DE ULTIEME GIDS VOOR

HYBRIDE WERKEN

Een stap-voor-stap gids voor het navigeren door de jungle van het hybride werken.

Insight

Introductie

In maart 2020 ging hybride werken binnen enkele dagen van niche naar normaal. Het was waarschijnlijk de snelste verandering in ons werkgedrag die we ooit hebben gezien. Deze ongekende gebeurtenis heeft geleid tot een verschuiving in prioriteiten, niet alleen voor individuen, maar ook voor organisaties. Ons rapport, **Fixing the Disconnect Between IT and Business**, stelde vast dat: "83% van de bedrijfsleiders gelooft dat de manier van werken permanent is veranderd." Het is duidelijk dat dingen nooit meer hetzelfde zullen zijn – en dat we moeten plannen voor een verandering op lange termijn in werkpraktijken.

Voor veel bedrijven is het experiment voor werken op afstand een succes geweest. Volgens een **onderzoek van McKinsey** zullen negen van de tien organisaties in de toekomst werken op afstand en op locatie blijven combineren. Hybride werken blijft gewoon bestaan, dus bedrijven hebben een langetermijnplan nodig om tijdelijke oplossingen te ontwikkelen en permanente strategieën te implementeren.

Bedrijfsleiders hebben een effectieve hybride werkstrategie nodig die zal helpen om:

- werknemers de tools te geven die ze nodig hebben om productief te werken
- werknemers de kennis te geven die ze nodig hebben om naar hun beste vermogen te werken
- ervoor te zorgen dat IT-systemen schaalbaar en toekomstbestendig zijn
- te veel uitgeven aan software en devices te vermijden
- de cloudomgeving te optimaliseren voor waarde en prestaties
- het beveiligingsprofiel van de organisatie te maximaliseren

Inhoud

Uw cloudomgeving optimaliseren

1. Het juiste cloudmodel en de juiste leverancier kiezen
2. Uw cloud optimaliseren voor waarde en prestaties
3. Downtime minimaliseren dankzij 24/7-ondersteuning

De juiste tools kiezen

1. De juiste samenwerkingssoftware selecteren
2. Uw telefoniesysteem integreren
3. Uw team uitrusten met de juiste tools – voor minder
4. Eenvoudig overstappen naar Windows 11
5. Nieuwe technologie omarmen

Niemand achterlaten

1. Waarom u een adoptie- en change managementplan nodig hebt
2. Een Prosci ADKAR-change manegementplan implementeren

Blijf veilig

1. Houd uw perimeter veilig met een zero-trust-aanpak
2. Cloud-gebaseerde beveiliging
3. Ervoor zorgen dat iedereen zijn/haar steentje bijdraagt

Uw cloudomgeving optimaliseren

Cloudplatforms zijn bij uitstek geschikt voor het ondersteunen van hybride werken. Werknemers kunnen veilig werken vanaf elke locatie en ze kunnen de operationele kosten verlagen door de uitgaven aan apparatuur, infrastructuur op locatie en software te verminderen.

Volgens ons rapport **Is IT Failing the Cost Optimisation Challenge**: “61% van de organisaties hebben nog geen onderzoek gedaan naar de eisen die aan de IT-infrastructuur worden gesteld door werken op afstand.” Als u, net als veel andere bedrijven, aan het begin van de COVID-19-pandemie snel naar de cloud moest migreren, is dit het moment om een stapje terug te doen en naar uw langetermijnplan te kijken. En zelfs als u al een cloudstrategie had, moet u deze bekijken om ervoor te zorgen dat deze voldoet aan uw nieuwe prioriteiten en uw mogelijkheid ondersteunt om flexibel, hybride werken op afstand aan te bieden.

De beslissing welke workloads te migreren naar de cloud en de keuze voor een public, private of hybride benadering zijn een goed begin. Er is geen one-size-fits-all-oplossing, maar met de juiste ondersteuning kan navigeren door uw migratie eenvoudiger worden gemaakt.

> “61%
> van de organisaties heeft nog geen onderzoek gedaan naar de eisen aan de IT-infrastructuur als gevolg van veranderingen in werken op afstand.”

1. Het juiste cloudmodel en de juiste leverancier kiezen

Migreren naar de cloud zonder de juiste expertise kan leiden tot te hoge uitgaven en beveiligingsissues, vooral als u gebruikmaakt van een eenvoudige 'lift-and-shift'-benadering. Cloudgebruik kan op- en afschalen en zonder het juiste inzicht en governance kunnen kosten onvoorspelbaar worden. Processen moeten mogelijk evolueren en werknemers zullen zich moeten aanpassen, wat leidt tot onzekerheid.

Hier zijn een paar dingen die u moet overwegen:

Beveiliging

Begin met het begrijpen van uw eigen beveiligingsdoelen en zet deze vervolgens af tegen de voorzieningen die door elke cloudprovider worden aangeboden. Zorg ervoor dat u begrijpt welke beveiligingsgebieden worden gedekt en welke uw verantwoordelijkheid blijven. Kijk welke beveiligingsfuncties zijn inbegrepen en welke beschikbaar zijn als betaalde extra's.

Compliance

Als u gevoelige gegevens in de cloud opslaat, moet u ervoor zorgen dat uw platform voldoet aan de juiste normen, zoals AVG (Algemene Verordening Gegevensbescherming) en PCI DSS (Payment Card Industry Data Security Standard). Nogmaals, u moet begrijpen welke bescherming wordt geboden door uw cloudhost en wat uw verantwoordelijkheid is.

Architectuur

Het is zeer waarschijnlijk dat u al afhankelijk bent van verschillende cloudplatforms. Als u uw workloads wilt verplaatsen naar een enkele cloudprovider, zijn er verschillende belangrijke overwegingen om aan te pakken, waaronder welk implementatiemodel u moet gebruiken (IaaS, SaaS of PaaS), hoe uw bestaande systemen zullen integreren met het door u gekozen platform, hoe u gevoelige gegevens zult beschermen en meer.

U kunt ook kiezen voor een hybride aanpak, meer beveiligingsgerichte workloads op uw on-premise servers houden en de cloud implementeren voor minder gevoelige data. Of u kunt besluiten om de optimale prestaties voor elke workload te krijgen en de beste kostenbesparingen te benutten, u wilt een multicloud-aanpak toepassen. Welk model u ook kiest, het moet het resultaat zijn van planning, niet van improvisatie.

Kosten

Bij het kiezen van een nieuwe cloudprovider is het essentieel om alle kostenfactoren te overwegen. Aangezien de belangrijkste spelers echter allemaal zeer verschillende prijsmodellen hebben, kan het lastig zijn om ze rechtstreeks te vergelijken. Een betere aanpak is om uw voorspelde gebruikspatronen te overwegen en te zien welk betalingsmodel van de leverancier het beste bij u past.

Dit zijn slechts enkele overwegingen. Er zijn er nog veel meer, waaronder serviceniveaus, ondersteuning en toekomstbestendig maken. Als u niet over de expertise beschikt om een volledige interne beoordeling uit te voeren, zoek dan een leverancieronafhankelijke cloudprovider die u kan helpen de risico's en de mogelijkheden te identificeren en een gestructureerd plan te ontwikkelen. Dit stelt u in staat om workloads en diensten op een gecontroleerde en zekere manier naar de cloud te verplaatsen.

2. Uw cloud optimaliseren voor waarde en prestaties

Gartner zegt het volgende: “Om optimaal te profiteren van cloudmogelijkheden is het essentieel om het model te begrijpen en realistische verwachtingen te hebben. U kunt niet zomaar alles naar de cloud verplaatsen en verwachten dat u dan klaar bent.” Bovendien, zelfs als u de best practices hebt gevolgd tijdens uw eerste implementatie, kan uw gebruiksmodel inefficiënt worden, kunnen de prestatieniveaus dalen en kan de beveiliging worden aangetast terwijl u nieuwe workloads naar de cloud blijft verschuiven.

Om ervoor te zorgen dat u de best mogelijke prestaties krijgt, moet u rekening houden met de voortdurende ontwikkeling van nieuwe services en platforms door cloudserviceproviders. Wat mogelijk ooit de best mogelijke implementatie was, moet zich blijven ontwikkelen om optimaal gebruik te blijven maken van de services die nu beschikbaar zijn. Om de beste waarde te krijgen, moet u ook het juiste model gebruiken voor uw huidige vereisten. Maar dit kan moeilijk zijn vanwege de complexiteit van cloudprijzen en facturering. Het is ook essentieel om goed op uw beveiliging te blijven letten tijdens de ontwikkeling van uw cloudplatform. U moet dan regelmatig het beveiligingsbeleid en de processen bestuderen, evenals de manier waarop u uw gebruikers, apps en devices beheert.

Het uitvoeren van cloud-optimalisatie op eigen locatie ligt buiten de scope van de IT-teams van de meeste organisaties. Het landschap ontwikkelt zich snel en er zijn gespecialiseerde kennis en tools nodig. De meest effectieve manier om uw cloudprestaties te optimaliseren is het gebruik van een externe leverancier die al geïnvesteerd heeft in het ontwikkelen van kostenoptimalisatiemogelijkheden voor public cloud-services.

3. Downtime minimaliseren dankzij 24/7-ondersteuning

Vergeet bij het beoordelen van de kosten van een nieuw cloudplatform niet om onderhoud daarin te betrekken. Het management van cloudservices en datacenters kan een grote last zijn voor uw IT-afdeling, vooral als het nodig is om aandacht te besteden aan meerdere technologieën en leveranciers. Het aannemen van nieuwe medewerkers met de juiste expertise (of het betalen voor doorlopende training) kan duur zijn. Een betaalbaar alternatief is het gebruik van een derde partij met alle kennis en ervaring voor uw ondersteuning.

Het kiezen van een partner voor uw cloudondersteuning:

- Geeft u toegang tot de expertise die u nodig hebt.
- Vermindert uw afhankelijkheid van uw eigen team en minimaliseert zo mogelijke onderbrekingen en uitvaltijd.
- Voorkomt de noodzaak om uw eigen supportteam op te schalen naarmate uw cloudgebruik groeit.
- Zorgt ervoor dat uw eigen team zich kan concentreren op het beheer en de innovatie, waardoor meer waarde wordt teruggebracht in uw bedrijf.

Zoek een partner die al uw supportcontracten in één kan te consolideren, zodat u ook issues met betrekking tot meerdere technologieën via slechts één organisatie kan afhandelen, wat de interne efficiëntie verhoogt.

Klik hier voor meer informatie.

“49% van de werknemers in het Verenigd Koninkrijk zal “waarschijnlijk van baan veranderen als ze gefrustreerd raken door technologie waarmee ze werken.”

De juiste tools kiezen

1. De juiste samenwerkingssoftware selecteren

Sinds het begin van de COVID-19-pandemie heeft technologie een aanzienlijk grotere rol gespeeld in de tevredenheid van werknemers. Volgens het **2021 Adobe State of Work Report** zal 49% van de werknemers in het Verenigd Koninkrijk “waarschijnlijk hun baan opzeggen als ze gefrustreerd raken door technologie waarmee ze moeten werken.” Dat is een toename van 33% in vergelijking tot voor de pandemie. Als uw organisatie het juiste talent wil aantrekken en behouden, moet u zorgvuldig overwegen welke samenwerkingstools u gebruikt.

Microsoft Office 365 is een van de sterkste oplossingen die er zijn. De bekendste functies, Teams en OneDrive, kunnen genoeg zijn voor veel organisaties. Anderen hebben mogelijk de extra functionaliteit nodig die wordt geboden door Azure Virtual Desktops (AVD), die is gebundeld met de Microsoft 365 E3- en E5-licenties voor ondernemingen. Dus hoe beslist u wat voor u het beste is?

Met Teams en OneDrive kunnen uw werknemers veilig inloggen vanaf elke locatie, op elk device en toegang krijgen tot werkdocumenten die veilig in de cloud zijn opgeslagen. Ze kunnen ook moeiteloos communiceren via chat, spraak of videoconferenties. De hosting wordt allemaal voor u gedaan, dus u hoeft niet te betalen voor een dure opslagoplossing. Een ander voordeel van Teams en OneDrive is dat ze deel uitmaken van het uitgebreide ecosysteem van Microsoft en profiteren van de geavanceerde beveiligingsmogelijkheden.

Azure Virtual Desktops hebben een andere aanpak. Uw werknemers gebruiken hun thuiscomputer om in te loggen op een externe server die een virtuele machine host. Dit heeft het grote voordeel dat werknemers toegang krijgen tot werkspecifieke apps. Het is dus een betere oplossing voor werknemers die toegang nodig hebben tot back-endsystemen. Als u bovendien een virtuele desktop gebruikt die wordt gehost in Azure en u deelt een document met een andere gebruiker in uw organisatie die zich ook op een virtuele machine in Azure bevindt, verlaat het document nooit uw privécloud, waardoor uw beveiligingsprofiel wordt versterkt. Virtuele desktops vereisen echter wel meer opslagcapaciteit, waardoor ze duurder kunnen zijn om te onderhouden.

Er zijn natuurlijk nog veel meer mogelijkheden. Als u niet zeker weet wat de juiste oplossing voor u is, zoek dan een partner die u kan helpen bij het beoordelen van uw huidige positie met betrekking tot de gewenste resultaten en u kan helpen bij het verkennen van de verschillende opties om hiaten te overbruggen.

2. Uw telefoniesysteem integreren

Een andere factor die de ervaring en efficiëntie van werknemers kan beïnvloeden, is de proliferatie van communicatiemiddelen op de werkplek. Door uw telefoniesysteem te integreren met uw interne samenwerkingssoftware kunt u het aantal kanalen verminderen dat uw werknemers nodig hebben om al hun communicatie te controleren en ze in staat te stellen om al hun communicatie te beheren via één enkele app.

Het integreren van uw interne en externe communicatiekanalen met een oplossing zoals 8x8 Voice voor Microsoft Teams heeft ook andere voordelen:

- Microsoft Teams-gebruikers hebben toegang tot het openbare telefoonnetwerk (PSTN) via de bekende Teams-interface – met spraakoproepen van topniveau naar 120 landen en onbeperkte belplannen in 47 landen.
- Uniforme platforms zoals 8x8 worden geleverd met een native contactcenteroplossing die kan worden geïntegreerd met Teams. Hierdoor kunnen uw agenten communiceren met zowel klanten als back-endteams, met behulp van de bekende Teams-interface, waardoor ze een betere service kunnen bieden. Bovendien integreert de 8x8-oplossing met meer dan 35 bedrijfsapplicaties, waaronder Salesforce en Zendesk, waardoor de efficiëntie van uw teams verder wordt verhoogd en de dienstverlening wordt verbeterd.
- Door uw telefoniesysteem te integreren met Teams, kunt u met uw CRM en uw contactcentrum gegevens verzamelen en analyseren over zowel interne als externe communicatie in één systeem, waardoor u meer inzicht krijgt in waar efficiëntieverbeteringen kunnen worden gerealiseerd.

De echte schoonheid van de oplossing is echter de eenvoud. Omdat hybride werk de norm wordt, is het logisch om toegang te hebben tot al uw communicatieplatforms en zakelijke apps op één bekende interface, die u kunt openen vanaf elk verbonden device.

3. Uw team uitrusten met de juiste tools – voor minder

Volgens ons rapport **Faalt IT in de uitdaging van kostenoptimalisatie** "staat 95% van de organisaties onder druk om kosten te verlagen, of wordt verwacht dat dit binnenkort zal gebeuren." Terwijl we ons aanpassen aan de nieuwe realiteit van hybride werken, moeten we nadenken over hoe we werknemers de juiste hardware bieden om hen in staat te stellen verbonden, productief en veilig te blijven – maar we moeten ook manieren vinden om kosten te besparen. Het oude inkoopmodel, waarbij we vooraf betalen voor devices, ze uitpersen totdat ze niet langer levensvatbaar zijn en vervolgens betalen om ze weg te gooien, heeft zijn langste tijd gehad. Vooruitstrevend denkende bedrijven stappen weg van de traditionele eigendomsbenadering naar een moderne aanpak van de hardware-lifecycle. Dit is hoe het Agile Lifecycle-model van Insight zich verhoudt tot het traditionele CAPEX-model.

> "95%
> van de organisaties staat onder druk om de IT-kosten te verlagen of verwacht dat binnenkort"

TRADITIONEEL CAPEX-MODEL	STADIUM VAN DE REIS	MODEL VOOR FLEXIBELE LIFECYCLE
	Acquisitie	
U kiest een device dat voldoet aan de behoeften van al uw gebruikers (waarschijnlijk wordt dit te veel gespecificeerd voor sommige gebruikers en te weinig voor anderen).	Kiezen	We kijken naar uw hele organisatie, maken een persoonlijk overzicht en selecteren drie of vier devices die zijn afgestemd op die personen.
U koopt meer devices dan u nodig hebt om vervangingen mogelijk te maken in geval van storing of verlies.	Inkoop	We gebruiken onze koopkracht om de devices tegen de beste prijs te kopen. U betaalt voor wat u gebruikt.
U betaalt vooraf voor alle devices die u nodig hebt, tegen de volledige prijs.	Betaling	U betaalt een maandelijks bedrag over een periode van drie jaar, verminderd om de restkosten van de devices te vergoeden. U betaalt 85% van de volledige prijs van de devices.
	Management	
Uw IT-team besteedt weken aan het instellen van devices, het toevoegen van de software en het configureren ervan, en levert deze vervolgens aan de eindgebruikers.	Device instellen	We kopen en integreren de vereiste software op uw devices en configureren deze voor u. Ze worden naar eindgebruikers gestuurd, klaar voor gebruik, direct uit de doos.
Uw IT-team beheert meerdere garanties en doet zaken met meerdere externe leveranciers. Vervangende devices moeten opnieuw worden geconfigureerd.	Onderhoud	Wanneer een device niet meer werkt, nemen we het terug en verzenden we een vervanging uit voorraad, volledig gepersonaliseerd en klaar voor gebruik. We gaan dan voor u in gesprek met de leverancier.
Uw IT-team ondersteunt gebruikers op alle devices. Uw IT-team moet regelmatig opnieuw trainen en moet mogelijk op ongebruikelijke uren werken.	Support	Wij bieden u 24/7/365 ondersteuning via één enkel contact voor al uw IT-behoeften, inclusief devices, datacenter en cloudinfrastructuur.
	Vernieuwing	
Wanneer uw devices niet langer nuttig zijn, moet u betalen om ze veilig van de hand te doen. De devices kunnen op de vuilstortplaats terechtkomen.	Einde van de lifecycle van het device	We halen uw devices terug en zorgen ervoor dat ze veilig worden opgeschoond en gereviseerd of gerecycled.

Zoals u kunt zien, is het flexibele model veel efficiënter, handiger en nog milieuvriendelijker. Het is ook veel beter geschikt voor een verspreid, hybride personeelsbestand - en stelt u in staat om zo snel als nodig op en af te schalen.

4. Eenvoudig overstappen naar Windows 11

Windows 11 komt eraan. Microsoft heeft het besturingssysteem op 24 juni 2021 onthuld en heeft een aanwijzing gegeven voor een mogelijke releasedatum van oktober van hetzelfde jaar. Van wat we al weten, lijkt het heel erg ontworpen te zijn met het hybride werkmodel in het achterhoofd.

Enkele functies die aantrekkelijk zijn voor mensen die op afstand werken, zijn:

- "De veiligste release tot nu toe" volgens Microsoft: een extra beschermingslaag voor externe werknemers.
- Optimalisatie voor tablet en touch, zodat gebruikers productief kunnen werken vanaf elk verbonden device.
- "Snap lay-outs" – biedt meer opties voor het ordenen van vensters op een enkel scherm en stelt gebruikers in staat om te multitasken met toegang tot slechts één scherm.
- Integratie van Teams – gebruikers kunnen rechtstreeks vanuit het dock toegang krijgen tot teams.

Dit zijn slechts enkele van de functies die aangeven dat Windows 11 hybride-vriendelijk zal zijn. Net als bij alle Windows-updates begint de upgrade als een 'leuke om te hebben' en naarmate de ondersteuning voor Windows 10 afneemt, wordt de upgrade geleidelijk een noodzaak. Ondanks de voordelen stellen veel organisaties de upgrade echter uit vanwege de waargenomen problemen. Maar dat hoeft niet zo te zijn.

Hier zijn een paar dingen die u kunt doen om het proces gemakkelijker te maken:

- De migratie uitbesteden aan een derde partij. Als uw organisatie multinationaal is, zorg er dan voor dat u een partner selecteert die wereldwijd aanwezig is.
- Overweeg het gebruik van implementatiegroepen als u zich zorgen maakt over verstoring. Upgrade gebruikers met een laag risico eerst en breid vervolgens geleidelijk uit naar het bredere team.
- Gebruik een tech partner als u aangepaste apps hebt die niet compatibel zijn met Windows 11 en u ze niet wilt herschrijven.
- Als u intern wilt upgraden naar Windows 11, is de beste aanpak het automatiseren van het proces met behulp van Systems Centre Configuration Manager (SCCM) of Intune. Als u deze tools niet hebt, kan een derde partij (zoals Insight) ze voor u implementeren. Door SCCM te installeren, wordt het eenvoudiger om uw bedrijfsmachines te beheren en verdere upgrades toe te passen.

5. Nieuwe technologie omarmen

Omdat hybride en werken op afstand de norm wordt, kunnen nieuwe digitale technologieën zoals Augmented Reality (AR) en Virtual Reality (VR) helpen bij het overbruggen van de fysieke kloof tussen werknemers.

Artsen in het **Alder Hey Children's Hospital** gebruiken bijvoorbeeld de Hololens 2-headset met **Microsoft Dynamics 365 Remote Assist** om in realtime te communiceren en informatie te delen met andere artsen.

"Ik was in de operatiekamer en voerde een complexe reparatie uit aan een klein hart, niet groter dan een aardbei. Door de HoloLens te gebruiken, konden we het beeld van het hart live naar andere collega's verzenden en tegelijkertijd het echocardiogram bekijken."

Rafael Guerrero, directeur harteenheid, klinisch directeur innovatie en hoofd aangeboren hartchirurgie

AR-technologie is ook zeer nuttig voor trainingsdoeleinden. Toen een toonaangevende Amerikaanse kruidenier nieuwe klantafhandelingscentra wilde uitrollen, liep het tegen problemen op omdat de ervaren ingenieurs van het bedrijf allemaal in Europa waren gevestigd en reisbeperkingen dreigden het project uit te stellen. Het **Digital Innovation**-team van Insight werkte samen met de klant om een AR-trainingsprogramma te creëren en het te leveren via **Microsoft Remote Assist** en **HoloLens 2**. Met behulp van AR konden de eigen ingenieurs van het bedrijf het lokale team bijscholen en de nieuwe klantafhandelingscentra zonder vertraging operationeel krijgen.

AR kan ook worden gebruikt om unieke, virtuele vergaderruimten te creëren, waardoor teams beter kunnen communiceren en samenwerken dan alleen via videoconferenties. Het Insight-managementteam nam deel aan een pilotprogramma met Oculus for Business-headsets en VR/AR-software, waardoor ze in staat waren om elkaar te ontmoeten en te communiceren in een virtuele ruimte - zonder de noodzaak om te reizen. De technologie, die meestal wordt geassocieerd met gamen, stelt deelnemers in staat om virtuele avatars te creëren die tot leven komen wanneer ze praten, bewegen en communiceren.

Deze technologieën lijken vandaag de dag misschien futuristisch, maar zullen al snel gemeengoed worden. Zelfs zonder sociale afstand en reisbeperkingen zijn de voordelen van minder reizen, verbeterde samenwerking en de mogelijkheid om te overleggen met specialisten over de hele wereld, moeilijk te negeren.

Klik hier voor meer informatie.

Niemand achterlaten

1. Waarom u een adoptie- en change managementplan nodig hebt

Technologie kan veel doen om de uitdagingen van hybride werken aan te gaan, maar tenzij uw team het omarmt, zal het onvermijdelijk tekortschieten op het potentieel om waarde toe te voegen aan uw bedrijf. Volgens McKinsey, "**veranderen organisaties niet, mensen veranderen**."

Prosci, 's werelds toonaangevende specialisten op het gebied van change management, stelt dat het implementeren van nieuwe technologie en processen zonder change management kan leiden tot:

- Mislukte projectresultaten
- Uitgebreide projectschema's
- Bijkomende projectkosten
- Lage adoptie en gebruik

Maar met een change management- en adoptiestrategie, hebt u:

2. Een Prosci ADKAR-change manegementplan implementeren

Bij Insight raden we aan om het **Prosci** ADKAR-model (Awareness, Desire, Knowledge, Ability and Reinforcement) te volgen voor change management. Elke fase van het model is even belangrijk voor het proces.

In de **Awareness-fase** willen we uw teams laten weten dat er verandering komt. Kies voor de beste practices een gerespecteerde persoon binnen uw organisatie als pleitbezorger voor de verandering (zoals een CTO) en stuur alle communicatie vanuit hen.

In de **Desire-fase** moet u de voordelen van de verandering, of nieuwe technologie, aan het team communiceren. Gebruik video's en e-mails om de voordelen te communiceren – zowel aan eindgebruikers als aan het bedrijf.

In de **Knowledge-fase** moet u het personeel de juiste training geven. Toen Insight bijvoorbeeld met één bedrijf werkte aan een adoptiestrategie voor Microsoft Teams, trainden we vrijwilligers binnen het bedrijf om super-users te worden. We gaven werknemers toegang tot een portal met alle leermaterialen die ze nodig hadden om deskundige Teams-gebruikers te worden, en de super-users hielpen hen om aan de slag te gaan met Teams en in te loggen op de portal.

Na Knowlegde komt **Ability**. Naast het verstrekken van informatie, moet u het personeel de ondersteuning bieden die ze nodig hebben om optimaal te profiteren van materialen. In het bovenstaande voorbeeld heeft het change managementteam van Insight vragen van personeel afgehandeld door samen te werken in Microsoft Teams en ervoor te zorgen dat er geen technische blokkades waren voor de leervoortgang van werknemers.

De **Reinforcement-fase** is van vitaal belang om het voortdurende succes van het project te garanderen. In ons Teams-voorbeeld bleven super-users het gebruik van alle Teams-capaciteiten promoten en hebben managers het gebruik gemeten om ervoor te zorgen dat afdelingen voldoen aan de adoptie-KPI's. De CIO van het bedrijf hield werknemers ook op de hoogte van het succes van het project en de voortdurende waarde ervan voor het succes van het bedrijf. Het resultaat van het project was dat het gebruik van Teams in minder dan drie maanden van 28% naar 75% ging – duidelijk bewijs dat het implementeren van technologie alleen geen verandering kan garanderen.

Klik hier voor meer informatie.

Blijf veilig

1. Houd uw perimeter veilig: een zero-trust-aanpak

Met een geografisch verspreid personeelsbestand wordt uw cyberbeveiligingsperimeter groter en een bedrijfsfirewall is niet langer voldoende om u te beschermen tegen cyberaanvallen. Om deze perimeter veilig te houden, hanteren veel organisaties een ‘zero-trust’ aanpak. Eenvoudig gezegd betekent dit dat u niets vertrouwt binnen of buiten de firewall van uw organisatie.

In praktische termen kan de zero-trust-benadering volgens Microsoft worden onderverdeeld in drie stappen:

1. Verificatie: bevestig altijd de identiteit van een gebruiker of machine die toegang tot gegevens nodig heeft. Gebruik een sterke identiteitscontrole zoals multifactor authenticatie voor eindgebruikers.
2. Toegangscontrole: geef gebruikers of machines nooit meer toegangsrechten dan ze absoluut nodig hebben.
3. Schadebeperking: ga ervan uit dat er een inbreuk zal plaatsvinden. Segmenteer toegang zodat een kleine inbreuk niet kan leiden tot een grotere inbreuk.

Als u niet zeker bent van uw vermogen om een zero-trust-aanpak te implementeren, praat dan met een derde partij met de juiste expertise. **Insight Security Services** kan u helpen met alle aspecten van het beveiligen van uw externe werknemers, waaronder het instellen van multifactor authenticatie en ervoor zorgen dat alle endpoints worden beschermd.

2. Cloud-gebaseerde beveiliging

Het is een gemeenschappelijke veronderstelling dat door uw bedrijfsdata naar de cloud te verplaatsen, u deze automatisch veiliger maakt. Hoewel de data mogelijk veilig zijn in een clouddatabase, loopt deze nog steeds risico tijdens de overdracht tussen gebruikers en organisaties. Het kan ook kwetsbaar zijn in rust, bijvoorbeeld wanneer het wordt geopend door een eindgebruiker. Om data volledig veilig te houden, moet u het hele dreigingslandschap bekijken, niet alleen uw dataopslagoplossing.

De meeste grote organisaties vertrouwen op Security Information and Event Management (SIEM) en Security Automation Orchestration and Response (SOAR)-software om cyberbeveiligingsdreigingen te volgen en erop te reageren. SIEM-software bewaakt het dreigingslandschap, categoriseert en analyseert beveiligingsgebeurtenissen, biedt beveiligingsrapporten en stuurt waarschuwingen die ongebruikelijke activiteiten markeren, SOAR-software automatiseert en beheert enkele van de tijdrovende, handmatige taken die betrokken zijn bij het reageren op geïdentificeerde bedreigingen.

Voor een grote organisatie kunnen de initiële software- en hardwarekosten voor SIEM en SOAR echter gemakkelijk oplopen tot £ 200.000. En, net als bij elke on-premise oplossing, zijn er problemen met toekomstbestendigheid en schaalbaarheid. Met de snelheid waarmee technologie zich in de 21e eeuw ontwikkelt, loopt elke grote hardware-upgrade het risico verouderd te raken voordat het zijn doel heeft bewezen.

Er is een alternatief dat de voordelen van SIEM en SOAR kan bieden, zonder de investering vooraf of een toegewijd team van IT-beveiligingsspecialisten. Met een cloudgebaseerd beveiligingssysteem heeft uw organisatie toegang tot alle analytische en organisatorische mogelijkheden van SIEM en SOAR zonder de voorafgaande investering in hardware. De software wordt virtueel gehost, in de cloud.

Zoals bij veel cloud-first oplossingen, zijn de directe verkoopargumenten slechts het uitgangspunt. Een cloud-first beveiligingssysteem is niet alleen de meest betaalbare oplossing, het is ook de meest effectieve.

Azure Sentinel van Microsoft is een klassiek voorbeeld van een grootschalige cloud-first-oplossing die drastische verbeteringen in uw beveiliging kan bieden. Terwijl een lokale SIEM-oplossing het dreigingslandschap analyseert op basis van uw eigen gegevens, heeft Sentinel toegang tot biljoenen operaties over de hele wereld, waardoor het veel meer informatie krijgt om aan te werken. Een lokale SIEM kan bijvoorbeeld detecteren dat malware afkomstig is van een phishing-e-mail en vervolgens die e-mail van andere machines blokkeren. Dankzij de toegang van Microsoft tot grootschalige clouddata, zou Azure Sentinel de phishingbedreiging bijna zeker hebben waargenomen en geblokkeerd voordat het zelfs maar bij uw organisatie terechtkwam.

In vergelijking met het opzetten van een on-premise beveiligingssysteem, is aan de slag gaan met Azure Sentinel relatief eenvoudig. Alles is al ingesteld in de cloud en u betaalt gewoon voor wat u nodig hebt. Maar net als bij on-premises SIEM- en SOAR-systemen moet u nog steeds een toegewijd team hebben om het te beheren. Door een stap verder te gaan en over te stappen op een oplossing voor beveiliging als service (zoals **Insight’s Managed Security Services voor Microsoft Sentinel**) kan uw organisatie ook de noodzaak vermijden om een gespecialiseerd IT-team te onderhouden.

3. Ervoor zorgen dat iedereen zijn/haar steentje bijdraagt

Zelfs met een zero-trust-aanpak en een intelligent, cloudgebaseerd beveiligingssysteem kunt u nog steeds risico lopen. Beveiliging is niet alleen een technisch probleem. Het is ook een probleem van mensen. Het veilig houden van een organisatie vereist dat alle mensen in die organisatie zich bewust zijn van beveiliging. Om deze bedreiging te beperken, moet u regelmatig training geven over belangrijke beveiligingsmaatregelen om ervoor te zorgen dat elke werknemer de rol die hij/zij speelt kent. Voor de best practices kunt u online trainingsmodules geven en uw personeel testen om ervoor te zorgen dat ze het materiaal hebben gelezen en begrepen. Cyberbeveiliging ontwikkelt zich voortdurend, dus zorg ervoor dat uw training up-to-date is.

Enkele van de belangrijkste dingen waar uw personeel zich bewust van moet zijn, zijn:

- Het belang van het maken van back-ups van werk in de cloud. Hierdoor kunt u blijven werken in het geval van een ransomware-aanval.
- De dreiging van malware. Installeer altijd de nieuwste softwarepatches en updates en download alleen software van vertrouwde bronnen.
- De behoefte aan sterke wachtwoorden. Gebruik een wachtwoordmanager om ze aan te maken en op te slaan en u hoeft slechts één sterk wachtwoord te onthouden.
- De tekenen van phishing-aanvallen. Klik nooit op een link tenzij u 100% zeker bent van de authenticiteit ervan – en neem bij twijfel contact op met de afzender.

Het produceren van trainingsmateriaal en het up-to-date houden van uw team met de nieuwste best practices op het gebied van cyberbeveiliging is een proces dat veel middelen bevat. Veel organisaties besteden hun training uit aan deskundige leveranciers die al trainingsmateriaal hebben.

Een **Insight Security Awareness Assessment** helpt u bij het realiseren van een beveiligingsbasis, het selecteren en aanmaken van sponsors, het opzetten van beveiligings 'champions' het opstellen van een trainingsprogramma, het ontwikkelen van een communicatieplan en het beheren van alle andere aspecten van veranderings- en weerstandsbeheer.

Klik hier voor meer informatie.

Alles bij elkaar brengen

Zoals u kunt zien, is er veel om rekening mee te houden bij het plannen voor doorlopend succes in de hybride jungle. Maar het goede nieuws is dat we hier zijn als uw partner om u bij elke stap te begeleiden.

Wij kunnen u helpen bij het identificeren en verkrijgen van de beste tools voor uw team en met u samenwerken om ervoor te zorgen dat u de volledige waarde uit uw investering haalt. Wij kunnen u helpen ervoor te zorgen dat uw IT-systemen schaalbaar en toekomstbestendig zijn. We kunnen u helpen te voorkomen dat u te veel uitgeeft aan software en devices door het oude CAPEX-model te verlaten en een meer flexibele benadering van inkoop te gebruiken. En we kunnen u helpen bij het kiezen van het juiste cloudplatform en het optimaliseren voor zowel prestaties als waarde. En natuurlijk kunnen we u helpen om te gaan met het verhoogde beveiligingsrisico van een geografisch verspreid personeelsbestand.

Dit zijn slechts enkele van de manieren waarop we u en uw bedrijf kunnen helpen niet alleen te overleven, maar ook de koning van de hybride jungle te worden. Als u hulp nodig hebt bij een van de bovenstaande problemen, aarzel dan niet om contact op te nemen.

Boek vandaag nog een afspraak met een Insight-specialist.

Insight