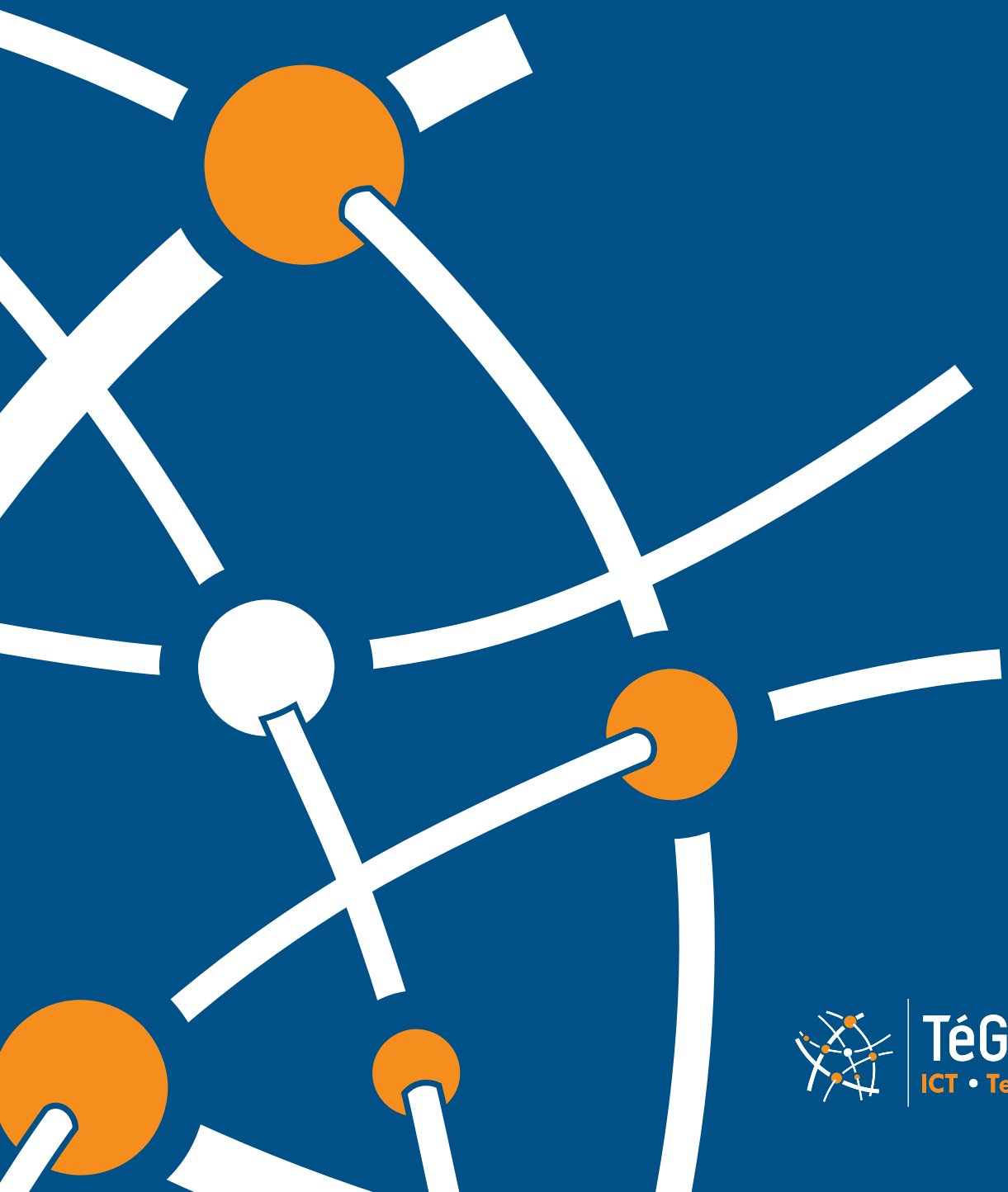
WHITEPAPER

SECURITY TIPS
VOOR HET MKB



TéGéTèl | HBA
ICT • Telecom Specialisten

SECURITY TIPS VOOR HET MKB

Hacking, phishing en ransomware: twintig procent van de Nederlandse bedrijven krijgt te maken met cybercrime (bron: **KPN**). Recente ransomware-aanvallen hebben laten zien hoe cruciaal ICT en telecom zijn voor het uitvoeren van de dagelijkse werkzaamheden. En dat geldt voor de meeste bedrijven. Het investeren in digitale veiligheid is dan ook noodzakelijk.

Wij delen in dit artikel graag een aantal security tips voor het mkb.

1. INSTALLEER SYSTEEM- EN SOFTWARE UPDATES DIRECT

Updates bevatten vaak patches om het systeem en de software beter te beveiligen. Het is dan ook belangrijk om deze updates direct te installeren. Gebruikers stellen het installeren van de updates vaak uit omdat het de dagelijkse werkzaamheden verstoord. Het is ook mogelijk om de updates zo in te stellen dat de gebruiker de installatie van deze updates niet (onbeperkt) kan uitstellen. Zo wordt voorkomen dat kwetsbaarheden ontstaan door systemen en software die niet up-to-date zijn.

2. GEBRUIK EEN VIRUSSCANNER EN FIREWALL

Een goede virusscanner en firewall vormen de basis voor security. Zorg dat een virusscanner en firewall zijn geïnstalleerd. Het eerste dat een hacker zal doen, is proberen om deze uit te schakelen. Wij adviseren dan ook om de virusscanner en de firewall onzichtbaar te maken. Zo voorkom je dat een eerste *security breach* resulteert in onnodig veel schade. Goede beveiliging bestaat uit meerdere lagen en verschillende voorzorgsmaatregelen.

3. GEBRUIK 2FA

Two factor authentication is een belangrijke stap in de beveiliging van accounts. Het inschakelen van *two factor authentication* (2FA) maakt dat een hacker niet zomaar met alleen een gebruikersnaam en wachtwoord in kan loggen op belangrijke accounts. 2FA kan op verschillende manieren worden ingesteld. Zo kan bijvoorbeeld worden gekozen voor 2FA met behulp van een SMS of authenticator (zoals bijvoorbeeld Google Authenticator of Microsoft Authenticator). Het is ook mogelijk om 2FA alleen in te schakelen wanneer vanaf een nieuw apparaat of locatie wordt ingelogd. Zo wordt voorkomen dat gebruikers *two factor authentication* als een vervelend proces beschouwen en worden de belangrijkste risico's beperkt.

4. KIES STERKE (UNIEKE) WACHTWOORDEN

Het gebruik van sterke wachtwoorden is een stuk eenvoudiger met behulp van een goede password manager. Het aantal accounts en wachtwoorden dat medewerkers moeten onthouden – zowel zakelijk als privé – maakt het aantrekkelijk om hetzelfde (makkelijke) wachtwoord voor meerdere accounts te gebruiken. Een password manager zorgt dat gebruikers zonder problemen sterke wachtwoorden kunnen gebruiken en voor ieder account een uniek wachtwoord kunnen gebruiken. Een sterk wachtwoord bestaat uit minstens 12 tekens. Gebruik zowel kleine letters als hoofdletters en cijfers en speciale tekens.

TéGéTèl HBA
ICT • Telecom Specialisten

SECURITY TIPS VOOR HET MKB

5. GEBRUIK EEN PASSWORD MANAGER

Een password manager zorgt niet alleen dat het werken met sterke en unieke wachtwoorden voor de gebruikers eenvoudiger wordt. Keeper Security biedt uitgebreide tools voor beheerders én gebruikers. Zo kunnen wachtwoorden met Keeper Security binnen het team worden gedeeld en kunnen beheerders monitoren hoe veilig het wachtwoordgebruik van de medewerkers is. Security start immers met het creëren van bewustzijn en het monitoren van potentiële bedreigingen.

6. MAAK BACK-UPS

Back-ups zorgen dat belangrijke informatie niet verloren raakt. Een verkeerde handeling van een medewerker of een ransomware-aanval kunnen grote gevolgen hebben als belangrijke data verloren gaat. Zorg daarom dat iedere dag minimaal 1 back-up wordt gemaakt van alle belangrijke gegevens. En zorg dat deze back-ups – in geval van nood – snel teruggezet kunnen worden.
Recente ransomware-aanvallen hebben laten zien hoe belangrijk data en ICT-systemen zijn voor het dagelijkse werk.

7. ZORG VOOR EEN AANSPREEKPUNT

Het kan natuurlijk gebeuren dat er ondanks alle voorzorgs-maatregelen toch een keer iets verkeerd gaat. En dan is het belangrijk dat medewerkers weten welke stappen ze moeten ondernemen en wie binnen (of buiten) de organisatie het aanspreekpunt is. Het is belangrijk om een incident zo snel mogelijk af te handelen. Of het nu gaat om data die per ongeluk verwijderd is door een medewerker of een security risk. Het is belangrijk dat medewerkers weten wie verantwoordelijk is en wie ze kan helpen het probleem op te lossen.

TéGéTèl HBA
ICT • Telecom Specialisten

SECURITY TIPS VOOR HET MKB

BEST PRACTICES

Wij delen tot slot nog een aantal best practices zodat je direct aan de slag kunt met het verbeteren van jouw security.

GEBRUIK ENCRYPTIE

Het gebruik van encryptie om de data op de harde schijf te versleutelen is verplicht conform de AVG. Persoonlijke gegevens en gevoelige informatie zijn voor hackers interessant. En voor bedrijven onmisbaar om hun dagelijkse werkzaamheden uit te kunnen voeren. Het gebruik van encryptie voorkomt dat (concurrentie)gevoelige informatie in verkeerde handen valt en dat je slachtoffer wordt van ransomware. Back-ups kunnen een deel van de schade van een ransomware-aanval beperken, maar een datalek moet worden gemeld. En dat kan serieuze gevolgen hebben voor je reputatie en het vertrouwen van klanten.

HET NEED TO KNOW-PRINCIPE

Het *need to know*-principe wordt binnen de security gebruikt om te bepalen welke rechten een gebruiker krijgt. Gebruikers krijgen alleen rechten om informatie in te zien en gegevens te bewerken wanneer dit voor hun functie noodzakelijk is.

DON'T BRING YOUR OWN DEVICE

Het komt steeds vaker voor dat medewerkers hun eigen devices gebruiken voor het werk. Het klinkt misschien als een aantrekkelijke optie, maar bring your own device brengt ook risico's met zich mee. Zeker op het gebied van security. Het is immers aan de werknemer om deze devices van de nodige beveiliging en updates te voorzien. Bovendien bestaat het risico dat bedrijfsinformatie verloren gaat op het moment dat de medewerker uit dienst gaat.

THUISWERKEN EN HYBRIDE WERKEN: ZORG ALTIJD EN OVERAL VOOR EEN VEILIGE WERKOMGEVING

Het hybride werken is een mooie combinatie van thuis en op kantoor (of op locatie) werken. Op de zaak werken de medewerkers op een beveiligd netwerk, maar hoe zit het met de veiligheid van het netwerk thuis en op locatie? En werken de medewerkers steeds op een device van de zaak of maken ze thuis gebruik van hun eigen devices? Het is belangrijk om medewerkers van een device te voorzien dat aansluit op hun werkzaamheden en behoeften. Zo wordt voorkomen dat medewerkers hun eigen devices gebruiken om thuis of op locatie te werken. Een online werkplek biedt uitkomst voor medewerkers die hybride werken: zo kan de veiligheid van data worden geborgd en hebben de medewerkers altijd en overal de beschikking over de noodzakelijke documenten en informatie.

TéGéTèl HBA
ICT • Telecom Specialisten

SECURITY TIPS VOOR HET MKB

BLIJF ALERT IN DE VAKANTIEPERIODE

Hoewel de meeste bedrijven in de vakantieperiode geopend zijn, is het op veel kantoren een stuk rustiger door de afwezigheid van collega's. En dat is een risico. Houd in de vakantieplanning rekening met de risico's op het gebied van veiligheid. Het komt helaas regelmatig voor dat beveiligings-risico's niet worden opgemerkt door afwezigheid van collega's. Zorg dus dat dit goed geregeld is. Het uitbesteden van de IT kan hier een goede oplossing voor zijn. Zorg dan in ieder geval dat de aanwezige medewerkers weten wie ze moeten bellen mochten er onverhoopt vragen zijn.

BEPERK HET AANTAL ACCOUNTS

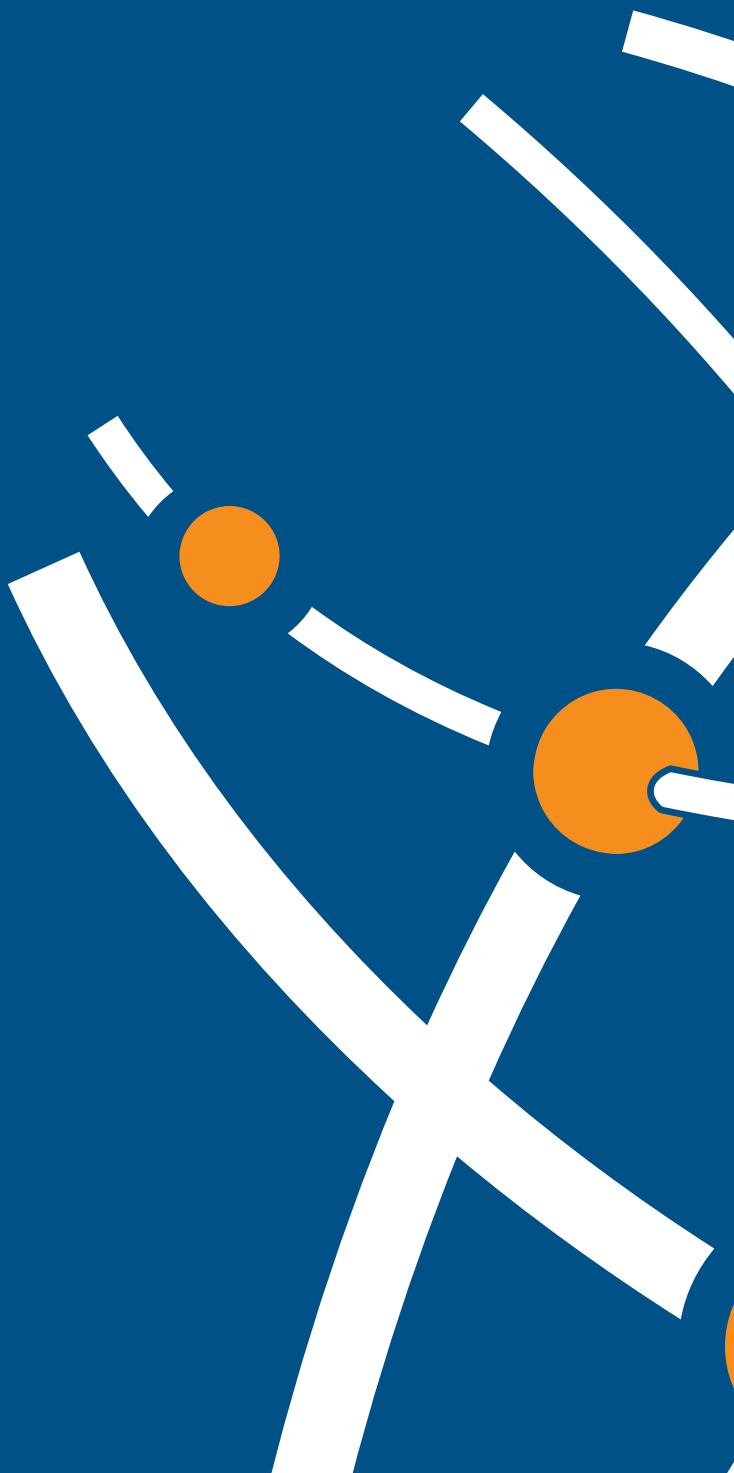
Het beperken van het aantal accounts maakt dat het een stuk eenvoudiger is om het overzicht te bewaren. Je loopt bovendien minder risico dat jouw gegevens op straat komen te liggen door een datalek bij een derde partij. En mocht er onverhoopt nieuws zijn over een datalek, dan heb je met een overzicht van je accounts snel inzicht in de stappen die ondernomen moeten worden.

Gebruik je een account niet meer? Probeer inactieve accounts op te zeggen en alle gegevens te laten verwijderen.

TéGéTèl | HBA
ICT • Telecom Specialisten

WETEN WAT SECURITY VOOR JOUW ORGANISATIE KAN BETEKENEN?

MAAK DAN EEN AFSPRAAK OP TEGETELHBA.NL/AFSPRAAK-MAKEN OF BEL NAAR 085 - 0479777.



TEGETELHBA.NL
085 - 0479777