
# WHITEPAPER WACHTWOORDPOLICY

## IK LUST GEEN SPRUITJES.

HOE U EEN GOED VERTEERBARE WACHTWOORDPOLICY MAAKT

# WHITEPAPER

## IK LUST GEEN SPRUITJES.

Bij het lezen van deze kop denkt u ongetwijfeld ‘Wat heeft dat met ICT maken?’. Dat leggen uw u graag uit. Kinderen lusten vaak geen groente. Als ouder kunt u dan twee dingen doen. Straffen, of het eten van groente zo aantrekkelijk mogelijk te maken. Straffen kan werken, alleen maakt zonder strijd er met de overwinning vandoor het leven voor iedereen een stuk aangenamer. Dus bakt u er spekjes doorheen et voilà, overheerlijke spruitjes.

Hetzelfde geldt voor het instellen van een gedegen wachtwoordbeleid. We weten allemaal hoe belangrijk het is om een sterk wachtwoord te hebben. Toch schrijven we het liefst Welkom123 op een post-it en plakken dat onder onze laptop. Werknemers straffen om gedrag te stimuleren kan een optie zijn, maar wat nu als het gebruik van sterke wachtwoorden zo makkelijk wordt gemaakt, dat iedereen het zonder al te veel moeite toe kan passen?

In deze whitepaper leggen we uit waarom een gedegen wachtwoordpolicy van belang is, welke thema’s in dit beleid aan de orde moeten komen en hoe u de toepassing hiervan in de praktijk door de medewerkers zo makkelijk mogelijk maakt. Vandaar de spruitjes.

**De zwakste schakel**

Met alle commotie rondom cybercrime wordt security op de werkvloer vaak onderbelicht. De paniek in de media richt zich vooral op hacks en datalekken. Echter, wanneer het gaat om IT-security, is de mens de zwakste schakel. Reden te meer om deze te verstevigen met een gedegen beleid als het gaat om digitale veiligheid.

Een belangrijk onderdeel hiervan is het wachtwoordbeleid, een richtlijn voor medewerkers hoe om te gaan met wachtwoorden. Cruciaal hierbij is, zoals we al aangaven, dat dit werkbaar moeten zijn, anders wordt het niet toegepast.

**Wat niet mag ontbreken in een gedegen wachtwoordpolicy**

Om een gedegen wachtwoordpolicy op te kunnen stellen, dient u eerst de volgende 5 zaken in kaar te brengen.

1. Waaraan dient een sterk wachtwoord te voldoen?

63% van de werknemers in de leeftijdscategorie van 18 tot en met 34 jaar gebruikt hetzelfde wachtwoord voor meer dan drie logins. De reden hiervoor is gemakzucht, daar kunnen we eerlijk over zijn. Een goed wachtwoord moet aan nogal wat eisen voldoen en vergt aardig wat werk en creativiteit. Het moet bestaan uit verschillende soorten karakters, een minimale lengte hebben en niet bestaan uit logische of

### WAAR DIENT U OP TE LETTEN?

De BrainCheck is o.a. opgesteld aan de hand van fouten die bedrijven regelmatig maken. Deze punten zijn van belang voor ieder bedrijf, ongeacht grootte of branche. Met de opkomst van cybercriminaliteit is men geneigd om, gedreven door paniek en publieke opinie, de nadruk hier op te leggen. Echter, voor een bedrijf dat zijn algehele digitale veiligheid goed op orde wil hebben, is het van belang deze top 10 punt voor punt door te lopen.

makkelijk te raden woorden. Bovendien is het verstandig om voor elke applicatie een uniek wachtwoord te gebruiken. Immers, wanneer één account wordt gehackt, dan zijn alle accounts de klos. En zorg ervoor dat de wachtwoorden regelmatig worden aanpast.

2. Hoe maakt u een sterk wachtwoord?

Hoe complexer het wachtwoord, hoe complexer het wordt voor internetcriminelen om een account te hacken. Een stevig wachtwoord is daarom noodzakelijk voor online veiligheid. Maak geen gebruik van persoonlijke informatie, zoals naam, adres, geboortedatum of de naam van een huisdier, want deze informatie is eenvoudig te achterhalen via social media. Binnen bovenstaand kader over de basisvoorwaarden geven we hier een aantal slimme tips voor een creatieve invulling.

- Teken een motief op uw toetsenbord zoals een vierkant, een ruit of een letter. Start bijvoorbeeld bij de 5 en teken een 'Z', waarbij u grote en kleine letters afwisselt. Uw wachtwoord wordt dan '5^7yGvBn'.
- Schuif 1 letter opzij bij het typen van een woord op uw toetsenbord. Kies een (simpel) woord en tik de toetsen in die rechts van dat woord staan. Voeg een teken toe en gebruik grote en kleine letters. Het woord ‘oliebol’ wordt dan 'P;orNp;’
- Gebruik een acroniem. Verzin een zin en gebruik alleen de eerste letters van de woorden voor uw wachtwoord. Deze laatste zin zou kunnen leiden tot ‘VezegadeLvdWvuW’.
- Verzin een nieuw woord, dat kent niemand, alleen u. Of verzin een nieuwe taal waarbij u letters door cijfers vervangt. Een E is een 3, een A is een 4, de i is een 1, een o is een 0, etc.
- Typ in WhatsApp-taal, varieer met afkortingen en leestekens en haal de spaties eruit. De zin ‘Hoe laat vertrekt de eerste trein naar Amsterdam’ zou worden ‘Hltvertrektd1stetrain@Adam?’
- Gebruik alleen medeklinkers en voeg een cijfer toe. De zin ‘Hoe laat vertrekt de eerste trein naar Amsterdam’ zou worden ‘Hltvrtrktd1sttrnnr4mst3R3d4M’
- Vervang de woorden van een zin met leestekens, hoofd- en kleine letters. De zin ‘All my troubles seemed so far away” zou worden @mT$sF@
- Zorg ervoor dat u uw wachtwoorden regelmatig aanpast!

3. Hoe worden wachtwoorden veilig bewaard?

Wachtwoorden in een tekstdocument of op papier bijhouden is makkelijk maar onveilig. Om dit proces eenvoudiger én veiliger te maken zijn er hulpmiddelen in de vorm van programma’s en apps die, beveiligd met een wachtwoord of vingerafdruk, al uw wachtwoorden kunnen bewaren.


Deze oplossingen staan bekend als Password Managers. Voorwaarde is dat het ‘hoofdwachtwoord’ veilig is en alleen bij de gebruiker bekend is. Een voordeel van een Password Manager is dat deze moeilijke wachtwoorden aan kan maken. Kortom, een Password Manager maakt het eenvoudig om complexe wachtwoorden te genereren en te onthouden. En: zorg ervoor dat u uw wachtwoorden regelmatig aanpast.

4. Hoe wordt een veilig inlogproces ingericht?

Maak gebruik van twee-staps-verificatie (two factor authentication oftewel 2FA). Dit houdt in dat u, nadat u met u gebruikersnaam en wachtwoord bent ingelogd, nog een extra code moet invullen. Deze code ontvangt u via e-mail, sms of app. Omdat deze extra code op een ander device wordt

ontvangen, is het voor hackers onmogelijk om deze code te achterhalen. Let er daarom bij de keuze van een softwareleverancier op dat zij 2FA aanbieden.

Veel websites ondersteunen 2FA. Gebruik 2FA in ieder geval bij systemen waar gevoelige data staat, zoals CRM-, ERP- en FSS-omgevingen. Bovendien beschermt u in het kader van de AVG uw eigen en andermans gegevens op deze manier nog beter tegen datalekken en toegang door onbevoegden. En: zorg ervoor dat u uw wachtwoorden regelmatig aanpast.

5. Wat gebeurt er als er een wachtwoord uitlekt?

Neem in de policy op dat wanneer er sprake is van een uitgelekt wachtwoord er direct contact wordt gezocht met de servicedesk. Zodra er vastgesteld is of er sprake is van een lek kunnen er maatregelen genomen worden, wat alleen kan als er duidelijkheid over de situatie is. Ook kunt u controleren of uw wachtwoord is gelekt of gestolen bij de website van de politie en bij de website haveibeenpwned.com

Tot slot, en voor de vierde keer, zorg ervoor dat u uw wachtwoorden regelmatig aanpast. In ieder geval wanneer u ontdekt dat uw wachtwoord gelekt is. Kortom, maak uw policy aan de hand van bovenstaande inzichten en deel de tips die het uzelf en uw medewerkers makkelijk maken!

**Doe de BrainCheck**

Om u inzicht te geven in uw huidige niveau van digitale beveiliging en veiligheid, heeft BrainCap de BrainCheck ontwikkeld. De wachtwoordpolicy is hier onderdeel van.

De BrainCheck behandelt 10 punten die essentieel zijn met betrekking tot ICT-beveiliging en de veiligheid van de gegevens binnen een bedrijf en bestaat uit de volgende lijst van aandachtspunten:

- Back-up policy
- Gebruikersrechten
- Patchmanagement
- Wachtwoordpolicy
- Cloud Bestandsdeling en Synchronisatie
- Awareness
- Toegang van buitenaf
- Endpoint beveiliging
- Versleuteling van data
- Security Network Monitoring

Zegt niet alles u iets? Geen paniek, daar zijn wij voor. Nadat deze cruciale aandachtspunten besproken zijn, volgt er een rapportage met uw score op het gebied van digitale beveiliging en een aanbeveling. Met dit rapport kunt u zelf beslissen hoe u verdere invulling geeft aan een veilig ICT-beleid, waar we u uiteraard graag en vakkundig in adviseren. Neem contact met ons op via services@braincap.nl of bel ons op 088-2754800.

BRAINCAP
SOFTWARE & SERVICES