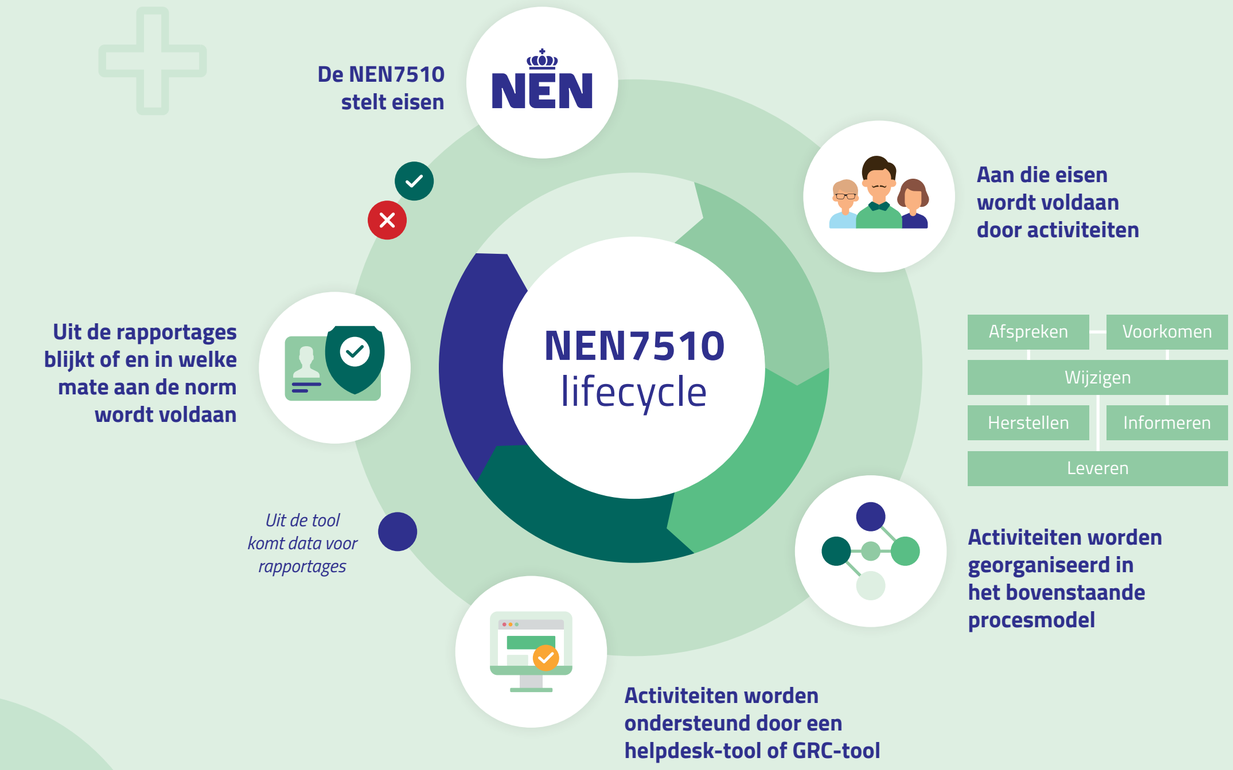
Onze missie is het **versterken van de digitale veiligheid** van de zorgsector.



Testen

Cybersecurity volwassenheid en hoe te bereiken

Meten is weten. Om te weten of uw organisatie volwassen is op het gebied van cybersecurity kunt u dit meten. Het meten vindt plaats door het uitvoeren van de tests aangegeven in de vier stappen. De volgorde van de stappen is belangrijk in het bereiken van volwassenheid op een effectieve en efficiënte wijze. Niet alleen dienen de stappen in de juiste volgorde doorlopen te worden, ook dienen de geconstateerde bevindingen ingevuld en/of verbeterd te worden.

	Frequentie	Rapportage	Focus	Gemiddelde duur/kosten
Audit	Jaarlijks	Meet de prestaties van de organisatie met betrekking tot het vastgestelde beleid, procedures en systemen gebaseerd op een risicoanalyse waarbij de bedrijfsrisico's het uitgangspunt zijn. De normen zijn vastgelegd in o.a. ISO 27001 en NEN 7510.	**CHECK** | Gebruik van checklists om afwijkingen te constateren.	3-7 dagen 4-8k per jaar
Vulnerability assessment	Doorlopend / Per kwartaal	Rapporteert een overzicht van issues. Identificeert en prioriteert. Voorziet in mitigatie advies.	**FIND** | Gebruik van geautomatiseerde scans om zoveel mogelijk kwetsbaarheden te vinden.	1-5 dagen 15-50k per jaar
Penetration test	Jaarlijks	Rapporteert bedrijfsrisico's door levering bewijs van gecompromitteerde data of netwerktoegang. Specifiek advies over verbeteraspecten.	**TEST (The Defence)** | het vinden van alle te misbruiken kwetsbaarheden, onveilige configuraties en het doordringen in de netwerken en systemen onder gecontroleerde omstandigheden.	2-4 weken 5-20k per test
Red Team test	om de 3 tot 5 jaar	Levert een "walk through" door de gebruikte TTP's. Presenteert een residual risk analyse en aanbevelingen voor verbetering van het complete security programma.	**ATTACK (The Defenders)** | Nabootsen van de tactieken, technieken en procedures (TTP's) van "real world" tegenstanders met het doel om de tekortkomingen in de verdediging, detectie en reactie van organisaties te meten aangaande de operationele omgeving.	4-8 weken 30-80k per test

De menselijke factor. Naast de technische aspecten van Cybersecurity is de mens ook een attack-vector en -surface en dient deze getraind en getest te worden. Met het huidige niveau van bijvoorbeeld phishing en social engineering technieken is de menselijke factor nogal eens de zwakste schakel.

Cybersecurity Awareness test	Halfjaarlijks	Rapporteert het niveau van cybersecurity awareness van de complete organisatie.	**RAISING AWARENESS** | Gebruik van jaarlijkse algemene en/of specifieke trainingen die vervolgens getest worden met behulp van o.a. phishingtests en algemene awareness tests.	10-30 minuten

Maturity scan

Wat is de maturity scan?

De maturity scan is een tool waarmee u inzicht kan krijgen in het volwassenheids-niveau van uw informatiebeveiliging en privacy. Aan de hand van vragen op basis van de NEN 7510 en de AVG krijgt u een visueel overzicht van hoe u er voor staat.

Wat komt er uit de maturity scan?

Per onderwerp, zoals toegangsbeveiliging of personeel, krijgt u een score toege-wezen. Deze wordt ook in één grote spingrafiek weergegeven. Zo vallen de onderwerpen die verbetering behoeven direct op. Op deze manier kunt u, in gesprek met management, gemakkelijker doelen stellen.

Waar vind ik de maturity scan?

De maturity scan is te vinden op **www.z-cert.nl/maturity**.

Wat heb ik aan de maturity scan?

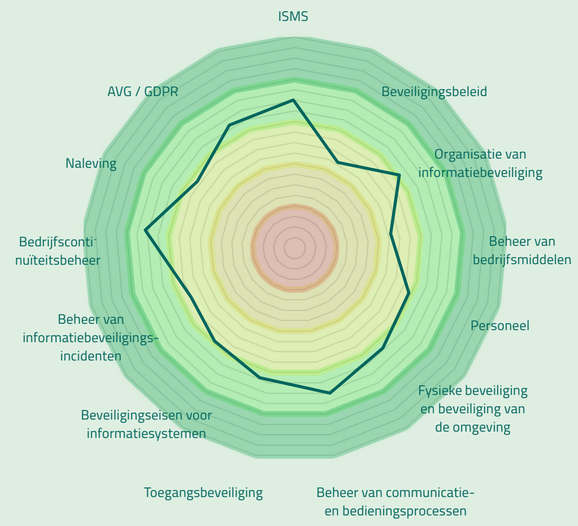
Het invullen van de maturity scan zelf kan al waardevol zijn om zo, in gesprek met diverse stakeholders, verbeterpunten te identificeren. Daarnaast is het een gemakkelijke praatplaat om te rapporteren richting het management. U ziet namelijk in één oogopslag hoe u scoort op de diverse onderdelen.

Hoe gebruik ik de maturity scan?

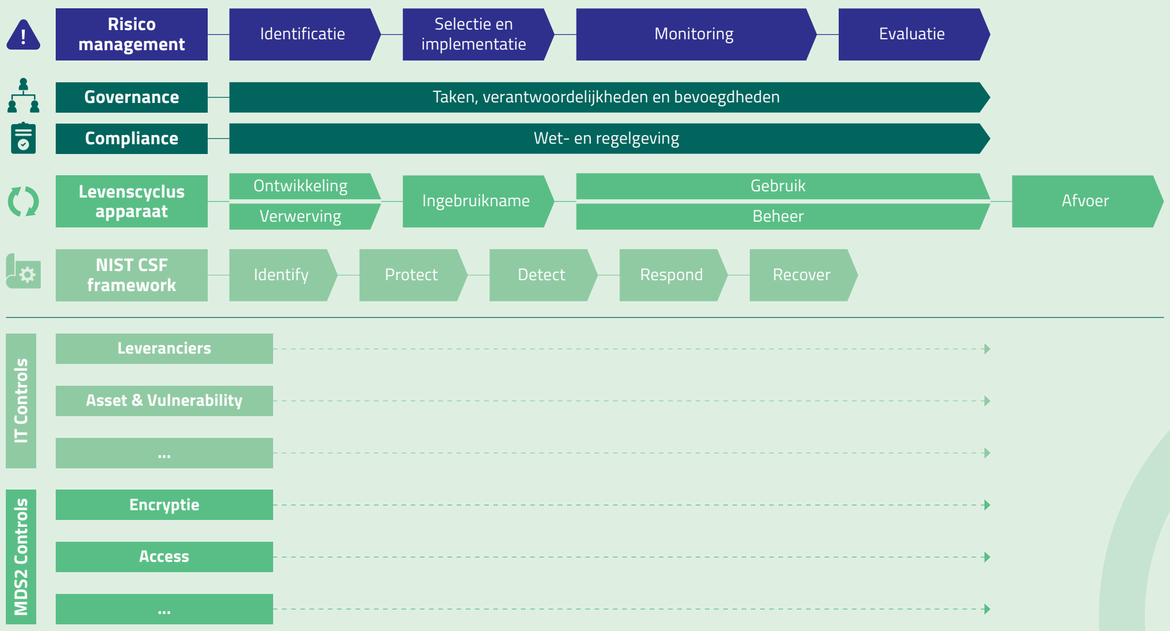
Veel van de waarde van de maturity scan komt voort uit het eerlijk invullen ervan met collega's. Z-CERT raadt u aan om met de volgende collega's de scan in te vullen:

- IT-manager
- Functionaris Gegevensbescherming
- (C)ISO
- Systeembeheerder

Trek hier, waar mogelijk, 1 à 2 uur voor uit. Dit zou moeten leiden tot een redelijk zuiver totaalbeeld van de stand van zaken omtrent informatiebeveiliging en privacy.



Raamwerk cybersecurity medische apparatuur



In zowel het schema, de NEN7510/ ISO2700x als het NIST-framework, staan risicomanagement, governance en compliance centraal. Het schema is van toepassing op alle fasen van medische apparatuur. Het initiële risicoprofiel bepaalt de maatregelen die moeten worden getroffen om het apparaat afdoende te beschermen en hiermee de patiëntveiligheid te garanderen. Actief risicomanagement waarborgt een blijvende effectieve werking van de maatregelen. In het raamwerk is een aantal maatregelen uit MDS2 en NIST opgenomen:

- MDS2 is als basis gebruikt voor de maatregelen die van toepassing kunnen zijn op het medische apparaat zelf (ook wel 1st layer genoemd).
- NIST is als basis gebruikt voor de maatregelen die van toepassing kunnen zijn rondom het medische apparaat (ook 2nd en 3rd layer genoemd).

Traffic light protocol

TLP:RED	NOT FOR DISCLOSURE	▪ Alleen voor deelnemers van het gesprek ▪ Vaak ter kennisgeving en voor eigen gebruik
TLP: AMBER	LIMITED DISCLOSURE	▪ Beperkt tot organisaties van deelnemers ▪ Mag gedeeld worden met deelnemers en partners op een need to know basis
TLP: AMBER +STRICT	LIMITED DISCLOSURE	▪ Delen beperkt alleen tot de organisatie (Your Organisation Only) ▪ Opmerking: als de bron het delen wil beperken tot alleen de organisatie, moet deze TLP:AMBER+STRICT specificeren
TLP: GREEN	LIMITED DISCLOSURE	▪ Beperkt tot gemeenschap ▪ Mag gedeeld worden met collega's, partnerorganisaties ▪ Niet via openbaar toegankelijke kanalen
TLP:CLEAR	NO LIMITED DISCLOSURE	▪ Voor iedereen ▪ Mag zonder beperking worden verspreid

Het TRAFFIC LIGHT PROTOCOL (TLP) is een richtlijn waarbij door middel van kleurcodering wordt aangegeven in hoeverre informatie gedeeld mag worden.

Het Traffic Light Protocol is gemaakt om effectiever te kunnen samenwerken met gevoelige informatie. TLP biedt een eenvoudig en intuïtief schema om aan te geven met wie mogelijk gevoelige informatie kan worden gedeeld. Binnen Z-CERT en haar deelnemers wordt gebruikgemaakt van het TLP-protocol. Z-CERT gebruikt de TLP-markering bijvoorbeeld bij webinars en advisories.

De verstrekker van TLP-gemarkeerde informatie is ervoor verantwoordelijk dat de ontvangers TLP-richtlijnen voor het delen van informatie begrijpen en kunnen naleven. Indien een ontvanger de informatie breder wil verspreiden dan aangegeven door de initiële TLP-markering, moet de verstrekker expliciet om toestemming worden gevraagd.

Hoe te gebruiken:

- E-mail: bij het versturen van een e-mail dient de TLP-markering van de informatie te worden aangeduid in de onderwerpregel en in de tekst van het e-mailbericht. De TLP-markering moet in hoofdletters met gebruikmaking van de kleur worden aangegeven: TLP:RED, TLP:AMBER, TLP:AMBER+STRICT, TLP:GREEN of TLP:CLEAR.
- In geschreven vorm MOETEN de TLP-markeringen geen spaties bevatten en MOETEN ze in hoofdletters staan. TLP-markeringen MOETEN in hun oorspronkelijke vorm blijven, zelfs wanneer ze in andere talen worden gebruikt: inhoud kan worden vertaald, maar de markering niet.

Meer informatie over TLP kunt u vinden op de website van het Forum of Incident Response and Security Teams (FIRST) **www.first.org/tlp/**

Incident Response

Security-incidenten zijn haast onvermijdelijk, 100% veiligheid bestaat immers niet. Een goede voorbereiding voorafgaand aan een incident is daarom zeer belangrijk. Met een goed incidentresponse-proces heeft u de juiste structuur en te nemen stappen klaarliggen voor als het nodig is. Hiermee kunt u iedere keer snel en adequaat reageren.

Er zijn diverse manieren om een incidentresponse-proces in te richten, instanties zoals NIST, ENISA en SANS bieden frameworks aan die u kunt gebruiken. Hoewel er verschillen zijn, is er een duidelijke lijn te vinden in de stappen die ieder incidentresponse-proces zou moeten bevatten. Dit zijn:

1

Voorbereiding

- Zorg voor de juiste faciliteiten;
- Bewaar belangrijke contactinformatie (Z-CERT, politie, collega's en leveranciers);
- Denk aan werkplekken en werkruimtes;
- Maak afspraken over wie er rapporteert en op welk moment.

2

Detectie, triage en analyse

- Zorg dat detectiemaatregelen aanwezig zijn en meldingen hiervan regelmatig gecontroleerd worden;
- Bied medewerkers duidelijke communicatiekanalen om meldingen te kunnen ontvangen;
- Doe aan triage. Dit voorkomt dat problemen worden onderschat en u later moet opschalen;
- Creëer inzicht. Klopt de melding? Wat is de impact? Wie zijn er getroffen?

3

Voorkomen verspreiding, wis geen sporen op weg naar herstel

- Voorkom verdere verspreiding. Isoleer geïnfecteerde werkplekken en servers van de rest van het netwerk;
- Zorg dat sporen van infectie achterhaald worden, leg deze vast en verwijder deze;
- Zet back-ups terug zowel van servers als werkplekken. Zorg voor offline en off-site back-ups.

4

Geleerde lessen

- Voorafgaande: Oefen geregeld een mogelijk security-incident, denk aan table-top oefeningen;
- Plan een meeting met stakeholders om dit te bespreken. Doe dit ook naderhand;
- Stel samen met de betrokkenen een verbeterplan op.

Kortom: blijf dit proces testen en verbeteren op basis van eerder opgedane ervaringen.

Incident? Bel dan direct!

Wat is een incident?

Elke gebeurtenis die communicatie, informatie of andere elektronische systemen compromitteert of het potentieel heeft om deze te compromitteren of de informatie die in deze systemen wordt opgeslagen, verwerkt of verzonden.

Voorbeelden van een incident

Meerdere van dezelfde phishingmails, aanval met ransomware, (poging tot) digitale inbraak/hack, verstoring digitale systemen (bij leverancier), (digitaal) datalek.

Hoe meldt u een incident?

Bel (24x7) ons speciale piketnummer, mail naar **CERT@z-cert.nl** of maak een melding via **portaal.z-cert.nl**.

Wanneer meldt u een incident?

Meld een incident altijd zo snel mogelijk bij Z-CERT. Zo kunnen we niet alleen u zo snel mogelijk helpen, maar mogelijk ook voorkomen dat andere zorginstellingen een zelfde incident zullen meemaken.

@z-cert.nl ieder doel een e-mailadres

CERT@z-cert.nl

Communicatie van operationele aard

- Het melden van incidenten en communicatie met 1e en 2e lijns support van Z-CERT en voor vragen over de TechOps-community

INFO@z-cert.nl

Communicatie van administratieve aard

- Doorgeven van mutaties van contactpersonen, IP-reeksen en domeinnamen
- Het stellen van algemene vragen aan Z-CERT of vragen over onze diensten
- Whitepapers, factsheets en uitnodigingen voor bijvoorbeeld webinars of kennissessies ontvangt u via dit mailadres

ZDN@z-cert.nl

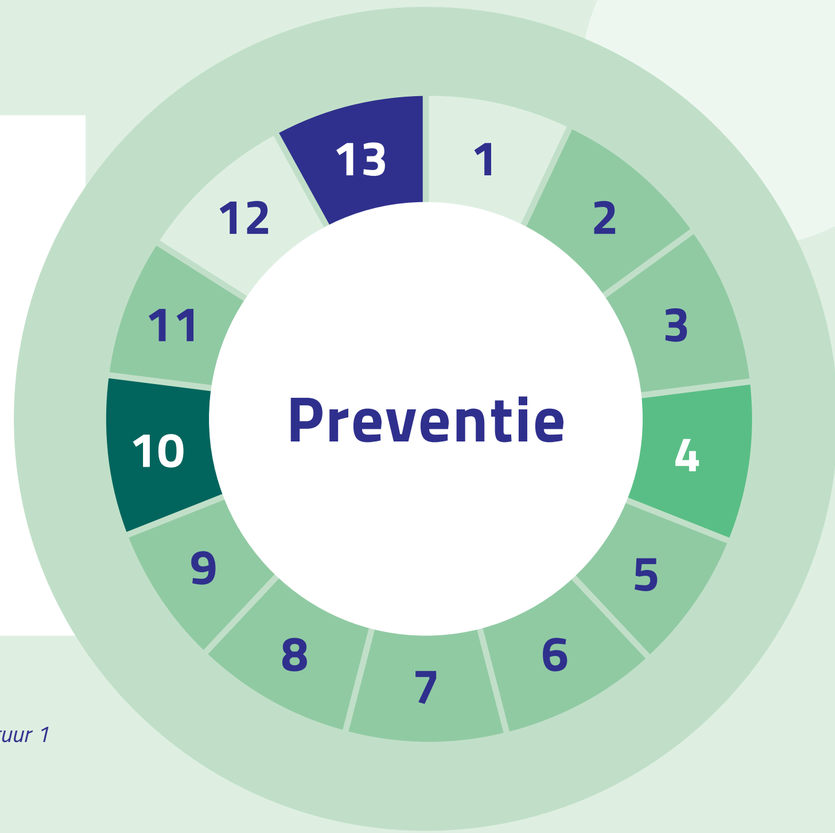
- Vragen over uw aansluiting op het Zorg Detectie Netwerk

Algemene gegevens

www.z-cert.nl of bel 033 - 737 06 09

Preventie van een **ransomware-incident**

Om een ransomware-incident te voorkomen kan men binnen de eigen zorgorganisatie een aantal maatregelen treffen. In *figuur 1* worden de belangrijkste maatregelen weergegeven die kunnen bijdragen aan de preventie van een ransomware-incident.



figuur 1

1.1 Applicatie whitelisting
Gebruik applicatie whitelisting en geef alleen betrouwbare software en code toegang tot de systemen en blokkeer de andere. Denk aan uitvoerbare bestanden, scripts, dll's, installers, packages en powershell.exe.

1.2 Office macro's
Wees terughoudend met het gebruik van Office macro's afkomstig van het internet. Blokkeer Office macro's van het internet of reguleer ze.

1.3 Patchmanagement
Stel binnen het patchmanagementproces prioriteiten en geef voorrang aan de kwetsbaarheden die voor zowel kans en impact ingeschaald zijn als high. Stel als doel om binnen 48 uur te patchen.

1.4 Op afstand werken
Zorg ervoor dat afstandswerkoplossingen zoals Remote Desktop Protocol, Teamviewer en VNC niet ontsloten zijn aan het internet. Deze mogen alleen via een beveiligde VPN of gateway-oplossing benaderbaar zijn.

1.5 Scan buitenkant IT-infrastructuur
Scan regelmatig de aan het internet ontsloten systemen op afwijkingen en kwetsbaarheden. Bijvoorbeeld de RDP die onbedoeld openstaat, of systemen die onbedoeld toegankelijk zijn via het internet.

1.6 Beveilig uw applicaties
Beveilig uw applicaties en controleer of de beveiligingsopties in webbrowsers optimaal worden benut. Er komen regelmatig functionaliteiten bij en schakel de niet gebruikte functionaliteiten met security-risico's uit, zoals OLE in Microsoft Office.

1.7 Least privilege principes
Gebruik een tiered administration model en geef geen localadmin rechten aan gebruikers. Geef alleen die rechten die noodzakelijk zijn voor het uitvoeren van de taken gedurende de tijd dat dit nodig is (JIT-admin oplossing).

1.8 Back-ups
Test het herstelproces regelmatig. Pas de 3-2-1-regel toe en zorg ook voor offline back-ups. Zorg ervoor dat de systemen waarop de back-ups worden bewaard niet toegankelijk zijn vanaf andere systemen.

1.9 Patch Operating Systems
Draai alleen versies van het operating system die ondersteund worden. Denk daarbij naast de servers en deskop-computers ook aan de medische- en netwerkappparaten. Zet systemen die niet kunnen worden geüpdatet achter de eigen firewall.

1.10 MFA
Gebruik multifactorauthenticatie voor toegang tot online diensten en voor alle externe toegangsoplossingen tot uw IT-infrastructuur.

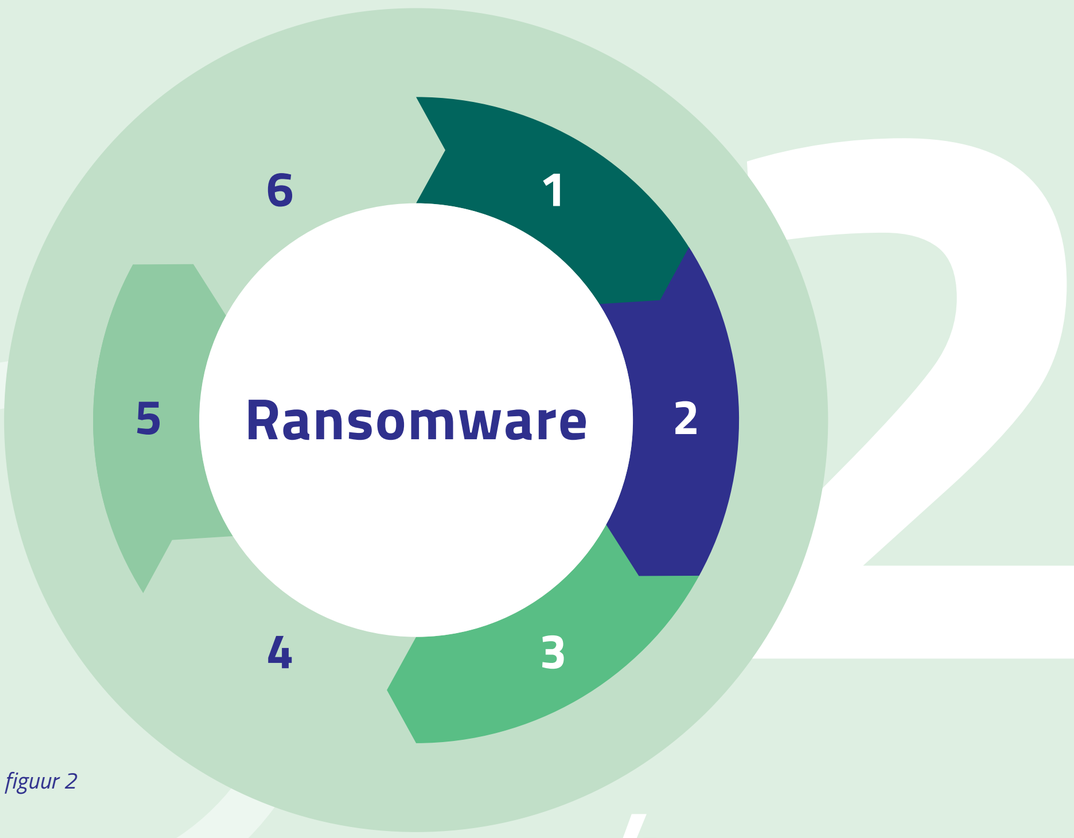
1.11 Endpoint Detection and Response
Installeer een Endpoint Detection and Response-tool zowel op de clients als op de servers.

1.12 Netwerksegmentatie
Implementeer netwerksegmentatie gebaseerd op functie, data classificatie en aanvalsmethodieken en maak hierbij gebruik van verschillende firewalls.

1.13 Awareness
Zorg voor kennis en bewustzijn bij medewerkers over phishing varianten en het herkennen hiervan, het signaleren van social engineering, de verspreiding van malware en ransomware, het herkennen van een ransomware-besmetting en hoe hierop te reageren, hoe verdachte waarnemingen of mogelijke besmettingen (eenvoudig) gemeld kunnen worden, het gebruik van verschillende wachtwoorden voor verschillende systemen en omgevingen, het social mediabeleid van de organisatie. Organiseer regelmatig Cybersecurity awareness trainingen binnen de zorgorganisatie.

Krijgt uw zorgorganisatie, ondanks de getroffen preventieve maatregelen, te maken met een ransomware-incident?

Dan is het raadzaam om een incidentresponse-plan paraat te hebben. Hierbij doorloopt u systematisch een aantal stappen die moeten leiden tot het herstel van de IT-infrastructuur en data. In *figuur 2* worden de belangrijkste stappen van een incidentresponse-plan weergegeven.



figuur 2

Let op:
Punten met dezelfde kleur staan met elkaar in verbinding. Zo is punt 1.13 gelinkt aan punt 2.2.

2.1 Inventarisatie
1. Breng in kaart welke systemen er zijn en welke zijn getroffen en wat de functie van de systemen is en wie er verantwoordelijke is voor het systeem en voer een impactassessment uit. Identificeer hierbij Patient Zero.
2. Let op malafide communicatie of netwerkverkeer, zoals bijvoorbeeld bekende patronen van exploit kits of verbindingen met bekende C2-servers. Let op ongebruikelijk netwerk of browse activiteit, ongebruikelijke e-mails met koppelingen naar verdachte of malafide websites of ongebruikelijke bijlagen in e-mails.
3. Let op het (achtereenvolgens) aanpassen van grote hoeveelheden bestanden op een (netwerk) bestandssyteem of op het signaal dat er data wordt weggesluisd.
4. Verricht onderzoek naar ongebruikelijke binaries, forensische images van het geheugen, ongebruikelijke processen (of taken) in de Taakplanner. Onderzoek ongebruikelijke patronen van e-mail bijlagen en/of netwerk- of browse-activiteit (bijv. TOR/crypto).

2.2 Contact
1. Bepaal de communicatiestrategie wanneer de gestolen data wordt gepubliceerd. Wie binnen de zorgorganisatie informeert wie? Welke berichten moeten worden verstuurd?
2. Bepaal welke toezichthouders geïnformeerd moeten worden. Denk hierbij ook aan het eventueel doen van een melding bij de Autoriteit Persoonsgegevens.
3. Moet de politie worden ingeschakeld of het NCSC of Z-CERT?
4. Bepaal een strategie voor het omgaan met de ransom note:
   - wie moet ingeschakeld worden om het gesprek aan te gaan met gijzelnemers
   - welke informatie moet in een onderhandeling vastgesteld worden
   - hoe wordt met de eis om losgeld omgegaan
   - wie doet wanneer aangifte of maakt melding bij de politie
5. Bepaal een interne/externe communicatiestrategie voor de zorgorganisatie:
   - wie moet er worden betrokken bij een cybersecurity incident?
   - gebruik een standaard overlegstructuur in crisisoverleggen (Beeld, Oordeelsvorming, Besluitvorming).
6. Zorg ervoor dat intern en extern de stakeholders duidelijk zijn. Zoals bijvoorbeeld de eigen medewerkers, de persvoorlichting, de ketenpartners, de klanten, de Raad van Bestuur, de DPO, de juridische afdeling. Informeer de stakeholders tijdig.

2.3 Mitigatie
1. Koppel direct systemen los van het netwerk (op alle interfaces: bekabeld, wifi of mobiel) waarvan is vastgesteld of het vermoeden bestaat dat deze gecompromitteerd zijn. Verbreek mogelijk de verbinding met netwerken of netwerkdelen die nog niet zijn getroffen door de ransomware.
2. Verzamel relevante logbestanden (Windows,Security, Emaillogs, Firewall logs en Linux System Logs).
3. Indien een ketenpartner is besmet, blokkeer dan de uitwisseling van e-mail en netwerkverkeer met deze organisatie totdat duidelijk is dat het besmettingsrisico geweken is.
4. Zet de systemen in de slaapstand en niet uit om de toestand van het systeem niet te verstoren en zo het beste beeld te kunnen verkrijgen en om te voorkomen dat aanwezig sleutelmateriaal verloren gaat en om forensische sporen te verliezen voor mogelijk onderzoek.
5. Blokkeer of deactiveer alle accounts die (mogelijk) bij de ransomware-aanval betrokken zijn.
6. Reset wachtwoorden en andere vormen van authenticatie voor administrator- en andere systeem- of service accounts en reset wachtwoorden voor gebruikers.
7. Blokkeer het verkeer met de mogelijk vastgestelde C2-servers.
8. Lever kenmerken van de nog onbekende malware die is gevonden of de forensische analyse aan bij de ESP. Rapporteer het incident zo vroeg mogelijk om verdere schade binnen de zorgsector te voorkomen.
9. Stel IOC's vast en blokkeer bekende malware (communicatie) en update antivirus signatures zodat de geïdentificeerde malware wordt geblokkeerd.

2.4 Eliminatie
1. Zorg ervoor dat de gehele scope van de aanval in kaart is gebracht voordat men overgaat tot het elimineren van de ransomware. Er dient uitgesloten te zijn dat er nog geïnfecteerde systemen aanwezig zijn.
2. Herinstalleer de getroffen systemen met een schone image nadat eventueel lokaal opgeslagen data en bestanden in quarantaine zijn geplaatst.
3. Voer in dit kader ook de interne en externe communicatiestrategie uit. Zorg dat stakeholders tijdig worden geïnformeerd.

2.5 Herstel
1. Gebruik alleen veilig verklaarde systemen voor herstel en indien er sprake is van een grote ransomware-aanval bouw de systemen parallel aan de bestaande systemen op.
2. Importeer geen systemen of gegevens zonder grondige controle op aanwezigheid malware en sluit geen systemen aan op de schone omgeving die mogelijk verbonden zijn met de besmette omgeving.
3. Ga na of er decryptiesleutels of -software beschikbaar is voor de ransomware die gebruikt is.
4. Scan de back-ups op malware voordat deze worden teruggezet.
5. Herstel de versleutelde of gecompromitteerde servers of systemen uit een niet gecompromitteerde back-up.
6. Upgrade en update de verouderde software en systemen.
7. Deel (technische) informatie over het incident met de politie los of tijdens de aangifte. Dit kan de (internationale) opsporing en verstoring van dadergroepen helpen en het kan leiden tot het notificeren van andere (potentiële) slachtoffers.
8. Als het niet lukt om de informatie te ontsleutelen of te herstellen uit een back-up en er is dataverlies, dan kan een kopie van de versleutelde informatie bewaard worden.
9. Corrigeer ongewenste configuratieaanpassingen die eventueel door kwaadwillenden zijn doorgevoerd. Test en verifieer of het afwijkende gedrag (o.a. het netwerkverkeer) is verdwenen na het herstellen van alle systemen en processen.

2.6 Evaluatie
1. Evalueer de doorlopen stappen van het incidentresponse-plan en verwerk dit in een rapportage.
2. Denk na over de door te voeren wijzigingen binnen de zorgorganisatie om toekomstige vergelijkbare incidenten te voorkomen of de impact ervan te verkleinen. M.b.t.:
   - Systeemaanpassing en technische wijzigingen;
   - Aanpassingen in procedures en beleid;
   - Aanpassingen in incidentresponse-procedures of in specifieke incidentresponse-plannen.
3. Deel de gevonden indicatoren en de rapportage met Z-CERT, zodat eventueel andere organisaties gewaarschuwd of geïnformeerd kunnen worden.
4. Rapporteer over het incident en neem informatie op over onder andere de initiële besmetting, de geraakte systemen, de impact op de beschikbaarheid, invloed op de afhankelijkheden van (keten)partners/ klanten, leveranciers of andere stakeholders.
   - kenmerken van de gebruikte ransomware
   - risico's van mogelijk gelekte gegevens in de buitenwereld
   - effectiviteit en uitvoering van het incidentrespons proces
   - kosten doorlooptijd van het incident
   - welke documentatie dient aangepast te worden op basis van de geleerde punten en welke persoon binnen de organisatie gaat dat doen.

Z-CERT Stationsplein 121, 3818 LE Amersfoort **www.z-cert.nl**