D35 C= bylage van D33

Concept Informatiebeveiligingsbeeld CSZ 2024

Geheel of gedeeltelijk buiten reikwijdte art 5.1 lid 2 onder h art 5.1 lid 2 onder e

Context College sanering zorginstellingen

Het College Sanering zorginstellingen (CSZ) is een Zelfstandig Bestuursorgaan (ZBO)dat in het kader van de Wtzi toezicht houdt op de vervreemding van onroerend goed in de zorgsector. Het betreft casusgericht toezicht. Momenteel is er sprake van ongeveer 600 lopende casus. Het secretariaat bestaat uit 5 medewerkers. Voor het toezicht in de praktijk, op het vervreemdingsproces en de marktconforme opbrengst, maakt het CSZ gebruik van zogenoemde gemachtigden die per casus worden aangewezen en ingehuurd en waarmee een raam-inhuurovereenkomst is afgesloten. Het CSZ heeft op dit moment 10 gemachtigden.

Het CSZ is gehuisvest bij de NZa in een separate ruimte met een aparte voordeur met toegangsbeveiliging. Het CSZ beschikt over eigen automatiseringstoepassingen (dit betreft met name het workflow-systeem Easy d en het casus-systeem Acces). Het CSZ heeft een eigen ICT-leverancier: ICT Teamwork. De separate ruimte en de eigen automatiseringsomgeving houden verband met de eis van een gescheiden informatiehuishouding die er tussen de ZBO's NZa en het CSZ moet bestaan.

Organisatie van de informatiebeveiliging

Sturing

De manager van het CSZ is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid.

De Chief Information Officer (CIO) is verantwoordelijk voor het kaderstellend beleid voor de informatiebeveiliging en het interne toezicht op de naleving daarvan.

De CIO en de Chief Information Security Officer (CISO) van de NZa kunnen ingeroepen worden voor de advisering over de informatiebeveiliging.

Plan-Do-Check-Act

Het College sanering heeft voor het informatiebeveiligingsbeleid een PDCA (Plan-DO-Check-Act) Cyclus ingericht met daarin als belangrijke elementen:

- het periodieke overleg met de ICT-leverancier die de prestaties van het geautomatiseerde gegevensverwerkende systeem (kantoorautomatisering, Easy, Acces) van het College sanering monitort;
- het jaarlijks actualiseren van de risicoanalyse;
- het bijhouden van een incidentenregistratie;
- het jaarlijks actualiseren van het informatiebeveiligingsbeeld;
- het in voorkomende gevallen treffen van maatregelen naar aanleiding van knelpunten, incidenten, de jaarlijkse risicoanalyse, het periodieke overleg met de ICT-leverancier en bevindingen naar aanleiding van (eventueel) uitgevoerde externe audits op de uitvoering van het informatiebeveiligingsbeleid;
- een periodieke check op het bestaan en de werking van de beheersmaatregelen.

Rollen

De volgende belangrijke rollen zijn te onderkennen:

1-CIO (Chief Information Officer), verantwoordelijk voor het beleidskader en het toezicht daarop;

2-CISO(Chief information Security Officer), verantwoordelijk voor (ongevraagde) advisering;

3-De Manager, verantwoordelijk voor de dagelijkse uitvoering;

4-ICT-teamwork, die als ICT-leverancier verantwoordelijk is voor de ongestoorde werking van de systemen en de monitoring van systeemprestaties en het signaleren en/of oplossen van knelpunten.

Te beschermen belangen

-De ongestoorde werking c.q. continuïteit van de bedrijfsapplicaties, het voorkomen- en oplossen van storingen en knelpunten;

-Het voorkomen van data-verlies c.q. het zo snel als mogelijk herstellen van in voorkomend geval dataverlies;

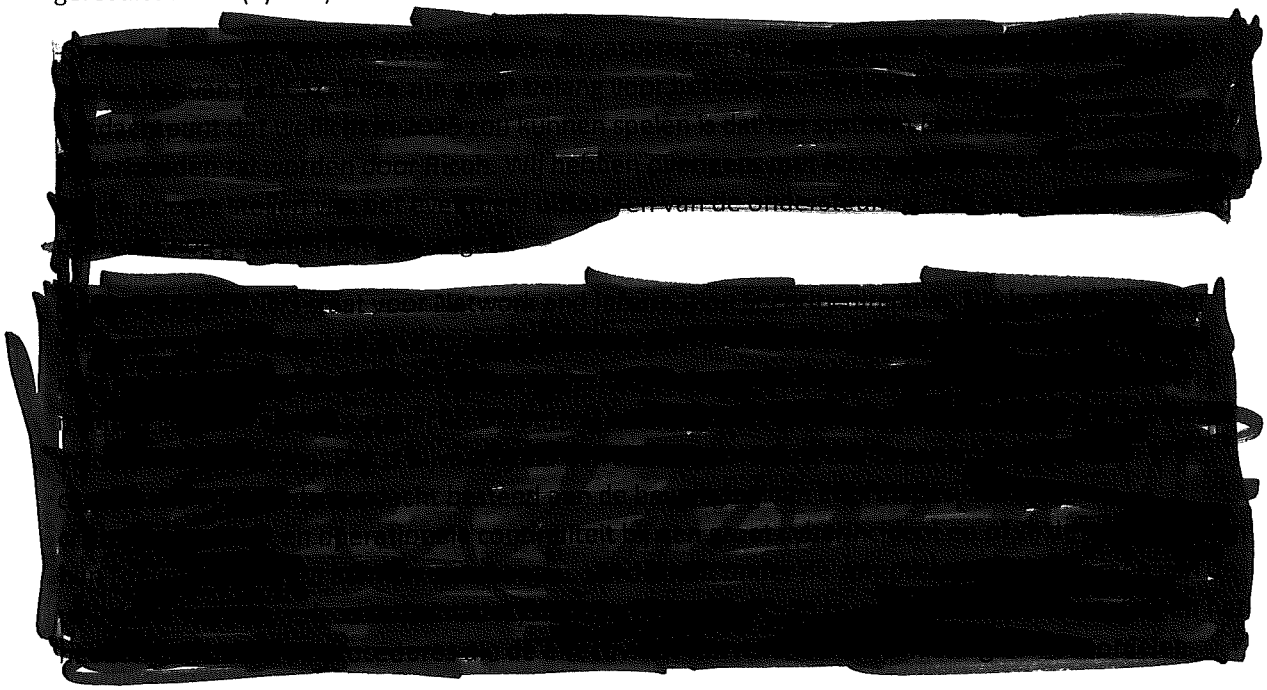
-Het beveiligen van de privacy- en bedrijfsgevoelige casusgegevens waaronder privacy gevoelige c.q. persoonlijke gegevens; het voorkomen van ongeautoriseerde toegang tot digitale- en fysieke casusgegevens c.q. het compliant zijn aan wet- en regelgeving.

Successen.

-Er hebben zich de afgelopen jaren geen belangrijke verstoringen voorgedaan.

Dreigingen

- Hoewel dreigingen gelet op het geopolitieke klimaat zeker aanwezig zijn, hebben zij niet geresulteerd in (cyber-)incidenten.



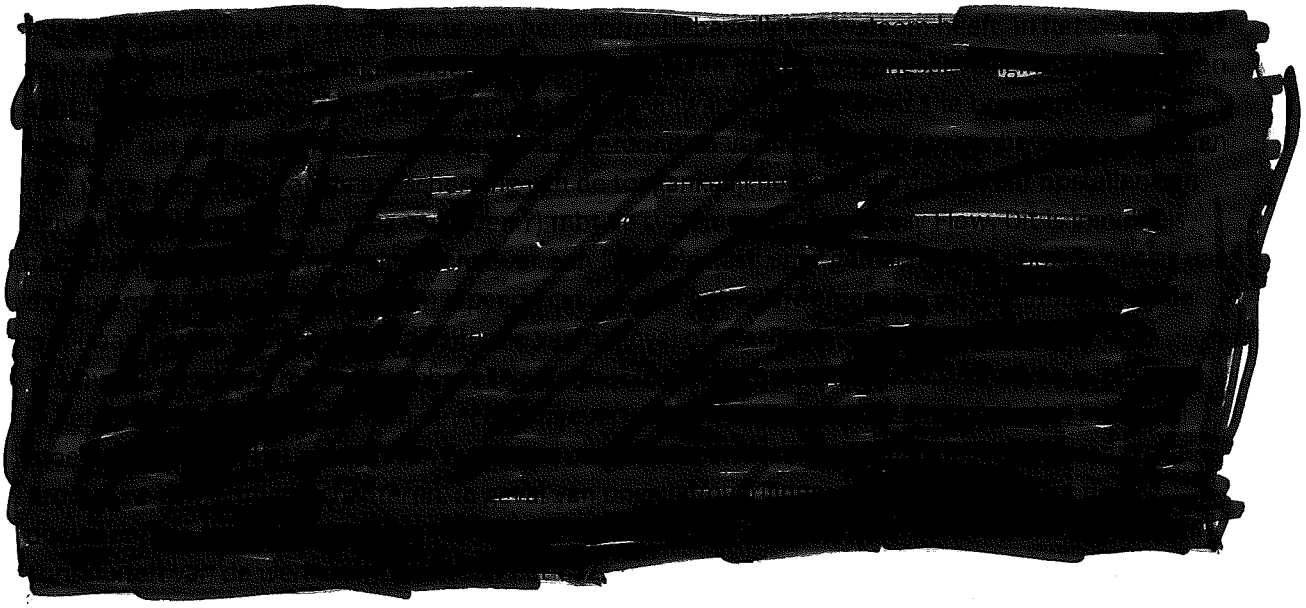
Wij hebben begrepen dat ICT-Teamwork zelf niet rechtstreeks onder de regelgeving van NIS2 valt. Wel volgt ICT teamwork op vrijwillige basis de wetgeving van NIS2 zoveel mogelijk vanuit andere normen waarvoor het gecertificeerd is, zoals ISO27001, DATAprocode en de eisen die de Nederlandse overheid stelt aan het verwerken van Bijzondere Informatie.

Incidenten

-Het CSZ beschikt sinds 2021 over een incidentenregistratie. Er heeft zich in die periode een beperkt aantal incidenten voorgedaan, die al bekend waren bij de ICT-leverancier en door de ICT-leverancier direct adequaat zijn opgepakt

Auditbevindingen/opvolging

-De monitoring door de ICT-leverancier van het CSZ-systeem levert soms aandachtpunten op die zijn c.q. worden verholpen, zoals het introduceren van two-factor-authentificatie

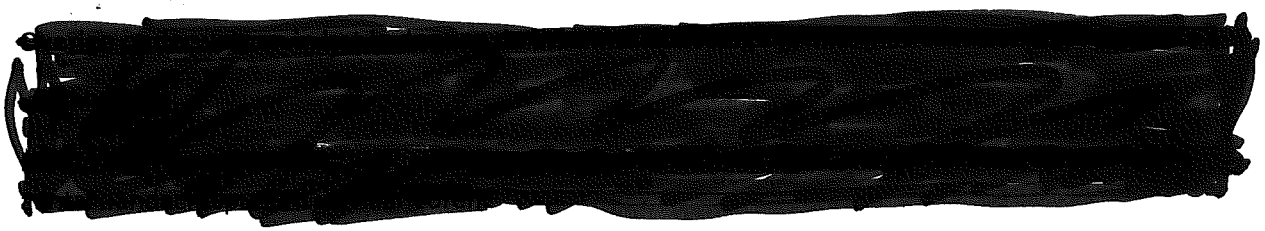


Organisatie-uitdagingen

Er zijn geen specifieke uitdagingen anders dan de aandachtpunten die hiervoor reeds zijn genoemd.

Beheersing van risico's

De beheersing van de risico's vindt plaats door de geschetste PDCA cyclus mede nav monitoring van het geautomatiseerde systeem van het CSZ door ICT teamwork.



[redacted]

augustus 2024