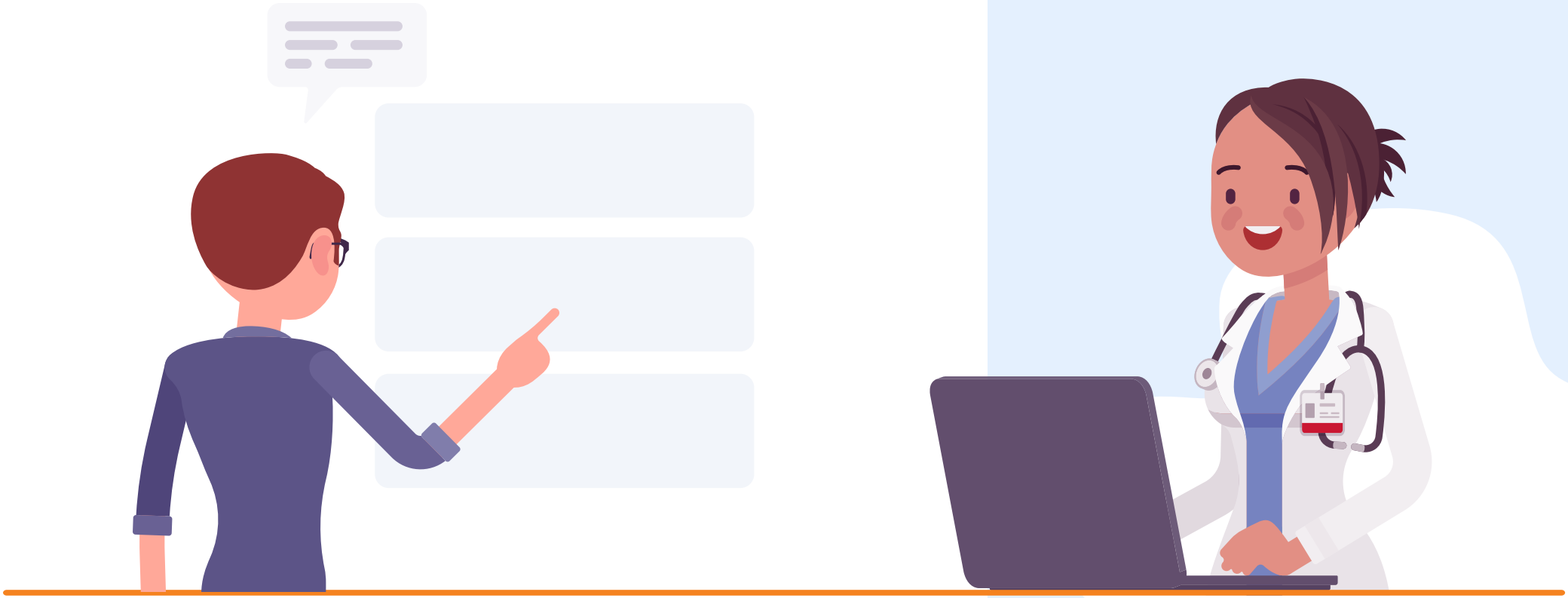
SLTN
Future Proof IT

UW IDEALE ZORGSECURITY



Uw Ideale ZorgSecurity - Inleiding

Zorgorganisaties gebruiken ICT bij een grote diversiteit aan werkzaamheden:

- Een thuiszorgmedewerker wil 's morgens de agenda kunnen bekijken op de tablet. Overdag bij een client 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 verslagen kunnen lezen, schrijven of bewerken. Dit via een goed functionerende en veilige verbinding. En met behulp van deze verbinding een videogesprek contact hebben met collega's en cliënten.
- Cliënten blijven langer thuis wonen en hierdoor wordt ambulante zorg en het technologisch ondersteunen hiervan onderdeel van het zorgproces.

De Cyber Security binnen de zorgsector is van essentieel belang. In de zorg wordt gewerkt met vertrouwelijke informatie van cliënten en patiënten. Hierbij is de werkdruk van de zorgmedewerker hoog en kan de Cyber Security awareness van de zorgmedewerker verbeteren.

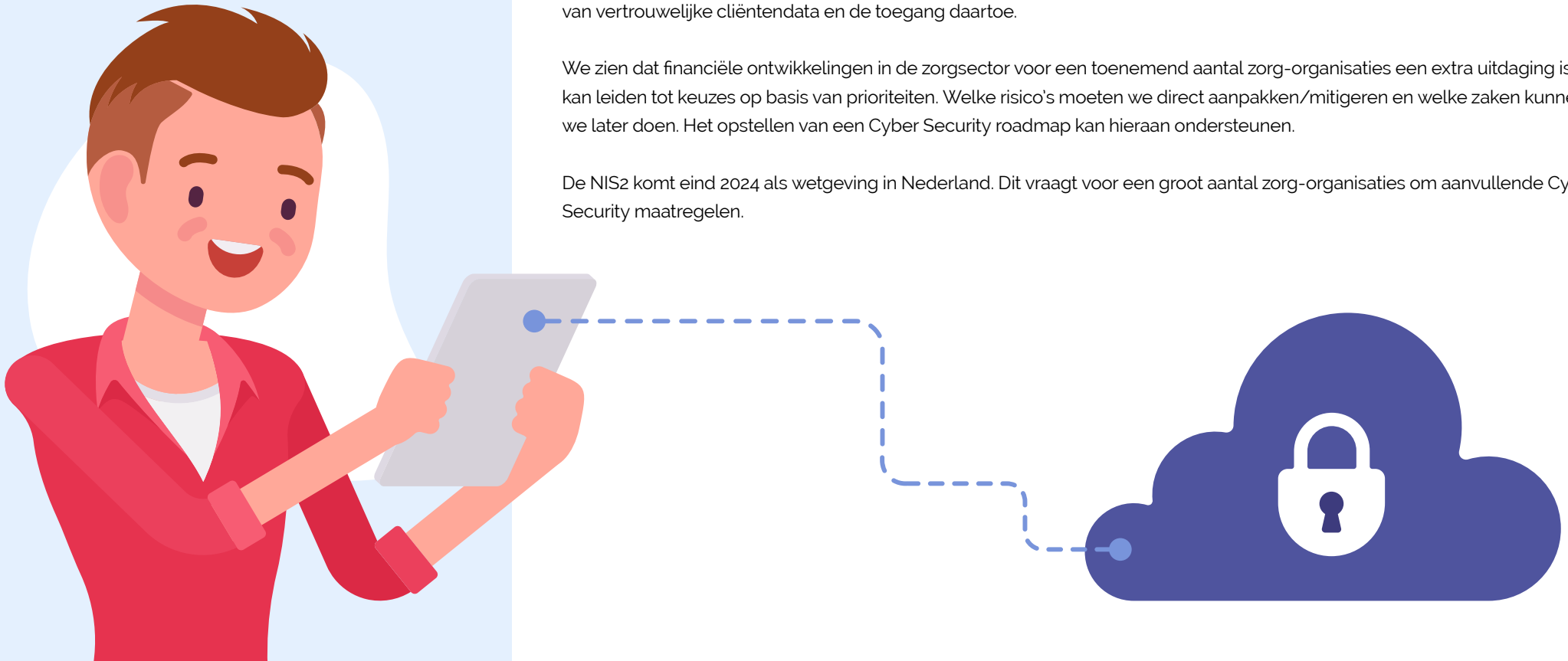
Dankzij de digitale transformatie is het steeds makkelijker voor zorgmedewerkers om altijd en overal data beschikbaar te hebben. Hiervoor gebruiken zij naast SaaS-applicaties en data in de Cloud ook applicaties en data op het device zelf. U wilt niet dat deze cliëntgegevens zomaar op straat komen te liggen. Daarom is het belangrijk om deze devices te beveiligen en ongeautoriseerde toegang te voorkomen.

Wij helpen u met het maken van de juiste keuzes voor Uw Ideale ZorgSecurity. Met behulp van een goed ingerichte securityomgeving waarborgt u de veiligheid van data en gegevens. Dit zonder afbreuk te doen aan de efficiëntie die de werkomgeving uw medewerkers biedt. Het verhogen van veiligheid bereiken we door het verminderen van risico's. Doordat het ICT-landschap voortdurend in ontwikkeling is en elke dag complexer wordt, is security een proces van voortdurende verbetering van drie belangrijke pijlers: mensen, processen en technologie.

Het beschermen van uw data tegen Cyber dreigingen is een combinatie van maatregelen zoals beschreven staan in dit whitepaper, gespecificeerd op uw organisatie. Voor zorginstellingen zijn er extra aandachtsgebieden, zoals de bescherming van vertrouwelijke cliëntendata en de toegang daartoe.

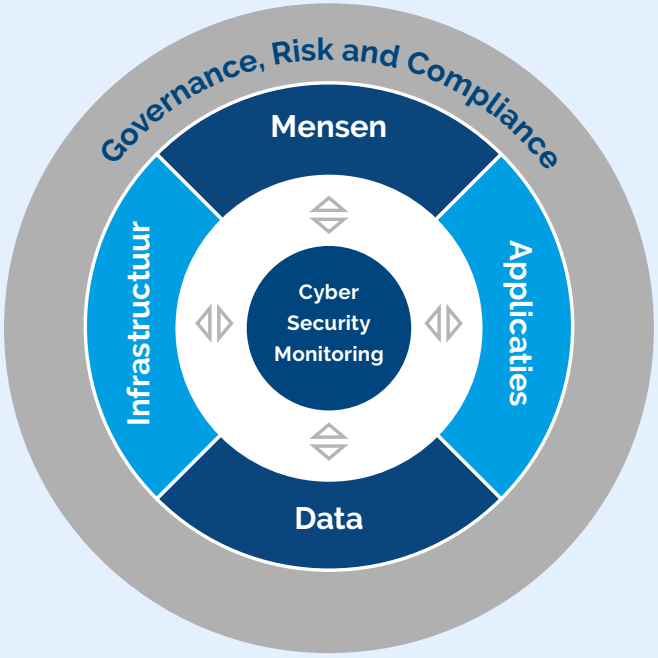
We zien dat financiële ontwikkelingen in de zorgsector voor een toenemend aantal zorg-organisaties een extra uitdaging is. Dit kan leiden tot keuzes op basis van prioriteiten. Welke risico's moeten we direct aanpakken/mitigeren en welke zaken kunnen we later doen. Het opstellen van een Cyber Security roadmap kan hieraan ondersteunen.

De NIS2 komt eind 2024 als wetgeving in Nederland. Dit vraagt voor een groot aantal zorg-organisaties om aanvullende Cyber Security maatregelen.



SLTN heeft een Framework met herkenbare blokken om uw Cyber Security te optimaliseren. De opzet, inrichting en borging van het Framework voor de Nederlandse zorgorganisaties is gebaseerd op NEN7510, de AVG wetgeving en de internationale Critical Security Controls (CIS). In het Framework staan drie belangrijke pijlers centraal: mensen, processen en technologie.

SLTN Cyber Security framework



Processen

De pijler processen is de overkoepelde schil met Governance, Risk en Compliance.
Vanuit Compliance worden de richtlijnen conform de AVG en NEN7510 gebruikt. NEN7510 bestaat uit een managementsysteem en een set aan maatregelen. Vanuit de AVG zijn er richtlijnen over hoe om te gaan met (bijzondere) persoonsgegevens. Het mitigeren van risico's (Risk) wordt vanuit een planning en control cyclus uitgevoerd. Binnen Governance stellen we vast wie welke rol heeft in het creëren van een steeds veiligere omgeving.

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 Cyber Security awareness training maken we de keten veiliger en verhogen we de continuïteit, betrouwbaarheid en kwaliteit van de zorg.

Technologie

Applicaties, Infrastructuur en Data met centraal de Cyber Security Monitoring. Binnen de zorg is er speciale aandacht voor patiënten/cliënten-data zoals bijzondere persoonsgegevens.

In deze whitepaper bieden wij u een richtlijn voor een goede Cyber Security.

Uw Ideale ZorgSecurity 20 sleutelonderdelen

20 sleutelonderdelen van Uw Ideale ZorgSecurity

1. Informatiebeveiligingsbeleid
2. Cyber-Security User-Awareness
3. Endpoint Protection
4. Vulnerability Management en penetratietesten
5. Email beveiliging
6. Wachtwoordbeleid
7. Multi Factor Authenticatie
8. Opslag logbestanden
9. Honeypots
10. Netwerk Monitoring
11. Netwerk segmentatie
12. Ransomware resistente backup
13. Beperkte Netwerk toegang
14. Privileged Access Management
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 een goede Cyber Security is een informatiebeveiligingsbeleid. Dit beleid wordt gedragen door de directie, is uitvoerbaar voor de security verantwoordelijke, is realistisch en haalbaar binnen de organisatie en verplicht voor leveranciers en partners. Een daadkrachtig lid van de directie communiceert het informatiebeveiligingsbeleid binnen de organisatie, motiveert de medewerkers en ziet toe op de naleving van het informatiebeveiligingsbeleid. Hij of zij wordt bijgestaan door een Chief Information Security Officer (CISO) en een Functionaris voor de Gegevensbescherming (FG).

Goed bestuur en verantwoord innoveren (plannen en organiseren)

Invoering en gebruik van e-health toepassingen

Betrokkenheid van patiënten

Samenwerken en uitwisselen van gegevens

Informatiebeveiliging en continuïteit (afhankelijk van technologie)

De CISO ontwerpt, definieert, implementeert en borgt het informatiebeveiligingsbeleid binnen de organisatie. Zorgorganisaties werken met bijzondere persoonsgegevens en zijn naast de CISO verplicht om een FG aan te stellen. De FG neemt samen met de CISO passende maatregelen om (bijzondere) persoonsgegevens te beschermen en houdt hier vervolgens toezicht op.

Een actief informatiebeveiligingsbeleid en een nauwe samenwerking tussen de directie, CISO, FG en ICT-manager is cruciaal voor een goede Cyber Security. Daarbij moeten zorg organisatie voldoen aan de NEN 7510 norm en vanaf eind 2024 ook aan de NIS2-richtlijn.

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).

Vanuit de NEN 7510 is een document opgesteld NEN 7510-2 waarin de concrete beheersmaatregelen in de vorm van een model beschreven staan. Op basis van het model kunnen vragen gesteld worden zoals;

- Is er een Information Security Management System (ISMS) ingericht en actueel?
- Is dit op basis van een risicoanalyse gebaseerd?
- Wordt er een PDCA cyclus toegepast?
- Is er een actueel informatiebeveiligingsbeleid?
- Vindt er toetsing van kritieke applicatie leveranciers plaats (Cloud en SaaS diensten)?

Naast de inspectie Gezondheidszorg en Jeugd zien we voor de vanuit de Autoriteit Persoonsgegevens een andere set van vragen ten aanzien van de AVG die meegenomen kan worden.

Om deze NEN 7510 en AVG bestuurlijk af te stemmen is onderstaande heatmap gemaakt. Deze heatmap is gebaseerd op de NEN7510 en AVG en geeft de actuele status over de assen; Organisatie, Techniek/3e partijen, Juridisch en Mens.

Organisatie

o1: Beveiligingsbeleid A.5	o7: Beheer van bedrijfsmiddelen/Media Handling A.8
o2: Beveiligingsbeleid / Management richtlijnen voor informatiebeveiliging A.5.1.1	o8: Beheer van informatiebeveiligings incidenten A.16.1
o3: Organisatie van informatiebeveiliging A.6	o9: Bedrijfscontinuiteitsbeheer A.17
o4: Organisatie van informatiebeveiliging/Mobiele apparaten en telewerken A.6.2	o10: Bedrijfscontinuiteitsbeheer/ Informatiebeveiligings-aspecten van bedrijfscontinuiteitsbeheer A.17.1
o5: Beheer van bedrijfsmiddelen/ Verantwoordelijkheid voor de bedrijfsmiddelen A.8.1	
o6: Beheer van bedrijfsmiddelen/ Classificatie van informatie A.8.2.1	o11: Bedrijfscontinuiteitsbeheer/ Flexibiliteit en continuiteit A.17.1.3

Techniek/Derde Partijen

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

Mens

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

Juridisch

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;

Niet aanwezig/niet | Onvoldoende | Matig | Voldoende | Goed | Uitstekend

Met behulp van bovenstaand model wordt de betrokkenheid van de bestuurders geborgd en kunnen de juiste prioriteiten en budgetten worden vastgesteld.

Vanuit SLTN maar ook via de inspectie Gezondheidszorg en Jeugd is het mogelijk om advies te krijgen over een plan van aanpak.

NIS2

Binnen de Europese Unie is de NIS2 (Network and Information Security directive version 2) opgesteld en aangenomen. Alle deelnemende landen (waaronder Nederland) moeten de NIS2 voor eind 2024 in wetgeving hebben omgezet. De richtlijn NIS2 gaat over het vergroten van de digitale weerbaarheid van organisaties en instellingen (de richtlijn spreekt van entiteiten) in onder meer de zorgsector. Een check of dit voor uw organisatie van toepassing is, kan eenvoudig uit gevoerd worden: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Om uw organisatie voor te bereiden op 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 personeel bewust van de mogelijke risico's en benodigde maatregelen.
5. Zorg dat uw organisatie voldoet aan bestaande normenkaders, zoals de NEN7510 in de zorg.

Ondanks dat de NIS2 nog niet in Nederlandse wetgeving is omgezet is de verwachting dat de volgende zaken in ieder geval toegevoerd worden:

- Het bestuur/management van de organisatie moet Cyber Security bewust te zijn en dient hiervoor doorlopend getrained te worden.
- Draaiboeken voor bedrijfscontinuïteit bij incidenten (zoals ransomware of inbraak in de mailomgeving) zullen beschikbaar en getest moeten worden.

Cyber Security User-Awareness

Bij de meeste organisatie zien wij dat de mens de zwakste schakel in de cyber security beveiliging is. Ook als we naar de meldingen van datalekken kijken. De Autoriteit Persoonsgegevens geeft aan dat in meer dan 90% van de datalekken de oorzaak een menselijke fout is. Een belangrijk advies voor elke organisatie, is het opzetten van een gestructureerde manier om al uw medewerkers periodiek te trainen in Cyber Security awareness. Maak van uw zwakste schakel uw sterkste schakel, uw human firewall.

Om een awareness programma succesvol te laten zijn is het essentieel om draagvlak en betrokkenheid van het management te hebben. Betrek het management als rolmodel bij het invullen van een goed awareness programma. Geef het programma een eigen bedrijfsidentiteit en maak de resultaten meetbaar en zichtbaar voor de organisatie.

Train uw medewerkers en management in het herkennen van kwaadwillende pogingen om hen om de tuin te leiden. Doe dit niet ad-hoc maar met een planmatige opzet en uitvoering. Waarbij trainingen afgestemd zijn op de verschillende functies en risicoprofielen van de medewerkers. Onderdeel van een user awareness programma is het sturen van gesimuleerde phishingmails. Dit is een must en ook gelijk een goede manier om de gebruikers op hun daadwerkelijke gedrag en kennis te testen.

Het is essentieel om op basis van de trainingsresultaten en de resultaten van de gesimuleerde phishingmail-campagnes het trainingsprogramma aan te passen. In de markt zijn verschillende oplossingen beschikbaar. Een goed opgezet trainingsprogramma bestaat uit de juiste dosering en de juiste content. Het draagt bij aan verschillende aspecten van het bewustzijn aangaande Cyber Security en het geeft mensen intrinsieke motivatie om deel te willen nemen aan het programma. Hierbij wordt uiteraard rekening gehouden met de schaarse tijd van de zorgmedewerkers. Dit door het awareness programma in kleine behapbare onderdelen beschikbaar te stellen.

Endpoint Protection

Een basiselement in de Cyber Security beveiliging is endpoint protectie. Dit is de antivirus, antimalware oplossing welke op elke server, laptop, PC, tablet en telefoon aanwezig dient te zijn. Deze oplossing wordt automatisch up-to-date gehouden en eventuele meldingen worden vanuit het bijbehorende managementplatform opgevolgd.

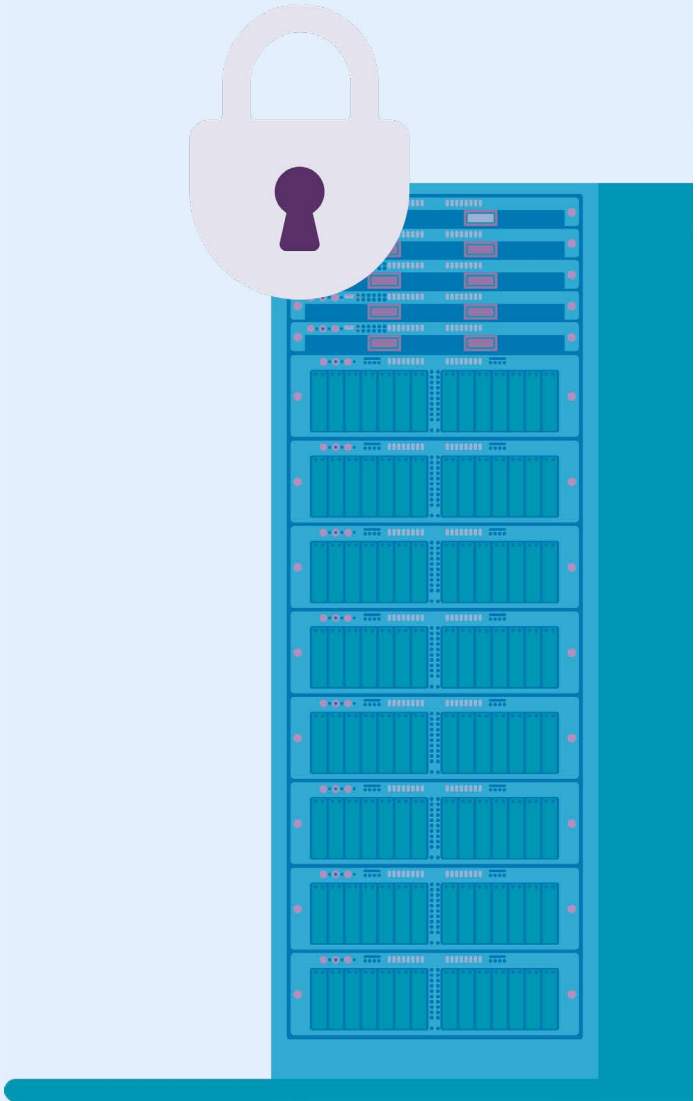
Dit is het basis beveiligingsnet dat over de digitale infrastructuur moet worden gespannen. Bij grote security incidenten zien we dit fout gaan.

Zet een endpoint protection oplossing in met een ransomware blokker en met een directe netwerkisolatie van verdachte systemen. Gelet op het actief misbruik van zero-day kwetsbaarheden is de bescherming tegen Zero-days vanuit de Endpoint protection noodzaak. Dit om schade te beperken en aanvallen direct te elimineren. De sleutel tot succes is dat alle devices worden meegenomen. In een goed ingerichte en onderhouden ICT omgeving heeft ransomware geen kans!

Vulnerability Management en patch management

Alle software en hardware kan fouten bevatten. Dit noemen we bugs. Sommige bugs maken het voor cyber criminelen mogelijk om misbruik van uw ICT-systemen te maken. Er kan toegang tot systemen en/ of applicaties worden verkregen zonder gelding wachtwoord of zelfs zonder gebruikersaccount. Dagelijks worden er nieuwe bugs ontdekt. Als een bug het mogelijk maakt om misbruik te maken noemen we het een Indicator of Compromise (IoC). Het is dan een zogenaamde "Bekende Kwetsbaarheid".

Ontdekte bugs worden door de betreffende leveranciers opgepakt en gaan aan de slag om de bug op te lossen. Zodra een update/patch beschikbaar is, wordt er een bericht uitgegeven waarin beschreven is wat het probleem is en hoe dit op te lossen is. Bij publicatie van het bericht weet iedereen wat de kwetsbaarheid is, hoe die op te lossen is, maar ook hoe dit te misbruiken is.



Vulnerability Management is het proces om dagelijks de gehele omgeving te controleren of er bekende kwetsbaarheden in de omgeving zitten. Maar deze oplossingen doen vaak veel meer. Ze kijken bijvoorbeeld ook of de instellingen van systemen en netwerken goed staan. Optioneel kunnen een aantal van deze oplossingen ook detecteren of er zwakke wachtwoorden in gebruik zijn. In meer dan 95% van de bekende gevallen van computercriminaliteit maakte de aanvallers gebruik van een bekende kwetsbaarheid die de organisatie die slachtoffer werd nog niet gerepareerd had.

Ook zorgdomotica (of zorgtechnologie) kan mogelijke kwetsbaarheden in zich hebben. Het is aan te bevelen deze mee te nemen binnen de scope van de Vulnerability Management.

Inzet van moderne werkplekken vraagt een andere aanpak daar een dagelijkse scan in de ICT-omgeving vaak niet goed mogelijk is. We zien dat een aantal EndPoint protection oplossingen de kwetsbaarheden in kaart kan brengen van de werkplekken zodat deze in de overzichten meegenomen kunnen worden.

Penetratie testen

Het uitvoeren van penetratietesten wordt vaak gedaan als een organisatie verwacht de ICT-security goed op orde te hebben. In de praktijk levert een penetratietest vaak een schat aan bruikbare informatie en verbeterpunten op. Niet alleen zaken die te verwachten waren maar ook onverwachte risico's worden inzichtelijk. Penetratietesten waren in het verleden vaak consultancy en veel handmatig werk. Nu zien we dat er diensten beschikbaar zijn die snel en eenvoudig een penetratietest kunnen uitvoeren op basis van specifieke penetratietesttools.

Door de autonome wijze waarop deze diensten de penetratietesten kunnen uitvoeren is het mogelijk om deze frequent te laten uitvoeren. Hiermee hebben we niet alleen een constant zicht op de reële risico's en bedreigen van de uw ICT maar blijven we ook up-to-date als het gaat om de nieuwe Cyber Security bedreigingen. De gebruikte tools geven naast bewijslast hoe misbruik te maken is ook een advies. In dit advies zijn prioriteiten opgenomen zodat de ICT-beheerders kunnen starten met het oplossen van de grootste risico's.

Email-beveiliging

91% van alle digitale aanvallen start met een email. Hierdoor is het belangrijk om de email goed te beveiligen.

Op of voor de mailserver dient er controle te zijn op spam- en phishing-emails. Deze mails dienen te worden verwijderd of in quarantaine geplaatst. Hoe goed deze beveiliging ook is, er zullen altijd berichten doorheen glippen. Maak uw gebruikers hierop attent. Dit kan bijvoorbeeld met behulp van User Awareness trainingen van waaruit test phishing-emails aan de gebruikers kunnen worden verzonden. Vanuit een dashboard kan gezien worden welke medewerkers op deze mails klikken. Voor deze doelgroep kunnen aanvullende trainingen worden gegeven.

De technische kant van email is redelijk complex. In de basis is email onveilig. Een veel voorkomend misbruik is gebaseerd op het feit dat een gebruiker geen controlemogelijkheden heeft en niet kan controleren of een email bericht daadwerkelijk wel afkomstig is van de naam die als afzender op het bericht staat. Cyber criminelen maken hier op grote schaal misbruik van (o.a. CEO-fraude) en dat doen ze onder meer door spoofing.Dit is een techniek om een email te versturen uit naam van iemand anders. Bijvoorbeeld uit naam van uw algemeen directeur aan het hoofd van de financiële administratie. Het kan zijn dat ze dergelijke emails naar uw medewerkers sturen, maar dat kunnen ze ook doen naar uw klanten en leveranciers. Dit kan worden voorkomen door een goede email beveiliging in te richten waarin onder meer uw DMARC-record goed is geactiveerd. Hiermee voorkomt u dat derden zich digitaal (per email) kunnen voordoen als één van uw medewerkers.

DMARC (Domain-based Message Authentication, Reporting and Conformance) is een verificatieprotocol voor e-mail. Het is ontworpen om de beheerders van e-maildomeinen de mogelijkheid te geven hun domein te beschermen tegen ongeoorloofd gebruik, beter bekend als e-mail spoofing. Het doel van DMARC is om een domein te beschermen tegen misbruik door CEO-fraude, phishingaanvallen en andere vormen van e-mailoplichterij (bron wikipedia). Niet altijd is email het juiste communicatiemiddel om informatie (zoals bijvoorbeeld cliëntendata) uit te wisselen. Inzet van zorgspecifieke veilige email/ berichten oplossingen zijn een beter alternatief.

Wachtwoordbeleid

In het wachtwoordbeleid worden de kaders gegeven waaraan de te gebruiken wachtwoorden moeten voldoen. Hoe lang en hoe complex moet het wachtwoord zijn en hoe vaak moet het worden gewijzigd.
Het is voor de meeste gebruikers moeilijk om een goed wachtwoord te bedenken, dus moeten we hier hulp bij aanbieden. In Cyber Security User Awareness trainingen wordt hier aandacht aan besteed en worden gebruikers hierbij geholpen. Gebruikers moeten wachtwoorden strikt privé houden en niet delen met bijvoorbeeld een collega die snel 'even iets' op wil zoeken. Ook is het gebruik van zogenaamde groep-accounts af te raden.

Te complexe wachtwoorden worden niet onthouden en worden opgeschreven op de bekende gele Post-it briefjes. Vaak zien we hergebruik van oude wachtwoorden. Daarbij bestaat het risico dat de wachtwoorden al eens zijn uitgelekt en in het bezit zijn van cybercriminelen.
Druk gebruikers op het hart om altijd unieke wachtwoorden te bedenken die dus ook niet voor de privé email en internetaccount worden gebruikt. Zorg er eventueel met technische middelen voor dat oude wachtwoorden niet worden geaccepteerd. En wachtwoorden zoals '1234567' 'Welkom123' en 'admin' zijn uiteraard uit den boze.

Om te voorkomen dat medewerkers voor allerlei verschillende toepassingen een wachtwoord moeten invoegen kan ook een toepassing worden geïmplementeerd waarbij er 1 keer om een wachtwoord gevraagd wordt. Dit noemen we Single Sign On (SSO). Door het toepassen van SSO-technologie verminderen we het aantal toepassingen en dus het aantal wachtwoorden wat een gebruiker moet onthouden. Een andere oplossing is de inzet van smartcards in combinatie met Pincode. Deze oplossing wordt selectief in de zorg ingezet en maakt snelle en veilige toegang voor de zorgverleners mogelijk echter heeft een dergelijke oplossing wel een hogere prijs.

Door inzet van SSO in de moderne werkplek hebben de meest zorgmedewerkers voldoende aan een enkel wachtwoord. Maar kennismedewerkers die van een veelvoud aan toepassingen gebruiken maken, hebben vaak meerdere wachtwoorden. Om deze medewerkers te faciliteren om goede en veilige wachtwoorden te blijven gebruiken, is de inzet van de veilige passwordmanager een overweging.

Multi-factor-authenticatie (MFA)

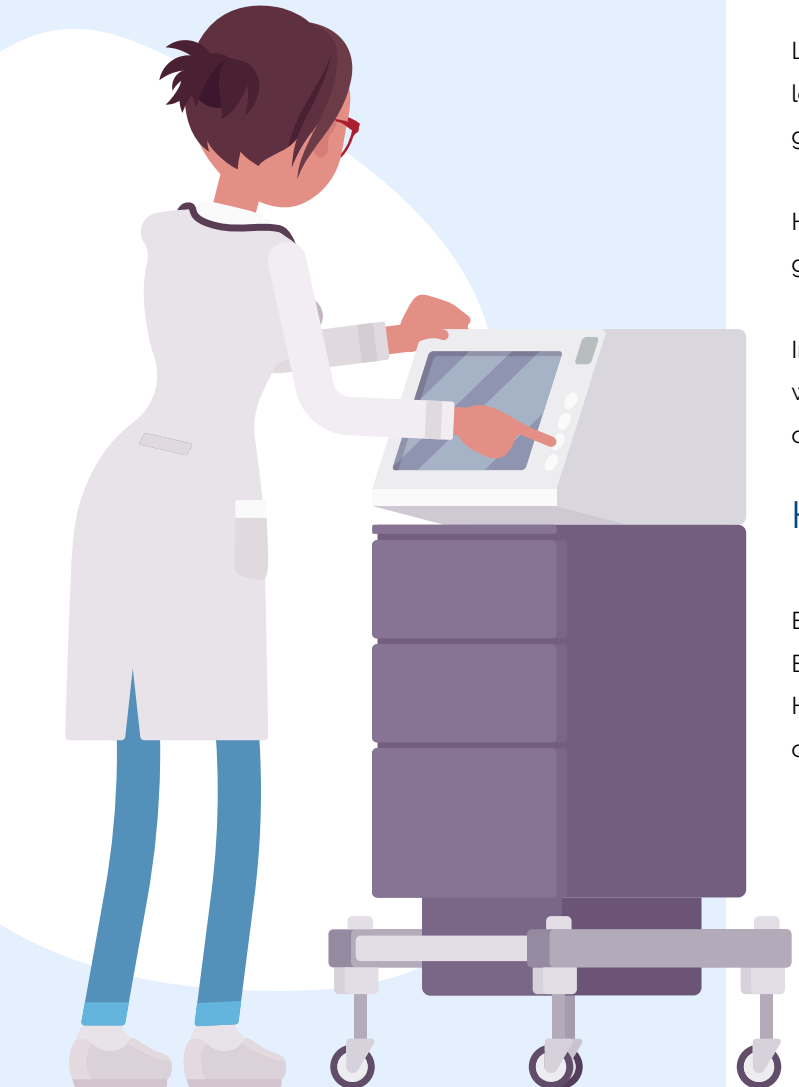
Een inlog met gebruikersnaam en wachtwoord volstaat niet meer om gevoelige gegevens af te schermen. Het gebruik van multi factor authenticatie is in veel situaties de beste optie. De gebruiker voert tijdens het inloggen iets in wat hij weet (zoals een wachtwoord) en iets wat hij heeft (zoals een sms-code).

Is de data zeer gevoelig? Dan is het verstandig om een identificatiemiddel te gebruiken met een 'substantieel' of 'hoog' betrouwbaarheidsniveau. Dit is een extra stap bij het aanloggen met een echte fysieke actie vanuit de gebruiker (bij voorkeur met een hardware token). De gemiddelde gebruiker zal dit als vervelend ervaren, maar het is tegenwoordig niet meer verantwoord om geen MFA te hebben. Alle gebruikers zullen op hun privé thuisbankier app een MFA geactiveerd hebben, waarom dan ook niet op het werk? Wij zien het gebruik van MFA voor de ICT-beheerder voor het aanloggen en het beheer van SaaS-oplossingen als een minimale eis om de veiligheid te kunnen garanderen.

Met de huidige computercapaciteit is het voor meeste hackers een fluitje van een cent om wachtwoorden te kraken. Daarnaast kunnen hackers relatief eenvoudig aan gelekte wachtwoorden komen met daarbij ook de gebruikersnamen. Het hebben van een goede MFA-oplossing geeft hier een goede bescherming tegen.

Sommige MFA-oplossingen zijn een eitje voor een gemiddelde hacker om te kraken. Zeker als de gebruiker de validatie 30 dagen geldig kan laten zijn en er met een soft-token wordt gewerkt.

MFA is dus altijd beter dan alleen wachtwoorden gebruiken. Maar niet alle MFA is gelijk. Vanuit SLTN adviseren wij om een MFA-oplossing te nemen die minimaal aan de FIDO2 standaard voldoet. Met de juiste MFA kunnen organisaties accountovernames elimineren en tegelijkertijd een geweldige gebruikerservaring bieden. MFA zou verplicht moeten zijn zowel voor de gebruikersaccounts maar helemaal voor de beheeraccounts. Het niet hebben van MFA geeft gebruikersgemak, maar geeft ook en heel groot extra risico. Kunt u en wilt u dat risico lopen?



Opslag logbestanden

Elk systeem produceert logbestanden en slaat deze lokaal op voor een beperkte tijd. Door het centraal verzamelen van alle logbestanden kunnen we deze log bestanden bekijken en beoordelen. Vanuit verschillende normeringen (zoals de NEN 7510 maatregel 12.4 en NEN 7513) wordt vereist dat u uw logbestanden op een veilige manier opslaat. Zodat er altijd teruggezocht kan worden in de logbestanden wat er gebeurd is. Na een security-incident is dit cruciaal om de oorzaak te kunnen vinden en verder te onderzoeken wat er allemaal geraakt kan zijn bij een aanval.

Logbeheer is een fundamenteel onderdeel van een goede Cyber Security. Essentieel voor elke oplossing voor logbeheer is de flexibiliteit om uiteenlopende gegevens op grote schaal vast te leggen en te beheren, of deze nu worden gegenereerd door on-premises tools, gegevensbronnen in de cloud of traditionele log bestanden.

Het archiveren, doorgeven opslaan en doorzoeken van loggegevens moet eenvoudig te realiseren zijn en geen geavanceerde programmeer- of query-vaardigheden vereisen.

In de praktijk zien we dat logs soms nog wel centraal opgeslagen worden maar zelden of nooit beoordeeld worden wegens de grote hoeveelheden logs, gebrek aan tijd en complexiteit. Door de logs door te sturen naar een SIEM omgeving met een SOC-dienst voor analyse wordt het mogelijk de logs op risico's te beoordelen.

Honeypots

Een goed ingerichte Honeypot informeert u dat er verdachte inventarisatie activiteiten worden uitgevoerd in uw netwerk. Eén van de eerste stappen die een hacker onderneemt in een netwerk is het zoeken naar bruikbare informatie. Een Honeypot detecteert dit en geeft vervolgens een melding aan de beheerders en/of een SOC afdeling zodat nader onderzoek kan plaats vinden.

Netwerkmonitoring

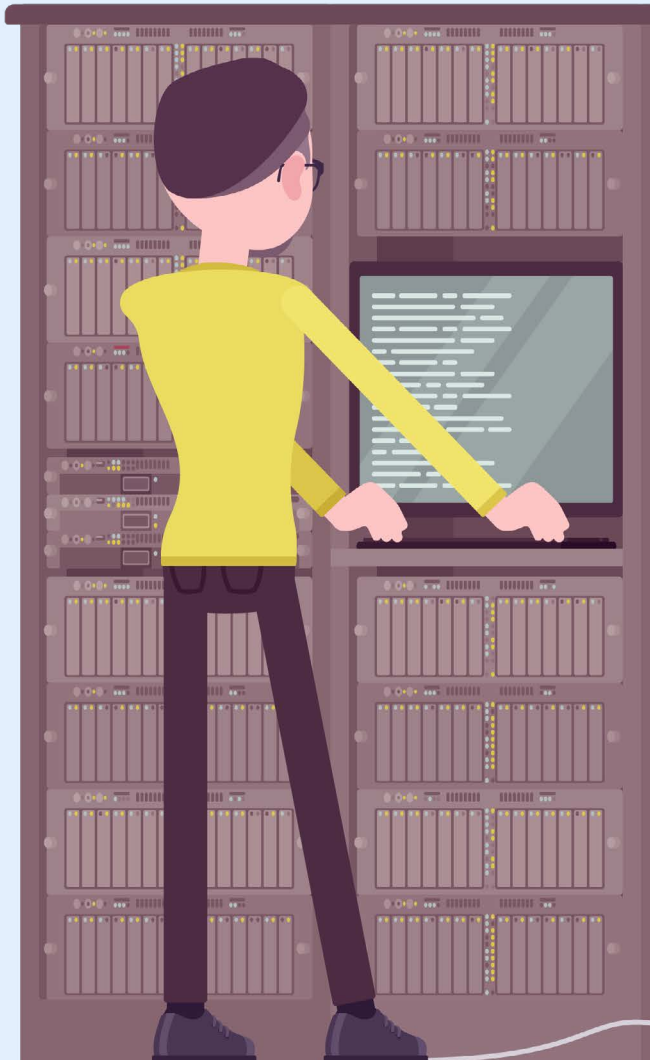
Additioneel op dat wat de moderne firewall aan detectie en preventie biedt adviseren wij om een separate netwerkmonitoring oplossing te implementeren. Deze oplossing biedt u goed inzicht in wat er zich op en rond uw computernetwerk afspeelt en worden afwijkingen en verdacht gedrag gesignaleerd.

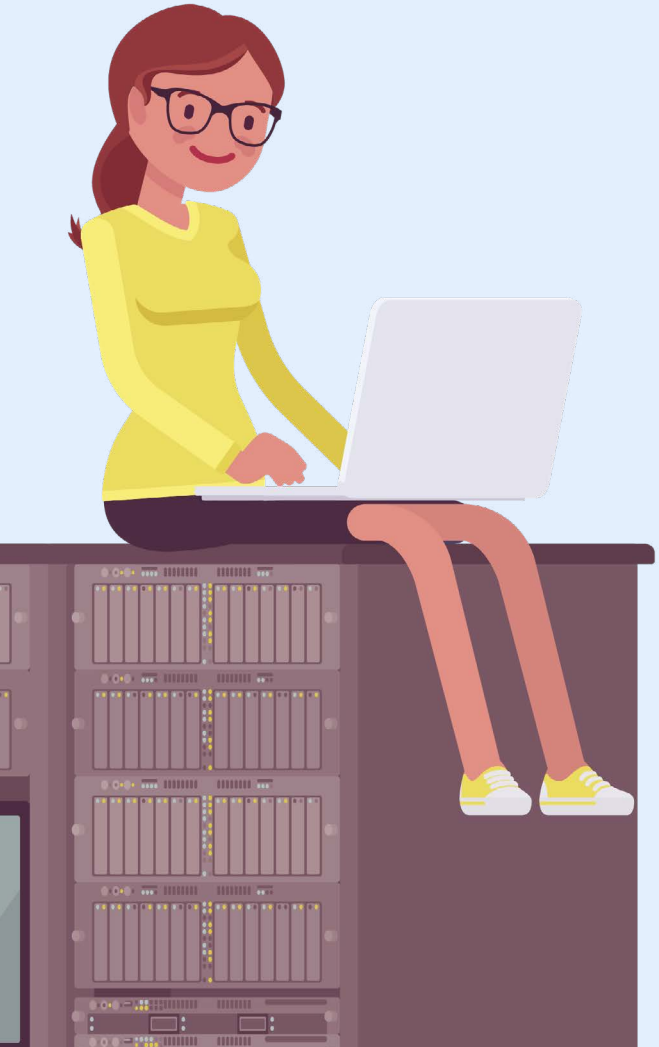
Een netwerkmonitoring oplossing, dient al het ingaande en uitgaande netwerkverkeer te analyseren. Dit om verdacht verkeer, afwijkend verkeer en ongewenst verkeer te spotten en hierop een alarm af te geven. Denk hierbij ook aan zogenaamde shadow IT. Bij het continue monitoren van het netwerkverkeer ligt de focus op het detecteren van potentieel kwaadaardige activiteiten en het zogenaamde Command & Controle verkeer.

Door de toename van SaaS-applicaties en het gebruik van de moderne werkplek op diverse locaties is het bedrijfsnetwerk niet altijd de plaats waar alles data door heen gaat en daarmee de functie van netwerkmonitoring niet altijd meer voldoende. Inzet van een DNS securityoplossing biedt inzicht aan netwerk verkeer buiten de locaties van uw bedrijfsnetwerk. Afhankelijk van de situatie kan DNS security als aanvulling op netwerkmonitoring een goed inzicht geven.

Netwerksegmentatie

Vanuit security oogpunt is het verstandig om uw netwerk in verschillende segmenten in te delen. We noemen dit segmenteren. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen zal beperken.





Netwerksegmentatie helpt om het netwerkverkeersvolume beter te kunnen regelen. Het belangrijkste voordeel van netwerksegmentatie is helpt om gevoelige gegevens te scheiden van ander verkeer. Dit maakt het voor hackers moeilijker om bij gevoelige informatie te komen. Het helpt ook voorkomen dat kwaadaardige software zich naar andere delen van het netwerk verspreidt. Een ander voordeel van netwerksegmentatie is dat het kan helpen de schade te beperken die een hacker kan aanrichten als deze erin slaagt in het netwerk binnen te dringen. Door gevoelige gegevens te scheiden van ander verkeer, maken we het moeilijk om informatie te stelen of te beschadigen. Tenslotte kan netwerksegmentatie ook helpen om het beveiligingsbewustzijn te verbeteren.

Hanteer het uitgangspunt dat netwerkverkeer in het algemeen niet toegestaan is en voeg vervolgens specifieke firewallregels toe voor verkeer dat wel nodig is. Als u netwerkverkeer al te rigoureus blokkeert, kan dat zorgen voor verstoringen in de bedrijfsvoering. Dit kunt u voorkomen door eerst het netwerkverkeer te monitoren om te bepalen welke informatiestromen nodig zijn, en daarna pas netwerkverkeer te blokkeren.

Ransomware-resistente-backup

Een ransomware-resistente-backup (immutable backup) is een backup die niet bereikbaar is vanaf het eigen netwerk. Ook niet voor admin accounts met de hoogste accountrechten. Een dergelijke opzet is met een moderne backup oplossingen of serviceprovider op te zetten. Mocht een hacker ondanks alle voorzorgsmaatregelen toch domain-admin rechten in handen krijgen en de organisatie plat te leggen, door alle data te versleutelen, is dit uw offline verzekeringspolis.

Zorg er wel voor dat een degelijke backup getest is door in een aparte omgeving een restoretest uit te voeren. Laat deze test regelmatig uitvoeren en zorg voor een werkend draaiboek om in een voorkomend geval deze bijzondere restore uit te kunnen voeren.

Beperk toegang tot netwerkpoorten en netwerkprotocollen

Sluit alle netwerkpoorten en netwerkprotocollen af die niet werkelijk nodig zijn voor de bedrijfsvoering. Alle poorten en protocollen die overbodig open staan vergroten onnodig de aanvalsoppervlakte en maken u kwetsbaar.

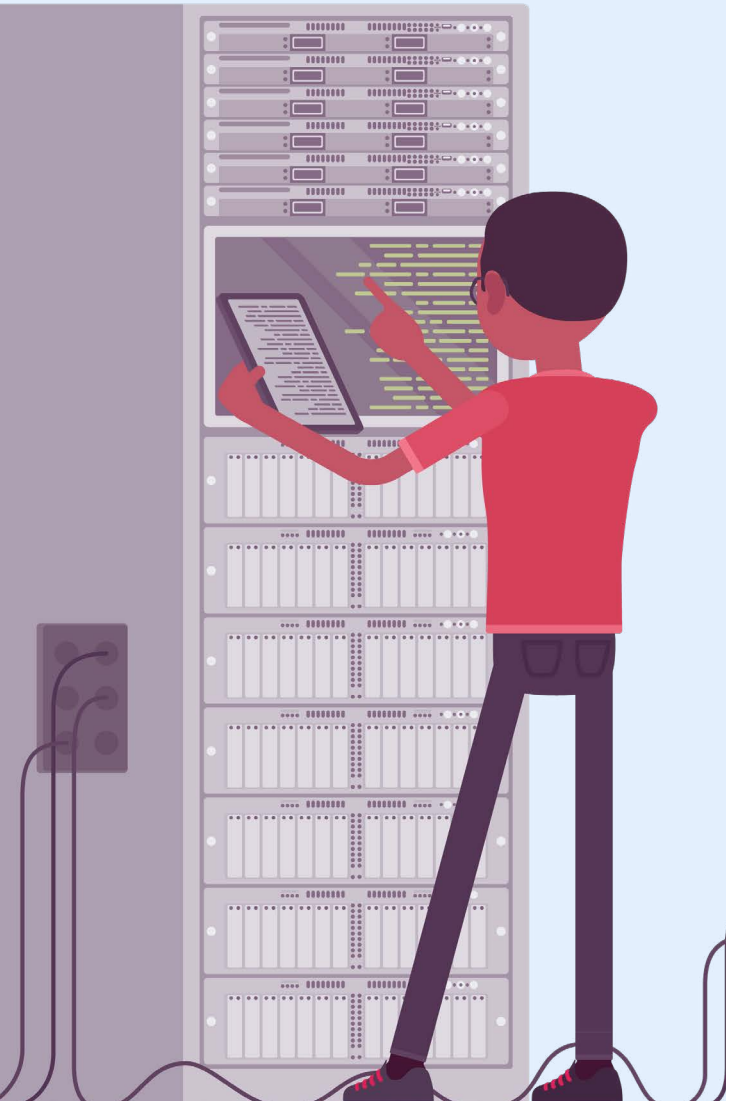
De basis regel is netwerkpoorten en protocollen staan dicht tenzij. In de praktijk zien wij vaak het omgekeerde, het staat open tenzij. Wij kunnen uw organisatie helpen om inzicht te krijgen en om stapsgewijs naar een veilige opzet toe te werken.

Het is belangrijk dat er alleen apparaten op het bedrijfsnetwerk worden toegelaten die je vertrouwt. Blokkeer de uitgifte van IP-adressen binnen het bekabelde of het draadloze netwerk aan devices die onbekend zijn voor de organisatie.

Privileged Access Management (PAM)

Organisaties hebben inzicht nodig op de administrator activiteiten die de ICT-omgeving worden uitgevoerd. Zowel van de activiteiten die door de eigen beheerder, maar ook door service engineers van partners en leveranciers worden uitgevoerd.

Privileged Access Management is een oplossing voor het monitoren van de administrators, de beheerders en alle andere privileged accounts, zodat alle activiteiten van privileged accounts worden vastgelegd. Gezond beheer verstand vertelt ons: gebruik geen Domein administrator accounts voor reguliere beheer werkzaamheden. Probeer zo veel mogelijk het principe van “least privilege” toe te passen.



Dit betreft ook een beetje de vraag: Wie bewaakt de bewakers? Met Privileged Access Management (PAM) krijgt u grip, zicht en controle over alle hoge risico-rechten in uw organisatie. Het merendeel van deze rechten zijn beheerrechten in applicaties en systemen. Zodra een hacker binnen is in uw organisatie zal hij/zij op zoek gaan naar privileged accounts. Een goede PAM oplossing zal dit moeilijker maken en bovendien inzichtelijk maken als er zich onverwachte wijzigingen voor doen. Wat een reden zou kunnen zijn voor verder onderzoek. Een goede PAM oplossing moet ook gelijk alle rechten van beheerders blokkeren en stoppen als mensen van functie wijzigen of de organisatie verlaten.

AD-monitoring

De Active Directory (AD) omgeving of Entra ID zoals de Azure variant heet is de plek in de ICT-infrastructuur waar alle gebruikers en rechten en privileges zijn geadministreerd en worden bijgehouden. Voor hackers de doos van Pandora. De plek waar ze graag toegang tot willen krijgen om totale controle over een ICT omgeving te krijgen.

Met monitoring van de AD-omgeving ontdekt u de zwakke plekken binnen uw bestaande Active Directory domeinen. Geconstateerde zwakke plekken worden opgelost op basis van prioritering.

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

Als uw organisatie de ICT-beveiliging naar een hoger niveau wil brengen is een SIEM oplossing een aan te bevelen overweging. Een SIEM oplossing brengt alle logbestanden, alle informatiebronnen over het gebruik en gedrag van de ICT-middelen en de gedragingen van de gebruikers van een organisatie bij elkaar. Hierbij wordt informatie uit de AD-omgeving gebruikt om deze gegevens leesbaar en traceerbaar te maken. Op deze manier is het mogelijk door automatische correlatie van deze bestanden verdacht of gevaarlijke situatie eerder op te sporen, of bedreigingen te vinden die anders onder de radar waren gebleven.

De moderne SIEM oplossingen kijken ook naar het gedrag van de gebruikers en de ICT-middelen. Als er een afwijkend patroon of ongewone correlaties naar boven komt, volgt er een alarm en wordt de betreffende situatie door Cyber Security-specialisten geanalyseerd.

Met een SIEM is het mogelijk om potentiële problemen en risico's in de kiem te smoren. Ook kan SIEM worden gebruikt om een analyse uit te voeren nadat een securityincident heeft plaatsgevonden. Een goede SIEM oplossing moet ook terug in de tijd kunnen kijken. Een SIEM oplossing is alleen zinvol als er binnen de organisatie een goed fundament is van basis security-oplossingen die de SIEM oplossing met relevante data kunnen voeden.

Een Security Operation Center (SOC) is een afdeling met cyber security analisten welke zich continu bezighouden met beoordeling en adviezen rondom cyber security incidenten. Een SIEM oplossing is een deel van hun dagelijks gereedschap om toezicht te houden op de ICT-omgeving. Gelet op de krapte op de arbeidsmarkt en de beperkte budgetten is het uitbesteden van de SOC-functie voor de zorgsector een logische keuze.

Geofencing

Geofencing is een techniek waarbij al het netwerkverkeer van en naar een regio geblokkeerd wordt. Wij stellen gezamenlijk vast welke landen we blokkeren.

Op firewall niveau wordt het verkeer geblokkeerd. Geofencing blokkeert ongewenst verkeer op basis van de regio waar het vandaan komt. Het helpt onder meer tegen massale Denial-of-Service (DoS) of bot-aanvallen. Deze komen vaak uit landen buiten Nederland en kunnen ervoor zorgen dat uw netwerk offline gaat. Simpelweg omdat het systeem niet alle aanvragen kan bijhouden. Geofencing is een oplossing die veel ongewenst verkeer (niet alles) tegenhoudt.

CASB/SASE

Door de toename van het aantal SaaS-applicaties en tegelijkertijd de reductie van het aantal lokale applicaties verandert ook de rol van het datacenter of de gebruikte Cloud omgeving. De moderne werkplek kan gebruik maken van de SaaS-applicatie waarbij de rol van het datacenter/Cloud omgeving beperkt is tot het aanmelden en opstarten van applicaties. Deze nieuwe werkwijze vraag ook een andere netwerk security. De rol van de firewall in de cloud of het datacenter wordt hierdoor beperkt en dat brengt nieuwe security bedreigingen met zich mee. Inzet van moderne technieken als Cloud Access Security Broker (CASB) en Secure Access Service Edge (SASE) geven gecontroleerde en veilige toegang tot de SaaS-applicaties. Deze technieken vormen de opstart naar een zero trust securitymodel. .

Incident Response plan

Wat gaat u doen als het ondanks alle voorzorgsmaatregelen toch fout gaat? Voor dat geval moet een goed doordacht plan worden gemaakt. Dit plan moet niet op een PC staan. De PC doet het mogelijk niet op het moment dat u het werkelijk nodig heeft. Wij adviseren om uw organisatie hierop voor te bereiden en een crisisteam samen te stellen. Als u erover gaat nadenken als het nodig is, bent u echt te laat.

Gedurende een crisissituatie zijn er veel acties die uitgevoerd moeten worden. Hiervoor zijn resources nodig die beschikbaar moeten zijn. Een incident responseplan helpt bij het plannen van deze benodigdheden. Een incident responseplan zorgt ervoor dat er sneller op incidenten gereageerd wordt en dat de effectiviteit van incident respons wordt verhoogd. Een doordacht plan bevat de allocatie van menselijke resources, de definitie van de crisisorganisatie, de processen en bovenal een goed doordacht communicatieplan.

Bedenk dat u in geval van een werkelijke ramp geen beschikking meer heeft over uw gebruikelijke ICT-middelen.
De email doet het niet meer. De intranetpagina's zijn offline. Het interne netwerk is uit de lucht. Mogelijk is ook het telefoonsystemen getroffen. Hoe gaat u dan de regie voeren, op welke manier gaat u communiceren met de mensen die betrokken zijn bij het oplossen van het security incident. Hoe gaat u met uw medewerkers communiceren? Hoe bereikt u uw cliënten? Wie staat de pers te woord? Kortom het geheim van snel en met minimale schade herstellen van een Cyber

Security incident staat of valt met en goede voorbereiding en het opzetten van een goed doordacht Incident Responseplan.

Onderdeel van de goede voorbereiding is ook een plan om specialisten te kunnen inzetten tijdens cyber security incident. Externe partijen welke ervaringen hebben kunnen op afroep beschikbaar zijn om te helpen of zelfs de regie te nemen. Deze ervaring gaat over diverse gebieden zoals forensisch onderzoek maar ook mogelijk onderhandeling/communicatie met cyber criminelen. Door vooraf een overeenkomst met specialisten aan te gaan is er directe lijn beschikbaar voor hulp troepen tijdens de calamiteit.

Data-governance

Organisaties zijn afhankelijk van data, van financiële data tot contactgegevens. Vandaag de dag creëren, verzamelen en wisselen organisaties enorme hoeveelheden data uit.

De data kan worden geclassificeerd van lage waarde tot zeer gevoelig, kritisch of gereguleerd. Zoals de persoonlijke informatie van werknemers, klanten, gezondheidsdossiers van patiënten/cliënten en intellectuele eigendomsgegevens.

Het beschermen van data wordt steeds belangrijker, maar wordt ook steeds moeilijker. Wat staat waar, wat zit er in de Cloud, en waar staat dat dan? Wat delen we met wie? Kortom hoe krijgt u en hoe behoudt u goed overzicht.

Snelle detectie van datalekken helpt de impact ervan te verminderen. Wanneer een potentieel datalek wordt gedetecteerd, moet de organisatie in staat zijn om snel te onderzoeken en te reageren. Het hebben van de juiste tools en een gedocumenteerd responsplan helpt deze inspanningen te stroomlijnen.

Met oplossingen op het gebied van automatische data classificatie, security monitoring en audit & compliance (waaronder AVG en NEN7510) brengen we de data-governance op orde.

Uw Ideale ZorgSecurity - Aanpak

Samen met u gaan wij stap voor stap naar een veiligere ICT-voorziening voor uw zorginstelling.

Met onze kennis over - en ervaring met security vraagstukken bij onze zorgklanten, adviseren en ondersteunen wij u graag. Samen bepalen we de voor u best passende security maatregelen. 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. Hierbij nemen we uw zorgen uit handen en verzorgen de regie over het traject: van ontwerp tot inrichting, beheer en doorontwikkeling. Uiteraard vergeten wij uw medewerkers niet en besteden veel aandacht aan de adoptie voor een soepele overgang naar een veiligere omgeving. Met minimale impact en belasting voor uw organisatie en medewerkers. Ook bij potentiële dreigingen en verstoringen staan wij voor u klaar en lossen dit met u op.

Vanaf het begin van onze samenwerking is onze security architect betrokken bij Uw Ideale ZorgSecurity. Deze kent uw omgeving door en door en beoordeeld nieuwe innovaties uit de markt en wensen vanuit uw organisatie op toepasbaarheid en uitvoerbaarheid. Deze bespreken wij regelmatig met u om Cyber Security up-to-date en veilig te houden.

Zo borgen wij samen Uw Ideale ZorgSecurity!

NEEM CONTACT OP

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

SLTN
Future Proof IT