Préconisation 1 : Isolation Stricte du Système d'Information d'Administration

Constat : L'administration des équipements réseau et serveurs (routeurs, switchs L3, serveurs DNS/Web) nécessite des privilèges élevés. Si les postes et le réseau utilisés pour l'administration sont les mêmes que ceux utilisés pour la bureautique ou la navigation Internet, ou s'ils ne sont pas correctement isolés, ils deviennent des cibles potentielles. Une compromission du poste d'un administrateur ou du réseau d'administration peut rapidement conduire à une compromission totale du SI de l'entreprise.

Mise en Œuvre :

Les administrateurs du service Informatique (VLAN 10) doivent utiliser un ou plusieurs postes physiques exclusivement dédiés aux tâches d'administration (configuration des switchs, routeurs, serveurs). Ces postes ne doivent jamais être utilisés pour la navigation web, la messagerie ou d'autres tâches bureautiques et ne doivent pas avoir accès à Internet.

Pour permetre cela nous pouvons créer un VLAN d'administration distinct (par exemple VLAN 99) pour connecter les postes d'administration dédiés et les interfaces de gestion/administration des équipements réseau (switchs Core, Distribution, routeurs) et serveurs (DNS, Web). Ce VLAN doit être strictement isolé des autres VLANs (utilisateurs, serveurs) par des règles de filtrage (ACLs) .

Préconisation 2 : Mise en Place d'une Politique et d'une Infrastructure de Sauvegarde Sécurisée

Constat : Les configurations des équipements réseau (routeurs, switchs Core et Distribution) sont essentielles au fonctionnement de l'infrastructure. De même, les données du serveur DNS et du serveur Web sont critiques. Une perte de ces configurations ou données (suite à une erreur humaine, une panne matérielle, une attaque type ransomware si des connexions externes existaient) paralyserait l'entreprise.

Mise en Œuvre :

Quoi sauvegarder : Configurations des routeurs et switchs L3 (running-config, startup-config), état système et configurations des serveurs DNS et Web, données des zones DNS, contenu du site Web.

Fréquence : Définir une fréquence adaptée à la criticité et à la volatilité des données.

Rétention : Déterminer combien de temps conserver les sauvegardes.

Emplacement : Définir où stocker les sauvegardes.

Serveur de Sauvegarde Dédié et Isolé : Déployer un serveur dédié (ex: serveur TFTP/SFTP/SCP pour les configurations réseau, serveur de fichiers pour les données serveurs) au sein d'un VLAN sécurisé (le VLAN d'administration - VLAN 99 - ou un VLAN de gestion spécifique). L'accès à ce serveur devra contrôlé par des ACLs, autorisant uniquement les flux nécessaires depuis les équipements à sauvegarder et les postes d'administration pour la gestion/restauration.

Préconisation 3 : Mise en Place d'une Journalisation Centralisée et Sécurisée

Constat : Sans une collecte et une analyse centralisées des journaux d'événements (logs), il est extrêmement difficile de détecter les activités suspectes, les tentatives d'intrusion, les erreurs de configuration ou de comprendre le déroulement d'un incident de sécurité après coup.

Mise en Œuvre :

Serveur de Logs Centralisé : Déployer un serveur dédié à la collecte des logs (serveur Syslog) au sein d'une zone sécurisée (VLAN d'administration, VLAN 99 - ou VLAN de gestion dédié). Protéger son accès via ACLs strictes.

Configuration des Équipements Sources : Configurer tous les équipements réseau critiques (Routeurs, Switch Core, Switchs Distribution), les serveurs (DNS, Web) pour envoyer leurs logs via syslog au serveur centralisé. Logs à inclure : connexions/déconnexions, échecs d'authentification, changements de configuration, activité OSPF/HSRP, alertes critiques, logs ACLs pertinents, logs DNS/Web...

Conclusion

L'implémentation de ces trois préconisations techniques (isolation de l'administration, sauvegarde sécurisée, et journalisation centralisée) renforcerait significativement la posture de cybersécurité de l'infrastructure réseau d'Impact Influence, en se basant sur les recommandations de l'ANSSI.