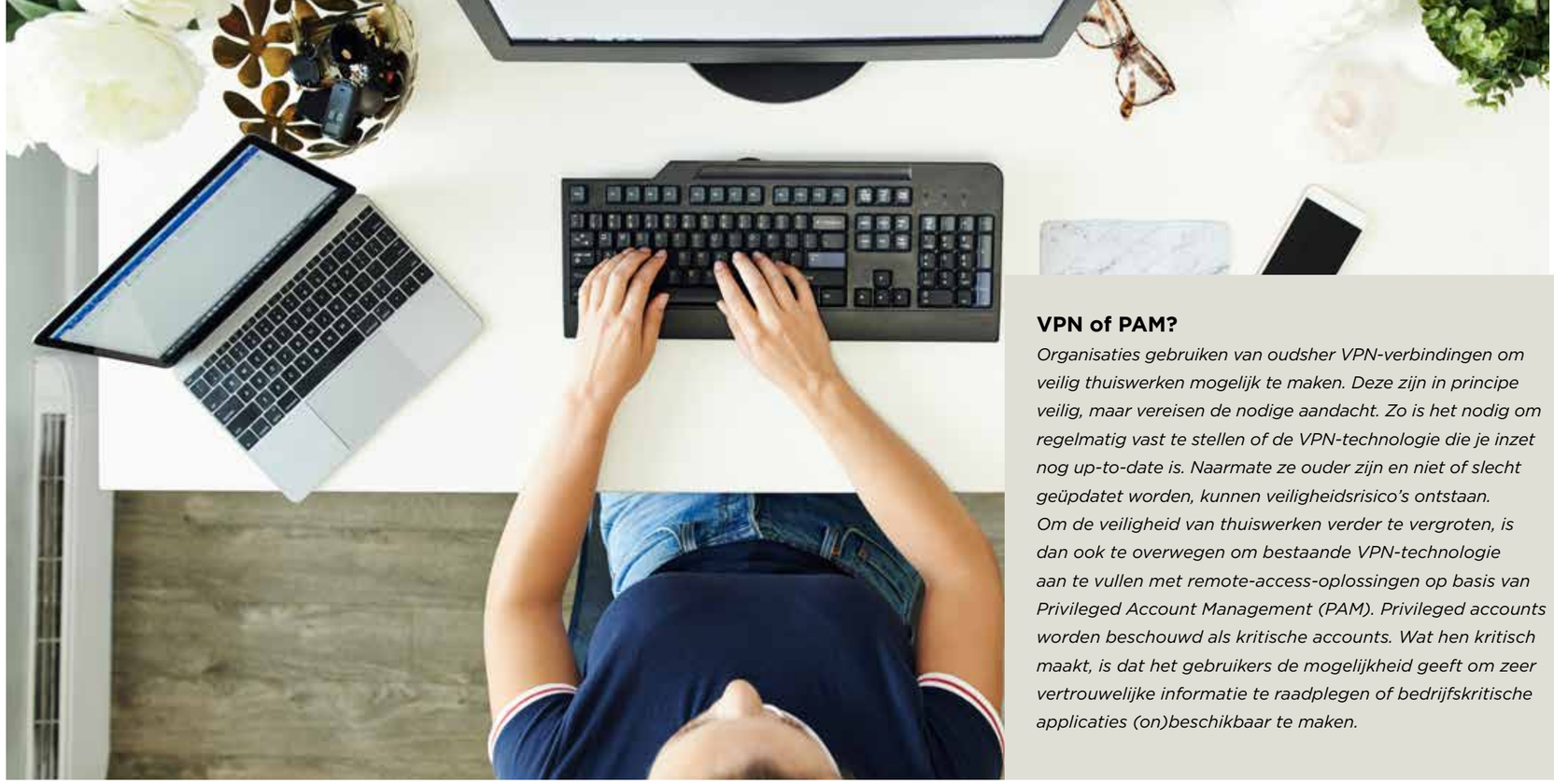
RESELLERS SPELEN EEN ROL BIJ HET VEILIG REMOTE WERKEN

De digitale werkplek is volwassen geworden

Al langer bestond de trend naar plaats- en tijdonafhankelijk werken, maar de COVID-19-uitbraak heeft dit proces versneld. Hoe ziet de digitale werkplek er anno 2021 uit? We schetsen een beeld aan de hand van 9 trends.

Tekst: Mels Dees



VPN of PAM?

Organisaties gebruiken van oudsher VPN-verbindingen om veilig thuiswerken mogelijk te maken. Deze zijn in principe veilig, maar vereisen de nodige aandacht. Zo is het nodig om regelmatig vast te stellen of de VPN-technologie die je inzet nog up-to-date is. Naarmate ze ouder zijn en niet of slecht geüpdatet worden, kunnen veiligheidsrisico's ontstaan.
Om de veiligheid van thuiswerken verder te vergroten, is dan ook te overwegen om bestaande VPN-technologie aan te vullen met remote-access-oplossingen op basis van Privileged Account Management (PAM). Privileged accounts worden beschouwd als kritische accounts. Wat hen kritisch maakt, is dat het gebruikers de mogelijkheid geeft om zeer vertrouwelijke informatie te raadplegen of bedrijfskritische applicaties (on)beschikbaar te maken.

Veel medewerkers moesten noodgedwongen overschakelen op een andere manier van werken – vooral vanuit de thuislocatie. Maar zeker ook de IT-beheerders moesten wennen aan een nieuw normaal. Hoe grip te houden op applicaties? Hoe zijn updates uit te rollen als medewerkers niet op kantoor zijn? Hoe beveiligen we data en houden we hackers buiten de deur? Welke verbindingen gebruiken de medewerkers? In veel gevallen kunnen resellers een rol spelen bij het veilig en flexibel maken van IT-systemen van hun eindklanten.

1 De migratie naar een digitale workplace

Het is inmiddels een feit: medewerkers moeten zowel op kantoor als daarbuiten op elk device snel en veilig kunnen inloggen. Met een managed workplace kan dat.
Waar een gebruiker traditioneel eerst moet inloggen op zijn pc en vervolgens nog eens voor de verschillende applicaties, daar voorziet een managed workplace in een single sign on – ook als bepaalde legacy-software nog steeds lokaal draait, of Office 365 toepassingen juist op externe (Azure-)servers draaien.

2 Toekennen van rechten

Belangrijk is het toekennen van rechten. Dat speelde altijd al, maar zeker bij remote werken is het van belang nauwkeurig vast te stellen welke gebruiker bepaalde data mag inzien, wijzigen en verwijderen – en wie niet. Dergelijke rechten zijn vaak historisch gegroeid en niet vastgelegd. De migratie naar een managed workplace geeft de mogelijkheid deze rechten in kaart te brengen en te koppelen aan functies. In het kader van compliancy en voor het voldoen aan de AVG-regelgeving is dit belangrijker dan ooit.

3 In huis of outsourcen?

De vraag die steeds vaker binnen organisatie gesteld wordt, is of het bedrijf een volledige workplace-omgeving in huis moet hosten, of dit juist moet uitbesteden aan een externe partij, zoals een reseller. Voor organisaties met minder dan honderd desktops is het in de praktijk vaak te duur om een workplace in huis te implementeren en te beheren. De onderneming zal goed opgeleide mensen in huis moeten hebben en krijgt te maken met licentiekosten.
Outsourcing heeft als voordeel dat eenvoudig gekozen kan worden voor pay-per-use: bij minder medewerkers zijn de kosten lager. In het verlengde daarvan is het voordeel van uitbesteden, dat piekbelastingen snel en tijdelijk opgevangen kunnen worden.

4 Zero touch

Nu medewerkers massaal buiten het kantoor werken, wordt ook het contact met bijvoorbeeld de helpdesk of de systeembeheerders in snel tempo virtueel. Om, zeker bij nieuwe werknemers of bij het vervangen van verouderde apparatuur efficiënt te werken, kan gekozen worden voor 'zero touch' deployment. Daarbij worden systemen met een koerier naar de medewerkers gebracht die al volledig zijn geconfigureerd. Alles wordt turnkey, eventueel met een beknopte handleiding opgeleverd. Dat laatste blijkt overigens vaak onnodig, mensen zijn privé inmiddels al gewend apparatuur online te bestellen en zelf te installeren. Om de IT-afdeling verder te ontlasten is te kiezen voor een maximale graad aan automatisering, of (ook hier) het uitbesteden van deze activiteiten aan een reseller.

5 Updates

Uiteraard spelen cloudapplicaties een belangrijke rol in de nieuwe digitale kantooromgeving. Deze applicaties worden in zekere zin ook zero touch geactualiseerd: ze worden immers automatisch door de leverancier geüpdatet.

6 Secure toegang

We schreven hierboven al over het toekennen van rechten en over 'single sign on' voor applicaties. Hoe zorg je ervoor dat de toegang tot de digitale werkplek ook maximaal veilig is? Het antwoord op de vraag is maximaal wantrouwen, ofwel zero trust access. Je gaat er daarbij vanuit dat een vertrouwde gebruiker niet bestaat. In de praktijk betekent dit dat een gebruiker zich voor elke sessie opnieuw moet aanmelden.
Naast een Identity Check (wachtwoord) zijn er ook mogelijkheden om 'conditional access' in te zetten. Denk bijvoorbeeld aan een 2-factor authenticatie voor gebruikers die actief zijn buiten het bedrijfsnetwerk, bijvoorbeeld door het versturen van een code via SMS. Ook zal steeds vaker biometrie een rol spelen. Denk aan vingerafdruk- of gezichtsherkenning. Of aan het gebruik van een QR-code in combinatie met een device met vingerafdruk- of gezichtsherkenning.

7 Hackers en malware

Security gaat uiteraard verder dan alleen het veilig toegang geven tot applicaties en systemen. Het afgelopen jaar was, helaas, een goed jaar voor kwaadwillenden. Duidelijk is dat VPN niet voldoende is. Medewerkers moeten alert blijven, trainingen mogen ook bij thuiswerken niet vergeten worden. De beveiliging tegen malware moet prioriteit hebben. Zeker als mensen minder vaak op kantoor komen. Zogenaamde CEO-fraude wordt dan wel een stuk eenvoudiger. Voor andere malware is next generation antivirus van belang, naast aandacht voor aanvallen op BIOS-niveau. Vergeet ook containerisering niet. Veel bedrijven doen dat al op smartphones, maar het kan ook op laptops nuttig zijn.

8 Vergeet de back-ups niet

Ook dit jaar zullen we steeds meer verwoestende ransomware-aanvallen zien. Organisaties zullen zich dan ook moeten richten op back-uptechnologieën en -diensten als hun laatste verdedigingslinie. Aangezien langdurige downtime bijna net zo duur is als het betalen van het losgeld, wordt de snelheid waarmee systemen weer up-and-running zijn steeds belangrijker. Daarom zullen organisaties op zoek gaan naar back-upoplossingen die ervoor zorgen dat systemen binnen enkele minuten of uren weer online zijn in plaats van een aantal dagen of nog langer.

9 Minder tolerant

Nu iedereen digitaal en vanuit huis werkt is de tolerantie voor storingen minder geworden – of die storing nu te wijten is aan de slechte wifi-verbinding van de medewerker of juist sprake is van problemen binnen het bedrijfsnetwerk.
Ontoegankelijkheid wordt niet alleen onacceptabel voor medewerkers, maar zeker ook voor klanten die steeds minder geduld lijken te hebben. Storingen en veiligheidslekken zijn net zo schadelijk voor de reputatie als voor het bedrijfsresultaat. ■