ont également migré une grande partie de leur infrastructure externe vers le cloud en utilisant des applications Software-as-a-Service (SaaS).

Par exemple, un service cloud comme Microsoft Azure permet à une organisation qui exécute des applications sur site et sur des réseaux privés virtuels (VPN) d'utiliser une approche hybride avec la DMZ située entre les deux. Cette méthode peut également être utilisée lorsque le trafic sortant doit être audité ou pour contrôler le trafic entre un centre de données sur site et des réseaux virtuels.

En outre, les DMZ s'avèrent utiles pour contrer les risques de sécurité posés par les nouvelles technologies telles que les dispositifs Internet des objets (IoT) et les systèmes de technologie opérationnelle (OT), qui rendent la production et la fabrication plus intelligentes mais créent une vaste surface de menace. En effet, l'équipement OT n'a pas été conçu pour faire face aux cyberattaques ou s'en remettre comme l'ont été les appareils numériques IoT, ce qui présente un risque substantiel pour les données et les ressources critiques des organisations. Une **DMZ fournit une segmentation du réseau** pour réduire le risque d'attaques pouvant endommager l'infrastructure.

EXEMPLES DE DMZ

Voici quelques-unes des différentes façons d'utiliser les DMZ :

1. **Services infonuagiques**. Certains services cloud, tels que Microsoft Azure, utilisent une approche de sécurité hybride dans laquelle une DMZ est implémentée entre le réseau sur site d'une organisation et le réseau virtuel. Cette méthode est généralement utilisée dans les situations où les applications de l'organisation s'exécutent en partie sur site et en partie sur le réseau virtuel. Il est également utilisé lorsque le trafic sortant doit être audité ou lorsqu'un contrôle granulaire du trafic est requis entre le réseau virtuel et le centre de données sur site.
2. **Réseaux domestiques**. Une DMZ peut également être utile dans un réseau domestique dans lequel des ordinateurs et d'autres appareils sont connectés à Internet à l'aide d'un routeur à large bande et configurés dans un LAN. Certains routeurs domestiques incluent une fonctionnalité d'hôte DMZ. Cela peut être mis en contraste avec le sous-réseau DMZ utilisé dans les organisations avec beaucoup plus d'appareils que ce qu'on trouverait dans une maison. La fonction d'hôte DMZ désigne un périphérique du réseau domestique pour fonctionner en dehors du pare-feu, où il agit comme DMZ tandis que le reste du réseau domestique se trouve à l'intérieur du pare-feu. Dans certains cas, une console de jeu est choisie comme hôte DMZ afin que le pare-feu n'interfère pas avec les jeux. En outre, la console est un bon candidat pour un hôte DMZ car elle contient probablement des informations moins sensibles qu'un ordinateur personnel.
3. **Systèmes de contrôle industriels (ICS).** Les DMZ offrent une solution potentielle aux risques de sécurité des ICS. Les équipements industriels, tels que les moteurs à turbine ou les ICS, sont fusionnés avec les technologies de l'information (TI), ce qui rend les environnements de production plus intelligents et plus efficaces, mais crée également une plus grande surface de menace. Une grande partie de l'équipement de technologie industrielle ou opérationnelle (OT) qui se connecte à Internet n'est pas conçu pour gérer les attaques de la même manière que les appareils informatiques. Une DMZ peut

fournir une segmentation accrue du réseau qui peut rendre plus difficile pour les ransomwares ou autres menaces réseau de combler le fossé entre les systèmes informatiques et leurs homologues OT plus vulnérables.

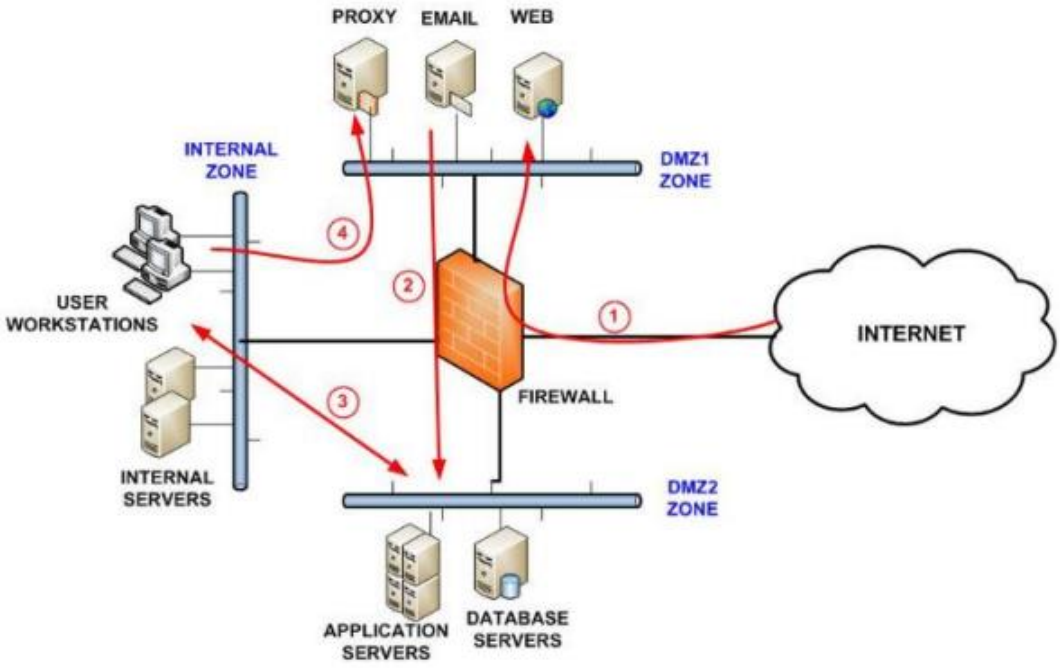

Figure 3. Vue des flux DMZ

LES AVANTAGES DE L'UTILISATION D'UNE DMZ

Le principal avantage d'une DMZ est de fournir à un réseau interne une couche de sécurité avancée en limitant l'accès aux données et aux serveurs sensibles. Une DMZ permet aux visiteurs du site Web d'obtenir certains services tout en fournissant un tampon entre eux et le réseau privé de l'organisation. En conséquence, la DMZ offre également des avantages de sécurité supplémentaires, tels que :

Activation du contrôle d'accès : les entreprises peuvent fournir aux utilisateurs un accès à des services en dehors des périmètres de leur réseau via l'Internet public. La DMZ permet d'accéder à ces services tout en mettant en œuvre une segmentation du réseau pour rendre plus difficile l'accès au réseau privé par un utilisateur non autorisé. Une DMZ peut également inclure un serveur proxy, qui centralise le flux de trafic interne et simplifie la surveillance et l'enregistrement de ce trafic.

Empêcher la reconnaissance du réseau : en fournissant un tampon entre Internet et un réseau privé, une DMZ empêche les attaquants d'effectuer le travail de reconnaissance qu'ils effectuent à la recherche de cibles potentielles. Les serveurs au sein de la DMZ sont exposés publiquement mais se voient offrir une autre couche de sécurité par un pare-feu qui empêche un attaquant de

voir à l'intérieur du réseau interne. Même si un système DMZ est compromis, le pare-feu interne sépare le réseau privé de la DMZ pour le sécuriser et rendre la reconnaissance externe difficile.

Blocage de l'usurpation d'adresse IP (Internet Protocol) : les attaquants tentent de trouver des moyens d'accéder aux systèmes en usurpant une adresse IP et en usurpant l'identité d'un appareil approuvé connecté à un réseau. Une DMZ peut découvrir et bloquer de telles tentatives d'usurpation lorsqu'un autre service vérifie la légitimité de l'adresse IP. La DMZ permet également une segmentation du réseau pour créer un espace d'organisation du trafic et d'accès aux services publics en dehors du réseau privé interne.

Les services d'une DMZ comprennent :

1. Serveurs DNS
2. Serveurs FTP
3. Serveurs de messagerie
4. Serveurs proxy
5. Serveurs Web

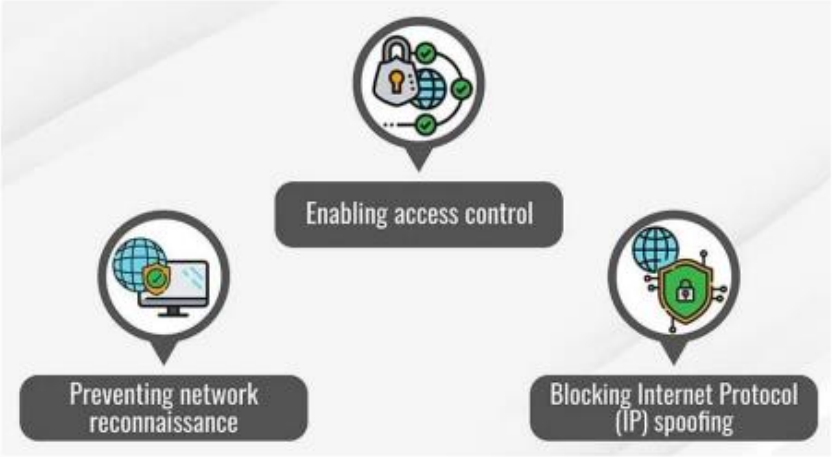

Figure 4. Avantages

QUELQUES CONSEILS POUR SÉCURISER UNE DMZ

Une DMZ réseau abrite certains des serveurs les plus à risque d'une organisation : ceux qui fournissent des connexions directes à Internet et qui sont exposés à un risque d'attaques importants. Une organisation doit faire tout ce qui est en son pouvoir pour verrouiller la DMZ et la protéger des menaces.

Voici quelques conseils pour vous assurer qu'une DMZ est sécurisée :

1. PRÉSERVEZ L'ISOLEMENT AUTANT QUE POSSIBLE.

Gardez les règles qui autorisent le trafic entre la DMZ et un réseau interne aussi strictes que possible. Trop souvent, les administrateurs cherchant à résoudre un problème créent une règle autorisant un accès complet entre un système DMZ et un serveur principal sur le réseau interne (ou l'ensemble du réseau interne). Cela va à l'encontre de l'objectif de la DMZ. Au lieu de cela,

créez des règles de pare-feu spécifiques qui autorisent la communication uniquement entre des serveurs spécifiques sur des ports spécifiques requis pour répondre aux exigences de l'entreprise.

2. PRATIQUEZ UNE BONNE GESTION DES VULNÉRABILITÉS.

Les serveurs DMZ sont exposés au monde entier, alors prenez des mesures supplémentaires pour vous assurer qu'ils sont entièrement corrigés pour faire face aux **dernières vulnérabilités de sécurité**. Nous recommandons des analyses quotidiennes et automatisées des vulnérabilités des systèmes DMZ qui fournissent des alertes rapides des vulnérabilités nouvellement détectées. En outre, envisagez de corriger les systèmes DMZ beaucoup plus fréquemment que les systèmes protégés afin de réduire la fenêtre de vulnérabilité entre le moment où un correctif est publié et son application aux serveurs DMZ.

3. UTILISEZ LES DÉFENSES DE LA COUCHE APPLICATION POUR LES SERVICES EXPOSÉS.

Choisissez un pare-feu réseau doté d'une protection renforcée de la couche application, plutôt qu'un simple filtre de port. Un pare-feu doit avoir la capacité d'inspecter le contenu du trafic et de bloquer les requêtes malveillantes. Un exemple courant de ceci est le filtrage des requêtes Web entrantes à la recherche de signes d'attaques par injection SQL embarqué, les empêchant même d'atteindre le serveur Web.

4. SURVEILLEZ, SURVEILLEZ, SURVEILLEZ.

La DMZ doit être l'un des principaux axes des efforts de surveillance du réseau d'une organisation. Utilisez des systèmes de détection d'intrusion, des systèmes de gestion des incidents de sécurité et des événements, la surveillance des journaux et d'autres outils pour rester vigilant aux signes d'une attaque.

Les systèmes DMZ sont à la pointe de la sécurité du réseau et sont quotidiennement soumis à des attaques externes. Pour cette raison, il est important de prendre le temps de s'assurer qu'ils font partie des serveurs les plus sécurisés d'une organisation et qu'ils sont rigoureusement entretenus.

Bien que la DMZ soit censée servir de point de contrôle du périmètre, sa fonction ressemble aujourd'hui davantage à un panneau publicitaire pour les attaquants.

Chaque service que vous publiez sur la DMZ est une autre source d'informations indiquant à un pirate potentiel combien d'utilisateurs vous avez, où vous conservez vos données critiques et si ces données incluent quelque chose qu'un attaquant pourrait vouloir voler. Voici quatre façons d'empêcher que cela se produise.

Faire de la DMZ une véritable discontinuité

L'idée derrière la DMZ est qu'elle doit vraiment être séparée du LAN. En tant que tel, vous devez établir des politiques de routage et de sécurité IP différentes dans la DMZ, par opposition au reste du réseau. Cela rend la tâche beaucoup plus difficile pour les attaquants ; ils pourraient comprendre votre DMZ, mais ils ne peuvent pas ensuite appliquer ces connaissances pour attaquer votre LAN.

Optimiser les flux de données

Idéalement, les services extérieurs à la DMZ établiront des connexions directes uniquement vers la DMZ elle-même. Les services à l'intérieur de la DMZ se connecteront au monde extérieur uniquement via des proxys. Les services à l'intérieur de la DMZ sont plus sécurisés que ceux à l'extérieur. Les services qui sont mieux protégés doivent assumer le rôle de client lorsqu'ils demandent des données provenant de zones moins protégées.

Utiliser une approche à deux pare-feu

Bien qu'il soit possible de créer une DMZ en utilisant un seul pare-feu avec trois interfaces réseau ou plus, deux pare-feu créent une dissuasion plus sûre. Le premier pare-feu représente le périmètre extérieur et dirige le trafic uniquement vers la DMZ. Le pare-feu interne autorise le trafic de la DMZ vers le réseau interne. Cette approche est considérée comme plus sûre, car elle fournit deux obstacles distincts à surmonter pour un attaquant.

Mettre en œuvre un accès réseau Zero Trust

Le concept "**Zero Trust**" avec ses différentes solutions d'implantation, change la façon dont les organisations accordent un accès externe sécurisé à leurs services. Il offre un accès sécurisé et transparent pour tous les types d'entités (personnes, applications et appareils connectés) à n'importe quelle application, service et données internes. Il oblige les utilisateurs à s'authentifier d'abord auprès des ressources, puis il leur accorde l'accès. Des politiques configurables définissent les étapes d'authentification que chaque utilisateur ou membre de groupe doit effectuer. Désormais avec ce type de solutions, les services back-end ne sont pas visibles pour les utilisateurs non authentifiés et la probabilité de subir une attaque réussie est minimisée. C'est comme si nous disons ici dans le réseau de l'Université du Québec (UQ) : **Autorise mais Ne faites confiance à rien** (*Autoriser = filtrer*).

La technologie d'accès inversé fonctionne en permettant d'authentifier les utilisateurs accédant avant qu'ils n'aient accès à vos applications critiques. Un attaquant ayant accès à vos applications via une session illégitime peut effectuer une reconnaissance sur votre réseau, tenter des attaques par injection de code ou même essayer de se déplacer latéralement sur le réseau. Sans la possibilité de se faire passer pour une session légitime, cependant, la boîte à outils d'un attaquant devient beaucoup plus limitée.

Une DMZ mal implémentée attire les attaquants comme des mites vers une flamme, mais une DMZ avec ZTNA activé ressemble plus à un bug zapper. Vous voulez en savoir plus sur la façon de vous approprier cette technologie ?

LA MATRICE DE FLUX

Dans le portail Azure, un utilisateur avec les privilèges d'Administrateur général peut configurer un délai d'inactivité qui s'appliquent à tous les utilisateurs du domaine. N'importe lequel utilisateur qui est inactif pour plus de 30 minutes (si le délai a été fixé à 30 minutes), sera automatiquement déconnecté de sa session.

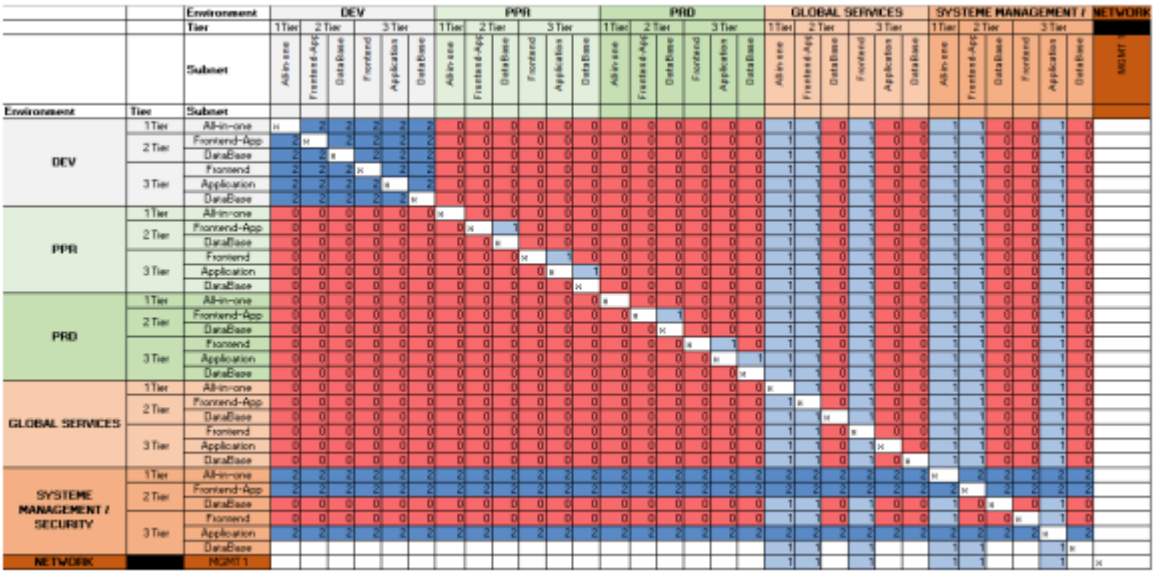

Figure 5. Matrice des flux

RÉVISIONS

Date	Action	Auteurs	Version
2022-05-05	Version initiale	Aboubakar C.	0.1
2022-05-24	Ajustement architecture	Aboubakar C.	0.2
2022-06-16	Conseils pour sécuriser une DMZ	Aboubakar C.	0.3
2022-07-14	Ajustement références, matrice de flux ainsi que rôles	Aboubakar C.	0.4
2022-12-07	Correction linguistique	BOUILLON, Marie-Josée	0.5
2022-12-12	Approbation	CESI	1.0