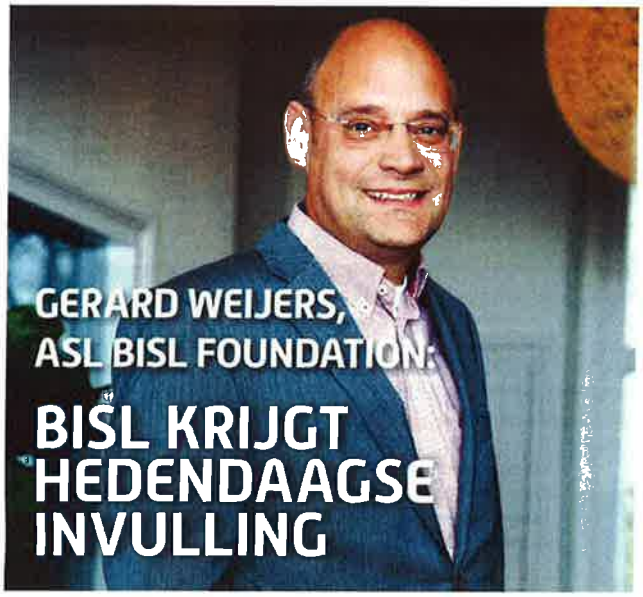
AutomatiseringGids
vak visie voorsprong>



EN VERDER: **AMPHIA ZIEKENHUIS CENTRALISEERT MONITORING** PROJECTPOLITIEK: EEN SLUIPMOORDENAAR **SLEUTELEN AAN DE KLOOF TUSSEN ONDERWIJS EN BEDRIJFSLEVEN**

PTI GAAT VOOR NIEUWE ISO 27001

Pincode Telenet in Woerden laat zich begin 2015 auditen voor een certificatie volgens de in 2013 geheel vernieuwde ISO-standaard 27001. Het bedrijf ziet er niet tegenop en heeft zich flink voorbereid. "Maar het is nooit af."

door: TANJA DE VREDE / T.D.VREDE@AUTOMATISERINGGIDS.NL **beeld:** DE BEELDREDAKTIE / JOOST HOVING

"Als aanbieder van een SaaS-applicatie verwachten klanten van ons dat de beveiliging op orde is en hun klandata veilig worden getransporteerd en opgeslagen", zegt contractmanager René Martina van Pincode Telenet BV (PTI) uit Woerden. "Daarnaast eisen wij dit op onze beurt van de partners waarmee wij samenwerken bij het leveren van onze diensten. Zij spelen een rol binnen de keten en bewerken op één of meerdere momenten tijdens het verwerkingsproces 'onze' klantdata. Dat moet veilig gebeuren."
PTI biedt oplossingen voor het verzamelen, bewerken en vastleggen van informatie uit verschillende datastromen. Daarbij kan het gaan om data afkomstig van (mobiel) internet, telefonie en fysieke documentenstromen. Een belangrijk product van het bedrijf is een SaaS-oplossing voor het verzamelen van meterstanden bij consumenten voor de energie- en waterbedrijven die PTI als klant heeft. Ook heeft het bedrijf een product ontwikkeld voor het plannen en managen van werkopdrachten; die oplossing ondersteunt werkzaamheden op fysieke locaties, onder meer met een app voor tablets.
Om aan te tonen dat PTI op een goede manier werkt, laat het bedrijf zich al sinds 2004 volgens ISO 9001 (kwaliteitsmanagement) certificeren. Sinds 2011 is PTI ook voor ISO27001 (informatiebeveiliging) met succes gecertificeerd. Met ingang van 2015 wordt voor ISO 27001 alleen nog gecertificeerd volgens de nieuwe versie 2013. PTI is dit voorjaar een van de eerste organisaties die zich volgens de nieuwe standaard laat certificeren.
"De ISO 27001-normering richt zich op informatiebeveiliging. Waar eerst vooral grote bedrijven zich certificeerden zie je nu dat ook kleinere bedrijven, zoals het onze, informatiebeveiliging hoog op de agenda hebben staan."

Commitment

De directie van PTI hecht veel belang aan informatiebeveiliging. Ze neemt deel aan het periodieke risico-overleg en minimaal tweemaal per jaar bespreekt de directie de stand van de informatiebeveiliging en wordt de risicoanalyse opnieuw uitgevoerd. Daarnaast krijgen twee medewerkers de ruimte flink wat tijd te besteden aan informatiebeveiliging en behoud van certificeringen. Martina werkt hiervoor nauw samen met kwaliteitsmanager Maaike van de Bovenkamp.
"ISO-certificatie begint met commitment van het management. Dat vertaal je in beleid. Vandaaruit zet je de beveiliging op. Vervolgens moet je steeds blijven toetsen of de informatiebeveiliging nog voldoet", zegt Martina.
Ook de geldende wettelijke eisen en regelgeving zijn bepalend voor de mate van informatiebeveiliging. De Wet Bescherming Persoonsgegevens, waarvan de eisen in 2013 zijn aangescherpt, stelt bewerkers van informatie medeverantwoordelijk voor het adequaat beschermen van persoonsgegevens van klanten. "Er is daardoor sprake van ketenaansprakelijkheid als er iets mis gaat bij het bewerken en verwerken van data. Gevolg hiervan is dat ook wij certificatie van onze partners eisen. Onze klant heeft de plicht te controleren of wij ons aan wet- en regelgeving houden bij de omgang met persoonsgegevens", zegt Martina. "Het is echter niet alleen de certificering op zich die voor ons telt. Het helpt ons ook de informatiebeveiliging op niveau te houden."

Nieuwe normen

In de vernieuwde normering 2013 is meer aandacht gekomen voor het onderkennen en minimaliseren van risico's, waar in de normering 2005 nog de focus lag op 'Plan-Do-Check-Act'. "Je kijkt naar de gehele organisatie, naar business continuity, wetgeving en het niveau van de informatiebeveiliging. Je stelt vast wat de risico's zijn die de organisatie loopt. Daar baseer je het beveiligingsbeleid op. Daarbij draait natuurlijk wel de PDCA-cyclus op de achtergrond", zegt Martina. Toch vindt hij de verschillen tussen beide normeringen wel meevallen. Het komt er wat hem betreft voornamelijk op neer dat een aantal van de beheersmaatregelen (controls) die voor PTI gelden vervalt, er een paar nieuwe bijkomen en sommige worden samengevoegd.
De nieuwe beheersmaatregelen hebben betrekking op veilig programmeren. Dit houdt in dat de organisatie in haar beleid moet opnemen dat bij het maken van programma's rekening gehouden wordt met beveiligingsaspecten. Deze moeten terug te vinden zijn in onder andere het functioneel- en technisch ontwerp. Martina: "Er zijn wel tools aanwezig om voor oplevering van (deel)programma's *code reviews* uit te voeren, maar dat is controle aan het eind van het ontwikkelproces. Na dit alles volgt het testen. Dit gebeurt op basis van functionele specificaties. Hieruit moet blijken dat we voldoen aan beschreven beveiligingseisen."
Ook in de nieuwe ISO-normering is het nogal eens puzzelen hoe iets bewezen moet worden. Martina: "Voor veilig programmeren kan het bijvoorbeeld betekenen dat je in de programmacode moet kijken of iets wel op de juiste, veilige manier is geprogrammeerd. Daarvoor heb je kennis van de materie nodig. Gelukkig hebben wij deze kennis in huis. Hadden wij die kennis niet zelf in huis gehad, dan zouden we hiervoor externe kennis hebben ingehuurd. We doen geen concessies. We willen stappen blijven maken in onze beveiliging."

IN DE NIEUWE NORMERING IS MEER AANDACHT VOOR HET ONDERKENNEN EN MINIMALISEREN VAN RISICO'S

R

7001

rtificatie volgens de
et tegenop en heeft

De Wet Bescherming Persoons-
zijn aangescherpt, stelt bewer-
ordelijk voor het adequaat
van klanten. "Er is daardoor
als er iets mis gaat bij het
ievolg hiervan is dat ook wij
. Onze klant heeft de plicht te
egelgeving houden bij de omgang
ina. "Het is echter niet alleen de
lt. Het helpt ons ook de informa-

s meer aandacht gekomen voor
van risico's, waar in de norme-
'Do-Check-Act'. "Je kijkt naar de
ntinuity, wetgeving en het
g. Je stelt vast wat de risico's zijn
r je het beveiligingsbeleid op.
CA-cyclus op de achtergrond",
chillen tussen beide normerin-
r hem betreft voornamelijk op
naatregelen (controls) die voor
we bijkomen en sommige worden

oben betrekking op veilig
organisatie in haar beleid moet
gramma's rekening gehouden
eze moeten terug te vinden zijn
technisch ontwerp. Martina: "Er
levering van (deel)programma's
is controle aan het eind van het
het testen. Dit gebeurt op basis
nt moet blijken dat we voldoen

het nogal eens puzzelen hoe iets
oor veilig programmeren kan het
programmacode moet kijken of
is geprogrammeerd. Daarvoor
Gelukkig hebben wij deze kennis
zelf in huis gehad, dan zouden we
gehuurd. We doen geen conces-
ken in onze beveiliging."

DACHT VOOR
AN RISICO'S

RENÉ MARTINA, RECHTS NAAST MAAIKE VAN DE BOVENKAMP:
'NIET ALLEEN DE CERTIFICERING OP ZICH TELT. HET
HELPT ONS OOK DE INFORMATIEBEVEILIGING OP
NIVEAU TE HOUDEN."

'WE DOEN GEEN CONCESSIES. WE WILLEN STAPPEN BLIJVEN MAKEN IN ONZE BEVEILIGING'

Begin 2015 gaat PTI op voor certificatie. Martina en Van de Bovenkamp zien er niet tegenop om de vernieuwde normering door te voeren. "Bij onze meest recente interne audit in 2014 is al getoetst naar de nieuwe normering. Zo komen we bij de aanstaande certificering niet voor verrassingen te staan", zegt Van de Bovenkamp.
Door de ervaring van eerdere jaren hebben Martina en Van de Bovenkamp een duidelijke marsroute voor ogen voor de certificering. De belangrijkste punten hiervan zijn:

1) **Doe een risico-inventarisatie.** Beschrijf en classificeer de risico's (samen met de directie).

2) **Bepaal de scope van certificering.** Welk deel van de organisatie en welke applicaties vallen er onder? Voor PTI is dat ontwerpen, ontwikkelen, op de markt brengen en onderhouden van de SaaS-applicatie. Daarvoor gelden 114 beheersmaatregelen. Beschrijf exact hoe dat goed moet worden geregeld.

3) **Stel een Statement of Applicability op.** "Daarvoor kijken wij samen met een geaccrediteerde partij naar de normen en beheersmaatregelen die voor ons gelden. Op het certificaat staat een verwijzing opgenomen naar de daarop van toepassing zijnde Statement of Applicability."

4) **Bepaal de maatregelen die nodig zijn** om aan de normen te voldoen en bepaal de manier en frequentie van toetsen.

5) **Plan audits.** Alle zogenoemde hoofdstukken van een ISO-certificering moeten periodiek worden getoetst. Het betreft hier in ieder geval één interne en één externe audit per jaar. Daarnaast kan een security audit gepland worden. Tijdens een interne audit toetst PTI, eventueel met inzet van externe expertise, of aan de genomen maatregelen wordt voldaan en of deze afdoende zijn.
Een voorbeeld is het hoofstuk over HR Security, daar staat de eis dat een bedrijf bepaalde informatie moet hebben over nieuwe medewerkers. "Wij eisen bijvoorbeeld een Verklaring Omtrent het Gedrag (VOG)", zegt Van de Bovenkamp. Ze toetst dat door een lijst namen van medewerkers op te geven waarvan ze de VOG wil zien. De HR-verantwoordelijke levert deze informatie als bewijslast. Als er een VOG ontbreekt, moet duidelijk worden hoe dat komt. Werkt de procedure niet goed, of is het een incident?

6) **Schakel een geaccrediteerde instantie in** voor de externe audit. Bij PTI is dat QMS International. Zij leveren de auditors.

7) **Kies passende security audits.** Security audits zijn er in verschillende soorten en maten. Afhankelijk van de infrastructuur, maar ook op verzoek van klanten kan getoetst worden hoe de informatiebeveiliging er werkelijk voorstaat.
Hierbij maakt PTI geregeld gebruik van ethische hackers. Dit audittype levert altijd nuttige informatie op dat PTI in staat stelt de beveiliging (nog) verder te verbeteren. Martina: "Het is niet zo dat leken eenvoudig naar binnen kunnen, maar de specialisten zien vaak wel mogelijkheden om de beveiliging te verbeteren."

Tips bij certificering

- **Onderschat de impact niet**
  Van de Bovenkamp en Martina zijn ieder jaarlijks zeker 40 dagen bezig met informatiebeveiliging. Daarbij zijn de interne controles (audits) inbegrepen die per persoon zeker 16 dagen vergen. "Het aantal dagen is een schatting, want het zit nu helemaal in je systeem – bij alles wat je doet denk je gelijk aan informatiebeveiligingsaspecten. En dan zijn wij al een paar jaar bezig waardoor het bijwerken van documentatie grotendeels een kwestie is van bijhouden. De beveiliging gaat wel steeds een stukje verder, al was het maar door steeds nieuwe dreigingen.
  Ook de overheid hecht steeds meer waarde aan privacy en veiligheid, wat resulteert in meer regeldruk. Zo is een wetsvoorstel in behandeling met betrekking tot meldingsplicht wanneer mogelijk privacygevoelige gegevens zijn ontvreemd of op straat komen te liggen. Deze wetgeving eist de benoeming van een 'privacy officer' in je organisatie. Houd daar rekening mee. Beveiliging is nooit af, het blijft in beweging. Je bent er altijd mee bezig", aldus Van de Bovenkamp.
- **Zorg voor een goed managementsysteem**
  "Van groot belang is het ISMS(information security management system). Gebruik hiervoor een geschikte tool. Dat is een zeer belangrijke ondersteuning voor het hele certificatietraject. Je kunt het echt niet een jaartje rustig aan doen als je gecertificeerd wilt blijven. Een goede ISMS-tool moet in elk geval de volgende functionaliteit bieden: auditplanning, de frequentie van controles kunnen invoeren, taken kunnen aanmaken met daaraan gekoppeld een vervaldatum, handige overzichten zodat je snel ziet wat nog open staat, en het moet ook zeker makkelijk in het gebruik zijn. Daarnaast is het handig als je de testprocedure per genomen maatregel hierin beschrijft, bewijslast kan koppelen en risico's kan administreren en classificeren", aldus Martina.
- **Zorg voor commitment en verhoog de awareness**
  "Commitment van de directie en awareness bij de medewerkers zijn van het grootste belang. Zorg voor vaste overlegstructuren waarin de risico-issues worden besproken en acties en besluiten worden vastgesteld. Certificering kun je er niet zo maar even bijdoen. Het moet echt op de agenda staan. Praat je medewerkers geregeld bij om de betrokkenheid en awareness te verhogen.", aldus Van de Bovenkamp.
- **Gebruik de uitleg uit ISO 27002**
  Martina: "ISO laat je redelijk vrij om eigen invulling te geven aan de te treffen maatregelen. Een voorbeeld: er wordt geëist dat je voor veilige wachtwoorden zorgt. Maar wat is dan veilig? Zes- of tien posities? Als jij geen IT'er bent, hoe bepaal je dan wat veilig is voor jouw organisatie? ISO 27002 geeft per beheersmaatregel uitgebreid weer wat je kunt doen om hieraan te voldoen. Deze uitleg helpt je een beeld te vormen over de inhoud en betekenis van de betreffende beheersmaatregel."
- **Zorg voor een privacy officer**
  Diverse meldingsplichten die de overheid binnenkort invoert, vereisen de komst van privacy officer in je organisatie. Houd daar rekening mee.