

IT-SPECIAL VOOR DE ZORG

5 onmisbare stappen voor meer grip op IT



Inhoudsopgave.

5 onmisbare stappen voor meer grip op IT

De IT-uitdagingen voor zorginstellingen.

Tegenwoordig kan geen zorginstelling er meer omheen: **IT vormt een essentieel fundament voor moderne zorgverlening**. Om dat goed te organiseren zijn verschillende aspecten belangrijk. Onderdelen die extra aandacht vragen zijn het waarborgen van de continuïteit, het beheersen van de kosten en het beveiligen van gevoelige clientgegevens. Alle onderdelen hebben invloed op elkaar. Dat maakt het organiseren van een goed IT-fundament een ingewikkeld vraagstuk. En als dat organiseren niet goed lukt, dan loopt u extra risico:

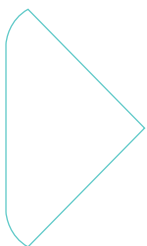
- ▶ De IT-kosten lopen uit de hand.
- ▶ Toename van IT-storingen.
- ▶ Beperkte weerbaarheid tegen cyberrisico's.
- ▶ Ontevredenheid over slecht functionerende IT.

Het is bekend dat veel zorginstellingen hier mee worstelen. Het kost steeds meer geld en tijd om een goed IT-fundament te organiseren. Herkenbaar?

In ons e-book beschrijven wij hoe zorginstellingen in **5 stappen** de grip op IT kunnen vergroten. Binnen iedere stap focussen we op een thema (bijvoorbeeld kostenbeheersing bij toenemende complexiteit of het op orde brengen van informatiebeveiliging). Bij elke stap geven we verschillende tips & tricks. Deze stappen helpen u om de continuïteit en veiligheid van zorg te waarborgen, kosten te beheersen en de efficiëntie van zorgverlening te optimaliseren.

Want het doel is duidelijk:

uw organisatie moet haar tijd effectief kunnen besteden aan zorgverlening, niet aan het organiseren van tijdrovende IT-gerelateerde taken.



Beheers uw IT-kosten bij toenemende complexiteit.

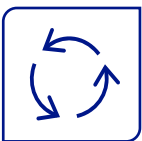
Het beheersen van IT-kosten is een voortdurende uitdaging voor zorginstellingen. Enerzijds biedt IT steeds meer mogelijkheden om de bedrijfsvoering efficiënter te maken en te automatiseren. Tegelijkertijd komen er steeds meer oplossingen om – met behulp van IT – de serviceverlening naar klanten te verbeteren. Door de toegenomen mogelijkheden kan de IT-omgeving onbedoeld complexer en duurder worden. Iedere organisatie zal hierin slimme keuzes moeten maken, zodat er maximale waarde wordt gerealiseerd voor iedere uitgegeven euro.

Het inzetten van een cloudoplossing kan helpen om meer waarde te realiseren voor uw dienstverlening en eventueel ontstane complexiteit binnen de IT-omgeving, te reduceren. Maar, het aanbod aan public- en private cloudoplossingen is groot. Daarbij voorziet lang niet iedere cloudoplossing in de specifieke behoeften en eisen van de zorg.

In het kader van kostenbeheersing en -optimalisatie voor uw zorginstelling zijn er drie belangrijke zaken om naar te kijken:



1. Het **opruimen van overtollige** IT-servers en applicaties: Bij veel organisaties helpt dit kosten te besparen. De migratie van on-premise naar cloud-oplossingen of een overstap van cloud-provider vormen mooie kansen om hiermee aan de slag te gaan.



2. Het **aanpakken van verouderde** applicaties of nalopen van virtuele servers op (oude) besturingssystemen: Maak een inventarisatie van alle platformen en applicaties en bekijk hoe deze slimmer ingericht kunnen worden, bijvoorbeeld door applicaties naar een SaaS-model te migreren.



3. Maak **gebruik van cloud-infrastructuur**: Hierdoor krijgt uw zorginstelling de mogelijkheid om alleen te betalen voor de daadwerkelijk benodigde capaciteit. In plaats van te blijven investeren in eigen servercapaciteit voor toekomstige groei, maakt u gebruik van een flexibele, schaalbare cloud-infrastructuur die capaciteit biedt op basis van actuele behoeften. Dit kan natuurlijk ook in kleinere stappen.

Beheers uw IT-kosten bij toenemende complexiteit.

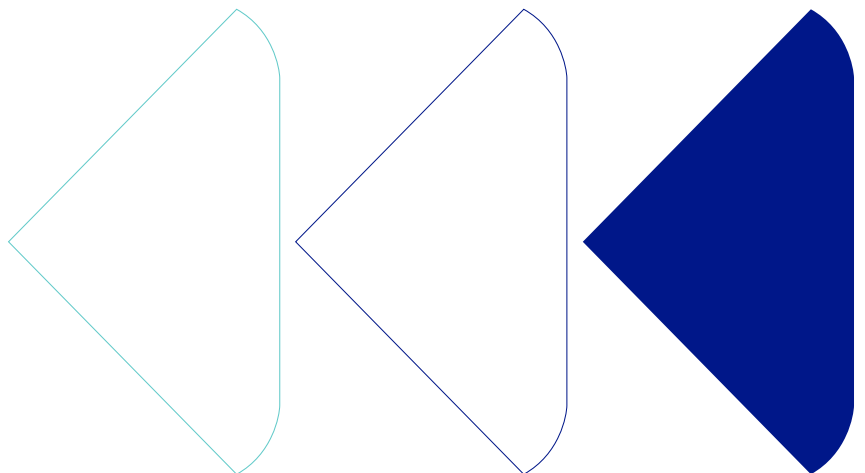
Complexiteit eenvoudig opgelost

Wat te doen met een alsmaar groeiende IT-omgeving? Met die groei neemt namelijk ook de complexiteit toe. Wat weer vaak leidt tot hogere kosten.

Door meer cloudtechnologie in te zetten, kunt u de IT-omgeving efficiënter indelen én geeft u de beheerlast en een stuk complexiteit uit handen. Hierdoor ontstaat ruimte om de focus te leggen op de eindgebruiker. Want: hoe beter de eindgebruiker wordt bediend, hoe hoger de productiviteit.



Maak kennis met de Intermax HealthCloud, **een platform dat 'purpose-built' is voor de zorgketen**. We zijn voor verschillende zorgorganisaties in Nederland, dé partner voor een compliant IT-infrastructuur. Betaal naar gebruik en schaal eenvoudig maandelijks capaciteit op of af. Uw data blijft bovendien gegarandeerd in Nederland.



STAP 2

Breng uw informatie-beveiliging op orde.

Informatiebeveiliging in de zorg levert altijd een uitdagend spanningsveld op tussen goed beveiligen en de bijkomende kosten en – aan de andere kant – prettig werken. Informatie moet namelijk veilig staan én tegelijkertijd snel en makkelijk beschikbaar zijn. Ook de groeiende afhankelijkheid van IT, nieuwe wetgeving en de toenemende hoeveelheid gevoelige gegevens bieden uitdagingen voor uw zorginstelling op het gebied van informatiebeveiliging. Het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van cliëntgegevens staat daarbij centraal. NEN7510 is hierin de normering die specifiek van toepassing is binnen de zorgsector en waaraan (wettelijk) voldaan moet worden. Maar ook NIS2 zal van toepassing zijn voor de meeste zorgorganisaties.



Versleutelen van gegevens

Een goede basis begint bij een robuuste cloud-infrastructuur die rekening houdt met de geldende regels rondom informatiebeveiliging voor de zorg in Nederland. Een grote rol is weggelegd voor data-encryptie, wat essentieel is voor het beveiligen van gevoelige cliënteninformatie.

Daarbij kan, naast het maken van versleutelde backups, gedacht worden aan het versleutelen van de virtuele schijven in de opslaglaag. Hierdoor wordt het haast onmogelijk voor onbevoegden om toegang te krijgen tot gevoelige informatie. Door de versleuteling van data slim in te richten hoeft dit geen impact te hebben op de prestaties van de virtuele machines.



Breng uw informatie-beveiliging op orde.



De werkplek

Het realiseren van een gebruiksvriendelijke werkplek die tegelijkertijd veilig is, kan een flinke uitdaging zijn. Via de werkplek hebben medewerkers toegang tot vertrouwelijke informatie, maar moeten ze ook eenvoudig online kunnen samenwerken. Als dit te omslachtig wordt, gaan medewerkers eigen oplossingen bedenken. Dan ontstaat er schaduw-IT en dat zorgt ervoor dat uw organisatie de grip kwijt raakt op de informatiebeveiliging van vertrouwelijke cliëntgegevens.

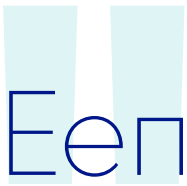
De belangrijkste aspecten bij het inrichten van een moderne werkplek zijn:

- ▶ Het afstemmen van de werkplek op de rol/taak van de medewerker: Werk met standaard-gebruikersprofielen om de werkplek kostenefficiënt en beheersbaar te houden. Gebruik single-sign-on (SSO) voor applicaties. Dat maakt het veilig én eenvoudig in gebruik. En het voorkomt dat een zorgmedewerker telkens opnieuw moet inloggen.
- ▶ Hanteer een effectief wachtwoordbeleid: Stel specifieke eisen aan het gebruik van wachtwoorden, zodat er unieke en sterke wachtwoorden worden afgedwongen.
- ▶ Dwing multi-factor authenticatie af bij het gebruik van de werkplek. Dit is een onmisbare stap in het beveiligen van de werkplek en gevoelige gegevens.
- ▶ Zorg voor een soepele integratie van legacy-applicaties in combinatie met andere web-based applicaties en randapparatuur. Hierdoor ervaart de medewerker zijn werkplek daadwerkelijk als één geheel.

De bovengenoemde tips kunt u zelf toepassen, of u besteedt het uit. Dan is investeren in techniek en (schaars) talent niet nodig. Dit is een eenvoudige manier om de informatiebeveiliging binnen uw zorginstelling naar een hoger plan tillen en tegelijkertijd de compliance te verbeteren. Benieuwd wat dit voor uw zorginstelling betekent? Onze experts denken graag met u mee over de oplossingen!

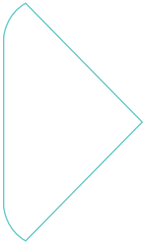
Word weerbaarder met veilige IT.

Met de groeiende dreiging van cyberaanvallen en datalekken is cybersecurity een topprioriteit geworden voor zorginstellingen. Het beschermen van gevoelige cliëntgegevens tegen hackers en het voldoen aan strikte wet- en regelgeving vormen een enorme uitdaging. Omdat cybersecurity over meerdere schijven wordt geïmplementeerd en verschillende toepassingsniveaus kent, hebben we voor het gemak in dit document cybersecurity opgedeeld in meerdere niveaus: basisbescherming, extra bescherming en hoogstaande bescherming.



Een datalek kan niet alleen financiële schade veroorzaken, maar ook het vertrouwen van cliënten, zorgverzekeraars en leveranciers aantasten.

Word weerbaarder met veilige IT.

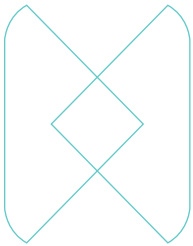


Basisbescherming

Ons advies: zorg allereerst voor een solide cybersecurity-basis. De basis bestaat uit minimaal de volgende elementen:

1. Train regelmatig medewerkers om verdachte activiteiten te herkennen en te vermijden. Medewerkers zijn vaak het zwakste punt in de beveiligingsketen en vormen een gemakkelijk doelwit voor cybercriminelen.
2. Zorg voor een robuust back-up- en herstelplan. Geautomatiseerde back-ups van kritieke systemen en gegevens helpen om de impact te verlagen bij een uitval van systemen of een ransomware-aanval.
3. Implementatie van technische maatregelen zoals anti-malware-software en netwerkmonitoring. Ook de keuze van de hosting- of cloud-provider speelt hierin een rol. Kies altijd voor een provider die aangesloten is op de 'Nationale Anti-DDoS Wasstraat'. Dan is uw zorginstelling beter beschermd tegen DDoS-aanvallen.
4. Richt een security patch management proces in voor het installeren van updates of aanpassen van configuraties bij de publicatie van urgente en aanbevolen patches door de hard- en softwarefabrikanten.

Word weerbaarder met veilige IT.



Uitgebreide bescherming

Voor een uitgebreider niveau van cybersecurity, is het implementeren van endpoint protection en Security Information and Event Management (SIEM) systemen een belangrijke stap. Met endpoint protection wordt op verschillende systemen een klein stukje software geïnstalleerd voor monitoring en bescherming van deze toegangspunten. Om uw Security Information and Event Management (SIEM) in te richten zijn de volgende stappen van belang:

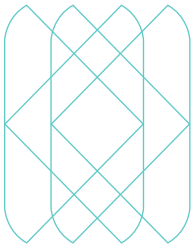
1. Bepaal welke applicaties het belangrijkst zijn voor uw zorginstelling. Deze 'kroonjuwelen' moeten koste wat het kost worden beschermd. Denk daarbij aan alle vertrouwelijke en persoonlijke gegevens van cliënten. Het kunnen ook systemen zijn die cruciaal zijn om de zorgverlening te borgen en niet mogen uitvallen.
2. Maak detectieregels aan voor het opsporen van verdachte activiteiten. Dat kan gaan over bijvoorbeeld bestanden die worden benaderd en geopend door onbekende of niet-bevoegde gebruikers. Bij een verdachte activiteit herkend door een detectieregel, wordt automatisch een alert gegenereerd.
3. Richt een proces in, inclusief wie waar verantwoordelijk voor is, om de gewenste acties uit te voeren wanneer er zich alerts voordoen. Bepaal ook de doorlooptijd waarbinnen een alert wordt opgepakt.

TIP

Gebruik voor het definiëren van detectieregels een kennisdatabase waarin verschillende aanvalstechnieken van hackers zijn vastgelegd.

Door dit steeds verder uit te bouwen voor meer systemen en kroonjuwelen, vergroot u overzichtelijk de bescherming van uw zorginstelling.

Word weerbaarder met veilige IT.



Hoogstaande bescherming

Is uw zorginstelling al uitgebreid beschermd? Dan zijn er nog een aantal zaken waar de cybersecurity kan worden verhoogd:

- ▶ Voer periodiek pentesten uit, waarbij doelgerichte cyberaanvallen worden nagebootst.
- ▶ Richt continue verbeter-terugkoppeling in door evaluaties in te plannen nadat er incidenten hebben plaatsgevonden. De uitkomst van de evaluaties vormt de basis om processen te verbeteren.
- ▶ Breid monitoring uit naar steeds grotere delen van het netwerk.
- ▶ Start met 'threat hunting', waarbij proactief logs worden doorzocht op mogelijkheden om kwetsbaarheden te exploiteren.

Iedere organisatie is uniek en hoewel de uitgangspunten van cybersecurity uniform zijn, zijn er altijd specifieke wensen en eisen in het toepassen van effectieve cybersecurity. Het kan daarom interessant zijn om te sparren met een expert om te kijken hoe cybersecurity voor uw zorginstelling op maat naar een hoger niveau getild kan worden.



STAP 4

Zorg dat de zorg altijd door kan gaan.



Het waarborgen van de beschikbaarheid van IT-systemen is cruciaal voor zorginstellingen. Zelfs korte uitvalperiodes kunnen ernstige gevolgen hebben voor de zorgverlening, de cliëntveiligheid en het imago van de organisatie. Het gebrek aan redundante systemen en een robuuste infrastructuur is dus een potentieel gevaar. Onderstaande tips kunt u gebruiken om een hogere beschikbaarheid van de IT-omgeving te realiseren.

- Realiseer een **geo-redundante opstelling (2N)** voor uw datacenter: in het geval van uitval van één volledig datacenter, kan de workload worden hervat op het tweede datacenter.
- Houd marge voor groei met **capaciteits-management**: dit houdt in dat uw organisatie altijd voldoende capaciteit reserveert om 10% te kunnen groeien (bovenop benodigde beschikbare capaciteit voor redundantie).
- Blijf altijd up-to-date met **update management**: Optimaliseer de installatie van updates, zodat het geen downtime en/of performance-impact heeft op de (virtuele) servers. Dit is cruciaal bij applicaties waar geen downtime toegestaan is en op te vangen door een uitgebreide redundantie in de hardwarelaag.
- Implementeer **24/7 proactieve monitoring**: alle onderdelen – van connectiviteit, firewalling tot en met compute en VM storage – moeten 24/7 worden gemonitord op afwijkingen en potentiële incidenten.
- **Certificering op business continuïteit**: Bij eigen IT-beheer is het belangrijk om ervoor te zorgen dat uw zorginstelling ISO 22301 gecertificeerd is. Door dit certificaat te behalen zorgt u ervoor dat u overzicht en een plan hebt in geval van nood. Of zorg ervoor dat, bij uitbesteding, uw IT-leverancier aan deze internationale normen voldoet.

STAP 5

Maak uw IT toekomstbestendig.

Indien uw zorginstelling afhankelijk is van verouderde IT-systemen, loopt u het risico om vast te komen te zitten in een vendor lock-in. Daardoor wordt uw organisatie beperkt in de mogelijkheden om over te stappen naar nieuwe technologieën of leveranciers. Dit kan leiden tot hoge kosten voor het onderhouden van verouderde systemen en tot 'technical debt'. Dat houdt in dat uw organisatie niet de mogelijkheid heeft om snel in te spelen op veranderingen in de markt, zoals wet- en regelgevingen.

Lijdt uw zorginstelling aan 'technical debt'? Dit zijn 7 mogelijke symptomen:

1. Alledaagse wijzigingen zijn al snel enorm complex. Soms zijn er zelfs externe specialisten nodig om deze wijzigingen door te voeren.
2. Toenemend aantal bugs-meldingen, storingen en incidenten.
3. Trage ontwikkeltijd: upgrades leiden tot uitval.
4. Regelmatig uitval van systemen en continuïteit onder druk.
5. Problemen om eenvoudig te schalen in aantal gebruikers voor specifieke systemen.
6. Hoge onderhoudskosten: dure contracten en inzet van externen nodig om systemen te kunnen onderhouden.
7. End of service vanuit leverancier.

STAP 5 (vervolg)

Maak uw IT toekomstbestendig.

Om uw IT-infrastructuur toekomstbestendig te maken en vendor lock-ins te voorkomen, zijn er een aantal aandachtspunten om rekening mee te houden.

- ▶ Ga voor inzicht en overzicht: maak een overzicht met verantwoordelijkheden per persoon, een overzicht van het applicatielandschap en de verschillende onderlinge koppelingen.
- ▶ Virtualisatie is voor iedere zorginstelling van essentieel belang. Als uw organisatie dit nog niet heeft ingeregeld, dan is dat een belangrijk punt om mee aan de slag te gaan.
- ▶ Richt het doorvoeren van updates en deployen van test- en acceptatie naar productie-omgeving zó in dat dit automatisch gaat. Het kan daarbij helpen om in te zetten op containerisatie. Dit is een veel toegepaste vervolgstap op virtualisatie waarmee uw organisatie meer flexibiliteit inbouwt en het risico op vendor lock-in nog verder beperkt.
- ▶ Zorg voor standaardisatie van processen en keuzes in software. Dit helpt bij het integreren van verschillende systemen en in een breder aanbod wanneer uw zorginstelling support van buitenaf nodig heeft.

TIP

Vermijd minder gangbare oplossingen voor virtualisatie, back-up oplossingen en andere ondersteunende IT. Gebruik marktstandaarden om interoperabiliteit en dataportabiliteit te verzekeren. Zodat switchen van IT-leverancier altijd mogelijk blijft.

Conclusie.



Het mag duidelijk zijn, het beheren van de IT-infrastructuur van uw zorginstelling brengt uitdagingen met zich mee. Helemaal door de toenemende complexiteit. Of het nu gaat over uw IT toekomstbestendig maken, de continuïteit van uw systemen waarborgen, of de beveiliging van cliënt-informatie, we begrijpen bij Intermax dat er enorm veel op het spel staat. Door onze jarenlange samenwerking met verschillende type zorgorganisaties weten wij waar het om draait binnen de zorg.

Uw organisatie staat voor de cruciale taak om de IT-systemen naadloos te laten integreren met uw zorgverlening. Dit vraagt om expertise en professionaliteit op het gebied van IT-beheer. Het uitbesteden van IT-beheer aan gespecialiseerde partners zoals Intermax kan een aantrekkelijke oplossing zijn.

Door te vertrouwen op een partner met toewijding aan de zorgsector én bewezen ervaring, kunnen u en uw medewerkers zich richten op waar ze het beste in zijn: het leveren van hoogwaardige zorg.

Met oplossingen zoals de HealthCloud van Intermax kunnen zorginstellingen profiteren van een zeer hoge beschikbaarheid van hun IT-omgeving en opslag van data in Nederland. En met de geruststelling dat het beheer en de 24/7 monitoring in ervaren handen zijn. Benieuwd wat de Intermax HealthCloud voor uw organisatie kan betekenen?





Slim in denken. Uniek in doen.

Ontdek de Intermax manier

Over Intermax

Intermax heeft zich de afgelopen 30 jaar gespecialiseerd in het waarborgen van de digitale continuïteit en veiligheid van maatschappelijk cruciale organisaties, waaronder zorginstellingen. Wij leveren verschillende cloud- en cybersecurity-oplossingen, afgestemd op de wensen en eisen van de zorg. Inclusief (moderne) werkplekken, zorgapplicaties en onze 100% Nederlandse Intermax HealthCloud. Wij richten onze oplossingen duurzaam, schaalbaar en kostenefficiënt in. Wij waarborgen daarbij de digitale continuïteit en veiligheid, en staan 24/7 voor onze klanten klaar. Op basis van onze kennis en kunde helpen we zorginstellingen met het maken van de juiste keuzes. Wij houden onze kennis en deskundigheid up-to-date, zodat we onze klanten ook in de toekomst de beste oplossingen kunnen blijven bieden.



ISAE 3402 TYPE II &
SOC2 ASSURANCE

Contact

Intermax

Schouwburgplein 30 – 34
3012 CL Rotterdam
+31(0) 10 – 710 4444
info@intermax.nl

Copyright Intermax Cloudsourcing B.V., 2024

