Uw Ideale ZorgSecurity

Zorgorganisaties gebruiken ICT bij een grote diversiteit aan werkzaamheden:

- Een thuiszorgmedewerker wil 's morgens de agenda kunnen bekijken op de tablet. Overdag bij een cliënt aan huis via een app op de smartphone een registratie uitvoeren. In de middag documenten zoals een zorgplan bewerken via een gedeelde werkplek.
- Een arts of verpleegkundige wil zowel thuis als op de zorglocatie vlot verslagen kunnen lezen, schrijven en bewerken. Daarvoor is een stabiele en veilige verbinding essentieel. Diezelfde verbinding maakt ook videogesprekken met collega's en cliënten mogelijk.
- Omdat cliënten langer thuis blijven wonen, wordt ambulante zorg en de technologische ondersteuning daarvan een vast onderdeel van het zorgproces.

Cybersecurity is van essentieel belang binnen de zorgsector. Er wordt namelijk gewerkt met zeer vertrouwelijke gegevens van cliënten en patiënten. Omdat de werkdruk hoog is, lopen medewerkers extra risico om onbewust fouten te maken. Juist daarom is het belangrijk dat hun cybersecurity awareness op peil is, zodat ze verdachte situaties herkennen en niet zomaar ergens op klikken.

Door de digitale transformatie hebben zorgmedewerkers altijd en overal toegang tot hun data. Ze gebruiken daarvoor niet alleen SaaS-applicaties en cloudopslag, maar ook toepassingen en bestanden op hun eigen toestellen. Het laatste wat u wilt, is dat gevoelige cliëntgegevens op straat belanden. Daarom is het cruciaal om devices goed te beveiligen en ongeautoriseerde toegang te voorkomen.

Wij helpen u met het maken van de juiste keuzes voor Uw Ideale ZorgSecurity. Met een goed ingerichte securityomgeving waarborgt u de veiligheid van data, zonder de efficiëntie van de werkomgeving van uw medewerkers te belemmeren. Veiligheid vergroten betekent risico's verkleinen. En omdat het ICT-landschap voortdurend verandert en steeds complexer wordt, is cybersecurity geen eindpunt maar een proces van voortdurende verbetering.

Het beschermen van uw data tegen cyberdreigingen is een combinatie van maatregelen zoals beschreven staan in deze whitepaper, aangepast aan uw organisatie. Voor zorginstellingen zijn er extra aandachtsgebieden, zoals de bescherming van vertrouwelijke cliëntendata en de toegang daartoe.

We zien dat financiële ontwikkelingen in de zorgsector voor een toenemend aantal zorgorganisaties een extra uitdaging is. Dit kan leiden tot keuzes op basis van prioriteiten. Welke risico's moeten we direct aanpakken of mitigeren en welke zaken kunnen we later regelen? Het opstellen van een cybersecurity roadmap kan hierin ondersteunen.

De NIS2-richtlijn (Network and Information Security directive, version 2) is inmiddels omgezet in Nederlandse wetgeving. Voor veel zorgorganisaties betekent dit dat zij aanvullende cybersecuritymaatregelen moeten nemen om aan de strengere eisen te voldoen.

SLTN ontwikkelde een helder framework om de cybersecurity van zorgorganisaties te versterken. Het is gebaseerd op NEN 7510, de AVG en de internationale Critical Security Controls (CIS). Daarbij staan drie belangrijke pijlers centraal: mensen, processen en technologie.

SLTN cybersecurity framework

1. Processen

De pijler processen vormt de overkoepelende schil en omvat Governance, Risk en Compliance (GRC).

→ Vanuit **Compliance** gelden de richtlijnen van NIS2, de AVG en NEN 7510. NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg. Deze norm is gebaseerd op een Information Security Management System (ISMS) en bevat concrete beheersmaatregelen om vertrouwelijke gegevens te beschermen. De AVG bepaalt hoe organisaties zorgvuldig omgaan met (bijzondere) persoonsgegevens. Daarnaast verplicht de NIS2-richtlijn zorginstellingen om hun digitale weerbaarheid te vergroten met extra aandacht voor de bescherming van cliëntgegevens en toegangsbeheer.

→ Binnen **Risk** draait het om het systematisch in kaart brengen en mitigeren van risico's. Dat doen we via een planning- en controlecyclus: risico's identificeren, passende maatregelen nemen, opvolgen en bijsturen. Zo zorgen we voor een continue verbetering van de beveiliging.

→ **Governance** legt vast wie binnen de organisatie welke verantwoordelijkheden en rollen heeft. Zo ontstaat er duidelijke eigenaarschap en wordt er actief gewerkt aan een steeds veiliger zorgomgeving.

2. Mensen

Gebruikers wensen complexe zaken te vereenvoudigen en barrières te verminderen om werkzaamheden uit te voeren. Wij zoeken een balans tussen veiligheid en gebruikersgemak, zodat uw medewerkers veilig en eenvoudig kunnen werken. Met aandacht voor uw medewerkers en cybersecurity awareness training maken we de keten veiliger en verhogen we de continuïteit, betrouwbaarheid en kwaliteit van de zorg.

3. Technologie

Onder technologie kijken we naar applicaties, infrastructuur en data. Deze brengen we samen in centrale cybersecuritymonitoring, waar alles aan elkaar wordt gekoppeld en continu wordt bewaakt. Zo detecteert u sneller risico's en kunt u direct ingrijpen bij afwijkingen. Binnen de zorg gaat daarbij extra aandacht uit naar patiënt- en cliëntgegevens: bijzondere persoonsgegevens vereisen maximale bescherming.

In deze whitepaper vindt u een praktische richtlijn om uw cybersecurity veilig én efficiënt in te richten, zonder de continuïteit van de zorg in gevaar te brengen.

Uw Ideale ZorgSecurity
20 sleutelonderdelen

20 sleutelonderdelen van Uw Ideale ZorgSecurity:

1. Informatiebeveiligingsbeleid
2. Cybersecurity user-awareness
3. Endpoint protection
4. Vulnerability management & patch management
5. Penetratietesten
6. E-mailbeveiliging
7. Wachtwoordbeleid
8. Multi-Factor Authentication
9. Opslag logbestanden
10. Netwerkmonitoring
11. Netwerksegmentatie
12. Ransomware-resistente back-up
13. Beperkte netwerktoegang
14. Privileged Access Management (PAM)
15. SIEM/SOC
16. Geofencing
17. Cloud Access Security Broker (CASB) en Secure Access Service Edge (SASE)
18. AD-monitoring
19. Incident response plan
20. Data governance

Informatiebeveiligingsbeleid

Het startpunt van goede cybersecurity is een stevig informatiebeveiligingsbeleid. Dit beleid moet gedragen worden door de directie, uitvoerbaar zijn voor de securityverantwoordelijke en haalbaar blijven binnen de organisatie. Ook leveranciers en partners zijn eraan gebonden. Een daadkrachtig directielid communiceert het beleid actief, motiveert medewerkers en ziet toe op de naleving ervan. Daarbij krijgt hij of zij ondersteuning van de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG).

De CISO ontwerpt, implementeert en borgt het informatiebeveiligingsbeleid binnen de organisatie, gedreven door de normen en wetgeving waaraan zorginstellingen moeten voldoen, zoals NIS2, NEN 7510 en de AVG. Omdat ze werken met bijzondere persoonsgegevens, zijn zorgorganisaties verplicht om naast een CISO ook een Functionaris Gegevensbescherming (FG) aan te stellen. Samen zorgen zij voor passende maatregelen om deze gegevens te beschermen en houden zij toezicht op de naleving ervan.

Zo ontstaat een stevig fundament voor cybersecurity, waarin beleid, verantwoordelijkheden en toezicht naadloos op elkaar aansluiten.

NEN 7510

De NEN 7510 is de norm voor informatiebeveiliging in de zorg. Er staat in hoe organisaties in de zorg hun informatiebeveiliging moeten inrichten en is gebaseerd op de kwaliteitscyclus (Plan, Do, Check, Act).

Op basis van de NEN 7510 is het document NEN 7510-2 opgesteld. Daarin staan de concrete beheersmaatregelen uitgewerkt in de vorm van een model. **Dit model helpt organisaties om zichzelf kritische vragen te stellen, zoals:**

- Is er een Information Security Management System (ISMS) ingericht en is het up-to-date?
- Is het gebaseerd op een risicoanalyse?
- Wordt er een PDCA-cyclus toegepast?
- Is er een actueel informatiebeveiligingsbeleid?
- Worden kritieke applicatieleveranciers (zoals cloud- en SaaS-diensten) regelmatig getoetst?

Om NEN 7510 en AVG bestuurlijk af te stemmen is onderstaande heatmap gemaakt. Deze geeft de actuele status weer over de assen Organisatie, Techniek/derde partijen, Juridisch en Mens.

Met behulp van dit model wordt de betrokkenheid van bestuurders geborgd en kunnen de juiste prioriteiten en budgetten worden vastgesteld. Door de komst van NIS2 wordt deze heatmap nog relevanter, omdat organisaties ook hun digitale weerbaarheid aantoonbaar moeten vergroten.

Organisatie - Mens

01: Beveiligingsbeleid A.5	07: Beheer van bedrijfsmiddelen/ Media Handling A.8
02: Beveiligingsbeleid/ Management richtlijnen voor informatiebeveiliging A.5.1.1	08: Beheer van informatiebeveiligings incidenten A.16.1
03: Organisatie van informatiebeveiliging A.6	09: Bedrijfscontinuiteitsbeheer A.17
04: Organisatie van informatiebeveiliging/ Mobiele apparaten en telewerken A.6.2	010: Bedrijfscontinuiteitsbeheer/ Informatiebeveiligings-aspecten van bedrijfscontinuiteitsbeheer A.17.1
05: Beheer van bedrijfsmiddelen/ Verantwoordelijkheid voor de bedrijfsmiddelen A.8.1	
06: Beheer van bedrijfsmiddelen/ Classificatie van informatie A.8.2.1	011: Bedrijfscontinuiteitsbeheer/ Flexibiliteit en continuiteit A.17.1.3
M1: Personeel (Human Resource Mngt)/IT Security Bewustzijn A.7.2.2	
M2: Personeel/Rollen en Verantwoordelijkheden A.6.1.1	M4: Personeel/Tijdens het dienstverband A.7.2
M3: Personeel/Voorafgaand aan het dienstverband A.7.1	M5: Personeel/Beëindiging of wijziging van dienstverband A.7.3

In dit model worden scores middels kleuren geduid;

Matig Voldoende Goed Uitstekend

Techniek/Derde partijen - Juridisch

T1: Toegangsbeveiliging/ Toegangsbeleid A.9.1.1	T8: Beheer van communicatie- en bedieningsprocessen/Bescherming tegen Malware A.12.2	T14: Communicatie beveiliging/ Uitwisseling van informatie A.13.2
T2: Toegangsbeveiliging/ Toegangsrechten van gebruikers A.9.2	T9: Beheer van communicatie- en bedieningsprocessen/Backup A.12.3	T15: Verwerving, ontwikkeling en onderhoud van informatiesystemen/Beveiligingseisen voor informatiesystemen A.14.1
T3: Toegangsbeveiliging/ Toegangsbeheersing voor toepassingen en informatie A.12	T10: Beheer van communicatie- en bedieningsprocessen/Logging en monitoring A.12.4	T16: Verwerving, ontwikkeling en onderhoud van informatiesystemen/ Beveiliging bij ontwikkelings- en ondersteuningsprocessen A.14.2
T4: Cryptografische beheersmaatregelen A.10	T11: Beheer van communicatie- en bedieningsprocessen/Controle over operationele applicaties A.12.5	T17: Verwerving, ontwikkeling en onderhoud van informatiesystemen/Test data A.14.3
T5: Fysieke en omgevingsbeveiliging A.11	T12: Beheer van communicatie- en bedieningsprocessen/Technisch applicatiebeheer A.12.6	T18: Externe partijen/(toegang) A.15
T6: Fysieke en omgevingsbeveiliging/ Beveiligde gebieden A.11.1	T13: Communicatie beveiliging/ Beheer van netwerkbeveiliging A.13.1	T19: Externe partijen/informatiebeveiliging met extrerne partijen A.15.1
T7: Fysieke en omgevingsbeveiliging/ Beveiliging van apparatuur A.11.2		T20: Externe partijen/Supplier service delivery management A.15.2
J1: Data Risk Assesment/Accountability	J6: Data Risk Assesment/Bewerkers	J10: Data Risk Assesment/Bewaartermijnen
J2: Data Risk Assesment/ Data Protection Offices	J7: Data Risk Assesment/Uitwisseling van persoonsgebonden informatie aan derde(n)	J11: Data Risk Assesment/Marketing
J3: Data Risk Assesment/Data uitwisseling		J12: Compliance
J4: Data Risk Assesment/Wettelijk toegestane verwerking van persoonsgebonden data	J8: Data Risk Assesment/Transparantie	J13: Compliance/Naleving van wettelijke voorschriften
J5: Data Risk Assesment/ Verantwoordelijke/bewerker	J9: Data Risk Assesment/Betrokkene	J14: Compliance/Beheersmaatregelen voor audits van informatiesystemen A.12.7.1 en A.18.2.1

In dit model worden scores middels kleuren geduid;

Matig Voldoende Goed Uitstekend

Om NEN 7510 en AVG bestuurlijk af te stemmen is bovenstaande heatmap gemaakt. Deze geeft de actuele status weer over de assen Organisatie, Techniek/derde partijen, Juridisch en Mens. Met behulp van dit model wordt de betrokkenheid van bestuurders geborgd en kunnen de juiste prioriteiten en budgetten worden vastgesteld. Door de komst van NIS2 wordt deze heatmap nog relevanter, omdat organisaties ook hun digitale weerbaarheid aantoonbaar moeten vergroten

NIS2

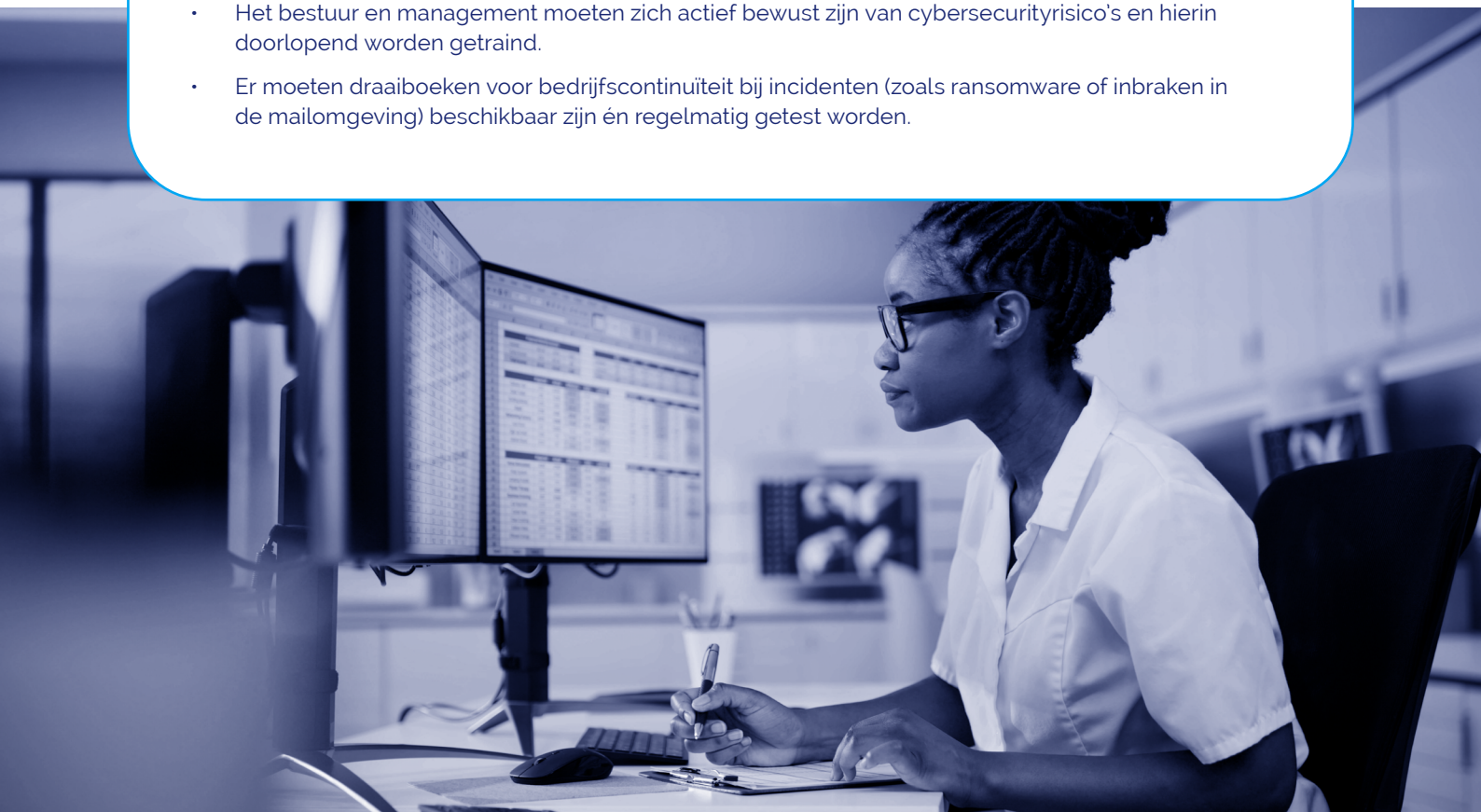
De NIS2-richtlijn is sinds 17 oktober 2024 van kracht in de Europese Unie. De richtlijn heeft als doel de digitale weerbaarheid van organisaties, waaronder zorginstellingen, te vergroten en de beveiligingsstandaarden te verhogen. Wilt u weten of dit ook voor uw organisatie geldt? **Doe de check via: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/**

Om uw organisatie te laten voldoen aan de nationale wetgeving die voortkomt uit de NIS2-richtlijn is het nodig om zo snel mogelijk te starten met de volgende maatregelen:

1. **Maak een risicoanalyse van digitale dreigingen die de dienstverlening van uw organisatie kunnen verstoren.**
2. **Neem waar mogelijk maatregelen die uw organisatie (beter) beschermen tegen deze risico's.**
3. **Zorg voor procedures die uw organisatie in staat stellen om incidenten die bedrijfsprocessen (kunnen) verstoren te detecteren, monitoren, op te lossen en te melden**
4. **Maak uw personeel bewust van de mogelijke risico's en de benodigde maatregelen.**
5. **Zorg dat uw organisatie voldoet aan bestaande normenkaders, zoals de NEN 7510 in de zorg.**

Er zullen sowieso bepaalde verplichtingen gelden:

- Het bestuur en management moeten zich actief bewust zijn van cybersecurityrisico's en hierin doorlopend worden getraind.
- Er moeten draaiboeken voor bedrijfscontinuïteit bij incidenten (zoals ransomware of inbraken in de mailomgeving) beschikbaar zijn én regelmatig getest worden.



2. Cybersecurity user-awareness

Bij de meeste organisaties zien we dat de mens de zwakste schakel in de cybersecurity is.
Dat blijkt ook uit cijfers van de Autoriteit Persoonsgegevens: bij meer dan 90% van de datalekken is de oorzaak een menselijke fout. Ons advies: zorg voor een gestructureerd programma waarmee u al uw medewerkers periodiek traint in cybersecurity awareness. Zo verandert u de zwakste schakel in uw sterkste verdediging: uw human firewall.

Om een awarenessprogramma te laten slagen, is het essentieel om een draagvlak en betrokkenheid van het management te hebben. Laat het management optreden als rolmodel, geef het programma een herkenbare bedrijfsidentiteit en maak de resultaten meetbaar én zichtbaar binnen de organisatie.

Train uw medewerkers en management om kwaadwillende pogingen tijdig te herkennen. Doe dit niet ad-hoc, maar via een planmatig programma dat is afgestemd op de functies en risicoprofielen binnen de organisatie. Een vast onderdeel daarvan zijn gesimuleerde phishingmails: een onmisbare manier om medewerkers te testen op hun daadwerkelijke gedrag en kennis.

Het is essentieel om de resultaten van trainingen en gesimuleerde phishingcampagnes te gebruiken om het awarenessprogramma continu te verbeteren. In de markt bestaan hiervoor diverse oplossingen, maar succes hangt af van de juiste mix van inhoud en dosering. Een goed programma vergroot het bewustzijn rond cybersecurity en geeft mensen bovendien intrinsieke motivatie om deel te nemen aan het programma. Voor zorgorganisaties is het belangrijk rekening te houden met de beperkte tijd van medewerkers, bijvoorbeeld door trainingen op te delen in korte, behapbare modules. Bovendien sluit dit aan bij de eisen van de NIS2-richtlijn, die bewustwording en regelmatige training van personeel verplicht stelt.

Endpoint protection

Een van de basiselementen van cybersecurity is endpoint protection: de antivirus- en antimalwareoplossing die op elke server, laptop, pc, tablet en telefoon aanwezig moet zijn. Deze wordt automatisch up-to-date gehouden en eventuele meldingen worden vanuit het bijbehorende managementplatform opgevolgd.

Dit vormt het basisbeveiligingsnet dat over de digitale infrastructuur moet worden gespannen. Toch zien we bij grote security-incidenten dat dit misgaat, vaak omdat niet alle devices zijn meegenomen, updates ontbreken of meldingen niet worden opgevolgd.

Kies voor een endpoint protection-oplossing met ransomwareblokkering en de mogelijkheid om verdachte systemen direct van het netwerk te isoleren. Omdat zero-day-kwetsbaarheden actief worden misbruikt, is bescherming hiertegen onmisbaar om schade te beperken en aanvallen snel tegen te gaan.

Het succes staat of valt met volledige dekking: alle devices moeten worden meegenomen. In een goed ingerichte en onderhouden ICT-omgeving krijgt ransomware zo geen kans. Bovendien sluit dit direct aan bij de eisen uit de NIS2-richtlijn, die passende technische beveiligingsmaatregelen verplicht stelt.

Vulnerability management en patch management

Alle software en hardware kan fouten bevatten, zogeheten bugs. Sommige bugs kunnen door cybercriminelen worden misbruikt om toegang te krijgen tot systemen of applicaties, soms zelfs zonder wachtwoord of gebruikersaccount. Dagelijks worden er nieuwe bugs ontdekt. Zodra een bug daadwerkelijk kan worden misbruikt, spreken we van een 'bekende kwetsbaarheid', ofwel een Indicator of Compromise (IoC).

Wanneer een bug wordt opgemerkt, is het de taak van de leverancier om daarmee aan de slag te gaan en een update of patch te ontwikkelen. Zodra die beschikbaar is, verschijnt er een bericht met uitleg over het probleem en de oplossing. Vanaf dat moment is de kwetsbaarheid niet alleen bekend bij de organisatie zelf, maar ook bij cybercriminelen, inclusief hoe ze kan worden misbruikt.

Vulnerability management is het proces waarbij uw omgeving dagelijks wordt gescand op bekende kwetsbaarheden. Maar deze oplossingen doen vaak veel meer. Ze kijken bijvoorbeeld ook of de instellingen van systemen en netwerken goed staan en kunnen zelfs zwakke wachtwoorden opsporen. Cijfers tonen aan dat in meer dan 95% van de cyberaanvallen misbruik wordt gemaakt van een bekende kwetsbaarheid die nog niet was verholpen.

Ook zorgdomotica en andere zorgtechnologie kunnen kwetsbaarheden bevatten. Het is daarom aan te raden deze systemen expliciet mee te nemen binnen de scope van uw vulnerability management.

Moderne werkplekken vragen om een andere aanpak, omdat medewerkers vaak thuis of onderweg werken en niet dagelijks inloggen op het bedrijfsnetwerk. Daardoor is een traditionele dagelijkse scan van de volledige ICT-omgeving niet altijd haalbaar en is endpoint protection dus essentieel: het biedt beveiliging en spoort automatisch kwetsbaarheden op, rechtstreeks op het device, ongeacht waar en wanneer medewerkers inloggen. Zo blijft de hele organisatie beschermd, ook buiten het bedrijfsnetwerk. Bovendien sluit dit direct aan bij de NIS2-richtlijn, die van organisaties eist dat zij hun endpoints en systemen structureel beveiligen tegen kwetsbaarheden.

Penetratietesten

Organisaties zetten penetratietesten vaak in wanneer ze denken hun ICT-security goed op orde te hebben. In de praktijk levert zo'n test echter altijd waardevolle inzichten en verbeterpunten op, zowel bij verwachte bevindingen als onverwachte risico's. Penetratietesten werden in het verleden vaak uitbesteed aan consultancybedrijven en gebeurden handmatig. Nu zijn er diensten beschikbaar die met gespecialiseerde tools snel en eenvoudig een test kunnen uitvoeren.

Omdat deze diensten penetratietesten grotendeels autonoom uitvoeren, kunnen ze veel vaker worden ingezet. Zo houdt u continu zicht op de actuele risico's en blijft u up-to-date met nieuwe dreigingen. De gebruikte tools leveren naast bewijsmateriaal van mogelijke misbruikscenario's ook duidelijke adviezen met prioriteiten. Daarmee kunnen ICT-beheerders direct aan de slag om de grootste risico's eerst op te lossen. Dit sluit tevens aan bij de NIS2-richtlijn, die organisaties verplicht hun digitale weerbaarheid periodiek te toetsen.

E-mailbeveiliging

91% van alle digitale aanvallen start met een e-mail. Daarom is een robuuste e-mailbeveiliging onmisbaar. Op of vóór de mailserver moeten spam- en phishingmails tegengehouden en in quarantaine geplaatst worden. Hoe goed deze beveiliging ook is, er zullen altijd berichten doorheen glippen. Maak medewerkers hiervan bewust, bijvoorbeeld via awareness-trainingen met gesimuleerde phishingmails. Via een dashboard ziet u welke gebruikers op deze berichten klikken, zodat u hen gericht aanvullende trainingen kunt aanbieden.

De technische kant van e-mail is complex en in de basis onveilig. Gebruikers kunnen meestal niet controleren of een bericht écht afkomstig is van de vermelde afzender. Cybercriminelen maken daar op grote schaal misbruik van, bijvoorbeeld via spoofing: een techniek waarbij e-mails worden verzonden in naam van iemand anders, zoals de algemeen directeur aan het hoofd van de financiële administratie. Zulke nepberichten kunnen niet alleen uw medewerkers bereiken, maar ook klanten en leveranciers. Dit risico is te voorkomen met goede e-mailbeveiliging, waaronder een correct geactiveerd DMARC-record. Daarmee voorkomt u dat derden zich digitaal als uw organisatie voordoen.

Domain-based Message Authentication, Reporting and Conformance (DMARC) is een e-mailverificatieprotocol. Het stelt beheerders in staat om hun domein te beschermen tegen ongeoorloofd gebruik, zoals e-mailspoofing, en misbruik te voorkomen door CEO-fraude, phishing en andere vormen van e-mailfraude. Daarnaast is e-mail niet altijd het juiste middel om gevoelige informatie, zoals cliëntendata, te delen. Daarvoor zijn zorgspecifieke, veilige berichtenoplossingen een beter en betrouwbaarder alternatief.

Wachtwoordbeleid

Een wachtwoordbeleid legt vast aan welke eisen wachtwoorden moeten voldoen: lengte, complexiteit en wijzigingsfrequentie. Voor veel gebruikers is het lastig om zelf sterke wachtwoorden te bedenken. Daarom is ondersteuning nodig. In awareness-trainingen leren medewerkers hoe ze veilige wachtwoorden maken en beheren. Belangrijk daarbij is dat wachtwoorden strikt persoonlijk blijven en nooit gedeeld worden, zelfs niet met een collega die 'even snel' wil inloggen. Ook het gebruik van groepsaccounts is sterk af te raden.

Wanneer wachtwoorden te complex zijn, vergeten gebruikers ze snel. Ze schrijven hun wachtwoorden dan op briefjes die ergens blijven rondslingeren. Ook zien we vaak dat oude wachtwoorden opnieuw gebruikt worden. Daarbij is er vaak het risico dat ze al eerder gelekt werden en dus in handen zijn van cybercriminelen. Maak medewerkers daarom duidelijk dat wachtwoorden altijd uniek moeten zijn en niet hergebruikt mogen worden voor privé e-mail- of internetaccounts. Technische maatregelen kunnen helpen door oude of zwakke wachtwoorden automatisch te blokkeren. Wachtwoorden als '1234567', 'Welkom123' of 'admin' zijn uiteraard niet aanvaardbaar.

Om te voorkomen dat medewerkers voor elke toepassing een apart wachtwoord moeten invoeren, kan Single Sign-On (SSO) worden ingezet. Daarmee logt een gebruiker één keer in en krijgt die vervolgens toegang tot meerdere toepassingen, waardoor het aantal wachtwoorden drastisch afneemt. Een alternatief is de inzet van smartcards in combinatie met een pincode. Deze oplossing wordt in de zorg selectief toegepast en biedt snelle en veilige toegang, maar heeft wel een hoger prijskaartje.

Met SSO volstaat voor de meeste zorgmedewerkers één wachtwoord. Kennismedewerkers die met veel verschillende toepassingen werken, hebben echter vaak meerdere wachtwoorden nodig. Voor hen kan een veilige passwordmanager een oplossing bieden, zodat ze toch sterke en unieke wachtwoorden kunnen gebruiken zonder in te leveren op gemak.

Multi-Factor Authentication (MFA)

Een gebruikersnaam en wachtwoord zijn niet langer voldoende om gevoelige gegevens te beschermen. Multi-Factor Authentication (MFA) is in veel gevallen een goede extra beveiligingslaag. De gebruiker voert tijdens het inloggen iets in wat hij weet (zoals een wachtwoord) en iets wat hij heeft (zoals een sms-code).

Bij zeer gevoelige data is het verstandig om middelen te gebruiken met een 'substantieel' of 'hoog' betrouwbaarheidsniveau, zoals een fysieke token. Dat lijkt misschien omslachtig, maar in de praktijk is het onmisbaar. Vrijwel iedereen gebruikt MFA al bij internetbankieren; waarom dan niet ook op het werk? Voor ICT-beheerders en bij het beheren van SaaS-oplossingen is MFA inmiddels een minimale vereiste.

Met de huidige rekenkracht kraken hackers wachtwoorden in een oogwenk, of ze kopen simpelweg gelekte combinaties van gebruikersnamen en wachtwoorden. Een goede MFA-oplossing biedt hiertegen effectieve bescherming.

Sommige MFA-oplossingen zijn eenvoudig te omzeilen, zeker wanneer de validatie 30 dagen geldig blijft. In dat geval heeft een aanvaller ruim de tijd om ongezien binnen het netwerk te opereren, zeker als er met een soft-token wordt gewerkt.

MFA is altijd beter dan alleen wachtwoorden, maar niet elke MFA-oplossing biedt hetzelfde beveiligingsniveau. SLTN adviseert daarom een oplossing die minimaal voldoet aan de FIDO2-standaard. Daarmee verkleint u het risico op accountovernames aanzienlijk en blijft de gebruikerservaring toch soepel. MFA zou verplicht moeten zijn voor alle accounts, zeker voor beheeraccounts. Daarnaast sluit dit aan bij de eisen van de NIS2-richtlijn, die organisaties verplicht sterke toegangsbeveiliging in te richten. Geen MFA betekent misschien meer gemak voor gebruikers, maar levert ook een enorm extra risico op. De vraag is: kunt u en wilt u dat risico nemen?

Opslag logbestanden

Elk systeem genereert logbestanden en slaat ze lokaal op voor een beperkte tijd. Door ze centraal te verzamelen, kunnen ze beter worden bekeken en beoordeeld. Normen zoals NEN 7510 (maatregel 12.4) en NEN 7513 verplichten bovendien dat logbestanden veilig worden bewaard. Na een security-incident is het cruciaal om de oorzaak te achterhalen en te onderzoeken welke onderdelen van de organisatie zijn geraakt. Ook de NIS2-richtlijn benadrukt het belang van logging en monitoring: organisaties moeten hun systemen continu inzichtelijk maken om digitale dreigingen tijdig te detecteren en correct te rapporteren.

Logbeheer is een fundamenteel onderdeel van een goede cybersecurity. Een effectieve oplossing moet flexibel genoeg zijn om uiteenlopende gegevens op grote schaal vast te leggen en te beheren, of die nu afkomstig zijn van on-premises systemen, cloudomgevingen of traditionele logbestanden. Het archiveren, doorgeven, opslaan en doorzoeken van loggegevens moet bovendien eenvoudig zijn en mag geen complexe programmeer- of query-vaardigheden vereisen.

In de praktijk worden logs vaak wel centraal opgeslagen, maar zelden geanalyseerd door de enorme hoeveelheid, tijdsdruk en complexiteit. Door loggegevens door te sturen naar een SIEM-omgeving, aangevuld met een SOC-dienst voor analyse, kunnen ze wel effectief op risico's worden beoordeeld. De NIS2-richtlijn onderstreept het belang van continue monitoring: organisaties moeten afwijkingen snel kunnen signaleren en opvolgen.

Netwerkmonitoring

Een firewall houdt veel tegen, maar niet alles. Daarom is het slim om netwerkmonitoring apart in te richten. Daarmee krijgt u helder inzicht in wat er op en rond uw netwerk gebeurt en worden afwijkingen of verdacht gedrag direct zichtbaar.

Een netwerkoplossing analyseert al het inkomende en uitgaande verkeer en slaat alarm bij verdachte of ongewenste activiteiten. Denk daarbij aan shadow IT of zogenaamde Command & Control-verkeer.

Omdat steeds meer medewerkers via SaaS-applicaties en externe werkplekken werken, loopt niet al het dataverkeer meer via het bedrijfsnetwerk. Traditionele monitoring schiet dan tekort. DNS-security kan dit gat opvullen door ook verkeer buiten het bedrijfsnetwerk inzichtelijk te maken en vormt zo een waardevolle aanvulling.

Netwerksegmentatie

Vanuit security-oogpunt is het verstandig om uw netwerk op te delen in segmenten. Deze 'netwerksegmentatie' voorkomt dat een virus of aanvaller zich vrij kan verspreiden, beperkt de impact van ransomware- of DDoS-aanvallen en maakt het voor hackers lastiger om bij gevoelige gegevens te komen. Mocht er toch een aanval plaatsvinden, dan blijft de schade beperkt. Bovendien vergroot segmentatie het beveiligingsbewustzijn binnen de organisatie.

Een goed uitgangspunt hierbij is: netwerkverkeer is standaard niet toegestaan. Voeg vervolgens specifieke firewallregels toe voor de toegestane stromen. Blokkeer verkeer niet te rigoureus, want dat kan de bedrijfsvoering verstoren. Begin daarom altijd met monitoren om vast te stellen welke datastromen noodzakelijk zijn, en stel pas daarna de blokkades in.

Ransomware-resistente back-up

Een ransomware-resistente back-up (immutable back-up) is een back-up die volledig losstaat van het eigen netwerk, ook voor admin-accounts met de hoogste rechten. Zo'n opzet kan eenvoudig worden ingericht met moderne back-upoplossingen of via een serviceprovider. Mocht een hacker ondanks alle voorzorgsmaatregelen toch domeinadminrechten bemachtigen en alle data versleutelen, dan is dit uw offline verzekeringspolis.

Zorg er wel voor dat de back-up regelmatig wordt getest. Voer in een aparte omgeving een restoretest uit, herhaal dit periodiek en zorg voor een duidelijk draaiboek. Alleen zo weet u zeker dat de back-up in geval van nood ook daadwerkelijk werkt.

Beperkte netwerktoegang

Sluit alle netwerkpoorten en -protocollen die niet nodig zijn voor de bedrijfsvoering. Overbodige open poorten vergroten onnodig het aanvalsoppervlak en maken uw organisatie kwetsbaar.

De basisregel is: dicht, tenzij expliciet nodig. In de praktijk zien we vaak het omgekeerde: alles staat open, tenzij niet nodig. Bij SLTN helpen we organisaties inzicht te krijgen en stap voor stap naar een veilige inrichting toe te werken.

Zorg er daarnaast voor dat alleen vertrouwde apparaten toegang krijgen tot het bedrijfsnetwerk. Blokkeer de uitgifte van IP-adressen aan onbekende devices, zowel bekabeld als draadloos.

Privileged Access Management (PAM)

Organisaties hebben volledig inzicht nodig in de activiteiten van beheerders binnen hun ICT-omgeving, zowel van de eigen admins als van externe service engineers van partners en leveranciers.

Privileged Access Management (PAM) biedt hiervoor de oplossing. PAM monitort en registreert alle acties van privileged accounts en geeft organisaties grip, zicht en controle over deze hoog-risico-rechten. Goed beheer betekent: geen domeinadmin-accounts voor regulier beheer en zo veel mogelijk het principe van 'least privilege' toepassen.

Het gaat hier om de vraag: wie bewaakt de bewakers? PAM maakt het voor aanvallers veel lastiger om misbruik te maken van beheerrechten en signaleert direct onverwachte wijzigingen die aanleiding kunnen zijn voor nader onderzoek. Daarnaast blokkeert een goed ingerichte PAM-oplossing automatisch de toegang van medewerkers die van functie veranderen of de organisatie verlaten.

Security Information and Event Management (SIEM) / Security Operations Center (SOC)

Als uw organisatie de ICT-beveiliging naar een hoger niveau wil tillen, dan is een Security Information and Event Management (SIEM)-oplossing een belangrijke stap. Een SIEM verzamelt logbestanden en informatie uit alle systemen, applicaties en gebruikersactiviteiten binnen de organisatie. Ook data uit Active Directory wordt meegenomen, zodat gegevens leesbaar en traceerbaar worden. Door deze data automatisch te correleren, worden verdachte patronen of dreigingen zichtbaar die anders onopgemerkt zouden blijven.

Moderne SIEM-oplossingen gaan verder dan loganalyse alleen: ze kijken ook naar gebruikers- en systeemgedrag. Zodra afwijkende patronen worden gesignaleerd, volgt er automatisch een alarm en kunnen cybersecurityspecialisten de situatie analyseren. Zo kunnen risico's vaak in de kiem worden gesmoord. Daarnaast maakt SIEM het mogelijk om achteraf incidenten te reconstrueren, doordat het ook terug in de tijd kan kijken. Een SIEM-oplossing is wel pas zinvol als er binnen de organisatie een goede basis security is die de SIEM-oplossing van relevante data kan voorzien.

Een Security Operations Center (SOC) ondersteunt dit proces. Cybersecurity-analisten houden hier continu toezicht, beoordelen incidenten en geven advies. Voor veel zorginstellingen is het uitbesteden van het SOC een logische keuze, gezien de beperkte budgetten en het tekort aan gespecialiseerde securitymedewerkers.

Geofencing

Geofencing is een techniek waarmee netwerkverkeer uit bepaalde regio's of landen wordt geblokkeerd. Samen bepalen we welke landen geen toegang krijgen.

Op firewall-niveau wordt dit verkeer automatisch tegengehouden. Zo helpt geofencing om massale Denial-of-Service (DoS)- of botaanvallen te beperken, die vaak afkomstig zijn uit het buitenland en een netwerk kunnen platleggen doordat systemen de hoeveelheid aanvragen niet meer aankunnen. Geofencing houdt veel ongewenst verkeer tegen.

CASB/SASE

Voorheen draaiden de meeste applicaties binnen het datacenter, terwijl nu steeds meer verkeer rechtstreeks via SaaS loopt. Het datacenter of de cloudomgeving wordt daardoor minder het middelpunt van alle applicaties, maar vooral een schakel voor toegang en authenticatie. Dat vraagt om een nieuwe aanpak van netwerksecurity.

De rol van de firewall in de cloud of het datacenter wordt hierdoor beperkt en dat brengt nieuwe risico's met zich mee. Moderne technieken zoals Cloud Access Security Broker (CASB) en Secure Access Service Edge (SASE) zorgen voor gecontroleerde en veilige toegang tot SaaS-applicaties en vormen zo de opstap naar een zero trust-securitymodel.

AD-monitoring

De Active Directory (AD) (of Entra ID in de Azure-variant) is het hart van de ICT-infrastructuur. Hier worden alle gebruikers, rechten en privileges beheerd. Voor hackers is dit de 'doos van Pandora': eenmaal binnen hebben ze vrijwel volledige controle over de omgeving.

Met AD-monitoring krijgt u inzicht in de zwakke plekken binnen uw domeinen. U kunt deze kwetsbaarheden vervolgens aanpakken op basis van prioriteit, zodat de kans op misbruik aanzienlijk wordt verkleind.

Incident response plan

Wat doet u als het ondanks alle voorzorgsmaatregelen toch misgaat? Daarvoor is een goed doordacht incident response plan nodig. Zo'n plan moet niet alleen op een pc staan. Die kan juist onbruikbaar zijn tijdens een aanval. Bereid uw organisatie daarom voor en stel een crisisteam samen. Wachten tot het moment wanneer het misloopt, is simpelweg te laat.

Tijdens een crisis moeten veel acties tegelijk worden uitgevoerd. Dat vraagt om beschikbare resources, duidelijke processen en heldere communicatie. Een incident response plan helpt dit te plannen: het versnelt de reactie, verhoogt de effectiviteit en legt vast wie welke rol vervult. Zo bevat het plan de allocatie van mensen en middelen, de opzet van de crisisorganisatie en een zorgvuldig uitgewerkt communicatieplan.

Bedenk dat u bij een serieus incident vaak geen toegang meer heeft tot de gebruikelijke ICT-middelen. E-mail ligt eruit, intranetpagina's zijn offline, het interne netwerk is niet bereikbaar en zelfs het telefoonsysteem kan getroffen zijn. Hoe voert u dan de regie? Hoe communiceert u met de mensen die het incident moeten oplossen? Hoe informeert u medewerkers, cliënten en de pers? De mogelijkheid om snel en met minimale schade te herstellen, hangt af van een gedegen voorbereiding en een goed uitgewerkt incident response plan.

Een belangrijk onderdeel daarvan is het vooraf regelen van externe expertise. Specialisten in forensisch onderzoek of zelfs in onderhandeling en communicatie met cybercriminelen kunnen op afroep beschikbaar zijn. Door vooraf afspraken vast te leggen, krijgt u tijdens een calamiteit direct toegang tot deze hulp.

De NIS2-richtlijn benadrukt dit uitdrukkelijk: organisaties zijn verplicht een incident response plan te hebben, inclusief communicatie- en escalatieprocedures, zodat incidenten effectief kunnen worden beheerst en gemeld.

Een belangrijk onderdeel daarvan is het vooraf regelen van externe expertise. Specialisten in forensisch onderzoek of zelfs in onderhandeling en communicatie met cybercriminelen kunnen op afroep beschikbaar zijn. Door vooraf afspraken vast te leggen, krijgt u tijdens een calamiteit direct toegang tot deze hulp.

De NIS2-richtlijn benadrukt dit uitdrukkelijk: organisaties zijn verplicht een incident response plan te hebben, inclusief communicatie- en escalatieprocedures, zodat incidenten effectief kunnen worden beheerst en gemeld.

Data governance

Organisaties zijn afhankelijk van data: van financiële gegevens en contactinformatie tot gezondheidsdossiers van cliënten en intellectueel eigendom. De hoeveelheid data die wordt gecreëerd, verzameld en uitgewisseld groeit explosief.

Niet alle data is even kritisch. Sommige informatie heeft een lage waarde, andere data is uiterst gevoelig, gereguleerd of zelfs bedrijfskritisch. Denk aan patiëntendossiers, personeelsgegevens of vertrouwelijke bedrijfsinformatie. Juist deze data vraagt om strikte bescherming.

Databeveiliging wordt dus steeds belangrijker, maar ook steeds complexer: wat staat waar, welke informatie bevindt zich in de cloud, met wie wordt data gedeeld en hoe houdt u overzicht? Snelle detectie van datalekken is cruciaal om de impact te beperken. Zodra een mogelijk lek wordt ontdekt, moet de organisatie direct kunnen onderzoeken en reageren. De juiste tools en een goed gedocumenteerd responsplan maken dit mogelijk.

Met oplossingen voor automatische dataclassificatie, security-monitoring en audit & compliance (waaronder de AVG en NEN 7510) brengen we data governance op orde. Ook de NIS2-richtlijn legt hier de nadruk op: organisaties moeten weten welke data ze beheren, hoe die wordt beschermd en hoe incidenten snel worden opgespoord en gemeld.

Uw Ideale ZorgSecurity

Samen met u werken wij stap voor stap aan een veiligere ICT-omgeving voor uw zorginstelling.

Dankzij onze ervaring met security-vraagstukken in de zorg adviseren en ondersteunen wij u bij het kiezen van de geschikte maatregelen voor uw organisatie. Iedere organisatie is anders. Via onderzoek en workshops bepalen we samen wat voor u nodig is om uw ICT-omgeving veiliger te maken.

Samen met u en onze partners creëren en beheren we Uw Ideale ZorgSecurity. We nemen de regie uit handen en begeleiden het volledige traject: van ontwerp en inrichting tot beheer en doorontwikkeling

Daarbij besteden we extra aandacht aan adoptie, zodat medewerkers soepel kunnen overstappen naar een veiligere werkomgeving. Ook bij dreigingen of verstoringen staan wij direct klaar om samen tot een oplossing te komen.

Vanaf het eerste moment is onze security-architect betrokken bij Uw Ideale ZorgSecurity. Hij of zij kent uw omgeving door en door, beoordeelt nieuwe innovaties en vertaalt uw wensen naar haalbare oplossingen. Deze bespreken wij regelmatig met u om uw cybersecurity up-to-date en veilig te houden.

Zo borgen wij samen Uw Ideale ZorgSecurity!

Neem contact op →

SLTN
Future Proof IT

Colosseum 9
1213 NN Hilversum
Email: sltnvoordezorg@sltn.nl
Tel: 035 - 688 84 00