Projet Verdannet : MFA sur AZURE

BTS SIO SISR – 2023 / 2025

Amine Laouar

24/04/2025

1. CONTEXTE

L'entreprise **Verdannet**, implantée à Annecy, compte environ **300 salariés** répartis en plusieurs pôles fonctionnels : **Comptabilité**, **Transport**, **Logistique**, **Ressources humaines** et **Direction**.

Tous les employés utilisent quotidiennement des services en ligne connectés au **cloud Microsoft Azure**, notamment la messagerie professionnelle, Microsoft 365 et des applications métiers internes.

Avec la montée en puissance du télétravail, les connexions à distance sont devenues fréquentes, ce qui a exposé l'entreprise à **un risque accru de cyberattaques**, notamment **des tentatives de hameçonnage et de vol d'identifiants**.

2. PROBLÉMATIQUE

Depuis le début de l'année, **plusieurs alertes de sécurité** ont été enregistrées dans le centre d'administration Microsoft 365 : tentatives de connexion depuis des pays suspects, comptes bloqués pour activités anormales, et signalements d'usurpation d'identité.

La méthode classique d'authentification par mot de passe ne suffit plus. Elle est **facilement contournable** en cas de mot de passe faible ou réutilisé.

3. SOLUTIONS POSSIBLES ENVISAGÉES

Avant de choisir la solution finale, plusieurs méthodes d'authentification forte ont été envisagées pour renforcer la sécurité des connexions aux services Microsoft Azure. Voici un aperçu des trois principales options évaluées :

a) Microsoft Authenticator (Application mobile)

Cette solution repose sur une application mobile développée par Microsoft. L'utilisateur reçoit une notification push à chaque tentative de connexion, qu'il doit approuver depuis son smartphone.

Avantages :

- Facile à déployer.
- Aucune infrastructure matérielle nécessaire.
- Compatible avec Microsoft 365.

Inconvénients :

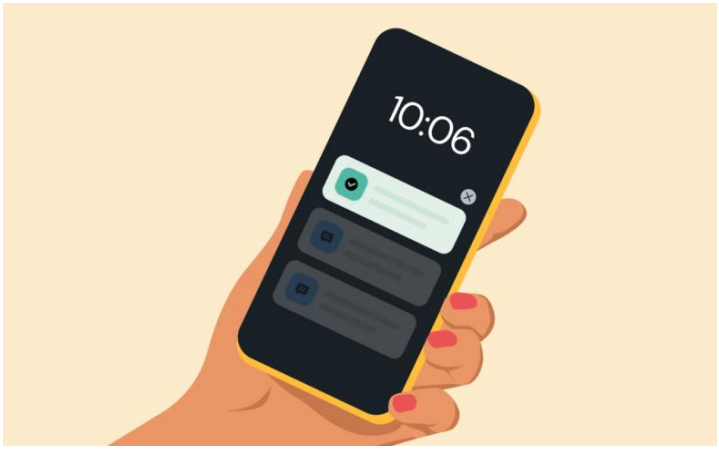
- Dépendance au smartphone et à la connexion internet.
- Risque si le téléphone est compromis ou perdu.

b) Authentification par SMS ou Appel téléphonique

Dans cette méthode, un code est envoyé par SMS ou un appel vocal est émis vers le téléphone de l'utilisateur. Ce code est ensuite saisi pour valider l'identité.

Avantages :

- Simple à comprendre pour les utilisateurs.
- Pas besoin d'installation d'application.



Inconvénients :

- Moins sécurisé (vulnérable au SIM-swapping ou interception).
- Moins fiable à l'étranger ou sans couverture réseau.

c) Clés de sécurité FIDO2 (YubiKey)

Les clés FIDO2 comme la YubiKey offrent une méthode d'authentification matérielle extrêmement sécurisée. Elles nécessitent une interaction physique (connexion USB ou NFC) pour valider l'accès.

Avantages :

- Très haut niveau de sécurité (résistance au phishing et aux attaques à distance).
- Aucune donnée ne transite par internet ou réseau mobile.

Inconvénients :

- Coût d'acquisition des clés.
- Nécessite une gestion logistique pour leur distribution et remplacement.

3. SOLUTIONS MISES EN ŒUVRE

a) Choix de la technologie

- **YubiKey** est une clé de sécurité physique compatible avec Azure Active Directory.
- Elle prend en charge le protocole **FIDO2**, un standard ouvert et sécurisé.
- Elle est **pratiquement impossible à dupliquer** ou à pirater à distance.

b) Organisation de la distribution

- Chaque département reçoit un lot de YubiKey :
    - **Comptabilité** : 40 clés
    - **Transport** : 90 clés
    - **Logistique** : 80 clés
    - **RH :** 30 clés
    - **Direction et IT** : 60 clés
- Les clés sont affectées à des groupes d'utilisateurs dans Azure AD.

c) Configuration sur Microsoft Azure

- Accès au **portail Azure Active Directory > Sécurité > Méthodes d'authentification** ;
- Activation de **FIDO2 Security Key** comme méthode autorisée ;
- Déploiement d'une **politique conditionnelle** pour exiger 2FA sur toutes les connexions hors réseau interne ;

- Attribution des **groupes de sécurité** correspondant aux différents services.

d) Procédure utilisateur

- L'utilisateur branche la **YubiKey** dans le port USB ou utilise NFC (selon modèle) ;
- Lors de la connexion à Microsoft 365, il entre son identifiant, puis active la clé ;
- Sans la clé, la connexion est refusée, même avec le bon mot de passe.

4. RÉSULTATS

- **Taux de réussite de connexion sécurisé : 100%** après le déploiement ;
- **Aucune tentative de piratage réussie** depuis la mise en place du dispositif ;
- **Satisfaction des utilisateurs** après une courte formation (prise en main simple) ;
- La direction dispose désormais d'une **vision claire de l'usage des clés** via les logs Azure ;
- **Renforcement de la conformité** RGPD et des bonnes pratiques de cybersécurité.

➤ CONCLUSION

La mise en place de **l'authentification multifacteur** chez **Verdannet** a permis de renforcer efficacement la sécurité des accès aux utilisateurs. Après avoir comparé plusieurs solutions, l'entreprise a fait le choix des clés de sécurité FIDO2, une méthode fiable et difficile à pirater.

Cette solution a permis de réduire les risques de piratage, tout en restant simple d'utilisation pour les employés. Le déploiement s'est fait progressivement par service, avec une bonne prise en main grâce à une courte formation.

Ce projet marque une étape importante pour **Verdannet** dans la protection de ses données et montre l'importance de mettre en place des outils modernes pour faire face aux menaces actuelles.