

© 2006 Centric IT Solutions B.V.

U ontvangt dit document onder de uitdrukkelijke voorwaarde dat u dit document vertrouwelijk zal behandelen. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van Centric IT Solutions B.V.

Centric Security & Continuity Services
“Voorkomen én genezen”

Documentgegevens

Uitgegeven door:

Centric IT Solutions
Doesburgweg 7
Postbus 751
2800 AT GOUDA
Tel. (0182) 56 26 00
Fax. (0182) 56 26 12
<http://www.centric.nl>

Publicatiegegevens:

Titel : Centric Security & Continuity Services
"Voorkomen én genezen"

Door : Ing. G. Stroeve CISSP

Datum : Oktober 2006

Versie : 2.1

Afdrukdatum : 2 oktober 2006

Inhoudsopgave

1.	Inleiding.....	4
2.	Centric Security Services.....	5
2.1	Informatiebeveiliging	6
2.2	De Code voor Informatiebeveiliging – NEN 17799	11
2.3	Het stappenplan.....	16
2.4	Het concept Centric Security Services	18
3.	Centric Continuity Services.....	32
3.1	Adviestraject Business Continuity	33
3.2	Project Continuïteitsplanning.....	34
3.3	Uitwijkregeling.....	36
3.4	Remote Backup Service.....	39
3.5	Back-up Test Service	41
3.6	Tape Collecting & Storage Service.....	42
Bijlage	Reactieformulier	

1. Inleiding

Vanuit onze afdeling Security & Continuity Services krijgen de aspecten informatiebeveiliging en continuïteit integrale aandacht. De diverse diensten binnen de portfolio's 'Security Services' en 'Continuity Services' zijn separaat af te nemen en sluiten zeer nauw op elkaar aan.

Het portfolio **Security Services** omvat een breed palet aan diensten op het gebied van informatiebeveiliging, ontwikkeld vanuit een duidelijke conceptvisie. Enkele centrale diensten binnen dit portfolio zijn: Awareness Programs, de QuickScan op de Code voor Informatiebeveiliging, de Network Security Scans, de WiFi Security Check, Business Impact Analyses en het opstellen van een beveiligingsplan.

Het dienstenportfolio **Continuity Services** richt zich op de continuïteit van uw organisatie. De diensten stellen u in staat uw continuïteitsorganisatie modulair vorm te geven. Enkele centrale diensten binnen dit portfolio zijn: Het opstellen van een continuïteitsplan, het verzorgen van uitwijk, de Backup Test Service en de Tape Collecting & Storage Service.



2. Centric Security Services

Er wordt veel over informatiebeveiliging gesproken en geschreven. En toch vinden we informatiebeveiliging nog regelmatig terug als *sluitpost* op de begroting. De redenen hiervoor verschillen: onbekendheid met de materie, tijdgebrek of bijvoorbeeld financiële prioriteitstelling. En dat terwijl verstoringen direct impact kunnen hebben op de continuïteit van uw organisatie en informatiebeveiliging in feite een *sleutelrol* vervult.

De keuze voor de wijze waarop u met de informatiebeveiliging omgaat, zal daarom een weloverwogen keuze moeten zijn. Een keuze op basis van bekendheid met de diverse beveiligingsrisico's. Om u bij deze keuze te ondersteunen, heeft Centric een integraal dienstenconcept ontwikkeld: Centric Security Services.

In deze conceptbeschrijving wordt in hoofdstuk 2 nader ingegaan op het begrip informatiebeveiliging en het belang van deze vorm van beveiliging. Vervolgens wordt in hoofdstuk 3 een introductie gegeven van de "Code voor informatiebeveiliging". Deze NEN-norm beschrijft een uitgebreide verzameling maatregelen voor een gedegen implementatie van informatiebeveiliging en vormt een belangrijk referentiekader binnen het totaalconcept.

Om te komen tot een passende vorm van beveiliging zal een aantal essentiële fasen doorlopen moeten worden. Deze fasen worden beschreven in hoofdstuk 4; Het stappenplan. Dit stappenplan vormt de basis voor het Centric Security Services concept. Het concept ondersteunt u bij het doorlopen van de betreffende fasen. In hoofdstuk 5 wordt een beschrijving gegeven van het totaalconcept. Hierbij worden tevens de diverse deeldiensten (modulen) binnen het concept toegelicht.

Hoofdstuk 6 tenslotte bevat een toelichting op de maatregelenmatrix, een model waarmee de koppeling wordt gemaakt tussen enerzijds het aandachtsgebied waarop beveiligingsmaatregelen effect hebben en anderzijds hun functionele aard.



2.1 Informatiebeveiliging

2.1.1 Het begrip Informatiebeveiliging

De vraag “wat verstaan we nu precies onder informatiebeveiliging?” zou eenvoudig kunnen worden beantwoord met “het beveiligen van informatie”. Toch gaat het bij informatiebeveiliging niet per definitie om het waarborgen van de informatie zelf, maar om het waarborgen van bepaalde waardekenmerken van die informatie.

We definiëren informatiebeveiliging daarom als: “Het waarborgen van kernwaarden van informatie”. We onderscheiden hierbij drie kernwaarden: Vertrouwelijkheid, Integriteit en Beschikbaarheid.

Vertrouwelijkheid

Onder vertrouwelijkheid verstaan we de mate waarin alleen geautoriseerde personen of processen kennis mogen nemen en/of gebruik mogen maken van de informatie. Dit betekent bijvoorbeeld dat het telefoonnummer van een bedrijf een lage vertrouwelijkheidswaarde heeft en dat de salarisadministratie een hoge mate van vertrouwelijkheid zal hebben.

Integriteit

De integriteit van de informatie wordt bepaald door de juistheid, de volledigheid en de correctheid in tijd van (de verwerking van) informatie. Met andere woorden: in hoeverre is de informatie (nog) gelijk aan hoe die zou moeten zijn en ooit bedoeld is.

Beschikbaarheid

De beschikbaarheid van informatie wordt bepaald door de mate waarin de informatie op de juiste momenten tijdig toegankelijk is voor geautoriseerde personen of processen.

Deze drie kernwaarden, vertrouwelijkheid, integriteit en beschikbaarheid, zijn van toepassing op elke informatie(stroom) binnen een organisatie. Of het nu gaat om de lijst met interne telefoonnummers, personeelsgegevens, omzetgegevens, verslagen van vergaderingen of inlogcodes; we kunnen bepaalde eisen stellen ten aanzien van de ‘hoogte’ van de drie kernwaarden. Het stellen van deze eisen noemen we het classificeren van de informatie.

Wanneer we nu onze definitie van informatiebeveiliging opnieuw bekijken, betekent het waarborgen van de kernwaarden dus in feite: “Het ervoor zorgen dat aan de gestelde eisen ten aanzien van die waarden wordt voldaan”.

Maar waarom is het nu zo belangrijk deze kernwaarden te waarborgen? Met andere woorden: “Wat is nu het belang van informatiebeveiliging?”

2.1.2 Het belang van informatiebeveiliging

Als we kijken naar het belang van informatiebeveiliging dienen we ons te realiseren dat er nogal wat bedreigingen zijn die de kernwaarden kunnen aantasten. Vervolgens heeft een aantasting altijd gevolgen (impact), hetzij direct of indirect, op de bedrijfsvoering.

Bedreigingen

In onderstaande opsomming wordt per kernwaarde een aantal voorbeelden van bedreigingen genoemd:

Bedreigingen ten aanzien van de vertrouwelijkheid:

- Informatie die 'op straat' komt te liggen;
- Het lekken van informatie door medewerkers;
- Infiltratie door criminelen in organisaties;
- Het slordig omgaan met privileges;
- Het hacken van informatiesystemen;
- Het afluisteren van informatiestromen.

Bedreigingen ten aanzien van de integriteit:

- Fouten die gemaakt worden bij het invoeren van gegevens;
- Het achterhouden van informatie;
- Manipulatie van gegevens;
- Onvolledigheid van bijvoorbeeld databasegegevens.

Bedreigingen ten aanzien van de beschikbaarheid:

- Diefstal van gegevens;
- Brand;
- Waterschade;
- Toegangsbeperking, bijvoorbeeld door een omgevingsincident;
- Uitval van communicatielijnen;
- Storing op apparatuur;
- Uitval van personeel.

Natuurlijk is bovenstaande opsomming niet compleet. Het is evenwel duidelijk dat er nogal wat vormen van bedreigingen zijn. Iedere bedreiging (en dus aantasting van één of meer van de kernwaarden) heeft een directe of indirecte impact op de bedrijfsvoering.

Gevolgen

De gevolgen (impact) die de aantasting van de kernwaarden voor de bedrijfsvoering heeft, kunnen divers van aard zijn. Zo onderscheiden we ondermeer:

- Operationele gevolgen;
- Organisatorische gevolgen;
- Financiële gevolgen;
- Juridische gevolgen;
- Politieke gevolgen;
- Maatschappelijke gevolgen;
- Gevolgen voor het imago van de organisatie.

Een tweetal voorbeelden:

1. Het toegankelijk zijn van privacygevoelige informatie voor ongeautoriseerde personen (aantasting van vertrouwelijkheid) zou juridische gevolgen kunnen hebben en binnen de lokale overheid mogelijk ook politieke gevolgen.
2. Het uitvallen van datacommunicatielijnen tussen twee vestigingen van een bedrijf (beschikbaarheid) kan daarentegen operationele gevolgen hebben en uiteindelijk tot financiële schade leiden. Wanneer het uitvallen van middelen betekent dat bepaalde diensten niet aan klanten kunnen worden geleverd, heeft dat niet alleen financiële gevolgen maar mogelijk ook gevolgen voor het imago van het bedrijf.

Toename aantal bedreigingen en afhankelijkheid

Naast de vele vormen van aantasting is ook een duidelijke stijging waarneembaar in het aantal beveiligingsincidenten binnen organisaties terwijl organisaties ook nog eens steeds afhankelijker worden van de informatievoorziening. Zo eist bijvoorbeeld een verscherpte regelgeving op het gebied van de privacy meer aandacht op voor vertrouwelijkheidsaspecten. Door de toenemende afhankelijkheid van de informatievoorziening heeft een verstoring van die informatievoorziening steeds grotere gevolgen voor de bedrijfsvoering.



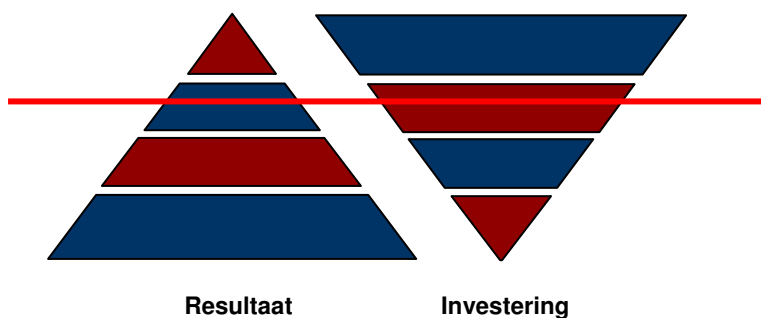
2.1.3 Het dilemma van kosten en baten

Wat is nu de juiste manier om met informatiebeveiliging om te gaan? Het beveiligingsbudget verhogen en de organisatie overladen met allerlei beveiligingsmaatregelen? Een niet eenvoudig te beantwoorden vraag met een voor iedere organisatie ander antwoord.

We dienen ons in dit kader te realiseren dat een “honderd procent” vorm van beveiliging een utopie is. Als het al te realiseren is, zijn de te nemen maatregelen onbetaalbaar en maken ze normale bedrijfsvoering vrijwel onmogelijk. Daarom moet een juiste balans gevonden worden tussen de benodigde investering, de kwetsbaarheid, de impact die verstoringen kunnen hebben op de bedrijfsvoering en de effectiviteit van de maatregelen.

Overigens kan een groot aantal zeer effectieve beveiligingsmaatregelen tegen een relatief lage investering genomen worden. Voorbeelden hiervan zijn het verhogen van de awareness bij het personeel en het implementeren en beheren van procedures.

Met een relatief lage investering is dan ook veel te bereiken. Het bereiken van een steeds hoger beveiligingsniveau vraagt doorgaans een relatief hogere investering. Onderstaande figuur geeft dit verband tussen resultaat en kosten weer. Voor iedere organisatie zal hierbij gezocht dienen te worden naar een goede balans (rode lijn).



We zien dat informatiebeveiliging een belangrijke rol speelt in de bedrijfsvoering, dat er vele vormen van bedreigingen zijn én dat het aantal bedreigingen ook nog eens toeneemt. Daarnaast zien we ook dat informatiebeveiliging een begrip is dat zich in feite uitstrekt tot in elke hoek van de organisatie.

Hoe geven we nu de juiste aandacht aan informatiebeveiliging zónder het overzicht te verliezen?

Een belangrijk hulpmiddel hierbij vormt “De Code voor informatiebeveiliging”. Deze Code kan worden gezien als standaardleidraad voor beleid en implementatie van informatiebeveiliging. Het boekwerk beschrijft op een praktische wijze richtlijnen om te komen tot een gemeenschappelijk niveau van integrale beveiliging.

In het volgende hoofdstuk wordt een bondige introductie gegeven van de Code voor informatiebeveiliging.

Aandachtspunten:

- **Informatiebeveiliging: Het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie**
- **Informatiebeveiliging is een organisatiebreed begrip**
- **Er zijn vele vormen van bedreiging**
- **Het aantal bedreigingen neemt toe**
- **De informatieafhankelijkheid neemt toe**
- **Dilemma: afweging risico's, beleid, investering en resultaat**

Hoe ziet de Code voor informatiebeveiliging er uit?

2.2 De Code voor Informatiebeveiliging – NEN 17799

De Code voor Informatiebeveiliging werd oorspronkelijk uitgegeven in 1994 en was gebaseerd op de conceptversie van de Britse standaard BS 7799. De Code biedt een uitgebreide verzameling maatregelen voor een goede implementatie (“best practices”) van informatiebeveiliging. De Code is bedoeld als het referentiepunt voor het vaststellen van de reeks beveiligingsmaatregelen die nodig zijn in de meeste situaties waarin informatiesystemen worden gebruikt. De Code kan worden gebruikt in grote, middelgrote en kleine organisaties. De term organisaties, zoals gebruikt in dit document, betreft zowel profit, non-profit als publieke sector organisaties.

In de revisie van 1999 is rekening gehouden met de recente ontwikkelingen in de toepassing van Informatietechnologie (IT), met name op het gebied van netwerken en communicatie. Ook wordt meer nadruk gelegd op de betrokkenheid van bedrijven bij en de verantwoordelijkheid voor informatiebeveiliging.

Om de informatiebeveiliging binnen een organisatie vanuit een breed, integraal perspectief te beschouwen, definieert de Code de volgende tien aandachtsgebieden:

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmiddelen
4. Beveiligingseisen ten aanzien van personeel
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatieprocessen en bedieningsprocessen
7. Toegangsbeveiliging
8. Ontwikkeling en onderhoud van systemen
9. Continuïteitsmanagement
10. Naleving



De hiernavolgende paragrafen behandelen beknopt de tien aandachtsgebieden binnen de Code voor Informatiebeveiliging.

2.2.1 Beveiligingsbeleid

In dit hoofdstuk worden richtlijnen gegeven voor het opstellen en uitdragen door het management van een beleidsdocument ten aanzien van informatiebeveiliging. Het betreffende beleid dient een 'eigenaar' te hebben die verantwoordelijk is voor de handhaving en evaluatie ervan volgens een gedefinieerd evaluatieproces.

2.2.2 Beveiligingsorganisatie

Dit hoofdstuk beschrijft onder andere de organisatorische infrastructuur voor informatiebeveiliging. Zo dient er een managementkader vastgesteld te worden om de implementatie van informatiebeveiliging in de organisatie op gang te brengen en te beheersen. Ook behandelt het hoofdstuk de beveiliging van toegang door derden en beveiligingseisen in uitbestedingscontracten.

2.2.3 Classificatie en beheer van bedrijfsmiddelen

Het bepalen van de verantwoordelijkheden voor bedrijfsmiddelen draagt ertoe bij dat deze op de juiste manier beveiligd blijven. Alle belangrijke bedrijfsmiddelen dienen een eigenaar te krijgen die verantwoordelijk is voor het handhaven van de juiste beveiligingsmaatregelen. Het is daarbij goed te realiseren dat niet alle informatie even gevoelig en kritiek is. Voor sommige bedrijfsmiddelen zal extra beveiliging of een speciale behandeling noodzakelijk zijn. Er dient gebruik gemaakt te worden van een informatieclassificatiesysteem om een adequate set beveiligingsniveaus te definiëren en om de noodzaak van een speciale behandeling kenbaar te maken.

2.2.4 Beveiligingseisen ten aanzien van personeel

Beveiliging dient te worden besproken bij indiensttreding van nieuwe personeelsleden en te worden opgenomen in functieomschrijvingen en contracten. Ook dienen gebruikers te worden getraind in het omgaan met de beveiligingsprocedures en het correcte gebruik van ICT-voorzieningen om eventuele beveiligingsrisico's te minimaliseren. Incidenten die de beveiliging aantasten, dienen direct via de geëigende managementkanalen te worden gerapporteerd.

2.2.5 Fysieke beveiliging en beveiliging van de omgeving

ICT-voorzieningen die kritieke of gevoelige zakelijke activiteiten ondersteunen, dienen fysiek te worden ondergebracht in beveiligde ruimten in een gecontroleerde omgeving, beveiligd met fysieke barrières en met toegangsbeveiliging. Ze dienen fysiek te worden beschermd tegen toegang door ongeautoriseerde personen, schade en storingen. Apparatuur dient fysiek te worden beveiligd tegen bedreigingen van de veiligheid en gevaren van buitenaf. Informatie en ICT-voorzieningen dienen te worden beveiligd tegen bekendmaking aan, wijziging of diefstal door ongeautoriseerde personen. Er dienen maatregelen te worden genomen om het verlies en de schade te minimaliseren.

2.2.6 Beheer van communicatie- en bedieningsprocessen

Er dienen verantwoordelijkheden en procedures te worden vastgesteld voor het beheer en de bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van bedieningsinstructies en procedures voor het reageren op incidenten. Daarnaast zijn een goede planning en voorbereiding noodzakelijk om te kunnen garanderen dat de juiste capaciteit en de juiste hulpbronnen beschikbaar zijn. Er dienen tevens maatregelen te worden getroffen om de introductie van kwaadaardige software te voorkomen en te ontdekken.

Er dienen routineprocedures te worden vastgesteld voor het ten uitvoer brengen van de overeengekomen backup strategie, het maken van reservekopieën van gegevens en het oefenen van tijdig herstel ervan, voor het bijhouden van logboeken van gebeurtenissen en storingen en waar nodig voor het bewaken van apparatuur en omgeving.

2.2.7 Toegangsbeveiliging

De toegang tot informatie en bedrijfsprocessen dient te worden beheerst op grond van zakelijke behoeften en beveiligingseisen. Er dienen formele procedures te bestaan voor het beheer van autorisaties voor informatiesystemen en -diensten. Ook dient aandacht te worden geschonken aan verantwoordelijk gedrag van gebruikers.

Dit hoofdstuk gaat tevens in op de toegangsbeveiliging voor netwerken, besturingssystemen en toepassingen, het monitoren van toegang tot en gebruik van systemen en het waarborgen van informatiebeveiliging bij het gebruik van mobiele computers en voorzieningen voor telewerken.

2.2.8 Ontwikkeling en onderhoud van systemen

Dit hoofdstuk richt zich op de beveiligingseisen ten aanzien van infrastructuur, bedrijfstoepassingen en applicaties die door de gebruiker zijn ontwikkeld. In toepassingssystemen, inclusief de toepassing die door de gebruiker zijn geschreven, dienen de benodigde beveiligingsmaatregelen en audit trails te worden ingebouwd. Hiertoe behoort de validatie van invoergegevens, van interne verwerking en van uitvoergegevens.

Daarnaast dienen cryptografische systemen en technieken te worden gebruikt ter beveiliging van gegevens die aan risico's blootgesteld kunnen worden en die onvoldoende beveiligd worden door andere maatregelen. Ook het beheer van ontwikkel- en ondersteuningomgevingen, de daaraan gerelateerde processen en van de toegang tot systeembestanden komt in dit hoofdstuk aan de orde.

2.2.9 Continuïteitsmanagement

Er dient een proces van continuïteitsmanagement te worden geïmplementeerd om de verstoring als gevolg van calamiteiten en beveiligingsincidenten (als gevolg van bijvoorbeeld natuurrampen, ongevallen, uitval van apparatuur en opzettelijke handelingen) tot een aanvaardbaar niveau te beperken middels een combinatie van preventieve en herstelmaatregelen.

De gevolgen van calamiteiten, beveiligingsincidenten en uitval van diensten dienen te worden geanalyseerd. Er dienen continuïteitsplannen te worden ontwikkeld en geïmplementeerd om te waarborgen dat bedrijfsprocessen binnen de gestelde tijdslijmieten kunnen worden hersteld. Dergelijke plannen dienen te worden bijgehouden en geoefend zodat ze een integraal deel van alle andere beheersprocessen worden. Continuïteitsmanagement dient maatregelen te bevatten voor het vaststellen en verminderen van risico's, het beperken van de gevolgen van incidenten die schade toebrengen en het tijdig hervatten van essentiële werkzaamheden.

2.2.10 Naleving

Het is belangrijk toe te zien op de naleving van het beveiligingsbeleid door het personeel. Daarnaast kunnen het ontwerp, de bediening, het gebruik en beheer van informatiesystemen onderworpen zijn aan statutaire, wettelijke of contractuele beveiligingseisen. Er dient derhalve deskundig advies over specifieke juridische eisen te worden ingewonnen bij de juridische adviseurs van de organisatie of bij gekwalificeerde juristen. De wettelijke voorschriften voor informatie die in het ene land wordt gecreëerd en naar een ander land wordt verzonden (een grensoverschrijdende gegevensstroom) verschillen van land tot land.

De beveiliging van informatiesystemen dient regelmatig te worden gecontroleerd. Dergelijke evaluaties dienen te worden uitgevoerd op basis van het desbetreffende beveiligingsbeleid. Ook zullen er bijvoorbeeld maatregelen getroffen moeten worden om operationele systemen en hulpmiddelen voor audits te beveiligen tijdens systeemaudits.

Aandachtspunten:

- De Code voor informatiebeveiliging biedt een uitgebreide verzameling maatregelen voor een goede implementatie van informatiebeveiliging
- De Code vormt een NEN-normering (ISO 17799)
- Er zijn binnen de code tien aandachtsgebieden gedefinieerd
- Bij het opstellen van de Code is ervan uitgegaan dat de uitvoering van de maatregelen wordt toevertrouwd aan gekwalificeerde en ervaren mensen

Welke stappen moeten nu doorlopen worden om te komen tot integrale informatiebeveiliging?

2.3 Het stappenplan

2.3.1 Het stappenplan

Er dient een aantal essentiële stappen te worden doorlopen om te komen tot een integrale vorm van informatiebeveiliging:

Bewustwording

De bewustwording is wellicht de belangrijkste van alle stappen. De bewustwording vormt uiteindelijk het draagvlak voor de te nemen beveiligingsmaatregelen.

Beeldvorming

Vervolgens zal men zich een beeld moeten vormen van de huidige beveiligingssituatie. Een goede methode hiervoor is het uitvoeren van een risicoanalyse.

Prioriteitstelling

Met het verkregen beeld van de beveiligingssituatie kunnen prioriteiten worden gesteld ten aanzien van de aandachtspunten op het gebied van informatiebeveiliging.

Beleid en organisatie

Op basis van de gestelde prioriteiten wordt een beveiligingsbeleid geformuleerd. De uitvoering van dit beleid zal moeten worden ingebed in de organisatie.

Planning en ontwerp

Vervolgens kan een beveiligingsplan worden samengesteld waarin het ontwerp van (een set van) beveiligingsmaatregelen centraal staat.

Implementatie

Het ontwerp kan vervolgens worden geïmplementeerd. Na de implementatie zal de effectiviteit periodiek moeten worden geëvalueerd; zonodig zal ook onderhoud gepleegd moeten worden.

2.3.2 Continu proces

Het stappenplan op de vorige pagina beschrijft de stappen die men neemt om te komen tot een adequate implementatie van beveiligingsmaatregelen. Zoals gesteld vormt het bewustzijn, zowel bij het management als bij het overige personeel, een belangrijke factor bij het slagen van deze maatregelen. Het is dus zaak deze bewustwording (awareness) hoog te houden.

De prioriteitstelling binnen het stappenplan vormt de basis voor de keuze van het pakket aan maatregelen. We dienen ons echter te realiseren dat deze prioriteitstelling voortkomt uit een beoordeling van de beveiligingsrisico's op een bepaald moment. In de tijd kunnen zowel de kwetsbaarheden als de afhankelijkheid veranderen. Om deze reden zullen we de diverse stappen als een continu proces voortdurend opnieuw moeten doorlopen en, waarnodig, het pakket aan maatregelen op de situatie moeten aanpassen.

Aandachtspunten:

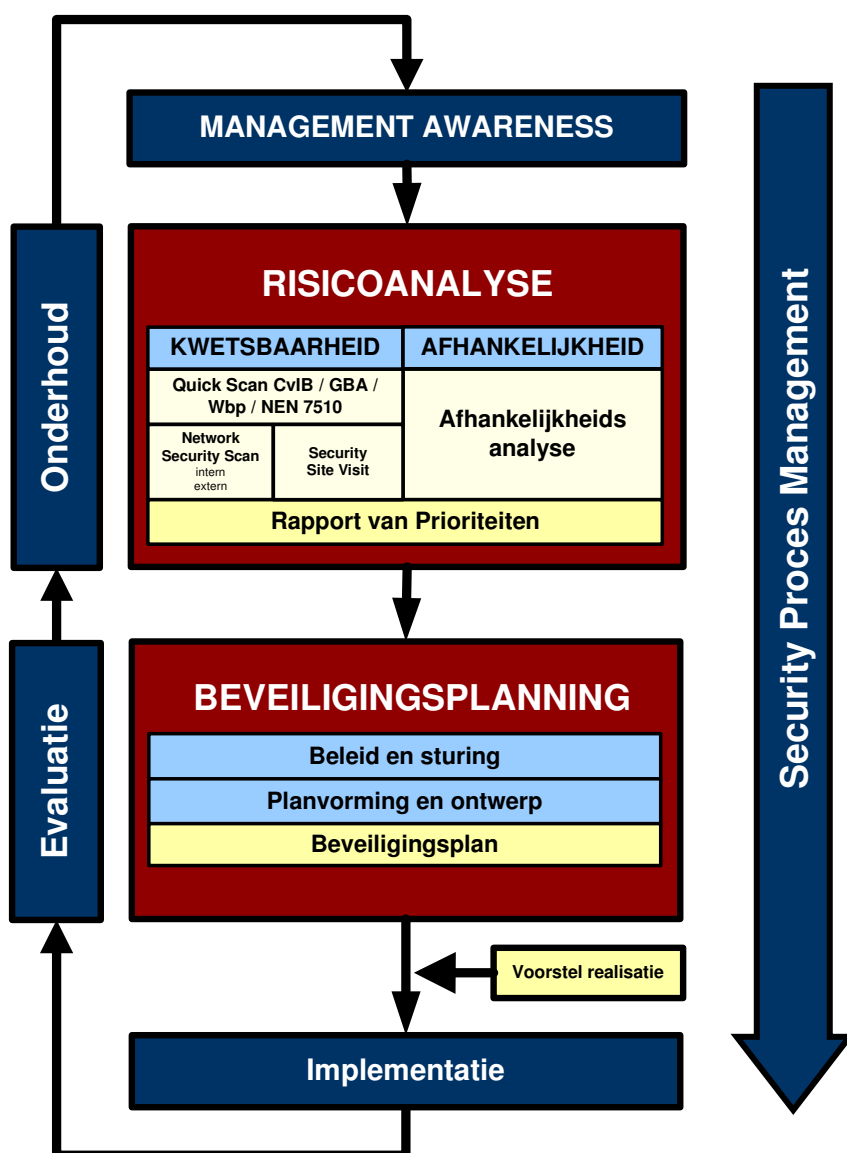
- **Er zijn zes basisstappen te onderscheiden**
- **Beveiligingsbewustzijn (Security Awareness) vormt een essentiële basis voor eventueel te nemen beveiligingsmaatregelen**
- **Informatiebeveiliging is een continu proces**

Hoe pakken we nu informatiebeveiliging aan?

2.4 Het concept Centric Security Services

2.4.1 Conceptmodel

Het stappenplan zoals beschreven in hoofdstuk 4 vormt de basis voor het Centric Security Services concept. De diverse stappen zijn vertaald in concrete (deel)diensten. Het concept is hieronder schematisch weergegeven:



Schema Centric Security Services

Awareness

Binnen de diverse stappen van het concept is veel aandacht voor de awareness binnen uw organisatie. Want uiteindelijk vormt het beveiligingsbewustzijn bij zowel het management als bij het overige personeel een belangrijke factor voor de effectiviteit van eventueel te nemen beveiligingsmaatregelen.

Risicoanalyse

Via een uitgebreide risicoanalyse wordt een duidelijk beeld verkregen van uw huidige beveiligingssituatie. Hierbij wordt niet alleen de kwetsbaarheid van uw organisatie vastgesteld maar ook de informatieafhankelijkheid van uw bedrijfsprocessen bepaald. De kwetsbaarheid en de afhankelijkheid vormen belangrijke factoren in het stellen van beveiligingsprioriteiten.

Beveiligingsplanning

Binnen de fase beveiligingsplanning staat vervolgens de vraag centraal hoe de informatiebeveiliging binnen uw organisatie kan worden bevorderd. Hiertoe zullen de gestelde prioriteiten worden belicht vanuit het beveiligingsbeleid van uw organisatie. Onze security consultants zullen uw beleid en de gestelde prioriteiten vervolgens vertalen in een ontwerp. Dit ontwerp zal de kern vormen van het beveiligingsplan.

Implementatie, evaluatie en onderhoud

Desgewenst kunnen we het beveiligingsplan vervolgens met u vertalen in een concreet realisatievoorstel en de implementatie voor u verzorgen. Vervolgens evalueren we de implementatie van het beveiligingsplan periodiek met u en voeren we zonodig onderhoud uit op het plan.

Security Proces Management

Een Security Proces Manager vormt uw centrale aanspreekpunt en begeleidt u tijdens de diverse fasen van het concept.

Op de volgende pagina's zijn de diverse modulen nader uitgewerkt.

2.4.2 Management Awareness Session

Binnen de diverse stappen van het concept is er veel aandacht voor de awareness binnen de organisatie. Want uiteindelijk vormt het beveiligingsbewustzijn bij zowel het management als bij het overige personeel een belangrijke factor voor de effectiviteit van eventueel te nemen beveiligingsmaatregelen.

Doelstelling

Het bereiken van de juiste mate van awareness ten aanzien van informatiebeveiliging zodat een goede basis ontstaat om eventueel benodigde beveiligingsmaatregelen te bepalen en te implementeren.

Scope

De scope van de Management Awareness Session omvat de bewustwording ten aanzien van informatiebeveiliging bij het organisatiemanagement. Dit laat onverlet dat ook de bewustwording bij het overige personeel essentieel is voor de effectiviteit van beveiligingsmaatregelen. Ook bij het bevorderen van de awareness bij het overige personeel kan Centric ondersteunen.

Werkwijze

De wijze waarop de awareness bij het management wordt bevorderd, is als maatwerkactiviteit te definiëren. Zo kan bijvoorbeeld worden gedacht aan een presentatie aan het management waarin wordt stil gestaan bij het begrip informatiebeveiliging en de impact die een verstoring kan hebben op de bedrijfsvoering. Ook het groepsgewijs doorlopen van een calamiteitenscenario kan in belangrijke mate bijdragen aan de bewustwording.

Rapportage

Afhankelijk van de gekozen vorm van de Management Awareness Session worden op bondige wijze de ervaringen van de deelnemers gerapporteerd.

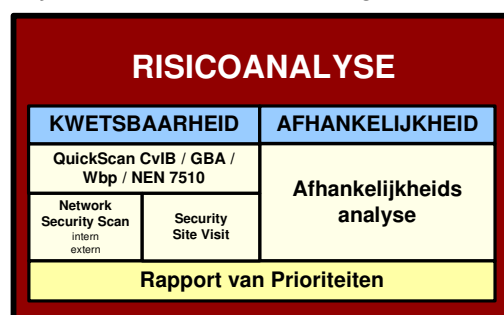
Tijdsduur

Doorgaans omvat de Management Awareness Session een bijeenkomst van circa 2 uur. Deze tijdsduur is uiteraard ook mede afhankelijk van de gekozen vorm.

2.4.3 Risicoanalyse

Via een risicoanalyse wordt een duidelijk beeld verkregen van de huidige beveiligingssituatie. Wanneer we daarbij kijken naar de informatie binnen organisaties worden risico's enerzijds bepaald door de mate waarin de organisatie beschermd is tegen verstoringen; de kwetsbaarheid, en anderzijds door de impact die een verstoring op de bedrijfsvoering heeft; de afhankelijkheid met betrekking tot de informatie(voorziening). Beide componenten vormen vervolgens belangrijke factoren in het stellen van beveiligingsprioriteiten.

De risicoanalyse is dan ook onder te verdelen in een kwetsbaarheidsanalyse en een afhankelijkheidsanalyse. Het dienstenkader van de risicoanalyse is in het schema hiernaast weergegeven.



Kwetsbaarheidsanalyse

Om een breed beeld te verkrijgen van de kwetsbaarheden op het gebied van informatiebeveiliging heeft Centric drie specifieke scans ontwikkeld:

- *QuickScan Informatiebeveiliging*
De QuickScan geeft door middel van interviews op een overzichtelijke wijze inzicht in de beveiligingsknelpunten binnen uw organisatie. Hierbij kunnen diverse referentiekaders worden gehanteerd (bijvoorbeeld: Code voor Informatiebeveiliging, GBA-wetgeving, Wet Bescherming Persoonsgegevens, NEN 7510).
- *Network Security Scan*
Met de Network Security Scan wordt een specifiek beeld verkregen van de (technische) beveiligingsinstellingen van uw netwerk en apparatuur. De scan kan zowel intern als extern gericht zijn.
- *Security Site Visit*
Om inzicht te verkrijgen in de fysieke beveiligingsstatus van uw informatiesystemen voeren onze consultants een beoordeling op locatie voor u uit.

Afhankelijkheidsanalyse

De afhankelijkheidsanalyse beschouwt uw centrale bedrijfsprocessen en onderzoekt de mate waarin deze processen afhankelijk zijn van de geautomatiseerde ondersteunende processen. Zo wordt in kaart gebracht wat de impact is van het uitvallen van de automatisering op de bedrijfsvoering.

Prioriteitstelling

Aan de hand van dit beeld kan vervolgens samen met u een prioriteitenoverzicht worden opgebouwd. Uiteindelijk vormt deze prioriteitstelling de basis voor een integraal ICT-beveiligingsplan.

Kwetsbaarheidsanalyse - QuickScan Informatiebeveiliging

De QuickScan Informatiebeveiliging geeft door middel van interviews op een snelle en overzichtelijke wijze inzicht in de beveiligingsknelpunten binnen uw organisatie.

Doelstelling

Het verkrijgen van inzicht in de mate van informatiebeveiliging binnen een organisatie. Als referentiekader wordt hierbij “De Code voor Informatiebeveiliging” (ISO 17799) gehanteerd (zie hoofdstuk 2.2).

Scope

De scope van de QuickScan Informatiebeveiliging omvat de tien aandachtsgebieden zoals die in de Code zijn gedefinieerd, geprojecteerd op uw organisatie.

Werkwijze

Door middel van interviews met één of meerdere personen wordt vastgesteld in hoeverre de beveiligingsorganisatie voldoet aan de in de Code gestelde richtlijnen. De resultaten van de interviews worden vertaald in een score per aandachtsgebied. Zo wordt een duidelijk totaalbeeld verkregen van de beveiligingsstatus en de knelpunten binnen de organisatie.

Rapportage

De rapportage omvat een compleet overzicht van de vragen en de specifieke antwoorden. Ook is hierbij inzichtelijk welke waardering aan de betreffende antwoorden is gekoppeld. In de managementsamenvatting is een kleurenkaart opgenomen waarmee in een oogopslag duidelijk wordt op welke aandachtsgebieden voldoende wordt gescoord en welke gebieden meer aandacht vragen. Desgewenst kunnen de resultaten worden gepresenteerd aan het management.

Tijdsduur

Afhankelijk van de grootte van de organisatie en het aantal personen dat kan voorzien in de benodigde informatie zullen de interviews gemiddeld 2 tot 3 dagen in beslag nemen. De rapportage vergt eveneens gemiddeld 2 tot 3 dagen. Er dient rekening gehouden te worden met een doorlooptijd van circa 3 weken.

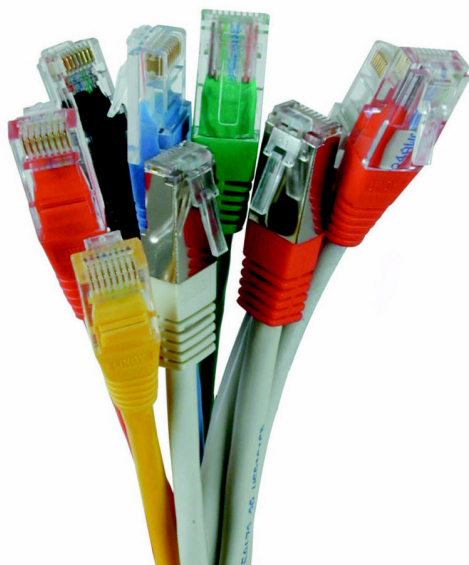
Kwetsbaarheidsanalyse - Network Security Scan

Interne en externe scan

Bij het spreken over een Network Security Scan wordt veelal direct gedacht aan het scannen van de internetkoppeling van uw bedrijf. Van buitenaf kunnen hackers zich immers mogelijk toegang verschaffen tot uw vertrouwelijke bedrijfsinformatie. De externe Network Security Scan brengt de (potentiële) gevaren aan het licht en biedt oplossingen om uw netwerk optimaal te beveiligen.

Het lijkt vaak niet noodzakelijk uw interne netwerk te scannen op mogelijke beveiligingslekken. Onderzoek wijst echter uit dat circa 70% van de bedreigingen op het gebied van informatiebeveiliging zich bevindt binnen de grenzen van het lokale netwerk. Beveiliging van de vitale onderdelen van het netwerk is derhalve bij veel organisaties een belangrijk punt op de agenda. De interne Network Security Scan geeft invulling aan deze behoefte.

Uw netwerk wordt gescand met behulp van diverse software tools. Aan de hand hiervan worden toegankelijke netwerkservices per machine in beeld gebracht. Er kunnen vervolgens conclusies worden getrokken ten aanzien van eventuele beveiligingslekken.



Network Security Scan – Interne scan

Uw interne netwerk wordt gescand met behulp van diverse software tools. Met behulp van deze tools worden, per machine, bereikbare netwerkservices in beeld gebracht. Aan de hand van de gevonden services worden de mogelijke problemen en bedreigingen in kaart gebracht.

Doelstelling

Het in beeld brengen van mogelijke beveiligingsknelpunten ten aanzien van het interne netwerk. De nadruk ligt hierbij op de ‘services’ die aanwezig zijn op de diverse serversystemen en de instellingen van poorten.

Scope

De scope van de scan omvat uw kritische serversystemen en netwerkcomponenten. De detailscope van de scan wordt in overleg met u bepaald.

Werkwijze

Ten behoeve van de scan wordt een laptop-configuratie gekoppeld aan uw netwerk. Op de laptop worden de scan tools geactiveerd. Gedurende de benodigde periode (afhankelijk van de detailscope) wordt door middel van de tool(s) de scan uitgevoerd. Een security operator zal periodiek de tool(s) bedienen. Na het beëindigen van de scan zullen de resultaten worden verwerkt in een rapportage.

Rapportage

De rapportage van de interne scan bevat een gedetailleerd overzicht van de gevonden knelpunten. Hierbij wordt tevens een opsomming gegeven van ontbrekende patches en/of servicepacks. Met dit overzicht als basis wordt een rapport van aanbeveling opgenomen.

Tijdsduur

Afhankelijk van de detailscope zal de scan, inclusief rapportageperiode, circa 5 dagen in beslag nemen. Er dient rekening gehouden te worden met een doorlooptijd van circa 3 weken.

Network Security Scan – Externe scan

Met de externe scan wordt een beeld verkregen van de mate van ongeautoriseerde toegang tot uw netwerk. Na formele toestemming van uw organisatie zullen onze beveiligingsspecialisten zich op een ethisch verantwoorde wijze trachten logische toegang te verschaffen tot uw netwerk.

De externe scan geeft u een goed beeld van de kwetsbaarheid van uw organisatie voor hackpogingen van buitenaf. Naar aanleiding van de bevindingen van de beveiligingsspecialisten zal een rapport van aanbeveling worden opgesteld.

Doelstelling

Het in beeld brengen van mogelijke beveiligingsknelpunten ten aanzien van externe toegang tot uw netwerk.

Scope

De scope van de scan omvat de externe toegang tot uw interne netwerk. Hierbij kan de focus worden gelegd op een aantal specifieke communicatielijnen.

Werkwijze

Binnen een vastgestelde periode zullen onze beveiligingsspecialisten zich op een ethisch verantwoorde wijze trachten logische toegang te verschaffen tot uw netwerk. Met behulp van diverse tools zullen de specialisten de scan uitvoeren. De toegankelijke informatie zal vertrouwelijk worden behandeld.

Rapportage

De rapportage van de externe scan bevat een overzicht van de gevonden knelpunten. Daarnaast zullen aanbevelingen worden opgenomen.

Tijdsduur

De scan zal, inclusief rapportageperiode, circa 3 dagen in beslag nemen. Er dient rekening gehouden te worden met een doorlooptijd van circa 3 weken.

Kwetsbaarheidsanalyse - Security Site Visit

Om inzicht te verkrijgen in de fysieke beveiligingsstatus van uw informatiesystemen voeren onze consultants een beoordeling op locatie voor u uit. Een dergelijke beoordeling kan bijvoorbeeld plaatsvinden als aanvulling op de QuickScan Informatiebeveiliging en/of de Network Security Scan.

Doelstelling

Het beoordelen van de fysieke beveiligingsstatus op één of meer specifieke aandachtsgebieden. Zo kan er bijvoorbeeld worden ingezoomd op de fysieke inrichting van de serverruimte of de backupprocedures.

Scope

De uitvoering van de Security Site Visit is volledig afgestemd op uw organisatie; de scope wordt vooraf gedefinieerd. Zo kan het wenselijk zijn een deskundige beoordeling op locatie te verkrijgen van specifieke beveiligingsonderdelen, bijvoorbeeld omdat er binnen de organisatie onvoldoende statusinformatie aanwezig is ten aanzien van het betreffende aandachtsgebied.

Werkwijze

In een intakegesprek wordt de scope van de Security Site Visit nader afgestemd. Vervolgens zullen de specialisten zich on-site een beeld vormen van de beveiligingsstatus van het betreffende aandachtsgebied. Dit beeld wordt duidelijk verwoord in een rapport van bevindingen.

Rapportage

De bevindingen van de Security Site Visit zullen in rapportvorm worden verwoord. De resultaten dragen bij tot het totaalbeeld van de kwetsbaarheid van de organisatie.

Tijdsduur

De benodigde tijd voor het uitvoeren van de Security Site Visit is direct afhankelijk van de gewenste scope.

Afhankelijkheidsanalyse

De afhankelijkheidsanalyse beschouwt uw centrale bedrijfsprocessen en onderzoekt de mate waarin deze processen afhankelijk zijn van de geautomatiseerde ondersteunende processen. Zo wordt in kaart gebracht wat de impact is van het uitvallen van de automatisering op de bedrijfsvoering.

Doelstelling

Het verkrijgen van een duidelijk beeld van de mate waarin de diverse (kritische) bedrijfsprocessen afhankelijk zijn van de informatievoorziening. Deze afhankelijkheid geeft het belang van het treffen van beveiligingsmaatregelen aan. De maat voor de afhankelijkheid wordt bepaald door de gevolgen die het wegvallen van de informatievoorziening heeft op het bedrijfsproces.

Scope

Uw organisatie geeft aan welke bedrijfsprocessen onderdeel uitmaken van de analyse, en bepaalt daarmee de scope.

Werkwijze

Om per bedrijfsproces een goed beeld te verkrijgen van de informatieafhankelijkheid worden interviews gehouden met de betreffende proceseigenaren. Daarbij staat de vraag centraal: “Welke gevolgen heeft het wegvallen van de informatievoorziening, in de tijd gezien, voor het betreffende proces en voor de totale organisatie”. De gevolgen worden gespecificeerd naar financiële, operationele, organisatorische, juridische, politieke, maatschappelijke en imago-impact.

Rapportage

De rapportage behandelt zowel de diverse bedrijfsprocessen afzonderlijk als de organisatie als geheel. Per bedrijfsproces worden de gevolgen in de tijd, naar type impact, weergegeven. In de managementsamenvatting is een kleurenkaart opgenomen waarmee in één oogopslag duidelijk wordt welke bedrijfsprocessen een hoge afhankelijkheid kennen en welke een lage. Desgewenst kunnen de resultaten worden gepresenteerd aan het management.

Tijdsduur

De benodigde tijd voor de afhankelijkheidsanalyse wordt direct bepaald door de gewenste scope. Per bedrijfsproces zal circa een halve dag benodigd zijn voor de interviews. De analyse en rapportage vraagt gemiddeld circa 3 dagen. Er dient rekening gehouden te worden met een minimale doorlooptijd van circa 8 weken.

Prioriteitstelling

Aan de hand van de resultaten van de kwetsbaarheids- en afhankelijkheidsanalyse kan vervolgens samen met u een prioriteitenoverzicht worden opgebouwd. Uiteindelijk vormt deze prioriteitstelling de basis voor een integraal ICT-beveiligingsplan.

Doelstelling

Het stellen van prioriteiten ten aanzien van het treffen van beveiligingsmaatregelen.

Scope

De scope van de prioriteitstelling wordt indirect bepaald door de scope van de uitgevoerde kwetsbaarheidsanalyse en de afhankelijkheidsanalyse. De gewenste detailscope van de prioriteitstelling wordt in overleg met u bepaald.

Werkwijze

De resultaten van de kwetsbaarheidsanalyse en de afhankelijkheidsanalyse worden in combinatie met elkaar nader onderzocht. Vervolgens worden, in overleg met uw organisatie, prioriteiten toegekend aan de risico's en de daarmee verband houdende maatregelen. Zo zal een kritische score op een bepaald beveiligingsvlak, gecombineerd met een hoge afhankelijkheid vanuit een bedrijfsproces, leiden tot een hoge prioriteit.

Rapportage

De prioriteitstelling resulteert in een overzicht van de gestelde prioriteiten. Dit overzicht wordt gepresenteerd in de vorm van een "Rapport prioriteitstelling".

Tijdsduur

De prioriteitstelling vindt normaliter plaats aansluitend op de uitvoering van de kwetsbaarheids- en/of afhankelijkheidsanalyse en vraagt doorgaans 1 tot 2 dagen.

Beveiligingsplanning

Binnen de fase beveiligingsplanning staat de vraag centraal hoe de informatiebeveiliging binnen uw organisatie kan worden bevorderd. Hiertoe zullen de met de risicoanalyse gestelde prioriteiten worden belicht vanuit het beveiligingsbeleid van uw organisatie. Onze security consultants zullen uw beleid en de gestelde prioriteiten vervolgens vertalen in een ontwerp. Dit ontwerp vormt de kern van het beveiligingsplan.

Doelstelling

Het ontwerpen van (een pakket van) maatregelen die zijn afgestemd op de met u geformuleerde prioriteiten. Bij het ontwikkelen van het ontwerp zal rekening worden gehouden met het door uw organisatie bepaalde beveiligingsbeleid. Hierbij vormt de speciaal hiertoe ontwikkelde matrix van maatregelen (zie bijlage) een belangrijk hulpmiddel. Het beveiligingsbeleid en een beschrijving van de beveiligingsorganisatie zal tezamen met het ontwerp worden opgenomen in het beveiligingsplan. Het beveiligingsplan kan daarmee gelden als beveiligingsbestek voor uw organisatie.

Scope

De scope van de beveiligingsplanning is direct gerelateerd aan de scope van de uitgevoerde risicoanalyse.

Werkwijze

Samen met u wordt gekeken naar het beveiligingsbeleid binnen uw organisatie. Wanneer dit beleid nog niet is geformuleerd, kunnen wij u daar desgewenst bij ondersteunen. Vervolgens zal een passend ontwerp worden gerealiseerd op basis van de prioriteitstelling die binnen de risicoanalyse is bepaald.

Rapportage

De beveiligingsplanning wordt opgeleverd in de vorm van een beveiligingsplan. Dit plan vormt de basis voor een Beveiligingshandboek. Desgewenst kan dit plan in een presentatie worden toegelicht.

Tijdsduur

Afhankelijk van de detailscope zal de fase beveiligingsplanning, inclusief rapportageperiode, circa 4 dagen in beslag nemen. Er dient rekening gehouden te worden met een doorlooptijd van circa 2 weken.

Implementatie, evaluatie en onderhoud

Desgewenst vertalen we het beveiligingsplan vervolgens met u in een concreet realisatievoorstel. Uiteraard kunnen we ook zorgdragen voor de implementatie. Vervolgens kunnen we de effectiviteit van het beveiligingsplan periodiek met u evalueren en voeren we, wanneer nodig, onderhoud uit op het plan.

Implementatie

Het beveiligingsplan vormt het als het ware het beveiligingsbestek voor uw organisatie. Desgewenst kunnen we een voorstel uitwerken ten aanzien van de realisatie van de ICT-gerelateerde maatregelen. Met betrekking tot de maatregelen die buiten het ICT-vlak vallen, kunnen wij u ondersteunen in het contact met leveranciers.

Wanneer u ingaat op ons realisatievoorstel zal hiertoe één of meerdere projecten worden gedefinieerd. Een ervaren projectleider zal in samenwerking met de Security Proces Manager de uitvering van de projecten begeleiden.

Evaluatie

Wij kunnen het effect van het totaalpakket aan beveiligingsmaatregelen periodiek met u evalueren. Wij bieden u in dit kader de mogelijkheid een evaluatiecontract af te sluiten.

Onderhoud beveiligingsplan

Naar aanleiding van de periodieke evaluatie zal het mogelijk nodig zijn aanpassingen te doen op het beveiligingsplan. Hiertoe bieden wij u een specifieke onderhoudsregeling.

2.4.4 Security Proces Management

Tijdens de diverse fasen van het concept vormt de Security Proces Manager het centrale aanspreekpunt voor uw organisatie. De Security Proces Manager coördineert tevens de uitvoering van de diverse activiteiten.

Doelstelling

Het efficiënt coördineren van de uitvoering van de diverse (deel)diensten die door de klant worden afgenomen en het fungeren als centraal aanspreekpunt voor de klant.

Scope

De scope van het Security Proces Management omvat de (deel)modulen die voor uw organisatie worden uitgevoerd.

Werkwijze

Na ontvangst van de opdracht tot uitvoering van één of meer deeldiensten zal de Security Proces Manager contact opnemen met de centrale contactpersoon binnen uw organisatie. Vervolgens zal afstemming plaatsvinden ten aanzien van de periode van uitvoering.

Rapportage

De Security Proces Manager zal de (deel)rapportages bundelen en in detail bespreken met uw organisatie. Hierbij kunnen tevens eventuele vervolgotrajecten worden besproken.

Tijdsduur

De duur van het Security Proces Management is direct afhankelijk van de periode van uitvoering van de deeldiensten.

Aandachtspunt:

- Centric Security Services is een totaalpakket aan diensten.
- Binnen het concept wordt een aantal essentiële stappen doorlopen om te komen tot een integrale vorm van informatiebeveiliging.

Met Centric Security Services vormt informatiebeveiliging niet langer een *sluitpost* op de begroting maar vervult het een *sleutelrol* binnen uw bedrijfsvoering!

3. Centric Continuity Services

Het dienstenportfolio Continuity Services richt zich op de continuïteit van uw organisatie. De diensten sluiten naadloos op elkaar aan en stellen u in staat uw continuïteitsorganisatie modulair vorm te geven.

- **Continuïteitsplanning**
De dienst Continuïteitsplanning beschouwt de voortgang van uw bedrijfsvoering vanuit een breed perspectief. Door middel van het formeren van teams binnen uw organisatie en het opstellen van een continuïteitsplan wordt invulling gegeven aan de vraag wat er moet gebeuren wanneer zich een calamiteit voordoet.
- **Uitwijkregelingen**
Centric kent diverse typen uitwijkregeling. Centraal binnen elk van deze regelingen staat de zorg en aandacht voor uw organisatie. Uniek is de garantie die wij u bieden ten aanzien van het operationeel brengen van uw Centric-applicaties.
- **Remote uitwijktest**
Wij bieden u de mogelijkheid om uw applicaties te testen vanuit uw eigen locatie. Zo kunnen uw applicatiebeheerders gewoon door blijven werken en vervolgens op een geschikt moment de testwerkzaamheden uitvoeren.
- **Uitwijktest op locatie**
Om zekerheid te verkrijgen ten aanzien van de fysieke en organisatorische mogelijkheden op uw eigen locatie bieden wij u de mogelijkheid om de periodieke test on-site uit te voeren.
- **Backup Test Service**
De backup van uw systeem vormt een cruciale rol in het restoreproces van uw informatiesysteem. Toch gebeurt het niet zelden dat de betreffende backup niet geschikt blijkt wanneer de restore daadwerkelijk wordt uitgevoerd. Om vroegtijdig zekerheid te verkrijgen ten aanzien van de bruikbaarheid van uw backup voeren wij periodiek een test uit met het teruglezen van uw tapes.
- **Tape Collecting & Storage Service**
Centric verzorgt voor uw organisatie het transport en de externe veiligstelling van backup bestanden. Dagelijks, wekelijks of zelfs permanent, kunnen deze bestanden op een duurzame wijze bij ons worden veiliggesteld.

3.1 Adviestraject Business Continuity

Het adviestraject Business Continuity geeft u in een korte tijd een breed beeld van de diverse aspecten van continuïteitsmanagement. Daarnaast wordt via een verkorte Business Impact Analyse een advies gevormd ten aanzien van de specifieke aspecten voor uw organisatie.

Doelstelling

Het doel van het adviestraject is het aftasten van het begrip Business Continuity en het verkrijgen van een globaal beeld van de diverse aandachtspunten met betrekking tot de continuïteit van uw organisatie.

Scope

De scope omvat uw gehele bedrijfsvoering. Een detailscope wordt tijdens het traject, in overleg met u, vastgesteld. U kunt binnen de scope denken aan bijvoorbeeld IT, telefonie, productie, personeel, e.d.

Werkwijze

- Inleiding Business Continuity
Ter inleiding zal een gesprek plaatsvinden met betrekking tot Business Continuity. Hierbij zullen de diverse begrippen worden toegelicht en zal de scope nader worden besproken.
- Beeldvorming
Vervolgens wordt een beeld gevormd van uw bedrijfsvoering en uw marktsituatie.
- Verkorte Business Impact Analyse (BIA)
In overleg met u wordt door middel van een verkorte BIA een beeld verkregen van de impact die een calamiteit zou hebben op uw bedrijfsvoering. Hiermee kunnen tevens BCC's (business critical components) worden geformuleerd.
- Advies
Op basis van de voorgaande activiteiten wordt een advies opgesteld ten aanzien van passende continuïteitsmaatregelen.

Rapportage

De rapportage omvat de vier aandachtsgebieden zoals die hierboven zijn verwoord. De kern van het rapport wordt gevormd door de aanbevelingen.

Tijdsduur

Het totale adviestraject zal doorgaans drie dagen in beslag nemen (inclusief interviews, analyses en rapportage). U dient hierbij rekening te houden met een totale doorlooptijd van twee weken.

3.2 Project Continuïteitsplanning

Het project Continuïteitsplanning omvat een gedegen stappenplan naar het opstellen van een continuïteitsplan voor uw organisatie. Het plan richt zich op de activiteiten die na een calamiteit genomen dienen te worden om de voortgang van uw bedrijfsvoering te bevorderen.

Doelstelling

De doelstelling van het project is primair het samenstellen van een passend continuïteitsplan voor uw organisatie. Secundair wordt in overleg met u een continuïteitsorganisatie vormgegeven en wordt de algehele bewustwording rond continuïteitsmanagement verhoogd.

Scope

De scope omvat primair uw IT-organisatie en de BCA's (Business Critical Applications). Optioneel kan deze scope worden uitgebreid naar overige aandachtgebieden binnen uw organisatie.

Werkwijze

- Samenstellen teams
Bij aanvang van het project worden binnen uw organisatie teams geformeerd. Ten aanzien van de primaire scope is dit een Crisis Management Team en IT Recovery Team.
- Gezamenlijke bijeenkomst (kick off)
In een gezamenlijke bijeenkomst worden alle betrokkenen geïnformeerd over het project en over wat er van hen verwacht wordt.
- Teambijeenkomsten
In overleg worden vervolgens per team separate bijeenkomsten gepland. Het gaat hierbij om circa 2 à 3 bijeenkomsten per team, gedurende de looptijd van het project. In deze bijeenkomsten worden de diverse aandachtsgebieden van Business Continuity geprojecteerd op de specifieke focus van het betreffende team. Stap voor stap wordt met de teamleden bezien hoe op een calamiteit gereageerd zou moeten en welke acties genomen zouden moeten worden. Hierbij wordt geïnventariseerd welke maatregelen al getroffen zijn, en welke actiepunten er liggen.
- Continuïteitsplan en sloepenrol
Op basis van deze informatie wordt een continuïteitsplan vormgegeven. In een afsluitende bijeenkomst wordt het plan met alle betrokkenen plenair doorgenomen en wordt een fictieve calamiteit uitgewerkt (sloepenrol).

Rapportage

De rapportage van het project Continuïteitsplanning omvat een continuïteitsplan ten behoeve van de gedefinieerde scope. Dit plan beschrijft de diverse aandachtspunten die van belang zijn om uw bedrijfsvoering voort te zetten na een calamiteit.

Tijdsduur

Het totale traject zal doorgaans per team circa 7 dagen in beslag nemen (inclusief alle bijeenkomsten, analyses en rapportage). U dient hierbij rekening te houden met een totale doorlooptijd van drie maanden.

Het traject vormt een vervolg op het adviestraject Business Continuity, waarin uw bedrijfskritische componenten worden vastgesteld.



3.3 Uitwijkregeling

Stelt u zich eens voor dat een incident uw pand en daarmee uw serverruimte ontoegankelijk maakt of dat een brand uw gehele computersysteem vernietigt, of...

De gevolgen voor de informatievoorziening, en daarmee voor de dienstverlening, kunnen zeer groot zijn. Centric IT Solutions biedt diverse uitwijkregelingen, juist voor dit soort situaties. Altijd met hetzelfde uitgangspunt: zodra dat nodig is, nemen wij alle zorg van u over voor zowel hardware als software!

3.3.1 Wat is nu precies een uitwijkregeling?

Een uitwijkregeling voorziet in een vervangend informatiesysteem wanneer uw eigen systeem onbruikbaar is geworden na een calamiteit. Zo wordt de continuïteit van uw bedrijfsvoering verhoogd.

Uitwijkconfiguratie

De basis voor deze voorziening vormt de uitwijkconfiguratie. Deze configuratie omvat een complete infrastructuur, inclusief serversystemen, netwerkfaciliteiten, werkstations en datacommunicatie. Wij kunnen de uitwijkregeling verzorgen ten aanzien van een zeer breed scala aan platformen. Hieronder valt bijvoorbeeld UNIX, Windows NT, Windows 2000/2003, Novell, Citrix en OS/400.

Draaiboek

Om de uitwijk zo efficiënt en effectief mogelijk te kunnen uitvoeren, stellen wij in overleg met u een passend uitwijkdraaiboek op. Dit draaiboek bevat naast essentiële informatie over contactpersonen en uw systemen ook een uitwijkprocedure die specifiek voor uw situatie wordt opgesteld.

Jaarlijkse test

Omdat uw situatie en omgevingsfactoren aan verandering onderhevig zijn, nodigen wij u jaarlijks uit om samen met ons uw uitwijkprocedure te testen. Uw kernapplicaties worden hierbij operationeel gebracht volgens het draaiboek. Om de test zo efficiënt mogelijk uit te voeren, wordt deze uitgebreid door onze specialisten voorbereid. Eventuele testissues worden door ons beschreven en waarnodig worden aanpassingen in het uitwijkdraaiboek verwerkt. Zo wordt het draaiboek up-to-date gehouden.

Calamiteit

Elke onverwachte, plotselinge gebeurtenis die leidt tot uitval van uw systeem kan als calamiteit worden aangemerkt. Is er sprake van een calamiteit, iets dat u overigens zelf bepaalt, dan neemt Centric IT Solutions de totale verantwoordelijkheid op zich en neemt zij de zorg voor het automatiseringssysteem van u over. U heeft op zo'n moment immers wel wat anders aan uw hoofd en het eigen personeel is vaak overal tegelijk nodig. Er gelden hierbij geen beperkingen ten aanzien het aantal meldingen.

Locatiekeuze

Wij kunnen de uitwijk voor u verzorgen op elke hiertoe toegankelijke locatie in Nederland. Zo kan bijvoorbeeld een ruimte worden ingericht op uw locatie of bijvoorbeeld op een nevenvestiging. Ook bent u welkom in ons uitwijkcentrum, waar wij speciaal hiertoe een ruimte en werkplekken hebben ingericht. De gewenste locatie is uiteraard mede afhankelijk van de aard van de calamiteit. U kunt uw keuze dan ook bij melding van de uitwijk kenbaar maken.

Binnen 2 x 24 uur weer operationeel

Een calamiteit komt altijd onverwacht. Onze uitwijkorganisatie staat dan ook 7 dagen per week, 24 uur per dag voor u klaar om de uitwijk te verzorgen. Wij zorgen er voor dat uw systeem binnen maximaal 2 x 24 uur na beschikbaarheid van uw back-up tape(s) weer operationeel is.

Aanvullende diensten

De uitwijkregeling is een zeer complete dienst, waarbij u de totale zorg voor het operationeel brengen van uw serversystemen uit handen wordt genomen. Centric gaat echter nog een belangrijke stap verder. Wij bieden u een breed dienstenpalet op het gebied van informatiebeveiliging en continuïteit. Als bijlage vindt u een korte beschrijving van de betreffende aanvullende diensten op het gebied van Continuity Management.

Unieke zorg, óók voor uw applicaties

Een belangrijk voordeel is dat Centric IT Solutions u, bij een calamiteit, desgewenst kan ondersteunen bij het tijdig operationeel krijgen van uw Centric-applicaties. U heeft immers niets aan een werkend computersysteem, als u uw programma's niet kunt gebruiken!



3.3.2 Bijzondere kenmerken Centric uitwijkregeling

Het realiseren van een vervangende omgeving bij een calamiteit vraagt specialistische kennis en een klantgerichte benadering. Graag noemen wij u enkele specifieke kenmerken van onze uitwijkservice:

- **Ervaring**
De Centric-organisatie heeft al ruim 20 jaar ervaring in het verzorgen van uitwijkfaciliteiten voor gemeenten en bedrijven.
- **Grote betrokkenheid**
Als klant ervaart men tijdens de testen de grote betrokkenheid van de specialisten met de specifieke klantsituatie. De specialisten zijn immers veelal persoonlijk betrokken geweest bij de implementatie van de betreffende infrastructuur bij de klant.
- **Uitgebreide voorbereiding test**
Om geen onnodige tijdsinvestering van u te vragen, wordt de jaarlijkse uitwijktest door onze specialisten voorbereid. Zo worden (indien gewenst) de tapes zonder meerprijs reeds van te voren teruggelezen en kunt u op de testdag dus direct gaan testen.
- **Intensieve begeleiding test**
Op de testdag wordt u begeleid door onze uitwijkspecialisten. Zo kunt u profiteren van de door ons opgebouwde kennis en ervaring en kunnen eventuele testissues op een passende wijze snel worden verholpen.
- **Soepele contract handling**
Deze flexibiliteit uit zich ook in een soepele opstelling ten aanzien van gewenste aanpassingen op de uitwijkspecificaties.
- **Gunstige tariefstelling**
Vanuit een speciaal ontwikkelde calculatiemethodiek kunnen wij een zeer gunstige tariefstelling realiseren. Binnen deze methodiek wordt voorkomen dat er een overlap in tarieven ontstaat wanneer u meerdere systemen in de uitwijkregeling wilt opnemen.
- **Garantie Centric-applicaties (!)**
Uniek is de garantie die wij u bieden ten aanzien van het operationeel brengen van uw Centric-applicaties. Wij hebben immers de benodigde kennis van de applicaties in huis. *Tijdens de testen vormt deze kennis een plezierige zekerheid, tijdens een calamiteit is zij onmisbaar.*

3.4 Remote Backup Service

De Remote Backup Service (RBS) vormt een online storage-dienst die wordt geleverd in samenwerking met en ondersteund wordt door gespecialiseerde partners.

Deze beheerde dienst borgt optimale zekerheid voor het veiligstellen van de data en de transactiegegevens. Door het gebruik van de NetApp-technologie in combinatie met de unieke Snapshot-technologie zijn de data en de transactiegegevens beschermd terwijl te allen tijde restores en recovery vanaf disk mogelijk zijn.

De gegevens worden door middel van SnapVault naar het datacenter gerepliceerd. Hierdoor is de consistente back-up in de vorm van Snapshots op een externe locatie beschikbaar voor archivering, restores en disaster recovery. Een tweede kopie (of mirror) hiervan zorgt er voor dat uw data beschikbaar blijft, zelfs na een calamiteit op in het (primaire) datacenter. Zo wordt optimale beschikbaarheid gewaarborgd.

Datacenters

Binnen onze dienstverlening kunnen wij beschikken over diverse datacenters. De storage systemen staan in een omgeving met een beschikbaarheidgarantie van 99,98% voor wat betreft de stroomvoorziening, klimaatbeheersing, toegang en beheer. Door een groot aantal beveiligingsmaatregelen zijn de risico's van diefstal, brand, inbraak, vandalisme en waterschade minimaal. De systemen worden 24 uur per dag, 7 dagen per week bewaakt door een professionele beveiligingsdienst, elektronisch beveiligde toegangsdeuren en videocamera's.

InControl Portal

De centrale interface binnen deze storage oplossing vormt de 'InControl Portal'. De portal vormt een interactief en veilig, SLA-gestuurd, communicatie- en managementplatform. Met de InControl Portal kan de individuele eindgebruiker via een beveiligde verbinding zijn storage- en replicatiediensten monitoren en beheren. Bovendien geeft de portal duidelijke up-to-date en real-time management overzichten over de storage en replicatie.

Hierdoor heeft u een duidelijk beeld over de status, capaciteit, verbruik en SLA's. Deze informatie ondersteunt uw organisatie bij korte en lange termijn capaciteitsplanning en bandbreedtemanagement.



Welke functionaliteit biedt de InControl Portal?

- Overzichtelijke, accurate, veilige, real-time toegang tot diverse diensten;
- Rapportage en statusoverzichten van de storage en replicatie;
- Rapportage over de voortgang van de service in relatie tot de SLA;
- Trends over de data, weergegeven in heldere grafieken;
- De mogelijkheid om online verzoeken tot escalatie te doen;
- Online herstellen of terugzetten van data naar de eigen omgeving;
- Eenvoudig doorvoeren van wijzigingen of toevoegingen.

3.5 Back-up Test Service

Het maken van uw dagelijkse of wekelijkse back-up is waarschijnlijk goed geregeld binnen uw organisatie.

Maar hoe zeker bent u ervan dat uw back-up ook de gewenste informatie bevat?

Tijdens de vele uitwijktesten die wij met onze klanten uitvoeren, constateren wij regelmatig dat een ogenschijnlijk goede back-up bij het teruglezen niet (voldoende) bruikbaar blijkt te zijn. Om meer zekerheid te verkrijgen omtrent de inhoud van de tape(s) is het verstandig deze regelmatig te (laten) controleren.

Hier toe bieden wij u onze Back-up Test Service. Een dienst waarbinnen wij een aantal keer per jaar uw tape(s) kunnen controleren op de juistheid van de inhoud. Deze test vindt plaats in ons Continuïteit Center.

Binnen de Back-up Test Service bieden wij u twee test-opties:

1. Back-up Content Scan
Binnen deze optie wordt de inhoud van de door u aangeleverde tape(s) bepaald. Deze Back-up Content Scan geeft u zekerheid ten aanzien van de aanwezigheid van de betreffende data. De bevindingen worden verwoord in een bondige rapportage.
2. Back-up Recovery Test
Binnen deze optie wordt onderzocht in hoeverre met de door u aangeleverde tape(s) uw omgeving daadwerkelijk kan worden teruggeplaatst. In de bondige rapportage worden screendumps opgenomen van de werkende omgeving.

Beide testopties kunnen, ook in combinatie, zowel éénmalig als in abonnementvorm voor u worden verzorgd. De Back-up Test Service vormt tevens een prima aanvulling op een eventuele uitwijkregeling.



3.6 Tape Collecting & Storage Service

Optimale zekerheid en beschikbaarheid van uw back-up bestanden.

De steeds verdergaande automatisering van bedrijfsinformatie brengt met zich mee dat ook steeds meer afhankelijkheid ontstaat van geautomatiseerde systemen. In verband hiermee dient men zich *vooraf* constant af te vragen of recente bedrijfsinformatie voorhanden is op het moment dat zich een ernstige calamiteit heeft voorgedaan. In dat kader is het van groot belang, procedures op te stellen op basis waarvan dagelijks/wekelijks back-up bestanden worden aangemaakt en veiliggesteld.

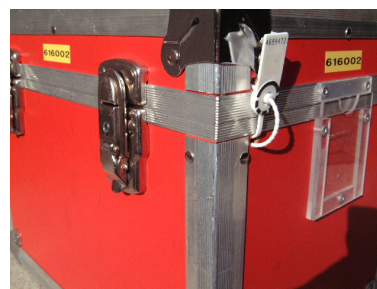
Centric verzorgt voor uw organisatie het transport en de externe veiligstelling van back-up bestanden. Dagelijks, wekelijks of zelfs permanent, kunnen deze bestanden op een duurzame wijze bij ons worden veiliggesteld. Volgens contractueel overeengekomen procedures worden de bestanden op vaste dagen opgehaald/gewisseld in speciaal daarvoor geconstrueerde en verzegelde data-transport-koffers die worden opgeslagen in ondergrondse, volledig geconditioneerde bunkers, gelegen in het noorden, midden en zuiden van het land.

Naast het feit dat met betrekking tot deze dienst constructieve afspraken kunnen worden gemaakt, bestaat ook de mogelijkheid om een stap verder te gaan door ook de *tapehandling* aan ons uit te besteden. Hiermee ontstaat een complete vorm van dienstverlening met de garantie dat de meest elementaire informatie(-dragers) dagelijks of wekelijks geruisloos wordt veiliggesteld.

Indien een beroep moet worden gedaan op de opgeslagen bestanden (bijv. calamiteit), zal volgens de bijgehouden registratie snel kunnen worden gehandeld om de benodigde informatie op de vooraf afgesproken plaats van bestemming af te leveren (locatie zelf of uitwijkcentrum). Daartoe verleent Centric de service om tijdens, maar ook buiten kantoor tijd, op afroep de opgevraagde informatie *binnen drie uur* op de plaats van bestemming te bezorgen.

De voordelen voor uw organisatie zijn groot:

- Continuïteit
- Verzorgd (anoniem) transport door gecertificeerde organisatie
- Duidelijke registratie van opgeslagen bestanden en activiteiten
- Duurzame opslag
- 24 uren bereikbaarheid, optimale beschikbaarheid
- *Discipline: contractuele afspraken*
- Ontlasting eigen personeel
- Gemak
- Optimale integratiemogelijkheden met overige diensten van Centric, bijvoorbeeld de uitwijkregeling.



Bijlage Reactieformulier

Centric IT Solutions
Cluster Systems & Services
T.a.v. Commerciële Binnendienst
Postbus 751
2800 AT GOUDA

FAX: (0182) 56 22 11

Graag worden wij nader geïnformeerd over de mogelijkheden die de portfolio's Centric Security & Continuity Services bieden voor onze organisatie.

Bedrijf :
Naam :
Functie :
Telefoonnummer :
E-mailadres :

Wij zullen hiertoe zo spoedig mogelijk contact met u opnemen. Bij voorbaat dank voor uw interesse.