Beknopt overzicht van bedreigingen en maatregelen

Dit voorbeelddocument omvat een beknopt overzicht van bedreigingen en maatregelen. De opgesomde componenten, bedreigingen en maatregelen zijn bedoeld om een eerste aanzet te geven voor het bepalen de relevante bedreigingen en maatregelen. Het pretendeert niet volledig te zijn en één op één aan te sluiten op de situatie binnen de praktijk.

De opgesomde maatregelen hebben geen directe relatie met de indeling van de NEN7510. Het moet beschouwd worden als achtergrondmateriaal en kan als inspiratie dienen bij het uitvoeren van een risicoanalyse en het bepalen van de gewenste maatregelen voor de beveiliging van een informatiesysteem.

Inleiding

Onderstaand overzicht bevat per mogelijke componenten een beknopte opsomming van mogelijke bedreigingen en maatregelen die van toepassing kunnen zijn op de informatiesystemen. Deze beknopte opsomming is gebaseerd op een vanuit de norm opgestelde lijst met essentiële onderwerpen. Het overzicht kan als eerste aanzet dienen bij het definiëren van componenten, bedreigingen en maatregelen van individuele informatiesystemen. Bovendien kan het worden gebruikt bij de bewustwording voor een structurele aanpak voor informatiebeveiliging. In het tweede overzicht is van de in het eerste overzicht benoemde maatregelen een uitgebreide omschrijving te vinden.

Overzicht componenten, bedreigingen en maatregelen

Component	Omschrijving van bedreiging	Maatregelen
Mensen		
Gebruikers	Gebruikers maken onopzettelijke fouten door onkunde, slordigheid of stress.	M006, M401: Opleidingen M601-603: Werkinstructies
	Gebruikers maken onopzettelijke fouten door onvoldoende of foutieve organisatorische sturing (AO beschrijvingen, procedures en instructies) en borging van kennis.	M601-603: Werkinstructies M404: Scholing inzake beleid en procedures M405: Functiebeschrijvingen
	Gebruikers maken onopzettelijke fouten door een complexe en foutgevoelige bediening.	M407: Verplichte melding zwakke plekken M408: Procedure rapporteren onvolkomenheden informatiesystemen
Programmatuur		
Applicatieprogrammatuur	Bij de installatie van nieuwe programmatuur wordt al dan niet bewust een virus geïntroduceerd waardoor de programmatuur niet meer juist functioneert (d.w.z. regelmatig uitvalt of gegevens niet op de juiste manier verwerkt).	M038: Maak schriftelijke afspraken met de relevante dienstverlener (ICT diensten, externe partijen) omtrent de bescherming tegen kwaadaardige programmatuur M014: Controleer naleving afspraken M036: Procedure voor incidentmanagement en –afhandeling M901: Noodprocedures
Server- en Netwerkprogrammatuur	Bij de installatie van nieuwe systeem- of toepassingprogrammatuur wordt al dan niet bewust een virus geïntroduceerd waardoor de server niet meer juist functioneert (d.w.z. regelmatig uitvalt of gegevens niet op de juiste manier verwerkt).	M038: Schriftelijke afspraken dienstverlener (ICT diensten, externe partijen omtrent de bescherming tegen kwaadaardige programmatuur M014: Controleer naleving afspraken M036: Procedure voor incidentmanagement en –afhandeling M901: Noodprocedures M903: Actueel houden noodprocedures

Component	Omschrijving van bedreiging	Maatregelen
Werkstationprogrammatuur	Bij de installatie van nieuwe systeem- of toepassingprogrammatuur wordt al dan niet bewust een virus geïntroduceerd waardoor het werkstation niet meer juist functioneert (d.w.z. regelmatig uitvalt of gegevens niet op de juiste manier verwerkt).	M038: Schriftelijke afspraken dienstverlener (ICT diensten, externe partijen omtrent de bescherming tegen kwaadaardige programmatuur M014: Controleer naleving afspraken M036: Procedure voor incidentmanagement en –afhandeling
	Gebruikers veranderen bewust of onbewust systeeminstellingen van de systeemprogrammatuur waardoor deze niet meer juist functioneert (d.w.z. regelmatig uitvalt of gegevens niet op de juiste manier verwerkt).	M401-403: Algemene trainingen, informatiebeveiligingstrainingen, bewustwording belang informatiebeveiliging M406: Disciplinaire maatregelen M618: Reservekopieën M734: Beperking toegang tot systeeminstellingen
	Gebruikers installeren (illegale) programmatuur waardoor het werkstation niet meer juist functioneert (d.w.z. regelmatig uitvalt of gegevens niet op de juiste manier verwerkt).	M401-403: Algemene trainingen, informatiebeveiligingstrainingen, bewustwording belang informatiebeveiliging M406: Disciplinaire maatregelen M618: Reservekopieën M1001: Gedragscodes, voorlichting misbruik
Gegevens		
Inhoud database	Gegevens zijn tijdelijk niet beschikbaar (bijv. door virussen, problemen met applicaties, fouten die hersteld moeten worden.)	M038: Schriftelijke afspraken dienstverlener (ICT diensten, externe partijen omtrent de bescherming tegen kwaadaardige programmatuur M014: Controleer naleving afspraken M036: Procedure voor incidentmanagement en –afhandeling M901: Noodprocedures M903: Actueel houden noodprocedures

Component	Omschrijving van bedreiging	Maatregelen
	Informatie die via het internet wordt verstrekt aan klanten wordt door ongeautoriseerde gebruikers verwijderd of gewijzigd.	M052: Vastleggen taken en verantwoordelijkheden omtrent autoriseren, uitvoeren wijzigingen
Gegevensdragers	Gegevensdragers (incl. back-ups) raken beschadigd door vuur, vocht, magnetische velden of verkeerde behandeling.	M055: Maak schriftelijke afspraken met de relevante dienstverlener (facilitaire diensten) omtrent het te realiseren beveiligingsniveau van gebouwen etc. M014: Controleer naleving afspraken
	Gegevensdragers (incl. back-ups) gaan verloren door diefstal, fout bij verzending of raken op een andere manier zoek.	M201: Toegang derden M409: Screening personeel (diefstal) M509, 510: Beveiligde ruimten M618: Reservekopieën M624-626: Beheer van verwijderbare computermedia op centraal beheerde apparatuur
	Gegevensdragers worden niet (juist) gewist bij hergebruik of afvoer waardoor gegevens aan ongeautoriseerde medewerkers of buitenstaanders ter beschikking komen.	M058: Schriftelijke afspraken met dienstverlener over het wissen van gegevensdragers bij afvoer M014: Controleer naleving afspraken M059: Vernietigen voor afvoer
Documentatie	Inzichtelijk voor derden (bijv. door afgevoerde dossiers in afvalbakken, documenten bij printer of kopieermachine)	M049: Gescheiden afvalverwerking M060: Gebruik van lokale printers M501: Clean desk
Organisatie		
Wet- en regelgeving	Er wordt niet voldaan aan de WBP.	M077, M079, M082, M084,M085: Implementatie wetgeving WBP
Gebruikersorganisatie	Taken, bevoegdheden en verantwoordelijkheden zijn onvoldoende beschreven of geïmplementeerd (hieronder wordt ook de aanwezigheid en gebruik van autorisatieniveaus in de toepassingsprogrammatuur verstaan).	M601: Formaliseer taken, bevoegdheden en verantwoordelijkheden M729–731: Toegangsbeveiliging voor programmatuur M732: Minimale toegangsrechten

Component	Omschrijving van bedreiging	Maatregelen
	Er is onvoldoende controle op de werkzaamheden van gebruikers waardoor bewuste of onbewuste fouten niet opgemerkt worden en foutief gebruikersgedrag niet wordt gecorrigeerd.	M406: Disciplinaire maatregelen M604: Functiescheiding en managementsupervisie
Beheerorganisatie	Taken, bevoegdheden en verantwoordelijkheden zijn onvoldoende beschreven of geïmplementeerd.	M601: Formaliseer taken, bevoegdheden en verantwoordelijkheden
Diensten		
Uitbestede diensten	Diensten zijn tijdelijk of definitief niet meer te leveren door de dienstverlener (bijvoorbeeld door faillissement, leegloop, afstoten van taken of het niet verlengen van een service overeenkomst, staking, slecht capaciteitsbeheer, verlegging van prioriteiten naar andere klanten en dergelijke.).	M072: Sluit mantelovereenkomsten met betrouwbare partijen

Overzicht van maatregelen

Nr.	Omschrijving maatregelen
M006	Alle medewerkers krijgen voldoende opleidingen om hun werkzaamheden naar behoren te kunnen vervullen.
M008	Werkplekken zijn voorzien van schermbeveiliging met wachtwoordcontrole.
M009	Gebruikers worden automatisch uitgelogd uit een toepassingsprogramma na een bepaalde periode van inactiviteit.
M014	De naleving van vastgelegde afspraken wordt gecontroleerd.
M036	Er is een procedure voor incidentmanagement en -afhandeling.
M038	Er zijn schriftelijke afspraken met de relevante dienstverlener (ICT diensten, externe partijen) gemaakt omtrent de bescherming tegen kwaadaardige programmatuur.
M049	Afvoer van documenten is gescheiden van het reguliere afval (evt. in combinatie met het gebruik van een papierversnipperaar).
M052	Taken en verantwoordelijkheden omtrent informatieverstrekking via internet worden vastgelegd (Wie mag wijzigingen autoriseren, wie mag wijzigingen uitvoeren).
M055	Er zijn schriftelijke afspraken met de relevante dienstverlener (facilitaire diensten) gemaakt omtrent het te realiseren beveiligingsniveau van gebouwen, computerruimten, werkplekken etc.
M058	Er zijn schriftelijke afspraken met de relevante dienstverlener (ICT dienstverleners) gemaakt over het wissen van gegevensdragers bij afvoer.
M059	Gegevens worden vernietigd voor het afvoeren van gegevensdragers.
M060	Wanneer mogelijk worden lokale printers gebruikt.
M072	Mantelovereenkomsten worden alleen afgesloten met betrouwbare partijen.
M077	Persoonsgegevens worden alleen voor een bepaald gerechtvaardigd doel verwerkt.
M079	Persoonsgegevens worden zo min mogelijk verspreid door de instelling. Ze zijn alleen beschikbaar voor wie ze echt nodig heeft.
M082	Persoonsgegevens worden niet onbeheerd (op het bureau) achtergelaten.
M084	De zorgafnemer heeft de mogelijkheid inzage te krijgen welke persoongegevens over hem voor welk doel worden verzameld.
M085	De zorgafnemer dient de mogelijkheid te hebben om persoongegevens te laten corrigeren .
M201	Elke systeemeigenaar heeft een overzicht van de toegang door derden tot de informatieverwerkende voorzieningen.
M401	Alle gebruikers krijgen een training in het correct gebruik van de ICT-voorzieningen, bijvoorbeeld logon-procedures, het gebruik van programmatuur, etc., voordat zij toegang krijgen tot deze voorzieningen.
M402	Bij de introductie van nieuw personeel in de zorginstelling wordt aandacht aan informatiebeveiliging besteed en de trainingen gegeven.
M403	Alle gebruikers worden bewust gemaakt van het belang van de informatiebeveiliging voor hun werkzaamheden.
M404	Alle gebruikers en, indien van toepassing , ook externe gebruikers, krijgen een passende training en regelmatig nascholing inzake het beleid en procedures van de zorginstelling.
M405	Taken worden beschreven in functiebeschrijvingen en (arbeids)contracten.
M406	Disciplinaire maatregelen.

Nr.	Omschrijving maatregelen
M407	Gebruikers van informatievoorziening zijn verplicht alle zwakke plekken in of bedreigingen van de beveiliging van systemen of diensten die zij opmerken of vermoeden te rapporteren aan de informatiebeveiligingscoördinator van hun dienst/afdeling.
M408	Er is een procedure bij de gebruikers bekend hoe te handelen bij onvolkomenheden in informatievoorzieningen.
M409	Aanstelling van een functionaris op een vertrouwensfunctie geschiedt eerst nadat de functionaris is gescreend.
M501	Clear desk en clear screen policy: De gebruiker van een werkplek is verantwoordelijk voor het voldoen aan de geldende wet- en regelgeving.
M509	Beveiligde zones zijn beschermd door adequate toegangsbeveiliging, zodat alleen geautoriseerd personeel toegang heeft.
M510	Personeel van derden heeft zonder begeleiding geen toegang tot de computerruimten.
M601	Er zijn verantwoordelijkheden en procedures en werkinstructies vastgesteld voor het beheer en de bediening van alle ICT-voorzieningen.
M603	De bedieningsprocedures bevatten gedetailleerde instructies voor de uitvoering van alle taken, bijvoorbeeld de verwerking en behandeling van gegevensbestanden.
M604	Bepaalde taken, bevoegdheden en verantwoordelijkheden worden gescheiden en verdeeld over meer personen om de kansen op ongeautoriseerde wijzigingen of misbruik van gegevens of diensten te verkleinen.
M618	Er worden regelmatig reservekopieën gemaakt van gegevens en programmatuur.
M619	Bescherming tegen kwaadaardige programmatuur: Er zijn procedures ingevoerd om het bewustzijn van de gebruikers te vergroten.
M624	Er zijn procedures opgesteld voor het beheer van verwijderbare computermedia, zoals banden, schijven, cassettes en (optische)diskettes.
M625	Alle procedures en autorisatieniveaus zijn duidelijk gedocumenteerd.
M626	In de procedures wordt aandacht besteed aan opslag van, autorisatie tot en identificatie van computermedia.
M701	Gebruikers zijn persoonlijk verantwoordelijk voor zorgvuldig beheer en gebruik van hun wachtwoorden.
M706	De toewijzing van wachtwoorden wordt beheerd aan de hand van een formele procedure.
M707	Wachtwoorden worden nooit in een onbeveiligde vorm in een computersysteem opgeslagen.
M708	Wachtwoorden zijn nooit zichtbaar voor derden.
M714	Alle gebruikers worden gewezen op de beveiligingseisen en procedures ter beveiliging van onbeheerde apparatuur, en op hun verantwoordelijkheid hiervoor.
M729	Er zijn beveiligingsvoorzieningen getroffen om de toegang binnen toepassingssystemen en de onderliggende gegevens te beperken.
M730	Elke applicatie vereist een toegangsautorisatie.
M731	De systeemeigenaar heeft een autorisatieprocedure voor zijn systemen.
M732	Een gebruiker van een toepassingssystemen krijgt alleen toegang tot gegevens en functies welke nodig zijn voor de uitvoering van de opgedragen taak.
M734	Toegang tot systeeminstellingen wordt beperkt.
M901	Er is een proces van continuïteitsplanning geïmplementeerd waarmee de verstoring als gevolg van calamiteiten en ontregeling van de beveiliging tot een aanvaardbaar niveau is beperkt met een combinatie van preventieve en herstelmaatregelen.

Nr.	Omschrijving maatregelen
M903	Continuïteitsplannen worden bijgehouden en geoefend, zodat ze een integraal deel van alle andere beheersprocessen vormen.
M1001	Het gebruik van ICT-voorzieningen voor niet-zakelijke doeleinden wordt gereguleerd (d.m.v. een gedragscode, voorlichting e.d.).