Deventer ziekenhuis

opsteller(s) Nijenhuis, Niels
status Definitief
Datum bijgewerkt 17-9-2020
referentie
onderwerp Beleid externe toegang leveranciers, partners en derden

Notitie

Inhoudsopgave

1. Inleiding

Het Deventer Ziekenhuis biedt leveranciers de mogelijkheid om op afstand onderhoud- en supportwerkzaamheden uit te voeren op hun systemen in het Deventer Ziekenhuis netwerk, via het door het Deventer Ziekenhuis aangeboden platform

Omdat het Deventer Ziekenhuis gebruik maakt van zeer veel verschillende applicaties en een meervoud aan leveranciers, partners en derden, is het voor het Deventer Ziekenhuis niet mogelijk om per leverancier een eigen oplossing te gebruiken.

1.1. Wet- en regelgeving

In het kader van de wet- en regelgeving (o.a. NEN7510 en AVG) ten aanzien van informatiebeveiliging, moet het Ziekenhuis te allen tijde in staat zijn aan te tonen wie welke informatie wanneer heeft geraadpleegd, gewijzigd en verwijderd. Ook als het daarbij gaat om applicaties die zelf geen privacygevoelige informatie bevatten, men heeft immers wel een verbinding met het ziekenhuis brede netwerk.

2. Beleid

Het beleid van het Deventer Ziekenhuis voor het verlenen van remote toegang aan leveranciers, partners en derden is gebaseerd op het basisprincipe van zero-trust (wij vertrouwen niemand) en onderstaande uitgangspunten:

Uitgangspunten:

1. Alleen toegang wanneer nodig,
2. Toegang via Multifactor authenticatie,
3. Alleen toegang tot de minimaal nodige systemen,
4. Monitor, registreer en analyseer, het creëren en analyseren van een auditspoor van alle activiteiten op het netwerk en controle op afwijkend gedrag.

In de gehanteerde procedure worden alle bovenstaande uitgangspunten geborgd.

3. Procedure

Hieronder wordt een korte beschrijving gegeven van de procedure zoals deze wordt gehanteerd. De actuele en uitgebreide procedure is beschikbaar op iProva.

3.1. Noodzaak tot toegang

Alleen de applicatie eigenaar, functioneel of technisch beheerder kunnen de ICT-helpdesk middels een ELS-melding verzoeken om een leverancier externe toegang te geven tot de applicatie en de daarbij behorende systemen.

3.2. Multifactor authenticatie

De ICT-helpdesk neemt contact op met de leverancier, en geeft het account vrij voor de periode die de leverancier nodig heeft voor de uitvoering van de werkzaamheden. De ICT-helpdesk past indien nodig het telefoonnummer aan waarop de sms binnenkomt. In deze stap wordt ook gecontroleerd dat diegene is wie hij/zij zegt te zijn.

3.3. Alleen toegang tot de minimaal nodige systemen

Bij de implementatie is vastgesteld tot welke systemen de leverancier minimaal toegang nodig heeft om werkzaamheden zoals overeengekomen uit te voeren.

3.4. Monitor, registreer en analyseer

Het Deventer Ziekenhuis gebruikt de tooling van Bomgar om automatisch een auditspoor te creëren en het gedrag te analyseren op afwijkingen. Alle externe toegang voor leveranciers, partners en derden verloopt middels de Bomgar oplossing.

4. Uitzondering

Er is alleen een uitzondering mogelijk voor de multifactor authenticatie, alle andere uitgangspunten, inclusief het gebruik van de Bomgar oplossing blijven vereist.

Er kan bij hoge uitzondering en pas na goedkeuring door zowel de security officer als de ICT-architect afgeweken worden van de multifactor authenticatie. Deze dient dan vervangen te worden door een site-to-site VPN-verbinding.

De voorwaarden verbonden aan deze uitzondering zijn:

- Er moet worden aangetoond dat men voor de eigen externe toegang gebruik maakt van multifactor authenticatie;
- Er moet worden aangetoond dat men NEN7510 en/of ISO 27001 en ISO27002 gecertificeerd is;
- Er jaarlijks een externe audit van het gehele netwerk inclusief alle externe IP-adressen plaatsvindt. De samenvatting hiervan wordt op aanvraag aan het Deventer Ziekenhuis overlegd.