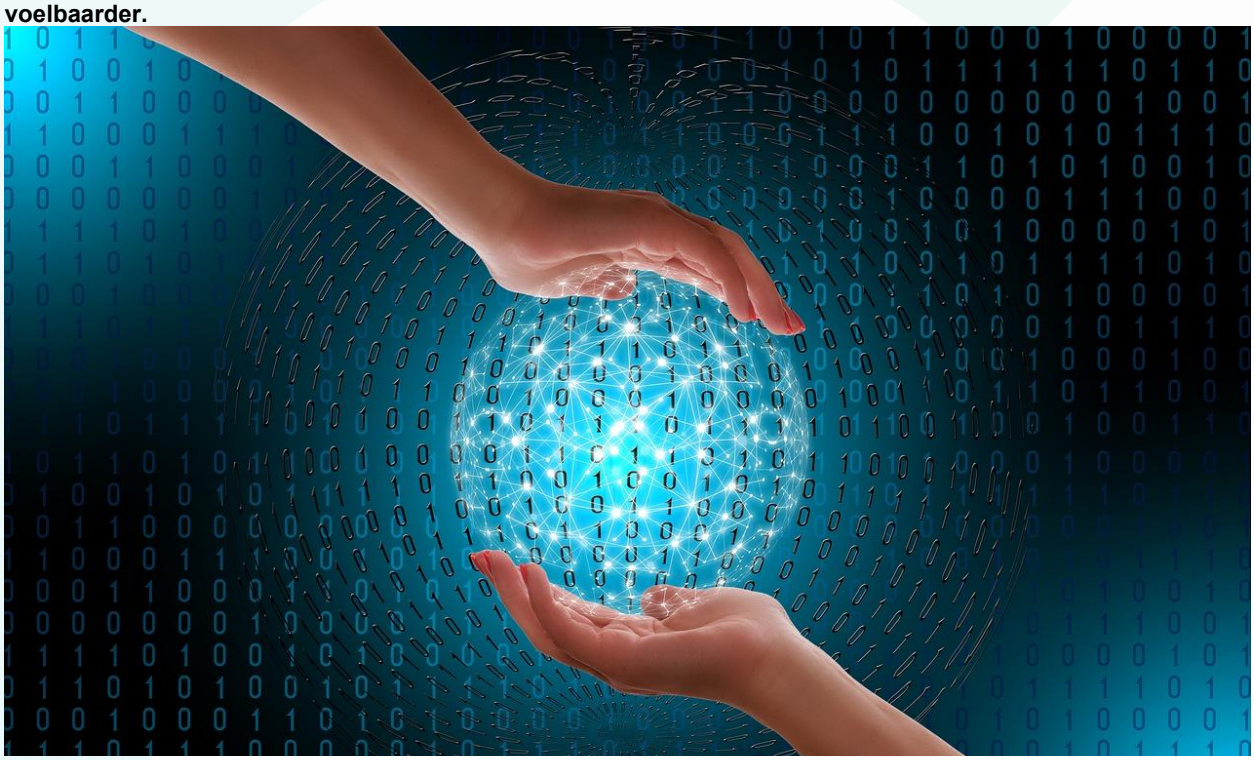
Cybersecurity vraagt om een andere manier van samenwerken

Niet nóg meer regels, maar bestuurlijke stelselvorming en gedeelde verantwoordelijkheid

Ir Philip J. van Klaveren, bestuursadviseur samenwerken bij Common Eye BV; verbinder van bestuurders • Zorg • ICT • Cybersecurity • Zorgcontractering & allianties die werken

Cybersecurity staat inmiddels stevig op de bestuurlijke agenda. Bestuurders in gemeenten, zorginstellingen, onderwijs, waterschappen en vitale sectoren voelen dagelijks dat digitale dreigingen toenemen. Tegelijkertijd groeit het ongemak: ondanks toenemende investeringen in maatregelen, audits en toezicht blijft de digitale weerbaarheid achter. Incidenten worden complexer, afhankelijkheden groter en de impact maatschappelijk voelbaarder.



De gebruikelijke reflex is om te grijpen naar extra regels, strengere controles of aangescherpt toezicht. Maar de vraag is of dat ons werkelijk verder helpt. Wie beter kijkt, ziet dat cybersecurity geen technisch probleem is dat je met techniek oplost, maar een bestuurlijke samenwerkingsopgave. Een opgave die vraagt om andere vormen van sturing, andere gesprekken en vooral: andere relaties.

De digitale werkelijkheid is een netwerk

In de fysieke wereld is vaak helder wie verantwoordelijk is voor veiligheid. In de digitale wereld ligt dat fundamenteel anders. Organisaties zijn via systemen, data en leverancierssketens diep met elkaar verweven. Een kwetsbaarheid bij een kleine leverancier kan grote gevolgen hebben voor publieke dienstverlening, zorgcontinuïteit of vitale infrastructuur.

Cybersecurity is daarmee geen hiërarchisch vraagstuk, maar een netwerkvraagstuk. Geen enkele organisatie heeft volledige regie, maar iedere organisatie draagt wel bij aan het gezamenlijke risico. Dat maakt klassieke sturingsmechanismen kwetsbaar. Regels blijven nodig, maar zijn onvoldoende om grip te krijgen op een dynamisch en onderling afhankelijk systeem.

Waarom samenwerken zo moeilijk blijft

Dat samenwerking rond cybersecurity zo moeizaam van de grond komt, heeft een aantal hardnekkige oorzaken. Allereerst zijn er juridische en institutionele grenzen aan informatie-uitwisseling. Wetgeving beschermt terecht gevoelige informatie, maar belemmert in de praktijk ook het delen van dreigingsbeelden en incidentervaringen. Daardoor blijft collectief leren achter. Daarnaast kijken betrokken partijen vanuit verschillende logica's. Toezichthouders richten zich op naleving en

handhaving. Securityprofessionals denken in risico's, dreigingen en responstijden. Bestuurders zoeken naar strategische afwegingen tussen veiligheid, continuïteit en betaalbaarheid. Al deze perspectieven zijn legitiem, maar sluiten niet vanzelf op elkaar aan.

Ten slotte ontbreekt vaak het besef van wederzijdse afhankelijkheid. Veel organisaties ervaren cybersecurity nog als een interne aangelegenheid, terwijl incidenten juist ontstaan in de keten. Dat versterkt de neiging om naar binnen te kijken, terwijl het probleem zich tussen organisaties afspeelt.

Een stelsel dat nog niet af is

Nederland beschikt over veel capabele organisaties op het gebied van digitale veiligheid: toezichthouders, inspecties, sectorale CERT's, opsporingsdiensten en kenniscentra. Ieder vervult een eigen rol en verantwoordelijkheid. Maar samen vormen zij nog geen samenhangend stelsel.

Het geheel functioneert te vaak als een verzameling eilanden. Ketenrisico's blijven onderbelicht en er is weinig structurele afstemming over rollen, verantwoordelijkheden en gezamenlijke leerprocessen. In andere veiligheidsdomeinen – zoals waterveiligheid of crisisbeheersing – is die stelselmatige benadering veel verder ontwikkeld. De digitale wereld vraagt om een vergelijkbare volwassenheid, zonder dat alle bevoegdheden bij één partij hoeven te liggen.

Vier principes voor betere samenwerking

Wat helpt dan wel? In de praktijk tekenen zich vier samenwerkingsprincipes af die richting kunnen geven aan bestuurlijk handelen. Ten eerste vraagt effectieve samenwerking om meer gelijkheid in informatieposities. Bestuurders moeten investeren in vertrouwensrelaties en veilige vormen van informatie-uitwisseling, zodat partijen een gedeeld beeld hebben van risico's en afhankelijkheden. Niet alleen verticaal, maar juist ook horizontaal, tussen organisaties die elkaar nodig hebben.

Ten tweede verschuift de focus van regels naar gedeelde verantwoordelijkheid. Wet- en regelgeving blijven noodzakelijk, maar echte weerbaarheid ontstaat wanneer organisaties zelf eigenaarschap nemen voor hun rol in de keten. Toezicht kan daarbij bijdragen door leren en verbeteren actief te stimuleren, niet alleen door te handhaven. Ten derde is ketenbewustzijn cruciaal. Digitale veiligheid is geen taak van de ICT-afdeling, maar een strategische opgave voor de hele organisatie en haar partners. Bestuurders moeten weten waar hun organisatie kwetsbaar is door afhankelijkheden van leveranciers, platforms en andere partijen, en welke gezamenlijke investeringen nodig zijn.

Ten slotte vraagt digitale weerbaarheid om een cultuur van openheid. Incidenten zullen blijven gebeuren. De vraag is niet hoe we ze voorkomen, maar hoe snel en gezamenlijk we ervan leren. Openheid over incidenten is bestuurlijk spannend, maar geslotenheid is uiteindelijk veel risicovoller.

Wat bestuurders vandaag al kunnen doen

Deze principes zijn niet abstract. Bestuurders kunnen vandaag al stappen zetten. Door digitale veiligheid expliciet te agenderen in bestuurlijke netwerken met ketenpartners en leveranciers. Door te vragen om inzicht in ketenrisico's in plaats van uitsluitend interne audits. En door transparantie over incidenten actief te waarderen en te normaliseren als onderdeel van professioneel handelen.

Tot slot

Cybersecurity is te belangrijk om te reduceren tot een technisch dossier of een compliancevraagstuk. In een wereld waarin alles met alles verbonden is, wordt digitale weerbaarheid vooral bepaald door de kwaliteit van samenwerking, vertrouwen en gezamenlijke verantwoordelijkheid.
De kernvraag is dan ook niet of we meer moeten doen, maar hoe?

- niet door steeds nieuwe regels toe te voegen,
- maar door elkaar beter te vinden
- niet door harder te sturen
- maar door slimmer samen te werken.

Digitale veiligheid begint niet bij technologie, maar bij bestuurlijke volwassenheid. En die ontstaat alleen in samenwerking.

Contact en doordenken?

philip@commoneye.nl
06-22417709
Met dank aan mijn collega Edwin Kaats, partner bij Common Eye BV