Projet : Sécurisez le réseau d'une grande entreprise

Table des matières

Introduction Générale

1. Présentation des objectifs de la mise à jour de la sécurité

L'objectif de cette mise à jour est de renforcer la sécurité de l'infrastructure réseau et des systèmes d'information en réponse aux menaces croissantes telles que les cyberattaques, les ransomwares, et les intrusions non autorisées. Cette mise à jour vise également à se conformer aux recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), garantissant ainsi une protection optimale des données sensibles et une continuité d'activité pour la PME.

Résumé des principaux changements et de leur importance

- Introduction de nouvelles politiques d'accès à distance sécurisées (VPN, 2FA).
- Segmentation du réseau par VLAN pour isoler les systèmes critiques.
- Renforcement de la gestion des comptes utilisateurs avec une authentification forte et des règles de mot de passe plus strictes.

2. Description des Évolutions

a. Connexions à Distance

- **Explication des nouvelles politiques d'accès à distance**

Les accès à distance, en particulier pour les employés en télétravail ou les prestataires externes, sont désormais sécurisés par la mise en place d'un VPN SSL. Ce dernier chiffre les connexions, garantissant que toutes les données échangées entre l'utilisateur et le réseau sont protégées. En complément, l'authentification à deux facteurs (2FA) renforce l'accès en demandant une vérification supplémentaire (mot de passe + code envoyé sur un appareil de confiance).

- **Rôle du pare-feu et des nouvelles procédures de sécurisation**

Le pare-feu est configuré pour filtrer le trafic entrant et sortant du réseau en fonction de politiques strictes, ne laissant passer que les connexions autorisées. L'ajout de règles spécifiques pour les connexions VPN SSL permet de surveiller et de restreindre les accès à certaines zones du réseau.

Recommandations ANSSI :

La mise en place de ces mesures répond aux recommandations R30 de l'ANSSI, qui préconisent de sécuriser les accès aux systèmes d'information en utilisant des mécanismes de chiffrement et d'authentification renforcée.

b. Accès Réseau et Segmentation VLAN

- **Utilisation des commutateurs L3 pour segmenter le réseau par VLANs**

Les commutateurs de niveau 3 (L3) permettent une segmentation réseau avancée via des VLANs. Chaque VLAN isole les différents services et groupes d'utilisateurs, limitant les risques de propagation d'une attaque ou d'une fuite de données. Par exemple, les systèmes de production seront dans un VLAN séparé des utilisateurs classiques, et les systèmes critiques auront un accès encore plus restreint.

- **Isolement des systèmes critiques**

Les serveurs contenant des données sensibles ou les systèmes de gestion critiques sont placés dans des VLANs isolés, inaccessibles directement depuis le réseau utilisateur. Cela réduit considérablement les risques d'intrusion en limitant les interactions potentielles entre les systèmes.

Recommandations ANSSI :

La segmentation réseau respecte la recommandation R16 de l'ANSSI, qui préconise de mettre en place une politique stricte de contrôle d'accès au réseau pour limiter les mouvements latéraux en cas de compromission.

c. Gestion des Comptes Utilisateurs

- **Amélioration des procédures de création et de gestion des comptes utilisateurs**

Les procédures de création de comptes utilisateurs sont renforcées avec une attribution de droits basée sur le principe du moindre privilège. Les utilisateurs n'ont accès qu'aux ressources nécessaires à l'exécution de leurs tâches. L'authentification forte est également mise en place, combinant mot de passe complexe et 2FA pour une sécurité accrue.

Recommandations ANSSI :

Ces mesures suivent les recommandations R18 de l'ANSSI, qui visent à renforcer la gestion des comptes utilisateurs en imposant des règles strictes de gestion des accès, de réinitialisation de mot de passe et de surveillance des comptes inactifs.

Nom	Type	Description	Collaborateur	Comptes de connexion
Windows / Outlook	Active Directory / Messagerie	Accès aux ordinateur / compte mail	Sylvain Bouchard	Compte personnel
			Hicham Laouini	Compte personnel
			Cynthia Caouren	Compte personnel
			Alexandre Levêque	Compte personnel
			Asma Ben Omar	Compte personnel
			Roberto Rivieira	Compte personnel
			Moussa Camara	Compte personnel
			Marilyn Chen	Compte personnel
			Laurie Garrido	Compte personnel
			Béatrice Jean-Robert	Compte personnel
			Yassine Ouari	Compte personnel
			Lyvia Kevain	Compte personnel
OPharma-B			Sylvain Bouchard	Compte personnel
			Hicham Laouini	Compte personnel
			Cynthia Caouren	Compte personnel
			Alexandre Levêque	Compte personnel
			Asma Ben Omar	Compte personnel
			Roberto Rivieira	Compte personnel
			Moussa Camara	Compte personnel
			Marilyn Chen	Compte personnel
			Laurie Garrido	Compte nominatif avec des droits de Responsables de Pôle
			Béatrice Jean-Robert	Compte nominatif avec des droits de Responsables de Pôle
			Yassine Ouari	Compte nominatif avec des droits de Responsables de Pôle
			Lyvia Kevain	Compte nominatif avec des droits d'administrateur
OPharma-C	Generaliste	Application d'accès aux congés	Sylvain Bouchard	Compte personnel
			Hicham Laouini	Compte personnel
			Cynthia Caouren	Compte personnel
			Alexandre Levêque	Compte nominatif avec des droits d'administrateur
			Asma Ben Omar	Compte personnel
			Roberto Rivieira	Compte personnel
			Moussa Camara	Compte personnel
			Marilyn Chen	Compte personnel
			Laurie Garrido	Compte personnel
			Béatrice Jean-Robert	Compte personnel
			Yassine Ouari	Compte personnel
			Lyvia Kevain	Compte personnel
OPharma-A	Generaliste	Application d'accès à l'annuaire de l'entreprise	Sylvain Bouchard	Compte personnel
			Hicham Laouini	Compte personnel
			Cynthia Caouren	Compte personnel
			Alexandre Levêque	Compte personnel
			Asma Ben Omar	Compte personnel
			Roberto Rivieira	Compte personnel
			Moussa Camara	Compte personnel
			Marilyn Chen	Compte personnel
			Laurie Garrido	Compte personnel
			Béatrice Jean-Robert	Compte personnel
			Yassine Ouari	Compte personnel
			Lyvia Kevain	Compte personnel
Avogadro	Métier	Outil d'édition et de visualisation de molécules chimiques en 3D	Béatrice Jean-Robert	Compte nominatif avec des droits d'administrateur
			Asma Ben Omar	Compte nominatif avec des droits d'administrateur
			Roberto Rivieira	Compte nominatif avec des droits d'administrateur
			Alexandre Levêque	Compte nominatif avec des droits d'administrateur
ImageJ	Métier	Outil de traitement et d'analyse d'images pour les applications biomédicales	Béatrice Jean-Robert	Compte nominatif avec des droits d'administrateur
			Sebastien Devilliers	Compte nominatif avec des droits d'administrateur
			Asma Ben Omar	Compte nominatif / Pôle Laboratoire
			Roberto Rivieira	Compte nominatif / Pôle Laboratoire
Laby	Métier	Outil de gestion et d'optimisation des processus du laboratoire	Lyvia Kevain	Compte nominatif avec des droits d'administrateur
			Béatrice Jean-Robert	Compte nominatif avec des droits d'administrateur
			Sebastien Devilliers	Compte nominatif avec des droits d'administrateur
			Asma Ben Omar	Compte nominatif / Pôle Laboratoire
			Roberto Rivieira	Compte nominatif / Pôle Laboratoire
			Yassin Ouari	Compte nominatif avec des droits d'administrateur
			Moussa Camara	Compte nominatif / Pôle Etudes
			Marilyn Chen	Compte nominatif / Pôle Etudes
			Cynthia Caouren	Compte nominatif avec des droits d'administrateur
			Hicham Laouini	Compte nominatif avec des droits d'administrateur

Tableau 1 : les comptes utilisateurs / Applications

3. Raisons des Changements

a. Présentation des menaces actuelles

Les cyberattaques, notamment via des ransomwares, des tentatives d'hameçonnage (phishing), ou des intrusions non autorisées, sont en augmentation. Ces attaques peuvent entraîner des pertes financières, la compromission de données sensibles ou l'interruption des activités.

b. Impact potentiel sur la PME

Sans protection adéquate, une PME peut être la cible de cybercriminels cherchant à voler des données ou à perturber les services. Un simple accès non sécurisé ou un compte mal protégé peut être exploité pour compromettre l'ensemble du réseau, ce qui pourrait paralyser l'activité de l'entreprise.

c. Réduction des risques avec les nouveaux équipements

Les nouveaux équipements, comme les commutateurs L3 et le pare-feu configurés avec des politiques strictes, permettent de réduire ces risques en segmentant les accès et en limitant les interactions entre les systèmes. La mise en place de la surveillance continue et l'authentification renforcée ajoutent une couche de protection supplémentaire.

4. Nouvelles Procédures pour les Utilisateurs

a. Accès à distance

Les utilisateurs doivent désormais utiliser un VPN SSL pour se connecter à distance au réseau de l'entreprise. L'accès est sécurisé par une authentification à deux facteurs (2FA) qui assure que seuls les utilisateurs autorisés peuvent se connecter, même si leurs mots de passe sont compromis.

b. Utilisation du réseau interne

Les utilisateurs sont affectés à des VLANs spécifiques selon leur rôle dans l'entreprise. Par exemple, les équipes techniques ont un accès restreint aux VLANs de gestion des systèmes, tandis que les utilisateurs standards sont isolés dans leur propre segment réseau.

c. Gestion des mots de passe et des comptes

Des règles de complexité plus strictes sont mises en place pour les mots de passe, avec une rotation périodique obligatoire. En cas de plusieurs tentatives de connexion échouées, le compte est verrouillé, réduisant ainsi les risques d'accès non autorisé par force brute.

5. Nouvelles Procédures pour les Administrateurs

a. Gestion des équipements réseau

Les commutateurs L3 et le pare-feu sont surveillés de manière proactive pour détecter les anomalies et assurer leur bon fonctionnement. Des audits réguliers sont réalisés pour vérifier les configurations et les mises à jour.

b. Maintenance régulière

Tous les équipements doivent être maintenus à jour avec les derniers correctifs de sécurité d'où la migration des serveurs Windows server 2012 R2 vers le Windows Server 2019 et le Debian 8 vers le Debian 12. Les administrateurs effectuent des audits de sécurité réguliers pour vérifier que les configurations respectent les politiques de sécurité de l'entreprise.

6. Conclusion

Résumé des bénéfices attendus

Grâce à ces mises à jour, l'infrastructure IT est plus sécurisée et les données de l'entreprise sont mieux protégées contre les cyberattaques. La segmentation réseau et la gestion renforcée des accès réduisent considérablement les risques d'intrusion.