Hoe een vergeten domeinnaam leidde tot een datalek

25 juni 2021

Het afsluiten van de domeinnaam is een voetnoot bij een fusie of reorganisaties. De gevolgen kunnen ernstig zijn als het niet goed wordt afgehandeld. Een aantal voorbeelden uit de afgelopen jaren in de jeugdzorg laat zien hoe, via een vergeten domeinnaam, derden toch aan gevoelige data konden komen.

Stichting Z-CERT en het Ministerie van Volksgezondheid Welzijn en Sport (VWS) hebben het initiatief genomen voor de handreiking (verlopen) domeinnamen. Het document bevat onder meer een uitgebreid stappenplan en een checklist voor het beheer van domeinnamen om het risico op datalek- ken te verkleinen. Het document is tot stand gekomen in samenwerking met de zorgsector. De handreiking is onlangs verspreid via de website van Z-CERT.

Directeur Wim Hafkamp van Z-CERT hoopt dat zorgorganisaties de handreiking gebruiken om hun eigen domeinnaambeheer tegen het licht te houden. “Cybersecurity is meer dan alleen ransomware of georganiseerde cybercrime. Een datalek zit soms in een klein

hoekje. In de zorgsector kan het pijnlijke gevolgen hebben voor cliënten, patiënten en familie-leden. Met een klein bedrag per jaar en een aantal administratieve handelingen verkleinen organisaties de kans op een datalek aanzienlijk. Het begint met weten wat je in huis hebt, wie heeft welke domeinnamen ooit geregistreerd. Daarna komt de rest.”

Risico verlopen domeinnaam

Wat is het risico van een verlopen domein- naam? Zo’n domeinnaam is een potentieel datalek. Dat betekent persoonlijk leed voor de patiënten en cliënten, mogelijke imagoschade voor de instelling, en aanzienlijke financiële schade bijvoorbeeld door herstel van systemen en

onderzoek van gespecialiseerde ICT-experts. In het geval van een datalek kan de Autoriteit Persoonsgegevens (AP) ook overgaan tot een boete als een datalek niet of niet op tijd gemeld wordt. “Een vervelende kwestie dus”, vertelt Haf- kamp. “En een die voorkomen had kunnen worden. Verreweg de makkelijkste manier om een datalek te voorkomen is door je domeinnamen aan te houden. Ook al gebruik je ze niet meer, en is er al jaren geen netwerk- verkeer meer overheen gegaan. In de praktijk zien we vaak het omgekeerde, zorgorganisaties die denken dat ze het netjes afhandelen door een domeinnaam juist niet meer te verlengen. Dan ontstaat de mogelijkheid dat derden de domeinnaam in handen krijgen en netwerkverkeer kunnen afvangen dat nog via dat domein loopt.”

ze niet meer, en is er al jaren geen netwerk- verkeer meer overheen gegaan. In de praktijk zien we vaak het omgekeerde, zorgorganisaties die denken dat ze het netjes afhandelen door een domeinnaam juist niet meer te verlengen. Dan ontstaat de mogelijkheid dat derden de domeinnaam in handen krijgen en netwerkverkeer kunnen afvangen dat nog via dat domein loopt.”

Dat kan als niet alle contacten, leveranciers of cli- enten goed op de hoogte waren van de wijziging in de contactgegevens zoals een nieuw e-mailadres of website. Ze blijven dan mailen naar het oude mail- adres dat in verbinding staat met de verlopen domeinnaam. De mails komen dus niet meer uit bij zorginstelling maar bij een willekeurige der- de die deze domeinnaam heeft geclaimed.

In sommige vallen is het niet mogelijk om een domeinnaam tot in de eeuwigheid aan te houden, waarschuwt Hafkamp. “Denk aan een faillissement of pensioen van een praktijkhouder zoals huisarts of fysiotherapeut. Het advies is om dan in elk geval de domeinnaam nog tien jaar te laten bestaan. De kans dat er daarna nog gevoelige data overheen gaat is erg klein.”

Hoe weet een zorgaanbieder of diens domein- naam in verkeerde handen is gevallen? Als je een test-e-mail stuurt naar een verlopen domein zul je een bericht terugkrijgen dat de e-mail niet kan worden afgeleverd. Maar als een andere partij het domein heeft geregistreerd en de e-mail afvangt, krijg je geen automatische reply. Dit kan een indicatie zijn dat het domein in verkeerde handen

is gevallen. Het loont de moeite om dan de contactgegevens van de nieuwe eigenaar te checken via SIDN.nl en contact op te ne- men. Hafkamp: “Een tip voor de kleinere zorginstellingen: bouw een overzicht op en voorkom dat belangrijke kennis over een domeinnaam verloren gaat op het moment dat iemand uit dienst treedt.”

Wat doet Z-CERT om incidenten als deze te voorkomen? “We informeren onze deelnemende zorgorganisaties zo veel en zo volledig mogelijk over kwetsbaarheden, incidenten en delen daarbij tips en adviezen”, vertelt Hafkamp. “Ook delen we actief informatie over security awareness. We drukken de zorg op het hart om de handreiking ter harte te nemen en het stappenplan te volgen. Zo werken we samen aan het verkleinen op de kans op datalekken en een digitaal veiligere zorgsector.”