Ziekenhuizen en energiebedrijven gaan wellicht boeten voor beveiligingsfouten

Nieuwe IT-wet bedoeld om 'potentiële maatschappelijke ontwrichting' te voorkomen

Axel Arnbak

ILLUSTRATIE: HEIN DE KORT VOOR HET FINANCIEELE DAGBLAD

Afgelopen zomer vielen wereldwijd ziekenhuizen, fabriekslijnen en energiebedrijven stil door de inmiddels beruchte cyberaanvallen WannaCry en NotPetya. De ontwrichtende ransomware-incidenten hebben het karakter van cybersecurityregulering voorgoed veranderd. Nederland was op grond van een Europese richtlijn al een tijdje verplicht een cybersecuritywet aan te nemen. Tot voor kort bleven de voorstellen vooral steken in abstracte normen over 'adequate beveiliging' en meldingsplichten bij incidenten. Sinds de gijzelsoftware-incidenten van de zomer, zijn toezicht en hoge boetes de nieuwe mantra.

Gek genoeg lijkt bijna niemand dit nieuwe strenge elan te hebben opgepikt. Misschien zijn de media te veel gefocust op de veelbesproken Europese Algemene Verordening Gegevensbescherming, de buitengewoon strenge privacywet die vanaf 25 mei 2018 in Nederland van kracht wordt. Of op een ander wetje over een meldplicht bij cyberincidenten, in juli als hamerstuk aangenomen in de Eerste Kamer. Maar de voorgestelde 'Cybersecuritywet' is het echte werk. Niet zozeer voor datagulzige internetbedrijven, maar juist voor organisaties die voorheen weinig met privacy van doen hadden.

Privacywetgeving kennen we al decennia. Organisaties die structureel veel data verwerken — grote retailers, banken en verzekeraars — beseffen dat IT-beveiliging essentieel is om aan privacywetten te voldoen. Voor organisaties die nauwelijks persoonsgegevens verwerken bestaan weinig tot geen wettelijke cybersecurityverplichtingen. En laat nu juist energiebedrijven (Rosneft), advocatenkantoren (DLA Piper) en autofabrikanten (Renault-Nissan) het hardst zijn getroffen door de ransomware-aanvallen. Zonder wetgeving staat IT-beveiliging binnen zulke organisaties niet altijd even hoog op de agenda.

De voorgestelde Cybersecuritywet probeert dat te veranderen. De wet wil niet alleen de vertrouwelijkheid van data waarborgen, maar ook garanderen dat de Deltawerken alleen door bevoegde personen worden aangestuurd ('integriteit'). En dat het betalingsverkeer niet door een puberale DDoS-aanval kan worden verlamd ('beschikbaarheid'). De wet focust op de grote incidenten en reguleert 'essentiële dienstverleners', organisaties die ons voorzien van drinkwater, stroom, geld, transport, gezondheidszorg en internetverkeer. Zo hoopt de wet 'potentiële maatschappelijke ontwrichting' door IT-incidenten te voorkomen.

Cruciaal detail: de 'essentiële dienstverleners' worden bij ministeriële regeling aangewezen. Na een groot IT-incident kan een minister zonder tussenkomst van het parlement sectoren labelen als 'essentieel'. Bijvoorbeeld, als terroristen passagiersvliegtuigen kunnen besturen via het entertainmentsysteem (Panasonic Avionics hack, 2016) of duizenden 'connected cars' tegelijk vanaf een laptop thuis kunnen laten remmen (FiatChrysler Jeep hack, 2015). Naarmate onze netwerksamenleving verder verknoopt en de incidenten heftiger worden, zullen ministers de lijst 'essentiële diensten' uitbreiden.

'Essentiële dienstverleners' worden door de minister aangewezen

Om de nieuwe verplichtingen kracht bij te zetten, introduceert de Cybersecuritywet overheidstoezicht op de naleving ervan. Anders dan bij privacy, belast het wetsvoorstel terecht de sectorale waakhonden met het cybertoezicht op hun sector. De Inspectie voor de Gezondheidszorg zal waken over de zorg, de zorgminister over de 'essentiële diensten' in de sector. Die benadering snijdt hout. De Autoriteit Persoonsgegevens kan ook niet in haar eentje de hele datawereld in het gareel houden. Bovendien mogen toezichthouders bij wanbeleid een boete opleggen tot € 5 mln per incident. Die boetebevoegdheid is nieuw, onopgemerkt en staat ook in de Britse cybersecuritywet, die kort na de ransomware-aanvallen van de zomer is geïntroduceerd. Ineens zien politici dat cybersecurity naast normen ook toezicht en boetes nodig heeft.

Cybersecurity en privacy volgen het model van het mededingingsrecht: normen, toezicht én boetes moeten cultuurverandering brengen. Het zou me niet verbazen als over vijf of tien jaar de reikwijdte, boetes en andere maatregelen in de Cybersecuritywet strenger worden en de nu strikte privacywetten juist iets milder. Voor veel mensen is privacy vooral een kosten-batenanalyse ('geef mij gratis gemak, en je krijgt mijn data'). Cybersecurity is eerder zwart-wit ('verboden toegang voor onbevoegden'). Dat basale gevoel zal zich vertalen naar toezicht. Voor ziekenhuizen en energiebedrijven die beveiligingsblunders maken, verwacht de samenleving een fikse boete.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Voor reacties: @axelarnbak