Technologies de l'information

Cours:

Sécurité des systèmes informatiques

DESS

Séance # 9

Préparé par: Blaise Arbouet

Contenu de la séance

- Concepts de base de la GIA
- Méthodes d'authentification (mots de passe, biométrie, authentification multi facteur)
- Contrôle d'accès basé sur les rôles

DÉFINITION DE LA GIA

La gestion des identités et des accès (GIA) désigne un ensemble de processus, de politiques et de technologies qui assurent de manière sécurisée et efficace la création, la gestion et l'authentification des identités numériques des utilisateurs et les **privilèges d'accès** associés aux ressources.

Objectifs de la GIA

L'objectif principal des systèmes GIA est une identité numérique par personne. Une fois cette identité établie, elle doit être gérée, modifiée et surveillée dans l'ensemble des utilisateurs.

Important: Elle doit avoir un cycle de vie.

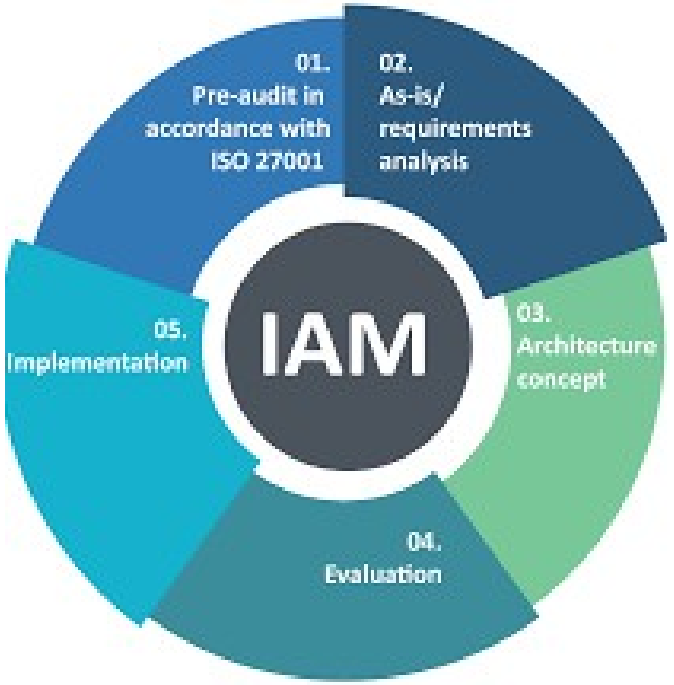
Que fournit la GIA?

La GIA fournit aux administrateurs les outils et les technologies nécessaires pour modifier le rôle d'un utilisateur, suivre ses activités, créer des rapports sur ces activités et appliquer des stratégies de manière continue. Ces systèmes sont conçus pour fournir un moyen de gérer l'accès des utilisateurs dans l'ensemble de l'entreprise et de garantir la conformité avec les politiques de l'entreprise et les réglementations gouvernementales.

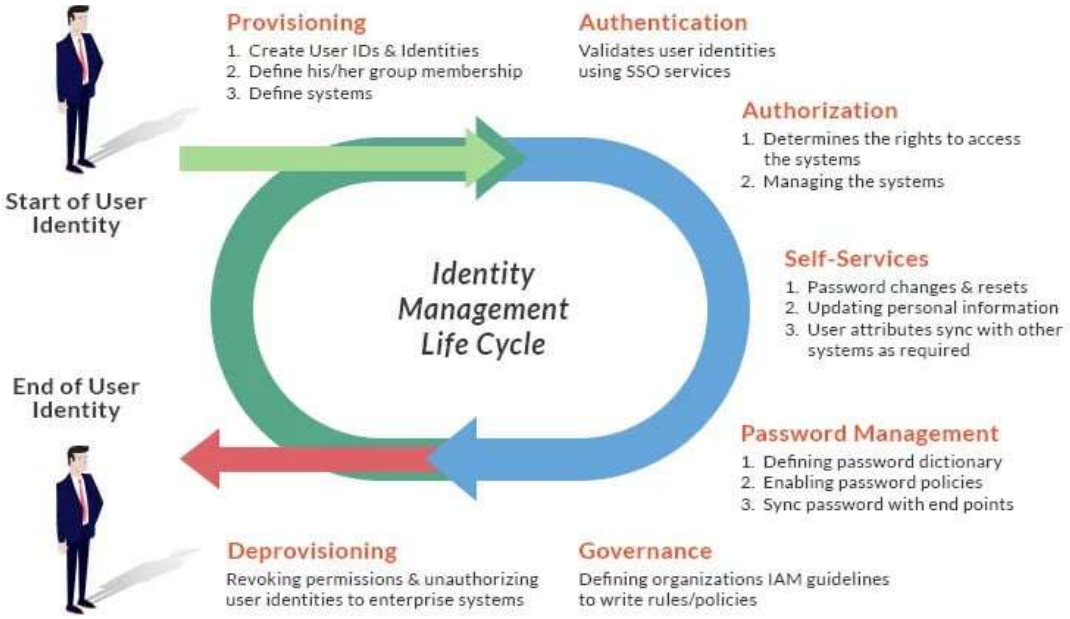
Avantages GIA

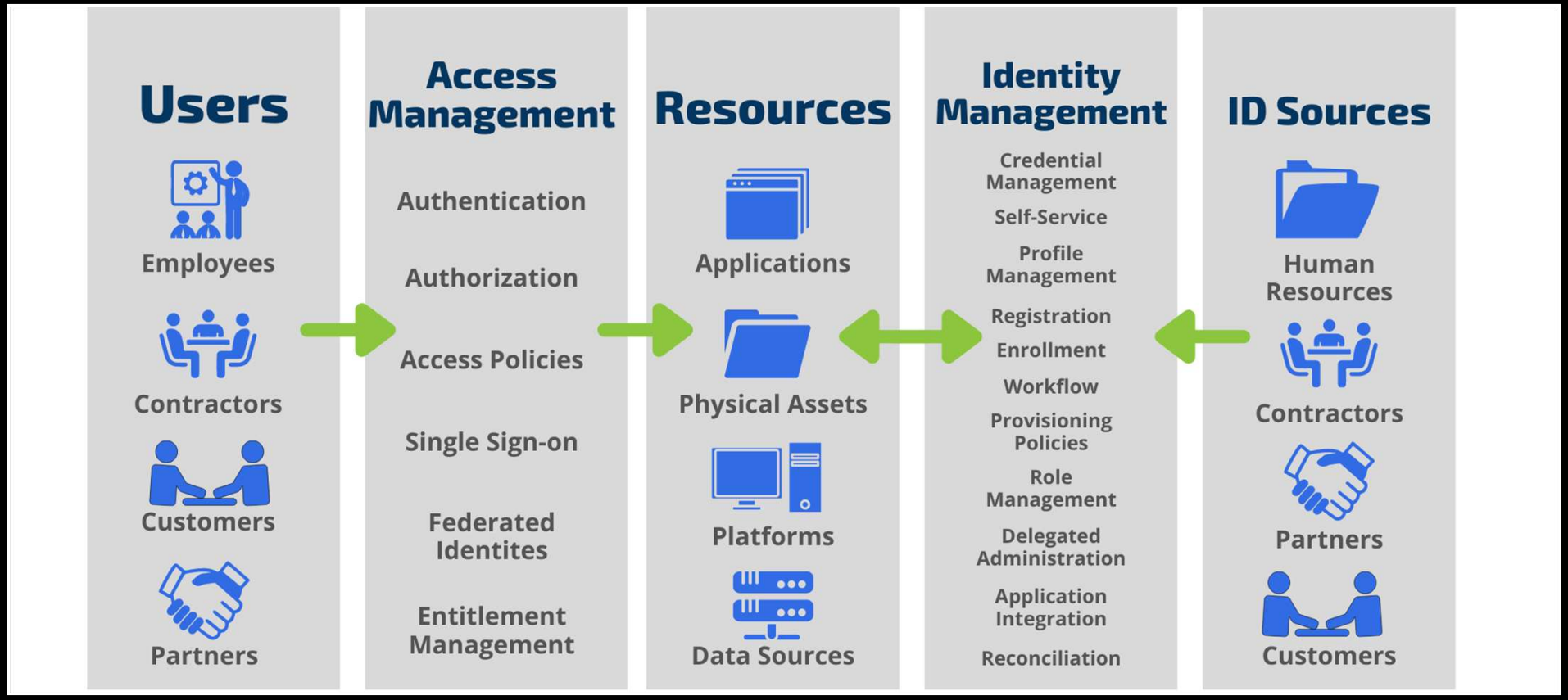
Les systèmes de gestion des identités peuvent permettre à une entreprise d'étendre l'accès à ses systèmes d'information à un grand nombre d'applications locales, d'applications mobiles et d'outils SaaS sans compromettre la sécurité.

La gestion des identités peut réduire le nombre d'appels du centre d'assistance aux équipes de support informatiques concernant la réinitialisation des mots de passe.



Cycle de vie d’un utilisateur



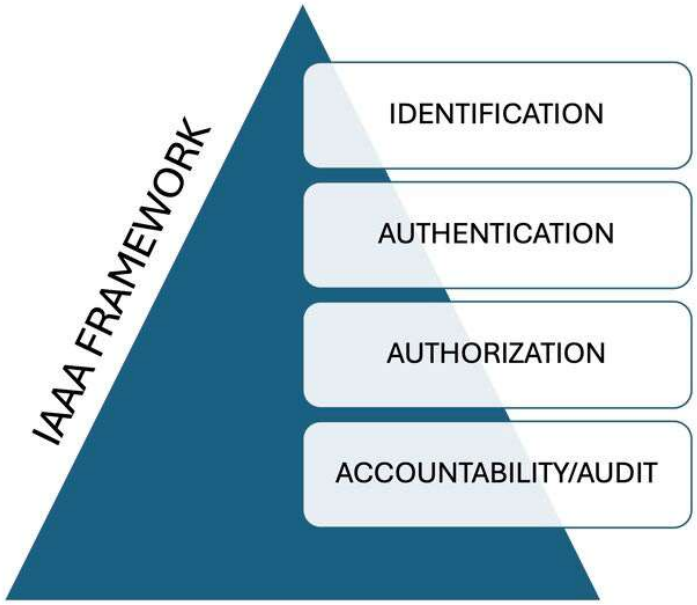


Braxton-Grant TECHNOLOGIES

Autres composantes

Model IAAA

Le modèle IAAA propose une approche structurée pour renforcer la sécurité de l'information en garantissant que les identités sont correctement identifiées, authentifiées, autorisées et tenues responsables. La mise en œuvre de ce modèle aide les organisations à protéger leurs données, à maintenir l'intégrité opérationnelle et à instaurer la confiance avec les utilisateurs et les parties prenantes.



Identification (1)

Identification

L'identification est le processus de reconnaissance d'un individu ou d'un système au sein d'un réseau. Elle implique la présentation d'un identifiant, tel qu'un nom d'utilisateur ou un numéro d'identification, pour revendiquer une identité. Une identification correcte est la première étape pour établir la confiance au sein d'un système.

Pratiques clés :

Identifiants utilisateur : Attribution d'identifiants uniques aux utilisateurs.

Biométrie : Utilisation de caractéristiques physiques (par exemple, empreintes digitales, reconnaissance faciale) pour identifier les utilisateurs.

Étiquettes RFID : Utilisation de l'identification par radiofréquence pour les systèmes et les équipements.

Authentification (2)

L'authentification vérifie l'identité revendiquée lors du processus d'identification. Elle garantit que l'entité est bien celle qu'elle prétend être, généralement au moyen de mots de passe, de codes PIN, de données biométriques ou de jetons de sécurité. Des mesures d'authentification rigoureuses sont essentielles pour empêcher tout accès non autorisé.

Pratiques clés :

Authentification multifacteur (AMF) : Combinaison de deux facteurs d'authentification ou plus (par exemple, une information connue, une information détenue, une information personnelle).

Politiques de mots de passe : Application de mots de passe complexes et de mises à jour régulières.

Vérification biométrique : Utilisation des empreintes digitales, de l'iris ou de la reconnaissance faciale pour une sécurité renforcée.

Autorisation (3)

Autorisation

L'autorisation détermine le niveau d'accès accordé à une entité authentifiée. Elle garantit que les utilisateurs ou les systèmes ne peuvent accéder qu'aux ressources et effectuer les actions pour lesquelles ils sont autorisés. Une autorisation appropriée empêche les actions et accès non autorisés au système.

Pratiques clés :

Contrôle d'accès basé sur les rôles (RBAC) : Attribution d'autorisations en fonction des rôles des utilisateurs.

Listes de contrôle d'accès (ACL) : Définition d'autorisations spécifiques pour les utilisateurs ou les systèmes.

Application des politiques : Mise en œuvre et maintenance cohérentes des politiques de sécurité.

Audit (4)

L’Audit garantit que les actions au sein d'un système peuvent être retracées jusqu'à l'entité responsable. Elle implique la journalisation et la surveillance des activités afin de détecter et de répondre efficacement aux incidents de sécurité. L’audit est essentiel au maintien de la confiance et de l'intégrité au sein d'un système.

Pratiques clés :

Journaux d'audit : Enregistrement des activités des utilisateurs et des tentatives d'accès.

Surveillance des activités des utilisateurs : Observation continue du comportement des utilisateurs pour détecter toute anomalie.

Plans de réponse aux incidents : Préparation à une intervention rapide en cas de faille de sécurité.

Les modèles de gestion des accès (MAC)

MAC(*Mandatory Access Control*)

Besoins de confidentialité sont très forts (armée, gouvernement),

- Donner un niveau de classification à la ressource par un *label* (Confidentiel, Secret, Top-Secret …)
- Donner parallèlement un niveau d'accréditation ou d'habilitation (*clearance*) au personnel censé pouvoir accéder à cette dernière.

Exemple : Dans un réseau gouvernemental classifié, l'accès aux documents sensibles est restreint en fonction des habilitations de sécurité et du principe du besoin de savoir.

Les modèles de gestion des accès (DAC)

DAC(*DiscretonaryAccess Control*)

le rôle de **propriétaire** de la ressource :

- A autorité pour conférer des droits d'accès à la ressource (à la seule «discrétion» du propriétaire). si la ressource dont on parle est une donnée critique, l'organisation est par défaut sa propriétaire nominale. Elle peut déléguer totalité ou partie de ses droits sur la ressource (un système, une donnée, un fichier). C'est une chaîne de propriété qui part de l'organisation puis descend jusqu'au niveau des entités. Dans certaines organisations, les propriétaires sont des services entiers (***data owners***) pour des données métier. Les **délégataires implicites** sur la ressource sont les créateurs de fichiers de données qui obtiennent le privilège de conférer des droits d'accès (logiques).
- Exemple : dans un dossier partagé sur un serveur de fichiers, le propriétaire du dossier peut définir des autorisations pour permettre à des utilisateurs ou des groupes spécifiques de lire, d'écrire ou de modifier des fichiers en fonction de leurs besoins.

Les modèles de gestion des accès (RBAC)

RBAC(*Role-BasedAccess Control*)

Par groupes d'utilisateurs possédant des droits identiques sur la même ressource:

Cette méthode est dite non discrétionnaire parce que la politique de contrôle d'accès est gérée de manière centralisée, contrairement au **DAC** où le propriétaire est capable de donner des droits selon ses critères (exemple le partage d'un dossier personnel sur son ordinateur). Tandis que le **DAC** se souciait seulement de l'identité de celui ou celle qui accède à la ressource, le **RBAC** s'intéresse à la fonction et aux tâches exécutées par ces **mêmes** personnes.

Dans une organisation de soins de santé, des rôles tels que « Médecin », « Infirmière » et « Administrateur » sont définis, chacun avec des privilèges d'accès spécifiques aux dossiers des patients et aux fonctions administratives.

Les modèles de gestion des accès (RAC)

- RAC(Rule-BasedAccess Control)
- L'accès basé sur des règles **(RAC)** contrôlera l'autorisation en fonction de conditions autres que votre identité (par exemple, l'heure du jour, l'emplacement, le type de périphérique).
- Par exemple, dans un contexte de contrôle d'accès basé sur des règles, un administrateur peut définir des heures d'accès pour la journée de travail habituelle. Dans ce cas, une personne ne peut pas entrer dans votre bâtiment en dehors des heures de 9 h à 17 h.

Protocole d’authentification

Un protocole d’authentification permet à la partie destinataire (p. ex. un serveur) de vérifier l’identité d’une autre partie (p. ex. une personne utilisant un terminal mobile pour se connecter). La vaste majorité des systèmes informatiques utilisent une forme quelconque d’authentification réseau pour vérifier l’identité des utilisateurs.

Exemples de protocoles d'authentification

1. **Kerberos:** si vous possédez un environnement Windows, vous avez utilisé ce protocole. Le système s'appuie sur des clés symétriques extraites d'un centre de distribution de clés centralisé. Même s'il dispose de mécanismes de protection importants, Kerberos n'est pas infaillible. En 2020, Kerberos a arrêté de fonctionner après une mise à jour système.
2. **LDAP :** comme nous l'avons expliqué dans un récent article de blog, les entreprises stockent les noms d'utilisateurs, les mots de passe, les adresses e-mail, les connexions des imprimantes et d'autres données statiques dans des annuaires. LDAP est un protocole d'application ouvert et indépendant, utilisé pour l'accès et la gestion de ces données.
3. **OAuth 2.0 :** si vous vous êtes déjà servi des identifiants que vous utilisez sur un autre site web (comme Facebook) pour accéder à un autre site (comme le New York Times), vous avez en fait utilisé OAuth 2.0. Une application récupère les ressources pour vous et vous n'avez pas à partager vos identifiants. Cela dit, ce système peut également être piraté, comme l'a constaté GitHub en 2020.

Exemples de protocoles d’authentication(suite)

1. **RADIUS (Remote Authentication Dial-In User Service) :** vous saisissez un nom d’utilisateur et un mot de passe, et le système RADIUS vérifie les informations en les comparant à celles d’une base de données.
2. **SAML 2.0 :** ce protocole XML échange des données d’authentification entre les fournisseurs d’identité et les fournisseurs de services.
3. **OpenID**: OpenID Connect (OIDC) est un protocole d'authentification d'identité qui est une extension de l'autorisation ouverte (OAuth) 2.0 pour normaliser le processus d'authentification et d'autorisation des utilisateurs lorsqu'ils se connectent pour accéder aux services numériques.

Authentification forte «MFA» et «2FA»

1)L'authentification multi-facteurs (MFA) est une méthode de confirmation de l'identité déclarée d'un utilisateur dans laquelle l'utilisateur est autorisé à accéder uniquement après avoir présenté avec succès deux ou plusieurs éléments de preuve (ou facteurs) à un mécanisme d'authentification:

- Quelque chose que je connais (ce que l'utilisateur sait)
- Quelque chose que je possède
- Quelque chose que je suis
- Emplacement geospatial

2) L'authentification à deux facteurs (2FA) est un type (sous-ensemble) d'authentification multi-facteurs. C'est une méthode de confirmation de l'identité des utilisateurs en utilisant une combinaison de deux facteurs différents:

- quelque chose qu'ils connaissent,
- quelque chose qu'ils ont, ou
- quelque chose qu'ils sont (biométrie).

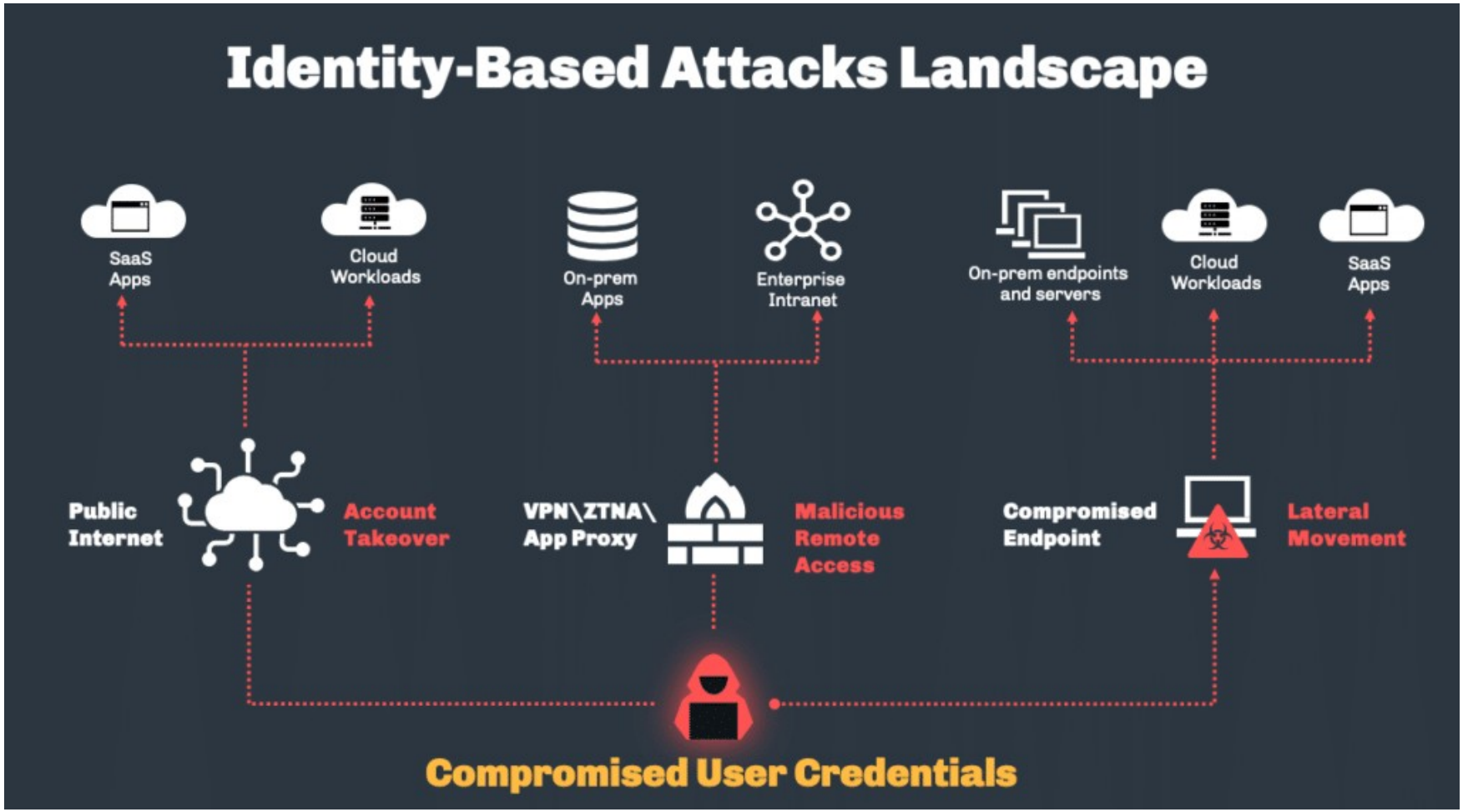
Exemple: guichet bancaire; seule la combinaison correcte d'une carte bancaire (quelque chose que l'utilisateur possède) et d'un code PIN (numéro d'identification personnel, quelque chose que l'utilisateur connaît) permet d'effectuer la transaction.

Gestion des comptes à haut privilege (PAM)

La gestion des accès privilégiés (PAM) est une stratégie de cybersécurité qui protège les ressources critiques d'une organisation en surveillant, en détectant et en empêchant l'accès non autorisé aux comptes privilégiés. PAM est basé sur le principe du moindre privilège, qui limite l'accès au niveau minimum requis pour effectuer le travail d'un utilisateur.

Types de comptes à haut privilège

- Comptes privilégiés
- Comptes de service
- Comptes d'administrateur de domaine
- Comptes d'utilisateur privilégiés (unités d’affaires)
- Comptes d'urgence
- Comptes d'administrateur local


Identity-Based Attacks Landscape
SaaS Apps
Cloud Workloads
On-prem Apps
Enterprise Intranet
On-prem endpoints and servers
Cloud Workloads
SaaS Apps
Public Internet
Account Takeover
VPN\ZTNA\ App Proxy
Malicious Remote Access
Compromised Endpoint
Lateral Movement
Compromised User Credentials

Ex d’attaques contre les identifiants

- Hameçonnage
- Enregistrement de frappe (key logging)
- Ingénierie sociale
- Bourrage d'informations d'identification (credentials stuffing)
- Fausse utilisation de données biométriques
- Attaque de l'homme du milieu (MITM)
- Attaque par dispersion de mots de passe (password spraying)
- Attaque par transmission de hachage (pass-the-hash)

Pour se protéger

- Implementation MFA
- Gestion de réponse aux incidents
- Journalisation et surveillance
- Adoption approche Zero Trust
- Détection basée sur l’IA
- Politique de GIA
- Etc..

Références

- https://www.proserveit.com/blog/what-is-microsoft-zero-trust-security-model
- https://www.microsoft.com/en-us/security/blog/2019/11/11/zero-trust-strategy-what-good-looks-like/
- https://www.tenable.com/blog/aws-azure-and-gcp-the-ultimate-iam-comparison
- https://www.okta.com/fr/identity-101/authentication-protocols
- https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam
- https://www.innominds.com/blog/open-source-tools-for-identity-and-access-management
- https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/identity-attack/
- https://www.cisco.com/site/us/en/learn/topics/security/what-is-identity-access-management.html
- https://www.keepersecurity.com/blog/2023/12/05/what-are-identity-based-attacks/
- **https://www.silverfort.com/glossary/identity-based-attacks/**