Beveiligingsbeleid

Alledaagse acitviteiten waar vrijwel niet bij stil wordt gestaan. Wij besteden met dit document extra aandacht aan de veiligheid van dagelijkse werkzaamheden.

- Heeft u binnen uw organisatie een beveiligingsbeleid opgesteld?
- Bent u zich bewust van de mogelijke digitale gevaren?
- Weet u tot op documentniveau de impact van dataverlies?

SAMEN VEILIG ONLINE WERKEN

TCA
SAMEN VEILIG ONLINE WERKEN

Boom&Co een groeiende organisatie waar dagelijks wordt gewerkt met verschillende bedrijfsapplicaties en data. Een veel gebruikte bedrijfsapplicatie voor Boom&Co is het CRM-systeem voor prospects en klanten. Boom&Co heeft werknemer Piet een laptop gegeven. Piet gebruikt deze zowel voor privé als zakelijke doeleinden. Ondanks dat Piet een hele harde werker is, staat hij niet altijd stil bij de mogelijke digitale gevaren.

Ook het MT ziet Piet als een betrouwbare en loyale werknemer. Als Piet 'even snel' klantgegevens wil opslaan, dan doet hij dat bij voorkeur op een lokale opslaglocatie van zijn laptop. Heel soms gebruikt hij een USB-stick. Ook verstuurt hij regelmatig klantgegevens via WeTransfer en download hij bestanden zonder na te denken over de opslaglocatie.

Boom&Co is zich niet bewust van:

- Dat Piet WeTransfer of de mail gebruikt om gevoelige informatie te delen
- Dat Piet van baan kan wisselen en hij alle klant- & bedrijsgegevens van Boom&Co eenvoudig kan meenemen
- Dat klant- en bedrijfsgevens (onbewust) in verkeerde handen terecht kunnen komen

In een veilige situatie werkt Boom&Co met een compleet beveiligingsbeleid

TCA
SAMEN VEILIG ONLINE WERKEN

In de praktijk hoort het zo

Piet wil een selectie van klantgegevens downloaden, om vervolgens de lijst via WeTransfer te versturen naar een ontvanger. Piet kan deze klantgegevens alleen downloaden in de downloadlocatie die is toegestaan door het informatiebeveiligingsbeleid. Boom&Co heeft hierin staan dat deze gegevens wel mogen worden opgeslagen op de bedrijfsopslaglocatie, maar niet op een lokaal apparaat (laptop/ USB-stick). Piet probeert nu het bestand met WeTransfer te versturen naar de ontvanger. Hiermee verlaat het bestand de (volgens het informatiebeveiligingsbeleid) toegestane bedrijfsomgeving. Piet krijgt een melding dat het niet op deze manier verstuurd mag worden. Dit wordt namelijk door het informatiebeveiligingsbeleid beperkt.

Hoe krijgt Piet de gegevens nu wel verstuurd? Piet moet dit melden bij zijn leidinggevende en die licht toe hoe hij deze bestanden veilig kan delen met de ontvanger.

Piet ziet daarnaast in alle documenten en e-mailberichten direct welk bijbehorend beveiligingslabel is toegekend. Hierdoor hoeft Piet niet zelfstandig te beoordelen of er belangrijke persoonsgegevens in documenten en/of e-mailberichten staan.

Mocht Piet toch een fout maken dan kan het MT de gegevensstroom analyseren en riskant gedrag direct detecteren. Hierdoor wordt misbruik van gegevens én de kans op datalekken voorkomen.

Met een zakelijke applicatie kan Piet een aanmerkelijke hoeveelheid persoonsgegevens met BSN-nummers versturen naar een ontvanger buiten Boom&Co. Ondanks het toegekende beveiligingslabel: ‘belangrijke persoonsgegevens’ is het Piet onduidelijk of hij deze gegevens intern/extern mag delen. Dankzij DLP wordt het versturen van belangrijke persoonsgegeven in dit geval gemaximaliseerd tot 10. Op het moment dat Piet een document verstuurd met meer dan 10 BSN-nummers wordt dit automatisch geblokkeerd.

Wilt u net zo veilig online werken als Piet? Wij helpen graag!

Het beveiligingsbeleid bestaat uit 3 elementen:

1. Applicatiebeveiligingsbeleid

Met behulp van het applicatiebeveiligingsbeleid kan Boom&Co verschillende rechten geven aan haar werknemers. Zo kan Piet dankzij het applicatiebeveiligingsbeleid alleen op voorgeschreven wijze 'beperkt' kopiëren, knippen, plakken en documenten verplaatsten.

2. Informatiebescherming

Dankzij informatiebescherming worden alle documenten waar belangrijke (persoons)gegevens in staan zoals, bijvoorbeeld creditcardgegevens en geboortedata beschermd en geclassificeerd met beveiligingslabels. Boom&Co kan alle documenten en e-mailberichten volgen en controleren hoe ze worden gebruikt. Ongeacht waar de gegevens worden opgeslagen of met wie ze worden gedeeld.

3. Dataverliesbescherming (DLP)

Als waardevolle aanvulling op informatiebescherming is dataverliesbescherming (DLP) nodig. Met DLP worden regels gedefinieerd. Alle regels hebben betrekking op het beschermen van de inhoud van e-mailberichten en documenten. Elke regel bestaat uit 5 componenten:

Voorwaarden:	naar wat voor type informatie bent u opzoek?
Actie:	als de juiste type informatie is gevonden, welke actie wordt dan gestart?
Notificeren:	notificeer de gebruiker over deze DLP-regel.
Ontwijken:	mag de gebruiker de DLP-regel vermijden bij een legitieme reden?
Rapporteren:	rapporteer alle regels in een bepaalde periode.