SYNACKTIV

SYNACKTALK #1

08/04/2021

Lumière sur nos Ninjas

Renaud Dubourguais
COO

Renaud Feil
CEO

Aymeric Palhière
Expert

SYNACKTIV

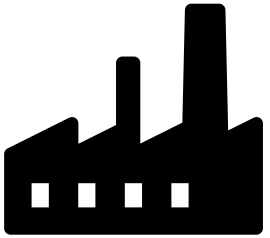
SYNACKTIV

SYNACKTALK #1

« L'évolution de la cybersécurité
ces 10 dernières années »

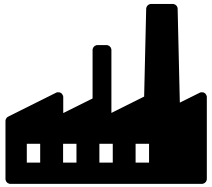
08/04/2021

Retex d’un ancien auditeur



- Auditeur / Pentester pendant 10 ans
  - Evolution de la menace
  - Evolution des environnements clients
  - Evolution et adaptation du métier

200x / La belle époque

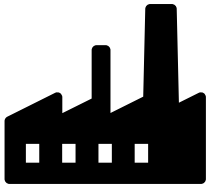


- SI clairement délimité et fermé
- Exposition externe “maîtrisée”
- Focus sur la menace extérieure

- Maturité en cybersécurité en devenir
- Peu de solutions clés en main
- Peu de cadrage réglementaire
- L’humain est laissé de côté

- Audits exclusivement orientés périmètre
- Taux d’intrusion élevé (~90%)
- Vulnérabilités souvent similaires
- La première brèche était suffisante
- Vecteur humain peu pris en compte
- Ticket d’entrée peu coûteux

2010-2015 / Une plus grande maturité

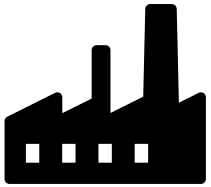


- Meilleure connaissance des sujets
- Cadres réglementaires
- Solutions clés en main
- Mesures internes renforcées

- L'humain reste vulnérable
  - Lancement des sensibilisations
  - Mot de passe, phishing, etc.
- Démocratisation du BYOD

- Méthodologies d'intrusion similaires
- Mais augmentation de la complexité
  - Sécurité par empilement
  - Rebonds et discrétion nécessaires
- Apparition de l'offre Red Team
  - Intégration du vecteur humain
  - Audit orienté assets / objectifs
  - Identification des SPOF

2010-2015 / SaaS, Paas, IaaS

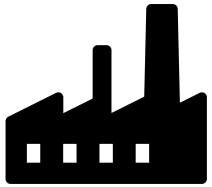


- + en + de solutions SaaS
  - Fonctions business
  - Fonctions de sécurité
  - Délégation à un tiers
- Naissance du PaaS et IaaS

- Eclatement du SI et frontières floues
- Exposition de biens sensibles
- De nouveaux SPOF potentiels
- Quid de la localisation des données

- Périmètres plus difficiles à définir
- Les éditeurs sont désormais acteurs
- Adaptation nécessaire
  - Plus de monde autour de la table
  - Changement des méthodologies
    - Focus sur les applicatifs
    - Interconnexions SaaS
    - Humains

2015-2020 / “on-premise” en option

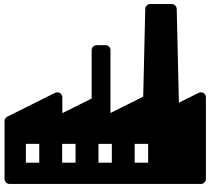


- Migration du SI interne dans le Cloud
  - Mails, applicatifs internes, etc.
- Tous ne suivent pas le mouvement

- “on-premise” devient plus coûteux
- Impression de perte de maîtrise

- Chemin d’intrusion de + en + complexe
- Compromissions “totales” plus rares
- Une hétérogénéité qui croît sans cesse
- Méthodologies rigoureuses nécessaires
- 2 types de profils nécessaires
  - Des spécialistes
  - Des généralistes

Et 2021 ?



- Continuité de la migration Cloud
  - PaaS, IaaS
  - Service d'authentification (Azure AD)
- Challenge de la maîtrise de son SI
- Utilisateur au centre des préoccupations
- Télétravail qui devient la norme
- Décentralisation toujours plus grande

- Le vecteur humain est une priorité
  - Phishing, vol de poste et téléphone
  - Mais renforcements techniques plus fréquents (2e facteur)
- Composants Cloud systématiques
  - ↑ des audits Azure, AWS, GCP
  - Réelle expertise nécessaire
  - La menace s'y intéresse de + en +

SYNACKTIV

SYNACKTALK #1

« Mots de passe
Mythes et réalités »

08/04/2021

Stockage des mots de passe

Clair
Encodage

≠

Chiffrement

≠

Hashage

Pourquoi casser les empreintes ?

- Avancée dans une intrusion
  - Élévation des privilèges sur un composant du SI
  - Rebond sur un autre système ou application
- Le cassage n'est parfois pas nécessaire
  - Mots de passe stockés en clair
  - Encodage (Base64)
  - Faiblesse dans le mécanisme d'authentification

    → Pass-The-Hash

Comment récupérer des empreintes ?

- Vulnérabilités dans une application
  - Injection SQL
- Par écoute réseau passive et active
  - Mise en place d'un Man-In-The-Middle
- Fuites d'information
  - Sauvegardes exposées

Comment casser une empreinte ?

- Calcul d'une empreinte candidat
  - Force brute sur la totalité de l'espace d'un *charset*
  - Dictionnaires régulièrement alimentés
  - Chaînes de Markov
  - Dérivations
  - Combinaisons de mots de dictionnaires
- Comparaison du candidat avec l'empreinte à casser
  - Si empreintes égales → Mot de passe en clair découvert

Comment se protéger ?

- Éviter les fuites d'empreintes
  - Audit des applications manipulant des empreintes
  - Appliquer le principe du moindre privilège
  - Chiffrer les disques pour éviter la récupération hors-ligne
  - Protéger les sauvegardes
- Durcir la politique de mot de passe
- Utilisation d'un 2e facteur
- Utiliser des mécanismes de hashage robustes

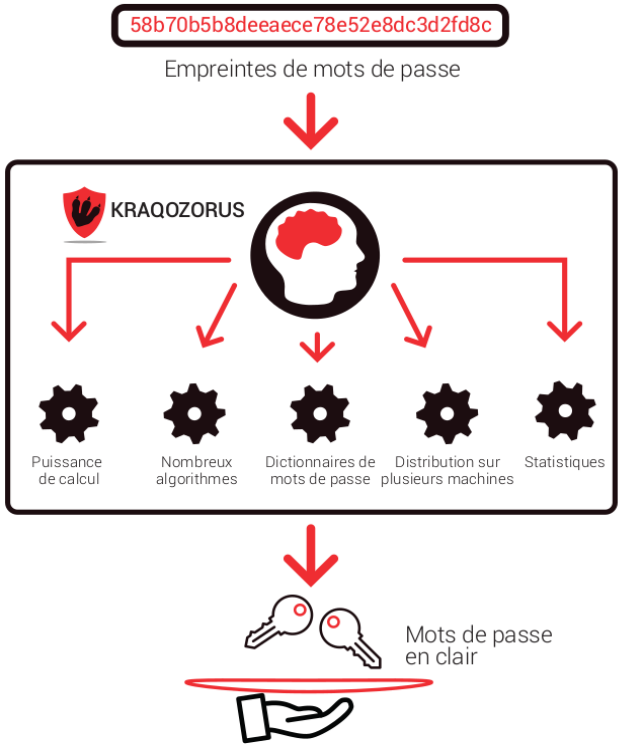
Algorithmes de hashage robustes ?

- Augmentation du temps de calcul nécessaire
  - Invisible à l'échelle d'une empreinte (lors d'une authentification)
  - Très lent à l'échelle de plusieurs milliers (cassage)
- Possible à plusieurs niveaux
  - Dans l'algorithme lui-même (Bcrypt)
  - Dans l'utilisation de l'algorithme (Key Streching)

Le jeu du chat et la souris

- C’est désormais une question de puissance de calcul
  - CPU, GPU, FPGA, ASIC
  - Calcul réparti (utilisation d’une infrastructure multi-noeuds)
- Des outils pour utiliser au mieux les ressources
  - Hashcat
  - John The Ripper

Et chez Synacktiv ?



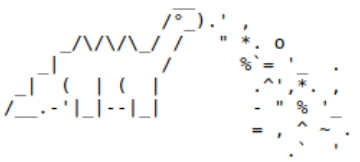
SYNACKTIV

Et chez Synacktiv ?

SYNACKTIV

Et chez Synacktiv ?

Leakozorus



14,256,637,119 entries from 36 dumps
Active DB connections (2/3)

Search: exact email 10000 submit

Or

upload email list: Choose File No file chosen match emails submit

SYNACKTIV

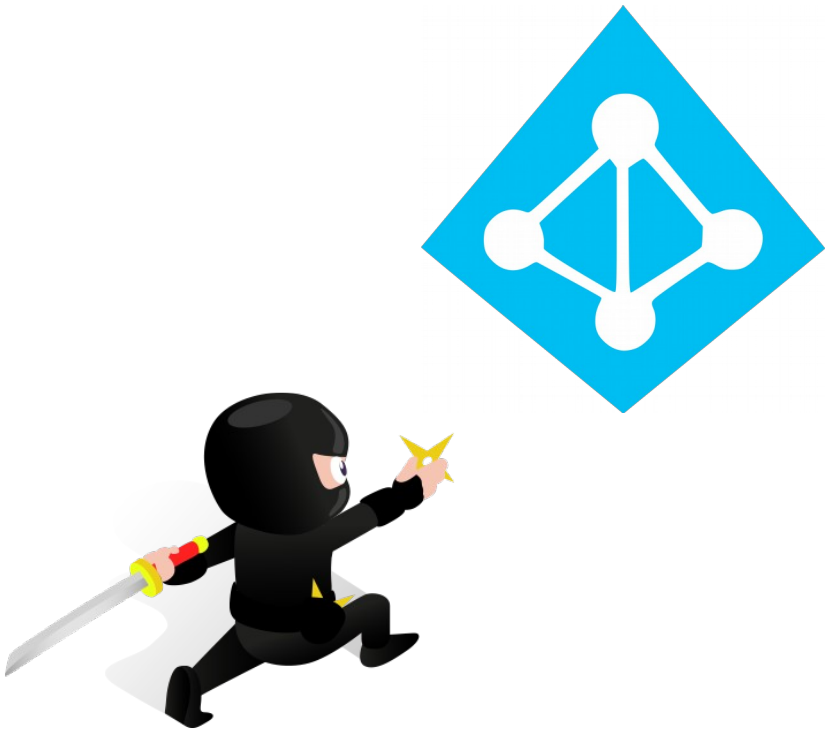
SYNACKTIV

SYNACKTALK #1

« La sécurisation d'Azure AD »

08/04/2021

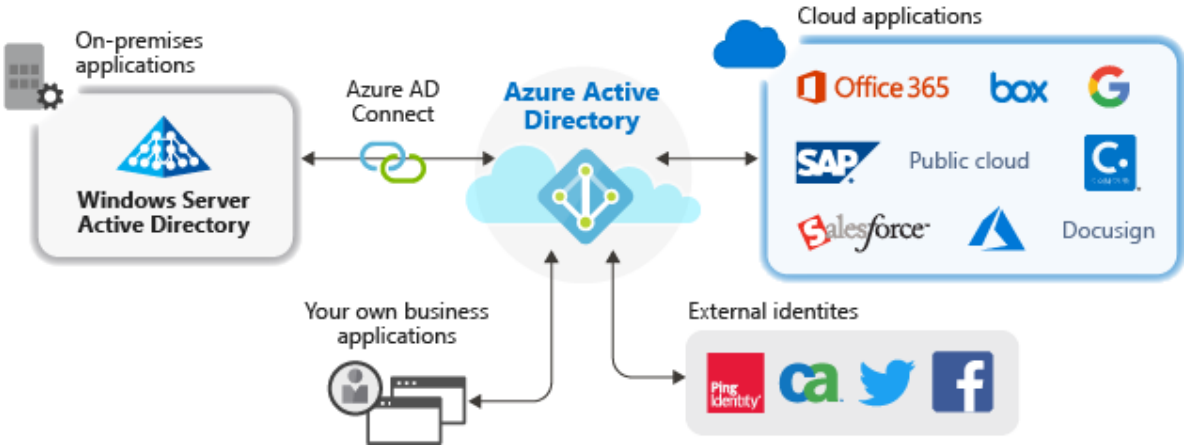
Introduction



- Principes généraux à propos d’Azure AD
- Tour d’horizon des fonctionnalités de sécurité mises à disposition
- Quelques chemins de compromission utilisés lors des tests d’intrusion

Principes généraux

- Solution de gestion des identités et des accès basée sur le cloud Microsoft.
- Permet l'accès aux ressources internes, comme externes, telles que ***Office365*** ou ***Azure RM***.
- Peut être considéré comme un "Active Directory dans le cloud".



https://docs.microsoft.com/en-gb/azure/active-directory/manage-apps/what-is-application-management

Intégration d’AD on-premises

- Unifier la gestion des identités entre Active Directory et le cloud :
  - Synchronisation des mots de passe entre Azure AD et Active Directory
  - Ajouter des fonctionnalités de sécurité aux environnements on-premises
- 3 méthodes de synchronisation disponibles :
  - **Password Hash Synchronization (PHS)**
  - Pass-Through Authentication (PTA)
  - Active Directory Federation Services (ADFS)

Menaces associées

- **Risques inhérents aux infrastructures cloud :**
  - Réutilisation de mots de passe entre les comptes personnels et professionnels
  - Scénario de phishing tout trouvés
  - Cible intéressante du point de vue d'un attaquant
  - Moins de flexibilité dans la réponse à une intrusion
- La compromission d'un compte Azure peut entraîner **la compromission de l'ensemble du SI**.
- Une mauvaise configuration des permissions des utilisateurs peut entraîner une **élévation de privilèges** sur les deux environnements.

  Azure AD est un composant critique du SI et doit être sécurisé en conséquence.

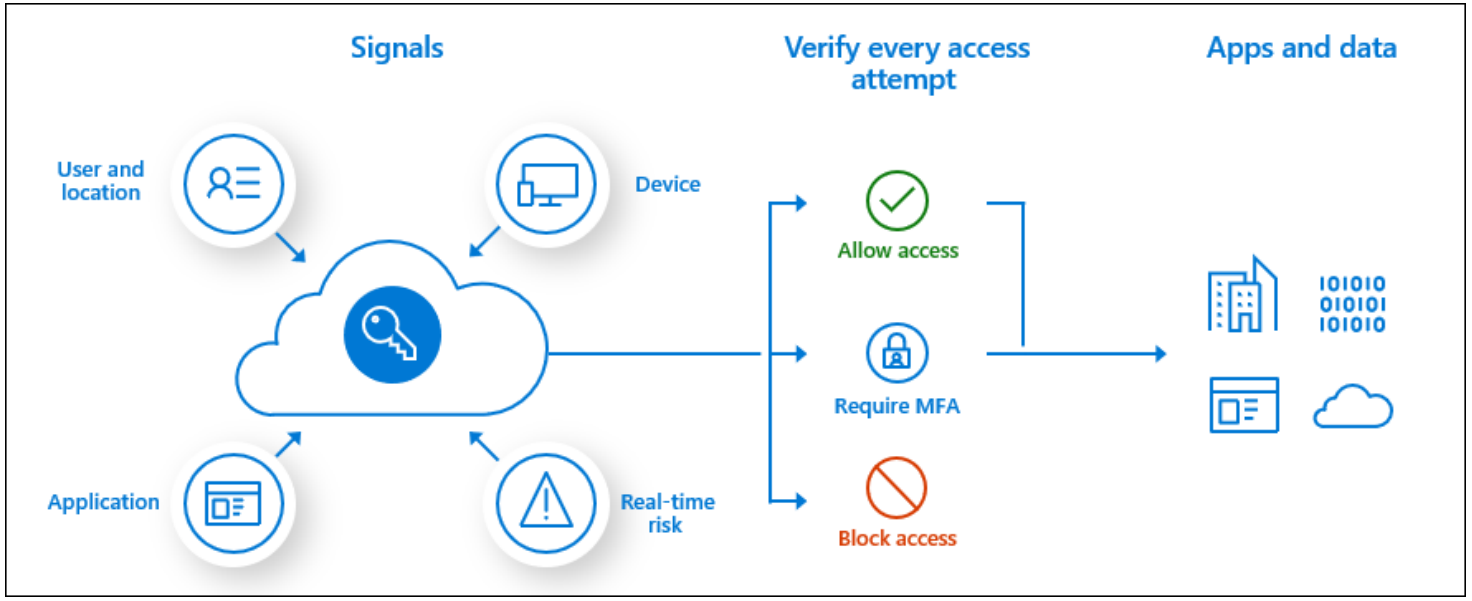
Security Defaults

- Un ensemble de paramètres de sécurité préconfigurés :
  - Exiger que **tous les utilisateurs** paramètrent **l'authentification multi-facteurs Azure AD**
  - Exiger des **administrateurs** qu'ils utilisent une **authentification multi-facteurs**
  - Bloquer les protocoles d'authentification “legacy”
  - Exiger des utilisateurs qu'ils utilisent une authentification multi-facteurs si nécessaire
  - **Protéger les activités privilégiées** comme l'accès au portail Azure

Ensemble de règles génériques et efficaces mais qui ne conviennent pas à tous les environnements. Une granularité plus fine pourrait être approprié, en particulier en ce qui concerne les *politiques d’accès conditionnel*.

Politique d’accès conditionnel

Les politiques d'accès conditionnel sont en quelque sorte des instructions if-then pour autoriser l'accès aux ressources.



https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Authentification multi-facteurs

- **Une fonctionnalité pour les gouverner tous.**
- Automatiquement activée pour tous les utilisateurs via les *Security Defaults.*
- Plusieurs formes de vérification disponibles :
  - Application Microsoft Authenticator
  - Jeton matériel OATH
  - SMS
  - Appel vocal
- Empêche 95%* des attaques possibles sur Azure AD.

* pourcentage abritairement élevé

Password Protection

- Détecte et **bloque les mots de passe faibles connus** et leurs dérivés
- Listes de **mots de passe interdits** enrichies par *Azure AD Identity Protection*
- Possibilité de bloquer certains termes **spécifiques à l'organisation** (ex : le nom de l'entreprise)
- S'applique également aux environnements **on-premises Active Directory**

Identity Protection

Un ensemble d'outils du portail *Azure AD*, aux objectifs suivants:

- Détection des risques basée sur l'identité (password spray, fuites de mots de passe, adresse IP suspecte, etc.)
- Investigations de ces risques
- Transmission des événements à des outils d'analyse tiers (par exemple un SIEM)

La détection des risques est basée sur la connaissance acquise par Microsoft auprès de tous les tenants Azure AD.

Permet la création de ***politiques d'accès conditionnel basées sur les risques***.

Fonctionnalité très intéressante mais coûteuse (nécessite le plan P2 Azure AD premium 9$/utilisateur/mois).

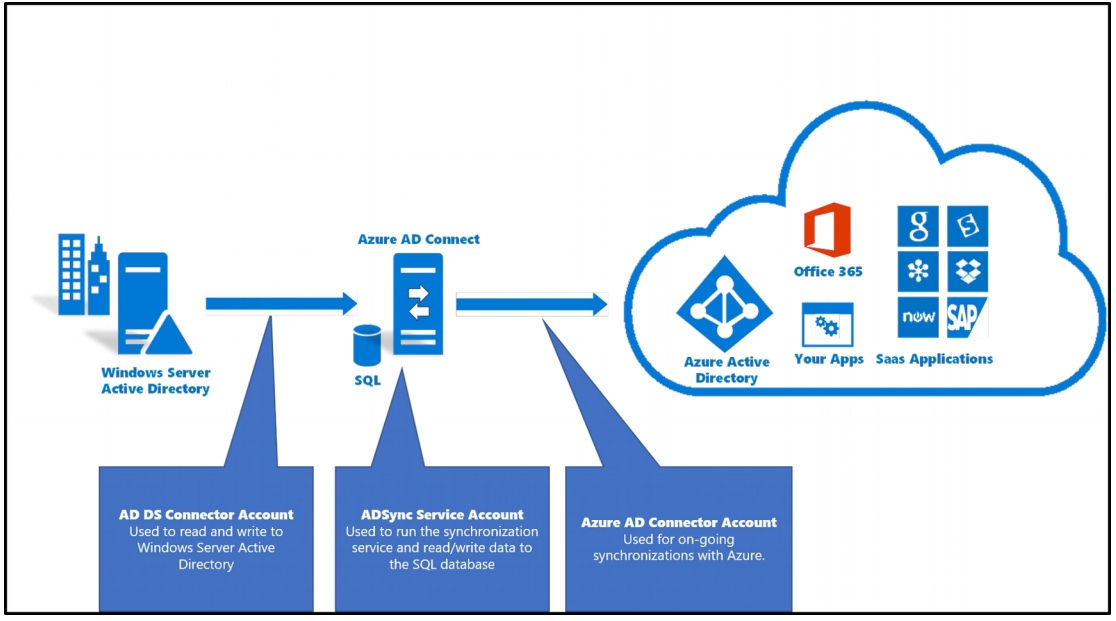
Authentification unique (SSO)

- Les utilisateurs saisissent leur mot de passe une seule fois : `user_experience_and_productivity ++`
- 2 implémentations du mécanisme SSO coexistent :
  - Seamless SSO (Windows 7 et 8.1)
  - SSO PRT (Windows 10)
- **Facile à déployer** pour les administrateurs
- Uniquement supporté par *Microsoft Edge* et *Google Chrome*

Les deux implémentations induisent **des risques de sécurité.**

Azure AD Connect

- Logiciel de synchronisation utilisé pour l'intégration d'Active Directory via PHS.
- Réplique les empreintes de mots de passe des utilisateur dans Azure AD.



https://docs.microsoft.com/fr-fr/azure/active-directory/hybrid/reference-connect-accounts-permissions

Azure AD Connect

- Le compte utilisé pour la réplication des empreintes est (très) privilégié sur le domaine Active Directory
- Une compromission du serveur de synchronisation **menace l'ensemble du domaine**, et éventuellement le tenant Azure AD

```
Le serveur hébergeant Azure AD Connect doit être traité
comme un composant de tier 0, tel que documenté dans le
modèle d’administration en 3 tiers d’Active Directory.
```

Seamless SSO

- Le *Seamless SSO* repose sur le protocole *Kerberos*
- Le compte d'ordinateur *AZUREADSSOACC* est créé lors de sa configuration
- Ce compte a la capacité d'**impersonifier l'identité de n'importe quel utilisateur du domaine** auprès du service HTTP
- Un attaquant obtenant son mot de passe (ou son empreinte) peut se faire passer pour n'importe quel utilisateur sans MFA auprès des applications cloud, à l'aide d'un *Silver Ticket*

SSO Primary Refresh Token

- Se base sur **un cookie JWT** nommé *Primary Refresh Token* (PRT)
- Ce cookie est demandé par l'utilisateur à la connexion et permet d'accéder ensuite aux applications
- Un attaquant capable d'exécuter du code arbitraire sur la machine d'un utilisateur peut **voler ou forger un PRT valide** et l’utiliser...
- … même si le MFA est activé sur le compte de la victime

Conclusion

- La migration de la gestion des identités vers le cloud présente de nombreux avantages :
  - Facile à administrer
  - Meilleure expérience utilisateur
  - Tableau de bord centralisé
  - Etc.
- Cependant, l'élargissement **inhérent de la surface d'attaque** ne doit pas être sous-estimé
- Heureusement, Microsoft propose **d'excellentes fonctionnalités de sécurité**, à condition d'y mettre le prix et de les configurer correctement
- Même ainsi, que se passe-t-il lorsqu'une vulnérabilité est découverte au sein d'Azure AD ?

Références

- https://docs.microsoft.com/en-us/azure/active-directory/
- https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/
- https://blog.xpnsec.com/azuread-connect-for-redteam/
- https://www.synacktiv.com/publications/azure-ad-introduction-for-red-teamers.html

https://www.linkedin.com/company/synacktiv
https://twitter.com/synacktiv
Nos publications sur : https://synacktiv.com