Elco Stofbergen heeft een lange staat van dienst in de informatiebeveiliging, zowel bij de overheid als in het bedrijfsleven. Hij werkte onder meer bij het Nationaal Cyber Security Center. Tegenwoordig is hij thought leader cybersecurity bij CGI. Stofbergen stelt dat de digitale transformatie van de overheid vraagt om een nieuwe aanpak van informatieveiligheid: “Niet meer, maar anders. Een aanpak die inspeelt op de essentie van deze transformatie. Namelijk dat digitalisering is doorgedrongen tot in de haarvaten van organisaties en de samenleving. Technologie is een randvoorwaarde geworden voor overheidsdienstverlening. Dat maakt dat we heel kwetsbaar zijn geworden voor cybercrime en andere vormen van cyberdreigingen. Dat betekent dat we informatieveiligheid vanaf het begin moeten meenemen in software, processen en werkwijzen. Het is als het maken van een auto: daarin moet je vanaf het begin remmen en airbags inbouwen.”

Door de digitale transformatie van de overheid neemt de afhankelijkheid van technologie en data toe. En daarmee de kwetsbaarheid. Dat vraagt om een andere aanpak, waarin informatieveiligheid is ingebed in de organisatie, in de processen en systemen. “Eigenlijk gaat het om digitaal verantwoord besturen”.

Informatieveiligheid moet in het DNA

Zo’n aanpak, die ook wel security-by-design of security-by-default wordt genoemd, ziet Stofbergen nog niet veel: “De aandacht voor informatiebeveiliging blijft helaas achter bij de inspanningen op het gebied van digitalisering.” Hoe dat kan? “Informatiebeveiliging is van oudsher een onderwerp dat naast de corebusiness staat. Het is iets van de IT-afdeling, iets dat er later wordt bijgehaald.” In de praktijk betekent dat dat organisaties bijvoorbeeld enthousiast inzetten op de mogelijkheden van informatiegestuurd werken, met analyse van big data, maar dat ze de beveiligings- en privacyaspecten daarvan niet vanaf het begin meenemen. Het heeft te maken met de focus van het bestuur, dat aandacht aan dit onderwerp hoort te geven maar dat nog onvoldoende doet, stelt Stofbergen. Maar het heeft ook te maken met verschillende culturen in organisaties. “Je hebt aan de ene kant de veranderaars, de ‘believers’ die in technologie vooral kansen zien. En aan de andere kant de mensen van de informatiebeveiliging en de IT-afdeling, die gechargeerd gezegd vooral de risico’s zien en veranderingen willen tegenhouden.”

Hij denkt dat er meer verbinding moet komen tussen beide culturen, want alleen dan krijgt informatieveiligheid de aandacht die nodig is: “De innovators moeten meer oog krijgen voor veiligheid en de beveiligers zullen echt veel meer moeten meedenken met de organisatie.” In ontwikkelmethodieken als Agile en DevOps werken programmeurs en beheerders samen in teams die software ontwikkelen. Informatiebeveiligers zouden daar goed deel van kunnen uitmaken, zegt Stofbergen.

Er is nog een reden waarom informatiebeveiliging vanaf het begin onderdeel moet zijn in een ontwikkelproces: “De digitale transformatie wordt gekenmerkt door ontwikkelingen die elkaar heel snel opvolgen. Daarom moet je alle aspecten meteen vanaf het begin voldoende aandacht geven. Achteraf inbouwen is geen optie, want dan is er alweer een nieuwe technologie.” Het komt erop neer dat informatieveiligheid een vast onderdeel wordt van de organisatie, zegt hij: “Het moet onderdeel zijn van het organisatie-DNA.” Dat is een bestuurlijke verantwoordelijkheid, stelt hij. Het betekent bijvoorbeeld dat een organisatie in haar visie en informatiebeveiligingsstrategie uitwerkt welke eisen ze stelt aan de gebruikte systemen en hoe men in dit opzicht zaken doet met leveranciers. “Of je nu systemen maakt of koopt of een dienst afneemt, het gaat erom dat je informatieveiligheid als een cruciale randvoorwaarde neerzet. Dat je ook op dit gebied duidelijke eisen stelt aan je leveranciers.” Door de afhankelijkheid van IT zijn de risico’s als het misgaat immers groot, dan kun je er niet op vertrouwen dat de leverancier “het wel goed heeft geregeld”, zegt hij. Kortom: informatieveiligheid is een bestuurlijke verantwoordelijkheid.

Foto: Dreamstime

Eelco Stofbergen, thought leader cybersecurity bij CGI: “Het gaat erom dat je informatieveiligheid als een cruciale randvoorwaarde neerzet.“

‘Nederland niet goed beschermd tegen cyberdreigingen’

Nederland is een aantrekkelijk doelwit voor cybercriminelen, hackers en cyberspionnen en zou veel meer moeten investeren in digitale weerbaarheid. Dat concludeert het Rathenau Instituut in het rapport ‘Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid’. Het instituut deed het onderzoek op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Een paar conclusies: buitenlandse inlichtingendiensten vormen de grootste dreiging, zij vallen stelselmatig technologiebedrijven en overheidsinstellingen aan om militaire, technologische en politieke informatie te verzamelen. Cybercriminelen gebruiken steeds geavanceerdere methoden om informatie en geld te stelen. Het Internet of Things vergroot de kwetsbaarheid voor cyberdreigingen.

Het Rathenau Instituut pleit voor een aantal maatregelen voor het vergroten van de digitale weerbaarheid, bijvoorbeeld een jaarlijkse ‘hacktest’ bij vitale sectoren zoals de zorg- en energiesector. De overheid zou daarnaast als grote IT-inkoper bij haar eigen inkoop cybersecurity veel zwaarder moeten laten wegen.

Symposium ‘Grip op cybersecurity’

Op 22 mei organiseren de Cyber Security Raad en iBestuur het symposium ‘Grip op cybersecurity’, in Nieuwspoort te Den Haag. Eelco Stofbergen is één van de sprekers. Meer informatie over het programma en aanmelden op: ibestuur.nl/symposium.