Tabel voor Risicobeoordeling

geïmplementeerd van [datum] tot [datum]

Nr	Naam bedrijfsmiddel	[illegible]	Bedreiging	[illegible]	Risico-eigenaar	[illegible]	[illegible]	Risico	Bestaande maatregelen

Categorieën van bedrijfsmiddelen

Het volgende zijn voorbeelden van informatiebedrijfsmiddelen die te vinden zijn in de organisatie.
Deze lijst is niet uitputtend. Elek organisatie dient haar eigen bedrijfsmiddelen te specificeren welke b

Mensen

- directie (leden van de directie, leden van de Raad van Toezicht, managers bedrijfsonderd
- midden management
- werknemers - experts (bijv. systeembeheerders, ontwikkelaars, beveiligingsexperts, enz.)
- andere werknemers
- tijdelijke externe werknemers
- externe bezoekers

Applicaties en databases

- applicatiesoftware (licenties)
- freeware; shareware
- systeemsoftwaare
- verschillende tools
- databases

Documentatie (in papieren of elektronische vorm)

- contracten
- correspondentie met cliënten en partners
- registraties
- logboeken
- handleidingen
- normen
- ontvangsten
- apparatuur documentatie
- trainingsdocumentatie
- interne documents
- besluiten
- rapporten
- plannen
- boekhoudadministratie
- werknemersdocumenten

IT, communicatie en andere apparatuur

- desktop computers
- laptops
- installatie-CDs
- UPS-apparaten
- generatoren
- air-conditioning
- netwerkapparatuur
- stroomkabels
- servers
- telefoons
- telefooncentralesystemen
- mobiele telefoons

PDA's
printers
scanners
kopieerapparatuur
backup tapes
mobiele opslagmedia
meetapparatuur
faxapparaten
alarmapparatuur
voertuigen
kaarten en kaartlezers
sluizen
sleutels

Infrastructuur

kantoren
archieven
opslagruimten
kluizen
opslagkasten

Uitbestede diensten

stroomtoevoer
communicatieverbindingen
onderhoud ICT-apparatuur
onderhoud informatiesystemen
mail-en koeriersdiensten
auditors
adviseurs
toezichthoudende instanties

Catalogus voor bedreigingen

Het volgende is een lijst van bedreigingen. Deze lijst is niet uitputtend. Een organisatie kan situatie-sp

onverwachte wijziging van gegevens van informatiesystemen
applicatiefouten
bomaanslag
bommelding
schending van contractuele betrekkingen
schending van de wetgeving
uitval van communicatieverbindingen
verbergen gebruikersidentiteit
schade veroorzaakt door activiteiten van derde partijen
schade opgelopen tijdens penetratietesten
vernietiging van registraties
verslechtering van media
openbaarmaking van wachtwoorden
afluisteren
verduistering
falen apparatuur
vervalsing van registraties
brand
overstroming
fraude
bedrijfspionage
onderscheppen van informatie
onderbreking van stroomtoevoer
lekken/openbaar maken van informatie
verlies van ondersteunende diensten
onderhoudsfouten
schadelijke virussen
misbruik van audit-tools
misbruik van informatiesystemen
andere rampen (kunstmatige)
andere rampen (natuurlijke)
vervuiling
social engineering (nadoen)
staking
bliksem
terroristische aanslag
diefstal
ongeautoriseerde toegang tot het informatiesysteem
ongeautoriseerde wijziging van registraties
ongeautoriseerde installatie van software
ongeautoriseerde netwerktoegang
ongeautoriseerde fysieke toegang
ongeautoriseerde gebruik van geleverde materiaal
ongeautoriseerde gebruik van software
gebruik van ongeautoriseerde of niet-geteste code
gebruikersfout

Catalogus van kwetsbaarheden

Het volgende is een lijst van kwetsbaarheden.
De lijst is niet uitputtend. Een organisatie kan situatie-specifieke kwetsbaarheden.

actieve sessies na werktijd
kabelplaatsing
gecompliceerde userinterface
cryptografische sleutels toegankelijk voor ongeautoriseerde personen
verwijdering van opslagmedia zonder de gegevens te wissen
uitgebreide bevoegdheden
ontoereikend capaciteitsbeheer
ontoereikend wijzigingsbeheer
ontoereikend niveau van kennis en/of bewustwording van werknemers
ontoereikend onderhoud
ontoereikend netwerkbeheer
ontoereikend functiescheiding
ontoereikend toezicht op externe leveranciers
ontoereikend toezicht op het werk van werknemers
ontoereikende gebruikersrechten
informatie beschikbaar voor ongeautoriseerde personen
gebrek aan bewijs van versturde of ontvangen berichten
gebrek aan beheer van invoer en uitvoer van gegevens
gebrek aan of slechte interne auditimplementatie
gebrek aan validatie van verwerkte gegevens
locatie gevoelig voor natuurrampen
locatie gevoelog voor waterlekkage
mobiele apparatuur onderhevig aan diefstal
netwerken toegankelijk voor ongeautoriseerde personen
geen deactivatie van gebruikersaccounts na beëindiging van het dienstverband
geen scheiding van de test- en productieomgeving
verouderde databases voor beveiliging tegen virussen
te grote afhankelijkheid van een apparaat/systeem
slechte selectie van testgegevens
gevoeligheid apparatuur voor vochtigheid en vervuiling
gevoeligheid apparatuur voor temperatuur
gevoeligheid apparatuur voor spanningsveranderingen
enkel exemplaar, maar één exemplaar van informatie
systeemgegenereerde gebruikersaccounts en wachtwoorden die onveranderd blijven
systemen onbeschermd tegen ongeautoriseerde toegang
onbewogde toegang tot toegestane faciliteiten
onduidelijk gedefineerde classificatie
onduidelijk gedefineerde cryptografische regels
onduidelijk gedefineerde organisatieregels
onduidelijke eisen voor softwareontwikkeling
onduidelijk gedefineerde regels voor toegangsbeheer
onduidelijk gedefineerde regels voor werken buiten het terrein
geen controle op kopieën
geen controle op downloads van het internet
geen controle op het gebruik van informatiesystemen

ongedocumenteerde software
ongemotiveerd of ontevreden werknemers
onbeschermde openbare netwerkverbindingen
gebruik van oude apparatuur
zwakke wachtwoorden