Factor	Omschrijving van de dreiging	Kans	Impact	Risico	B	I	V	Mogelijke maatregelen	Kans	Impact	Risico
Mens (0onbewust)	Onzorgvuldige omgang met wachtwoorden	2	4	8	X	X	X	Spreek medewerkers aan op het niet delen van wachtwoorden. Persoonlijke accounts.	1	4	4
Mens (0onbewust)	Onvoldoende kennis/training	2	4	8		X		Train nieuwe medewerkers bij in dienst. Evalueer het werken van bestaande medewerkers.	1	4	4
Mens (0onbewust)	Niet werken volgens voorschriften/procedures	2	4	8		X	X	Evalueer het werken van bestaande medewerkers.	1	4	4
Mens (0onbewust)	Fraude/diefstal/lekken van informatie	1	4	4	X	X	X	Zorg voor bewustwording. Spreek medewerkers aan.Zorg voor gedragscode en geheimhoudingsverklaring. Datalekken melden.	1	4	4
Mens (0onbewust)	Ongeautoriseerde toegang met account van medewerker met hogere autorisaties	1	4	4		X	X	Spreek medewerkers aan op het niet delen van wachtwoorden. Enkele inlog toestaan. Log activiteiten.	1	4	4
Mens (bewust)	Onzorgvuldige omgang met wachtwoorden	3	4	12		X	X	Spreek medewerkers aan op het niet delen van wachtwoorden. Enkele inlog toestaan. Log activiteiten.	1	4	4
Mens (bewust)	Niet werken volgens voorschriften/procedures	3	4	12	X	X	X	Evalueer het werken van bestaande medewerkers.	1	4	4
Mens (bewust)	Fraude/diefstal/lekken van informatie	4	4	16	X	X	X	Blokkeer functionaliteiten, Privacy by design. Enkele inlog toestaan. Log activiteiten.	2	3	6
Mens (bewust)	Ongeautoriseerde toegang met account van medewerker met hogere autorisaties	2	4	8	X	X	X	Spreek medewerkers met hogere autorisaties aan op het niet delen van wachtwoorden. Enkele inlog toestaan. Logging en monitoring	1	4	4
Apparatuur	Diefstal/schade	2	3	6	X		X	Encryptie op de gegevensdrager. Vergrendel scherm na x tijd. Zorg voor beveiligde ruimtes en kluisjes.	1	3	3
Apparatuur	Verkeerde instellingen	1	4	4	X			Mak gebruik van SCOM monitoring, patch systemen tijdig. Voer controle uit.	1	4	4
Apparatuur	Beschadiging/vernieling	3	2	6	X			Omgangsregels met apparatuur, medewerker aansprakelijkheid	2	2	4
Apparatuur	Verlies/diefstal (onder andere. verlies USB-sticks of andere gegevensdrager)	1	4	4	X		X	Encryptie op gegevensdrager	1	3	3
Programmatuur	Ontwerp-, programmeer-, invoering, beheer/onderhoudsfouten	3	4	12	X	X	X	Review functionaliteiten. Evaleer met medewerkers/beheerders. Escaleer indien nodig.	2	3	6
Programmatuur	(Ongeautoriseerde) functieverandering en/of toevoeging	1	4	4	X	X	X	Inrichten procedure voor autorisatiewijzigingsverzoeken adhv mandaatregister. Autorisatiematrix. Controle op autorisaties.	1	4	4
Programmatuur	Installatie van virussen, Trojaanse paarden en dergelijke	2	4	8	X			Instructie op phishingmails. Blokkeren executables.	1	4	4
Programmatuur	Kapen van autorisaties van collega's	2	4	8	X	X	X	Versterk wachtwoorden naar min. 12 karakters. Monitoring van logs	1	4	4
Gegevens	Diefstal/zoekraken/lekken	3	4	12	X		X	Uitschakelen print en dumpfunctionaliteiten. Logging en monitoring.	2	4	8
Gegevens	Foutieve of geen versleuteling	3	3	9		X	X	Encryptie op database	2	3	6
Gegevens	Foutieve of vervalste gegevens	3	3	9		X	X	Ondersteuningstool bij invoer. Validatie van gegevens. Logging en monitoring.	2	2	4
Gegevens	Ongeautoriseerde toegang door onbevoegden (hackers/hosters)	3	4	12	X	X	X	Logging en monitoring. 2FA inrichten. Enkele inlog toestaan.	2	4	8
Gegevens	Ongeautoriseerde wijziging of verwijdering van gegevens	3	4	12	X	X	X	Logging en monitoring. Enkele inlog toestaan.	2	4	8
Gegevens	Onvoldoende toegangsbeperking tot apparatuur	2	4	8	X		X	Versterk wachtwoorden naar min. 12 karakters. 2FA. Monitoring van logs	1	4	4
Gegevens	Doorwerking van virussen/malware	2	4	8	X	X	X	Inrichten Firewall/IDP/IDS. Monitoring en Logging. Zorg voor bewustwording.	1	3	3
Gegevens	(On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data	3	4	12		X	X	Logging en monitoring. Gebruik persoonlijke accounts. Evalueer werk.	2	3	6
Gegevens	Onbevoegde toegang door onbevoegden	3	4	12			X	Logging en monitoring. Gebruik persoonlijke accounts. Controle op autorisaties. Controle op kitische functionaliteiten en gebruik.	2	3	6
Gegevens	Onbevoegd kopiëren van gegevens	4	4	16	X		X	Uitschakelen print en dumpfunctionaliteiten. Dataminimalisatie. Logging en monitoring.	2	3	6
Gegevens	Meekijken over de schouder door onbevoegden	3	4	12	X		X	Zorg voor bewustwording	2	4	8
Gegevens	Onzorgvuldige vernietiging	2	4	8	X		X	Afspraken over vernieting van documenten. Proces inrichten om gegevens te vernietigen op verzoek.	1	4	4
Gegevens	Niet toepassen clear screen/clear desk	3	3	9	X	X	X	Zorg voor bewustwording. Spreek elkaar aan. Automatische vergrendeling na 15 minuten.	2	3	6
Gegevens	Oneigenlijk gebruik van autorisaties	2	4	8	X	X	X	Zorg voor bewustwording. Spreek elkaar aan op verwachtingen bij het werken met vertrouwelijke gegevens.	1	4	4
Gegevens	Toegang verschaffen tot gegevens door middel van identiteitsfraude of social engineering	4	4	16			X	Indien vertrouwelijke gegevens worden gedeeld altijd vragen naar legitimatie. Dit geldt ook organisatiebreed!	3	4	12
Organisatie	Onvoldoende interne controle	3	3	9		X	X	Richt steekproeven in op naleving van regels.	2	3	6
Organisatie	Onvoldoende toetsing op richtlijnen	2	3	6		X	X	Toets regelmatig op kennisnieveau van medewekers. Breng richtlijnen onder de aandacht.	1	3	3
Organisatie	Onvoldoende kwaliteitsborging	3	3	9		X	X	Evalueer regelmatig. Richt steekproeven in op naleving van regels.	2	3	6
Organisatie	Onvoldoende beheer van systemen en middelen	2	4	8	X	X	X	Dubbel bemensen van beheertaken. Controle en monitoring van beheer.	1	4	4
Omgeving	Ongeautoriseerde toegang tot gebouw(en)	2	4	8	X	X	X	Zorg voor bewustwording. Spreek elkaar aan. Spreek bezoekers aan. Scherp inrichten toegangspassen.	1	4	4
Omgeving	Diefstal op werkplekken	2	4	8	X		X	Scherp inrichten toegangspassen. Sociale controle. Vergrendel schermen. Berg spullen op in lockers.	1	3	3
Omgeving	Gebreken in ruimtes, waardoor kans op insluiping/inbraak	2	3	6	X		X	Regelmatig beoordelen van werkruimtes. Laagdrempelig signaleren.	1	3	3
Diensten	Slecht opgeleid personeel	4	3	12		X	X	Train nieuwe medewerkers bij in dienst. Evalueer het werken van bestaande medewerkers.	2	3	6
Diensten	Groot personeelsverloop (in, door en uitsroom)	3	2	6			X	Train nieuwe medewerkers bij in dienst. Evalueer het werken van bestaande medewerkers.	2	2	4
Diensten	Onvoldoende capaciteit in personeel	3	2	6	X		X	Train nieuwe medewerkers bij in dienst. Evalueer het werken van bestaande medewerkers.	2	2	4
Diensten	Onvoldoende of geen kwaliteitsborging	3	2	6	X	X	X	Evalueer regelmatig. Richt steekproeven in op naleving van regels.	2	2	4
Diensten	Personeel voldoet niet aan eisen zoals een geldige VOG en getekende geheimhoudingsverklaringen	3	3	9		X	X	Strak inrichten van proces en controle op uitvoer. Regelmatig steekproeven .	1	3	3
Diensten	Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie	3	4	12	X	X	X	Logging en monitoring. Breng disciplanire maatregelen onder de aandacht.	2	3	6
Diensten	Maakt gebruik van te zware autorisatie, niet functie gebonden	4	3	12		X	X	Autorisaties inrichten op basis van autorisatieschema. Regelmatig evalueren. Alleen persoonsgebonden accounts. Evalueer bevoegdheden.	2	2	4
Diensten	Levert diensten niet conform overeenkomst	3	3	9	X	X	X	Controle op dienstverlener. Dienstverlener richt eigen kwaliteitsproces in.	2	3	6