27 JANUARI 2021

In deze whitepaper:

- *Veilige wachtwoorden*
- *Multifactor Authenticatie*
- *Is e-mail gevoelig voor hackers?*
- *BYOD: Bring your own device!*
- *Maakt u gebruik van de cloud?*
- *UnitIT Cyberverzekering*

AANDACHT VOOR EEN BEVEILIGDE IT-OMGEVING!

2020 heeft opnieuw uitgewezen dat digitalisering tegenwoordig hét begrip is. Het genereren en delen van data is nog nooit zo belangrijk geweest. Nieuwe technologieën zoals het werken in de Cloud zorgt ervoor dat we steeds meer verbonden zijn met ICT maar ook afhankelijker worden van ICT. Dat biedt kansen maar er zijn ook risico's aan verbonden.

Wanneer moet het systeem vervangen worden of een update krijgen? Hoe is de veiligheid van systemen gewaarborgd? Of hoe gebruik ik mijn systeem of software op de juiste manier? Zijn vragen welke bij ons dagelijks voorbij komen.

Lees in deze whitepaper hoe u uw IT-beveiliging kunt verbeteren!

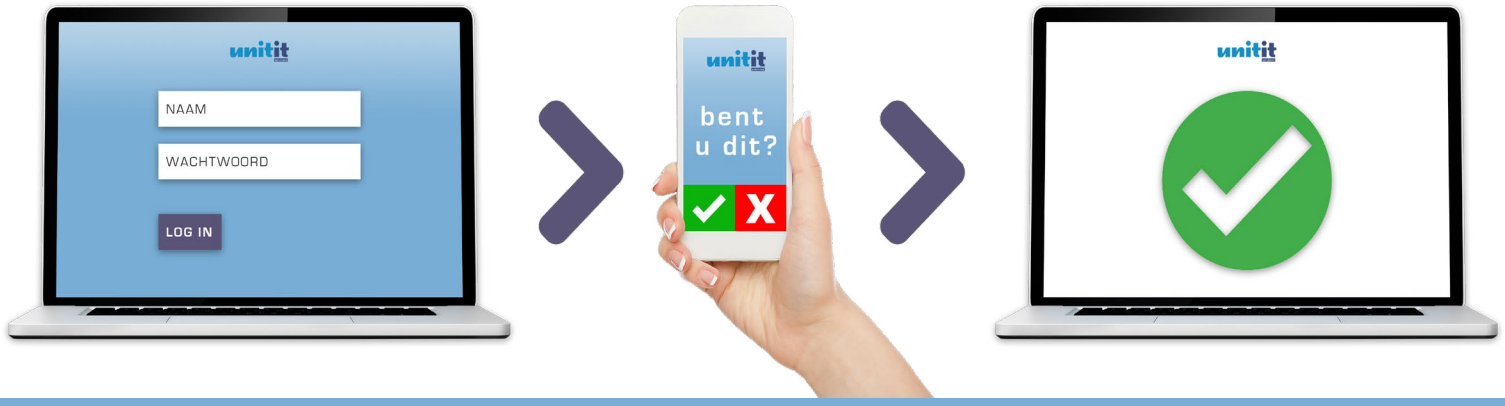
VEILIGE WACHTWOORDEN EN MFA

Maakt u gebruik van een sterk wachtwoord?

Wachtwoorden zijn de eerste verdediging om kwaadwillenden buiten uw organisatie te houden! Informeer uw medewerkers zo goed mogelijk over het belang van het gebruik van een sterk wachtwoord. Stuur bijvoorbeeld eens een e-mail rond om uw medewerkers hierop te attenderen. Of nog beter: een policy instellen binnen uw organisatie. Een andere methode is op technisch niveau het gebruik van sterke wachtwoorden afdwingen.

Wij horen u denken, hoe doe ik dit dan? Hier wat tips voor een sterk wachtwoord-beleid:

- Een wachtwoord omvat minimaal 8 karakters maar hoe meer karakters, hoe veiliger;
- Een wachtwoord bestaat uit minimaal 1 hoofdletter, 1 cijfer en 1 leesteken (-!@ etc.);
- Vervang regelmatig uw wachtwoord. U kunt dit als organisatie ook technisch afdwingen;
- Limiteer het aantal aanmeldpogingen;
- Het gebruik van Multifactor authenticatie (MFA).



Check, dubbelcheck

"Multifactor authenticatie" is een beveiligingsmethode waarmee een gebruiker in twee stappen zijn identiteit bij het inloggen kan aantonen. Naast het gebruik van een unieke gebruikersnaam met wachtwoord wordt een extra identificatie van de gebruiker geëist, meestal via een SMS, een app op de mobiele telefoon van de gebruiker of een RSA-token.

IS E-MAIL GEVOELIG VOOR HACKERS?

Het antwoord is ja! Ondanks de opkomst van videobellen zoals bijvoorbeeld Microsoft Teams, Zoom etc., is e-mail nog steeds de meest gebruikte vorm van communicatie tussen en binnen bedrijven. E-mailverkeer is daarom een belangrijk doelwit voor cyberaanvallen.

Wist u dat ruim 70% van alle cyberaanvallen wordt veroorzaakt door menselijke fouten? Door bijvoorbeeld het klikken op links in phisingmails. Net zoals de ICT-oplossingen slimmer worden, worden hackers helaas ook slimmer. Daarom is het van groot belang om bewustwording te creëren bij uw medewerkers zodat zij alert blijven en geen verkeerde links aanklikken . Hiermee bent u de hackers te slim af!

Vertrouwt u de e-mail niet? Pas dan deze tips toe!

- **Kijk altijd naar het e-mailadres van de afzender:** Ziet deze er betrouwbaar uit?
- **Let op met het openen van links in de e-mail:** Ga altijd eerst met uw muis op de link staan, voor u deze aanklikt. Door met de muis op de link te gaan staan, verschijnt het adres van de link. Ziet deze er betrouwbaar uit?
- **Let op de afsluiting:** Bedrijven maken vaak gebruik van een e-mailhandtekening waarin de gegevens van het bedrijf staan. Is er een fysiek bedrijfsadres, zijn er mogelijkheden om het bedrijf te contacten. Zien deze er betrouwbaar uit?

Twijfelt u nog steeds? Dan is het raadzaam om de e-mail te verwijderen!

BYOD: BRING YOUR OWN DEVICE

Wat handig dat u en uw werknemers vanuit huis kunnen werken met hun privé apparatuur. Maar niks is minder waar...

BYOD is de afkorting voor Bring Your Own Device en refereert aan de trend waarbij werknemers privé apparatuur inzetten voor hun werk. Het gebruiken van een eigen mobiele telefoon, laptop of tablet om werktaken uit te voeren zoals het lezen van e-mail, zorgt voor gebruiksgemak en flexibiliteit. We werken steeds vaker vanuit huis en vinden het dan fijn om eigen apparatuur in te zetten. Dit scheelt het heen en weer sleuren van apparatuur en we kunnen vaak goed overweg met onze eigen apparatuur. Ook als werkgever kan het gebruik van eigen apparatuur interessant zijn vanwege een potentiële kostenbesparing op de aanschaf van hardware.

Echter zitten er ook nadelen aan het inzetten van eigen apparatuur en thuiswerken. Met name zijn er de veiligheidsrisico's. Wanneer bedrijfsgegevens toegankelijk zijn of zelfs opgeslagen worden op privé-apparaten, kunnen organisaties in bepaalde mate de controle over deze data verliezen. Daarnaast zijn privé laptops, telefoons en thuisnetwerken vaak veel minder goed beveiligd dan uw bedrijfsnetwerk. Tips om thuiswerken veiliger te maken?

- Maak altijd gebruik van een VPN-verbinding;
- Zorg voor een proactief antivirusprogramma;
- Vermijd het gebruik van openbare Wi-Fi-netwerken;
- Maak duidelijke afspraken met uw werknemers over het gebruik van privé apparatuur;
- Maak afspraken met uw huidige ICT-partner om het beveiligingsniveau op te schalen of behoefte aan meer inzicht? Neem vrijblijvend contact op!

MAAKT U GEBRUIK VAN DE CLOUD?

Steeds meer applicaties en gegevensopslag draaien via de Cloud. Dit levert veel voordelen op zoals een kostenbesparing op onderhoud en flexibiliteit omdat u met elk device en vanaf elke locatie kan werken.

Wanneer u gebruikt maakt van de Cloud wordt dit vaak voorzien door een of meerdere externe partijen. Hierdoor weten bedrijven vaak niet meer goed waar nu precies welke data is ondergebracht. Kunt u onderstaande vragen met zekerheid beantwoorden?

- **Beleid en policy's:** Heeft u afspraken gemaakt hoe uw medewerkers zich aanmelden op uw omgeving en/of applicaties?
- **Netwerkbeveiliging:** Maakt u gebruik van firewalls en VPN-verbindingen? Wordt het gebruik van uw omgeving gemonitord?
- **Databeveiling:** Heeft u een back-up ingesteld? Gebruikt u encryptie? Hoe lang duurt het om uw data terug te zetten vanuit de Cloud?

Om cyberaanvallen te voorkomen is het van groot belang dat u zich bewust bent van de risico's die de Cloud met zich meebrengt. Blijf daarom altijd alert en kritisch wanneer uw gebruik maakt van de Cloud. Wij snappen dat het een enorme klus kan zijn om grip op uw data te houden en bieden daarom een kijkje in ons datacenter!

UNITIT CYBERVERZEKERING

Voorkom dat uw bedrijfsgegevens op straat komen te liggen. Loop geen imagoschade op door een hack, datalek of andere cybercriminaliteit.
Organisaties die slachtoffer worden van cybercriminaliteit hebben vaak de beveiliging niet op orde. Zo zijn systemen niet up-to-date, is er geen duidelijk beleid, wordt er gebruik gemaakt van verschillende applicaties die niet samenwerken en is er geen goede back-up oplossing. Gedupeerden komen hier pas achter als het te laat is. Wij helpen u graag uw beveiliging op orde te brengen met de UnitIT cyberverzekering.

De voordelen?

- Preventieadvies op maat; weet precies welke cyberrisico's uw bedrijf loopt;
- Bescherming tegen eventuele financiële gevolgen van hacking, systeeminbraak, verloren data, gegevensdiefstal en andere vormen van cybercriminaliteit;
- De juiste dekking bij schade.

Met ons continuïteitsplan zorgen wij ervoor dat u ten alle tijden kunt blijven werken!

HEEFT U VRAGEN OF WILT U MEER WETEN?

Neem vrijblijvend contact met mij of mijn collega's op.

Pierre Koopman
account manager MKB

06-15862167
p.koopman@unitIT.nl
www.unitit.nl/pierre