Sécurité et gestion des identités : la lutte contre les comptes orphelins et les comptes inactifs

formind netwrix

Quelle est la crainte partagée par toutes les DSI et les responsables d'IAM, quel que soit le secteur d'activité, la taille de l'entreprise et le chiffre d'affaires ?

Que des collaborateurs ou prestataires externes laissent derrière eux de multiples comptes ouverts après leurs départs, promotions ou leurs mobilités. Ce phénomène de comptes dit dormants (ou orphelins) est une réelle menace aussi bien pour le coût non maitrisé sur les licences des logiciels et services en ligne que sur la surface d'attaque cyber non négligeable qu'elle crée. Cette gestion lacunaire du cycle de vie aussi bien des comptes utilisateurs standards que des comptes à privilèges reste un réel défit pour les organismes et pour les services Informatiques car elle est la principale cause de la prolifération des comptes orphelins.

Mais avant de poursuivre, qu'est-ce qu'est exactement **un compte orphelin ?**

Un compte orphelin est un compte technique ou applicatif avec ou sans privilèges, qui n'est associé à aucune identité active ou existante.

La présence de comptes orphelins est dangereuse pour un système d'information. La chasse de ces comptes « fantômes » permet de réduire considérablement le budget informatique alloué aux systèmes et services technologiques d'autant plus que sans cela, nous constatons les écueils suivants identifiés par thématique :

Gestion des Identités et des habilitations	• Une gestion des droits et des accès complexifiés avec des audits « creux » ou difficiles à mener ; • Une visibilité réduite sur « qui a accès à quoi, pourquoi et depuis quand ».
Cybersécurité	• Un No man's land qui est une brèche idéale pour les cyberattaquants ; • Une pollution du réseau ; • La propagation d'une mentalité du Shadow IT dans l'entreprise, ce qui augmente les risques sur la cybersécurité et les failles de vulnérabilités.
Licences et coûts	• Une augmentation du nombre de tickets, durant le run, pour des demandes de dé-provisionnement de ces comptes actifs à tort ; • Une augmentation du temps d'onboarding de collaborateurs pour cause d'absence de licences disponibles (bloquées sur des comptes fantômes), entrainant une perte de productivité générale ; • Un surplus de budget Informatique pour le suivi, le contrôle et la gestion de licences ; • Des procédures chronophages et très souvent manuelles pour la libération de licences non utilisées.
Responsabilité numérique et RGPD	• Une non-inscription à une démarche d'un numérique responsable ; • Des problèmes juridiques si des contrats sont violés ; • Des responsabilités RGPD non respectées si ces comptes venaient à être utilisés par d'autres utilisateurs.

La liste regroupée dans le tableau ci-dessus ne se veut pas exhaustive, mais les principaux enjeux étant ainsi identifiés, **comment éviter l'apparition de comptes orphelins dans son SI ?**

La prolifération de ces comptes est principalement due à une gestion incomplète ou inexistante du cycle de vie de l'identité qui, elle, influe sur le cycle de vie des accès et des habilitations. Un lien direct entre le statut d'une identité et le calcul automatique de l'attribution des ressources, avec derrière une synchronisation fréquente auprès des systèmes cibles permettent cette vision et gouvernance holistique et exhaustive qui empêche et endigue à la racine l'apparition des comptes orphelins :

c'est-à-dire une solution de Gestion des Identités et des Accès avec une architecture assez souple et structurante qui permet de couvrir avec facilité tous les scénarios de mobilité et de turn-over de collaborateurs au sein de l'entreprise, qu'il s'agisse :

- d'un départ programmé après lequel il faudra garantir la suspension puis le retrait des rôles et le dé-provisionnement de l'ensemble des comptes, en gérant une période de grâce éventuelle,
- d'un départ immédiat,
- d'une suspensions longue durée,
- de réorganisations internes,
- de la prise en charge de cumul de postes et de fonctions qui peut devenir très vite complexe.

L'architecture de solution Netwrix Usercube permet nativement de répondre à ce besoin de distinction entre l'identité numérique du collaborateur et ses ressources informatiques (notamment les multiples comptes qui lui sont attribués).

Netwrix Usercube fournit une distinction claire entre les identités et leurs droits et les ressources techniques qui matérialisent ceux-ci au sein du système d'information.

En effet, la solution IGA (Identity Governance & Administration) de Netwrix est conçue dès son origine pour gérer les identités numériques de l'entreprise et les droits nécessaires à la réalisation de leur mission. Usercube fait une séparation nette entre l'identité et ses droits (rôles) et les ressources techniques qui devront lui être allouées dans le SI en lien avec ces rôles. Ces ressources techniques se matérialisent par des comptes de connexions (permettant d'accéder aux différents systèmes et applications), et des droits spécifiques pouvant se matérialiser entre autres par le rattachement d'un compte de connexion à un groupe Active Directory (ou LDAP ou Entra ID) ou par l'attribution à un profil applicatif au sein d'une application.

En gérant le cycle de vie de l'identité (arrivée, départ, mutation, multi-affectations, absence longue, changement de contrat, ...), la solution permet sur chaque situation de fournir à l'identité les moyens que nécessite son activité, mais également de les supprimer lorsque sa situation évolue.

Netwrix Usercube, au travers de ses connecteurs, découvre automatiquement les comptes de votre SI et permet de les rattacher à des identités. Ce faisant, les comptes orphelins sont immédiatement démasqués et peuvent être traités.

Pour Netwrix Usercube, une identité numérique est une personne ou une chose qui nécessite d'avoir des moyens pour interagir avec le système d'information. Sont donc ainsi gérées les personnes (internes ou externes à l'entreprise), mais également les applications (pouvant nécessiter des comptes de services pour accéder à certaines ressources du SI), les objets connectés (IoT, salle de réunion connectée, …), les bots (RPA), etc. En couvrant l'ensemble des identités numériques et en gérant les comptes de connexion qui leur sont rattachés, cette IGA garantit la supervision de l'ensemble des comptes de l'entreprise et leur cycle de vie en lien avec celui des identités.

Netwrix Usercube est une tour de contrôle du SI, détectant tout écart entre les droits qui sont nécessaires et définis dans son référentiel et ce qu'il constate dans le SI. Ces écarts peuvent ensuite être traités, que ce soit techniquement en demandant la suppression des comptes directement dans la solution, mais également fonctionnellement en identifiant les axes d'amélioration nécessaires à l'organisation (communication, formation, changement).

Au-delà des comptes et des identités, Netwrix Usercube assure de façon aussi efficace les droits attribués à ces identités, mais ce sera sans doute l'objet d'un prochain échange.

Le partenariat Formind x Netwrix

Formind et Netwrix, partenaires depuis des années et acteurs clés du marché français, interviennent ensemble sur des projets auprès d'entreprises et organismes de secteurs d'activités variés tels que Banque, Assurance, Industrie et Energie.

Formind dispose d'une expertise de premier plan en matière d'IAM – tant sur le plan fonctionnel que technique - qui permet de proposer à ses clients les meilleures solutions adaptées à leur contexte.

L'association des deux sociétés permet de présenter une proposition de valeur unique, à la hauteur de votre projet et des attentes qui y sont associées.

A propos de Netwrix Corporation

Cybersecurity that works for you

Netwrix est un leader de cybersécurité et assure un avenir numérique plus prometteur toutes les organisations. Les solutions innovantes de Netwrix protègent les données, les identités et les infrastructures, réduisant à la fois le risque et l'impact d'une violation pour plus de 13 500 organisations dans plus de 100 pays. Netwrix permet aux professionnels de la sécurité de faire face aux menaces numériques en toute confiance en leur permettant d'identifier et de protéger les données sensibles, ainsi que de détecter les attaques, d'y répondre et de s'en remettre.

Pour plus d'informations, visitez www.netwrix.fr

A propos de Formind

Security for Business Performance

Formind est un leader français indépendant expert en cybersécurite dont la mission est simple et belle : protéger ses clients.
Qualifié PASSI, en cours de qualification PRIS par l'ANSSI et certifié ISO 27001, Formind aide ses clients à être plus résilients et à se protéger des risques numériques à travers ses trois métiers:
CONSEIL - INTÉGRATION - SOC&CERT.
Formind propose également une offre dédiée au tissu économique des ETI et PME-PMI, venant répondre à leurs problématiques spécifiques de cybersécurité.

Pour plus d'informations, visitez www.formind.fr ou contact@formind.fr