

|  |
| --- |
| Recommandations Sécurité Réseaux et systèmes |
|  |
|  |
| HATIM BENHADDOUCH | HATIMBENHADDOUCH@GMAIL.COM |

Pare-feu

|  |  |  |
| --- | --- | --- |
| **SLNon** | **Conseils** |  |
| 1 | Mettez à jour le routeur avec la dernière version du micrologiciel. |  |
| 2 | Activez l’inspection des paquets avec état (SPI). |  |
| 3 | Désactivez la réponse ping (ICMP) sur le port WAN. |  |
| 4 | Désactivez UPnP (plug-and-play universel). |  |
| 5 | Désactivez IDENT (port 113). |  |
| 6 | Désactivez la gestion à distance du routeur. |  |
| 7 | Modifiez le mot de passe administrateur par défaut. |  |
| 8 | Les paramètres d'une politique de pare-feu doivent être aussi spécifiques que possible. N'utilisez pas 0.0.0.0 comme adresse. |  |
| 9 | Vérifier la politique de sécurité du trafic entrant/sortant |  |
| 10 | Vérifiez les mises à jour du micrologiciel du pare-feu/du système d'exploitation |  |
| 11 | Autoriser uniquement l'accès HTTPS à l'interface graphique et l'accès SSH à la CLI |  |
| 12 | Rediriger les connexions HTTP GUI vers HTTPS |  |
| 13 | Remplacez les ports d'accès administrateur HTTPS et SSH par des ports non standard |  |
| 14 | Restreindre les connexions à partir d'hôtes de confiance |  |
| 15 | Configurer l'authentification à deux facteurs pour les administrateurs |  |
| 16 | Créer plusieurs comptes d'administrateur |  |
| 17 | Modifier la durée de verrouillage du compte administrateur et les valeurs de seuil |  |
| 18 | Vérifiez si tous les accès de gestion depuis Internet sont désactivés, s'il n’a pas de besoin commercial clair. Tout au plus, HTTPS et PING devraient être activé. |  |

|  |  |  |
| --- | --- | --- |
| 19 | Assurez-vous que vos paramètres SNMP utilisent SNMPv3 avec cryptage  et configurez vos profils UTM |  |
| 20 | Toutes les politiques de pare-feu doivent être révisées tous les 3 mois pour vérifier des fins commerciales |  |

Routeurs

|  |  |  |
| --- | --- | --- |
| **SLNon** | **Conseils** |  |
| 1 | N'utilisez pas le mot de passe par défaut pour votre routeur |  |
| 2 | Vérifiez si le routeur bloque l'accès à un modem par adresse IP |  |
| 3 | Assurez-vous que l'administrateur du routeur reçoit une alerte lorsqu'un nouvel appareil rejoint le réseau |  |
| 4 | La plupart des routeurs vous permettent de désactiver UPnP côté LAN |  |
| 5 | Activez la redirection de port et le filtrage IP pour votre routeur |  |
| **ADMINISTRATION LOCALE** | | |
| 6 | Vérifiez si le routeur prend en charge HTTPs, sur certains routeurs, il est désactivé par défaut |  |
| 7 | Si HTTPS est pris en charge, l'accès administrateur peut-il être limité exclusivement à HTTPS ? |  |
| 8 | Vérifiez si le port TCP/IP utilisé pour l'interface Web peut être modifié |  |
| 9 | Pour vraiment empêcher l'accès des administrateurs locaux, limitez l'adresse IP du réseau local à l’ adresse IP unique qui est à la fois en dehors de la plage DHCP et non normalement attribué. |  |
| 10 | Vérifiez si l'accès administrateur peut être limité à Ethernet uniquement |  |
| 11 | Vérifiez si l'accès au routeur peut être restreint par SSID et/ou par VLAN |  |
| 12 | Le routeur ne doit pas permettre à plusieurs ordinateurs de se connecter en même temps en utilisant le même identifiant |  |

|  |  |  |
| --- | --- | --- |
| 13 | Vérifiez s'il y a un certain type de verrouillage après trop de tentatives infructueuses pour vous connecter à l'interface web |  |
| **ADMINISTRATION À DISTANCE** | | |
| 14 | Assurez-vous que les paramètres d'administration à distance sont désactivés par défaut |  |
| 15 | Vérifiez si le numéro de port peut être modifié à distance |  |
| 16 | Si vous oubliez de vous déconnecter du routeur, votre session finira par expirer et vous devriez pouvoir définir le délai, le plus court, plus c'est sûr |  |
| **PARE-FEU DU ROUTEUR** | | |
| 17 | **Réseau étendu entrant :** Quels ports sont ouverts côté WAN/Internet ?  La réponse la plus sûre est aucun et vous devez vous attendre à ce qu'aucun routeur ne le fasse  fournir par un FAI pour ne pas avoir de ports ouverts côté Internet. Une exception est l'administration à distance à l'ancienne, qui nécessite un port ouvert. Chaque port ouvert côté WAN doit être pris en compte,surtout si le routeur a été fourni par un FAI, ils disposent souvent eux-mêmes une porte dérobée. La page Teste de votre routeur renvoie à de nombreux sites Web proposant des tests de pare-feu. Cela dit, aucun d'entre eux ne scannera tous les 65 535 ports TCP ou les 65 535 ports UDP. Le meilleur moment pour tester ceci est avant de mettre en service un nouveau routeur. |  |
| 18 | **Réseau local entrant :** Quels ports sont ouverts côté LAN ? Attendez-vous au port 53 à être ouvert au DNS (probablement UDP, peut-être TCP). Si le routeur dispose d'une interface Web, cela nécessite alors un port ouvert.  Le classique/standard L'utilitaire pour tester le pare-feu côté LAN est Nmap. Comme pour le côté  WAN, Chaque port ouvert doit être pris en compte. |  |

|  |  |  |
| --- | --- | --- |
| 19 | **Sortant :** Le routeur peut-il créer des règles de pare-feu sortantes ?  Il y a toutes sortes d'attaques qui peuvent être bloquées avec des règles de pare-feu sortantes. Généralement, les routeurs grand public n'offrent pas de règles de pare-feu sortantes contrairement aux routeurs de classe affaires. En plus de bloquer, ce serait bien si les blocs étaient enregistrés à des fins d'audit. Notez cependant, que les appareils connectés à  Tor ou à un VPN n'obéiront pas aux messages sortants règles de pare-feu. |  |

Commutateurs

|  |  |  |
| --- | --- | --- |
| **SLNon** | **Conseils** | |
| 1 | Vérifiez si le dernier firmware est utilisé. |  |
| 2 | Consultez le guide d'utilisation du commutateur pour connaître les fonctionnalités de sécurité et voyez si le ceux requis ont été correctement mis  en œuvre. |  |
| 3 | Créer un mot de passe secret d'activation Crypter les mots de passe sur l'appareil |  |
| 4 | Utiliser un serveur AAA externe pour l'authentification des utilisateurs |  |
| 5 | Créer des comptes locaux distincts pour l'authentification utilisateur, Configurer  Le nombre maximal de tentatives d'authentification ayant échoué |  |
| 6 | Restreindre l'accès à la gestion aux appareils à des adresses IP spécifiques uniquement |  |
|  |  |  |
| 7 | Activez la journalisation pour la surveillance, la réponse aux incidents et l’audit. Pouvez-vous permettre la journalisation dans un tampon interne de l'appareil ou dans un Serveur de journaux externe. |  |
| 8 | Activer le protocole NTP (Network Time Protocol) : vous devez disposer |  |
| 9 | d'informations précises et paramètres d'horloge uniformes sur tous les périphériques réseau afin que les données du journal soient estampillées avec l'heure et le fuseau horaire corrects. Cela aidera énormément dans la gestion  des incidents et la surveillance appropriée des journaux et corrélation. |  |

|  |  |  |
| --- | --- | --- |
| 10 | Restreindre et sécuriser l'accès SNMP |  |

Serveurs Linux

|  |  |  |
| --- | --- | --- |
| **SLNon** | **Conseils** | |
| 1 | Mettez à jour votre liste de packages et mettez à niveau votre système d'exploitation |  |
| 2 | Supprimez les packages inutiles |  |
| 3 | Détectez les mots de passe faibles avec John l'Éventreur |  |
| 4 | Vérifiez qu'aucun compte n'a de mot de passe vide |  |
| 5 | Définir des règles de mot de passe |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6 | | | Définir l'expiration du mot de passe dans login.defs |  |
| 7 | | | Désactiver les périphériques USB (pour les serveurs sans tête) |  |
| 8 | | | Vérifiez quels services sont démarrés au moment du démarrage |  |
| 9 | | | Détecter tous les fichiers accessibles en écriture dans le monde entier |  |
| 10 | | | Configurez iptables pour bloquer les attaques courantes |  |
| 11 | | | Définir le mot de passe du chargeur de démarrage GRUB |  |
| 12 | | | Désactiver le démarrage par raccourci clavier interactif au démarrage |  |
| 13 | | | Activer audité pour vérifier les événements de lecture/écriture |  |
| 14 | | | Sécurisez tous les serveurs Apache |  |
| 15 | | | Installer et configurer UFW |  |
| 16 | | | Configurez SSH en toute sécurité |  |
| 17 | | | Désactiver Telnet |  |
| 18 | | | Configurer sysctl en toute sécurité |  |
| 19 | Verrouiller les comptes d'utilisateurs après des tentatives infructueuses avec Fail2Ban | |  | |
| 20 | Configurer le délai d'expiration de l'utilisateur root | |  | |
| 21 | Vérifiez les ports ouverts cachés avec netstat | |  | |
| 22 | Définir les autorisations root pour les fichiers système principaux | |  | |
| 23 | Rechercher des rootkits | |  | |
| 24 | Vérifiez que le mode d'arrêt est activé pour les alertes du journal des événements sensibles | |  | |
| 25 | Vérifiez que toutes les données du journal des événements sont sauvegardées en toute sécurité | |  | |
| 26 | Évaluer le processus de surveillance du journal des événements | |  | |
| 27 | Surveillez tout utilisateur se connectant dans des circonstances suspectes | |  | |
| 28 | Vérifiez régulièrement les journaux d'accès à distance | |  | |
| 29 | En cas d'activité d'accès à distance : Assurez-vous que les éléments suspects  l'activité est signalée et documentée | |  | |
| 30 | Assurez-vous que les privilèges du compte suspect sont temporairement gelés | |  | |
| 31 | Évaluer le processus de contrôle de la configuration du serveur | |  | |
| 32 | Mettre à jour les service packs et les correctifs pour les logiciels | |  | |
| 33 | Vérifiez que la surveillance du journal des événements est correctement configurée : | |  | |
| 34 | Vérifiez que toutes les connexions aux comptes utilisateur sont enregistrées | |  | |
| 35 | Vérifiez que toutes les modifications de configuration du système sont enregistrées | |  | |
| 36 | Assurez-vous qu'un processus est en place pour changer le système de configurations | |  | |
| 37 | Assurez-vous que les processus de démarrage sont correctement configurés | |  | |
| 38 | Supprimez les processus de démarrage inutiles | |  | |
| 39 | Assurez-vous que les utilisateurs réguliers ne peuvent pas modifier la configuration de démarrage du système | |  | |
| 40 | Supprimer les logiciels et services inutilisés | |  | |
| 41 | Exécutez une analyse antivirus complète du système | |  | |
| 42 | Vérifiez les paramètres de sécurité du pare-feu de votre serveur et assurez-vous  tout est correctement configuré | |  | |
| 43 | Désactivez ou supprimez tous les comptes d'utilisateurs qui n'ont pas été actifs dans les 3 derniers mois | |  | |
| 44 | Assurez-vous que l'adhésion à l'administrateur et au super administrateur  le groupe est limité au moins d'utilisateurs possible sans provoquer de problèmes | |  | |

Serveurs Windows

|  |  |  |
| --- | --- | --- |
| **SLNon** | **Conseils** | |
| 1 | Installez les derniers service packs et correctifs logiciels de Microsoft. |  |
| 2 | Activez la notification automatique de la disponibilité des correctifs. |  |
| 3 | Définissez la longueur minimale du mot de passe. |  |
| 4 | Activez les exigences de complexité des mots de passe. |  |
| 5 | Ne stockez pas les mots de passe en utilisant un cryptage réversible. (Défaut) |  |
| 6 | Configurez la stratégie de verrouillage de compte. |  |
| 7 | Restreindre la possibilité d'accéder à cet ordinateur à partir du réseau pour Administrateurs et utilisateurs authentifiés. |  |
| 8 | N'accordez à aucun utilisateur le droit « d'agir en tant que partie du système d'exploitation ».(Défaut) |  |
| 9 | Restreindre l’accès à la connexion locale aux administrateurs. |  |
| 10 | Refuser aux comptes invités la possibilité de se connecter en tant que service, de tâches par lots, localement ou via RDP |  |
| 11 | Placez la bannière d'avertissement dans le texte du message pour les utilisateurs qui tentent de se connecter. |  |
| 12 | Interdire aux utilisateurs de créer et de se connecter avec des comptes Microsoft. |  |
| 13 | Désactivez le compte invité. (Défaut) |  |
| 14 | Exiger Ctrl+Alt+Del pour les connexions interactives. (Défaut) |  |
| 15 | Configurez la limite d'inactivité de la machine pour protéger les sessions interactives inactives. |  |

|  |  |  |
| --- | --- | --- |
| 16 | Configurer Microsoft Network Client pour toujours signer numériquement les  communications. |  |
| 17 | Configurer Microsoft Network Client pour signer numériquement les communications  Si le serveur est d'accord. (Défaut) |  |
| 18 | Désactiver l'envoi de mots de passe non chiffrés à une PME tierce les serveurs. |  |
| 19 | Configurer Microsoft Network Server pour toujours signer numériquement les  communications. |  |
| 20 | Configurer Microsoft Network Server pour signer numériquement les communications si le client est d'accord. |  |
| 21 | Désactivez la traduction anonyme du SID/Nom. (Défaut) |  |
| 22 | N'autorisez pas l'énumération anonyme des comptes SAM. (Défaut) |  |
| 23 | N'autorisez pas l'énumération anonyme des comptes et des partages SAM. |  |
| 24 | N'autorisez pas les autorisations de tout le monde à s'appliquer aux utilisateurs anonymes. (Défaut) |  |
| 25 | N'autorisez pas l'accès anonyme aux canaux nommés. |  |
| 26 | Restreindre l’accès anonyme aux canaux nommés et aux partages. (Défaut) |  |
| 27 | Ne permettez pas l’accès anonyme aux partages. |  |
| 28 | Exiger le modèle de partage et de sécurité « Classique » pour les comptes locaux.(Défaut) |  |
| 29 | Autoriser le système local à utiliser l'identité de l'ordinateur pour NTLM. |  |
| 30 | Désactivez le repli de session NULL du système local. |  |
| 31 | Configurez les types de chiffrement autorisés pour Kerberos. |  |
| 32 | Ne stockez pas les valeurs de hachage de LAN Manager. |  |
| 33 | Définissez le niveau d'authentification de LAN Manager pour autoriser uniquement NTLMv2 et refuser LM et NTLM. |  |

|  |  |  |
| --- | --- | --- |
| 34 | Activez le pare-feu Windows dans tous les profils (domaine, privé, public). (Défaut) |  |
| 35 | Configurez le pare-feu Windows dans tous les profils pour bloquer le trafic entrant par défaut. (Défaut) |  |
| 36 | Configurez le pare-feu Windows pour restreindre les services d'accès à distance (VNC,RDP, etc.) vers des réseaux autorisés réservés à l'organisation. |  |
| 37 | Configurez le pare-feu Windows pour restreindre les services d'accès à distance (VNC,RDP, etc.) au VPN de l'organisation. |  |
| 38 | Cryptez ou signez numériquement les données des canaux sécurisés (toujours). (Défaut) |  |
| 39 | Configurez la limite d'inactivité de la machine pour protéger les sessions interactives inactives. |  |
| 40 | Nécessite des clés de session fortes (Windows 2000 ou version ultérieure). |  |
| 41 | Configurez le nombre de connexions précédentes à mettre en cache. |  |
| 42 | Configurez la stratégie d’audit de connexion au compte. |  |
| 43 | Configurez la stratégie d’audit de gestion des comptes. |  |
| 44 | Configurez la stratégie d’audit de connexion/déconnexion. |  |
|  | Configurez la stratégie d’audit de changement de stratégie et la stratégie d’audit d’utilisation des privilèges. |  |
| 39 | Configurez la méthode et la taille de conservation du journal des événements. |  |
| 40 | Configurez l'envoi des journaux (par exemple vers Splunk). |  |
| 41 | Désactivez ou désinstallez les services inutilisés. |  |
| 42 | Configurez les droits des utilisateurs pour être aussi sécurisés que possible : suivez le principe du moindre privilège |  |
| 43 | Assurez-vous que tous les volumes utilisent le système de fichiers NTFS. |  |
| 44 | Configurez le système de fichiers ainsi que les autorisations de registre. |  |
| 39 | Interdisez l’accès au registre à distance s’il n’est pas nécessaire. |  |

|  |  |  |
| --- | --- | --- |
| 40 | Réglez la date/l'heure du système et configurez-la pour qu'elle se synchronise avec Serveurs de temps de l'organisation. |  |
| 41 | Installez et activez les logiciels anti-spyware et antivirus. |  |