



Digitale weerbaarheid in de zorg: Waarom organisaties nú in actie moeten komen

Digitale weerbaarheid is geen los IT-thema, maar een vast en vanzelfsprekend onderdeel van de totale weerbaarheid van een organisatie – net zoals goede sloten, brandveiligheidsinstallaties en crisisplannen. Het is daarom cruciaal dat ook de zorgsector hier werk van maakt.

& DOOR ANNEMARIE LAMAIN

Met de inwerkingtreding van de Cyberbeveiligingswet (Cbw) - waarschijnlijk deze zomer - worden bestaande verplichtingen voor een deel van de sector aangescherpt en uitgebreid. Voor organisaties die nog niet op het vereiste niveau zitten, is dit het moment om in actie te komen. Directeur Informatiebeleid/CIO van VWS, Bianca Rouwenhorst, reageert op vragen uit het veld.

Het afgelopen jaar zijn diverse grote organisaties – ChipSoft, Odido, Clinical Diagnostics – door cyberincidenten geraakt. Wat zegt dat over het belang van digitale weerbaarheid?
“Die incidenten tonen dat digitale weerbaarheid net zo’n basisvoorwaarde is als fysieke

beveiliging. Tegelijkertijd maken ze duidelijk dat het niet de vraag is óf, maar wanneer het misgaat. We moeten ons niet blindstaren op het volledig voorkomen van cyberincidenten, maar focussen op het verkleinen van de risico’s en het beperken van de impact. Die impact kan groot zijn: systemen die uitvallen, processen die stilvallen en gegevens die op straat komen te liggen.”

Waarom is digitale weerbaarheid juist in de zorgsector zo belangrijk?
“Als systemen of gegevens niet beschikbaar zijn, raakt dat direct de continuïteit van zorg en dus de patiëntveiligheid. Ook worden mensen direct geraakt wanneer gestolen persoonsgegevens worden misbruikt, bijvoorbeeld voor identiteitsfraude of chantage. Daar komt bij dat de maatschappij – dus ook de zorg

– steeds meer digitaliseert. Dat heeft voordelen, maar maakt ook kwetsbaar. Daarom moet digitale weerbaarheid integraal onderdeel zijn van de totale veiligheid van de sector.”

Welke rol speelt digitale weerbaarheid in het toekomstbestendig houden van de zorg?
“De zorg staat onder druk door onder meer vergrijzing en personeelstekorten. Datagedreven werken en betere databeschikbaarheid kunnen bij die uitdagingen helpen. Maar databeschikbaarheid staat of valt met de bereidheid van mensen om data te delen – en die bereidheid is direct afhankelijk van vertrouwen in de veiligheid van data en systemen. Daarom gaat digitale weerbaarheid over veel meer dan techniek. Het is een randvoorwaarde voor veilige, betrouwbare en toekomstbestendige zorg.”

WEERBAARHEID

Binnenkort treedt de Cyberbeveiligingswet in werking. Wat verandert er voor organisaties in de zorgsector en hun verantwoordelijkheid inzake cyberveiligheid?

“Voor organisaties die onder de Cbw vallen, wordt cyberveiligheid nadrukkelijk een bestuurlijke verantwoordelijkheid. Het onderwerp moet in de hele organisatie ‘top of mind’ zijn. Verder moeten zij beter inzicht hebben in hun digitale risico’s en passende maatregelen nemen om systemen en gegevens te beschermen. En ze zijn wettelijk verplicht om cyberincidenten te melden.”

“Die meldplicht betekent dat cyberincidenten centraal worden geregistreerd via het meldportaal van het Nationaal Cyber Security Centrum (NCSC). Voor de zorgsector is Z-CERT – het expertisecentrum voor cybersecurity in de zorg – hierop aangesloten en verantwoordelijk voor de behandeling van meldingen. Z-CERT monitort meldingen en ondersteunt zorgorganisaties actief bij het afhandelen van incidenten en het beperken van de impact.”

Zorgorganisaties moeten al voldoen aan verschillende normen en kaders voor informatiebeveiliging. Hoe verhoudt de Cbw zich tot die verplichtingen?
“De nationale norm voor informatiebeveiliging in de zorg, NEN7510, blijft gelden. Waar

NEN7510 zich richt op zorgaanbieders, geldt de Cbw ook voor andere organisaties in de zorgketen, zoals fabrikanten van medische hulpmiddelen en geneesmiddelen. Zij moeten voldoen aan de norm ISO27001. De Cbw vervangt NEN7510 en ISO27001 niet, maar bouwt hierop voort en verbreedt de scope.”

“Daarnaast kijkt de Cbw nadrukkelijker naar de hele keten. Organisaties die onder de wet vallen, zijn verantwoordelijk voor hun eigen digitale weerbaarheid, maar moeten ook nagaan of de netwerk- en informatiebeveiliging van hun toeleveringsketen op orde is.”

Wat kunnen zorgorganisaties nú doen om hun digitale weerbaarheid te versterken?

“Zie digitale weerbaarheid als een vast onderdeel van je totale veiligheidsaanpak. Net zoals je periodiek controleert of brandmelders werken en noodplannen actueel zijn, moet je ook je digitale risico’s en maatregelen blijven toetsen.”

“Concrete stappen kunnen zijn: inzicht creëren in kritieke systemen en processen, zorgen voor heldere (bestuurlijke) verantwoordelijkheden, registratie in het meldportaal van het NCSC en cyberincidenten daar melden, een goed ingerichte incidentrespons via Z-CERT organiseren en actuele beveiligingsmaatregelen treffen.”

“En misschien nog belangrijker: zet in op bewustwording en gedrag bij medewerkers én bestuurders. Want van alle datalekken is een groot deel gedragsgerelateerd.” ■

GEÏNTERVIEWDE

Bianca Rouwenhorst studeerde Organisatieontwikkeling en Veranderkunde en is sinds juni 2022 directeur Informatiebeleid en chieff information officer (CIO) bij VWS.



Wil je weten of jouw organisatie onder de Cbw valt? Ben je benieuwd welke verplichtingen daarbij horen? Scan de qr-code:



Op pagina 88-89 vertellen Stijn Strous (bestuurder bij Hadoks) en Ronald Westerveen (CISO bij het Prinses Máxima Centrum) hoe cyberveiligheid zich in de praktijk ontwikkelt en welke rol de Cyberbeveiligingswet (Cbw) hierin speelt.

advertentie

BLIJF OP DE HOOGTE VAN ZORGINNOVATIE DIE ER ÉCHT TOE DOET

Abonneer u op de ICT&health nieuwsbrief en ontvang elke maand de meest relevante inzichten, innovaties en praktijkvoorbeelden uit de zorg. Van beleid tot technologie – kort, krachtig en gericht op impact.

NIEUWSGIERIG?
Ga naar icthealth.nl/nieuwsbrief en meld uzelf aan!

ICT&health
Het officiële kennisplatform voor zorginnovatie