Rapport d’évaluation des risques de sécurité - Analyse du renforcement du réseau

Google Cybersecurity Certificate

Partie 1 : Sélection de trois outils et méthodes de renforcement à mettre en oeuvre

L’entreprise a récemment subi une violation de données, et il est crucial de renforcer les pratiques de sécurité pour prévenir les attaques futures. A cette fin, nous recommandons les trois outils et méthodes de renforcement suivants :

1. **Authentification multifacteur (AMF)** : L'AMF exige que les utilisateurs fournissent deux méthodes d'identification indépendantes, comme un mot de passe et un code OTP envoyé sur leur mobile, pour accéder au système. Cette approche réduit significativement le risque d'accès non autorisé et empêche les attaquants de se connecter au système même s'ils ont volé un mot de passe. L'AMF est particulièrement efficace pour protéger contre les attaques par force brute.

2. **Politiques de mots de passe strictes** : Des mots de passe forts et régulièrement mis à jour sont la première ligne de défense contre les intrusions. Une politique de mots de passe stricte, qui exige au moins 12 caractères, combinant des lettres majuscules et minuscules, des chiffres et des symboles, empêchera les attaquants de deviner les mots de passe. Cette politique doit être appliquée à tous les utilisateurs, en particulier aux comptes administrateurs. La mise en place de formations pour sensibiliser les employés à l'importance de mots de passe forts et de les inciter à ne pas les réutiliser sur d'autres comptes est également essentielle.

3. **Maintenance du pare-feu** : Un pare-feu est un élément crucial de la sécurité du réseau. La maintenance proactive du pare-feu comprend la mise à jour régulière des règles de filtrage, la vérification des configurations et l'activation de la protection DDoS. La mise à jour des règles de filtrage permet de bloquer les tentatives d'accès malveillants et de protéger le réseau contre les attaques de

déni de service. Des configurations rigoureuses du pare-feu garantissent que seuls les ports et services nécessaires sont ouverts, limitant ainsi les points d'accès potentiels pour les attaquants.

Partie 2 : Explication des recommandations

1. **AMF** : L'AMF est essentielle pour protéger contre les attaques par force brute et autres tentatives d'accès non autorisé, en ajoutant une couche de sécurité supplémentaire au-delà du simple mot de passe. Une fois mise en place, elle offre une protection continue avec un entretien minimal.

2. **Politiques de mots de passe strictes** : Des mots de passe forts et régulièrement mis à jour sont la première ligne de défense contre les intrusions. En formant les employés à ces politiques, nous réduisons le risque que des mots de passe faibles ou réutilisés compromettent la sécurité.

3. **Maintenance du pare-feu** : Une gestion proactive du pare-feu, incluant des audits et des mises à jour régulières, permet de s'adapter rapidement aux nouvelles menaces et de maintenir un niveau élevé de sécurité. Cela aide à prévenir les accès non autorisés et les attaques DDoS, en s'assurant que le trafic réseau est légitime et sécurisé.