Verlopen domeinnamen

handreiking

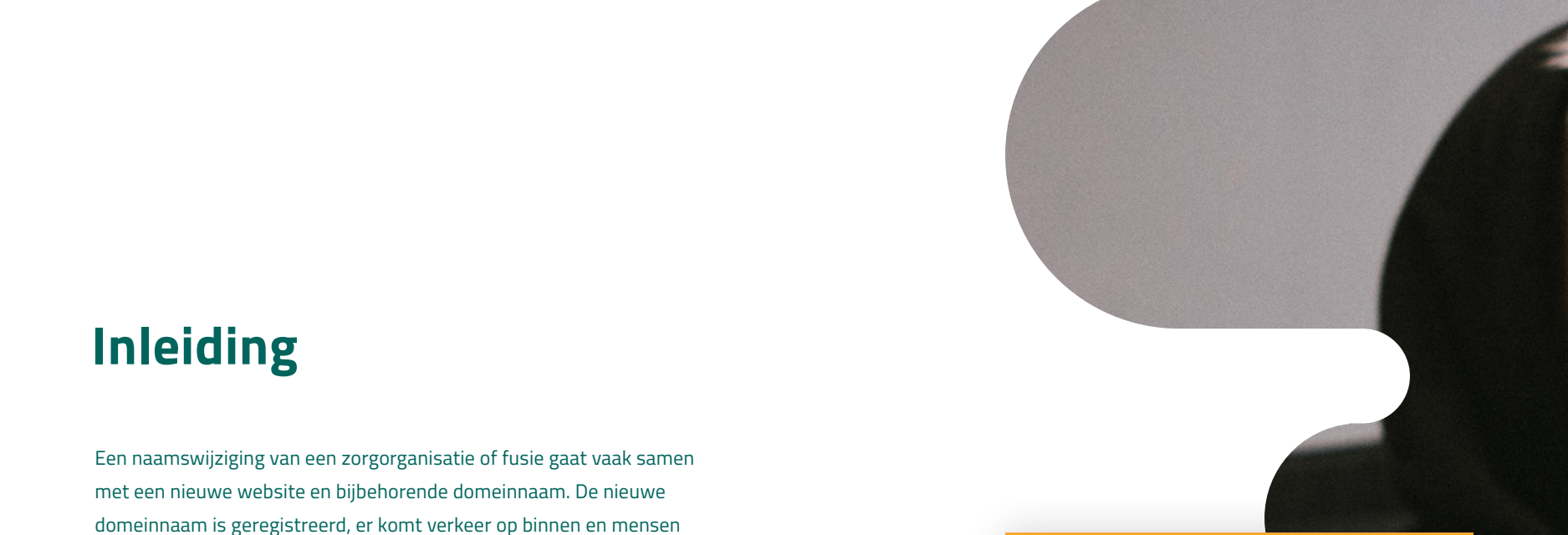
COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

ZCERT

Inleiding

Een naamswijziging van een zorgorganisatie of fusie gaat vaak samen met een nieuwe website en bijbehorende domeinnaam. De nieuwe domeinnaam is geregistreerd, er komt verkeer op binnen en mensen weten je online te vinden. Maar wat doe je met het oude domein? Een domeinnaam die niet meer wordt gebruikt, verloopt na verloop van tijd en kan in de verkeerde handen vallen met datalekken als gevolg.

Het ministerie van Volksgezondheid, Welzijn en Sport heeft samen met de experts van Stichting Z-CERT en in nauwe samenwerking met zorginstellingen deze handreiking samengesteld. Hierin staat wat zorgorganisaties kunnen doen om een datalek door een verlopen domeinnaam te voorkomen.



Wist je dat:

- Een verlopen domeinnaam heeft geleid tot datalekken bij twee jeugd-zorginstellingen, advocatenkantoren en de politie?
- Derden daardoor toegang hadden tot (privacy) gevoelige informatie?
- Dit relatief makkelijk te voorkomen is?
- De te nemen maatregelen hiervoor aansluiten/onderdeel zijn van huidige wet- en regelgeving?


03

Wat is een domeinnaam?

Een domeinnaam is het adres van je website; zoals bijvoorbeeld www.zorginstelling.nl. Iedereen kan deze naam, mits deze niet al door iemand anders is geregistreerd, registreren. Je betaalt hiervoor vaak een vast bedrag per jaar.

Wat zijn verlopen domeinnamen?

Verlopen domeinnamen zijn domeinnamen waarvan de registratie niet verlengd is door de eigenaar. Soms stoten organisaties hun domeinnamen bewust af, bijvoorbeeld bij:

- Fusies
- Naamswijzigingen
- Faillissementen
- Beëindiging van praktijk of project.

SIDN (de organisatie die Nederlandse domeinnamen registreert) geeft domeinnamen, nadat deze niet zijn verlengd, na 40 dagen weer vrij. Na deze tijd kan de betreffende domeinnaam geregistreerd worden door ieder willekeurig persoon.

Wat is het risico van een verlopen domeinnaam?

Een verlopen domeinnaam is een potentieel datalek. In de zorgsector betekent dat al snel dat privacygevoelige data van patiënten, cliënten of familieleden op straat komt te liggen. 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 ook overgaan tot een boete als een datalek niet op tijd gemeld wordt.

Gelukkig is met een paar stappen de kans op een datalek door een verlopen domeinnaam aanzienlijk te verkleinen.

> **“Als zorginstelling is het je morele plicht om voorzichtig met bijzondere gegevens om te gaan en moet je er alles aan doen om ervoor te zorgen dat deze informatie niet misbruikt wordt.”**

Hoe groot de gevolgen kunnen zijn wanneer domeinnamen niet goed beheerd worden werd duidelijk rondom de data-lekken bij de politie (2017), verschillende advocatenkantoren (2018) en het meest recent bij twee jeugdzorginstellingen (2019 en 2020). Zo hadden beide zorginstellingen na een naamswijziging nieuwe domeinnamen aangemaakt en de oude domeinnamen niet voldoende verlengd. Nadat deze weer beschikbaar kwamen zijn deze geregistreerd door derden. Op deze manier hebben onderzoeksjournalisten toegang gekregen tot duizenden dossiers van de zorginstel-lingen. Zij konden hierbij privacygevoelige gegevens inzien van patiënten en hun familieleden.

Stappenplan voor het beheer van domeinnamen

Stap 1: Breng domeinnamen in kaart

Maak een overzicht van alle domeinnamen die de organisatie gebruikt. Hiermee draag je automatisch bij aan de NEN 7510 (het inventariseren van bedrijfsmiddelen). De NEN7510 norm is wettelijk verplicht voor zorginstanties.

- **Houd bij waar de domeinnamen voor worden gebruikt:** e-mailadressen, adresboeken, geautomatiseerde mail naar het domein etc.
- **Houd bij welke applicaties/systemen informatie uitwisselen** met de domeinnaam.
- **Is er een mailserver aan de domeinnaam verbonden?** Bepaal dan van welke applicaties een wachtwoord reset aangevraagd kan worden via het mailadres.
- **Registreer wie de eigenaar en wie de aanvrager van de domeinnaam is.** De eigenaar van de domeinnaam is de medewerker die geautoriseerd is om de domeinnamen aan te vragen, wijzigingen door te voeren en af te stoten. De aanvrager van de domeinnaam kan iedere medewerker/team/afdeling binnen de zorginstelling zijn. Met hem of haar kan contact worden gezocht als er vragen zijn over de actualiteit van de domeinnaam.
- **Leg de periode dat de domeinnaam loopt vast** en het doel waarvoor de domeinnaam is geregistreerd. Dit maakt het in de toekomst makkelijker om het nut en de actualiteit van een domeinnaam te controleren.
- **Zorg dat het overzicht op een centrale plek is ondergebracht.**

Doe een historiecheck!
Vergeet niet om tijdens het opbouwen van een overzicht ook in kaart te brengen of de zorginstelling in het verleden van andere domeinnamen gebruikt maakte. Weten welke domeinnamen je hoort te hebben is de eerste stap. Doe hiervoor een historiecheck waarbij bijvoorbeeld de domeinnamen na worden gelopen van organisaties waaruit de zorginstelling gefuseerd is. Ga na wat er met deze domeinnamen is gedaan en wanneer van toepassing registreer deze domeinnamen opnieuw.

Stap 2: Doe een check bij de Registrar

Voorkom dat een domeinnaam onbedoeld verloopt door de volgende zaken te controleren bij je Registrar (de partij waarbij je de domein-extensie hebt gekocht):

- **of je een melding krijgt** wanneer de domeinnaam gaat verlopen/ opgezegd wordt.
- **of de domeinnamen stilzwijgend worden verlengd.** Op deze manier wordt voorkomen dat een domeinnaam 'per ongeluk' verloopt.
- **wie een melding krijgt** wanneer de domeinnaam gaat verlopen/opgezegd wordt. Zorg dat deze informatie up-to-date is en dat hier geen contact-gegevens staan van een medewerker die bijvoorbeeld niet meer in dienst is. Het heeft de voorkeur om hier een algemeen mailadres op te geven zodat het uit dienst treden van een medewerker niet onbedoeld kan leiden tot een onterecht verlopen domeinnaam. Toch liever contactgegevens van een persoon? Zorg dan dat bij uit dienst treden dit overgedragen wordt aan een ander persoon.

Stap 3: Beleg het beheer van domeinnamen centraal en leg dit vast

Beleg zowel het aanvragen als het opzeggen van domeinnamen op een centrale plek. Hiermee behoud je zicht op welke domeinnamen de zorginstelling heeft en voorkom je dat je er wildgroei van domeinnamen ontstaat.

- **Bepaal en leg vast wie (of welke afdeling) geautoriseerd is om domeinnamen aan te vragen en af te sloten.** Het is belangrijk om dit bij een afdeling te beleggen die kennis heeft over het adequaat beheren van domeinnamen. Deze kan bijvoorbeeld inschatten of het registreren van een nieuwe domeinnaam inderdaad nodig is (of dat het doel op een andere manier bereikt kan worden).

- **Zorg dat wijzigingen altijd worden doorgevoerd in het centrale overzicht.**

> **“Een van de belangrijkste dingen om vast te leggen is wie domeinnamen mag afstoten.”**

- **Leg in de beheerfase ook de volgende zaken vast in protocollen/ procedures/beleid** zodat duidelijk is wat gedaan moet worden:

  - de procedure bij het in gebruik nemen van een nieuwe domeinnaam (wie mag het aanvragen, wie autoriseert, wie registreert in het centrale overzicht).
  - de procedure bij het uit gebruik nemen van een oude domeinnamen (zie de volgende stap ‘Bouw activiteit op een domeinnaam netjes af”)
  - leg in ieder geval vast hoelang oude domeinnamen aangehouden worden nadat ze uit gebruik genomen worden (zie stap 5 “nazorg oude domeinnaam”). Wanneer van toepassing leg ook de procedure voor het afstoten (niet verlengen) van een domeinnaam vast.

Stap 4: Bouw activiteit op een domeinnaam netjes af

Op het moment dat je een domeinnaam uit gebruik gaat nemen is het belangrijk dat het verkeer van en naar de oude domeinnaam wordt afgebouwd. Ongeacht of je de domeinnaam blijft aanhouden (parkeert) of de domeinnaam uiteindelijk afstoot (niet meer verlengd). Volg hiervoor de volgende stappen:

- **Informeer medewerkers.** Stel medewerkers op de hoogte dat mailadressen van het oude domein vanaf een bepaalde datum niet meer beschikbaar zijn. Geef duidelijk aan wat er gaat gebeuren en wat er nu van hen verwacht wordt (bijvoorbeeld informeren van cliënten of patiënten).
- **Informeer partners/externen waarmee je informatie uitwisselt over het uitfaseren van de oude domeinnaam.**
- **Geef wijzigingen door in applicaties die informatie uitwisselen met de domeinnaam.**
- **Stel een overgangsperiode in wanneer je een domeinnaam wilt afsluiten.** Denk hierbij aan een periode van een half jaar tot een jaar. In deze periode controleer je of de afbouw inderdaad naar wens verloopt. Zendende partijen worden in de eerste fase van de overgangsperiode gewaarschuwd dat de domeinnaam/het mailadres uit gebruik genomen gaat worden en waar ze voortaan terecht kunnen. In de tweede fase krijgen partijen bericht dat de domeinnaam/het mailadres niet langer geldig is, wederom met informatie over waar men voortaan terecht kan.
- **Monitor het verkeer op de oude domeinnaam.** Monitor of er in de vooraf bepaalde overgangsperiode nog (mail)verkeer binnenkomt op de oude domeinnaam. Komt er nog (gevoelige) informatie binnen? Ga na waar de informatie vandaan komt en informeer de zendende partij (nogmaals).

Stap 5: Nazorg voor oude domeinnamen

Wanneer een zorginstelling een domeinnaam niet langer verlengd (afstoot) kan deze door eenieder worden geregistreerd. De nieuwe eigenaar kan hierdoor toegang krijgen tot vertrouwelijke informatie. Dat kan op een aantal manieren:

- **Doordat er nog e-mail met (privacy)gevoelige informatie binnenkomt op mailadressen van de oude domeinnaam.** In de praktijk gebeurt dit vaak met automatisch verstuurde mail. Derden kunnen gemakkelijk een catch-all e-mailadres aanmaken waardoor alle e-mail die verstuurd wordt naar dit domein doorgestuurd wordt naar een e-mailadres. Op deze manier kan gemakkelijk alle e-mail van een organisatie worden afvangen.

- **Doordat er toegang tot applicaties of systemen mogelijk is (direct of indirect) via e-mailadressen gelieerd aan de domeinnaam.** Medewerkers kunnen met hun mailadres direct toegang hebben tot applicaties of systemen met (privacy)gevoelige informatie. Of ze kunnen indirect toegang hebben tot inloggegevens die via een wachtwoord reset - naar een mailadres van de domeinnaam - opnieuw aan zijn te vragen.

- **Doordat deze persoon een e-mailadres aan kan maken van een mede-werker van de organisatie.** Uit naam van deze persoon kan phishing mail worden verstuurd .

Verreweg de makkelijkste manier om een datalek te voorkomen is door de oude domeinnaam aan te houden. Een domeinnaam kost vaak maar een tientje per jaar.

In sommige gevallen kan het onwenselijk of zelfs onmogelijk zijn om de domeinnaam te blijven verlengen, zoals bijvoorbeeld in het geval van een faillissement of pensioen. Houd een domeinnaam die niet meer wordt gebruik tenminste nog 10 jaar aan, met de voorwaarde dat er al minstens een jaar geen netwerkverkeer overheen loopt.

10

Vervolg stap 5: Waarom 10 jaar en een jaar geen netwerkverkeer?

Derden kunnen nog toegang krijgen tot (privacy)gevoelige informatie via mails of informatie die nog uitgewisseld wordt met de domeinnaam en door middel van toegang tot inloggegevens.

- **Toegang tot privacygevoelige informatie in mails ondervang je met de eis van een jaar geen netwerkverkeer.** Verstuur tijdens de 10 jaar mails naar partijen die nog naar het domein mailen, dat het domein niet meer in gebruik is.

- **Dat derden geen toegang hebben tot applicaties of systemen met privacygevoelige informatie ondervang je met de 10 jaar termijn.** De gemiddelde levensduur van applicaties is 10 jaar. Ook al zou iemand via de domeinnaam nog toegang hebben tot systemen of applicaties, is de kans hierop na tien jaar sterk verminderd.

Weet je zeker dat er via de domeinnaam geen toegang te krijgen is tot applicaties of databanken (bijvoorbeeld doordat je kan garanderen dat er overal gebruikt wordt gemaakt van multifactor-authenticatie)? Dan kan je deze termijn verkorten. Hiermee wordt niet de kans op phishing ondervangen. Het kan dat een langere termijn wenselijk is ter bescherming van de goede naam.

Extra: gebruik multifactor-authenticatie
In het geval van één van de jeugdzorginstellingen is er toegang verkregen tot gevoelige informatie door middel van een wachtwoord reset. Een gemakkelijke manier om dit te voorkomen is door middel van multifactor-authenticatie. Een tweede inlog factor maakt het aanzienlijk moeilijker voor kwaadwillende om toegang te krijgen tot systemen/ applicaties en/of e-mails met (privacy)gevoelige informatie in te zien. Zorg ervoor dat de tweede factor niet via de e-mail verstuurd wordt. Het gebruik van multifactor-authenticatie is conform de NTA 7516, die standaarden zet voor veilig mailen binnen de zorg.

Checklist

Wanneer heb je het beheer van domeinnamen goed ingeregeld?

☐ 1. Historiecheck gedaan

Je hebt gecontroleerd of je alle domeinnamen in beheer hebt die je, historisch gezien, in beheer zou moeten hebben.

☐ 2. Bouw een overzicht op van de domeinnamen die je beheert

Je hebt minimaal vastgelegd, op een centrale plek, (a) welke domeinnamen je hebt (b) wat je er mee kan of doet (bijvoorbeeld mailen), (c) welke applicaties er eventueel mee uitwisselen (d) wie er eigenaar/contactpersoon van is en (e) het doel waarvoor de domeinnaam is aangevraagd en (f) de periode dat de domeinnaam hoort te lopen.

☐ 3. Faciliterende maatregelen ingeregeld bij je Registrar

Je hebt gezorgd dat een domeinnaam niet 'per ongeluk' kan verlopen door:

- in te stellen dat domeinnamen automatisch verlengd worden.
- te zorgen dat iemand/afdeling een melding krijgt wanneer een domeinnaam gaat verlopen en de contactgegevens van deze persoon (of ideaal afdeling) hier een melding over krijgt up-to-date is.

☐ 4. Beheer van domeinnamen op een centrale plek belegd

Je hebt afspraken gemaakt over (en vastgelegd) wie aanvragen, wijzigingen en het afstoten van domeinnamen beheert en het is op een centrale plek (afdeling) belegd. De aanvragen worden altijd geautoriseerd door iemand/een afdeling met voldoende IT-kennis.

☐ 5. Beleid/protocol/procedure vastgelegd

Je hebt minimaal vastgelegd:

- Wat het protocol is bij het in gebruik nemen van een nieuwe domeinnaam.
- Wat het protocol is voor het uit gebruik nemen van een domeinnaam (denk aan een overgangsperiode, het controleren van netwerkverkeer enz.). Zie punt 4 in het stappenplan.
- Hoelang je een domeinnaam aanhoudt nadat je deze uit gebruik neemt. Zie punt 5 in het stappenplan.

Ministerie van Volksgezondheid,
Welzijn en Sport

Dit document is een initiatief van Stichting Z-CERT en het Ministerie van Volksgezondheid, Welzijn en Sport.