Microsoft 365

Diagnostic de configuration sécurité

Advens
Security for the greater good

Nous existons pour vous protéger des menaces Cyber.

Advens est un leader européen de la Cybersécurité, indépendant et souverain.

Nos 500 experts forment un collectif engagé et solidaire, présents partout en France (Paris, Lille, Lyon, Toulouse, Bordeaux, Nantes et Rennes), ainsi qu'à Madrid, Barcelone, Montréal et Papeete

Notre mission : protéger les organisations publiques et privées, toujours plus dépendantes du numérique et toujours plus exposées à des attaquants nombreux et professionnels.

Objectif

.Évaluer votre niveau de risque au travers d'un diagnostic de configuration sécurité Microsoft 365 :

.Est-ce que mon tenant est à risque ?

.Est-ce que la configuration actuelle des services souscrits me protège contre les fuites de données , les compromissions de comptes, etc ?

Les risques en quelques chiffres

+10%

de compromissions de comptes

Les cyberattaques observées par Microsoft liées à des États-nations sont de plus en plus efficaces, passant d'un taux de compromission réussie de 21 % en 2020 à un taux de 32 % en 2021.

50 M

d'attaques sur les mots de passe par jour

Malgré ce constat, seuls 20% des utilisateurs et 30% des Global Administrator ont activé l'authentification forte

Cible ?

Tous les secteurs d'activité sont touchés

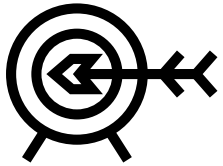
Advens a pu constater au travers de ses nombreux diagnostics que les principaux risques sont :

Les accès non contrôlés

Une maîtrise partielle des données

Un service de messagerie vulnérable

Pourquoi faire un diagnostic ?



Une cible privilégiée

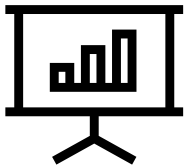
Microsoft 365 est le service SaaS le plus utilisé d'Europe.

La pandémie Covid19 a accéléré fortement son implémentation. Il est donc également de plus en plus pris pour cible.

Configuration par défaut

Ce service est livré avec des configurations par défaut qui permettent un fonctionnement immédiat des solutions.

Mais en contrepartie il est nécessaire d'effectuer un travail de paramétrage et de contextualisation pour éviter la surexposition.

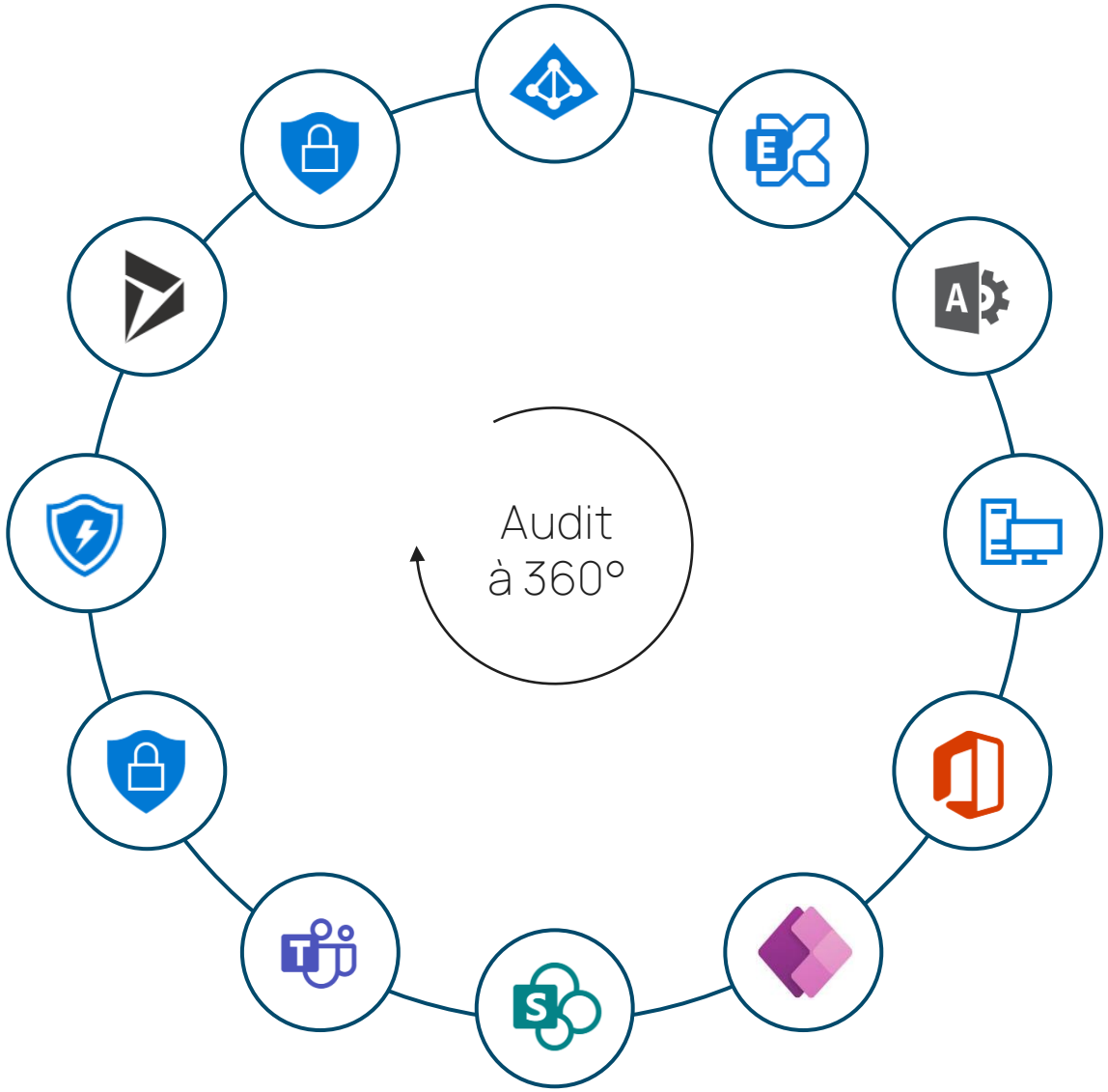


Evolution rapide

Microsoft 365 voit ses services évoluer très rapidement.

Les interfaces d'administration changent régulièrement, ce qui rend difficiles le maintien en condition opérationnelle et l'appréciation des impacts de ces changements.

L’approche d’ADVENS : un diagnostic complet



Diagnostic de configuration

Vérification du paramétrage de tous les composants du tenant Microsoft 365.

Diagnostic Organisationnel

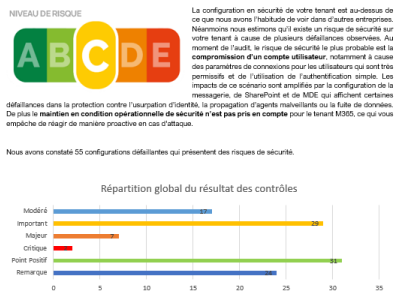
Vérification de la mise en place de l’organisation et des processus nécessaires à la supervision des menaces et à leurs traitements

Composition du diagnostic Microsoft 365

Le diagnostic est composé de 140 points de contrôle issu du CIS, de l'expertise de Advens et de la cartographie des risques du CLUSIF.

Le rapport final constitue le principal livrable de la prestation et comprend une synthèse des chantiers de remédiation.

Synthèse globale



II. Synthèse managériale

NIVEAU DE RISQUE

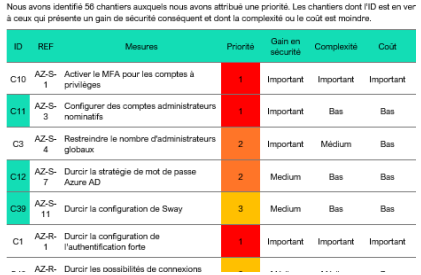
A B C D E

La configuration en sécurité de votre tenant est au-dessus de ce que nous avons l'habitude de voir dans d'autres entreprises. Néanmoins nous estimons qu'il existe un risque de sécurité sur votre tenant à cause de plusieurs défaillances observées. Au moment de l'audit, le risque de sécurité le plus probable est la **compromission d'un compte utilisateur**, notamment à cause des paramètres de connexions pour les utilisateurs qui sont très permissifs et de l'utilisation de l'authentification simple. Les impacts de ce scénario sont amplifiés par la configuration de la messagerie, de SharePoint et de MDE qui affichent certaines défaillances dans la protection contre l'usurpation d'identité, la propagation d'agents malveillants ou la fuite de données. De plus le **maintien en condition opérationnelle de sécurité n'est pas pris en compte** pour le tenant M365, ce qui vous empêche de réagir de manière proactive en cas d'attaque.

Nous avons constaté 55 configurations défaillantes qui présentent des risques de sécurité.

Répartition global du résultat des contrôles

Synthèse des actions



IV. Synthèse des mesures correctives

Nous avons identifié 56 chantiers auxquels nous avons attribué une priorité. Les chantiers dont l'ID est en ver à ceux qui présente un gain de sécurité conséquent et dont la complexité ou le coût est moindre.

ID	REF	Mesures	Priorité	Gain en sécurité	Complexité	Coût
C10	AZ-S-1	Activer le MFA pour les comptes à privilèges	1	Important	Important	Important
C11	AZ-S-3	Configurer des comptes administrateurs nominatifs	1	Important	Bas	Bas
C3	AZ-S-4	Restreindre le nombre d'administrateurs globaux	2	Important	Médium	Bas
C12	AZ-S-7	Durcir la stratégie de mot de passe Azure AD	2	Medium	Bas	Bas
C39	AZ-S-11	Durcir la configuration de Sway	3	Medium	Bas	Bas
C1	AZ-R-1	Durcir la configuration de l'authentification forte	1	Important	Important	Important
	AZ-R-	Durcir les possibilités de connexions				

Constats détaillés

V.1.2.12 Restriction géographique

Objectif du contrôle : S'assurer que l'accès par restriction géographique est en place

Description : le modèle SaaS permet la connexion au service de Microsoft depuis n'importe où sur la planète. Les connexions frauduleuses par compromission de compte sont un des facteurs de risque principal dans ce modèle. Un des moyens de réduire la probabilité de ce risque est de restreindre l'accès au service à des pays ou IP spécifiques.

Preuve de contrôle : NA

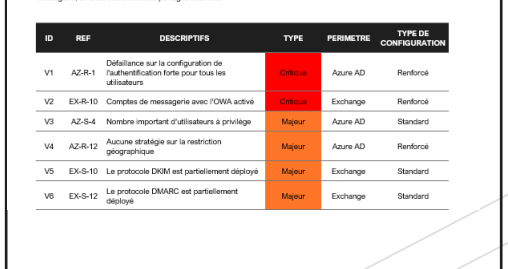
Vulnérabilité V4	Aucune stratégie sur la restriction géographique
MAJEUR	Nous avons constaté que vous ne disposiez d'aucune stratégie restreignant l'accès géographiquement. À travers les nombreux audits qu'Advens a réalisés, nous avons constaté que les tenants Microsoft 365 sont souvent pris pour cible. Mettre en place une politique d'accès conditionnel sur les pays où vous avez l'habitude de travailler permet de diminuer votre surface attaque de limiter les attaques courantes venant des pays dits « à risque » (Asie, Russie, Amérique du Sud, etc)
	Risque associé : RS01 / RA03
Chantier C4	Mettre en place une politique d'accès conditionnelle sur la restriction géographique

Nous vous recommandons de mettre en place une stratégie d'accès conditionnel pour autoriser les connexions au tenant dans les pays avec lesquels vous avez l'habitude de travailler.

- Fonctionner par liste blanche plutôt que liste noire
- Vous pouvez augmenter le durcissement en autorisant uniquement vos IP de sorties. Si cette solution offre une protection très intéressante, elle peut également provoquer un goulot d'étranglement réseau qui ralentit vos communications. N'utilisez cette option que si vous avez une infrastructure réseau en capacité de tenir la charge.

Nous sommes conscients que cette restriction peut avoir des impacts pour les utilisateurs, surtout lors de déplacement exceptionnel ou en période de congés. Mais la solution forcera l'utilisation du VPN d'entreprise qui permettra de sortir sur un pays autorisé ou une IP autorisée.

Vulnérabilités



III.1 Synthèse technique

Les chantiers les plus importants concernent le durcissement de l'Azure AD, des connexions, le durcissement de la messagerie, et le durcissement des partages externes.

ID	REF	DESCRIPTIFS	TYPE	PERIMETRE	TYPE DE CONFIGURATION
V1	AZ-R-1	Défaillance sur la configuration de l'authentification forte pour tous les utilisateurs	Critique	Azure AD	Renforcé
V2	EX-R-10	Comptes de messagerie avec l'OWA activé	Critique	Exchange	Renforcé
V3	AZ-S-4	Nombre important d'utilisateurs à privilège	Majeur	Azure AD	Standard
V4	AZ-R-12	Aucune stratégie sur la restriction géographique	Majeur	Azure AD	Renforcé
V5	EX-S-10	Le protocole DKIM est partiellement déployé	Majeur	Exchange	Standard
V6	EX-S-12	Le protocole DMARC est partiellement déployé	Majeur	Exchange	Standard

Pourquoi choisir Advens ?

Solution Partner - Sécurité

Advens est Solution Partner de Microsoft depuis 2023 sur l'aspect Sécurité.

Ce partenariat garantit son expertise des technologies Microsoft et permet un lien privilégié dans l'accès aux ressources, formations et nouveautés des solutions Microsoft Cloud.

Collaborateurs certifiés

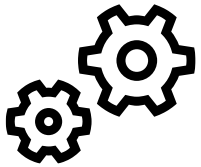
Advens dispose nombreux collaborateurs certifiés sur les produits de sécurité de Microsoft : SC-200, SC-300, SC-400, MS-500 et AZ-500…

Vision globale des environnements Microsoft

Advens intervient sur de nombreuses prestations de sécurité autour des environnements Microsoft.

Exemples : mise en place du MFA, remédiation d'un tenant, formation sur l'investigation d'événement de sécurité, sensibilisation, sécurité des données, durcissement de la PowerPlateform, etc….

Cadre de la prestation



Prérequis et limites

Compte administrateur général Microsoft 365
(un compte « global reader » n'est pas suffisant)

Prestation 100% à distance

Offre valable pour un tenant

Aucune limite sur le nombre d'utilisateurs

Planification

Semaine 1 : Lancement

Semaines 1 à 2 : atelier d'échange, diagnostic et rapport

Fin semaine 2 / semaine 3 : Restitution

Livrable

Compte rendu d'entretien

Rapport de diagnostic

Support de restitution

Wavens

Security for the greater good

Paris Lille Lyon Bordeaux Nantes Rennes Toulouse Montréal Madrid Barcelone Papeete