

High level Design (HLD) - KyK scholen

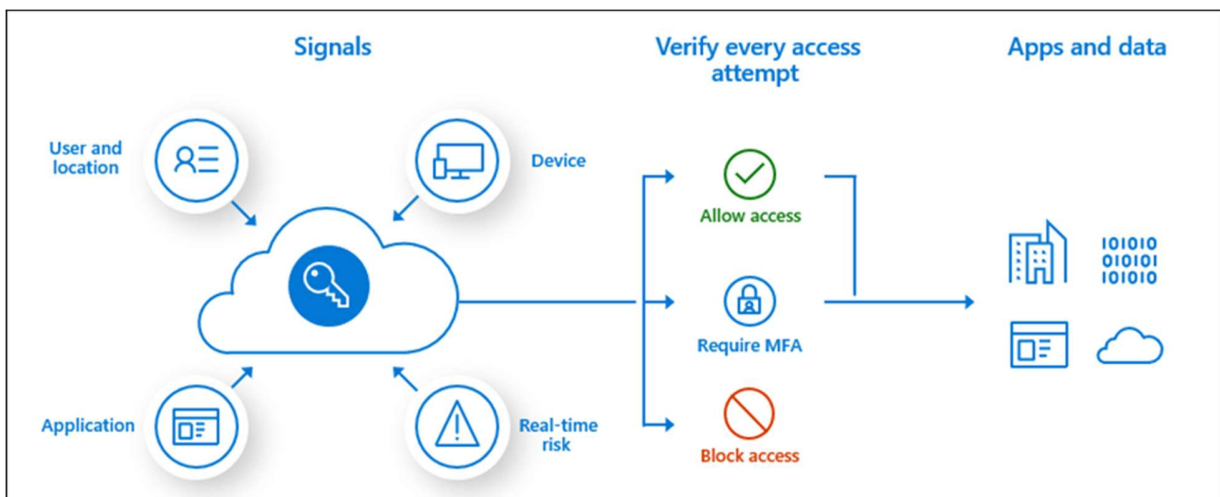
Bijlage 7 bij aanbesteding ICT beheersdiensten

Inhoudsopgave

INHOUDSOPGAVE	1
IDENTITEITEN EN TOEGANGSBEHEER	2
ONTWERPBESLUITEN	2
WINDOWS INSCHRIJVING	6
ONTWERPBESLUITEN	7
WINDOWS CONFIGURATIE	9
ONTWERPBESLUITEN	9
WINDOWS UPDATE	15
ONTWERPBESLUITEN	15
WINDOWS BEVEILIGING	17
ONTWERPBESLUITEN	17
TABLETS EN SMARTPHONES	20
ONTWERPBESLUITEN	21

Identiteiten en toegangsbeheer

In dit hoofdstuk gaan we in op de fundamentele rol die identiteits- en toegangsbeheer spelen binnen de ambitie van KyK om een omgeving te creëren die goed beveiligd is. Centraal staat het belang van een doeltreffend beheer van identiteiten en toegang, wat de basis vormt van KyK's veiligheidsstrategie. Met de keuze voor Microsoft 365 en het gebruik van de Identity provider Microsoft Entra ID, heeft KyK een solide basis gelegd om moderne beveiligingstechnieken te omarmen. Een cruciaal aspect van dit alles is het nauwkeurig stellen van voorwaarden voor toegang tot de omgeving. Door deze voorwaarden zorgvuldig af te stemmen op de specifieke behoeften en risico's van KyK, wordt een robuuste verdedigingslinie opgebouwd tegen potentiële bedreigingen en ongeautoriseerde toegang. Dit hoofdstuk verkent de strategische beslissingen die KyK heeft genomen om deze doelstellingen te bereiken en werpt een licht op de operationele en technische aspecten van het identiteits- en toegangsbeheer binnen de organisatie.



Ontwerpbesluiten

Ontwerpbesluit
Microsoft Entra ID is de te gebruiken Identity Provider.
Motivatatie
Door Entra ID als primaire authenticatie bron in te zetten kan gebruik worden gemaakt van de beveiligingsmogelijkheden van Azure.

Ontwerpbesluit
Koppelingen naar externe applicaties, zoals Single Sign-On (SSO), mogen alleen geconfigureerd worden door een administrator.
Motivatatie
Beperking van de configuratie van externe applicatiekoppelingen tot administrators verhoogt de controle over de toegang en beveiliging van gegevens.

Ontwerpbesluit

Alle niet Microsoft applicaties die worden afgenomen als SAAS applicatie dienen bij voorkeur gebruik te kunnen maken van Entra ID voor applicatie authenticatie (SAML /Oauth)

Motivatie

Hierdoor kunnen gebruikers met het zelfde account authenticeren bij SAAS applicaties. Dit is de meest gebruiksvriendelijke manier maar is niet altijd mogelijk.

Ontwerpbesluit

De Microsoft 365 omgeving wordt voorzien van een herkenbare huisstijl.

Motivatie

Door een consistente huisstijl toe te passen binnen de Microsoft 365-omgeving creëren we een uniforme en professionele uitstraling.

Ontwerpbesluit

Het verlopen van wachtwoorden is uitgeschakeld.

Motivatie

Het uitschakelen van het wachtwoordverloop vermindert de gebruikersfrustratie en bevordert een betere gebruikerservaring zonder afbreuk te doen aan de beveiliging. Moderne beveiligingspraktijken richten zich meer op sterke wachtwoorden en het monitoren van verdachte activiteiten in plaats van periodieke wachtwoordwijzigingen.

Ontwerpbesluit

Gebruikers dienen bij elke inlogpoging een MFA challenge te doorlopen. Dit is uitgezonderd voor het noodaccount en leerlingen. Op beheerde Windows apparaten zal dit met Windows Hello gedaan worden. Anders wordt het met behulp van de Microsoft Authenticator App gedaan. Ook is het mogelijk om FIDO2-securitykeys te gebruiken voor MFA. Sessies kunnen maximaal twee weken blijven, zodat er om de twee weken altijd opnieuw geauthentiseerd wordt. Serviceaccounts en het noodaccount worden uitgesloten van deze regel.

Motivatie

Deze regel dient als baseline van de omgeving, en geldt dus voor alle type gebruikers. Er wordt gekozen voor MFA methodes die bestand zijn tegen phishing aanvallen en een sessie tijd van 2 weken is gekozen uit balans tussen veiligheid en gebruiksgemak.

Ontwerpbesluit

Er zijn binnen de omgeving gebruikers accounts die gedeeld worden. Dit zijn namelijk accounts die gebruikt worden voor invallers. Deze accounts dienen ook te authenticeren met MFA, hiervoor komt voor elk inval account een FIDO2 security key. Daarnaast is toegang tot de omgeving met deze accounts alleen mogelijk vanuit een school locatie.

Motivatie

Omdat de andere MFA methodes allemaal persoons gebonden zijn moeten we een methode ondersteunen die het overdraagbaar maakt, hierbij is een FIDO2 key de veiligste methode. Omdat het delen van accounts risico met zich mee brengt is toegang tot de omgeving alleen mogelijk vanuit een KyK school locatie.

Ontwerpbesluit
Gebruikers met een beheerder rol toegewezen dienen bij elke inlogpoging een MFA Challenge te doorlopen, met uitzondering van noodaccounts. De sessietijd is verkort naar 4 uur en toegang is alleen mogelijk vanuit Nederland.
Motivatie
Account met beheer rollen toegewezen hebben dus meer mogelijkheden in de omgeving en dienen dus te worden voorzien van een sterke beveiliging. De sessie tijd verkorten is van belang om het risico op sessies overnemen door een kwaadwillende te beperken.

Ontwerpbesluit
Binnen KyK wordt Windows Hello en de Microsoft Authenticator-app gebruikt als methoden voor Multi-Factor Authentication (MFA). Deze methoden worden ook ingezet voor Self Service Password Reset (SSPR). Binnen de Microsoft Authenticator-app worden de authenticatiemodes "Push" en "Passwordless" beide toegestaan. Bij de MFA-melding wordt ook de betreffende applicatiennaam aangegeven. Wanneer een gebruiker zelf een FIDO2-securitykey heeft en deze toegevoegd heeft als MFA-methode kan deze ook gebruikt worden voor toegang tot de omgeving en dient dit als een MFA-methode.
Motivatie
Deze methodes worden gezien als de veiligste methodes. Het vermindert het risico op phishing aanvallen maar biedt toch een prettige gebruikerservaring. De applicatie naam weergeven bij een Authenticator verzoek zorgt voor herkenbaarheid.

Ontwerpbesluit
Voor alle gebruikers zal beperk worden zodat inloggen in de omgeving alleen mogelijk is vanuit landen die expliciet zijn aangemerkt als veilig. In overeenstemming hiermee worden de landen België, Nederland, Frankrijk en Duitsland als veilig beschouwd. Dit betekent dat gebruikers alleen toegang hebben tot de omgeving als ze zich in een veilig land bevinden. Voor een specifieke gebruikersgroep is naast deze landen de toegang vanuit alle EU landen mogelijk.
Motivatie
Door de toegang te beperken verminder je aanzienlijk het risico dat kwaadwillende toegang tot de omgeving verkrijgen. Er is echter een uitzondering op dit beleid voor een specifieke gebruikersgroep. Deze groep bestaat uit medewerkers die hebben aangegeven dat ze zich in een van de niet-veilige landen bevinden, maar toch hun werk moeten uitvoeren. Deze medewerkers kunnen ondanks hun locatie in een niet-veilig land nog steeds inloggen en toegang krijgen tot de omgeving, vanwege hun specifieke werkvereisten. Deze groep kan gevuld worden met medewerkers die veel reizen voor het werk, of tijdelijk met medewerkers die op vakantie zijn buiten de EU.

Ontwerpbesluit
Voor onveilige Windows apparaten en onbeheerde Windows apparaten geldt dat deze alleen webapplicaties mogen gebruiken. Dit betekent dat ze uitsluitend via het web toegang hebben tot resources. Lokaal werken op deze apparaten is niet mogelijk en de synchronisatie met OneDrive wordt stopgezet. Binnen de browser zijn er vervolgens beperkingen opgelegd om de veiligheid te waarborgen. Zo is het bijvoorbeeld niet mogelijk om gegevens te downloaden naar het lokale apparaat. Deze maatregelen zijn genomen om de beveiliging van het systeem te waarborgen en het risico van ongeautoriseerde toegang tot gegevens te minimaliseren voor apparaten die niet compliant zijn.
Motivatie

Door te zorgen dat lokale applicaties en data niet actief gebruikt kan worden wanneer het apparaat onveilig is versterk je de beveiliging aanzienlijk. Wanneer er bijvoorbeeld kwaadaardige software op het apparaat is terecht komt zorgt deze regel ervoor dat de OneDrive sync stopt.

Ontwerpbesluit

Het besturingssysteem Linux en MacOS wordt niet gebruikt binnen de organisatie, toegang tot de KyK omgeving vanaf het besturingssysteem Linux en MacOS is daarom niet toegestaan.

Motivatie

KyK maakt geen gebruik van Linux en MacOS, om risico tot ongewenste toegang te beperken staan we Linux en MacOS niet toe.

Ontwerpbesluit

Voor de besturingssystemen iOS en Android wordt de toegang tot resources beveiligd met app protection policies. Deze maatregel maakt het mogelijk om Microsoft applicaties veilig te gebruiken op onbeheerde apparaten. Met dit beleid wordt het gebruik van deze beveiligingsbeleidsmaatregelen verplicht gesteld, waardoor het gebruik van native applicaties zoals Apple Mail niet mogelijk is.

Motivatie

Deze maatregel maakt het mogelijk om Microsoft applicaties veilig te gebruiken op onbeheerde apparaten. Dit is bedoeld om een hoger niveau van beveiliging te waarborgen en het risico van ongeautoriseerde toegang tot gegevens te minimaliseren bij het gebruik van onbeheerde apparaten.

Ontwerpbesluit

Gebruikers krijgen de mogelijkheid om zelf zijn of haar wachtwoord te wijzigen, dit kan op elk moment ook wanneer de gebruiker het wachtwoord vergeten is. Dit wordt gedaan door middel van het gebruik van de MFA methodes. Het configureren van deze methodes is alleen mogelijk vanaf vertrouwde locaties, dit is alleen binnen Nederland.

Motivatie

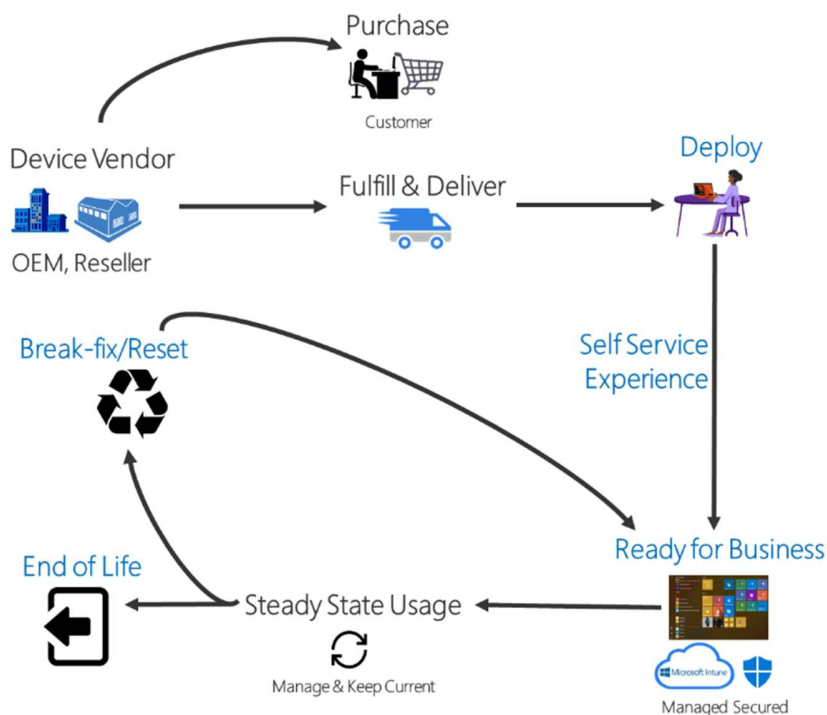
Door gebruikers dit zelf te laten verklein je de beheerlast en kunnen gebruikers snel weer aan het werk wanneer ze het wachtwoord zijn vergeten. Hiervoor gebruik je je MFA methodes, het is van groot belang dat dit alleen door geauthentiseerd personen te laten registreren daarom wordt dit enkel toegestaan op veilige locaties. Dit ondersteund de Zero Trust principes.

Ontwerpbesluit

Accounts die uitgesloten zijn van MFA zullen worden voorzien van een extra beveiligingsregel. Accounts die momenteel uitgesloten zijn van MFA zijn leerlingen, serviceaccounts en noodaccounts. Om deze accounts toch beter te beschermen, zal authenticatie met deze accounts alleen mogelijk zijn vanaf de hoofdlocatie van KyK (Kantoor Sneek). Voor leerlingen is dan in Nederland het mogelijk om mail en teams te benaderen, echter is buiten Nederlands geen toegang mogelijk. Daarnaast wordt het gebruik van de noodaccounts gemonitord. Wanneer het account wordt gebruikt, ontvangt de organisatie hiervan een melding.

Motivatie

Deze accounts kunnen geen MFA gebruiken, hierdoor vormen ze in principe een risico binnen de omgeving. Om toch deze accounts veilig te kunnen gebruiken worden de toegang beperkt en het gebruik gemonitord.



Ontwerpbesluit
Vanwege het verhoogde risico dat gepaard gaat met verouderde authenticatie protocollen wordt dit geblokkeerd. Hierdoor is een gebruiker verplicht om gebruik te maken van moderne authenticatie. Verouderde authenticatie protocollen zijn: Exchange ActiveSync (EAS), SMTP, Autodiscover, Exchange Online PowerShell, Exchange Web Service (EWS), IMAP4, MAPI over HTTP, Offline Address Book (OAB), Outlook Anywhere (RPC over HTTP), Outlook Service, POP3 en Reporting Web Service.
Motivatie
Verouderde authenticatie protocollen vormen een hoog risico. MFA wordt niet ondersteund op deze protocollen en zijn een doelwit voor kwaadwillende.

Windows inschrijving

Voor de geconfigureerde Windows werkplekken van KyK scholen hebben we gekozen voor het gebruik van Windows Autopilot. De essentie van Autopilot is om nieuwe Windows-apparaten vóór gebruik te configureren.

Tevens biedt het de mogelijkheid om bestaande apparaten opnieuw in te stellen, waardoor ze eenvoudig door andere gebruikers kunnen worden overgenomen. De strategische beslissing om Autopilot te implementeren is gebaseerd op de aanzienlijke tijdsbesparing bij de (her)installatie van apparaten, en het verbeterde gebruiksgemak doordat de hardware direct is gekoppeld aan de tenant. Deze keuze draagt bij aan een efficiënt beheer van de werkplekken, waarbij de configuratie en toewijzing van hardware naadloos geïntegreerd zijn.

Ontwerpbesluiten

Ontwerpbesluit
De medewerkers van KyK worden voorzien van beheerde Windows 11 Pro laptops.
Motivatie
Dankzij deze beheerde Windows Pro laptop heeft de medewerker de mogelijkheid om zowel binnen als buiten de muren van KyK mobiel te zijn. Met slechts één apparaat kan de medewerker op een veilige manier toegang krijgen tot de applicaties en gegevens van KyK, ongeacht de locatie.

Ontwerpbesluit
We kiezen ervoor om OEM-sleutels te gebruiken voor de activering van Windows. Laptops zullen worden geleverd met een Windows Pro licentie.
Motivatie
Deze keuze waarborgt een voortdurende activering van Windows zonder de noodzaak van een activeringsserver. Dit draagt bij aan het verminderen van de beheerlast.

Ontwerpbesluit
Het onderscheid van alle type werkplek wordt op basis van Autopilot profielen gedaan. Zo wordt er voor elke locatie onderscheid gemaakt op basis van medewerkers laptops, leerling laptops, gedeelde apparaten voor invallers en scherm gebonden computers. Hiervoor worden aparte Autopilot profielen voor gemaakt waarbij de toewijzing via een unieke "tag" gaat.
Motivatie
Het Autopilot-profiel is verantwoordelijk voor het bepalen of een apparaat is toegewezen aan een specifieke gebruiker of gedeeld wordt door meerdere gebruikers. Het is van essentieel belang om dit onderscheid op dit niveau aan te brengen. Dit onderscheid vormt namelijk de basis voor verdere configuratie. Aangezien we van plan zijn om dit onderscheid te gebruiken voor uitgebreidere configuratiedoelinden, is het noodzakelijk om alle verschillende categorieën in deze context te identificeren en benoemen.

Ontwerpbesluit
De nieuwe Windows-werkplekken worden geleverd met een vooraf geïnstalleerd Windows besturingssysteem, verzorgd door de leverancier. Het betreft een schone Windows 11 Pro installatie, vrij van overbodige software (bloatware), maar wel voorzien van de juiste drivers. De leverancier initieert de Autopilot-registratie binnen Intune, inclusief de benodigde tags. Verdere configuratie van de endpoints wordt uitgevoerd met behulp van Microsoft Autopilot.
Motivatie
Het minimaliseren van beheerinspanningen staat centraal in dit proces. KyK Scholen hoeft geen eigen OS-image bij te houden en te installeren op beheerde laptops. De registratie die door de leverancier in Autopilot wordt uitgevoerd, zorgt ervoor dat de installatie van de KyK configuratie zonder extra handelingen kan worden gestart zodra de laptop voor het eerst wordt ingeschakeld. Hierdoor wordt het

opstartproces aanzienlijk vereenvoudigd en geautomatiseerd, waardoor de beheertijd en -inspanningen worden geminimaliseerd.

Ontwerpbesluit

Op basis van de diverse soorten apparaten zoals beschreven in ontwerpbesluit 0 worden dynamische Entra ID device groepen gecreëerd. Hierbij wordt gefilterd op de bijbehorende tag, waardoor alle apparaten met de specifieke tag automatisch in de juiste groep worden ingedeeld.

Motivatie

Deze groepen zullen de basis vormen voor verdere configuratie van de apparaten. Het uitgangspunt is dan ook dat binnen deze drie groepen een aanzienlijke mate van standaardisatie zal plaatsvinden. Dit stelt ons in staat om op een gestructureerde en geautomatiseerde manier configuraties door te voeren, waarbij rekening wordt gehouden met de specifieke kenmerken van elk type apparaat.

Ontwerpbesluit

Gebruikers krijgen standaard user rechten op de beheerde Windows endpoints.

Motivatie

In het kader van "Just Enough Administration" krijgen gebruikers met standaard user rechten voldoende ruimte om hun werkzaamheden te kunnen doen.

Ontwerpbesluit

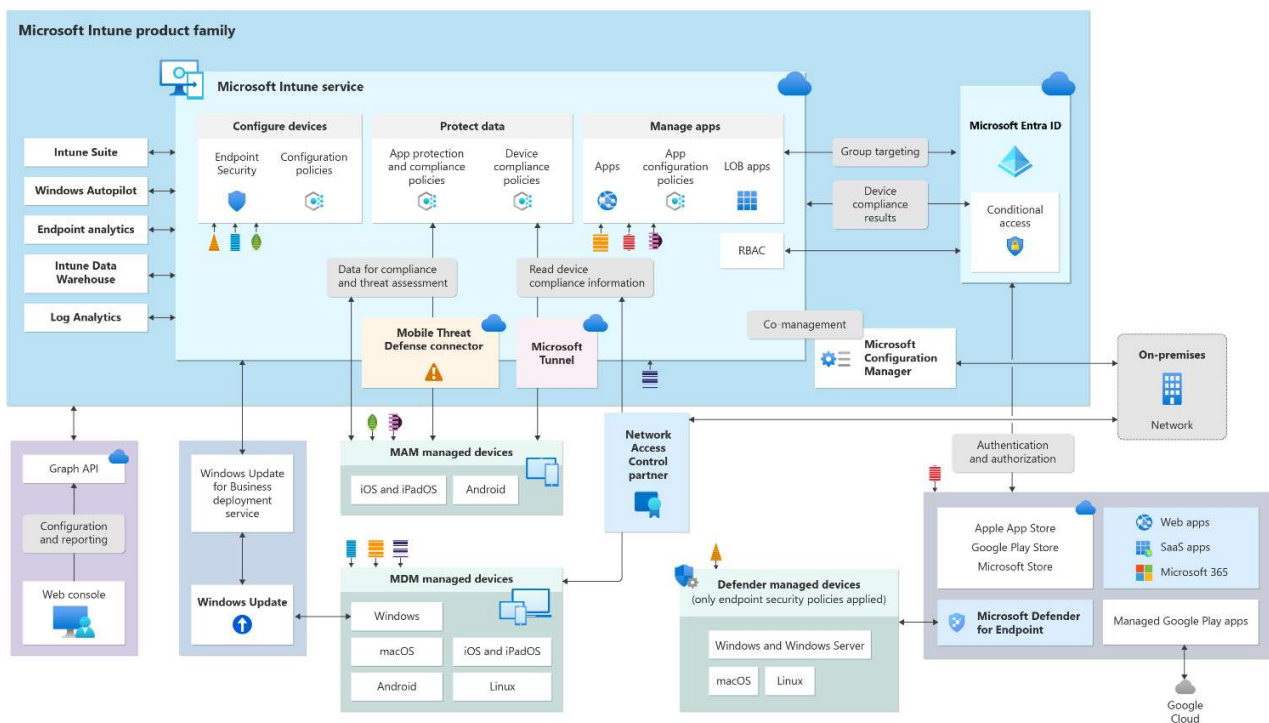
Het is enkel toegestaan om apparaten als zakelijk apparaat te registreren binnen Intune via Autopilot. Voor persoonlijke Windows-apparaten is het niet toegestaan dat gebruikers zelf het apparaat registreren in Intune. Persoonlijke apparaten zullen dus altijd gezien worden als Bring Your Own Device (BYOD) en dus onbeheerd.

Motivatie

Door dit toe te passen staan er altijd en alleen Windows apparaten binnen Intune die eigendom zijn van het bedrijf en volledig te managen zijn. Hiermee voorkom je dat op onbeheerde apparaten dezelfde toegang tot de omgeving mogelijk is als op beheerde apparaten.

Windows configuratie

De werkplek is zorgvuldig samengesteld met het oog op optimalisatie en functionaliteit. Het hoofddoel is ervoor te zorgen dat de gebruikers een gestroomlijnde en efficiënte werkomgeving ervaren, waarbij overbodige schermen en gegevens worden geminimaliseerd. Een dergelijke opzet bevordert niet alleen de productiviteit, maar biedt ook een aangename en veilige werkomgeving. Specifiek voor de Windows werkplek wordt de configuratie volledig beheerd via Microsoft Intune, een krachtige tool die zorgt voor een gestandaardiseerde en gecontroleerde inrichting van de werkstations. In het voorgaande hoofdstuk over Autopilot is uitvoerig beschreven hoe deze inrichting plaatsvindt, waarbij de nadruk ligt op het geautomatiseerde proces om nieuwe apparaten snel en efficiënt te implementeren.



Ontwerpbesluiten

Ontwerpbesluit
De Windows 10/11 lokale desktop wordt beheerd met Microsoft Intune.
Motivatie
Intune is dé management tool vanuit Microsoft voor het beheer van het Windows OS. De beheervoorzieningen wordt aangeboden als SAAS dienst waardoor er voor het beheer van het OS op de endpoints geen infrastructuur door KyK onderhouden hoeft te worden. Daarnaast is de lokale desktop met de beheervoorzieningen locatie onafhankelijk over het internet te beheren.
Ontwerpbesluit
De toewijzing van configuraties en applicaties proberen we in grote mate te standaardiseren. Het onderscheid in deze standaardisatie brengen we aan op het niveau van de Autopilot profielen. We zullen

hiervoor zoveel mogelijk gebruik maken van dynamische AAD device groepen. Wanneer dit niet mogelijk is, omdat een applicatie of configuratie niet voor alle Autopilot apparaten geldt maar voor een specifieke groep, zullen we hiervoor aparte groepen gaan gebruiken.

Motivatie

Door gebruik te maken van dynamische AAD device groepen op basis van Autopilot profielen kan per laptop eenvoudig worden aangegeven voor welke functie de laptop moet worden ingericht. Op basis van deze functie worden de aan de device groep gekoppelde configuratie en applicaties op de laptop aangebracht. Omdat van dynamische groepen gebruik wordt gemaakt, wordt de beheerlast beperkt en wordt de betreffende laptop ook bij een herinstallatie altijd op dezelfde wijze ingericht.

Ontwerpbesluit

Microsoft Entra ID wordt ingezet als primaire authenticatie bron voor de gebruikers. Na authenticatie bij Entra ID kunnen gebruikers binnen de werkplek bij voorkeur gebruik maken van alle applicaties en data waarvoor zij zijn geautoriseerd zonder zich opnieuw te authenticeren (SSO).

Motivatie

Door Entra ID als primaire authenticatie bron in te zetten kan gebruik worden gemaakt van de beveiligingsmogelijkheden van Azure. Ook als alleen gebruik wordt gemaakt van de Online Microsoft Office 365 omgeving. Voorbeelden hiervan zijn voorwaardelijke toegang en Multifactor Authenticatie als extra beveiliging tot de werkplekomgeving.

Ontwerpbesluit

Voor de apparaten die door meerdere gebruikers gebruikt zullen worden en dus met de het gedeelde autopilot profiel zijn gedeployed zullen een "Shared multi-user device" configuratie profiel krijgen. Deze zet het apparaat in gedeelde PC mode

Motivatie

Shared PC biedt opties om het beheer en de optimalisatie van gedeelde apparaten te vergemakkelijken. (<https://learn.microsoft.com/en-us/windows/configuration/set-up-shared-or-guest-pc?tabs=intune#shared-pc-mode-concepts>)

Ontwerpbesluit

Intune faciliteert een Wi-Fi verbinding met het KyK Scholen netwerk op de Windows apparaten. De authenticatie wordt gedaan op basis van SSID en wachtwoord.

Motivatie

Dit biedt het voordeel dat apparaten tijdens enrollment al verbonden zijn met het Wi-Fi netwerk en gebruikers zelf geen handelingen hoeven te ondernemen.

Ontwerpbesluit

De beheerde werkplekken worden voorzien van een KyK huisstijl. Er wordt een KyK bureaublad achtergrond en vergrendelscherm ingesteld.

Motivatie

Dit creëert een uniforme uitstraling en verhoogt veiligheid omdat de KyK werkplek herkenbaar wordt.

Ontwerpbesluit

De applicaties en de snelkoppelingen naar webapplicaties worden geïnstalleerd via Intune. Via Intune wordt vervolgens een uniforme startmenu lay-out gemaakt waarin alle applicatie en snelkoppelingen terecht komen.

Motivat

Intune als uniforme applicatiebeheertool maakt het mogelijk om applicaties en snelkoppelingen op verschillende besturingssystemen te installeren. Door een consistente lay-out van het startmenu wordt een eenduidige gebruikerservaring gecreëerd. Het gebruik van Intune zorgt er tevens voor dat snelkoppelingen en applicaties buiten de KyK-infrastructuur via het internet geïnstalleerd en beheerd kunnen worden.

Ontwerpbesluit

Zover technisch mogelijk worden alle applicaties aangeboden via Intune. Hierbij wordt een splitsing gemaakt tussen standaard applicaties zoals bijvoorbeeld een browser en een PDF-reader. De standaard applicaties worden via Intune geïnstalleerd op alle werkplekken. Alle andere applicaties worden met behulp van Intune aangeboden via de Company Portal. Wanneer de gebruiker een applicatie wil gebruiken kan deze zelf worden geïnstalleerd via deze Company Portal.

Motivat

Door alleen de standaard applicaties voor te installeren duurt het uitrollen van een laptop minder lang dan wanneer alle applicaties automatisch zouden worden geïnstalleerd. De gebruiker heeft meteen de belangrijkste applicaties beschikbaar bij het ontvangen van de laptop en kan daarna extra benodigde applicaties zelf installeren vanuit de Company Portal.

Ontwerpbesluit

Gebruikers kunnen applicaties installeren die met standaard gebruiker rechten kunnen worden geïnstalleerd. Daarnaast is het geblokkeerd dat gebruikers applicaties installeren vanuit de Microsoft store.

Motivat

Gebruikers krijgen geen aanvullende lokale administrator rechten op het apparaat, echter is het niet tegen te gaan dat gebruikers applicaties zoals bijvoorbeeld Google Chrome downloaden en vervolgens installeren aangezien er geen gebruik wordt gemaakt van een app locker.

Ontwerpbesluit

Intune regelt de configuratie van de standaard te gebruiken applicaties voor meest voorkomende bestandsextensies. Zo wordt voor mail bestanden Outlook als standaard ingesteld, voor PDF bestanden Adobe Reader en voor html bestanden is Microsoft Edge de standaard browser

Motivat

Door dit centraal in te regelen wordt gezorgd voor uniformiteit en duidelijkheid. Daarnaast worden er zo min mogelijk onnodige schermen getoond.

Ontwerpbesluit

De particuliere versie van Microsoft Teams, die alleen gebruikt kan worden met een persoonlijk Microsoft account en dus niet met een zakelijk Microsoft KyK account, wordt verwijderd van de werkplek.

Motivat

Door twee versies van de Teams app op de Windows werkplek beschikbaar te hebben wordt er onduidelijkheid gecreëerd. Daarom wordt alleen de juiste zakelijke Teams client beschikbaar gesteld op de werkplek.

Ontwerpbesluit

Onnodige snelkoppelingen worden van de taakbalk verwijderd. Bijvoorbeeld de Store app, het Chat icoon en News and Interest zijn niet relevant en worden daarom verwijderd.

Motivatie

Snelkoppelingen die verwijzen naar functies of applicaties die worden uitgeschakeld, zoals de Windows store app, hoeven niet worden getoond om verwarring voor de gebruiker te voorkomen. Daarnaast zijn een aantal applicaties die standaard onderdeel zijn van het Windows besturingssysteem niet relevant voor de dagelijkse werkzaamheden. Deze snelkoppelingen hoeven dus ook niet te worden getoond.

Ontwerpbesluit

Applicaties die via Intune op de laptop worden geïnstalleerd, worden bij voorkeur geïnstalleerd vanuit de nieuwe Microsoft Store for Business. Als de gewenste applicatie niet beschikbaar is in de store, moet de applicatie worden omgezet naar een ingepakt installatie bestand. Dit vereist wel dat de applicatie installatie beschikbaar is als een uitvoerbaar bestand dat op een Windows-apparaat geïnstalleerd kan worden zonder tussenkomst van de gebruiker en zonder een grafische interface (silent).

Motivatie

Installatie vanuit de Microsoft store zorgt voor een eenvoudiger installatie van de applicatie dan via een ingepakt installatie bestand. Ook houdt de Microsoft Store de applicaties via WinGet up to date en worden applicatie updates op de laptop automatisch doorgevoerd.

Ontwerpbesluit

Microsoft Edge wordt geconfigureerd als de primaire browser voor de werkplek. Naast Microsoft Edge wordt ook de Google Chrome-browser beschikbaar gesteld. Beide browsers worden beheerd via Intune. Voor Edge wordt automatisch het zakelijke KyK Microsoft-account ingelogd, inclusief synchronisatie van onder andere favorieten, wachtwoorden en geschiedenis. Voor Chrome wordt de mogelijkheid om gegevens te synchroniseren en wachtwoorden op te slaan uitgeschakeld.

Motivatie

Microsoft Edge integreert optimaal in de omgeving en biedt veiligheidsvoordelen. Authenticatie kan beveiligd worden met Conditional Access en ook Defender is geïntegreerd in Edge. Omdat Chrome binnen KyK nog veel wordt gebruikt, bieden we deze browser aan met zoveel mogelijk dezelfde ervaring als in Edge. Echter, omdat het niet mogelijk is om met het zakelijke account in te loggen, wordt account synchronisatie uitgeschakeld voor Chrome.

Ontwerpbesluit

Wanneer een medewerker Edge opstart wordt dit altijd gedaan met de SharePoint landingspagina van KyK. Voor een leerling wordt Prowise en de School SharePoint pagina standaard geopend in Edge en ook in Chrome

Motivatie

Dit sluit aan bij de huidige gebruikerservaring en zorgt ervoor dat medewerkers en leerlingen snel zijn of haar spullen kunnen vinden.

Ontwerpbesluit
Persoonlijke bestanden van de gebruiker (homedrive) worden opgeslagen op Microsoft OneDrive. Hierbij worden de bekende mappen (Bureaublad, documenten en afbeeldingen) gesynchroniseerd.
Motivatie
Centrale Cloud opslag van persoonlijke gebruikersgegevens die zonder extra infrastructuur over het internet beschikbaar is binnen en buiten de muren van KYK. Daarnaast kan de gebruiker de persoonlijke bestanden op een veilige manier delen met derden waarbij de data de Cloud locatie niet verlaat. Door gebruik te maken van de synchronisatie van de bekende mappen zorg je dat de gebruiker altijd zijn persoonlijke bestanden bij de hand heeft.

Ontwerpbesluit
Microsoft Teams wordt ingezet als dagelijks samenwerkingsplatform om samen met interne en externe collega's en partijen te werken aan data.
Motivatie
Centrale Cloud opslag van KyK Organisatie data die zonder extra infrastructuur over het internet beschikbaar is binnen en buiten de muren van KyK. Daarnaast kunnen de bestanden op een veilige manier worden gedeeld met derden waarbij de data de Cloud locatie niet verlaat.

Ontwerpbesluit
De lokale C-schijf wordt verborgen en onbruikbaar gemaakt voor de gebruikers in Windows Explorer.
Motivatie
Dit zorgt ervoor dat de gebruiker naar de juiste locaties, zoals OneDrive en Teams, wordt gestuurd voor het opslaan van de bestanden.

Ontwerpbesluit
De toegang tot de commandoprompt en het register wordt geblokkeerd voor de gebruikers.
Motivatie
Deze tools dienen alleen benadert te worden door administrators, hierom wordt de toegang voor gebruikers geblokkeerd.

Ontwerpbesluit
De beheerde apparaten worden in slaapstand geschakeld na een uur wanneer de laptop op accu werkt en na 3 uur wanneer de laptop is aangesloten op het netstroom.
Motivatie
Deze huidige opzet wordt ook gehanteerd op de huidige gedeelde werkplekken. We willen hierin de zelfde ervaring blijven aanbieden voor de gebruikers.

Ontwerpbesluit
Er wordt gebruikt gemaakt van docking stations. Gebruikers moeten de mogelijkheid hebben om de klep van de laptop dicht te doen wanneer ze aangesloten zijn op de docking station zonder dat het apparaat in slaapstand treedt. De laptop zal wanneer hij op accu werkt wel in slaapstand treden.
Motivatie

Dit zorgt ervoor dat gebruikers die op 1 scherm willen werken de laptop dicht kunnen klappen zonder daar nog aanvullende handelingen voor te verrichten.

Ontwerpbesluit

Op de beheerde Windows endpoints wordt Windows Hello ingericht. Hiermee kunnen gebruikers inloggen zonder het gebruik van een wachtwoord door gebruik te maken van een pincode of biometrische gegevens in de vorm van gezichtsherkenning of een vingerafdruk scan. Dit kan alleen gebruikt worden op de persoonlijke beheerde apparaten.

Motivatie

Verbeteren van de gebruikerservaring en vergroten security door gebruik van wachtwoorden te beperken. Ook voorkomt dit dat gebruikers "MFA moeheid" ervaren.

Ontwerpbesluit

Wanneer een gebruiker remote support nodig heeft kan er contact opgenomen worden met de servicedesk van Leverancier. Wanneer een support medewerker met de KyK gebruiker wil mee kijken kan er gebruik gemaakt worden van Quick Assist. Deze applicatie wordt op alle werkplekken voor-geïnstalleerd.

Motivatie

Dit verhoogt gebruikersgemak en verbetert de ondersteuning. In het geval van een probleem kan de gebruiker meteen geholpen worden zonder dat er eerst iets geïnstalleerd moet worden.

Ontwerpbesluit

De huidige Cloud print oplossing wordt ingezet voor het afhandelen van de printopdrachten naar de Ricoh printers. Gebruikers worden automatisch aangemaakt in de Ricoh Cloud print oplossing en kunnen nadat ze in Windows ingelogd zijn automatisch printen zonder zich hierbij opnieuw te hoeven authenticeren.

Motivatie

Deze omgeving wordt reeds gebruikt en past binnen het concept van de nieuwe werkplek op basis van Windows 10/11.

Ontwerpbesluit

Het gebruik van eigen printers op de thuiswerkplek wordt geblokkeerd. Wanneer er geprint wordt, dient er gebruik gemaakt te worden van de Ricoh Cloud print oplossing.

Motivatie

De Cloud print oplossing biedt de mogelijkheid om over het internet te printen. Zo zorgen we ervoor dat printjes niet blijven liggen bij onbekende printers.

Ontwerpbesluit

Voor het speciaal onderwijs verwachten we dat er specifieke applicaties geïnstalleerd moeten worden op de werkplek, voor nu wordt dit handmatig gedaan door een beheerder. Deze mogelijk moet in de nieuwe werkplek omgeving ook gefaciliteerd worden.

Motivatie

Dit zorgt ervoor dat applicaties die niet uitgerold kunnen worden via de MDM oplossing en maar op kleine schaal gebruikt worden toch op een snelle manier de applicaties kunnen gebruiken.

Windows update

Het belang van het actueel houden van het besturingssysteem en alle software kan niet genoeg benadrukt worden. Door regelmatig updates te installeren, worden niet alleen eventuele kwetsbaarheden gedicht, maar wordt ook de algehele stabiliteit en prestatie van de systemen verbeterd. Verouderde software kan een gemakkelijk doelwit zijn voor kwaadwillende actoren die op zoek zijn naar zwakke plekken om in te breken en schade aan te richten. Daarom is het van cruciaal belang dat organisaties proactief zijn in het bijwerken van hun systemen om de kans op beveiligingsinbreuken te minimaliseren en de operationele continuïteit te waarborgen.

Wanneer updates snel worden geïmplementeerd, wordt de kans op exploitatie van bekende kwetsbaarheden aanzienlijk verminderd. Dit is vooral belangrijk in een tijd waarin cyberdreigingen voortdurend evolueren en steeds geavanceerder worden. Door proactief te zijn in het bijwerken van systemen kunnen organisaties een robuuste

creëren tegen een potentiële variërend van gegevensinbreuken.

verdedigingslinie breed scala aan bedreigingen, malwareaanvallen tot



Ontwerpbesluiten

Ontwerpbesluit
Windows Update for Business wordt ingezet voor het beheren en installeren van Windows updates.
Motivatie
Windows Update for Business biedt een gestroomlijnde aanpak voor het beheer van Windows-updates, waardoor een consistente en veilige update-ervaring wordt gegarandeerd voor alle apparaten binnen KyK.

Ontwerpbesluit
Verschillende update-ringen zullen worden geconfigureerd om updates geleidelijk uit te rollen binnen de organisatie. Dit stelt ons in staat om een klein deel van de organisatie updates eerder te laten ontvangen,

waardoor eventuele problemen met een update vroegtijdig worden ontdekt en de impact op de hele organisatie wordt beperkt.

Motivatie

Het configureren van verschillende update-ringen biedt ons de mogelijkheid om updates op een gecontroleerde manier uit te rollen, waardoor we operationele stabiliteit kunnen handhaven. Door een klein aantal gebruikers updates eerder te laten ontvangen, kunnen we potentiële problemen identificeren en oplossen voordat ze invloed hebben op de gehele organisatie.

Ontwerpbesluit

Windows Driver-updates zullen, waar technisch mogelijk, automatisch worden bijgewerkt binnen een update-ring.

Motivatie

Het automatisch bijwerken van Windows Driver-updates binnen een update-ring bevordert de operationele efficiëntie en zorgt voor een consistente en up-to-date driveromgeving.

Ontwerpbesluit

Een aparte kwaliteitsupdate-ring wordt geconfigureerd, waardoor het mogelijk is om alle apparaten indien nodig snel van de nieuwste beveiligingsupdates te voorzien. Deze aanpak maakt het mogelijk om kwetsbaarheden zoals die na patch Tuesday gedicht zijn versneld uit te rollen, zonder aanpassingen te hoeven doen aan de reguliere update-ringen.

Motivatie

Het instellen van een aparte kwaliteitsupdate-ring biedt flexibiliteit en snelheid bij het implementeren van essentiële beveiligingsupdates, waardoor de reactietijd op nieuwe bedreigingen wordt versneld.

Ontwerpbesluit

De applicaties uit de Microsoft store worden, met behulp van het update mechanisme binnen de Microsoft Store en "Win-Get" up to date gehouden.

Motivatie

Het update mechanisme is geïntegreerd in de Microsoft Store en vereist minimaal beheer. Het zorgt ervoor dat de applicaties altijd zijn voorzien van de laatste beveiligingsupdates.

Ontwerpbesluit

Voorlopig wordt geen alternatieve beheervoorzieningen ingezet om patching, updates en upgrades van 3rd party applicaties op de endpoints te ondersteunen. Applicatie patches, updates en upgrades worden handmatig in Intune geconfigureerd door beheer.

Motivatie

De meeste applicatie die worden geïnstalleerd zijn automatisch te updaten. Voor de applicaties waar dat niet mogelijk is zal om de zoveel tijd een nieuwe versie geïnstalleerd moeten worden. We verwachten dat dit geen grote hoeveelheid is.

Ontwerpbesluit

We gaan gebruik maken van Edge Progressive Web Apps (App Snippets). Dit zorgt ervoor dat een specifieke URL als app wordt toegevoegd zonder dat de applicatie geïnstalleerd hoeft worden.

Motivatie

Dit zorgt ervoor dat er geen applicaties ingepakt en uitgerold hoeft worden naar de werkplek en dat er ook geen applicatie updates hoeven te verricht worden. Dit verlicht aanzienlijk de beheerlast.

Ontwerpbesluit

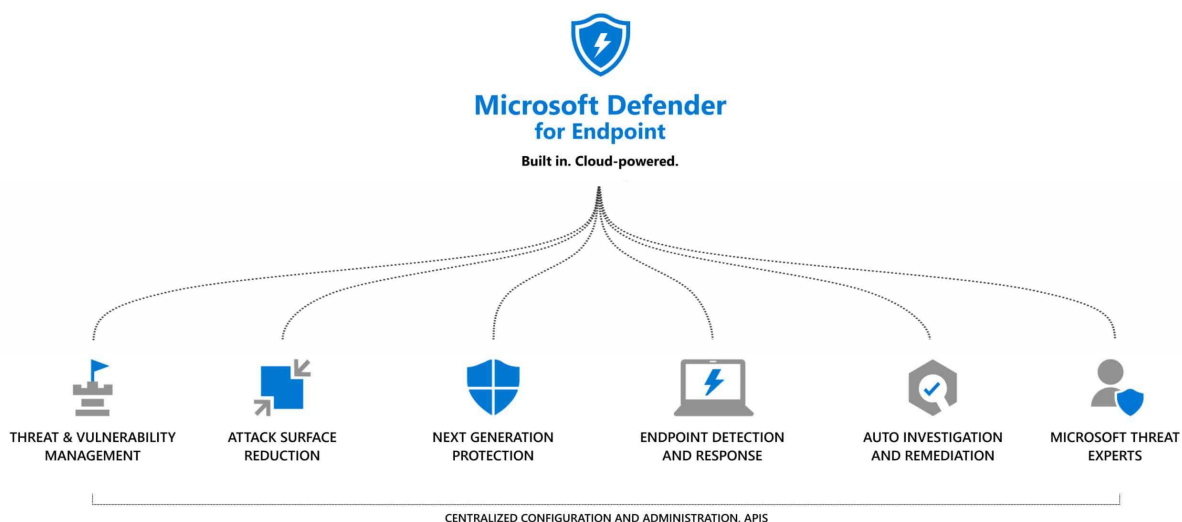
Applicaties van 3rd party leveranciers met auto update functionaliteit mogen automatisch updates uitvoeren wanneer dit mogelijk is zonder administrator rechten. Wanneer hier aanvullende rechten nodig zijn zal voor zover mogelijk de auto update functie er uit gehaald worden.

Motivatie

Waar mogelijk worden alle applicaties automatisch up-to-date gehouden worden. Dit verlaagt de beheerlast.

Windows beveiliging

Een solide beveiligingsaanpak op beheerde werkplekken vormt de basis van een robuust



cyberbeveiligingsbeleid voor KyK. Door gebruik te maken van de best practices van Microsoft kan KyK profiteren van geavanceerde beveiligingsfuncties en robuuste bescherming bieden tegen een breed scala aan dreigingen.

Een essentieel onderdeel van deze aanpak is het implementeren van Defender for Endpoint, een krachtige tool die geavanceerde beveiligingsfuncties biedt, zoals endpoint detection and response (EDR), antivirusbescherming, detectie van verdachte activiteiten en geautomatiseerde responsmogelijkheden. Door Defender for Endpoint te implementeren en te integreren in de beheerde werkplekken kan KyK snel reageren op potentiële bedreigingen en proactief hun systemen beschermen tegen malware, ransomware en andere kwaadaardige activiteiten.

Ontwerpbesluiten

Ontwerpbesluit

Bij alle Windows apparaten is het vereist dat "Secure Boot" in de BIOS is ingeschakeld.

Motivatie
Secure Boot verhoogt de beveiliging van Windows-apparaten door ervoor te zorgen dat alleen ondertekende en vertrouwde software tijdens het opstartproces wordt geladen, waardoor de kans op het opstarten van kwaadaardige of niet-geautoriseerde code wordt verminderd.
Ontwerpbesluit
Microsoft Defender for Endpoint wordt ingezet als securityoplossing om de fysieke werkplekken te beschermen tegen virus- en malwarebedreigingen. Het biedt geavanceerde beveiligingsfuncties en integratie met de Microsoft Office en Windows infrastructuur.
Motivatie
Het gebruik van Microsoft Defender for Endpoint als beveiligingsoplossing biedt een robuuste bescherming voor de fysieke werkplekken. Het biedt geavanceerde beveiligingsfuncties en naadloze integratie met de bestaande Microsoft Office en Windows infrastructuur. Bovendien ondersteunen Azure en Endpoint Manager diverse dashboards die het beheer van de werkplekken efficiënt ondersteunen.
Ontwerpbesluit
Er wordt gebruik gemaakt van één Microsoft Defender Antivirus profiel. Deze zal de antivirusbeleidsinstellingen voor alle Windows-apparaten instellen en beheren.
Motivatie
Defender Antivirus is het next-generation beschermingscomponent van Microsoft Defender for Endpoint. Next-generation bescherming brengt technologieën zoals machine learning en cloud-infrastructuur samen om apparaten te beschermen.
Ontwerpbesluit
Er wordt een Windows beveiligingservaring profiel geconfigureerd in Intune. Dit profiel bepaalt hoe de instellingen van de Windows Beveiligingsapp worden geconfigureerd. Het profiel bepaalt wat een eindgebruiker kan zien in het beveiligingscentrum en welke meldingen er op het scherm worden getoond.
Motivatie
De Windows Beveiligingsapp wordt gebruikt door een aantal Windows beveiligingsfuncties om meldingen te geven over de gezondheid en beveiliging van de machine. Beveiligingsapp-meldingen worden onder andere gegeven voor firewalls, antivirusproducten en Windows Defender SmartScreen.
Ontwerpbesluit
Microsoft BitLocker wordt op beheerde Windows endpoints geconfigureerd om lokaal op het endpoint opgeslagen data te versleutelen.
Motivatie
De opgeslagen data op de endpoints wordt beschermd tegen ongeautoriseerd gebruik en kan alleen worden ontsleuteld met behulp van de encryptie sleutels die zijn opgeslagen in de Azure AD.
Ontwerpbesluit
Het is niet toegestaan om externe data dragers te gebruiken op de beheerde apparaten. Alle externe data dragers worden geblokkeerd.
Motivatie

Data dragers worden als niet veilig beschouwd en zijn daarom niet toegestaan.

Ontwerpbesluit

Er wordt een Windows Firewall policy gemaakt om de ingebouwde Windows firewall van de Windows apparaten te beheren.

Motivatie

Windows Firewall biedt host gebaseerde tweerichtingsfilters voor netwerkverkeer en blokkeert ongeautoriseerd netwerkverkeer dat het lokale apparaat binnenkomt of verlaat.

Ontwerpbesluit

Microsoft Application Control for Business wordt ingezet om te zorgen dat geaccepteerde en veilige Windows applicaties worden toegestaan. Applicaties die uitgerold worden via Intune worden automatisch als veilig beschouwd met behulp van de Managed Installer Extensie.

Motivatie

Door deze functionaliteit nu al in te schakelen worden alle uitgerolde applicaties als veilig beschouwt. Gebruikers zijn geen lokale administrator. Door deze functionaliteit worden apps die als gebruiker worden geïnstalleerd toch gecontroleerd op veiligheid.

Ontwerpbesluit

Web beveiliging zorgt voor beveiliging binnen de Edge browser. Het maakt gebruik van netwerkbeveiliging om machines te beveiligen tegen webbedreigingen. Webbeveiliging houdt de toegang tegen tot phishing sites, malwarevectoren, exploit sites, niet-vertrouwde sites of sites met een lage reputatie tegen.

Motivatie

Web beveiliging zorgt ervoor dat gebruikers veilig kunnen browsen. Het risico dat een gebruiker op onveilige websites zit of gevaarlijke bestanden download wordt verminderd.

Ontwerpbesluit

Web content filtering wordt toegepast om toegang tot websites te reguleren op basis van inhoudscategorieën. De gebruikers zien een blokkeringsmelding als een element op de pagina die ze bekijken een geblokkeerde bron aanroept. Deze functionaliteit zal werken op beheerde werkplekken op beveiligde browsers (Edge met Defender SmartScreen en Chrome met Netwerk Protectie)

Motivatie

Dit is een makkelijk hulpmiddel om toegang tot websites op apparaten met Defender for Endpoint te reguleren. Met behulp van Web content filtering kan eenvoudig worden bepaald welke thema's niet gebruikt kunnen worden binnen de webbrowser.

Ontwerpbesluit

Attack surface reduction policies worden ingezet ter beperking van het aanvalsoppervlak op de endpoints. De tooling detecteert gedrag dat malware en schadelijke apps gewoonlijk gebruiken om computers te infecteren, waaronder:

- Uitvoerbare bestanden en scripts die worden gebruikt in Office-apps of webmails om bestanden te downloaden of uit te voeren
- Versleutelde of anderszins verdachte scripts

- Gedragingen die apps gewoonlijk niet starten tijdens normaal dagelijks werk
[Manage attack surface reduction settings with endpoint security policies in Microsoft Intune | Microsoft Learn](#)

Motivatie

Door het aanvalsoppervlak te verkleinen wordt ervoor gezorgd dat aanvallers minder manieren hebben om aanvalen uit te voeren op de zakelijke Windows apparaten

Ontwerpbesluit

Met een Windows Local Administrator Password Solutions (LAPS) policy zal het standaard local administrator account worden beheerd en beveiligd. Het account wordt beveiligd met minimale wachtwoord vereisten, wachtwoord rotation en het opslaan van de credentials in Microsoft Entra.

Motivatie

Het gebruik van LAPS-beleidsregels helpt je Windows-apparaten te beschermen tegen aanvalen die gericht zijn op het misbruiken van lokale gebruikersaccounts. Ook kan het helpen bij het verbeteren van de beveiliging voor helpdeskscenario's op afstand en het herstellen van apparaten die anders ontoegankelijk zijn.

Ontwerpbesluit

Er worden nalevingsregels (compliance policies) aangemaakt om op meerdere vlakken de beheerde apparaten te controleren op veiligheid. Zo wordt er bijvoorbeeld gekeken naar wat de risico score is van Defender for Endpoint. Aan de verschillende policies wordt een prioriteit verbonden. Een grace period moet vervolgens voldoende tijd bieden om een geconstateerd probleem op te kunnen lossen en daarnaast moet de gebruiker niet te snel op de hoogte gebracht worden van een false non compliance melding. Er zal voor elk controle punt een aparte regel worden aangemaakt zodat er heel gericht een notificatie naar de gebruikers en beheerders kan worden gestuurd

Motivatie

Naleving (Compliance) is de tool om de veiligheid te waarborgen van de werkplekken. Door er meerdere aan te maken en te prioriteren kunnen er gemakkelijk verschillende acties aan gekoppeld worden.

Ontwerpbesluit

Internet wachtwoorden mogen worden opgeslagen binnen Microsoft Edge. Dit is de standaard ingestelde browser en wordt automatisch geconfigureerd met het zakelijke account. Wachtwoorden worden hier op een veilige manier automatisch opgeslagen en zijn daardoor ook beschikbaar in de mobiele authenticator app.

Motivatie

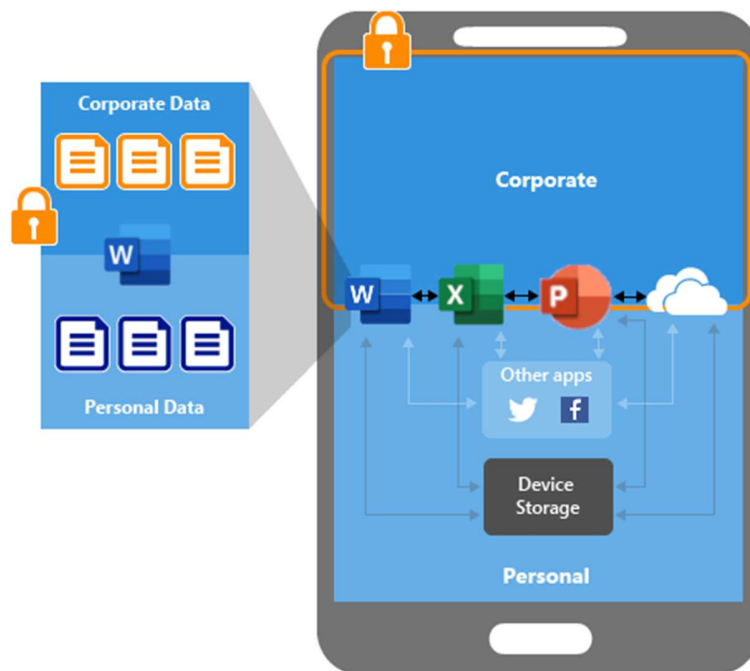
Er wordt momenteel geen gebruik gemaakt van alternatieve tooling voor het opslaan van wachtwoorden. Edge biedt binnen dit werkplekconcept de meeste veilige en gebruiksvriendelijke wachtwoord oplossing.

Tablets en smartphones

Binnen de organisatie KyK worden geen zakelijke mobiele apparaten verstrekt aan het personeel; alle apparaten worden dus beschouwd als Bring Your Own Device (BYOD) apparaten. Om deze apparaten veilig toegang te geven tot zakelijke bronnen zonder ze in beheer te nemen, zullen we gebruik gaan maken van Mobile Application Management (MAM).

Dit betekent dat de apparaten niet in beheer hoeven te worden genomen; in plaats daarvan wordt alleen de zakelijke applicatie beveiligd wanneer er toegang wordt gevraagd tot zakelijke bronnen. Wanneer een gebruiker een zakelijke applicatie benadert, zoals Outlook of Teams, wordt er eerst een automatische configuratie gestart. Hierdoor kunnen gebruikers de zakelijke apps veilig gebruiken, waarbij wordt voorkomen dat zakelijke gegevens terechtkomen op het privégedeelte van het apparaat.

Ontwerpbesluiten



Ontwerpbesluit

Er zullen Applicatie Beveiliging Policies (Mobile Application Management) worden toegepast op mobiele apparaten wanneer toegang tot zakelijke resources benodigd is. Deze policies zorgen ervoor dat alleen data-uitwisseling tussen beveiligde applicaties is toegestaan en dat data alleen kan worden opgeslagen op veilige, beheerde locaties zoals OneDrive en Teams.

Motivatie

Door Applicatie Beveiliging Policies (MAM) toe te passen op onze zakelijke iOS-toestellen, kunnen we een strikte scheiding tussen zakelijke en persoonlijke gegevens handhaven, zelfs als privégebruik wordt toegestaan. Deze policies zorgen ervoor dat gevoelige bedrijfsinformatie alleen wordt uitgewisseld tussen beveiligde applicaties en dat deze informatie alleen wordt opgeslagen op goedgekeurde en veilige locaties, zoals OneDrive en Teams. Hierdoor wordt de vertrouwelijkheid, integriteit en beschikbaarheid van bedrijfsgegevens gewaarborgd, terwijl tegelijkertijd de privacy van persoonlijke gegevens van medewerkers wordt gerespecteerd.

Ontwerpbesluit
Alle apps die te beveiligen zijn met app protection policies zullen beveiligd worden. De applicaties moeten hiervoor de Intune SDK ondersteunen en er dient een authenticatie plaats te vinden met een KyK account.
Motivatie
Hierdoor creëer je een veilige bubbel om al je zakelijke resources.

Ontwerpbesluit
Bij de eerste toegang van een gebruiker tot zakelijke gegevens met een ondersteunde app, zullen de app protection policies automatisch worden toegepast. Dit vereist een kleine configuratie, zoals het instellen van een pincode, die niet vervalt.
Motivatie
Dit proces waarborgt een simpele en gebruiksvriendelijke toepassing van app protection policies bij de eerste toegang. De niet-vervallende pincode zorgt voor gebruiksgemak.

Ontwerpbesluit
Het is niet toegestaan om zakelijke gegevens op te nemen in Android- of Apple-back-ups, aangezien deze back-ups persoonlijk zijn en het risico met zich meebrengen dat zakelijke gegevens op privéback-ups worden opgeslagen.
Motivatie
Dit beleid voorkomt dat zakelijke gegevens op onbedoelde locaties worden opgeslagen.

Ontwerpbesluit
Organisatiegegevens mag uitsluitend worden gedeeld met applicaties die beveiligd zijn met app protection policies. Het is niet toegestaan voor zakelijke data om buiten deze beveiligde bubbel te worden verspreid. Echter, het toevoegen van data binnen deze veilige bubbel is wel mogelijk.
Motivatie
Hierdoor wordt het risico op ongeautoriseerde verspreiding van zakelijke informatie geminimaliseerd.

Ontwerpbesluit
Alle zakelijke data zal worden versleuteld.
Motivatie
Door zakelijke data te versleutelen wordt de vertrouwelijkheid en integriteit ervan gewaarborgd, zelfs in het geval van ongeautoriseerde toegang.

Ontwerpbesluit
Wanneer er vanuit de veilige bubbel op een URL wordt geklikt, wordt deze geopend met Microsoft Edge, aangezien deze browser ook binnen de veilige bubbel valt.
Motivatie
Door URLs te openen in Microsoft Edge, een browser die ook onder de veilige bubbel valt, wordt de consistentie van de beveiligingsmaatregelen gehandhaafd.

Ontwerpbesluit

Voor toegang tot zakelijke applicaties zal een aanvullende verificatie vereist zijn, die kan worden uitgevoerd met biometrische gegevens zoals gezichtsherkenning of een pincode.
Motivatie
Het gebruik van biometrische gegevens of een pincode biedt een extra beveiliging laag en minimaliseert het risico op ongeautoriseerde toegang tot bedrijfsgegevens.