IT1 ICT-audit Light
Geconsolideerd overzicht
Cloudsecurity

VERTROUWELIJKHEIDSLCLAUSULE

Scandatum: 08/03/2023

Opgesteld voor: KLANTNAAM

Opgesteld door: IT1 bv

2021/02/03

Inhoudsopgave

1 - Overzicht

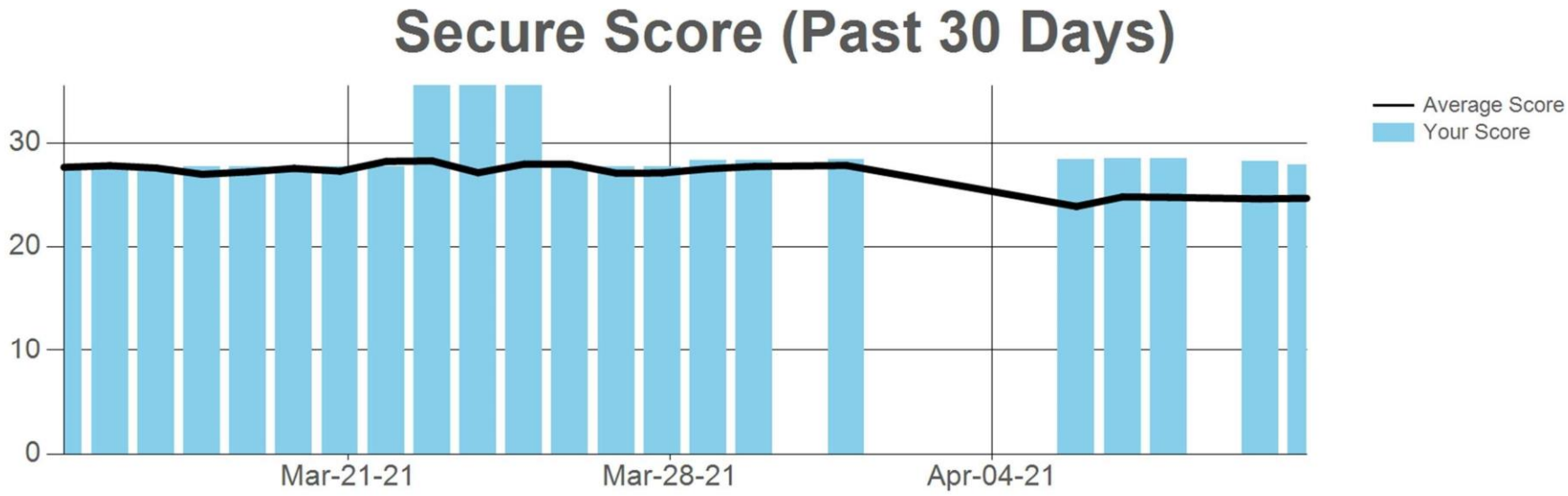
Dit rapport geeft een geconsolideerd beeld van de beveiliging van de Microsoft Cloud-omgeving. De beoordeling bestaat uit een overzicht van uw huidige Microsoft Secure Score en toont trends in de tijd. De Microsoft Secure Score is een eigen beveiligingsscore van Microsoft. Het is een optelsom van scores die worden verkregen door het implementeren van verschillende beveiligingscontroles en best practices. De score is een relatieve maatstaf en hoewel er een theoretisch maximum is, is het niet altijd mogelijk of wenselijk voor het bedrijf om de maximaal mogelijke score te behalen. In dit rapport worden de verschillende Microsoft Controls en hun bijbehorende Control Scores verder uitgesplitst. Een opgeleide IT-professional moet de controles beoordelen en helpen bij het identificeren en prioriteren van de controles die moeten worden uitgevoerd. Het laatste aspect van deze beveiligingsbeoordeling is een beoordeling van waarschuwingen die onlangs zijn opgetreden.

2 - Huidige veiligheidsscore

Dit is uw huidige Microsoft-beveiligingsscore. Het spectrum is gecentreerd rond de gemiddelde score van uw referentiegroep. Ook al lijkt uw score aan de maximale kant van het spectrum te staan, het is mogelijk dat deze niet aan de theoretische max ligt. Het theoretische maximum verandert op basis van het aantal gebruikers, apparaten, groepen en abonnementen. Uw huidige theoretische maximum is 59.

3 - Veiligheidsscore Trend

De volgende grafiek toont veranderingen in uw Veilige Score in de loop der tijd. Het toont ook de gemiddelde score van uw peer group als referentie. De Secure Score moet worden gebruikt als een relatieve maatstaf voor beveiliging. Een gekwalificeerde IT-professional kan beoordelen en prioriteren welke beveiligingsmaatregelen geschikt zijn voor uw organisatie.



4 - Controle Scores

Het implementeren van best practice controles kan resulteren in een veiligere omgeving. Microsoft kent een controlescore toe op basis van de voortgang van de organisatie bij het implementeren van deze maatregelen. Hieronder vindt u een tabel met de afzonderlijke controles en uw specifieke scores. Scores van 0 geven controles aan die moeten worden geëvalueerd en indien mogelijk geïmplementeerd.

CONTROLENAAM	BESCHRIJVING	SCORE
app		
TLSDeprecatie	Controleer al uw clients om na te gaan welke TLS 1.0/1.1 en 3DES gebruiken om met Office 365 te communiceren. Het doel is om uw clients te upgraden om af te stappen van het gebruik van zwakkere protocollen en versleuteling. U kunt een rapport opvragen met alle TLS 1.0/1.1 en 3DES verbindingen in uw tenants gegroepeerd per gebruiker en agent informatie. Nadat al uw clients zijn gemigreerd en het gebruik hieronder nul is, krijgt u volledige punten.	1
CustomerLockBoxEnabled	Het inschakelen van de klant lockbox functie vereist dat er goedkeuring wordt verkregen voor datacenter operaties die een Microsoft medewerker directe toegang tot uw inhoud geeft. Toegang kan nodig zijn voor Microsoft support engineers als zich een probleem voordoet. Er zit een vervaltijd op het verzoek en de toegang tot de inhoud wordt verwijderd nadat de supportmedewerker het probleem heeft opgelost.	0
App		
vergadering_restrictanonymousjoin_v1	Door anonieme gebruikers te beperken tot deelname aan Microsoft Teams-vergaderingen, hebt u volledige controle over de toegang tot vergaderingen. Anonieme gebruikers zijn mogelijk niet van uw organisatie en zouden zich voor kwaadaardige doeleinden kunnen aanmelden, zoals het verkrijgen van informatie over uw organisatie via gesprekken.	0
identitei		
AdminMFAV2	Het vereisen van multi-factor authenticatie (MFA) voor alle administratieve rollen maakt het moeilijker voor aanvallers om toegang te krijgen tot accounts. Administratieve rollen hebben hogere rechten dan gewone gebruikers. Als een van deze accounts in gevaar komt, kunnen kritieke apparaten en gegevens worden aangevallen.	10
PWAgePolicyNew	Onderzoek heeft uitgewezen dat wanneer periodieke wachtwoordresets worden afgedwongen, wachtwoorden minder veilig worden. Gebruikers hebben de neiging een zwakker wachtwoord te kiezen en dit bij elke reset enigszins te variëren. Als een gebruiker een sterk wachtwoord aanmaakt (lang, complex en zonder pragmatische woorden) moet het in de toekomst net zo sterk blijven als nu. Het is het officiële beveiligingsstandpunt van Microsoft om wachtwoorden niet periodiek te laten verlopen zonder een specifieke reden, en adviseert cloud-only huurders het wachtwoordbeleid in te stellen op nooit verlopen.	8

CONTROLENAAM	BESCHRIJVING	SCORE
MFARegistratieV2	Multi-factor authenticatie (MFA) helpt apparaten en gegevens te beschermen die toegankelijk zijn voor deze gebruikers. Het toevoegen van meer verificatiemethoden, zoals de Microsoft Authenticator-app of een telefoonnummer, verhoogt het beschermingsniveau als één factor wordt gecompromitteerd.	6.75
OneAdmin	Het hebben van meer dan één globale beheerder helpt als u niet in staat bent om aan de behoeften of verplichtingen van uw organisatie te voldoen. Het is belangrijk om een gedelegeerde of een noodaccount te hebben waar iemand van uw team zo nodig toegang toe heeft. Het geeft beheerders ook de mogelijkheid om elkaar te controleren op tekenen van een inbreuk.	1
BlockLegacyAuthentication	Tegenwoordig zijn de meeste compromitterende aanmeldingspogingen afkomstig van verouderde verificatie. Oudere kantoorclients zoals Office 2010 ondersteunt geen moderne verificatie en gebruikt verouderde protocollen zoals IMAP, SMTP en POP3. Legacy-verificatie ondersteunt geen multifactorauthenticatie (MFA). Zelfs als in uw omgeving een MFA-beleid is geconfigureerd, kunnen kwaadwillenden deze afdwinging omzeilen via verouderde protocollen.	0.2
IntegratedApps	Scherp de beveiliging van uw diensten aan door de toegang van geïntegreerde apps van derden te reguleren. Geef alleen toegang tot noodzakelijke apps die robuuste beveiligingscontroles ondersteunen. Toepassingen van derden zijn niet gemaakt door Microsoft, dus de kans bestaat dat ze worden gebruikt voor kwaadaardige doeleinden, zoals het exfiltreren van gegevens uit uw huurwoning. Aanvallers kunnen via deze geïntegreerde apps blijvende toegang tot uw diensten behouden, zonder te vertrouwen op gecompromitteerde accounts.	0
SelfServicePasswordReset	Met self-service password reset in Azure Active Directory hoeven gebruikers niet langer de helpdesk in te schakelen om wachtwoorden te resetten. Deze functie werkt goed met Azure AD dynamisch verboden wachtwoorden, die voorkomen dat gemakkelijk te raden wachtwoorden worden gebruikt.	0
UserRiskPolicy	Als het gebruikersrisicobeleid is ingeschakeld, detecteert Azure Active Directory de waarschijnlijkheid dat een gebruikersaccount gecompromitteerd is. Als beheerder kunt u een voorwaardelijk toegangsbeleid configureren om automatisch te reageren op een specifiek risiconiveau van een gebruiker. U kunt bijvoorbeeld de toegang tot uw bronnen blokkeren of een wachtwoordwijziging eisen om een gebruikersaccount weer in een schone staat te brengen.	0
Identiteit		
RoleOverlap	Beperkte beheerders zijn gebruikers die meer rechten hebben dan standaardgebruikers, maar niet zoveel rechten als globale beheerders. Door gebruik te maken van beperkte beheerdersrollen voor het uitvoeren van vereiste administratieve werkzaamheden, vermindert u het aantal houders van rollen met een hoge waarde en een grote impact als Global Administrator. Door gebruikers rollen toe te wijzen als wachtwoordbeheerder of Exchange Online Administrator, in plaats van Global Administrator, verkleint u de kans dat een bevoorrechte account van de Global Administrator wordt geschonden.	1
SigninRiskPolicy	Het inschakelen van het sign-in risk beleid zorgt ervoor dat verdachte sign-ins worden uitgedaagd voor multi-factor authenticatie (MFA).	0

5 - Waarschuwingsanalyse

EVENEMENTDATUM	TITEL
2020/05/20 11:45:00 AM -04:00	E-mail door gebruiker gemeld als malware of phish
2020/05/20 9:15:00 AM -04:00	E-mail door gebruiker gemeld als malware of phish
2020/05/19 7:15:00 PM -04:00	Gebruiker mag geen e-mail versturen
2020/05/19 4:30:00 PM -04:00	Verdachte e-mail verzendpatronen gedetecteerd
2020/05/19 3:30:00 PM -04:00	Verdachte e-mail verzendpatronen gedetecteerd
2020/05/19 3:00:00 PM -04:00	E-mail door gebruiker gemeld als malware of phish
2020/05/19 2:00:00 PM -04:00	Verdachte e-mail verzendpatronen gedetecteerd
2020/05/19 11:45:00 AM -04:00	Creatie van een doorstuur-/omleidingsregel
2020/05/19 9:15:00 AM -04:00	Verdachte e-mailverzendpatronen gedetecteerd

2020/05/19 9:00:00 AM -04:00	Creatie van een doorstuur-/omleidingsregel
2020/05/18 5:00:00 PM -04:00	Verdachte e-mailverzendpatronen gedetecteerd
2020/05/18 12:45:00 PM -04:00	Creatie van een doorstuur-/omleidingsregel
2020/05/18 9:30:00 AM -04:00	Creatie van een doorstuur-/omleidingsregel
2020/05/17 11:45:00 AM -04:00	Gebruikers doelwit van phish-campagnes

EVENEMENTDATUM	TITEL
2020/05/15 11:45:00 PM -04:00	Gebruikers doelwit van phish-campagnes
2020/05/15 11:45:00 PM -04:00	Gebruikers doelwit van malwarecampagnes
2020/05/15 6:15:00 PM -04:00	Verdachte e-mailverzendpatronen gedetecteerd
2020/05/15 2:59:00 PM -04:00	Creatie van een doorstuur-/omleidingsregel
2020/05/15 11:15:00 AM -04:00	Verdachte e-mailverzendpatronen gedetecteerd
2020/05/15 12:00:00 AM -04:00	Gebruikers doelwit van phish-campagnes