Security Update

Apple devices gebruiken op het werk?

03 Pro Warehouse

Met deze hardware til jij jouw organisatie naar een hoger niveau

04 Managed Devices

Zakelijke MacBooks veilig en zorgeloos laten beheren?

12 Mac does that

Mac om loyaliteit te versterken: een win-win situatie

06 Security

Makkelijk(er) werken met veilige wachtwoorden



pro warehouse

Authorised Enterprise Reseller

Security Update

Deze editie van de Pro Update heeft het thema security. Een steeds belangrijker onderwerp voor alle bedrijven. Zeker nu er sinds een aantal jaar ook vanuit de Europese Unie een grote focus is op de beveiliging van bedrijfsnetwerken en met name data. Bedrijven moeten altijd alert zijn op mogelijke kwetsbaarheden. We gaan dieper op dit onderwerp in en leggen de focus op oplossingen om ervoor te zorgen dat jouw organisatie zo veilig mogelijk wordt.

We wensen je veel leesplezier en voel je vrij om deze te delen met mensen die je kent, of laat 'm ergens achter, zodat een ander hem weer kan lezen.

De Pro Update redactie

Wij versnellen de continuïteit van jouw bedrijf

Optimaliseer je bedrijfsvoering door rendement en continuïteit op Apple werkplekken te vergroten.

hardware

customer portal

- Altijd devices beschikbaar
- Inclusief accessoires
- On demand Apple devices
- Online inzicht in voorraad
- Managed Lifecycle

software

security

- Managed Workplace
- Patch management
- Managed Devices
- Licentieverkoop

services

logistics

- Verzending naar alle (thuis-) adressen binnen EU
- Asset management
- Assemblage

remote & onsite support

- Daily Server Backup
- Managed Devices
- Enduser Support

Meer weten?

Rick, IT-beheerder bij Quanza

"Je hoeft alleen maar het lijstje af te gaan en aan te geven: dit wil ik wel en dit wil ik niet."



Pro Warehouse

Met deze hardware til jij jouw organisatie naar een hoger niveau



MacBook en iPhone zijn enorm populair onder studenten, jonge werknemers, vormgevers en content creators. De afgelopen jaren heeft Apple een opmerkelijke verschuiving doorgemaakt in de zakelijke markt. Waar er voorheen een tweedeling bestond tussen Mac computers, die vooral gebruikt werden door vormgevers en designers en pc's met Windows, die op het bureau van de rest van het-op-kantoor-werkend-Nederland stonden, is er de laatste jaren duidelijk sprake van een shift.

Steeds meer bedrijven stappen massaal over op MacBook of Mac desktopcomputers. Zij ervaren dat Apple devices om meerdere redenen goed geschikt zijn voor uiteenlopende IT-vraagstukken. En dat een Apple device er dan ook nog eens strak en fraai uitziet, is zeker mooi meegenomen. Peter Bekkering, Business Development Manager bij Pro Warehouse – een Enterprise Reseller die als enige in Nederland 100 procent met Apple producten werkt, snapt de overstap wel: "Eén van de belangrijkste redenen voor de toenemende acceptatie van Apple in de zakelijke wereld, is de toegenomen focus op gebruiksvriendelijkheid en intuïtieve interfaces vanuit het bedrijf zelf. Apple staat al jaren bekend om zijn herkenbare design en gebruiksvriendelijke ervaring; een belangrijke eigenschap voor bedrijven die hun werknemers willen voorzien van productieve en efficiënte tools. Bovendien merken wij dat jongere werknemers steeds vaker om een MacBook vragen. Op die manier sijpelt er steeds meer Apple-DNA een organisatie binnen. Aan ons de taak om organisaties hierbij te helpen en te ontzorgen."

De naadloze integratie tussen hardware, software en services van Apple biedt een soepele en consistente ervaring, wat essentieel is in een zakelijke omgeving waar tijd en productiviteit van essentieel belang zijn. "Het klinkt misschien een beetje als wij van WC-Eend", lacht Bekkering, "maar Apple devices staan gewoon voor kwaliteit. Apple ontwerpt zelf de hardware en de software en dat merk je. De producten zijn perfect op elkaar afgestemd en het ecosysteem werkt naadloos met elkaar."

Veiligheid en mobiliteit

Daarnaast zijn Apple devices en besturingssystemen ontworpen met privacy en security ingebouwd. In een tijd van toenemende zorgen over beveiliging en cyberaanvallen, bieden Apple devices een sterk beveiligd ecosysteem dat aantrekkelijk is voor bedrijven die waarde hechten aan de bescherming van vertrouwelijke informatie. De introductie van functies zoals Face ID, de Secure Enclave en de Apple T2 Security-chip in Mac computers benadrukken dit. Een andere belangrijke factor die heeft bijgedragen aan de keuze voor Apple devices in de zakelijke wereld, is de groeiende populariteit van mobiele technologie. Smartphones en tablets zijn tegenwoordig onmisbare hulpmiddelen geworden voor werknemers om altijd en overal toegang te hebben tot informatie en om efficiënt te kunnen communiceren. Apple heeft met iPhone en iPad een sterke positie verworven in de mobiele markt en de naadloze integratie tussen deze apparaten en Mac computers heeft bedrijven aangespoord om voor een allesomvattende Apple ervaring te kiezen.

Impact van de cloud

Bovendien ziet Pro Warehouse dat er veel Apple devices zeer geschikt zijn voor het zakelijke segment. Met de introductie van producten zoals iPad Pro, die krachtige prestaties heeft en ondersteuning biedt voor de Apple Pencil, heeft Apple zich gericht op professionals in sectoren zoals design, architectuur en gezondheidszorg. Daarnaast zijn er samenwerkingstools zoals iCloud Drive en iWork en sluiten Apple devices naadloos aan op apps van derden, waardoor het gemakkelijker is geworden voor bedrijven om efficiënt samen te werken en gegevens te delen.

"De cloud heeft sowieso een enorme impact gehad op de manier waarop we werken", stelt Bekkering. "Voorheen draaide software lokaal en dat was een beperkende factor. Iedereen moest met dezelfde hardware werken. Tegenwoordig maakt het met bijvoorbeeld een Office 365 niet meer uit op welk platform en welk apparaat je werkt. Het is allemaal compatible met elkaar. Met mobiel apparaatbeheer (MDM) en cloudgebaseerde beheerhulpmiddelen kunnen IT-teams Apple devices bovendien eenvoudig implementeren, configureren en beheren op schaal. Dit vereenvoudigt het beheer van Apple devices binnen bedrijfsomgevingen en maakt het gemakkelijker om updates, beleidsregels en beveiligingspatches toe te passen. "Veiligheid staat bij organisaties op nummer één, maar in de praktijk sluipen er soms slordigheden in het IT-beleid", aldus Bekkering. "Door gebruik te maken van onze Managed Devices en Managed Workplace zijn organisaties altijd safe én voorzien van de juiste apparatuur en tools. Of het nu gaat om het installeren van een nieuwe MacBook het reguleren van toegang tot de diverse cloudapplicaties of het beheren van updates en nieuwe instellingen, wij zorgen overal voor."

Kostenplaatje

Ook de kosten spelen mee in de overweging van veel organisatie om Apple producten aan te schaffen. Een MacBook is in aanschaf vaak duurder dan Windows laptops en computers, maar Apple producten gaan dan ook veel langer mee. "De hardware is aantoonbaar beter in kwaliteit", zegt Bekkering. "Er zijn minder reparaties nodig, wat weer leidt tot veel minder verstoring van de workflow. En door de langere levensduur van het product is de restwaarde van het product ook hoger, waardoor je uiteindelijk meestal goedkoper uit bent."

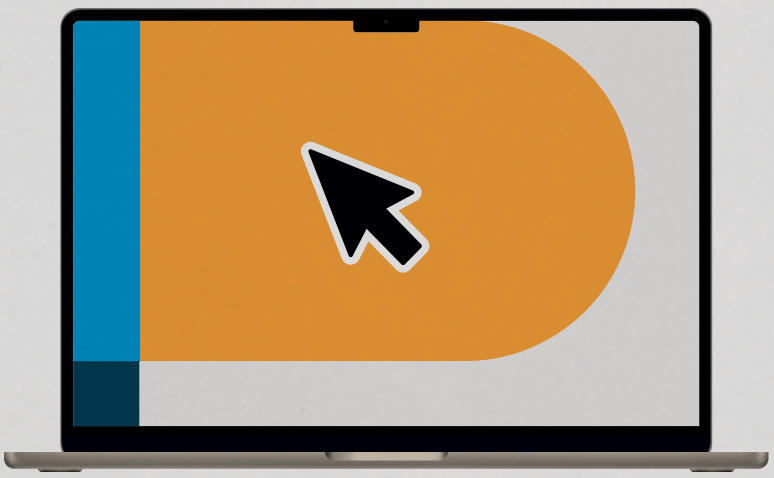
"Apple devices en besturingssystemen zijn ontworpen met privacy en security ingebouwd"

Corona als business driver?

Door corona kwamen we allemaal plotseling in ons thuiskantoor terecht. Dit heeft Pro Warehouse geen windeieren gelegd, want het gebruik van Apple devices steeg explosief. 60 à 70 procent van werknemers wereldwijd werkten in april en mei 2020 vanuit huis. Dat resulteerde ook in een stijging van het aantal aanvragen voor Apple producten door werknemers. In 2021 werd deze migratie een trend. Volgens het International Data Corporation (IDC) steeg het gebruik van macOS-apparaten in Amerikaanse ondernemingen naar 23 procent, terwijl iPhone goed was voor 49 procent van de zakelijke smartphones en iPad de meest gebruikte tablet op de werkplek was. "De groei van het gebruik van Apple devices onder zakelijke gebruikers, met name voor werknemers die op afstand werken en de keuze hebben uit verschillende apparaten, zette meer bedrijven ertoe aan om te kiezen voor macOS, samen met iOS/iPadOS en tvOS", aldus Phil Hochmuth, program vice president, Enterprise Mobility and Client Endpoint Management bij IDC.

Dit artikel is tot stand gekomen in samenwerking met Business Insider.

Zakelijke MacBooks veilig en zorgeloos laten beheren?



Het is voor het mkb zeer interessant om het installeren van nieuwe computers, het inregelen van de software en de beveiligingen, de updates en dagelijkse back-up uit te besteden aan gecertificeerde partners met kennis van Apple voor de continuïteit en groei van jouw bedrijf. Geen omkijken meer naar de juiste Apple werkplek zodat jij je kunt focussen op de aandacht die jouw klant verdient. Op het gebied van Apple devices is Pro Warehouse als Apple Autorised Enterprise Reseller de enige in Nederland die 100 procent focus heeft op Apple producten en diensten. Echte specialisten dus.

Managed Devices	Entry level	Advanced level	Pro level
Full Device Protection			
Mobile Device Management	✓	✓	✓
Patch Management	✓	✓	✓
24/7 Monitoring	✓	✓	✓
Quarantaine mogelijkheden	✓	✓	✓
Anti-Virus	✓	✓	✓
Anti-Spyware	✓	✓	✓
Anti-Malware	✓	✓	✓
Passwordmanager			✓
Installatie nieuw device	Per uur	✓	✓
Vast contactpersoon			✓
Support op afstand	Per uur	✓	✓
Support op locatie	Per uur	Per uur	✓
Online contact per jaar		2	
Consultant bezoek per jaar	1	2	4
Reiskosten en parkeerkosten	Per keer	Per keer	✓
Prijs per device per maand			
Per jaar vooruit gefactureerd	**€20**	**€30**	**€40**
Per maand achteraf gefactureerd	€22	€33	€44

“Er lopen bij ons veertig service engineers rond die heel veel ervaring hebben”, zegt Oskar Petersen, business development manager. Pro Warehouse biedt organisaties de optie om voor Managed Devices te kiezen en neemt ze daarmee veel werk uit handen.

“Voor een vast bedrag alle Apple devices altijd veilig en up-to-date”

“Voor een vast bedrag per maand hebben bedrijven geen omkijken meer naar hun Apple devices. Wij regelen de software, de security, alle belangrijke updates, de installatie van devices voor nieuwe werknemers en de vervanging van oudere apparatuur die vaak nog een hoge restwaarde heeft”, legt Petersen uit. “Binnen twintig minuten heeft iemand desgewenst een volledig nieuwe MacBook met alle gewenste software op kantoor staan. Dat scheelt bedrijven veel tijd en zorgen, waardoor de workflow nagenoeg onverstoord door kan gaan.”

Gemaakte kosten? Zakelijk aftrekbaar

Pro Warehouse werkt met drie levels van ondersteuning: Entry, Advanced en Pro level. Hoe hoger het niveau hoe uitgebreider de ondersteuning is. Bij het Pro level komt een vaste engineer vier keer per jaar fysiek langs, terwijl bij Entry en Advanced de bezoeken tot twee keer is beperkt en de overige contactmomenten telefonisch zullen plaatsvinden. Welk niveau je ook kiest, de gemaakte kosten zijn zakelijk aftrekbaar. Als zzp’er of mkb’er kan je ook in aanmerking komen voor de kleinschaligheidsinvesteringsaftrek. Deze regeling biedt een extra aftrekpost voor investeringen. Bij bedragen van €2.601 tot en met €63.716 mag je 28 procent van het investeringsbedrag aftrekken. Dat is nogal substantieel en komt boven op de hoge restwaarde van Apple producten, bij inruil of een upgrade naar een zwaardere MacBook.

Dit artikel is tot stand gekomen in samenwerking met Business Insider.

Meer weten?

pro warehouse

Choose Your Own Device-strategie bij Pro Warehouse



Het bieden van keuze aan medewerkers heeft verschillende voordelen. Natuurlijk hanteren we bij Pro Warehouse ook een strategie, Employee Choice. Steven van der Keur, manager engineering en Hans van der Linden, marketing manager bij Pro Warehouse, leggen dit concept uit.

"Ongeveer twee jaar geleden hebben we voor het eerst ons concept gelanceerd. We merkten aan onze medewerkers dat ze niet allemaal even tevreden waren over de MacBook Pro waarmee ze werkten. Op dat moment kreeg iedereen dezelfde laptop, met dezelfde hoeveelheid opslag en werkgeheugen én allemaal in dezelfde kleur. Sommige collega's hadden bijvoorbeeld continu last van een volle harde schijf en voor anderen was de laptop niet snel genoeg voor de veeleisende programma's die ze gebruiken. Ook kregen we vaker aanvragen voor speciale accessoires, want ja, ook daarvan kreeg iedereen precies hetzelfde. Als laatste vertelden we wel aan onze klanten dat een Choose Your Own Device-strategie een goede strategie is om te hanteren, terwijl we het zelf niet faciliteerden, dat is natuurlijk gek", vertelt Steven.

"Om een keuzestrategie op te kunnen zetten, hebben we eerst met een pilotgroep geïnventariseerd wat de wensen van medewerkers nu eigenlijk zijn. Hieruit bleek dat er best veel verschillende wensen en eisen zijn, die ook nog eens erg ver uit elkaar liggen. Daarom hebben we per afdeling, en soms per persoon, een budget vastgesteld. Sommige afdelingen of medewerkers hebben uiteindelijk toch een sterker device nodig dan anderen en daarom zit hier dus verschil in. Medewerkers kunnen dan hardware en accessoires bestellen tot het budget dat voor hun geldt. Zo kan iedereen precies de devices kiezen waarmee iemand graag wil werken", aldus Hans. Uiteraard zijn er ook een aantal regels. Zo dient men drie jaar met de laptop te doen en twee jaar met de gekozen telefoon. Ook moet het device waarop je wil werken draagbaar zijn om thuiswerken te kunnen faciliteren. "Als laatste kan je alleen kiezen voor Apple devices en accessoires die wij zelf in het assortiment hebben. We zijn immers volledig gefocust op Apple", vult Steven aan.

"Na verloop van tijd is het keuzeprogramma ook uitgegroeid met onze eigen lijn van werkkleding. Ook hiervoor kregen we vragen vanuit collega's voor herkenbare kleding. Als onze mensen bij een klant op locatie werken, dan willen ze goed herkenbaar zijn. We zijn hiervoor op zoek gegaan naar een kwalitatief goede kledingleverancier en maken dan een ruime voorselectie. Omdat de kleding bedrukt wordt, is het lastig om het volledige assortiment aan te bieden als keuze. Collega's kunnen dan weer, net zoals bij de hardware, voor een bepaald budget kleding bestellen in Pro Warehouse stijl. Dit kan op twee momenten. Vlak voor de zomer en voor de winter", vertelt Hans. "Dit is erg goed ontvangen en we krijgen regelmatig vragen voor nieuwe kleding of andere items. Ook hierin liggen de wensen van de verschillende medewerkers soms ver uit elkaar."

"Sinds een paar jaar is het ook bij ons mogelijk om thuis te werken. Na de verplichte lockdowns hebben we deze mogelijkheid gewoon doorgezet. We merkten namelijk dat collega's hierdoor meer vrijheid ervaarden en werkzaamheden beter konden indelen, zonder in te leveren op kwaliteit. Bij thuiswerken is het natuurlijk belangrijk dat je de juiste devices hebt, maar bijvoorbeeld ook dat je een goede ergonomische houding hebt, net als op kantoor. Om dit goed te faciliteren, bieden we een aantal opties aan", vertelt Steven. "Zo kunnen medewerkers een goede bureaustoel uitzoeken, leveren we monitors, keyboards en andere hardware én we geven een bijdrage voor een (sta-zit) bureau voor thuis."

"We hebben veel positieve reacties ontvangen van collega's over de keuzeprogramma's", zegt Hans. "Ze zijn zeer te spreken over de mogelijkheid om precies die devices te kunnen kiezen die zij nodig hebben. We zien bijvoorbeeld ook dat veel mensen ervoor kiezen om een MacBook Pro te combineren met een iPad Pro. Dat is natuurlijk ideaal als je veel onderweg bent of veel stukken door moet lezen." Steven vult aan: "de implementatie was in ons geval relatief eenvoudig. Voor het beheer van de devices hoefden we bijvoorbeeld weinig aan te passen, omdat iedereen hetzelfde besturingssysteem bleef gebruiken. Het zijn wel steeds meer devices geworden, want we zijn aan het groeien, zeker na de recente overnames."

"Zo kunnen medewerkers een goede bureaustoel uitzoeken, leveren we monitors, keyboards en andere hardware én we geven een bijdrage voor een bureau voor thuis."



Wil jij ook een CYOD-strategie in jouw organisatie? Download ons stappenplan om je te ondersteunen bij het bepalen van de juiste strategie.

Security

Makkelijk(er) werken met veilige wachtwoorden



Bij veel organisaties staat security onverminderd hoog op de agenda, vooral omdat het aantal bedreigingen snel toeneemt en traditionele beveiligingsoplossingen niet altijd meer voldoen. Onze field engineer Roy licht het onderwerp toe en deelt hoe hij security terugziet in zijn werkzaamheden.

Wanneer je een nieuwe Mac of iPhone uitpakt, zijn er direct al diverse beveiligingsfeatures ingebouwd. Bij de eerste opstart worden automatisch verschillende instellingen voorgesteld, die te maken hebben met beveiliging. Je kunt bijvoorbeeld een langere toegangscode instellen voor je telefoon, maar ook wordt je geadviseerd om je Apple ID in te stellen en 'Find My' te gebruiken. Daarnaast wordt aangeraden om FileVault in te schakelen en een herstelcode te gebruiken via iCloud, indien nodig. Met FileVault kun je de gegevens op je Mac beveiligen door ze te versleutelen. Het device begeleidt je meteen in het beveiligingsproces, zonder daarbij te dwingend te zijn.

Ingebouwde beveiliging

Apple devices zijn voorzien van ingebouwde beveiligingsinstellingen. Bij het opstarten wordt alleen vertrouwde Apple software geladen. De beveiliging begint met de onveranderbare code van het Boot-ROM. Op Mac met een Apple T2 Security-chip, zorgt de Secure Enclave voor veilige aanmelding via Touch ID of Face ID, zonder blootstelling van biometrische gegevens. Gebruikers profiteren van sterke en complexe toegangscodes en wachtwoorden, maar kunnen zich in de meeste gevallen toch snel aanmelden. Roy legt uit, "Wat ik heel sterk vind aan Apple devices, is dat zoveel mogelijk informatie lokaal verwerkt wordt. Bijvoorbeeld gezichtsherkenning in foto's. Dat doet jouw iPhone zelf. Deze gegevens worden nooit op een server opgeslagen, het gebeurt allemaal op jouw telefoon zelf. Hetzelfde geldt bijvoorbeeld voor de app HomeKit. Deze draait zoveel mogelijk lokaal, dus je bent en niet afhankelijk van het internet. Dat is natuurlijk een stuk veiliger en moeilijker te hacken.

Stel, je hebt een slim deurslot die werkt via HomeKit. Als deze eerst een signaal naar een server moet sturen, dan kan dat makkelijker opgepikt worden. Het HomeKit protocol is vanuit zichzelf versleuteld en dat is waarom je, toen HomeKit net op de markt kwam, zag dat er heel weinig apparaten gebruik van maakten. Het was eigenlijk zo veilig dat je een krachtige processor nodig had. In een device als een speaker werd dat vaak veel te duur."

Vervanging voor wachtwoorden

"Het meest voorkomende probleem is dat mensen hun wachtwoorden niet kunnen onthouden en dan maar doen wat voor hun de makkelijkste manier is. Wachtwoorden noteren op een post-it, in een notitie op hun telefoon of in een boekje. De ene manier is nog minder veilig dan de andere. Het addertje onder het gras? Mensen gebruiken onveilige en te makkelijk te raden wachtwoorden. En erger nog, ze hergebruiken dezelfde wachtwoorden op meerdere plekken.

Een handige optie om dit te ondervangen is 1Password. Zoals de naam al zegt, hoef je maar één wachtwoord te onthouden. Zorg er wel voor dat het wachtwoord niet makkelijk te raden is, het moet natuurlijk wel veilig zijn. Een goede manier om één wachtwoord te bedenken is door een unieke zin te gebruiken, die niet te achterhalen is. Met 1Password kun je ook notities maken, creditcardgegevens opslaan en zelfs je identiteitskaart bewaren. Als je 1Password gaat gebruiken, dan raad ik aan om alle automatische invulopties van bijvoorbeeld Safari uit te schakelen, zodat ze elkaar niet in de weg zitten. Dit is namelijk een veelvoorkomend probleem in de praktijk.

Passkeys

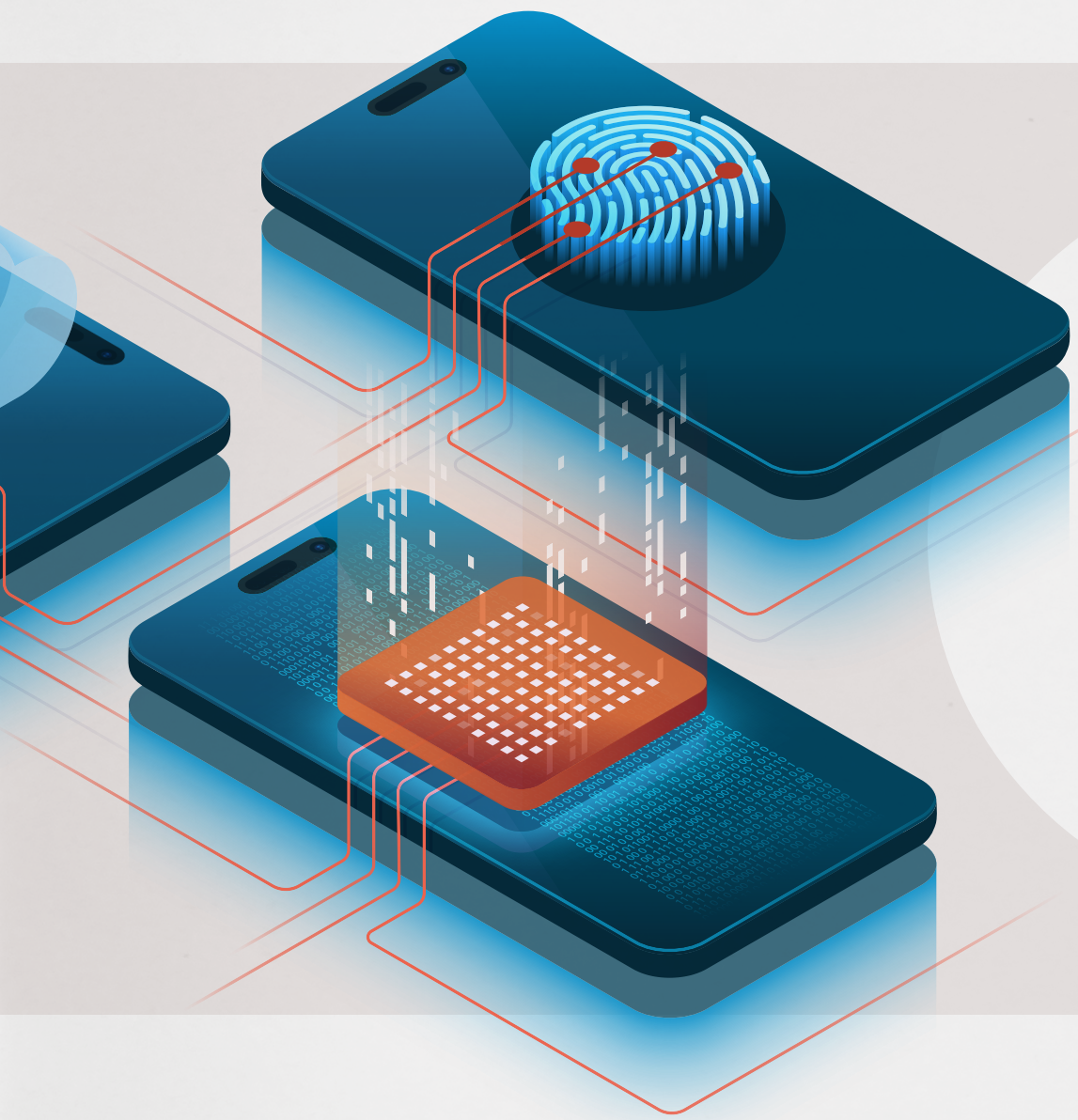
Het inloggen met een passkey werkt op vrijwel dezelfde manier als met een wachtwoord uit iCloud Sleutelhanger. Passkeys zijn een vervanging voor wachtwoorden. Bij het maken van een passkey wordt er een unieke digitale sleutel gemaakt, die alleen werkt voor die ene website. Passkeys maken gebruik van encryptie met een publieke sleutel en worden alleen op het toestel bewaard, niet op een webserver. Daarnaast wordt gebruik gemaakt van biometrische verificatie, waardoor het systeem minder gevoelig is voor hackers. Zij beschikken immers niet over jouw unieke vingerafdruk of gezichtsscan, die alleen lokaal op het toestel kan worden uitgevoerd. Hiermee kun je aanmelden bij websites en apps zonder een wachtwoord te gebruiken. Dat is niet alleen handiger, maar ook veiliger. Je geeft aan met welk account je wilt inloggen en gebruikt Touch ID of Face ID om te bewijzen dat jij het bent. Wil je inloggen op een apparaat dat niet van jou is, dan verschijnt er een QR-code. Je richt dan de camera van je iPhone of iPad op deze QR-code en bevestigt met Touch ID of Face ID dat jij het bent. Je kunt ook passkeys delen via AirDrop naar een ander apparaat.

"Veel bedrijven zijn enthousiast over het potentieel van deze technologie", geeft Roy aan. "Passkeys is een functie die op alle platformen moet gaan werken en waarbij je geen wachtwoorden meer nodig hebt. Apple heeft met externe ontwikkelaars, de FIDO Alliance, met onder andere Google en Microsoft, gewerkt aan een toekomst zonder wachtwoorden. Passkeys is het resultaat daarvan. Deze zijn veiliger en gemakkelijker in gebruik. Bij een passkey is phishing namelijk niet mogelijk, omdat de sleutel nooit het Apple device verlaat. Hackers kunnen je ook niet verleiden om een passkey te delen op een nagemaakte website, want de passkey is altijd gekoppeld aan een bepaalde app of website. Passkeys zijn te gebruiken vanaf macOS Ventura, iOS 16 en iPadOS 16."

Tweefactorauthenticatie

Een belangrijke aanvullende beveiligingsmaatregel die extra bescherming biedt voor je online accounts is tweefactorauthenticatie. Het is een proces waarbij je naast je gebruikersnaam en wachtwoord nog een extra verificatiemethode moet doorlopen om toegang te krijgen tot je account.

"We kunnen niet genoeg benadrukken hoe belangrijk het is om overal tweefactorauthenticatie te gebruiken", vertelt Roy. "Zowel zakelijk als privé. Neem even de tijd



“Werk en privé daadwerkelijk gescheiden houden kan best lastig zijn, maar het kan wel.”

om te controleren welke websites deze beveiligingsfunctie ondersteunen. We horen vaak verhalen van mensen in onze omgeving waarbij hun Facebook- of Instagram-account is gehackt of is overgenomen. Door tweefactorauthenticatie in te stellen, kun je dit risico aanzienlijk verminderen. Het kost maar een paar minuten en het is zeker de moeite waard voor de extra beveiliging van jouw accounts.”

Mobile Device Management

Het veiligste is, als je de zakelijke Mac beheert via Mobile Device Management (MDM), want daarmee is het voor een beheerder mogelijk om beleid vanuit de organisatie te bekrachtigen. Bijvoorbeeld wanneer de Mac in sluimerstand gaat of na hoeveel minuten je het wachtwoord verplicht bent om in te voeren om te ontgrendelen. Met MDM kun je dus voorkomen dat gebruikers dit vergeten in te stellen. Je kunt FileVault gebruiken om de gegevens op je Mac te versleutelen. Vanuit de software kun je FileVault standaard aanzetten en daarbij meteen een herstelcode genereren om deze te kunnen resetten. De herstelcode wordt opgenomen in het systeem, waardoor je als IT-beheerder niet afhankelijk bent van de eindgebruiker.

“MDM maakt het ook makkelijker om single-sign-on uit te rollen voor de beheerder. Je maakt één account aan voor de gebruiker en die heeft daardoor meteen toegang tot alle services die het bedrijf gebruikt. Ook bij offboarden, wanneer mensen uit dienst gaan, is dit handig, want je hoeft minder accounts te blokkeren en kun je dus ook minder vergeten. Wel zo veilig. We geven vaak advies aan IT’ers die Windows beheren en de middelen gebruiken die ze kennen. Microsoft Intune is bijvoorbeeld een MDM die kan worden gekoppeld aan Apple devices, maar met alleen Intune is het beheer van deze devices beperkt. Wij adviseren om hiervoor een gespecialiseerde MDM-oplossingen te implementeren en deze twee wel met elkaar te laten communiceren”, vervolgt Roy.

Snelle beveiligingsmaatregelen

Apple heeft Rapid Security Response geïntroduceerd. Dit zijn vaak kleine updates die snel kunnen worden geïnstalleerd en gemakkelijk naar alle apparaten kunnen worden verspreid. Op die manier kunnen de devices zo snel mogelijk up-to-date zijn en veilig worden gebruikt. Zodra je melding krijgt dat een kwetsbaarheid daadwerkelijk actief wordt misbruikt, is het van groot belang dat je de update zo snel mogelijk installeert. Als de IT-omgeving goed is ingesteld, zul je hier weinig van merken. De updates worden op de achtergrond geïnstalleerd. Het enige wat jij als gebruiker hoeft te doen, is je Mac een keer herstarten en de meldingen van het besturingssysteem in de gaten te houden die je vragen om de update te starten. Probeer dit bijvoorbeeld in te plannen tijdens je lunchpauze, aan het begin of einde van de dag.

Endpoint Protection

Roy gaat verder, “Waar je vroeger antivirus-, antimalware- en antiphishing-software had, heb je nu eigenlijk meer endpoint protection, SentinelOne is daar een voorbeeld van. Een antivirus werkt, die scant een bestand en herkent bepaalde eigenschappen van een virus door de koppeling met een database. Maar de nieuwste virussen of malware zullen nog niet in die database staan en dus ook nog niet herkend worden.

SentinelOne maakt gebruik van artificial intelligence en gaat als het ware op jacht naar virussen. Die ziet een bestand iets doen of iets uitvoeren, wat als verdacht wordt aangemerkt. De beheerder krijgt daar een bericht van. Als SentinelOne het zelf al zeker weet, dan wordt de opdracht automatisch stopgezet”.

Secure Enclave-coprocessor

De Secure Enclave vormt de basis voor de beveiliging van opgeslagen gegevens, de veilige opstartprocedure van macOS en de opslag van biometrische gegevens. Deze Secure Enclave-coprocessor is te vinden is in alle moderne iOS-, iPadOS-, watchOS- en tvOS-devices en alle Mac devices met Apple T2 Security-chip en Apple Silicon.

De Secure Enclave zorgt ervoor dat gebruikers zich op Apple devices veilig kunnen aanmelden via Touch ID en Face ID, zonder dat de biometrische gegevens van de gebruiker kunnen worden achterhaald. Deze gegevens staan versleuteld op het device en worden niet geupload naar een cloud. Er is daardoor geen verbinding met internet nodig om deze te gebruiken. Het geeft een gerust gevoel dat er geen gegevens opgeslagen worden op een server, waar potentiele hackers bij kunnen.

Bring Your Own Device

“Werk en privé daadwerkelijk gescheiden houden kan best lastig zijn, maar het kan wel. Sommige bedrijven kiezen ervoor om een Bring Your Own Device-strategie te hanteren, dat houdt in dat een medewerker devices mag meenemen van thuis, zoals een telefoon, en daarmee bij bedrijfssystemen mag inloggen in software die door de baas beschikbaar gesteld wordt. Met een MDM wordt jouw mobiele telefoon op de achtergrond als het ware in tweeën gesplitst, waarbij je de zakelijke apps in het ‘werk gedeelte’ zet. Dit betekent dat een beheerder dus niks kan inzien wat privé is. Ook niet de locatie van de telefoon. Een MDM kan alleen het zakelijke gedeelte beheren.

Een term die vaak wordt genoemd, is Shadow IT. Alle IT die niet officieel is goedgekeurd door de IT-afdeling valt daaronder. Hoogstwaarschijnlijk vindt dit ook plaats in jouw organisatie. Dit verwijst eigenlijk naar alle ICT-middelen waar je geen weet van hebt. Het gaat om de apparatuur en diensten die gebruikers zelf meebrengen. Soms ervaren mensen problemen met hun internetverbinding of wifi en denken ze: “Ik heb nog een extra router thuis liggen, ik sluit die gewoon aan en stel een nieuw wifi-netwerk in.” Dit creëert echter een afweging tussen beveiliging en gemak. Het is belangrijk om het gebruikers zo eenvoudig mogelijk te maken, zodat ze dit soort oplossingen niet gaan proberen. Daarnaast is het essentieel om in het netwerk een systeem te hebben dat hiermee om kan gaan en het beheer ervan kan ondersteunen”, sluit Roy af.



Pro Warehouse

Aan het werk met de eindgebruiker in het achterhoofd



Onze Pro's staan graag voor iedereen klaar. Of dit nu in de vorm van gebruikerssupport of een adviesgesprek is, ze denken graag mee. Maar wie is nu die Pro? In iedere editie geven we het woord aan één van onze specialisten en vragen we naar hun kijk op verschillende onderwerpen.

"Als cloud engineer onderhoud ik alles wat klanten in de cloud hebben draaien en help ik onze supportdesk om de uitgebreidere supportvragen op te lossen. De hoofdtaak van het cloudteam is het beheren van de devices van klanten via het Mobile Device Management-systeem. We gebruiken daarbij meestal Jamf, maar ook andere systemen zijn geen probleem. We kijken dan periodiek of de omgeving nog is zoals het hoort te zijn en of er bepaald onderhoud uitgevoerd dient te worden. Dit leggen we natuurlijk allemaal vast, waarvan de klant een rapport krijgt. Omdat je als cloud engineer vaak meer rechten hebt binnen een applicatie dan een Support Engineer, helpen wij bij bepaalde vragen die binnenkomen bij deze afdeling.

Ik ben in 2008 bij Xando, een IT-bedrijf dat in januari 2023 is overgenomen door Pro Warehouse, begonnen als engineer, nadat ik een ICT-opleiding had afgerond in Zwolle. Halverwege mijn opleiding kwam ik in aanraking met producten van Apple en wist ik meteen dat ik hier meer mee wilde gaan doen. Deels door de goede gebruikerservaring en deels door de achterliggende architectuur. Ik ben hierin ook een beetje aangestoken door mijn vader die, na het houden van een melkveehouderij, ook de ICT is ingegaan. Wat ik altijd wel interessant vind, zijn bijvoorbeeld de keuzes die Apple maakt in het ontwerp van nieuwe producten. In het begin vinden mensen die keuzes dan niet logisch, maar als je gaat kijken naar de reden achter die keuzes, het wel heel logisch is. Bijvoorbeeld voor toegankelijkheid of het aansluiten van externe apparaten.

We proberen altijd om proactief de omgevingen te beheren. Daarmee bedoel ik dat we vooruit proberen te kijken met wat er nodig is om bepaalde systemen en omgevingen optimaal te laten draaien en problemen te voorkomen. Dat is natuurlijk altijd beter dan achteraf issues op te moeten lossen. Helaas lukt dit niet altijd, maar het is wel het streven. Gelukkig is het team nu uitgebreid en gegroeid, dus ik verwacht dat dit in de toekomst nog beter gaat lukken.

Als ik zelf aan een systeem werk, dan zit ik graag op de stoel van de gebruiker. Het is een mooie uitdaging om de balans te vinden tussen een optimale ervaring en de beveiliging van het device. Ik wil niet dat de gebruikerservaring minder wordt of dat iemand zich beperkt voelt, omdat er allerlei zaken zijn dichtgezet, terwijl er ondertussen natuurlijk wel gedacht moet worden aan de veiligheid van bedrijfsgegevens die op het device staan. Ik wil dat de gebruiker echt het idee heeft van; dit is mijn computer, hier heb ik 'alle' vrijheid."

Kleine uitstap buiten ICT

"Tussen de jaren door heb ik nog een kleine uitstap gemaakt buiten de ICT. Ik heb namelijk mijn brevet gehaald als helikopterpiloot, in Lelystad. Dat is echt heel leuk om te doen en je moet best veel weten. Wanneer je een vlucht maakt, zijn er heel veel zaken waaraan je aandacht moet besteden, voordat je überhaupt de lucht in kunt. Je moet bijvoorbeeld het weer checken, berekenen of je genoeg brandstof hebt om je bestemming te bereiken, inclusief eventuele uitwijkhavens, de luchtvaartberichten checken of er geen evenementen met drones of vuurwerk zijn en je checkt natuurlijk de helikopter volledig voor vertrek. Tegenwoordig wordt er in de luchtvaart veel met iPads gewerkt en zijn er handige apps die de meeste van deze checks voor jou uitvoeren. Hierdoor hoef je eigenlijk geen handmatige berekeningen meer te maken. Helaas kwam ik erachter dat het toch niet de wereld is waarin ik gelukkig wordt. Het werk is erg ad-hoc en je bent snel aangewezen op offshore, terwijl ik het vliegen boven water niet zo leuk vind als boven land. Nu ben ik als cloud engineer op een andere manier aan het werk in de wolken."

"Nu ben ik als cloud engineer op een andere manier aan het werk in de wolken"

Ontspanning is ook belangrijk

"Soms heb je van die dagen dat je even je hoofd leeg wil maken na werk. Dan zet ik graag even de Playstation aan met een niet te ingewikkelde game. Ik heb bijvoorbeeld een mooie opstelling om te racen, compleet met stuur, stoel en pedalen. Op kantoor hebben we dit ook en we houden altijd een kleine competitie voor de snelste ronde op een bepaalde baan, dus ik kan thuis mooi oefenen! Ook houd ik van Lego, Star Wars en een wandelingetje maken."

De tip van Martin

"Iedereen weet dat het belangrijk is om een goed en sterk wachtwoord te gebruiken, maar het gebeurt maar al te vaak dat mensen meerdere keren hetzelfde wachtwoord gebruiken, die ze ook nog eens jarenlang gebruiken. Je Mac, iPhone of iPad kan zelf sterke wachtwoorden maken en door iCloud Sleutelhanger kun je ze op al je apparaten gebruiken. Zo hoeven complexe wachtwoorden geen ingewikkelde kwestie te zijn! Om het nog makkelijker te maken kunnen wachtwoorden kunnen automatisch ingevuld worden bij het inloggen. Als één van je wachtwoorden ooit is buit gemaakt bij een datalek, dan krijg je hier een melding van, zodat je daarvoor een nieuw wachtwoord kunt genereren. Zet indien mogelijk ook tweefactorauthenticatie aan. Dit is een extra beveiligingslaag, waardoor iemand anders niet kan inloggen. Zelfs als ze het wachtwoord hebben."

pro warehouse

Consultants Network

Willen jij en je collega's ook liever met Apple devices werken?

Bestel onze gratis QuickScan!



Wil je weten of deze Apple devices makkelijk te integreren zijn binnen de huidige IT-omgeving bij jou in het bedrijf? Of wil je weten of je huidige Apple omgeving veilig en up-to-date is? Bestel een gratis en vrijblijvende QuickScan!

De QuickScan is een gratis inventarisatie van jouw IT-netwerk door één van onze gecertificeerde Apple engineers. Je krijgt een duidelijk beeld van de status van het Apple platform binnen jouw organisatie en de vervolgstappen die genomen kunnen worden. Na het uitvoeren van de QuickScan wordt een vrijblijvend rapport met bevindingen en aanbevelingen opgesteld en gedeeld.

Meer weten?

Neem contact op met sales@prowarehouse.nl
of bel naar +31 20 423 16 37

Bekijk de privacyfilters van Dicota op de website van Pro Warehouse

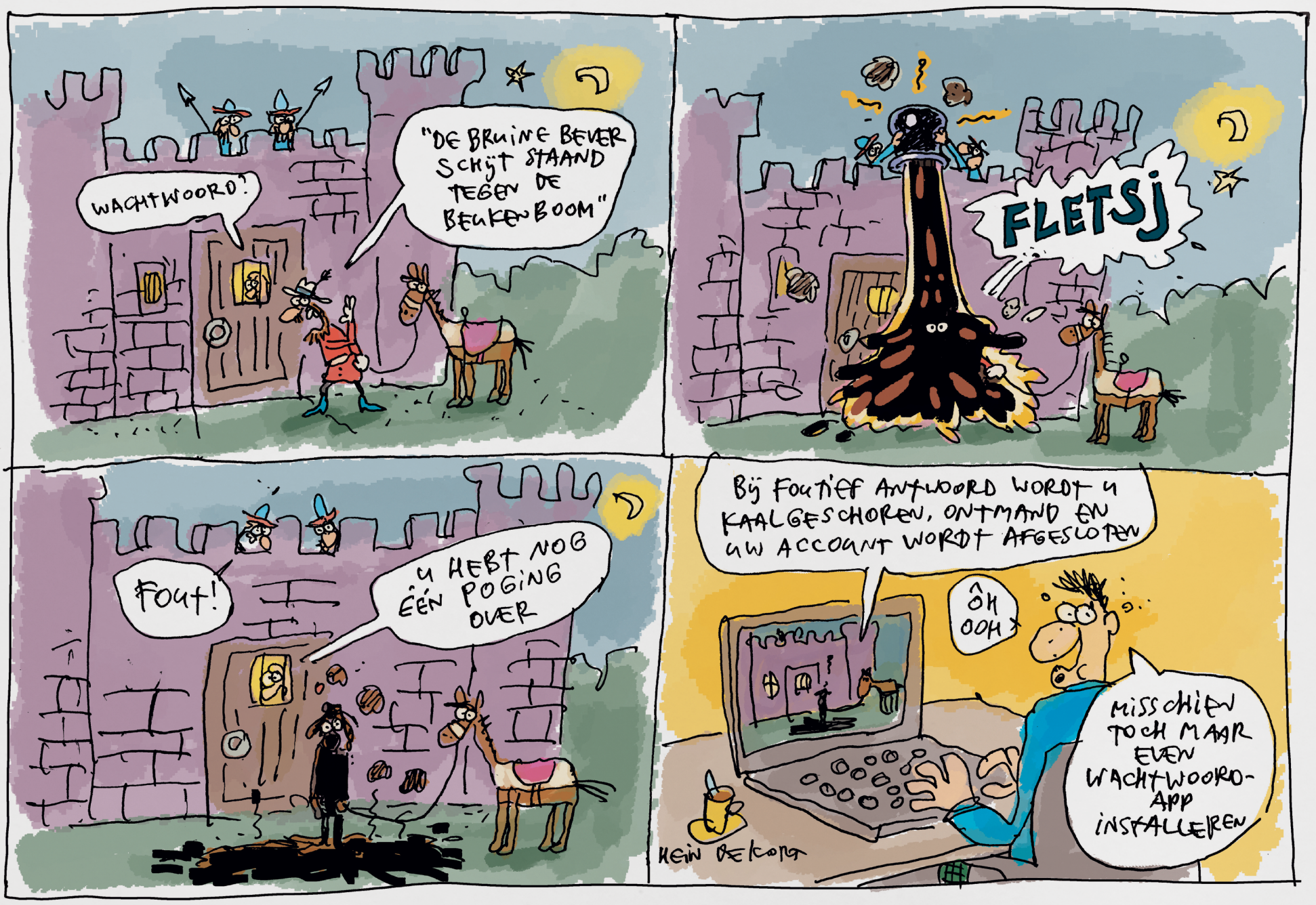


Privacyfilters voor Apple devices

Ongewenst meekijken op een beeldscherm wordt ook wel visueel hacken genoemd, tegenwoordig een serieus probleem. Het geeft je een onveilig gevoel en het tast je privacy aan. Een toenemend probleem, omdat we overal werken waar we zijn. De werkgever heeft hierin ook een zorgplicht, niet alleen naar het personeel, maar ook vanuit de Europese verordening omtrent General Data Protection Regulation (GDPR) ook welbekend als AVG.

De bescherming van persoons- en klantgegevens wordt steeds relevanter omdat we overal werken: op het kantoor, in openbare ruimtes of de trein, bus of vliegtuig. Men moet kunnen aantonen dat op een verantwoordelijke manier wordt omgaan met gegevens en privacy. Doet men dat niet of onvoldoende, dan kan dat leiden tot flinke boetes. De werknemer daarbij ondersteunen is meer dan wenselijk, omdat van hem ook wordt verwacht dat hij de gegevens op een goede manier beheert. Verder kan het de werknemer in mogelijk kwetsbare situaties brengen en dat vormt mogelijk een bedreiging voor de privacy.

Magnetische Privacyfilters van Dicota zijn een interessante en flexibele oplossing. Het 2-way privacyfilter schermt zones af zodat meekijken niet mogelijk is. Door het magnetisme in het frame hecht het filter zich direct op het scherm. Een zeer eenvoudige en gebruikersvriendelijke oplossing. Het filter verwijder je net zo makkelijk als dat je het aanbrengt, als de informatie op het scherm even gedeeld moet worden met een collega of klant. Zeer geschikt dus voor een effectieve afscherming van jouw display en een veilig gevoel.





Tips & Tricks

Wil je meer uit jouw Apple devices halen?

Om je te ondersteunen geven we in deze column uiteenlopende tips, leuke weetjes en direct toepasbare tricks waarmee jij nóg productiever aan de slag kan.

Vingerprintscanner

Vliegensvlug inloggen en bevestigen met de vingerprintscanner op het toetsenbord van je nieuwe MacBook. Ontgrendel je MacBook, krijg toegang tot je opgeslagen wachtwoorden en bevestig betalingen met één 'druk' op de knop. Stel via systeeminstellingen in welke vinger of vingers je hiervoor wilt gebruiken. Scan de afdruk, sla 'm op, ready to go, Buitengewoon beveiligd, razendsnel en super simpel.

Find My...

Met 'Find My' kun je gemakkelijk je iPhone, iPad, AirPods of andere Apple items weer tevoorschijn toveren, mocht je deze uit het oog verloren zijn. Ga op een device met hetzelfde Apple ID naar 'Find My' en zie waar het item voor het laatst was. Staat het product aan en is het dichtbij? Speel dan een geluid af waar je naartoe kan lopen. Ook erg handig als je iets ergens bent verloren of als een product gestolen is.

Apple Pay

Overal gemakkelijk, veilig & contactloos betalen? Plaats dan je credit- en/of debitcard in jouw persoonlijke Apple Wallet. In de winkel of online, je hebt niet langer last van onnodig veel handelingen. Voor fysieke betalingen kun je gebruikmaken van je Apple Watch of iPhone en hoef je geen kaart meer mee te nemen. Online kies je in je browser bij het afrekenproces vervolgens eenvoudig voor Apple Pay.

AirTag

Raak je weleens je sleutels kwijt? Vergeet je soms waar je je portemonnee of tas hebt neergelegd? AirTags zijn de ultieme oplossing. Bevestig er een aan je sleutelbos of plaats 'm in je tas, portemonnee of zelfs aan de halsband van je huisdier. Geef de AirTag een naam en ze verschijnen automatisch in je 'Find My' app op je andere devices. Gebruik het kompas of speel simpelweg een geluid af waar je naartoe kunt lopen - nooit meer lang speuren naar spullen.

Veiligheid voor alles

Je weet dat een sterk wachtwoord essentieel is. Bovendien is het erg onverstandig om hetzelfde wachtwoord meermaals te gebruiken voor verschillende accounts of inlogportals. Al die wachtwoorden onthouden zou een hels karwei zijn. Hoe kun je ervoor zorgen dat je overal sterke en identieke wachtwoorden hebt, zonder dat je ze onveilig opslaat? Kies een wachtwoordkluis zoals 1Password. Hier sla je beveiligd allerlei moeilijke wachtwoorden op, inclusief mogelijkheden om de website of tweefactorverificatie erbij te plaatsen. De kluis zelf vergrendel je vervolgens goed met één sterk wachtwoord én een speciale noodcode, mocht je toch dat wachtwoord vergeten.. Veilig, slim en snel!

Vergrendeling

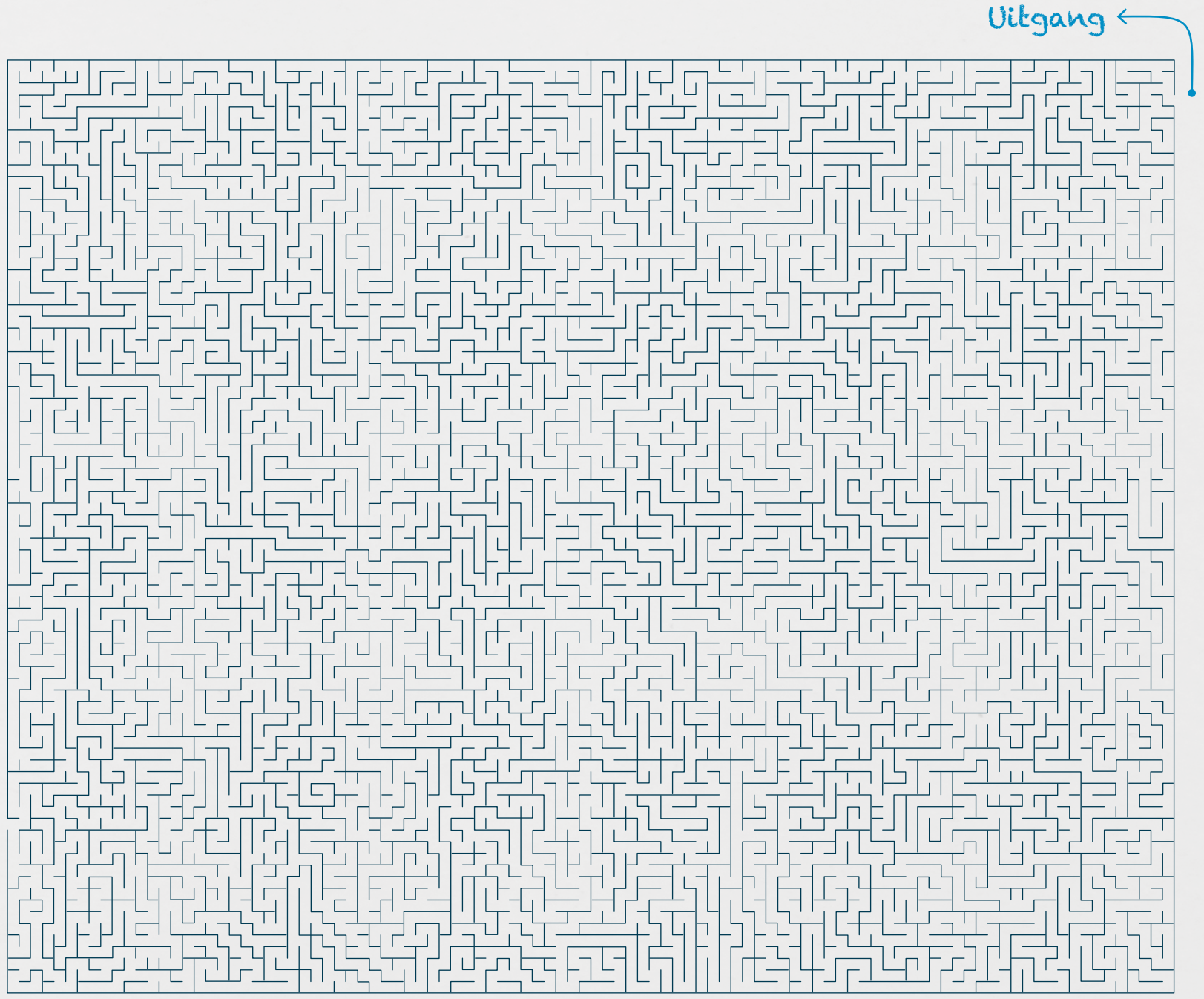
Zorgeloos aan het werk, overal. Thuis, op kantoor of in een koffiezaak? Waar je ook aan het werk bent, veiligheid moet altijd voorop staan. Niet alleen voor jezelf, maar ook zeker voor belangrijke gegevens. Zorg er daarom voor dat je je MacBook, iPhone, Mac of ander werkapparatuur altijd vergrendeld, zodra je erbij wegloopt. Zo komt data niet zomaar op straat te liggen en kun je verantwoord werken, waar dan ook.

Face ID

Beveilig je devices, werk en belangrijke gegevens goed, zodat alleen jij er toegang tot hebt. Ideaal op iPhone en iPad Pro. Sluit bepaalde chats, foto's, bestanden, notities of documenten af met Face ID en je bent er zeker van dat écht enkel jij erbij kunt. Ook voor het doen van aankopen een ware uitkomst. iPad Air heeft ongeveer een zelfde functie, maar dan met een scanner voor je vingerafdruk aan de zijkant van het device. Zo bespaar je tijd en ben je ook nog eens super safe!

Zoek de weg door het doolhof

Begin linksonder en eindig rechtsboven.



Mac does that

Mac om loyaliteit te versterken: een win-win situatie

Het is algemeen bekend dat tevreden en loyale medewerkers essentieel zijn voor het succes van een bedrijf. Het creëren van een positieve werkomgeving en het bieden van de juiste tools en technologie spelen een belangrijke rol bij het bevorderen van medewerkerstevredenheid en -betrokkenheid. In dit artikel leggen we uit hoe Mac kan bijdragen aan het vergroten van medewerkersloyaliteit.

Intuïtieve gebruikerservaring

Apple devices staan bekend om hun intuitieve en gebruiksvriendelijke interface. Medewerkers vinden het gemakkelijk om met Mac te werken, vanwege de consistente gebruikerservaring en de intuïtieve bedieningselementen. Deze positieve gebruikerservaring leidt tot minder frustratie en een verhoogde productiviteit. Dit motiveert medewerkers misschien niet direct om loyaal te blijven aan een organisatie, maar veel frustratie en een verlaagde productiviteit vanwege niet goed werkende devices, verhogen wel de kans om een organisatie te verlaten.

Creatieve tools en productiviteit

Mac computers bieden krachtige tools en software voor creativiteit en productiviteit. Of het nu gaat om grafisch ontwerp, videobewerking, muziekproductie of andere creatieve taken, tools zoals Final Cut Pro, Logic Pro en Keynote stellen medewerkers in staat om hoogwaardige output te leveren. Doordat medewerkers beter in staat zijn hun creatieve vaardigheden te benutten met behulp van Mac, voelen ze zich gewaardeerd en kunnen ze hun volledige potentieel bereiken, wat hun loyaliteit aan het bedrijf versterkt.

Betrouwbaarheid en prestaties

Eén van de frustraties die medewerkers kunnen ervaren, is het omgaan met technologische problemen en vertragingen. Apple devices staan bekend om hun betrouwbaarheid en prestaties. Ze zijn gebouwd met hoogwaardige componenten en een stabiel besturingssysteem, waardoor ze minder gevoelig zijn voor crashes en storingen. Door medewerkers te voorzien van betrouwbare apparaten, kunnen ze hun taken efficiënter uitvoeren en wordt hun werkplezier vergroot, wat indirect weer leidt tot een hogere mate van loyaliteit.

Beveiliging en gegevensbescherming

In een tijdperk waarin gegevensbeveiliging een topprioriteit is geworden, biedt Apple een robuust beveiligingskader. Mac computers zijn standaard voorzien van ingebouwde beveiligingsfuncties, zoals FileVault-encryptie, Gatekeeper en XProtect, die bescherming bieden tegen malware en ongeoorloofde toegang tot gegevens. Door medewerkers te voorzien van veilige en goed beveiligde apparaten én ze te voorzien van informatie over hoe je gegevens ook zelf goed beschermd, kunnen zij onbezorgd aan het werk.

Ondersteuning

Medewerkers waarderen het hebben van toegang tot een betrouwbaar ondersteuningssysteem voor support, dat hen helpt bij technische problemen en vragen. Daarnaast heeft Apple een grote gemeenschap van gebruikers en ontwikkelaars die ideeën, tips en ondersteuning delen. Dit creëert een gevoel van verbondenheid en ondersteuning onder medewerkers.

Stijl en prestige

Het gebruik van Apple devices straalt een zekere stijl en prestige uit. Apple producten worden vaak geassocieerd met innovatie, design en kwaliteit. Medewerkers die met Mac werken, voelen zich vaak trots op hun werkplek en zijn enthousiast om deel uit te maken van een organisatie die investeert in hoogwaardige technologie. Dit gevoel van trots en prestige draagt bij aan de loyaliteit van medewerkers en hun positieve perceptie van de organisatie.

Het kiezen van Mac devices binnen een organisatie kan bijdragen aan het vergroten van medewerkersloyaliteit op verschillende manieren. De intuïtieve gebruikerservaring, de creatieve tools en het stijlelement dragen allemaal bij aan een positieve werkomgeving en tevredenheid onder medewerkers. Dit resulteert, naast andere HR-gerelateerde zaken natuurlijk, in een hogere loyaliteit en betrokkenheid, wat op zijn beurt de productiviteit en het succes van de organisatie bevordert. Kortom, het investeren in Mac is een win-win situatie voor zowel medewerkers als werkgevers.



Colofon

Pro Warehouse Update

Nummer 5

De Pro Update is een businesskrant vanuit Pro Warehouse, dat zich richt op personen die graag met Apple willen werken en IT-professionals. Verschillende thema's passeren de revue, die allen raakvlakken hebben met de IT-sector.

Pro Warehouse Marketingteam

Redactie & vormgeving

Ingezonden artikelen, recensies, discussies en/of mededelingen zijn welkom. Stuur deze inzendingen naar de redactie van Pro Update via marketing@prowarehouse.nl. Richtlijnen voor auteurs zijn op te vragen bij de redactie.

De redactie behoudt zich het recht voor om artikelen, zonder opgave van reden, te weigeren, te verkorten of anderszins te wijzigen.

Copyright

Niets van deze uitgave mag op welke wijze dan ook gekopieerd of verveelvoudigd worden, zonder nadrukkelijke toestemming van de auteur(s). De auteursrechten van de artikelen in deze krant behoren aan de desbetreffende auteur(s).

Wil je deze krant op kantoor ontvangen en je inschrijven voor onze nieuwbrief?
Scan de QR-code en meld je aan.

Adres: Paasheuvelweg 34c
1105 BJ Amsterdam
Nederland

Tel: +31 20 423 16 37
Mail: sales@prowarehouse.nl
Web: www.prowarehouse.nl

pro warehouse