IRISONE ICT

De 10 fundamenten van de moderne werkplek in het mkb

Deze functies heb je nodig om efficiënt en veilig te werken

Wat zou het fijn zijn als je meer kon doen in minder tijd. Dat kan met slimmere ICT, maar dit is nog lang niet bij elk mkb-bedrijf goed geregeld. Je wilt niet schakelen tussen tools, voor elk wissewasje e-mailen of lang hoeven wachten op correcties. Bovendien moeten al je bestanden, apparaten en je apps goed beveiligd zijn. Eigenlijk wil je één digitale werkplek die dit allemaal regelt. Welke cruciale onderdelen daar in moeten zitten, lees je hier.

1. Iedereen kan overal bij,...

Op de kantoorschijf is het een ratjetoe van documenten en toegang, lees- en schrijfrechten zijn niet ingesteld. De stagiair kan ook bij offertes en HR-documenten... Dit werkt wel gemakkelijk, maar echt veilig is het niet. En als je een document deelt dan kan dat maanden bij een klant blijven liggen. Je mist grip op de toegang tot je bestanden.

...maar met Azure Information Protection heb je wel grip op toegangsrechten

Met Azure Information Protection regel je gemakkelijk wie waar bij kan op basis van rollen. Hiermee kan een stagiair bijvoorbeeld bepaalde bestanden wel inzien, maar niet wijzigen of delen. Krijgen onbevoegden een bestand? Dan kunnen ze die niet inzien. Dit soort regels gelden voor alle documenten die je online en lokaal hebt staan. Je kunt zelfs de geldigheid intrekken van een offerte die je naar een klant hebt gestuurd. Op die manier reageert die niet meer op een verlopen offerte.

2. Neutraliseer phishingmail en kwaadaardige bijlagen...

Je hebt vast wel eens een e-mail van een 'bank' gekregen met de vraag in te loggen. Je weet niet altijd dat de afzender niet koosjer is. En dan kan één klik zomaar je computer of zelfs het hele bedrijfsnetwerk lamleggen. De meeste succesvolle pogingen van cybercriminaliteit zijn dan ook het resultaat van de onvoorzichtigheid of nieuwsgierigheid van collega's. Je zou daarom het liefst criminele e-mail eruit filteren voordat je collega's in de verleiding komen.

...met Advanced Threat Protection

Advanced Threat Protection beveiligt zowel de online e-mail van Office 365 als de lokale Outlook op smartphones en pc's. Klik je toch op gevaarlijke links, dan kom je op een veilige pagina met uitleg over het gevaar van gevaarlijke links. ATP screent ook bijlagen en maakt ze onschadelijk als dat nodig is. Afhankelijk van het ingestelde beleid worden gevaarlijke e-mails in de map 'ongewenste e-mail' geplaatst of in quarantaine gezet. Zo is het meteen duidelijk dat een e-mail een boosaardige intentie heeft. ATP maakt gevaarlijk bestanden in SharePoint, OneDrive en Teams ook op deze manier onschadelijk.

3. Krijg grip op alle apparaten...

Iedereen heeft smartphones, tablets en laptops, maar die zijn niet altijd goed beveiligd. Bestanden zijn niet versleuteld, de apparaten en tools zijn niet vergrendeld via een pincode, vingerafdruk of multi-factor authenticatie. Het is onmogelijk elk apparaat te inspecteren en te checken of alle updates gedraaid zijn.

...met Microsoft Endpoint Manager

Dit regel je centraal met Microsoft Endpoint Manager. Dit geeft jou op afstand volledige controle over Android, Windows én alle Apple-apparaten. Deze kun je met een paar klikken goed beveiligen. Dat kan zowel op apparaat- als op appniveau. Het is zelfs mogelijk het apparaat op afstand te vergrendelen, alle bestanden te versleutelen en bedrijfsgegevens te wissen. Wel zo veilig bij verlies of diefstal. Bepaald niet onbelangrijk is dat medewerkers nu ook met multi-factor authenticatie (MFA) veiliger inloggen. Via een extra check met hun smartphone of token komen alleen collega's bij bestanden.

4. Privacygevoelige gegevens per ongeluk lekken...

Ook wel eens een e-mail naar de verkeerde Jan of Marieke gestuurd? Het overkwam ons allemaal wel eens. Werk je met privacygevoelige gegevens dan wil je liever helemaal niet dat dit gebeurt, want dat betekent meteen een datalek.

...automatisch tegengaan met Data Loss Prevention

Werk je bijvoorbeeld in de zorg of in de accountancy? Dan is Microsoft Data Loss Prevention (DLP) jouw vriend. Dit checkt of er gevoelige informatie in je e-mail(bijlage) zit en controleert direct of deze gegevens gedeeld mogen worden met de afzender. Dit werkt meteen voor alle programma's van Microsoft waarmee je bestanden deelt zoals OneDrive, SharePoint en Outlook. Staan er BSN-nummers, adresgegevens of andere gegevens in die je van tevoren aanmerkte als vertrouwelijk, dan heb je daar veel meer grip op.

5. Is iedereen op het netwerk te vertrouwen?

We werken allang niet meer allemaal op kantoor. Een dagje thuiswerken, bij de klant of aan de andere kant van de wereld is heel gewoon. Daarom wil je natuurlijk wel weten dat degene die inlogt wel echt diegene is. Soms zijn wachtwoorden gestolen en is er een hacker aan het rondsnuffelen in bestanden.

Azure AD Conditional Access regelt het automatisch

Azure AD Conditional Access is de vriendelijke uitsmijter van je netwerk. Heb je de juiste toegangsgegevens dan kom je erin. Gedraag je je apart omdat je niet vanuit Utrecht, maar vanuit Jakarta inlogt met een onbekend apparaat? Dan kan automatisch de toegang worden geweigerd. Of de uitsmijter vraagt of je misschien nog iets hebt om je mee te identificeren zoals een smartphone. Op die manier komen alleen genode gasten op je netwerk.

6. Van gebonden aan je kantoor…

Wil je buiten kantooruren of op vakantie nog even die offerte aanpassen, kun je er niet bij! Privé hebben we overal en altijd toegang tot e-mail en bestanden, was het ook maar zo op de zaak…

…naar tijd- en plaatonafhankelijk werken met Microsoft 365

De keuze om thuis of onderweg te kunnen werken is geen luxe meer, maar noodzaak. Met Word, Excel, Outlook, PowerPoint en alle andere bekende Office tools in de cloud, werken jij en collega's waar en wanneer jullie willen.

Dat kan vanuit een browser of met apps op het device naar keuze, ongeacht het besturingssysteem. Omdat je vanuit de cloud werkt, heb je altijd beschikking tot de nieuwste mogelijkheden om (samen) te werken. Omdat je natuurlijk niet alleen een smartphone of een computer hebt, kun je deze tools allemaal installeren op meerdere apparaten. Handig, niet?

7. Veiliger en efficiënter chatten en bellen…

Al jaren is onze mailbox hét startpunt van de werkdag. Contact met collega's, klanten en leveranciers en onze agenda: het zit allemaal in jouw digitale brievenbus. Die zit zo vol dat je soms de bomen in het bos niet meer kunt zien. Chatten is vaak een veel snellere manier om even af te stemmen. Daarom gebruiken we WhatsApp, maar dat kan niet bij je contacten uit je e-mail. Hierdoor krijg je gescheiden communicatiestromen en adreslijsten. Dat is bepaald niet handig en veel chattools op je smartphone lijken veilig, maar zijn het niet. Worden foto's en documenten die je ermee opstuurt automatisch geback-upt? En waar dan precies?

…met Microsoft Teams

Teams, de alles-in-één samenwerkingstool van Microsoft combineert een gemakkelijk te gebruiken chatfunctie met bellen. Het is geïntegreerd met alle bekende kantooroplossingen van Microsoft waardoor je gemakkelijk en onder de veiligheidsparaplu van Microsoft bestanden deelt. Omdat het uit hetzelfde adresboek put als Outlook, leg je gemakkelijk intern en extern contact. Daarnaast

klik je zo een projectteam bij elkaar waarbinnen je (video)belt, presentaties geeft en bestanden deelt. Het succes van deze tool zit in het gemak. Daarnaast draait het op pc's, Macs, Android-telefoons en iPhones waardoor je iedereen in de organisatie en daarbuiten kan aansluiten. Verlaat iemand je onderneming, dan deactiveer je met een paar klikken de toegang tot Teams, Microsoft 365 en alle eerder gedeelde documenten. Voeg je iemand toe aan een bestaand team? Dan heeft het nieuwe teamlid ook meteen inzicht in de volledige historie van het project, ook eerdere chats en bestanden. Zo heeft iedereen direct toegang tot alle relevante informatie.

8. De gescheiden werelden van telefoon en computer...

De ene keer pak je de telefoon, de andere keer beeldbel je met Teams en waar staat het telefoonnummer van die ene klant? Zat dat in de e-mail of in je adresboek van je smartphone? Bellen met telefoon en computer is niet altijd handig.

...breng je samen met Teams Direct Routing

Met Teams Direct Routing krijgt elke medewerker in Teams een vast telefoonnummer en toegang tot het gedeelde adresen telefoonboek. Dit integreert je smartphone volledig in Teams voor bellen en gebeld worden, doorverbindfuncties
en voicemail. Je stelt ook in of collega's met het algemene bedrijfstelefoonnummer of eigen telefoonnummer naar buiten bellen. Hiermee ben je altijd perfect bereikbaar!

9. Wachten op correcties...

Vervelend hè, al die lange correctierondes wanneer je samenwerkt aan een tekst. Met zijn tweeën is dit soms al een gedoe, laat staan bij drie, vier of meer. En wat was ook alweer de meest actuele versie? Het is soms behelpen met enorm veel versies van versies van documenten.

...hoeft niet meer dankzij Microsoft SharePoint

Microsoft SharePoint maakt in één keer een einde aan wachten en zoeken omdat je tegelijkertijd in één versie werkt. Dit kan met welk apparaat dan ook met een internetaansluiting. Versiebeheer is hierdoor een stuk eenvoudiger. Tegelijk kun je een proces automatiseren voor de goedkeuring van documenten zodat bijvoorbeeld een offerte pas naar buiten mag als alle noodzakelijke collega's hun goedkeuring hebben gegeven.

10. Bestanden delen ging omslachtig,...

Bestanden zijn vaak te groot om ze even te e-mailen. Daarom gebruik je vaak WeTransfer of Dropbox, maar waar staan dan die bestanden? En na een paar dagen is de downloadlink alweer verlopen en krijg je het verzoek om de bestanden weer op te sturen.

...maar met OneDrive is het een eitje

Met OneDrive deel je je bestanden gemakkelijk en goed beveiligd. Vanwege de integratie met de Office-toepassingen hoef je niet eerst bestanden op te slaan en op te zoeken. Je deelt ze direct uit bijvoorbeeld Word. Omdat het gebruikmaakt van je gedeelde adresboek hoef je ook geen adressen meer uit je e-mail te kopiëren en te plakken. Microsoft cybersecurity houdt bovendien een oogje in het zeil over de bestanden in OneDrive. Zo kan je rekenen op de beste dataveiligheid.

Wil je gebruik maken van deze oplossingen (en een hoop meer handige extra's)?

Wil je dat jij en je collega's ook overal en altijd kunnen werken met het apparaat van je keuze? En altijd met de best denkbare veiligheid? Wacht dan niet langer en stap ook over op Microsoft 365. Met alle mogelijkheden van Office 365, Teams en een optimale beveiliging bespaar jij tijd, elke dag opnieuw!

IRIS ONE ICT

Graafsebaan 111,
5248 NL Rosmalen
073 523 2288
iris@iris-one.nl
www.iris-one.nl

Het maximale uit jezelf halen, iedere dag.