8 PRAKTISCHE TIPS

OM VEILIG (THUIS) TE WERKEN IN MICROSOFT OFFICE 365

Microsoft Partner

ITEAMPLAY
JOUW IT AFDELING

Veilig werken is belangrijk

...Maar waarom eigenlijk?

Overal hoor je dat je veilig moet werken.

Je beveiliging moet van de laatste versie zijn. Als je niet secure bent dan is het een wonder dat je nog kunt werken als je alle berichten moet geloven.

Maar waarom is dit nou zo belangrijk?

Met de tips in document willen we je praktische stappen geven die je zelf kunt ondernemen om veiliger te werken. En niet onbelangrijk, wat het risico is als je dit niet doet.

Op de werkplek

Tip 1: Installeer updates

Wat is het risico?

Hackers zijn constant op zoek naar kwetsbaarheden in software. Vroeger was dit een handmatige klus, tegenwoordig hebben hackers ook zoekmachines om kwetsbaarheden eenvoudig op te sporen.

Softwarefabrikanten “repareren” een kwetsbaarheid middels software updates.

Door te zorgen dat je de laatste updates van Windows/MacOS/Adobe/Chrome/etc. installeert zorg je dat je minder kwetsbaar bent.

Wat kun je zelf doen?

De meeste software zal zelf melden als het bijgewerkt kan worden.

Stel deze updates niet te lang uit. Herstart Windows bijvoorbeeld iedere dag zodat updates uitgevoerd kunnen worden.

Controleer van software die je veel gebruikt zelf ook regelmatig op de website of er nieuwe versies beschikbaar zijn.

Wat kun je als bedrijf doen?

Je wilt als bedrijf geen uren bezig zijn met het langslopen van alle computers om te controleren of alle updates geïnstalleerd zijn.

Door alle werkplekken centraal te beheren kun je eenvoudig een realtime overzicht creëren van alle werkplekken en welke softwareversies er aanwezig zijn.

Vanaf deze centrale plek kun je ook updates goedkeuren, forceren of blokkeren.
Zo weet je zeker wat de huidige status van je omgeving is zonder dat dit enorm veel tijd kost.

Tip 2: Bestanden veilig opslaan

Wat is het risico?

Er zijn verschillende manieren waarop data verloren kan gaan op je computer.

Misschien denk je gelijk aan cryptolockers of ransomware, maar ook minder kwaadaardige oorzaken kunnen leiden tot dataverlies.
Denk bijvoorbeeld aan het defect van je harde schijf of door diefstal/verliezen van je laptop. Menig laptop zal ook een val van tafel niet overleven.

Dataverlies kan tot gevolg hebben dat je werk opnieuw moet doen of veel tijd kwijt bent aan het herstellen.

Wat kun je zelf doen?

Maak gebruik van bestandsopslag in de cloud. Bijvoorbeeld OneDrive, Dropbox of Google Drive.
OneDrive heeft als voordeel dat het vaak inbegrepen is in je Microsoft 365 licentie. Daarnaast kun je OneDrive zo instellen dat bestanden op je bureaublad, in je documenten map en je afbeeldingen automatisch in de cloud worden opgeslagen.
Gaat je laptop kapot of kun om wat voor reden niet meer bij de bestanden op je computer. Dan kun je eenvoudig inloggen vanaf een andere computer en verder werken aan je bestanden.

Wat kun je als bedrijf doen?

Je wilt als bedrijf zijnde graag dat iedereen hetzelfde werkt en dus ook zijn bestanden op dezelfde plek opslaat. Het is lastig om je gevoelige data in de gaten te houden als dit verspreid is over meerdere cloud diensten.

Door een combinatie van endpoint management om beleid op de computers toe te passen en training om werknemers met bestanden om te leren gaan worden veel problemen voorkomen.
Door automatische controle van de naleving van het beleid zijn “overtredingen” eenvoudig op te sporen.

Tip 3: Antivirus en Firewall

Wat is het risico?

Het nut van een antivirus programma en firewall behoeft waarschijnlijk geen verdere uitleg.
Deze voorkomen dat schadelijke bestanden zoals een virus zich op jouw computer kunnen nestelen. Daarnaast zorgt een firewall ervoor dat er niet zomaar een verbinding van of naar je computer gemaakt kan worden.

Zonder deze 2 beschermingen kan een virus of hacker je computer of bestanden misbruiken of beschadigen.

Wat kun je zelf doen?

Zorg ervoor dat je virusscanner en firewall ingeschakeld zijn.
In Windows 10 kun je dit controleren door de app *Windows Beveiliging* te openen.
Deze kun je vinden door op de startknop te klikken en *Beveiliging* in te typen.
Hier kun je ook zien wanneer de virusscanner voor het laatst een update heeft gehad. Het is belangrijk dat deze dagelijks een update krijgt om de nieuwste virussen te kunnen herkennen.
Het meegeleverde antiviruspakket *Windows Defender* komt uitstekend uit diverse testen, het is dus niet nodig een los pakket aan te schaffen.

Wat kun je als bedrijf doen?

Staat bij iedereen de virusscanner wel aan en is die voorzien van de laatste versie?
Als bedrijf zijnde zou je die vraag zonder al te veel moeite en met veel zekerheid moeten kunnen beantwoorden.
Door middel van het centraal beheren en monitoren van werkplekken weet je altijd het antwoord op deze vraag en kun je automatisch actie ondernemen als er een werkplek afwijkt.
Daarnaast kan een Endpoint Detection & Response (EDR) meerwaarde bieden door meer inzicht te bieden. Zo kun je sneller achterhalen hoe een dreiging binnen is gekomen en hoe deze verspreid is.

Op de werkplek

Tip 4: Encryptie

Wat is het risico?

Het kan iedereen overkomen, je vergeet je laptop in een taxi, restaurant, trein of waar dan ook. Of nog vervelender, je wordt bestolen.

Misschien bevat je laptop of een usb schijf wel gevoelige data. Denk bijvoorbeeld aan persoonsgegevens zoals een patiëntendossier of gevoelige bedrijfsinformatie zoals receptuur of andere geheime informatie.

Data die in de verkeerde handen valt kan veel financiële of imago schade tot gevolg hebben.

Wat kun je zelf doen?

Zowel Windows 10 als Macos beschikken over mogelijkheden om data te versleutelen, Bitlocker en Filevault.

Beide systemen werken in grote lijnen hetzelfde. Nadat je ze inschakelt krijg je een digitale sleutel waarmee je in noodgevallen toegang kunt krijgen tot je data.
Het is dus belangrijk dat je deze sleutel op een veilige plek opslaat, bijvoorbeeld in een kluis.

Wat kun je als bedrijf doen?

Om te zorgen dat op alle laptops en computers van het bedrijf alle data versleuteld is kun je gebruik maken van een centrale managementtool zoals Microsoft InTune. Hiermee kun je een beleid toepassen welke het versleutelen van data op harde schijven en ook usb sticks verplicht. Herstelsleutels worden automatisch veilig opgeslagen zodat je geen stapel herstelsleutels in een kluis op hoeft te slaan.

Is een laptop verloren? Dan is het mogelijk op afstand alle data van de computer te verwijderen.

Tip 5: Veilig verbinding maken met je netwerk

Wat is het risico?

Wanneer is de laatste keer dat het wachtwoord van je Wi-Fi Netwerk is aangepast?

Door regelmatig het wachtwoord aan te passen zorg je alleen de mensen en apparaten met het netwerk verbonden zijn die er ook thuis horen.

Wat kun je zelf doen?

Pas periodiek het wachtwoord van je Wi-Fi netwerk aan.

Dit kun je meestal eenvoudig zelf aanpassen via de router van je provider.

Wat kun je als bedrijf doen?

Als er veel apparaten verbinding maken met je netwerk dan is een goed idee om gebruik te maken van verschillende subnets. Zo kun je verschillende soorten apparaten van elkaar scheiden. Maak bijvoorbeeld gebruik van een apart netwerk voor je bezoekers, je werknemers en je servers.

Ook kun je technieken als dot1x gebruiken om toegang tot je netwerk beter te beveiligen.

Veilig werken met Microsoft 365

Tip 6: Schakel multi-factor authenticatie in

Wat is het risico?

Je moet tegenwoordig veel wachtwoorden onthouden, veel mensen gebruiken daarom hetzelfde wachtwoord voor verschillende diensten.

Het risico is dat je wachtwoord door een datalek bij een dienst openbaar wordt en hackers eenvoudig toegang kunnen krijgen tot de andere diensten.

Wat kun je zelf doen?

Gebruik zoveel mogelijk multi-factor authenticatie (MFA), soms ook wel 2-staps authenticatie genoemd.

Hierbij moet je naast je wachtwoord ook nog een wisselende code uit een app of een sms invullen. Zo voorkom je dat iemand toegang krijgt tot je diensten wanneer ze je wachtwoord weten.

Wat kun je als bedrijf doen?

Gebruik een identity management systeem zoals Azure Active Directory om het gebruik van MFA te verplichten.

Ook kun je sommige applicaties aan Azure Active Directory koppelen zodat werknemers in de applicatie kunnen inloggen met hun Microsoft 365 gegevens. Hierdoor hoeven ze weer een wachtwoord minder te onthouden en je krijgt meer controle of wie wanneer en waar mag inloggen.

Azure Active Directory is in veel gevallen al onderdeel van je Microsoft 365 licentie.

Tip 7: Gebruik aparte accounts met beheerrechten

Wat is het risico?

Heeft er toch iemand toegang gekregen tot je account? Als je met jouw dagelijkse account ook beheerrechten hebt in bijvoorbeeld Microsoft 365 dan krijgen hackers ineens toegang tot je hele organisatie.

Omdat je vaak ook met dit account inlogt op je computer heeft een eventueel virus ook direct beheerrechten.

Wat kun je zelf doen?

Maak voor het beheren van belangrijke onderdelen aparte accounts aan met complexe wachtwoorden en MFA ingeschakeld.

Hiermee beperk je de schade als jouw gebruikersaccount gehackt wordt of als je computer besmet wordt met een virus.

Wat kun je als bedrijf doen?

Waar mogelijk kun je beheerrechten toekennen aan groepen. Zo hou je een goed overzicht van wie toegang heeft tot welke systemen. Ook is het eenvoudiger om aanpassingen te maken zoals het toevoegen of verwijderen van beheerders.

Tip 8: Blijf een backup maken

Wat is het risico?

Hoewel je data in de cloud staat is het nog nodig om backups te maken. Als je een bestand of email kwijt raakt kan een Cloud Provider vaak niet alleen dat ene bestand of mailtje terugzetten.

Naast dat de herstelopties zeer beperkt zijn ben je mogelijk ook veel tijd kwijt aan het terugzetten van bestanden na een herstelactie.

Wat kun je zelf doen?

Maak gebruik van een cloud backup dienst om je data veilig te stellen.

Door gebruik te maken van een cloud dienst hoef je zelf geen systeem te beheren zoals een NAS waar de backups opgeslagen worden.

Wat kun je als bedrijf doen?

Houdt bij het kiezen van een backup tool altijd rekening met hoeveel data je hierin kwijt kunt en hoe je hiervoor betaald. Vaak betaal je per gebruiker of per GB die opgeslagen wordt in je backup.

Kijk ook goed naar de locaties van je gevoelige data. Is het voldoende als er een backup van bestanden en email wordt gemaakt of wil je bijvoorbeeld ook een backup van Microsoft Teams of een volledige server hebben?

Wie we zijn?

Wij zijn ITeamplay en wij zijn je IT afdeling.

We geloven dat iedereen, overal op een veilig manier moet kunnen werken. We hebben een oplossing die ervoor zorgt dat werkplekken, netwerken en servers op een veilig manier vanuit de Cloud door ons worden beheerd. We helpen bedrijven graag met de migratie naar Office 365.

Ben je nieuwsgierig geworden? Wil je dat we je omgeving toetsen door een IT quickscan uit te voeren?

Vraag een gratis IT Quickscan aan via onderstaande knop of ga naar https://iteamplay.nl/it-quick-scan/.

Vraag een gratis IT Quickscan aan

Kennis maken?

www.iteamplay.nl

info@iteamplay.nl

024 23 40 455

Microsoft Partner