Compte Rendu : Cas d’usage

Compromission d’un compte utilisateur en entreprise

Rédigé par :

Mathéo Moussé

Sommaire

Définitions

Compte utilisateur

Un compte utilisateur est un identifiant personnel permettant à un employé d'accéder aux ressources du système d'information (SI) de l'entreprise, comme les messageries, les fichiers, les applications internes, etc. Il est généralement associé à un mot de passe et parfois à une authentification multifacteur (MFA).

Compromission de compte

La compromission d'un compte correspond à un accès non autorisé à ce compte par une personne malveillante. Cela peut résulter du vol de mot de passe, d'une attaque de phishing, ou d'une faille de sécurité.

Système d'information (SI)

Le système d'information d'une entreprise regroupe l'ensemble des moyens techniques, humains, logiciels et matériels qui permettent de stocker, traiter, sécuriser et transmettre l'information.

Question 1 : Quel risque y a-t-il à avoir un compte compromis au sein d'une entreprise ?

Un compte compromis peut entraîner plusieurs risques majeurs pour une entreprise :

1. Vol de données sensibles

Un compte compromis peut donner accès à :

- Des informations sensibles : documents internes, contrats, données personnelles (RH, clients).
- Des informations stratégiques : plans d'affaires, codes sources, projets confidentiels.
    - Cela peut entraîner une fuite de données ou une violation du RGPD, passible de sanctions financières.

2. Escalade de privilèges

Un attaquant peut utiliser un compte standard pour tenter une élévation de privilèges, par exemple en compromettant un autre compte mieux doté en droits (admin local, AD, etc.).

- Cela permet un contrôle accru sur le réseau et les systèmes, voire une prise de contrôle complète.

3. Propagation de logiciels malveillants

Le compte compromis peut servir à :

- Installer des malware ou des ransomwares (Rançongiciel) sur le réseau de l'entreprise.
    - Cela peut causer une paralysie des systèmes, avec demande de rançon et perte d'exploitation.

4. Usurpation d'identité

Les cybercriminels peuvent se faire passer pour des employés légitimes pour tromper d'autres membres de l'organisation ou des partenaires externes.

Le compte légitime peut être utilisé pour :

- Envoyer des emails de phishing internes ou à des clients.

5. Atteinte à la réputation

Une compromission rendue publique peut :

- Nuire à la confiance des clients et des partenaires.

- Avoir un impact boursier ou commercial, surtout dans les secteurs réglementés (banque, santé, télécoms).
    - L'image de l'entreprise est durablement affectée.

6. Coûts financiers et juridiques

- Fraude financière : Les comptes compromis peuvent être utilisés pour effectuer des transactions frauduleuses ou des virements bancaires non autorisés3.
- Détection, réponse à incident, audit, reconstruction du SI : coûts techniques élevés
- Amendes RGPD, actions judiciaires : risques juridiques
- Pertes de revenus et opportunités : conséquences économiques

Cas réels de compromission

- Microsoft Exchange (2021) : exploitation de failles et comptes compromis, fuite massive de données.
    - https://www.lemagit.fr/actualites/252507160/Exchange-une-faille-de-lauto-decouverte-laisse-fuiter-des-identifiants
- Uber (2022) : compte d'un employé compromis par ingénierie sociale, accès aux systèmes internes.
    - https://www.bitdefender.com/fr-fr/blog/hotforsecurity/piratage-des-systemes-internes-duber-par-un-adolescent
- Cyberattaque contre un groupe hospitalier de Rennes (2024) : un ancien responsable de la sécurité informatique arrêté
    - https://www.tf1info.fr/justice-faits-divers/video-tf1-piratage-cyberattaque-contre-un-groupe-hospitalier-de-rennes-un-ancien-responsable-de-la-securite-informatique-arrete-2341293.html

Question 2 : Quelles sont les attaques possibles pour compromettre un compte utilisateur ?

Un attaquant dispose de nombreuses techniques pour compromettre un compte utilisateur. Ces attaques exploitent à la fois des faiblesses humaines, techniques et organisationnelles. Voici les attaques les plus courantes :

1. Phishing (Hameçonnage)

Le phishing est l'attaque la plus fréquente. L'attaquant envoie un email (ou SMS) usurpant l'identité d'un tiers de confiance (banque, Microsoft, DSI…) pour pousser l'utilisateur à :

- cliquer sur un lien malveillant
- saisir ses identifiants sur une fausse page de connexion
- ou ouvrir une pièce jointe infectée

Variantes : spear-phishing (ciblé), smishing (SMS), vishing (appel vocal)

2. Ingénierie sociale

Manipulation psychologique exploitant la confiance ou la méconnaissance de la victime :

- usurpation d'identité d'un collègue ou du support informatique
- demande d'accès "urgent" à un service
- création de scénarios crédibles (faux incidents, fausses urgences)

3. Brute Force et attaques par dictionnaire

L'attaquant tente de deviner le mot de passe par des essais automatisés :

- Brute force : toutes les combinaisons possibles
- Dictionnaire : liste de mots de passe courants
- Risque élevé si la politique de mot de passe est faible ou absente.

4. Exploitation de vulnérabilités

Certaines applications ou services web (portails d'authentification, serveurs RDP, VPN) peuvent contenir des failles permettant :

- d'intercepter des identifiants
- de contourner l'authentification
- ou d'injecter des commandes (SQL Injection, XSS)

5. Keyloggers et Malwares

Un malware installé sur le poste utilisateur (via pièce jointe ou site piégé) peut :

- enregistrer les frappes clavier (keylogger)
- intercepter les mots de passe

6. Man-in-the-Middle

L'attaquant intercepte les communications entre l'utilisateur et le serveur (ex : Wi-Fi public non sécurisé) pour :

- capturer des identifiants

7. Utilisation de mots de passe faibles ou réutilisés :

Les mots de passe simples ou réutilisés sur plusieurs comptes sont plus faciles à compromettre.

Question 3 : Comment protéger le système d'information d'une entreprise d'une compromission de compte ?

La protection du système d'information (SI) contre la compromission de comptes repose sur une stratégie de défense en profondeur, combinant des mesures techniques, organisationnelles et humaines. L'objectif est de réduire la surface d'attaque, détecter les comportements anormaux et limiter l'impact en cas de compromission.

1. Renforcer l'authentification des utilisateurs

- Politique de mots de passe robuste
    - Longueur minimale, complexité (majuscule, chiffre, caractère spécial)
    - Utilisation d'un gestionnaire de mot de passe
    - Détection de mots de passe compromis (via HaveIBeenPwned par exemple)
- Authentification multifacteur (MFA)
    - Ajout d'un deuxième facteur (application mobile, clé PKI, SMS) pour sécuriser les connexions.
    - Même en cas de vol de mot de passe, l'accès reste protégé.
- Accès conditionnel
    - Bloquer l'accès depuis des pays à risque, ou en dehors des heures ouvrées. Fonctionnalité intégrée à Microsoft Entra ID (ex-Azure AD Conditional Access).

2. Sensibiliser les utilisateurs

Formation continue

Former régulièrement les collaborateurs à :

- la détection de phishing
- les bonnes pratiques d'hygiène numérique
- la reconnaissance des comportements suspects
- Formation interne

Simulations d'attaques

Lancer des campagnes de phishing simulé par mail pour tester la réactivité des employés.

3. Surveiller et détecter les comportements suspects

- Supervision des journaux et des accès
    - Surveillance des connexions anormales (heure inhabituelle, IP géolocalisée à l'étranger, multiples échecs)
    - Alertes en cas d'activités suspectes : MFA désactivé, changements de droits, ouverture massive de fichiers
- SIEM (Security Information and Event Management)
    - Exemple : Microsoft Sentinel pour centraliser et analyser les logs de sécurité.

4. Appliquer le principe du moindre privilège

- Gestion fine des droits d'accès
    - Attribution des droits minimum nécessaires à chaque rôle utilisateur
    - Suppression immédiate des comptes inactifs ou d'anciens employés
- Comptes à privilèges séparés
    - Compte "admin" distinct du compte de travail quotidien
    - Mises à jour régulières des logiciels
    - Maintenir les systèmes et les logiciels à jour pour corriger les vulnérabilités connues

Question 4 : Quelles sont les solutions Microsoft qui peuvent permettre de lutter contre la compromission de comptes ?

Pour lutter contre la compromission de comptes, Microsoft propose plusieurs solutions intégrées qui aident à sécuriser les environnements informatiques des entreprises.

Voici quelques-unes des principales solutions Microsoft :

1. Microsoft Defender for Office 365

- **Description** : Microsoft Defender for Office 365 est une solution de sécurité qui offre une protection avancée contre les menaces par e-mail, les liens malveillants (URL), et les pièces jointes infectées.
- **Fonctionnalités clés** :
    - **Protection contre le phishing** : Détecte et bloque les tentatives de phishing ciblant les utilisateurs.
    - **Protection contre les logiciels malveillants** : Analyse les pièces jointes et les liens pour détecter et bloquer les logiciels malveillants.
    - **Investigation et réponse automatisées (AIR)** : Automatise la réponse aux incidents de sécurité, réduisant ainsi le temps de réponse aux menaces.

2. Microsoft Entra ID (anciennement Azure Active Directory)

- Description : Microsoft Entra ID est un service d'identité et d'accès basé sur le cloud qui aide les employés à se connecter et à accéder aux ressources internes et externes.
- Fonctionnalités clés :
    - Authentification multifacteur (MFA) : Ajoute une couche supplémentaire de sécurité en exigeant une deuxième forme de vérification.
    - Gestion des identités et des accès : Permet de gérer les accès des utilisateurs et de sécuriser les identités dans un environnement hybride ou cloud.
    - Protection des identités : Utilise l'apprentissage automatique pour détecter les activités suspectes et les risques potentiels.

3. Microsoft Sentinel

- Description : Microsoft Sentinel est une solution de gestion des événements de sécurité et des informations (SIEM) qui offre une analyse de sécurité intelligente et une réponse aux menaces.
- Fonctionnalités clés :

- Détection des menaces : Utilise l'IA pour détecter les menaces et les comportements anormaux.
- Réponse aux incidents : Fournit des outils pour enquêter sur les incidents et y répondre rapidement.
- Intégration avec d'autres outils Microsoft : S'intègre avec d'autres solutions de sécurité Microsoft pour une protection complète.

4. Microsoft Defender pour le cloud

- Description : Microsoft Defender pour le cloud est une solution de protection des charges de travail hybrides qui offre une visibilité et un contrôle sur la sécurité des ressources cloud et locales.
- Fonctionnalités clés :
  - Évaluation de la sécurité : Évalue en continu la posture de sécurité de vos ressources.
  - Protection contre les menaces : Détecte et répond aux menaces dans les environnements cloud.
  - Gestion des vulnérabilités : Identifie et aide à corriger les vulnérabilités dans vos systèmes.

5. Microsoft Defender XDR

- Description : Microsoft Defender XDR est une solution de détection et réponse étendue (XDR) qui intègre la protection contre les menaces sur les endpoints, les identités, les e-mails et les applications.
- Fonctionnalités clés :
  - Protection intégrée : Combine les signaux de sécurité de plusieurs sources pour une détection et une réponse unifiées.
  - Automatisation et orchestration : Automatise les réponses aux incidents pour une efficacité accrue.
  - Analyse des menaces : Fournit des informations détaillées sur les menaces et les attaques.

Sources

1. Proofpoint - Ces compromissions de comptes qui échappent à Microsoft
2. Proofpoint - Qu'est-ce qu'un compte compromis
3. Cybermalveillance.gouv.fr - Piratage de compte, que faire ?
4. Keeper Security - Compte en ligne compromis : De quoi s'agit-il et comment l'éviter ?
5. Silverfort - Three Cyberattacks Where Compromised Service Accounts Played a Key Role
6. Splunk - SIEM: Security Information and Event Management
7. TryHackMe - Introduction to XDR