okta

Checklist de sécurité de l'identité

40 questions pour aider votre entreprise à se protéger des cyberattaques basées sur l'identité

Les brèches de sécurité survenues au cours de l'année écoulée l'ont clairement montré : l'identité est un vecteur d'attaque significatif pour les cybercriminels et les acteurs étatiques. Plus qu'un simple espace de connexion, l'identité est la première et la dernière ligne de défense pour les infrastructures et les données les plus sensibles des entreprises. La sécurité passe par l'identité.

Okta s'est fixé pour mission d'aider ses clients et le secteur dans la lutte contre les attaques ciblant l'identité.

Nous prenons en charge quelque 10 milliards de connexions dans le monde et protégeons plus de 18 000 clients contre près de 2 milliards de requêtes malveillantes par mois. En tant que leader du secteur, Okta s'attache à partager les bonnes pratiques, telles que cette checklist, pour aider ses clients à évaluer leurs besoins et à adopter la posture de sécurité la plus forte possible en matière d'identité. Notez que ces conseils ne constituent jamais qu'un élément de votre programme de sécurité global.

okta

Sécurité de l'identité unifiée et approche Zero Trust

Concepts fondamentaux

1. Votre solution de sécurité des identités s'inscrit-elle dans une ***stratégie de cybersécurité globale*** englobant la gestion des identités et des accès, la résolution des incidents, la gestion des risques et l'amélioration continue ?
2. Avez-vous instauré des mesures pour ***authentifier et autoriser les utilisateurs, terminaux et applications*** de façon dynamique en fonction du contexte de la demande d'accès ?
3. Existe-t-il des processus établis pour ***approuver, examiner et mettre à jour les accès à privilèges*** ?
4. Implémentez-vous l'***accès sur le principe du moindre privilège*** dans votre solution d'identité pour minimiser les surfaces d'attaque potentielles ? En particulier, limitez-vous ou supprimez-vous les droits administrateur chaque fois que c'est possible ?

Concepts avancés

5. Disposez-vous d'une bonne stratégie pour ***surveiller et évaluer en continu le comportement des utilisateurs et des terminaux*** pour détecter des activités anormales ou suspectes ?
6. ***Limitez-vous les permissions du personnel de support IT*** afin de l'empêcher d'effectuer des opérations sur les comptes à privilèges élevés ? Par exemple, créez-vous et attribuez-vous des rôles administrateur personnalisés pour ces utilisateurs ?
7. Avez-vous mis en place des mécanismes pour ***un contrôle strict des identités au niveau du service d'assistance pour les utilisateurs à privilèges***, par exemple à l'aide d'une vérification visuelle ?
8. Avez-vous implémenté des mesures pour ***vérifier en continu*** l'identité des utilisateurs lors de leurs interactions avec vos ressources les plus critiques ?
9. Exigez-vous une ***sécurité Zero Trust de la part de tiers accédant à votre environnement IT*** ? En particulier, procédez-vous à une vérification et à un audit de la posture de sécurité de ces tiers, au lieu de compter implicitement sur leur capacité à gérer leur périmètre réseau ?

Gestion des identités et des accès

Concepts fondamentaux

10. Avez-vous implémenté l'***authentification multifacteur (MFA) avec résistance au phishing*** pour l'accès à toutes les ressources sensibles ?
11. ***Étendez-vous la résistance au phishing à tout le cycle de vie des collaborateurs*** de l'inscription/onboarding à la récupération de comptes ?
12. Exigez-vous une ***authentification renforcée*** lorsque les administrateurs effectuent des actions sensibles ?
13. ***Alertez-vous automatiquement les utilisateurs en cas d'événements à risque élevé (par exemple lors de la réinitialisation de tous les facteurs MFA)*** pour un compte ou lors de l'accès d'un compte à un nouveau terminal ?
14. La ***gestion du cycle de vie des identités***, y compris l'onboarding, l'offboarding et les analyses d'accès, est-elle automatisée pour améliorer la précision et l'efficacité ?
15. Quels critères votre entreprise utilise-t-elle pour ***définir l'inactivité d'un compte*** ? À quelle fréquence réexaminez-vous les comptes inactifs ?
16. Disposez-vous d'une stratégie pour les identifiants des comptes de service, par exemple la ***modification des mots de passe à intervalles réguliers ou après chaque accès interactif*** ?
17. Possédez-vous une ***stratégie de gouvernance des identités*** et comment celle-ci s'aligne-t-elle sur les normes sectorielles et les bonnes pratiques ?
18. Avez-vous mis en place des mécanismes ***pour l'attestation et la certification périodiques des droits d'accès des utilisateurs*** ?
19. Avez-vous appliqué des mécanismes pour offrir un accès transparent et fluide aux ressources pour les utilisateurs distants sur les ***terminaux personnels et d'entreprise*** (ordinateurs portables et mobiles) ?

Concepts avancés

20. Votre solution de gouvernance des identités met-elle en œuvre la ***séparation des responsabilités*** pour éviter les combinaisons toxiques de droits d'accès ?
21. La sécurité des comptes à privilèges est-elle renforcée par des mesures d'***authentification MFA forte avec résistance au phishing*** pour garantir un niveau de sécurité élevé ?
22. Une solution ***PAM (Privileged Access Management) complète*** a-t-elle été déployée pour découvrir, sécuriser, consigner et surveiller les comptes à privilèges ?
23. Exigez-vous des ***tiers qui accèdent à votre environnement IT de s'authentifier via des solutions IAM*** pour toutes les applications professionnelles ?
24. ***Appliquez-vous la liaison des adresses IP pour authentifier les utilisateurs accédant à des ressources critiques*** ? Les administrateurs sont-ils en mesure de révoquer automatiquement une session d'administration si l'adresse IP détectée au cours d'une demande web ou d'API diffère de celle enregistrée lors de l'ouverture de la session ?
25. ***Bloquez-vous les demandes envoyées à votre solution d'identité en fonction du type de réseau*** (par exemple un proxy d'anonymisation) ?

okta

Stratégies de correction et de réduction des risques

Concepts fondamentaux

26. Quels outils et méthodes existants utilisez-vous pour ***renforcer la surveillance des comptes à privilèges*** ?
27. Comment l'***analyse du comportement des utilisateurs*** est-elle intégrée à la stratégie globale de sécurité des identités pour les fonctionnalités de détection et réponse ?
28. Avez-vous configuré des ***alertes automatiques*** en cas de modification de vos agents AD on-premise ?
29. Votre plateforme d'identité prend-elle en charge une approche ***IaC (Infrastructure as Code)*** pour le développement et la gestion des systèmes ?
30. Votre solution d'identité peut-elle identifier les demandes des terminaux connus pour ***éviter les verrouillages de comptes*** lors d'attaques par force brute ?

Concepts avancés

31. Pouvez-vous ***appliquer des restrictions basées sur l'emplacement*** pour les accès utilisateurs et machine to machine (M2M) ?
32. ***Autorisez-vous les administrateurs à détecter et à bloquer les demandes d'un anonymiseur*** s'il est démontré que l'adresse IP correspond à celle d'un anonymiseur ?
33. Pouvez-vous ***appliquer la liaison des tokens pour les intégrations M2M*** à l'aide d'une preuve de possession de telle sorte que seules les applications autorisées puissent utiliser des tokens pour accéder aux API ?
34. ***Tirez-vous parti de fonctions avancées de détection et de protection contre les bots*** à l'aide de scores d'outils tiers et de signaux de composants déployés en périphérie ?
35. Lorsque vous créez des applications, ***implémentez-vous des contrôles de gestion des sessions alliés à une sécurité renforcée des tokens*** ? En particulier, développez-vous vos propres tableaux de bord de sessions pour personnaliser l'expérience utilisateur ?

Formation et sensibilisation des collaborateurs

Concepts fondamentaux

36. Organisez-vous régulièrement pour vos collaborateurs des ***formations de sensibilisation au phishing*** et à la cybersécurité de manière générale, afin de les sensibiliser aux bonnes pratiques et aux dernières menaces ?
37. Les collaborateurs reçoivent-ils des formations et des conseils concernant l'implémentation et les avantages des politiques de mots de passe forts et des options d'***authentification sans mot de passe*** ?
38. Procédez-vous à des ***exercices de simulation de phishing*** pour tester la résilience des collaborateurs aux tentatives de phishing et offrir des formations ciblées à ceux susceptibles d'être victimes de telles attaques ?
39. Existe-t-il un ***mécanisme permettant aux collaborateurs de signaler des problèmes de sécurité potentiels*** ou de demander des explications sur les questions liées à la sécurité ?
40. Les collaborateurs ont -ils été sensibilisés à l'importance ***des mises à jour des logiciels et des terminaux*** avec les derniers correctifs de sécurité ?