Deloitte.

Handreiking informatiebeveiliging

Jeugdinstellingen

Aanbevelingen voor veiligere IT in de jeugdzorg

Kenmerk: HB/dd/20-1875a

Dit document is verstrekt aan het Ministerie van Volksgezondheid, Welzijn en Sport (hierna: Ministerie van VWS) door Deloitte Risk Advisory B.V. (hierna: Deloitte). Op dit document zijn onze voorwaarden van toepassing, zoals beschreven in ons voorstel met referentie HB/dd/20-1363, opgemaakt op donderdag 17 september 2020.

Deze rapportage is enkel bedoeld voor de in de offerte opgenomen doelstelling. Het maken van aanpassingen of verspreiding naar derden is slechts toegestaan na voorafgaande schriftelijke toestemming van Deloitte. Dit rapport bevat geen conclusies of een andere vorm van zekerheid over de financiële huishouding, interne beheersingsmaatregelen of het voldoen aan wet- en regelgeving.

Uitgebracht aan:

Ministerie van Volksgezondheid, Welzijn en Sport
Parnassusplein 5
2511 VX Den Haag
Postbus 20350
2500 EJ Den Haag
Nederland

Uitgebracht door:

Deloitte Risk Advisory B.V.
Gustav Mahlerlaan 2970
1081 LA Amsterdam
Postbus 58110
1040 HC Amsterdam
Nederland
Tel: 088 288 2888
Fax: 088 288 9711
www.deloitte.nl

Inhoudsopgave

Digitale weerbaarheid jeugdzorg: op weg naar veiligere IT

Inleiding

Voor u ligt de Handreiking Informatiebeveiliging Jeugdinstellingen - vol praktische tips, aandachtspunten en handvatten waarmee u de cyberweerbaarheid van uw jeugdzorgorganisatie kunt vergroten.

In deze handreiking komen specifieke aandachtspunten voor jeugdinstellingen op het gebied van informatiebeveiliging aan bod. Daarnaast worden leading practices rondom de digitale beveiliging van de systemen, applicaties en data gedeeld.

Betrokken partijen

De handreiking is opgesteld door Deloitte Risk Advisory B.V. (hierna 'Deloitte') op verzoek van Ministerie van Volksgezondheid, Welzijn en Sport (hierna Ministerie van VWS) en is mede tot stand gekomen na interviews met een aantal jeugdzorg instellingen en Jeugdzorg Nederland. Daarnaast is er kennis opgedaan via diverse pentesten welke eind 2019 zijn uitgevoerd door Deloitte op de interne en externe IT-infrastructuur van een zestal jeugdzorginstellingen. Dit gaf inzicht in relevante aandachtspunten en de meest voorkomende technische risico's en kwetsbaarheden binnen de IT-infrastructuur van deze jeugdinstellingen. Waardevolle informatie waar andere jeugdzorginstellingen ook van kunnen profiteren.

Met name IT-managers binnen de jeugdzorg staan, gezien hun doorgaans kleine IT-organisatie en beperkte capaciteit, kennis en budget vaak voor uitdagingen waar het de beveiliging van hun systemen betreft. Met deze handreiking stelt het Ministerie van VWS in samenwerking met Jeugdzorg Nederland informatie beschikbaar voor deze instellingen en andere geïnteresseerden, welke als startpunt kan dienen voor activiteiten die erop gericht zijn om de staat van informatiebeveiliging binnen uw organisatie te verbeteren.

Deloitte

De wereld verandert radicaal door de exponentiële groei van nieuwe technologieën. Deloitte's security en privacy experts volgen de ontwikkelingen op het gebied van informatiebeveiliging op de voet en vertalen kansen naar oplossingen om de mogelijkheden die de digitale wereld biedt optimaal te benutten. Deloitte heeft deze handreiking opgesteld op basis van de eerdere bevindingen uit de pentesten (eind 2019) en diverse interviews met jeugdzorginstellingen en Jeugdzorg Nederland.

Ministerie van Volksgezondheid, Welzijn en Sport

Het Ministerie van Volksgezondheid, Welzijn en Sport wil dat mensen erop kunnen vertrouwen dat de zorg goed, betaalbaar en beschikbaar is en blijft. Nederland gezond en wel. Dat is het motto van het ministerie van VWS. Veilige zorg voor ouderen en jongeren en voor mensen met een lichamelijke of verstandelijke handicap. Ongeveer 5000 ambtenaren maken het overheidsbeleid op het terrein van de gezondheidszorg, de maatschappelijke zorg en sport. Het ministerie van VWS heeft Deloitte opdracht gegeven om deze handreiking op te stellen.

"Goede informatiebeveiliging is van groot belang voor de kwaliteit en continuïteit van de jeugdzorg. Deze handreiking helpt de sector de juiste stappen te zetten."

Robert van Someren
Directeur ICT/IV, Jeugdzorg Nederland

Jeugdzorg Nederland

Jeugdzorg Nederland is de branche-vereniging voor organisaties die jeugdhulp, jeugdbescherming en/of jeugdreclassering bieden. Jeugdzorg Nederland behartigt de belangen van haar leden, treedt op als werkgevers-organisatie in de cao-onderhandelingen en draagt bij aan professionalisering van de zorg voor jeugd. Ze biedt zelf geen zorg voor jeugd, maar ondersteunt de aangesloten organisaties zodat die optimaal hun werk kunnen doen. Jeugdzorg Nederland heeft een aantal onderwerpen ingebracht en ondersteuning geleverd bij het leggen van de contacten met de jeugdinstellingen.

Leeshulp

Deze handreiking bestaat uit twee delen:

1. **P. 7 |** een **snelstartgids**: een beknopt overzicht van mogelijk te nemen maatregelen evenals een korte beschrijving per onderwerp.

2. **P. 16 |** de **deep dive**: achterliggende hoofdstukken waarin meer (achtergrond)informatie over diverse onderwerpen uit de snelstartgids te vinden is.

Let wel: de handreiking informatiebeveiliging jeugdzorginstellingen is geen uitputtende lijst van maatregelen, maar is bedoeld als startpunt voor het verbeteren van de informatiebeveiliging binnen uw organisatie.

Snelstartgids

Snelstartgids

De zorg digitaliseert in rap tempo. Naast het bieden van goede en veilige jeugdzorg, spelen ICT en informatiebeveiliging een steeds belangrijkere rol in het veilig zorgen voor kwetsbare jeugdigen. Dit hoofdstuk geeft concrete tips voor beveiligingsmaatregelen in veelvoorkomende probleemgebieden.

Cybersecurity in de jeugdzorg

ICT en digitale oplossingen spelen vandaag de dag een belangrijke rol in de maatschappij en zijn niet meer weg te denken. De rol en afhankelijkheid van ICT is hierdoor de laatste jaren enorm groot geworden, zo ook in de jeugdzorg. Voor een sector die over uiterst privacygevoelige informatie van tienduizenden gezinnen en jeugdigen beschikt is goede informatiebeveiliging cruciaal.

Elk jaar stijgt het aantal datalekken en cyberdreigingen blijven zich in een snel tempo ontwikkelen. Uit de eerdere penetratietesten en nadere analyse van de resultaten is gebleken dat, naast de technische bevindingen, er niet altijd voldoende zicht is op IT-risico's. Daarnaast zijn IT-beheer- en ontwikkelprocessen op een aantal vlakken onvoldoende geborgd binnen de jeugdzorgorganisaties. Jeugdinstellingen werken op dagelijkse basis met (bijzondere) persoonsgegevens van jongeren en zorgdossiers. Daarnaast is de beschikbaarheid van data en systemen van belang om adequate zorg te kunnen leveren en moeten instellingen veilig en betrouwbaar gegevens uit kunnen wisselen met gemeenten, de kinderbescherming et cetera. Voor een kwaadwillende is de (jeugd)zorg aantrekkelijk aangezien er veel (medische) gegevens verzameld worden en verstoring van dagelijkse processen al snel media-aandacht oproept. Cybersecurity is gericht op het beschermen van computers, servers, mobiele apparaten, elektronische systemen, netwerken en gegevens tegen schadelijke aanvallen. Het op orde hebben van de IT-beveiliging is dus een must.

"Medische patiëntgegevens zijn voor cybercriminelen meer waard dan creditcardgegevens. Voor een patiëntendossier wordt maximaal $ 250 per record gerekend, vergeleken met $ 5,40 voor een creditcard"

Born: Trustwave, *"2019 Trustwave Global Security Report", 5 februari 2020.*

1. Cyber Awareness

Iedereen binnen jeugdzorg instellingen heeft dagelijks te maken met (cyber)-security. Denk aan het werken met gevoelige persoonsgegevens en medische patiëntendossiers. Sommige acties, zoals inloggen op een openbaar wifinetwerk en het per ongeluk openen van links uit een phishing e-mail, kunnen gemakkelijk grote impact hebben op de levens van (minderjarige) jeugdigen als mede de reputatie van de (jeugd)zorg.

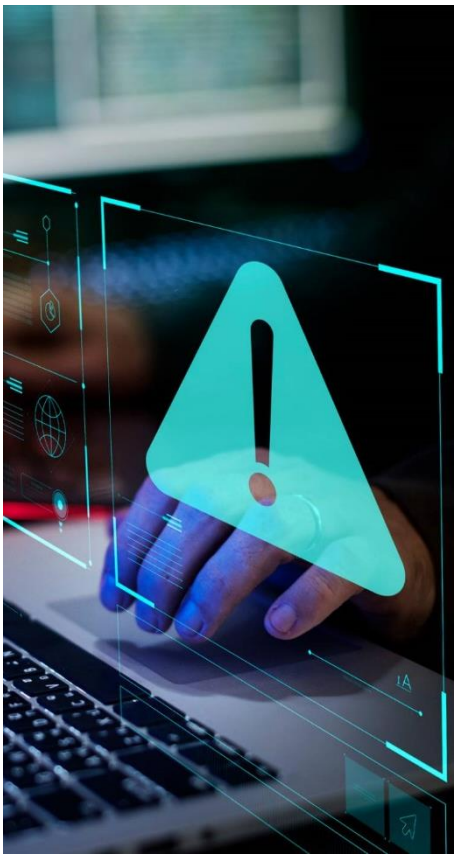
Aanvallers maken vaak misbruik van onoplettendheid, onwetendheid en vertrouwen van medewerkers om binnen te kunnen dringen in het IT-netwerk van een organisatie. En hoewel iedereen wel een keer in een goede phishing mail kan trappen, kan veel ellende worden voorkomen door medewerkers meer bekend te maken met dit soort aanvallen.

Daarom is bewustzijn creëren van de cyberrisico's bij alle medewerkers een belangrijke stap om te voorkomen dat aanvallers digitaal binnendringen in het netwerk van de jeugdinstelling.

Een aantal maatregelen op het gebied van cyber awareness die een organisatie kan nemen zijn:

- Een cyber awareness campagne welke periodiek, bijvoorbeeld jaarlijks, wordt herhaald om medewerkers bewust te maken van relevante cyber risico's en hoe ze met die risico`s moeten omgaan.
- Een phishing test welke periodiek herhaald wordt om medewerkers te trainen in het herkennen van en acteren op phishing e-mails. Resultaten worden hierbij gemonitord worden zodat men ervan kan leren.
- Veilig omgaan met gegevens en systemen als standaard onderdeel van de on-boarding van nieuwe medewerkers en periodieke trainingscurricula.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk '1. Cyber Awareness' op pagina 17-18 van de deep dive.



Cyber awareness is erop gericht om effectief bewustzijn te creëren van IT-risico's binnen de gehele organisatie.

Casus: Universiteit van Maastricht

Op 23 oktober 2019 werd de Universiteit van Maastricht geraakt door een ransomware aanval, waardoor systemen van de universiteit en/of gegevens die erop staan versleuteld en dus ontoegankelijk werden. De aanvallers hadden hiervoor slechts 50 minuten nodig. Uiteindelijk betaalde de universiteit de aanvallers € 197.000 om te toegang tot de systemen terug te krijgen.

Dit alles begon op 15 oktober met een **phishing email** waarop een medewerker klikte waarna de criminelen toegang hadden tot het interne netwerk van de universiteit. Vanaf die ene laptop verkregen de criminelen toegang tot overige systemen van de universiteit.

2. Veilig data delen

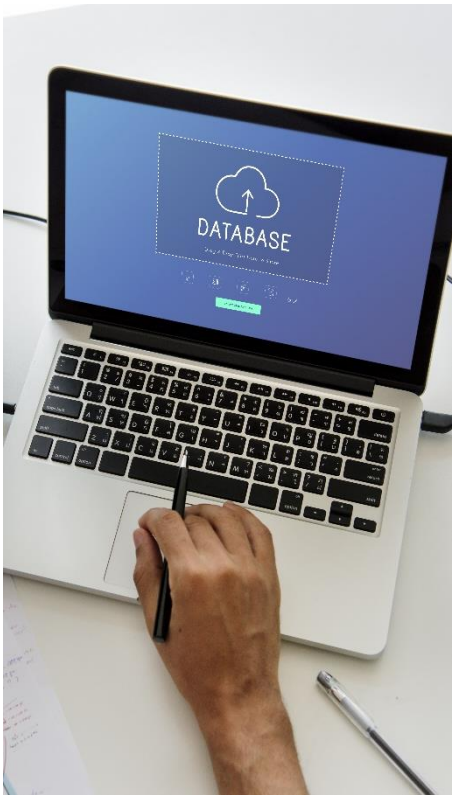
Medewerkers hebben dagelijks toegang tot data die vertrouwelijk moet blijven. Een van de grootste beveiligingsrisico's waar organisaties tegenwoordig mee te maken hebben is het feit dat medewerkers niet goed weten hoe ze met bepaalde data moeten omgaan. Daardoor wordt gevoelige informatie op een onveilige manier gedeeld en kan het bij kwaadwillende personen terecht komen. Daarom is het belangrijk dat medewerkers kennis wordt bijgebracht over hoe ze data veilig kunnen delen. Daarnaast moeten ze ook over middelen beschikken om dat op een juiste manier kunnen doen.

De middelen moeten gebruiksvriendelijk zijn zodat medewerkers het gebruik ervan niet als obstakel ervaren. Als dit wel het geval is zijn mensen eerder geneigd om alternatieven te zoeken.

Een aantal maatregelen op het gebied van data delen die een organisatie hiervoor kan nemen zijn:

- Stel een beleidsdocument op voor het delen van data en maak dit kenbaar binnen de organisatie (bijvoorbeeld via een cyber bewustzijn campagne, zie vorige pagina) zodat iedereen op de hoogte is van de vertrouwelijkheid van data en hoe je data op elk classificatie-niveau veilig mag en kan delen.
- Train medewerkers in manieren om veilig met data om te gaan en deze te delen**.** Medewerkers moeten de gevoeligheden van verschillende soorten informatie begrijpen en de risico's die verbonden zijn aan het verkeerd omgaan met gevoelige gegevens. Laat ze daarbij ook zien welke veilige mogelijkheden er in de organisatie al zijn om gegevens op te slaan en te delen. Ook hierbij kan een bewustwording campagne helpen (zie vorige pagina).
- Stel beleid op rondom het gebruik van USB-sticks en dwing dit af (bijvoorbeeld door data standaard te versleutelen of het gebruik van USB-sticks onmogelijk te maken).
- Stel een veilige data uitwisselingsplatform beschikbaar als medewerkers regelmatig data moeten uitwisselen met andere partijen zodat data te allen tijde veilig en gemakkelijk gedeeld kan worden.
- Voorkom het gebruik van niet-geautoriseerde apparaten (bijvoorbeeld USB-sticks) zodat alleen apparaten die als vertrouwd zijn gedefinieerd, verbinding kunnen maken met een bedrijfscomputer.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk '2. Veilig data delen' op pagina 18-19 van de deep dive.



Veilig omgaan met (privacy) gevoelige data van jeugdigen is cruciaal.

Casus: datalek drie ziekenhuizen

In 2016 werd er gemeld dat er door een 'ernstige fout' de gegevens van patiënten van het St. Anna Ziekenhuis in Geldrop, het Canisius-Wilhelmina Ziekenhuis in Nijmegen en een Belgisch ziekenhuis op straat zijn komen te liggen.

De informatie - het patiëntnummer, geslacht, de naam, geboortedatum en de locatie van in totaal 158.000 Nederlandse en Belgische patiënten - waren via een openbare en onbeveiligde internetlink in te zien. Dit was het resultaat van een verkeerde configuratie.

De link werd gebruikt voor uitwisseling van medische informatie tussen de ziekenhuizen.

3. Sterk wachtwoordbeleid & multi-factor authenticatie (MFA)

Medewerkers gebruiken vaak onveilige wachtwoorden die makkelijk (geautomatiseerd) te raden zijn. Aanvallers zetten daarvoor vaak snelle computers in die in razend tempo duizenden wachtwoorden per minuut kunnen uitproberen. Met zwakke wachtwoorden kunnen onbevoegden toegang krijgen tot interne systemen en bijvoorbeeld informatie stelen of zich voordoen als een medewerker.
Om te voorkomen dat medewerkers makkelijk te raden wachtwoorden gebruiken is het van belang dat een wachtwoordbeleid wordt opgesteld en afgedwongen binnen de organisatie. Een goed wachtwoordbeleid moedigt medewerkers aan betrouwbare en veilige wachtwoorden te maken en deze vervolgens op de juiste manier op te slaan en te gebruiken.

Een aantal maatregelen op het gebied van wachtwoorden die een organisatie kan nemen zijn:

- Stel een minimum van 8 tekens voor de wachtwoordlengte. Lange wachtwoorden zijn over het algemeen moeilijker te kraken.
- Screen nieuwe wachtwoorden tegen een lijst met bekende gecompromitteerde wachtwoorden. Beperk het aantal mislukte verificatiepogingen.
- Maak gebruik van passende tooling welke medewerkers helpt aan om voor elke applicatie een uniek wachtwoord te gebruiken. Het gebruik van Single Sign On (SSO) is een andere optie.

Een aantal maatregelen op het gebied van MFA die een organisatie kan nemen zijn:

- Creëer een extra verdedigingslinie door multi-factor authenticatie in te stellen voor alle gebruikers. Dit is vooral relevant voor apparaten die benaderbaar zijn vanaf het internet.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk ‘3.1 Het belang van een sterk wachtwoordbeleid’ op pagina 17-18 en ‘3.2 multi-factor authenticatie (MFA)’ op pagina 20-21 van de deep dive.

Maak gebruik van sterke wachtwoorden en multi-facotr authenticatie voor kritische systemen, applicaties en apparaten.

Casus: wachtwoord Trump gehackt

De Nederlandse ethische hacker Victor Gevers heeft naar eigen zeggen het Twitter-account van Donald Trump gehackt. Het wachtwoord was eenvoudig te raden, zei Gevers. De president gebruikte volgens hem het wachtwoord ‘maga2020!’.

Maga is een afkorting van Make America Great Again, zijn campagneslogan uit 2016. Verder waren er geen andere beveiligingsmaatregelen zoals tweestapsverificatie actief. Gevers deed een rondje langs de accounts van verschillende politici om te kijken of die nog veilig waren. Hij probeerde een handjevol wachtwoorden en kwam toen bij maga2020! terecht. Dat bleek te werken, luidt de claim.

4. Accountbeheer: Identity & Access Management

Bij organisaties die veel gevoelige data beheren en verwerken is het belangrijk om een overzicht te hebben van wie toegang heeft tot welke systemen en (vertrouwelijke) data. Daarnaast wil je voor de meeste gevoelige data en systemen zoveel mogelijk informatie vastleggen welke account wanneer toegang heeft gehad. Identity & Access Management (IAM) en Privileged Access Management (PAM) zijn erop gericht om account beheer in goede banen te leiden. Wanneer een organisatie accountbeheer goed op orde heeft, wordt voorkomen dat er gebruikers zijn die informatie kunnen zien die niet voor hun bestemd is.

Daarnaast zorgt het ervoor dat IT een duidelijk beeld heeft van de accounts/rollen en bijbehorende rechten evenals wanneer er gebruik wordt gemaakt van deze rechten.

Een aantal maatregelen op het gebied van IAM/PAM die een organisatie kan nemen zijn:

- Loggen van acties van accounts. Hiermee is IT altijd in staat om te traceren wie toegang heeft (gehad) tot systemen en/of data en wanneer gebruik wordt gemaakt van toegangsrechten. In een later stadium is het mogelijk om de logs actief te (centraal) gaan monitoren.
- Tijdig melden van functiewisselingen en (in)uitdiensttreding van medewerkers aan IT. Hiermee zorg je ervoor dat je altijd tijdig de juiste rollen en toegang aan de juiste medewerkers kan toewijzen.
- Controleer regelmatig de rollen van je medewerkers ten opzichte van de taken die ze uitvoeren. Om ervoor te zorgen dat medewerkers te allen tijde de juiste rol toegewezen krijgen is het van belang om goed in de gaten te houden welke taken ze uitvoeren en wat voor rol bij de taak past.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk ‘4. Accountbeheer’ op pagina 22 van de deep dive.

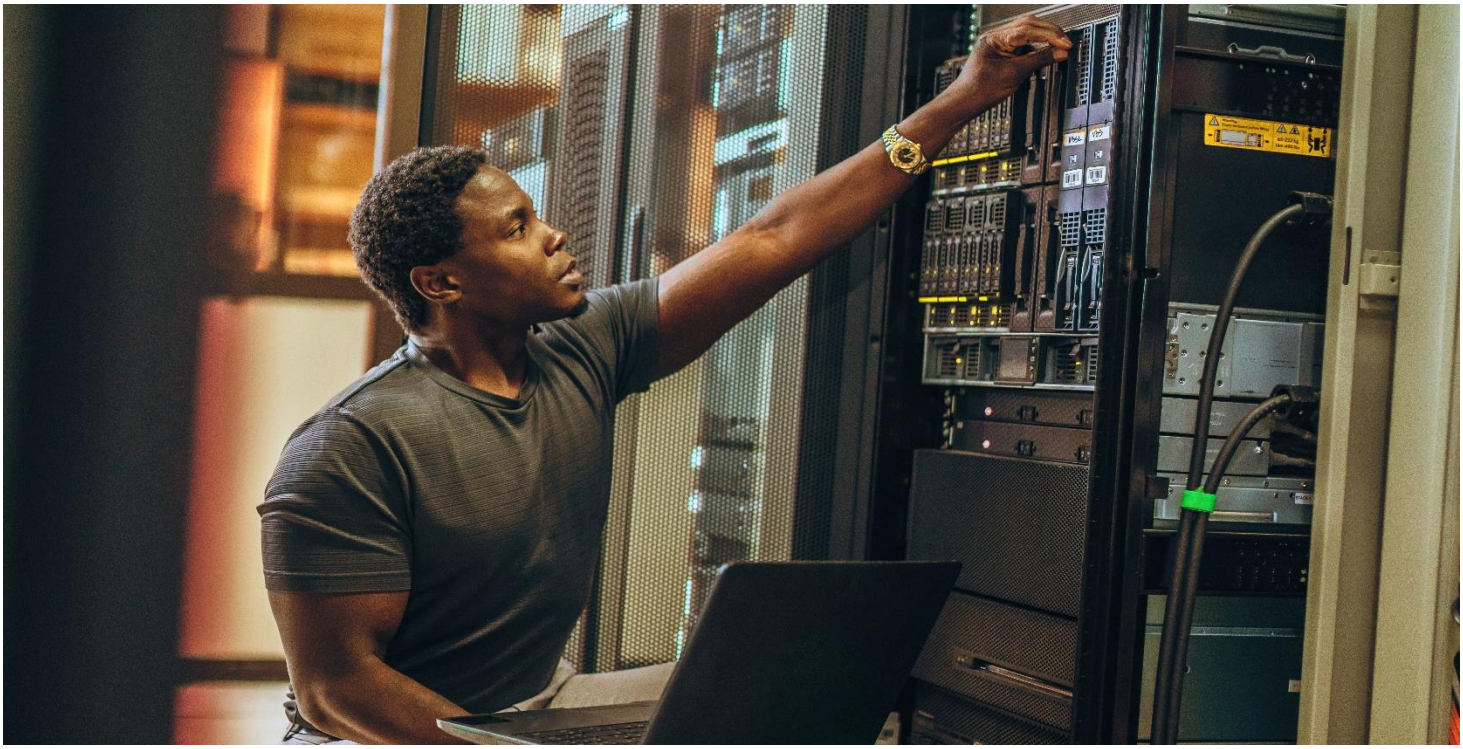
5. Patching

Patchen is gericht op het tijdig updaten van systemen en applicaties en zorgt er niet alleen voor dat systemen en applicaties soepel blijven werken, het is ook noodzakelijk om de organisatie veilig te houden. Door systemen niet te patchen, zijn ze kwetsbaar voor cyberaanvallen. Volgens het Ponemon instituut kunnen de meeste datalekken (57%) zelfs direct worden toegeschreven aan aanvallers, die misbruik maken van een bekende kwetsbaarheid die niet was gepatcht[1]. Wanneer patches voor het publiek worden vrijgegeven, wordt de kwetsbaarheid er vaak mee onthuld. Aanvallers gaan meteen mee aan de slag zodat organisaties weinig tijd hebben om hun kwetsbaarheden tijdig te patchen. Hierdoor is het van belang om een solide patchproces te hebben. Hoe sneller de juiste patch op de juiste applicatie wordt toegepast hoe veiliger je systemen worden.

Een aantal maatregelen op het gebied van patching die een organisatie kan nemen zijn:

- Inventariseer al je hardware. Je kunt pas weten wat je moet patchen als je duidelijk inzicht en overzicht hebt van de computers, servers en netwerkapparatuur die je gebruikt.
- Inventariseer al je software. Net zoals bij hardware geldt dat je een duidelijk beeld nodig hebt van welke besturingssystemen, server applicaties en desktopapplicaties je bezit en welke versies het betreft zodat je die regelmatig kan updaten.
- Leg een patch proces vast met vaste patch momenten. Kies een wekelijks of maandelijks moment waarbij je al je systemen patched. Zorg dat dit wordt vastgelegd in een proces, bijvoorbeeld UPMS (Update Patch Management System), zodat het patchen niet vergeten wordt en altijd duidelijk is wat wanneer gepatched is en door wie.
- Zorg voor duidelijke afspraken (SLA's) met leveranciers waar je mee samen werkt aangezien je afhankelijk bent van geïmplementeerde patches door derden.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk '5. Patching' op pagina 23 van de deep dive.



[1] Bron: Separating the Truths from the Myths in Cybersecurity, Ponemon Institute LLC, June 2018.

6. Derde partijen

Vrijwel alle jeugdzorg instellingen maken gebruik van derde partijen bij het bouwen en onderhouden van hun IT-systemen en applicaties. Deze partijen hebben de kennis in huis om de organisatie te kunnen ondersteunen bij zowel kleine als grote IT-vraagstukken. Een relatie aangaan met een partij heeft invloed op de beveiliging van de jeugdzorg instelling. De derde partij krijgt veelal toegang tot gevoelige informatie en systemen van de instelling. Als de derde partij kwetsbaar is voor beveiligings- of privacy incidenten, kan de instelling ook (reputatie) schade lijden. Hierdoor is het van belang dat er goed wordt gekeken naar welke partijen worden aangenomen en moeten er duidelijke afspraken zijn over het delen van data met deze partijen.

Een aantal maatregelen op het gebied van derde partijen die een organisatie kan nemen zijn:

- Kiezen voor de juiste derde partij**.** Bij het contracteren van een derde partij is het belangrijk om voor een partij te kiezen die zichzelf al bewezen heeft (bijv. door middel van certificering of een hoge score in benchmarks). Voorbeelden en referenties geven vaak meer zekerheid dat de organisatie daadwerkelijk in staat is de gevraagde diensten naar wens te leveren. Een brancheorganisatie zoals Jeugdzorg Nederland of gesprekken met IT-managers van andere instellingen kunnen ook ondersteunen bij het maken van de juiste keuzes.
  Het opnemen van afspraken over security en privacy in contracten met derde partijen. In het contract kan worden gewaarborgd wat voor data de derde partij mag inzien en hoe de beveiligingsrisico's door de derde partij worden geminimaliseerd. Neem eventueel ook bepalingen op die mogelijk maken dat je als afnemer het recht hebt om een audit of pentest op je leverancier uit te (laten) voeren. Derde partijen zouden altijd in staat moeten zijn om een TMP (of bijvoorbeeld een ISAE-verklaring) te overleggen.
- Het off-boarden van derde partijen**.** Wanneer het contract met een derde partij wordt beëindigd, is het belangrijk ervoor te zorgen dat alle gegevens worden opgehaald of vernietigd en dat de toegang van de derde partij tot de gegevens is uitgeschakeld.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk '6. Derde partijen' op pagina 24 van de deep dive.

7. Incident response

Een cybersecurity incident zorgt vaak voor ophef en negatieve impact op de organisatie. Vandaag de dag is het voor organisaties geen kwestie meer *of* het zal gebeuren, maar vooral *wanneer* het zal gebeuren. Het hebben van een gedegen incident response plan zorgt ervoor dat je als organisatie weet wat je te doen staat bij een incident zodat je de juiste stappen kan nemen om de impact van het incident zoveel als mogelijk te minimaliseren. Hoe sneller je handelt hoe groter de kans is dat de schade kleiner zal uitvallen.

Een aantal maatregelen op het gebied van incident response die een organisatie kan nemen zijn:

- Wijs iemand aan die het incident response plan beheert en up to date houdt.
- Stel een incident response team aan die op de hoogte is van wat er moet gebeuren tijdens een incident zodat zij medewerkers kunnen instrueren in het geval van een incident.
- Definieer in je plan wat een incident is en welke reactie daarbij hoort. Om misvattingen binnen de organisatie te voorkomen is het van belang dat er duidelijke definities zijn over wat een incident is en hoe werknemers daarmee moeten omgaan.
- In het incident response plan moet het op voorhand duidelijk zijn welke externe partij je nodig hebt voor assistentie en hoe je die kan bereiken. Het is aan te raden om vooraf afspraken te maken met zo een partij zodat het duidelijk is wat je van ze kan verwachten en hoe ze kunnen helpen.
- Bepaal welke gegevens en systemen extra bescherming en beveiliging vereisen zodat je de meest kritische informatie voor de organisatie meteen aanvullend kunt beschermen tijdens een incident.
- Stel een disaster recovery plan op welke naast natuurrampen ook rekening houdt met IT-incidenten zoals een ransomware aanval. Een risk assessment is een goed startpunt voor dit plan.

De bovenstaande en andere maatregelen worden in meer detail besproken in het hoofdstuk ‘7. Incident response’ op pagina 25-26 van de deep dive.

8. NEN-7510

De NEN-7510 is een leidende Nederlandse norm voor informatiebeveiliging in de zorgsector in Nederland. Voor de zorgsector is er een aangepast normenkader kosteloos beschikbaar gesteld door het Ministerie van VWS bij de Stichting Koninklijk Nederlands Normalisatie Instituut. Redenen voor het bestaan van een aangepaste norm voor de zorg zijn zorg specifieke aandachtspunten zoals privacybescherming en het beveiligen van medische gegevens evenals het taalgebruik, wat is aangepast op de zorgsector.

In de deep dive is op pagina 27 meer informatie over de NEN-7510 opgenomen.

NEN-7510
In de volgende sectie de ‘Deep dive’ wordt na elke deep dive de link gelegd tussen de geadviseerde maatregelen en de NEN-7510 norm.

Deep dive

Deep dive

In dit deel van de handreiking zal dieper worden ingegaan op de verschillende onderwerpen en aandachtsgebieden uit de snelstartgids.

1. Cyber Awareness

Bewustzijn van cyberrisico's bij IT- en zorgmedewerkers creëren is van cruciaal belang om te voorkomen dat dreigingen zich kunnen manifesteren in het IT-netwerk van de jeugdinstelling. Cyber dreigingen zijn namelijk in overvloed aanwezig, zowel van binnenuit als van buitenaf, en veranderen continu. Hierdoor is het van belang dat medewerkers zich bewust zijn van de verschillende risico`s die ze lopen en potentiële negatieve effecten van bepaalde handelingen zoals het delen van informatie.

Medewerkers hebben vaak de beste intenties om veilig te werken, maar zijn vaak onbekend met cyber risico's. Aanvallers maken vaak misbruik van medewerkers hun onoplettendheid of onwetendheid om relatief gemakkelijk binnen te kunnen dringen in het interne netwerk van de organisatie. Bekende voorbeelden hiervan zijn:

- **Phishing**: een frauduleuze poging om gevoelige gegevens te verkrijgen, zoals wachtwoorden waarbij aanvallers zich voordoen als een betrouwbare entiteit.
- **Zwakke wachtwoorden**: het gebruik van simpele wachtwoorden die gemakkelijk te raden of kraken zijn.

Om deze onwetendheid tegen te gaan, bewustzijn van risico's te creëren en ervoor te zorgen dat medewerkers op de hoogte zijn van de maatregelen die ze kunnen nemen om te voorkomen dat hun account gehackt wordt of dat ze per ongeluk data delen met personen voor wie deze data niet bestemd is komen hieronder een aantal maatregelen aan bod. Deze kan elke jeugdinstelling nemen om het bewustzijn van haar IT- en (zorg)medewerkers te vergroten:

- **Bepaal de focus van de bewustwordingscampagne op basis van de belangrijkste dreigingen voor de organisatie.** Een overzicht van cybersecurity incidenten van de organisatie zoals recente phishing aanvallen of het uitvoeren van een aanvalssimulatie zou hier objectief inzicht in kunnen geven.
- **Start een awareness campagne over bijvoorbeeld phishing e-mails.** Door middel van periodieke campagnes wordt bewustzijn gecreëerd en kan een organisatie haar medewerkers weerbaarder maken tegen cyber dreigingen. Denk hierbij bijvoorbeeld aan simpele oplossingen zoals het vergrendelen van een werkplek wanneer deze verlaten wordt en oplettendheid bij bijlagen en links in e-mails van externe verzenders.
- **Herhaal de awareness campagne regelmatig (minimaal 1 keer per jaar)**. Mensen leren door herhaling. Meerdere kleine awareness initiatieven over lange tijd hebben vaak meer effect dan één groot eenmalig event.
- **Maak gebruik van een interactief element als onderdeel van de awareness campagne(s).** Om de security awareness campagne onder de aandacht te brengen en mensen er over te laten praten werkt het vaak goed om in de campagne verschillende soorten spellen in te verwerken. Door een vorm van interactie of gamificatie worden mensen enthousiast om deel te nemen aan de training en onthouden ze de geleerde stof beter.
- **Zorg dat het vergroten van weerbaarheid bij medewerkers altijd het primaire doel van de awareness campagne is.** Als eerste inventariseer je mogelijke risico's zoals bijvoorbeeld phishing en vervolgens biedt je perspectief door aan te geven welke maatregelen medewerkers kunnen nemen om deze risico`s zoveel als mogelijk te verkleinen. Hierbij is het goed om voorbeelden van risico`s te gebruiken die dicht bij

de organisatie zelf staan. Denk hierbij bijvoorbeeld aan een dossier wat gelekt is doordat het via email in verkeerde handen is gekomen.

- **Voorkom naming en shaming en promoot goed gedrag.** Stimuleer het melden van verdachte incidenten, mailtjes, personen en telefoontjes**.** Als iemand bijvoorbeeld een phishing email herkent en rapporteert kan diegene uitgelicht worden om te laten zien dat ze het goed hebben gedaan. Dit werkt motiverend voor het gehele team.
- **Maak de drempel tot het melden van incidenten en risico's zo laag mogelijk**. Dit kan bijvoorbeeld door het implementeren van een phishing meldt knop in Outlook.
- **Zorg dat awareness en de voortuitgang meetbaar wordt gemaakt.** Een phishing test kan hiervoor bijvoorbeeld een goede methode zijn. Je stuurt je medewerkers phishing e-mails om te kijken of ze het herkennen en wat ze er vervolgens mee doen. De moeilijkheidsgraad kan gedurende verschillende testen verhoogd worden. Andere punten zal je door middel van kennis testen bij personeel (bijvoorbeeld via een survey of een quiz) kunnen ophalen. Hoe vaker er getest wordt, des te meer inzicht men krijgt in deelgebieden welke nog meer getraind moeten worden. Del resultaten niet enkel met het bestuur van de jeugdzorg organisatie maar ook met het (zorg)personeel.

NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 6, 7, 13, 18 inclusief bijlage A en C.

2. Veilig data delen

Bij het gebruiken, opslaan en delen van (privacy)gevoelige data is het belangrijk dat dit op een passende en veilige manier gebeurd. Het risico dat de integriteit of vertrouwelijkheid van de data wordt aangetast moet te allen tijde voorkomen worden. Uit onderzoek blijkt dat Nederlandse respondenten het delen van patiëntgegevens relatief vaak als uitdaging noemen (44 procent)[2]. Vandaag de dag zijn er gelukkig verschillende manieren en tools beschikbaar die gebruikt kunnen worden om data op een veilige manier te delen. Binnen de jeugdzorg instellingen kan dat bijvoorbeeld via de JeugdNet applicatie. Alle data in deze applicatie is versleuteld en de applicatie voldoet aan de privacywetgeving (GDPR) van de EU.

Hieronder staan een aantal algemene maatregelen die een jeugdinstelling kan nemen om ervoor te zorgen dat data op een veilige manier gedeeld wordt:

- **Stel een beleidsdocument op voor het delen van data en maak het kenbaar binnen de organisatie.** Binnen de organisatie moet er één duidelijk beleidsdocument zijn waarin tenminste de volgende punten worden beschreven: 1) definitie van wat gevoelige data is, 2) in welk geval wat voor soort data gedeeld mag worden, 3) door wie dat gedaan mag worden en 4) op wat voor manier dat moet gebeuren. Dit beleidsdocument moet gemakkelijk te vinden zijn voor alle medewerkers van de organisatie. Daarnaast is het aan te bevelen om het document te behandelen tijdens dataprivacy trainingen. Door middel van training kunnen medewerkers op een toegankelijke manier leren over de inhoud van het document en hoe ze naar de richtlijnen moeten handelen.
- **Train en leid medewerkers op.** Medewerkers moeten de gevoeligheden van verschillende soorten informatie begrijpen evenals de risico's en mogelijk consequenties die verbonden zijn aan het verkeerd omgaan met gevoelige gegevens. Een eenduidig en duidelijk beleid ten aanzien van welke data ze wel en niet buiten de organisatie kunnen delen kan hiervoor opgezet worden. Daarnaast kunnen medewerkers getraind worden waarbij ze op een veilige manier leren de juiste informatie met externe partijen te delen. Als een jeugdzorginstelling beschikt over een veilige oplossing om data te delen, is het de verantwoordelijkheid van de organisatie om ervoor te zorgen dat medewerkers deze optie ook gebruiken.
- **Voorkom het gebruik van niet-geautoriseerde apparaten (bijvoorbeeld USB-sticks)** zodat alleen apparaten die als vertrouwd

[2] Shaping the future of European healthcare, Deloitte, September 2020.

zijn gedefinieerd, verbinding kunnen maken met een bedrijfscomputer.

- **Encryptie instellen voor gevoelige data.** Zorg ervoor dat data die geclassificeerd is als 'gevoelige data' automatisch wordt versleuteld of niet via e-mail kan worden verzonden. Hiermee voorkom je dat de data bekeken kan worden door mensen voor wie het niet bedoeld is.
- **Maak het delen van data zo gemakkelijk mogelijk.** Door te kiezen voor een gemakkelijke en toegankelijke oplossing om (intern en extern) data te delen zullen medewerkers deze optie gebruiken en minder snel opzoek gaan naar niet goedgekeurde en vaak onveilige alternatieven.
- **Blokkeer bekende kwaadaardige en sharing websites.** Stel computers en telefoons zodanig in dat de toegang tot bekende kwaadaardige websites wordt geblokkeerd. Daarnaast kan een website filter eenvoudig worden geconfigureerd om websites voor het delen van bestanden te blokkeren. Denk hierbij aan websites zoals Dropbox en Google Drive. Hiermee wordt voorkomen dat dit soort websites gemakkelijk kunnen worden gebruikt en het verkleint het risico op het lekken van data. Door websites voor het delen van bestanden te blokkeren, stimuleer je medewerkers om gebruik te maken van de veilige optie die wordt geboden door de organisatie zelf. Deze opties dienen natuurlijk wel aanwezig en gecommuniceerd te zijn.

Datalekken in zorg & welzijn

De Autoriteit Persoonsgegevens (AP) ontving in 2017 ruim 10.000 meldingen van datalekken, zo liet de toezichthouder eind maart weten. Meer recente cijfers zijn er niet. De meeste meldingen, 3.105 in totaal (31%), kwamen zoals elk kwartaal uit de sector zorg en welzijn.

Bij datalekken in zorg en welzijn ging het in 2017 in 60 procent van de gevallen om persoonsgegevens die aan een verkeerde ontvanger zijn gestuurd. Meldingen van kwijtgeraakte persoonsgegevens, zoals een verloren of gestolen laptop of usb-stick, vormen 10 procent van het totale aantal gemelde datalekken. In 3 procent van de gevallen ging het om hacking, malware of phishing. Datalekken moeten sinds januari 2016 gemeld worden.

Bron*: ICT Health, 13 december 2018, https://www.icthealth.nl/nieuws/gelre-ziekenhuizen-gehackt-na-openen-phishing-mail.*

JeugdConnect PrivacyApp

Jeugdigen hebben recht op privacy. De PrivacyApp van JeugdConnect maakt het voor zorgmedewerkers mogelijk om een zelf een snelle toetsing uit te voeren rondom het delen van data op basis van het type data en de ontvanger. Deze privacy wijzer kan een handig hulpmiddel zijn om via een aantal simpele vragen te bepalen hoe men om mag gaan met data van jeugdigen. De applicatie geeft (zorg)medewerkers inzicht in welke data ze wel én welke data ze niet mogen delen evenals hoe de data gedeeld mag worden en onder welke voorwaarden.

Voor gratis toegang tot de (mobiele) webapplicatie van JeugdConnect ga naar: https://www.jeugdconnect.nl/privacy

NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 11, 13, 14, 15, 18 inclusief bijlage A en C evenals de NTA 7516.

3.1 Het belang van een sterk wachtwoordbeleid

Een wachtwoordbeleid is een reeks regels die zijn opgesteld om de toegangsbeveiliging te verhogen door gebruikers aan te moedigen sterke en veilige wachtwoorden te kiezen, deze vervolgens op de juiste manier op te slaan en te gebruiken. Een sterk en streng wachtwoordbeleid is noodzakelijk om de vertrouwelijkheid van informatie en de integriteit van systemen te beschermen. Met een sterk wachtwoordbeleid wordt voorkomen dat onbevoegde gebruikers gemakkelijk toegang krijgen tot interne systemen.

Hieronder staan een aantal algemene maatregelen die ervoor zorgen dat medewerkers sterke wachtwoorden gaan gebruiken en die op de juiste manier opslaan:

- **Stel een minimum van 8 tekens voor de wachtwoordlengte.** Lange wachtwoorden zijn over het algemeen moeilijker te kraken**.**
- **Een beleid voor wachtwoordgeschiedenis implementeren.** In een beleid voor wachtwoordgeschiedenis wordt bepaald hoe vaak een oud wachtwoord opnieuw kan en mag worden gebruikt. Dit beleid ontmoedigt gebruikers om een eerder wachtwoord te hergebruiken, waardoor ze niet kunnen wisselen tussen verschillende veelgebruikte wachtwoorden. Een leading practise hierbij is om een wachtwoordhistorie aan te houden van minimaal 10 wachtwoorden.
- **Voorkom snelle wijzigingen van wachtwoorden.** Dit beleid bepaalt hoe lang gebruikers een wachtwoord moeten behouden voordat ze het kunnen wijzigen. Hiermee voorkom je dat dat een gebruiker het wachtwoordbeleid ontwijkt door een nieuw wachtwoord te gebruiken en het vervolgens meteen terug te veranderen naar het oude wachtwoord. Het is veelal gebruikelijk om de termijn waarin het wachtwoord niet veranderd kan worden tussen drie en zeven dagen te zetten.
- **Screen nieuwe wachtwoorden tegen een lijst met bekende gecompromitteerde wachtwoorden.** Hiermee voorkom je dat aanvallers wachtwoorden gemakkelijk kunnen uitproberen en raden.
- **Beperk het aantal onjuiste wachtwoordpogingen en blokkeer het account indien nodig.** De meest voor de hand liggende manier om brute-force-aanvallen te blokkeren, is door simpelweg accounts te vergrendelen na een bepaald aantal onjuiste wachtwoordpogingen. Hiermee voorkom je dat aanvallers in korte tijd meerdere pogingen kunnen ondernemen om een account te hacken. Daarnaast zorgt het ervoor dat je op de hoogte bent van mogelijke poging tot misbruik. Accountvergrendelingen kunnen een bepaalde duur duren, zoals een uur, of de accounts kunnen vergrendeld blijven totdat ze handmatig worden ontgrendeld door een beheerder. Daarnaast is het aan te bevelen om bijvoorbeeld op IP-adres te blokkeren bij meerdere onjuiste wachtwoordpogingen.
- **Maak gebruik van passende tooling welke medewerkers helpt aan om voor elke applicatie een uniek wachtwoord te gebruiken.** Bij het gebruik van een uniek wachtwoord kan een hacker die toegang krijgt tot één account, niet noodzakelijkerwijs toegang verkrijgen tot andere accounts. Het gebruik van Single Sign On (SSO), waarbij de gebruiker maar eenmalig hoeft in te loggen om daarna veilig toegang te krijgen tot meerdere applicaties en resources in het netwerk, is een goed alternatief.

Indicaties wachtwoordaanval

Acties die kunnen duiden op een brute-force aanval met brute kracht of ander accountmisbruik:

- Veel mislukte aanmeldingen vanaf hetzelfde IP-adres of logins met meerdere gebruikersnamen vanaf hetzelfde IP-adres.
- Logins voor één account afkomstig van veel verschillende IP-adressen
- Overmatig gebruik en bandbreedteverbruik bij eenmalig gebruik.
- Mislukte inlogpogingen van alfabetisch opeenvolgende gebruikersnamen of wachtwoorden.
- Logins met een verwijzende URL van iemands e-mail of IRC-client.
- Logins met verdachte wachtwoorden.

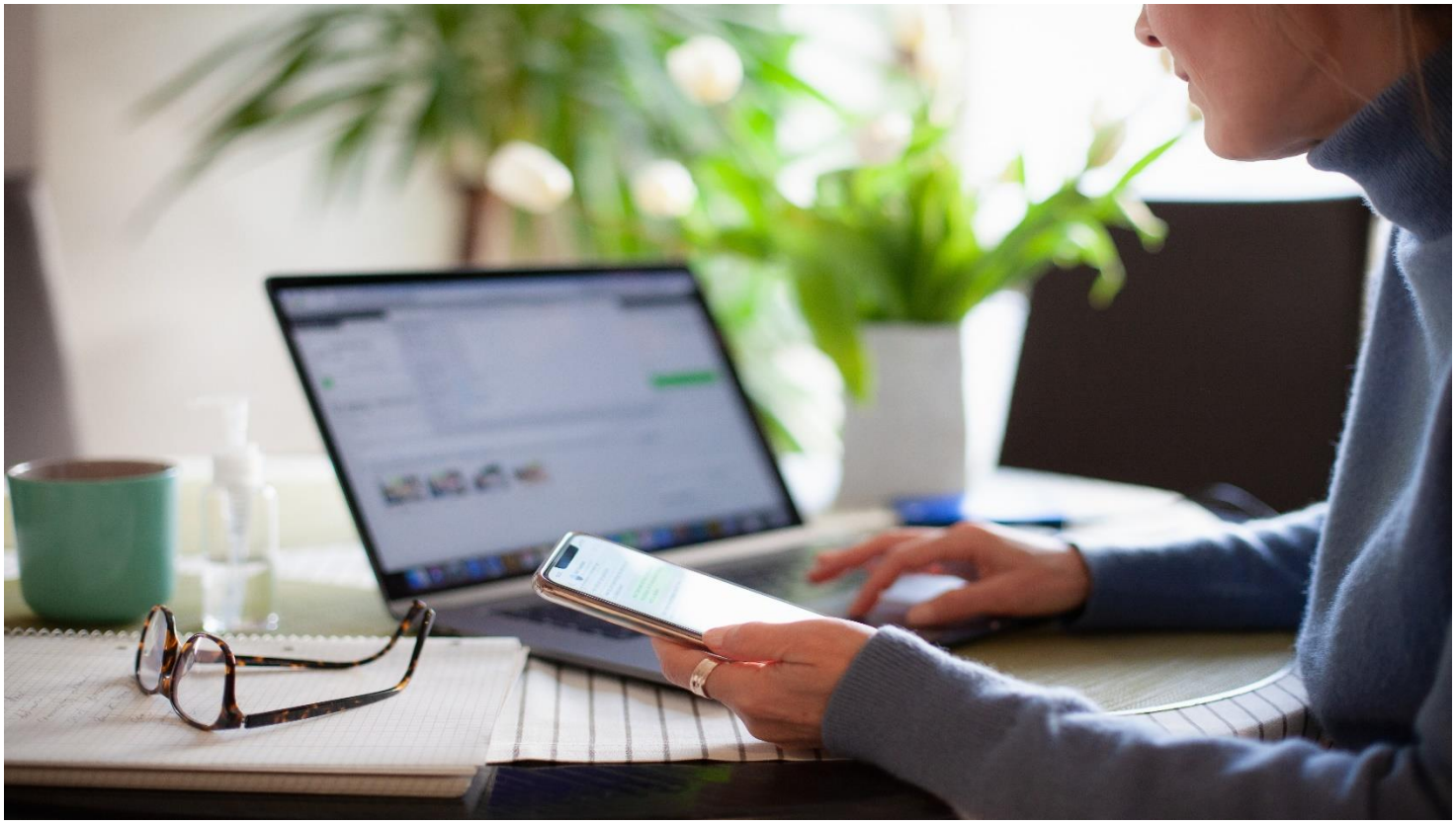
NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 7, 9, 10 inclusief bijlage A en C.

3.2 Multi-Factor Authenticatie (MFA)

Naast het afdwingen van het gebruik van sterke wachtwoorden wordt ook het gebruik van multi-factor authenticatie (MFA) tegenwoordig sterk aanbevolen. MFA is een verificatiemethode waarbij een gebruiker twee of meer verificatiefactoren moet opgeven om toegang te krijgen tot bijvoorbeeld een applicatie, online account of een VPN. Authenticatiemiddelen vallen in vijf categorieën (of factoren) indelen: iets dat je weet, iets dat je bent, iets dat je hebt, locatie en tijd. Een voorbeeld van MFA is dat je eerst een wachtwoord moet invoeren en vervolgens een code moet verifiëren via een smartphone. In plaats van alleen om een gebruikersnaam en wachtwoord te vragen, heeft MFA een of meer aanvullende verificatiefactoren nodig. Hiermee zorg je ervoor dat het voor iemand niet genoeg is om enkel in het bezit te zijn van jouw gebruikersnaam en wachtwoord. Diegene zal ook in het bezit moeten zijn van bijvoorbeeld je smartphone voor de tweede stap van de verificatie. Hierdoor is bij het gebruik van MFA de kans dat je wordt gehackt klein.

Hieronder benoemen wij algemene informatie welke een jeugdinstelling kan
gebruiken om ervoor te zorgen dat multi-factor authenticatie ingeregeld wordt:

- **Creëer een extra verdedigingslinie: stel multi-factor authenticatie in voor alle gebruikers.** Dit is vooral relevant voor apparaten die benaderbaar zijn vanaf het internet. Tegenwoordig bieden veel diensten multi-factor authenticatie aan door middel van een authenticatie applicatie zoals Google Authenticator of Microsoft Authenticatie. Hiermee is het gemakkelijker om MFA in te stellen voor de gebruikers van de organisatie. Het is belangrijk om gebruikers hierbij te begeleiden en de kans te geven deze applicaties juist in te stellen zodat hun account en de data van de organisatie extra beveiligd is tegen dreigingen. Daarnaast is het van belang dat IT te allen tijde kan helpen om een gebruiker weer toegang te verlenen als deze niet meer beschikt over zijn andere factor(en).



NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 9.4 inclusief bijlage C.

4. Accountbeheer: Identity & Access Management

IAM (Identity access management) gaat over het definiëren en beheren van de rollen en toegangsrechten van individuele gebruikers.

Rechtenbeheer

Het doel van IAM is om één digitale identiteit toe te wijzen aan één individu. Zodra de digitale identiteit is vastgesteld, wordt deze onderhouden, wanneer noodzakelijk tijdig gewijzigd en strikt gemonitord. Met de juiste IAM-maatregelen kan een jeugdzorginstelling gebruikers toegang verlenen tot de juiste data, op het juiste moment: vanaf dat de identiteit gecreëerd wordt totdat de gebruiker de toegang wordt ontzegd (bijvoorbeeld bij het vertrek van een werknemer). Als een organisatie controle heeft over de gebruikersaccount voorkomt dit vaak het hacken van ongebruikte accounts, ongeautoriseerde handelingen en vergeldingsacties.

Accounts met hogere rechten

Een speciale categorie binnen IAM is Privileged Access Management (PAM). PAM is een term die wordt gebruikt om speciale toegang of mogelijkheden aan te duiden die verder gaan dan die van een standaardgebruiker zoals beheerdersaccounts. Door middel van geprivilegieerde toegang kunnen organisaties hun infrastructuur en applicaties beveiligen en de vertrouwelijkheid van gevoelige gegevens en kritieke infrastructuur behouden. Een voorbeeld hiervan is een gebruikersaccount die rechten heeft om configuraties aan een systeem of applicatie te maken, gebruikers toe te voegen of te verwijderen of juist om gegevens te verwijderen. Het idee van PAM is dat er wordt nagedacht over wat voor soort toegang gebruikers nodig hebben zodat ze enkel het minimale toegangsniveau krijgen dat nodig is om de toegewezen taken uit te voeren. Zowel IAM als PAM zijn belangrijk om te voorkomen dat medewerkers toegang hebben tot data die niet voor hun bedoeld is. Met een goede implementatie verklein je direct het risico dat medewerkers in het bezit komen van data waar ze eigenlijk geen gebruik van mogen maken: ze kunnen er gewoon weg niet bij.

Hieronder wordt een aantal maatregelen behandeld welke elke jeugdinstelling kan nemen om ervoor te zorgen dat gebruikersaccounts en accounts met hoge rechten gestructureerd en veilig worden onderhouden:

- **Controleer regelmatig de rollen van alle medewerkers ten opzichte van de taken die ze uitvoeren evenals op conflicterende rechten**. Medewerkers hebben verschillende taken en op basis van hun taken horen ze een rol toegewezen te krijgen waarmee ze toegang hebben tot data dat bij hun taken past. Om ervoor te zorgen dat ze te allen tijde de juiste rol toegewezen krijgen is het van belang om goed in de gaten te houden welke taken ze uitvoeren en wat voor rol bij de taak past. Daarnaast is het van belang om tenminste jaarlijks te controleren of bepaalde rollen niet beschikken over conflicterende rechten.
- **Volgen van accounts.** Het is van belang om alle accounts zowel van normale gebruikers als gebruikers met hoge rechten centraal te beheren en te monitoren zodat IT-beheer altijd op de hoogte is van wie er toegang heeft (gehad) tot gevoelige data en wanneer er gebruik wordt gemaakt van deze toegangsrechten. Dit helpt ook bij forensisch onderzoek bij een incident.
- **Tijdig zorgen voor functie- en afdelingswisselingen van medewerkers aan IT**. Elke organisatie dient een gedegen proces te hebben voor het in- en uit dienst treden van medewerkers evenals het wisselen van functies. Dankzij dit proces kan de jeugdzorginstelling ervoor zorgen dat tijdig de juiste rollen en toegangsrechten aan de juiste medewerkers kan worden toegewezen zodat medewerkers alleen informatie kunnen zien die voor hun bedoeld is. Medewerkers die vertrekken mogen bijvoorbeeld geen toegang meer hebben tot gevoelige data.
- **Gebruik persoonlijke beheerdersaccounts.** Zorg dat elke beheerder zijn eigen account heeft in plaats van beheerdersaccounts te delen met meerdere personen. Hierdoor wordt voorkomen dat er bijvoorbeeld gevoelige wachtwoorden gedeeld worden binnen de organisatie en hiermee kan een overzicht gecreëerd worden van wie de beheerdersaccount op wat voor manier gebruikt. Zorg dat hiervoor een gedegen aanvraag proces bestaat inclusief een vorm van formele goedkeuring.
- **Beperkt ook de Domain Administrator Account rechten.** In de meeste organisaties wordt er gebruik gemaakt van duidelijke functiescheiding van rechten. De rechten van de domain administrator worden echter minder vaak aan een kritische review onderworpen. Vaak kunnen de rechten van een dergelijk account tot een minimum beperkt worden zonder dat dit impact heeft op de dagelijkse werkzaamheden.
- **Sla wachtwoorden van serviceaccounts veilig op.** De wachtwoorden van beheerdersaccounts zijn uitermate waardevol voor mogelijke aanvallers hierdoor is het van belang dat ze apart en veilig worden opgeslagen

NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 7, 9.2 & 9.3 inclusief bijlage C.

5. Patching

Patchen, het tijdig updaten van systemen en applicaties, is een essentieel onderdeel van de informatiebeveiliging van iedere organisatie. Het zorgt ervoor dat bekende lekken in software tijdig verholpen worden waardoor aanvallers ze niet meer kunnen misbruiken. Daarnaast zorgt patchen ervoor dat uw organisatie over de laatste functionaliteit van software beschikt en leveren patches met enige regelmaat ook oplossingen voor fouten in de software (bugs). Er hebben de afgelopen jaren meerdere incidenten plaatsgevonden waarbij aanvallers toegang wisten te krijgen tot servers van organisaties met gevoelige data via software dat niet gepatched was en daardoor kwetsbaar was tegen misbruik. In sommige gevallen heeft dit tot desastreuze gevolgen geleid zoals het geval was bij een van de grootste vervoerders bedrijven ter wereld. In 2017 werden zij slachtoffer van een ransomware aanval waarbij ze rond de 300 miljoen dollar aan verliezen hebben geleden[3]. Via systemen die niet geüpdatet waren wisten aanvallers de interne systemen binnen te dringen en beslag te leggen op kritische data die ervoor zorgde dat het hele bedrijf voor een aantal dagen plat kwam te liggen. Dit incident liet zien dat het van essentieel belang is om alle soorten software die je bezit regelmatig en tijdig te patchen. Bij patching is er een aantal maatregelen die je te allen tijde kan hanteren om je software en hardware goed te beveiligen.

Hieronder staat een aantal maatregelen welke een organisatie kan nemen om te zorgen dat de software up to date blijft:

- **Inventariseer al je hardware**. Je kunt pas weten wat je moet patchen als je duidelijk inzicht en overzicht hebt van de gebruikte hardware en welke kwetsbaarheden de hardware met zich op een bepaald moment meedraagt. Denk hierbij aan computers, servers en netwerkapparatuur.
- **Inventariseer al je software.** Net zoals bij hardware geldt dat je een duidelijk beeld nodig hebt van welke besturingssystemen, server applicaties en desktopapplicaties je bezit en welke versies het betreft zodat je die regelmatig kan updaten en bij ernstige kwetsbaarheden snel kunt lokaliseren waar de kwetsbare software in je netwerk in gebruik is (en dus welk risico er mee gemoeid is).
- **Leg een patch proces vast met vaste patch momenten.** Kies een wekelijks of maandelijks moment waarbij je al je systemen patched. Zorg dat dit wordt vastgelegd in een proces, bijvoorbeeld UPMS (Update Patch Management System), zodat het patchen niet vergeten wordt en altijd duidelijk is wat wanneer gepatched is en door wie. Hierbij is het van belang dat je goed oplet dat je tijdig patched en dat je patches van tevoren test zodat je eventuele updateproblemen tijdig kan mitigeren. In het geval van een derde partij moet er contractueel duidelijk worden afgesproken wat de update-rate en doorlooptijden zijn van de patches evenals wanneer deze worden geïmplementeerd (patch window) om verstoring van werkzaamheden te voorkomen.
- **Stel een duidelijke hoofdverantwoordelijke aan.** Het moet te allen tijde duidelijk zijn wie binnen de organisatie verantwoordelijk is om de patches tijdig uit te voeren en de inventaris op orde te houden. Deze verantwoordelijkheid kan ook bij een derde partij liggen. Maak hierover duidelijke afspraken en leg deze vast (bijvoorbeeld in het contract).
- **Monitoren**. Naast het inventariseren van de software en hardware is het van belang dat er regelmatig wordt gekeken of alle patches nog up to date zijn zodat de organisatie tijdig op de hoogte is van mogelijke problemen of kwetsbaarheden in de software.
- **Houd je applicaties up to date**. Zorg dat de nieuwste, veilige versies van software zijn geïnstalleerd. Aanvallers misbruiken graag al bekende kwetsbaarheden in software. Aangezien deze informatie vaak openbaar beschikbaar is, is dit een veel gebruikte eerste stap om binnen te dringen bij organisaties. Wanneer patches en updates tijdig uitgevoerd worden is een organisatie een lastiger doelwit voor kwaadwillende.
- **Zorg voor duidelijke afspraken (SLA's) met leveranciers.** Aangezien je afhankelijk bent van geïmplementeerde patches door derden kun je met een SLA afdwingen dat systemen en applicaties tijdig bijgewerkt worden.

NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 6, 12, 14 en 18 inclusief bijlage C.

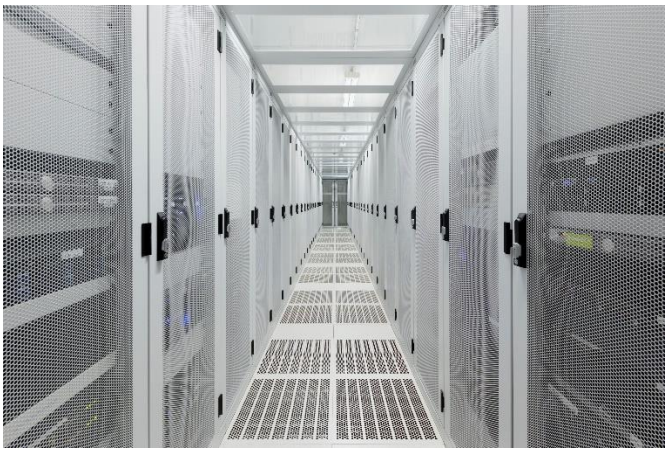
[3] Bron: The untold story of NotPetya, the most devastating cyber attack in the world, Wired, augustus 2018.

6. Derde partijen

Tegenwoordig besteden veel organisaties hun IT uit aan derde partijen. Deze partijen hebben specifieke kennis in huis waarmee ze JZ-instellingen kunnen ondersteunen met verschillende IT-werkzaamheden. Wanneer er een relatie aangegaan wordt met een derde partij, heeft de benadering van de derde partij op het gebied van beveiliging en privacy rechtstreeks invloed op de eigen instelling. Als de derde partij kwetsbaar is voor beveiligings- of privacy incidenten, kan dit ook negatieve invloed hebben op de JZ-instelling (bijvoorbeeld reputatie schade). Hierdoor is het van belang dat er duidelijke processen en afspraken zijn over het aannemen van derde partijen en het delen van data met deze partijen. Hierbij worden ook duidelijke eisen geformuleerd over wat voor soort beveiliging de systemen, applicaties en data moeten hebben. Vervolgens wordt dit gedeeld met de partijen die de instelling in dienst neemt zodat zij weten aan welke eisen zij in ieder geval moeten voldoen om de instelling goed te kunnen beveiligen.

Hieronder komen een aantal aanbevelingen aan bod die een organisatie in acht kan nemen wanneer men te maken heeft met derde partijen. Deze aanbevelingen kunnen door iedere jeugdzorgorganisatie worden genomen om risico's rondom derde partijen te verkleinen:

- **Kiezen voor de juiste derde partij.** Bij het contracteren van een derde partij is het belangrijk om voor een partij te kiezen die zichzelf al bewezen heeft (bijv. door middel van certificering of een hoge score in benchmarks). Voorbeelden en referenties geven vaak meer zekerheid dat de organisatie daadwerkelijk in staat de gevraagde diensten naar wens te leveren. Kijk hierbij ook naar bijvoorbeeld een ISAE-verklaring voor meer zekerheid over de geïmplementeerde beheersmaatregelen om de kritische processen van jou als klant te beveiligen. Een brancheorganisatie zoals Jeugdzorg Nederland of gesprekken met IT-managers van andere instellingen kunnen ook ondersteunen bij het maken van de juiste keuzes.
- **Het opstellen van contracten met derde partijen.** Een duidelijk contract vormt de basis voor een gestructureerde en succesvolle relatie met een derde partij. Bij het opstellen van het contract moeten alle vereisten, controles en procedures worden meegenomen die relevant zijn voor jouw organisatie met betrekking tot het minimaliseren van risico. Daarbij moet ook geformuleerd worden op welke manier data verwerkt en gedeeld wordt zodat het contract aan alle juiste privacywetgeving kan voldoen.
- **Monitoren van derde partijen.** Het is belangrijk om toezicht te houden op derde partijen waarmee je een relatie aangaat. Het monitoren zorgt ervoor dat het duidelijk is wat beide partijen van elkaar kunnen verwachten en er kan gekeken worden hoe de derde partij omgaat met de vooraf in kaart gebrachte risico`s. Door regelmatig te monitoren worden potentiële risico's tijdig gesignaleerd en kan potentiële (reputatie) schade worden vermeden. Het monitoren kan bijvoorbeeld in de vorm van een maandelijks afstemmingsmoment tussen de derde partij en de jeugdzorginstelling.
- **Het off-boarden van derde partijen.** Wanneer het contract met een derde partij wordt beëindigd, is het belangrijk ervoor te zorgen dat alle gegevens worden opgehaald of vernietigd en dat de toegang van de derde partij tot de gegevens is uitgeschakeld. Om dit op een goede manier te laten verlopen is het van belang dat er bij het aflopen van het contract duidelijke afspraken worden gemaakt met de derde partij over hoe en wanneer ze jouw data gaan verwijderen.



NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 6, 9, 11, 15 en 18 inclusief bijlage C.

7. Incident response

Incident response is een term voor het proces waarmee een organisatie een datalek of een cyberaanval afhandelt. Uiteindelijk is het doel om het incident effectief te managen, zodat de schade beperkt blijft en zowel hersteltijd, kosten als bijkomende schade zoals merkreputatie tot een minimum worden beperkt. Hierbij is het cruciaal dat organisaties een duidelijk incident response plan hebben zodat elke medewerker op de hoogte is van wanneer iets een mogelijk incident is en waar diegene dat vervolgens kan melden. Een goed incident response plan bestaat uit een vast, doordacht draaiboek waarbij gedefinieerd is wat de afgesproken tijd is over wanneer een incident moet worden opgepakt en afgehandeld. Het draaiboek kan verschillende scenario's bevatten. Daarbij moeten er specifieke medewerkers worden aangewezen die verantwoordelijk worden gesteld voor het up-to-date houden van het plan. Deze medewerkers moeten ook regelmatig een basistraining krijgen over incident response zodat ze continu op de hoogte zijn van wat er moet gebeuren tijdens een incident. Dit is bijvoorbeeld ook het geval met BHV'ers in een organisatie waarbij er iemand aangewezen wordt om BHV'er te zijn en zijn kennis vervolgens regelmatig op pijl moet houden.

Hieronder staan een aantal algemene maatregelen die een jeugdinstelling kan nemen om ervoor te zorgen dat men voorbereid is op een incident:

- **Stel specifieke teams en individuen aan die het incident response plan beheren en up to date houden**. Deze teams en individuen moeten verantwoordelijk zijn voor de verschillende stappen in het incident response plan zodat het altijd duidelijk is wie waarvoor verantwoordelijk is tijdens een incident.
- **Definieer wat een incident is en welke reactie daarbij hoort.** Om misvattingen binnen de organisatie te voorkomen is het van belang dat er duidelijke definities zijn over wat een incident is en hoe werknemers daarmee moeten omgaan. Dit kan vervolgens worden verwerkt in een draaiboek.
- **Bepaal welke gegevens extra bescherming en beveiliging vereisen.** Bij een incident wil je de meest kritische informatie die je bezit extra beschermen en beveiligen om ervoor te zorgen dat er niets ernstigs mee kan gebeuren. Hierbij is het van belang dat je van tevoren hebt vastgesteld wat je kroonjuwelen zijn en wat dat betekent in termen van beveiliging. Denk hierbij ook aan het regelmatig back-uppen van data, testen van roll-backs en adequate beveiliging van back-ups. Een goede voorbereiding versnelt het herstel van een cyber aanval.
- **Stel procedures op over wie wanneer op de hoogte moet worden gesteld over een incident.** Per type incident moet er beoordeeld worden welke personen en/of instanties op de hoogte moeten worden gebracht. In sommige gevallen hoeft bijvoorbeeld alleen de security officer op hoogte te worden gebracht maar in andere gevallen kan het zijn dat de politie ingeschakeld moet worden of de Autoriteit Persoonsgegevens.
- **Behoud alle gegevens van getroffen systemen voor forensische doeleinden.** Om te kunnen analyseren wat er precies mis is gegaan en hoe eventuele aanvallers te werk zijn gegaan is het van belang dat alle gegevens van getroffen systemen gelogd en opgeslagen worden zodat ze kunnen worden geanalyseerd. Hiermee kunnen soortgelijke incidenten in de toekomst worden voorkomen.
- **Voer een review uit na het incident.** Het is altijd van belang om na het afhandelen van het incident te analyseren hoe alle stappen in het incident response plan zijn gegaan. Hierbij kan er kritisch gekeken worden naar het hele proces zodat de gehele organisatie ervan kan leren en het plan aanpassen aan de hand van de lessen die geleerd zijn.
- **Zorg dat je voorbereid bent, ook op onvoorziene situaties.** Een goed proces voor het managen van een onvoorbereide crisis bestaat vaak uit de iteratieve stappen beschreven in het grijze blok. Het is aan te raden om ervoor te zorgen dat er al concept communicatieplannen klaarliggen. Stel een disaster recovery plan op welke naast natuurrampen ook rekening houdt met IT-incidenten zoals een ransomware aanval. Een risk assessment is een goed startpunt voor dit plan.

Diensten | Jeugdzorg Nederland

Jeugdzorg Nederland wil jeugdzorg organisaties ook ondersteunen op het gebied van incident response door afspraken te maken met geselecteerde partners over response services. In het geval van een incident bij een van de leden kan de brancheorganisatie dan snel de juiste derde partij betrekken en zo de impact zoveel mogelijk beperken.

NEN-7510
Voor meer informatie zie onder andere de NEN 7510-2:2017 hoofdstuk 16 en 17 inclusief bijlage C.

Besluitvormingsproces gedurende een crisis

1. Initiëren en verklaren crisis en/of incident. Dit is een belangrijke stap, wanneer is iets een incident en wanneer moet een gebeurtenis als een incident behandeld worden. Dit dient van tevoren duidelijk te zijn zodat iedereen binnen de organisatie ervan op de hoogte is wanneer er onverwachts een groot incident is.

Kernvragen tijdens incident:

- Wat is de belangrijkste informatie - nieuw of gewijzigd?
- Wat weten we, wat weten wij niet en wie is erbij betrokken?

2. Bepalen effecten, mogelijke impact en scenario's. Zodra een incident als een crisissituatie of groot incident is aangemerkt is het cruciaal om na te denken over de effecten en mitigerende acties.

Kernvragen tijdens incident:

- Wat betekent het voor ons - wat zijn de effecten en wat is de toekomstverwachting?
- Welke kritieke bedrijfsactiviteiten zijn beïnvloed?
- Op welke ontwikkelingen anticiperen we?

3. Besluitvorming en acties formuleren. Als de mogelijke effecten en acties in korte tijd geanalyseerd zijn (zonder alle informatie te hebben) is het van belang om direct stappen uit te denken om de impact te beperken.

Kernvragen tijdens incident:

- Wat zijn onze prioriteiten?
- Wat is onze strategie?
- Welke beslissingen en acties zijn vereist?
- Wat en wie hebben wij nodig om te communiceren?

4. Reflectie. Na het opzetten van een korte termijn actieplan is het van belang dat iedereen de strategie en acties erkent. Zodra dit het geval is kan men direct actie ondernemen om de impact daadwerkelijk te gaan beperken.

- Bevestig overeengekomen strategie, beslissingen, eigenaren en tijdschema's.

5. Volgende crisis bijeenkomst. Stem duidelijk met het crisisteam af wanneer men elkaar weer ontmoet om de cyclus nogmaals door te lopen.

- Wat is de volgende keer dat het team elkaar ontmoet?

8. NEN-7510

Voor wie is de NEN 7510?

De norm is ontwikkeld voor instellingen in de zorg. NEN 7510 geeft u handvatten voor het inrichten van adequate ICT-systemen en beheersmaatregelen. De NEN 7510 dekt het hele gebied van informatiebeveiliging en blijft dus niet beperkt tot technische specificaties maar geeft ook richting aan de organisatie en het menselijk handelen.

Wat is de NEN 7510?

De norm NEN 7510 bestaat uit twee delen. NEN 7510-1 stelt eisen aan het informatiebeveiligingsmanagementsysteem en NEN 7510-2 geeft richtlijnen voor passende beheersmaatregelen. Dankzij een overeenkomst met het Ministerie van VWS zijn deze en de aanvullende normen NEN 7512, NEN 7513 en NTA 7516 vrij beschikbaar.

Voordelen van NEN 7510 certificering

De NEN 7510 biedt een aantal voordelen voor jeugdinstellingen, zoals:

- U leert uw beveiligingsrisico's kennen waarop u vervolgens kunt inspelen.
- Het geeft een praktisch kader om uw informatiebeveiliging in te richten volgens de wettelijke eisen rond het Elektronisch Patiënten Dossier (EPD).
- Met een NEN 7510 certificering laat de organisatie aan zorgverzekeraars en patiënten zien dat (privacygevoelige) gegevens van patiënten in goede handen zijn.
- De NEN 7510 helpt u uw processen en informatiebeveiliging naar een hoger niveau te tillen waardoor het aantal beveiligingsincidenten zeer waarschijnlijk zal verminderen.

Diensten | Jeugdzorg Nederland

De leden van Jeugdzorg Nederland zetten zich elke dag keihard in voor de beste zorg voor onze jeugd. Een goede informatievoorziening en ICT-infrastructuur zijn daarbij onmisbaar: jeugdzorgprofessionals moeten erop kunnen vertrouwen dat alles naar behoren werkt.

Tegelijkertijd is het van groot belang dat organisaties zich bewust zijn van de risico's en voorzorgsmaatregelen nemen om informatielekken te voorkomen. Jeugdzorg Nederland wil haar leden, met de steun van het Ministerie van VWS, daarom helpen, ontzorgen en adviseren als het gaat om het verbeteren van awareness, het organiseren van red teaming, het implementeren van de NEN 7510 en het laten monitoren van netwerken en infrastructuur.

NEN-7510

Voor meer informatie zie:

- *NEN 7510-1 Medische informatica – Informatiebeveiliging in de zorg Deel 1: Managementsystemen*
- *NEN 7510-2 Medische informatica – Informatiebeveiliging in de zorg Deel 2: Beheersmaatregelen*
- *NEN 7512 Medische informatica – Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling*
- *NEN 7513 Medische informatica – Logging – Vastleggen van acties op elektronische patiëntdossiers*
- *NTA 7516 Medische informatica – Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie)*

Naslagwerken

Hieronder hebben staan een aantal bronnen opgesomd die de organisatie kan raadplegen voor aanvullende informatie over de adviezen welke in de handreiking aan bod zijn gekomen. Onderstaande bronnen zijn opgenomen in volgordelijkheid op basis van relevantie voor de jeugdzorgsector.

NEN7510

De NEN 7510 is een nationale norm, specifiek toegespitst op organisaties die te maken hebben met persoonlijke gezondheidsinformatie.

Zie ook: https://www.nen.nl/nen-7510-1-2017-a1-2020-nl-267179

CIS-20

Het Center for Internet Security Critical Security Controls for Effective Cyber Defense (CIS) is een organisatie die jaarlijks richtlijnen publiceert voor computerbeveiliging.

Zie ook: https://www.cisecurity.org/controls/cis-controls-list

OWASP® Foundation

De OWASP® Foundation werkt aan het verbeteren van de beveiliging van software door middel van door de gemeenschap geleide open source softwareprojecten, honderden afdelingen wereldwijd, tienduizenden leden en door het hosten van lokale en wereldwijde conferenties. Op de website is een overzicht te vinden van de OWASP Top-10: een lijst met de meest voorkomende security risico’s evenals beheersmaatregelen.

Zie ook: https://owasp.org/www-community/controls

NCSC

Het Nationaal Cyber Security Centrum (NCSC) is onderdeel van het ministerie van Justitie en Veiligheid. Een kennis- en expertisecentrum dat werkt aan een digitaal veilig Nederland. Het is niet gericht op de zorg maar publiceert ook algemene tips rondom informatiebeveiliging en actuele dreigingen.

Zie ook: https://www.ncsc.nl & https://www.ncsc.nl/actueel/beveiligingsadviezen

NERC

De North American Electric Reliability Corporation (NERC) is een internationale regelgevende instantie die als doel heeft de risico's voor de betrouwbaarheid en veiligheid van het net effectief en efficiënt te verminderen. NERC ontwikkelt en handhaaft de CIP standaard die organisaties

kunnen gebruiken om te kijken welke veiligheidsmaatregelen ze kunnen nemen op het gebied van IT.

Zie ook: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Digital Trust Center

Het Digital Trust Center (DTC), een initiatief van het Ministerie van Economische Zaken en Klimaat, heeft als missie om 1,8 miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. Op hun website delen ze kennis, informatie en advies die organisaties kunnen overnemen om de basale digitale veiligheidsmaatregelen van hun organisatie op orde te krijgen.

Zie ook: https://www.digitaltrustcenter.nl

Gartner

Gartner is een toonaangevende onderzoeks- en adviesbedrijf die onder andere advies geeft over IT-beveiliging. Op hun website publiceren ze regelmatig verschillende adviezen over cyberbeveiliging. Sommige kun je kosteloos inzien en als IT-manager kan overnemen. Daarbij zijn ze goed op de hoogte van de nieuwste ontwikkelingen binnen het cyber domein.

Zie ook: https://www.gartner.com/smarterwithgartner/category/it

Deloitte digitale transformatie gezondheidszorg na COVID-19

De zorg in Nederland digitaliseert snel. Dit rapport biedt inzichten in de uitdagingen en mogelijkheden na COVID-19.

Zie ook: https://www2.deloitte.com/nl/nl/pages/publieke-sector/articles/nederlandse-gezondheidszorg-digitale-voorloper-binnen-europa.html

Deloitte.