Nextens

KENNISDOCUMENT

SNEL EN TO THE POINT INZICHT

# DATAVEILIGHEID VOOR BELASTINGADVIES- EN ACCOUNTANTSKANTOREN

FISCAALTOTAAL

**Als medewerker van belastingadvies- of accountantskantoor werkt u met veel privacygevoelige gegevens van klanten. Deze zijn alleen bestemd voor een beperkt paar ogen en mogen absoluut niet op straat belanden. Met de komst van de Algemene Verordening Persoonsgegevens (AVG) is hier nog meer focus op komen te liggen en riskeert uw bedrijf zelfs een hoge boete als de dataveiligheid niet op orde is. Hoe gaat u om met data? Maakt u uw collega's voldoende bewust van het belang van dataveiligheid? En volgen zij uw advies en het protocol van uw bedrijf ook op?**

Henk Overbosch, Adviseur IT & Verandermanagement bij Docco, Romano Herrie, cyber security business development expert bij Fox-IT en onze eigen Nextens-expert op het gebied van dataveiligheid stellen allemaal dat een aantal, ogenschijnlijk simpele, dataveiligheidsaspecten nog vaak onderbelicht zijn in het bedrijfsleven. Dataveiligheid is voor veel accountants of fiscaal specialisten geen onderdeel van de dagelijkse praktijk en 'komt er dus een beetje bij'.

## CHECKLIST: ZIJN UW SYSTEMEN OP ORDE?

Uw systemen en die van collega's moeten goed beveiligd worden om dataveiligheid te waarborgen. Denk hierbij aan de volgende aspecten:

1. Up-to-date virusscanners
2. Up-to-date browsers
3. Unieke, moeilijk te achterhalen wachtwoorden
4. Two-Factor Authentication
5. Veilig netwerk
6. Encryptie op laptop, tablet en telefoon
7. Regelmatige back-ups

**1. Virusscanners updaten**
U heeft ongetwijfeld gezorgd dat u en andere medewerkers een virusscanner op de computer hebben. Maar is deze ook up-to-date bij iedereen? Zoals u natuurlijk weet, blijft software veilig en stabiel draaien dankzij de regelmatige updates van software-leveranciers. Zonder deze updates ontstaan er gaten in het systeem, waar hackers gebruik van kunnen maken. Hoe ouder dus de virusscanner, hoe minder malware deze tegenhoudt.

**2. Browser updaten**
Denk eraan dat ook de browsers van alle medewerkers up-to-date gehouden moeten worden. Accountants en belastingadviseurs staan

‘met de voeten in de modder’ en drukken deze updates in de waan van de dag vaak weg. ‘Dat komt later wel’, is de gedachte. Onze Nextens-expert waarschuwt: ‘Ik merk dat klanten soms nog met Windows XP inloggen, terwijl dit vanuit veiligheidsoogpunt door Microsoft niet meer wordt ondersteund.’

Maak medewerkers daarom bewust dat een up-to-date internetbrowser om meerdere redenen belangrijk is. De voornaamste reden is de beveiliging van je gegevens en surfgedrag om je privacy en veiligheid te kunnen waarborgen. Net als met de virusscanner geldt dat oude versies vaak makkelijker te hacken zijn. Ook de prestaties, weergave en mogelijkheden van de browser worden met elke nieuwe versie verbeterd.

**Tip!** Raad medewerkers aan om de automatische updates van hun browser aan te zetten. Door deze functionaliteit in te schakelen checkt de browser zelf regelmatig of er een nieuwere versie is.

**Let op** Nextens ondersteunt (onveilige) oude browsers, die geen TLS 1.2 of hoger hebben, niet meer.

**3. Wachtwoorden**

Een applicatie of software kan nog zo veilig zijn, ook bij een bedrijf en de individuele medewerkers ligt een verantwoordelijkheid om te zorgen voor dataveiligheid. Dit kan onder andere door het instellen van unieke en moeilijk te achterhalen wachtwoorden. Henk Overbosch van Docco ligt toe: “Als er een nieuwe gebruiker binnen de software wordt aangemaakt en die heet Piet met wachtwoord Welkom123, dan is dit vrij vlot te hacken. Focus op moeilijk te raden wachtwoorden en het regelmatig aanpassen hiervan is van groot belang.”

Wachtwoorden regelmatig aanpassen is niet het eerste waar medewerkers aan denken. Als zij, al dan niet verplicht, hun wachtwoord aan moeten passen, dan wordt het nieuwe wachtwoord vaak een variant van de vorige. Het is voor hun van belang om regelmatig een reminder te krijgen van het belang van goede wachtwoorden. Hierover leest u later in dit document meer.

**Tip!** Een sterk wachtwoord bestaat uit minimaal 10 karakters en is een mix van kleine en grote letters, cijfers en symbolen.

**Tip!** Laat uw collega's een veilige wachtwoordenkluis gebruiken, zoals Keepass of Lastpass. Deze kunnen ook random wachtwoorden aanmaken.

**4. Two-Factor Authentication**
Als uw medewerkers sterke wachtwoorden hebben ingesteld, kunt u hen stimuleren hier nog een extra beschermlaag aan toe te voegen: Two-Factor Authentication. Met deze methode worden twee verschillende factoren gebruikt om de identiteit van de gebruiker vast te stellen. Hierbij kunt u bijvoorbeeld denken aan het invoeren van een gebruikersnaam en wachtwoord, waarna uw collega een melding krijgt op zijn/haar telefoon om de identiteit te verifiëren.

**5. Veilig netwerk**
Met een slecht beveiligd draadloos netwerk is het voor hackers eenvoudig de gegevens van het bedrijf, de medewerkers én de klanten in te zien. Ook kan de internetverbinding misbruikt worden voor bijvoorbeeld het versturen van spam. Een beveiligd draadloos netwerk draait om het versleutelen van het signaal van de router. WPA2 is hierbij de beste encryptietechniek.

**Let op** Maak collega's alert van het gevaar van gratis WIFI in het café. Gegevens die over zo'n onbeveiligde verbinding worden verstuurd, kunnen makkelijk worden onderschept. Standaard werken met een VPN-verbinding kan hiervoor een oplossing zijn.

**6. Encryptie**
Het versleutelen van data en bestanden op alle (bedrijfs-)smartphones, tablets en laptops is aan te raden. Via volledige schijfencryptie kan een hacker niets met de harde schijf van de computer en is de data onleesbaar voor anderen. Mocht een computer of telefoon gestolen worden, dan kan de dief er niets mee.

De meeste vormen van versleuteling werken met een wachtwoord om de encryptie en latere decryptie mogelijk te maken. Ook hier geldt weer: een zwak wachtwoord geeft de hacker de mogelijkheid de encryptie eenvoudig te kraken. Zo valt de meerwaarde van versleuteling weg.

**Tip!** De BitLocker-software van Microsoft is een eenvoudig programma om schijfencryptie mogelijk te maken. Deze software is gratis in Windows 10, maar ook voor eerdere versies te downloaden.

**Let op** Is de data op het gestolen device onvoldoende beschermd, dan dient de verantwoordelijke in het bedrijf in het kader van de AVG melding te maken van een datalek. Indien er data op dit device staat dat niet met encryptie beveiligd is en persoonsgegevens bevat, is het in het kader van de AVG ook verplicht dit aan de betrokkenen te melden. Werkt uw bedrijf daarentegen volledig in de cloud (geen data lokaal) en is het device encrypted, dan is een vermelding in het interne 'Logboek datalekken' voldoende.

**7. Back-ups**

Mocht de hacker toch toegang krijgen tot (bedrijfs-)gegevens, dan kan het zo zijn dat deze verwijderd worden of niet meer toegankelijk zijn. Daarom blijft het belangrijk om regelmatig back-ups te draaien. Bij de meeste computers is het mogelijk om eenmalig een automatische back-up aan te zetten. Dan zijn opgeslagen documenten veilig.

**Let op** Cloudapplicaties zoals Nextens maken in veel gevallen al automatische back-ups van gegevens in de software, waardoor u (bedrijfs-)gegevens nooit definitief kwijt kunt raken.

## HEEFT U OOK GEDACHT AAN DE MENSELIJKE FACTOR?

Zoals eerder in dit document al aan de orde kwam, speelt de menselijke factor bij dataveiligheid een belangrijke rol. Uiteindelijk bepalen uw medewerkers of een maatregel werkt. Hierbij staan de volgende vragen centraal:

1. Hoe bewust zijn medewerkers van dataveiligheid?
2. Hoe wordt er omgegaan met medewerkers die vertrekken?
3. Hoe wordt ervoor gezorgd dat medewerkers hun wachtwoorden veranderen en systemen updaten?

**1. Bewustzijn medewerkers**
"Alles begint bij awareness", benadrukt Romano Herrie van Fox-IT. De systemen kunnen nog zo goed beveiligd zijn, als de medewerkers er niet naar handelen, dan bestaat er alsnog een risico dat de gegevens op straat komen te liggen. "Het is van belang dat er aandacht besteed wordt aan het 'waarom' van het beschermen van de data", voegt Henk Overbosch van Docco toe. Natuurlijk is het verplicht vanuit de AVG, maar dit moet niet de beweegreden zijn. De experts geven aan dat het een interne drijfveer moet zijn en daarbij is voorlichting essentieel. Denk bij deze voorlichting aan de eerste 7 punten in dit document, waaronder browserupdates en een digitale wachtwoordenkluis.

**Let op** Het klinkt wellicht als een open deur, maar de meeste datalekken ontstaan doordat een medewerker vertrouwelijke gegevens naar de verkeerde persoon mailt.

**Tip!** Monitoring en afdwingen van het online bedrijfsbeveiligingsbeleid kan bijvoorbeeld met MindYourPass worden gerealiseerd.

**2. Exitstrategie**
Er ontstaat ook een veiligheidsrisico als medewerkers vertrekken. Hoe gaat uw bedrijf daarmee om? Wie houdt de toegangsrechten bij? Dit is een aspect dat vaak vergeten wordt. Medewerkers maken veelal gebruik van een complex geheel van applicaties. Ze hebben niet alleen een inlogcode voor Outlook en Nextens, maar bijvoorbeeld ook van FiscaalTotaal, Exact Online en Snelstart. Voor al deze applicaties maken ze aparte wachtwoorden aan. Het is ingewikkeld en tijdrovend om na uitdiensttreding al deze applicaties te blokkeren.

U kunt voor medewerkers natuurlijk lijsten bij gaan houden, maar er zijn ook tools beschikbaar die dit een stuk makkelijker maken. Denk bijvoorbeeld aan Single Sign On software, waardoor een medewerker met één inlogcode toegang krijgt tot alle applicaties. Het handige daarvan is dat de medewerker niet alle wachtwoorden van de applicaties zelf kent en zodra de medewerker uit dienst treedt, hoeft u maar één account te blokkeren.

**3. Mobile device management**
Hoe geeft u medewerkers een duwtje in de rug om de protocollen voor dataveiligheid na te leven? Er kan natuurlijk encryptiesoftware op de laptops en telefoons van medewerkers staan, maar hoe controleert u dat deze ook 'aan' staat?

Met mobile device management, zoals bijvoorbeeld Microsoft Enterprise Mobility + Security, kunnen smartphones, tablets en laptops op afstand worden beheerd. Bijvoorbeeld op het gebied van security, updates, en het resetten van wachtwoorden.

## CLOUD

De experts van Nextens, Docco en Fox IT zijn het erover eens: een applicatie in de Cloud is in veel gevallen veiliger dan desktop-software. De beveiliging van de data ligt dan namelijk bij een partij die dat voor veel klanten doet en daar dus ook meer budget voor heeft. Er worden daarnaast hogere eisen gesteld aan deze dienstverlener en er worden continue back-ups gemaakt. Ook ontvangen grote bedrijven de zogenaamde security patches eerder dan particulieren. Een applicatie in de Cloud betekent dus dat u een deel van de beveiliging niet meer zelf hoeft te doen.

Fox IT benadrukt echter dat dit niet de focus op dataveiligheid mag verslappen. Ook bij gebruik van clouddiensten blijven bedrijven zelf verantwoordelijk voor de veiligheid van de data die zij beheren of verwerken. Daarnaast zullen bedrijven zichzelf ook de vraag moeten stellen: waar staat de data? Voor sommige partijen zou het namelijk een probleem kunnen vormen als de data in het buitenland gestald wordt. Houd dit zelf in de hand door vragen te stellen aan de provider.

**Wilt u meer lezen over de veranderingen van ons vak door digitalisering en automatisering?**
Zoekt u inspiratie hoe hiermee om te gaan?
Hebt u vragen als: hoe zorgt ik dat ik mijn klanten behoudt, hoe past ik de dienstverlening aan en welke verdienmodellen passen bij deze tijd?

Bekijk onze themapagina “Toekomst van het Vak” Bekijk thema