De US-CCU Checklist voor cybersecurity

Door John Bumgarner en Scott Borg

DEFINITIEVE VERSIE

2007

Vertaald door het

Nationaal Adviescentrum **Vitale Infrastructuur**

Deze checklist voor cybersecurity wordt gratis ter beschikking gesteld, maar er rusten wel auteursrechten op en mag daarom zonder de uitdrukkelijke instemming van de U.S. Cyber Consequences Unit (een onderzoeksinstituut zonder winstoogmerk) niet in een andere vorm worden verkocht of doorverkocht.

Gebruikers van deze lijst wordt erop gewezen dat geen enkele checklist volmaakt en volledig is en dat alle maatregelen die in deze lijst worden beschreven in principe omzeild kunnen worden. De U.S. Cyber Consequences Unit, verder aangeduid als US-CCU, aanvaardt geen aansprakelijkheid voor de consequenties van het uitvoeren van deze checklist noch voor de fouten die er mogelijk in staan.

US-CCU beoogt deze checklist jaarlijks te actualiseren. Suggesties voor verbetering zijn meer dan welkom en kunnen gestuurd worden naar: checklist_comments@usccu.us

De opstellers zijn de mensen die suggesties hebben gedaan naar aanleiding van de concepten veel dank verschuldigd.

De US-CCU Checklist voor cybersecurity

Door John Bumgarner en Scott Borg

Deze checklist is bedoeld als een uitgebreid overzicht van de stappen die ondernemingen en organisaties moeten nemen om minder kwetsbaar te worden voor cyberaanvallen. Deze lijst is gebaseerd op een groot aantal zwakke plekken in de netwerkbeveiliging die John Bumgarner, Research Director for Security Technology van de U.S. Cyber Consequences Unit, en Scott Borg, als directeur verbonden aan hetzelfde instituut, bij hun werk zijn tegengekomen. Pas toen deze lijst de huidige lengte begon te naderen, hebben de opstellers eerdere checklists op dit gebied geraadpleegd, om ervoor te zorgen dat relevante onderwerpen van die lijsten ook op deze lijst zouden komen te staan. Daarna werden voorlopige versies van de nieuwe lijst voorgelegd aan grote aantallen deskundigen op het gebied van cybersecurity, waar honderden opmerkingen op kwamen. Door alle meer praktische suggesties op te nemen in een document, hebben de opstellers geprobeerd een zo compleet mogelijk overzicht te geven van bekende routes voor cyberaanvallen en de maatregelen die nodig zijn om ze te beschermen.

Om de lijst zo duidelijk en bruikbaar mogelijk te maken, zijn de zwakke punten en tegenmaatregelen ondergebracht in zes makkelijk van elkaar te onderscheiden componenten van informatiesystemen: 1) hardware, 2) software, 3) netwerken, 4) automatisering, 5) personen en 6) leveranciers.

Met een aantal andere punten wordt duidelijk gemaakt hoe deze categorieën worden gehanteerd. Zwakke punten in software zijn vooral de zwakke punten in de toegang ervan, want zodra software geproduceerd, geverifieerd en geïnstalleerd is, moet iemand er toegang toe hebben voordat het een veiligheidsrisico wordt. Kwetsbare punten in de levering van software moeten behandeld worden als een vast onderdeel van de kwetsbare plekken van een informatiesysteem, omdat softwareleveranciers ook lang na de oorspronkelijke aankoop of licentieverlening regelmatig toegang hebben tot hun informatiesystemen. Andere leveranciers hoeven meestal niet als kwetsbare plekken te worden behandeld, aangezien ze meestal niet lang betrokken blijven bij het functioneren van het informatiesysteem. Kwetsbare punten in de automatisering zijn niet alleen alle systemen die als brug tussen de informatieprocessen en de fysieke processen fungeren, maar ook alle automatische processen waaruit fysieke producten ontstaan. Aangezien uit vrijwel elk informatiesysteem ten minste een fysiek product voortkomt (zijn eigen

backupmedia), zijn kwetsbare plekken niet alleen belangrijk voor de fysieke industrie, maar voor alle informatiesystemen.

Alle belangrijke gebieden waarop cyberaanvallen kunnen plaatsvinden zijn onderverdeeld in twee of meer aanvalsroutes. Deze beperktere aanvalsroutes zijn onderverdeeld naar de activiteiten die moeten plaatsvinden of waarop toezicht moet worden uitgeoefend om de veiligheid van deze systeemcomponenten te handhaven. Dit resulteert in zestien routes die zijn georganiseerd volgens de onderstaande tabel.

OVERZICHT VAN DE BELANGRIJKSTE AANVALSROUTES
Gebied 1: Kwetsbare plekken in de hardware
Route 1: fysieke apparatuur
Route 2: fysieke omgeving
Route 3: fysieke nevenproducten
Gebied 2: Kwetsbare plekken in softwaretoegang
Route 4: authenticatie van identiteit
Route 5: applicatierechten
Route 6: validatie van input
Route 7: passende gedragspatronen
Gebied 3: Kwetsbare plekken in netwerken
Route 8: permanente netwerkverbindingen
Route 9: intermitterende netwerkverbindingen
Route 10: netwerkonderhoud
Gebied 4: Kwetsbare plekken in de automatisering
Route 11: sensoren en controlesystemen op afstand
Route 12: backup-procedures

Gebied 5: Kwetsbare plekken onder menselijke beheerders
Route 13: onderhoud van beveiligingsprocedures door personen
Route 14: opzettelijke acties die de veiligheid bedreigen
Gebied 6: Kwetsbare plekken in de levering van software
Route 15: intern beleid voor software-ontwikkeling
Route 16: relaties met externe leveranciers

Binnen deze 16 routes zijn er nog lagere categorieën met daarin de tegenmaatregelen ter bescherming van de aanvalsroutes. Alle kwetsbare punten in de checklist worden beschreven met behulp van de bijbehorende tegenmaatregelen. Er wordt gebruik gemaakt van vragen, zodat degene die een punt controleert weet dat de desbetreffende maatregelen inderdaad zijn getroffen als het antwoord “ja” luidt. Sommige vragen kunnen nogal vaag lijken. De termen “strikt”, “streng”, "adequaat” en “voldoende” kunnen bijvoorbeeld nogal onduidelijk overkomen, maar toch hebben ze een vrij precieze betekenis in het verband waarin ze worden gebruikt. In de meeste gevallen hoeft u zich alleen af te vragen wat de bedoeling van een tegenmaatregel is om dan na te gaan of de getroffen maatregelen passen bij dat doel.

We hebben geprobeerd modekreten en technische termen zoveel mogelijk te vermijden. We hebben ook geprobeerd zo kort, duidelijk en eenvoudig mogelijk te zeggen wat we bedoelen. Mocht iemand een onderwerp zoeken met behulp van een trendy woord, dan zal het hier vast in staan, maar dan niet onder die trendy term.

Veel vragen over “beleid van de onderneming” en “verificaties” hebben we met opzet weggelaten in deze checklist, want we mogen aannemen dat die meestal voor zich spreken. *Elke* maatregel die in deze checklist is opgenomen moet worden uitgevoerd als bedrijfsbeleid. *Elke* beveiligingsmaatregel uit deze checklist moet op de een of andere manier worden geverifieerd. Er moet voor gezorgd worden dat de beveiligingsmaatregelen uit de checklist ook echt worden uitgevoerd. Beleid en verificatie zijn daar vooral hulpmiddelen bij. Wanneer “ondernemingsbeleid” of “verificatie” in de checklist worden gebruikt, moet nagegaan worden waar er speciale procedures moeten worden ingesteld. Doorgaans blijkt uit de grondbeginselen van goed management wel welk beleid en de verificaties nodig zijn.

In deze checklist staat meestal niet welke administratieve en organisatorische maatregelen nodig zijn voor de uitvoering van een goede cybersecurity oftewel

netwerkbeveiliging. Deze maatregelen komen namelijk neer op het goed inzetten van rollen, verantwoordelijkheden, prikkels en bevelsstructuren en dat hoort bij de algemene managementpraktijk en niet bij netwerkbeveiliging. Sommige beginselen en richtlijnen voor het administratieve deel van netwerkbeveiliging zijn opgenomen in andere documenten afkomstig van US-CCU. Er zijn wel veel andere administratieve maatregelen die uitgevoerd kunnen worden ingezet voor dezelfde voor netwerkbeveiliging maatregelen.

Hoewel overal in de tekst "onderneming" gebruikt wordt, moet dat woord heel ruim worden opgevat. Elke organisatie met een budget en informatiesystemen waar praktische activiteiten worden uitgevoerd kan voor de netwerkbeveiliging worden gezien als een “onderneming”. Dat zijn dus ook overheidsinstellingen, non-profitorganisaties en de meeste non-gouvernementele organisaties. Deze organisaties voeren activiteiten uit waarbij waarde ontstaat en het doet er niet toe of die waarde in financiële termen wordt uitgedrukt of beoordeeld. We hebben voor de term “onderneming" gekozen omdat het grootste deel van de informatiesystemen in een land in het eigendom zijn van en beheerd worden door ondernemingen.

Veel ondernemingen zullen ontdekken dat niet alle vragen in de checklist van toepassing zijn op hun informatiesystemen. Bij sommige ondernemingen wordt bijvoorbeeld geen gebruik gemaakt van de sensors en besturingssystemen die op afstand worden bestuurd en die behandeld worden in de meest vragen onder route 11. Andere zullen vinden dat fysiek gescheiden datacentra, zoals die in veel vragen aan bod komen, voor hen niet praktisch zijn. Weer andere ondernemingen zullen geen systemen hebben die zo ontzettend kritisch zijn dat er de meest uitgebreide beveiligingsmaatregelen uit de checklist voor nodig zijn. Voordat ondernemingen denken dat een punt op hen niet van toepassing is, moeten ze nagaan of het toch niet hoort bij een kwetsbaar punt dat ze misschien over het hoofd hebben gezien. Eigenschappen van een informatiesysteem die niet echt opvallen in bepaalde bedrijfstakken kunnen daar toch een grote kwetsbare factor zijn.

De tegenmaatregelen waar een astriks (*) achter staat zijn op dit moment nog erg ingewikkeld of erg duur om uit te voeren met de producten en technologieën die meestal verkrijgbaar zijn bij commerciële leveranciers. Dit betekent dat er, voorlopig, speciale initiatieven voor nodig zijn, die variëren van geïmproviseerde hardware tot en met het bestellen van programmatuur op maat. Vooral beveiligingsleveranciers, overheidsinstanties en instellingen die onderzoek en ontwikkeling financieren op het gebied van beveiliging moeten letten op de punten met een astriks. Hier zijn heel hard nieuwe producteigenschappen of nieuwe diensten voor verbetering van de informatiebeveiliging nodig.

Wanneer u deze US-CCU checklist gebruikt als norm voor informatiebeveiliging, moet u de punten met een astriks als facultatief beschouwen. De komende maanden en jaren zullen er steeds weer nieuwe technologieën, producten en diensten bijkomen en zal de checklist regelmatig bijgewerkt worden, waarbij er veel astriksen zullen kunnen verdwijnen, en veel punten die nu nog facultatief zijn van lieverlee standaard worden in de beveiligingspraktijk. Voorlopig kan van ondernemingen niet verwacht worden dat ze beveiligingproblemen oplossen waarvoor nog geen standaardoplossingen beschikbaar zijn, ook al kunnen deze problemen heel belangrijk zijn.

Bepaalde punten op de checklist die *niet* voorzien zijn van een astriks kunnen ingewikkeld klinken of te duur lijken om geïmplementeerd te worden, maar in de meeste gevallen lijkt dat maar zo. Toegegeven: er zijn zeer kostbare manieren en producten om deze kwetsbare punten te verhelpen. Voor bijna alle punten zonder astriks geldt echter dat er ook relatief goedkope manieren zijn om aan een veiligheidsvereiste te voldoen.

We kunnen netwerkbeveiliging beschouwen als een “risicodriehoek”, waarvan de hoeken bedreigingen, gevolgen en kwetsbare punten zijn; in deze checklist gaat het alleen over de kwetsbare punten. Maar om deze checklist op een kosteneffectieve manier toe te passen moet ook rekening worden gehouden met de andere hoeken van de risicodriehoek. Dit betekent dat we de bedreigingen goed genoeg moeten begrijpen om een beeld te krijgen van de soort aanvallen die in een bepaalde periode verwacht kunnen worden. En belangrijker: het betekent dat we de gevolgen voldoende moeten begrijpen om te beseffen hoe kritisch bepaalde softwareapplicaties en hoe kwetsbaar de verschillende soorten informatie zijn en welk type beveiligingskosten gerechtvaardigd is om ze te beschermen. Deze onderwerpen vallen weliswaar buiten de checklist zelf, maar worden vrij uitgebreid beschreven in het lijvige rapport van Scott Borg met de titel *Cyber-Attacks: A Handbook for Understanding the Economic and Strategic Risks*, dat binnenkort verschijnt.

Deze checklist van US-CCU is niet bedoeld als vervanger van alle eerdere checklists op dit terrein en ook niet om ze overbodig te maken. Om deze lijst te kunnen gebruiken zullen er meestal juist aanvullende, gespecialiseerde checklists nodig zijn met meer details van specifieke beveiligingsproblemen, van de nieuwste technische ontwikkelingen en van de speciale behoeften van afzonderlijke bedrijfstakken. We hopen echter dat deze lijst van US-CCU helpt de aandacht te richten op veel kwetsbare punten die anders misschien over het hoofd zouden worden gezien.

Gebied 1: Kwetsbare plekken in de hardware

Route 1: Fysieke apparatuur

Inventariseren van fysieke apparatuur

1.01. Heeft de onderneming een correcte beschrijving van de elektronische apparatuur in elke ruimte op elke fysieke locatie?

1.02. Is er een snelle en eenvoudige procedure om deze lijst bij te werken zodra de verantwoordelijke medewerker toestemming heeft gegeven voor verplaatsing van de apparatuur?

1.03. Is elk elektronisch apparaat voorzien van een barcode of een ander middel voor eenvoudige herkenning?

1.04. Indien informatieapparatuur gevoelig is, is die dan voorzien van RFID-chips zodat verplaatsingen bijna in real-time gevolgd kunnen worden met behulp van radiogolven? *

1.05. Is er specifiek beleid voor welke apparatuur vanuit de onderneming mag worden meegenomen en welke toestemming daarvoor nodig is?

1.06. Als er elektronische apparatuur moet worden meegenomen, is er dan een efficiënte procedure om de verplaatsingen ervan te volgen?

1.07. Vinden er regelmatig onaangekondigde inspecties plaats om te controleren of de elektronische apparatuur op de locatie staat die vermeld is in de apparatuurlijst?

Bewaken van fysieke apparatuur

1.08. Is zeer belangrijke elektronische apparatuur geïntegreerd in datacentra om ze makkelijker te beschermen?

1.09. Zijn er fysieke veiligheidsbarrières om elektronische apparatuur te beschermen tegen diefstal of vernieling?

1.10. Wanneer externe harde schijven en andere externe opslagapparatuur die gevoelige informatie bevatten eenvoudig mee te nemen zijn, zijn ze dan verankerd als een extra beveiligingsmaatregel? *

1.11. Zijn de kabelkasten altijd goed afgesloten?

1.12. Zijn de datacentra en kabelkasten voorzien van inbraakalarmen?

1.13. Worden de inbraakalarmen van de datacentra en kabelkasten op afstand bewaakt?

1.14. Is de fysieke toegang tot de console interfaces van beveiligingsvoorzieningen, zoals die voor het beheer van firewalls en inbraakdetectiesystemen beperkt tot bevoegde gebruikers?

1.15. Zijn er in de datacentra en andere ruimten met kritische informatieapparatuur verlaagde plafonds of verhoogde vloeren en zijn die beveiligd tegen toegang vanuit aangrenzende vertrekken en ventilatiesystemen?

Beveiliging van elektronische toegangspoorten

1.16. Zijn netwerktoegangspoorten die niet in gebruik zijn fysiek uitgeschakeld door middel van netwerk switches of fysieke barrières om toegang door onbevoegden te voorkomen?

1.17. Wanneer de netwerkpoorten niet werkelijk zijn uitgeschakeld, zijn er dan procedures voor de controle op onbevoegde toegang tot deze poorten?

1.18. Zijn er fysieke veiligheidsbarrières, zoals afgesloten behuizingen of pluggen om alle mediatoegangen van het systeem, bijvoorbeeld USB-poorten, CD-drives etc. te beschermen?

1.19. Wanneer de mediapoorten niet werkelijk zijn uitgeschakeld, zijn er dan procedures voor de controle op onbevoegde toegang tot deze poorten? *

1.20. Is de fysieke toegang tot alle ongebruikte poorten op netwerk switches uitgeschakeld, met name de SPAN-port (Switched Port Analyzer)?

1.21. Is de fysieke toegang tot alle console- en hulppoorten op de routers beveiligd?

Bescherming van de communicatieverbindingen

1.22. Zijn er fysieke beveiligingsbarrières geplaatst ter bescherming van de netwerkkabels die naar en van het systeem lopen, zodat ze niet makkelijk doorgesneden of beschadigd kunnen worden?

1.23. Zijn de kritische communicatiekabels en kabelbehuizingen binnen de onderneming zo aangelegd dat fysieke toegang om transmissies te onderscheppen bemoeilijkt wordt?

1.24. Is de locatie waar de telefoon- en datakabels het gebouw binnen komen fysiek beveiligd?

1.25. Onderzoekt de onderneming de fysieke beveiligingspraktijk van internet service providers (ISP) en andere communicatiebedrijven voordat besloten wordt van welke leveranciers diensten worden ingekocht?

Controle op de fysieke toegang tot apparatuur

1.26. Is het datacentrum altijd goed afgesloten en worden de toegangsdeuren gesloten gehouden?

1.27. Is op de toegangsdeuren van het datacentrum te zien dat het een zone is die alleen voor bevoegden toegankelijk is?

1.28. Wordt de toegang tot het datacentrum gecontroleerd met behulp van bijv. scanbare badges, smart cards, elektronische toegangspassen, biometrische voorzieningen of sloten voorzien van persoonlijke combinaties?
1.29. Worden de logs voor de toegangscontrole (bijv. sleutelkaarten en logs voor videosurveillance) regelmatig getoetst/gecontroleerd?
1.30. Wordt daarbij een analyse gemaakt van mislukte fysieke toegangspogingen?
1.31. Wordt er gebruik gemaakt van videosurveillance voor het monitoren van de toegangsportalen tot datacentra en andere zones met apparatuur voor informatieverwerking?
1.32. Wanneer er videosurveillance plaatsvindt in de datacentra, wordt er dan op afstand gemonitord?
1.33. Wanneer er videosurveillance plaatsvindt in de datacentra, worden de beelden dan opgeslagen in een vast medium dat bestand is tegen manipulatie/sabotage?
1.34. Wanneer er videosurveillance plaatsvindt in de datacentra, worden de beelden dan lang genoeg bewaard om eventuele beveiligingsincidenten die een aantal maanden niet zijn opgemerkt te onderzoeken?
1.35. Wanneer er gebruik wordt gemaakt van beveiligingscamera's, met name draadloze, voor monitoring, zijn deze beschermd tegen blokkeren, bekijken door onbevoegden en het manipuleren van beelden? *
1.36. Is de toegang tot de beheerconsoles van beveiligingscomponenten, zoals firewalls en IDS, fysiek beperkt tot bevoegde gebruikers?
1.37. Wordt de fysieke toegang tot alle draadloze en infrarood uplinks gecontroleerd en gemonitord?
1.38. Zijn faxmachines waarmee gevoelige informatie wordt ontvangen en afgedrukt beschermd tegen toegang door onbevoegden?

Controleren welke medewerkers fysiek toegang hebben

1.39. Wordt er gecontroleerd wie de grotere fysieke faciliteit waar de informatiesystemen draaien binnengaat en verlaat?
1.40. Gelden er duidelijke beperkingen voor de medewerkers die toegang hebben tot het datacentrum en worden die beperkingen strikt gehandhaafd?
1.41. Zijn er duidelijke regels voor de toegang tot de kabelkasten en wordt daar strikt op gecontroleerd?
1.42. Wordt er strikt op toegezien dat de rechten voor fysieke toegang worden gewijzigd zodra de functie van een medewerker verandert?

1.43. Zijn er rechten voor de fysieke toegang en worden de badges etc. direct geblokkeerd zodra een medewerker wordt ontslagen, ontslag neemt of met pensioen gaat?
1.44. Vinden er strenge controles plaats wanneer leveranciers het datacentrum binnenkomen en dan zo dat alleen bevoegd personeel van de leverancier wordt toegelaten?
1.45. Geldt voor het datacentrum een registratieprocedure wanneer derden tot de beveiligde ruimten worden toegelaten?
1.46. Worden de rechten en middelen voor de fysieke toegang voor leveranciers regelmatig gecontroleerd en onmiddellijk opgeheven of geblokkeerd wanneer de status van de medewerkers van de leverancier verandert?
1.47. Geldt er streng beleid voor de toegang tot het datacentrum buiten kantoortijd door personeel zoals beheerders of conciërges?
1.48. Wordt in het beveiligingsbeleid beschreven hoe de toegang tot het datacentrum in noodgevallen verloopt?

Route 2: Fysieke omgeving

Klimaatregeling

2.01. Is er klimaatregeling, bijv. verwarmings- en koelsystemen, waarmee de temperatuur bij de elektronische apparatuur constant gehouden wordt?
2.02. Wordt de elektronische apparatuur beschermd tegen vocht of extreme luchtvochtigheid?
2.03. Wanneer de klimaatregeling op afstand wordt aangestuurd, is deze dan voldoende beveiligd tegen toegang door onbevoegden?
2.04. Is er klimaatregeling waarmee het systeem wordt beschermd tegen andere factoren dan temperatuur en luchtvochtigheid, bijv. tegen rook, stof en chemische dampen?
2.05. Zijn er omgevingssensors, met name voor temperatuur, rook en vocht, in het datacentrum en de kabelkasten?
2.06. Zijn de zones waar elektronische apparatuur is geplaatst voorzien van een brandbestrijdingssysteem dat geschikt is voor elektrische apparatuur?
2.07. Zijn er brandbestrijdingssystemen waarmee brand in de aangrenzende zones rond de zone met de elektronische apparatuur kan worden bestreden?

Elektrische voeding

2.08. Zijn de noodschakelaars om de stroomvoorziening te onderbreken voorzien van duidelijke labels, staan ze onder cameratoezicht en zijn ze afgedekt met

beveiligingspanelen om te voorkomen dat de stroomvoorziening door onbevoegden wordt onderbroken?

2.09. Zijn er fysieke beveiligingsbarrières geplaatst om de verbindende voedingskabels in de nabijheid van het datacentrum te beschermen, zodat ze niet makkelijk doorgesneden of beschadigd kunnen worden?

2.10. Zijn er maatregelen getroffen om te voorkomen dat verder van het datacentrum gelegen verbindende elektriciteitskabels door makkelijk herkenbare onveilige locaties lopen?

2.11. Zijn de componenten van de stroomvoorziening, zoals bedieningspanelen en zekeringkasten beveiligd tegen toegang door onbevoegden?

2.12. Wanneer er gebruik wordt gemaakt van UPS (*uninterrupted power supply*), zijn deze beveiligd tegen toegang op afstand door onbevoegden?

2.13. Zijn kritische systemen via twee verschillende routes aangesloten op de stroomvoorziening?

2.14. Zijn noodstroomgeneratoren beveiligd met bijv. sloten, alarmen en hekken met prikkeldraad?

2.15. Zijn er voldoende noodstroomvoorzieningen, met name voor systemen die onmisbaar zijn voor het draaiende houden van de onderneming?

2.16. Is er bij de noodstroomvoorziening voldoende brandstof voor relatief lange onderbrekingen van de brandstofvoorziening?

2.17. Wordt de noodstroomvoorziening regelmatig getest onder volle belasting en draait deze dan lang genoeg om te controleren of alles functioneert?

2.18. Staat de noodstroomvoorziening op een plaats waar geen gevaar voor overstroming bestaat?

2.19. Is er een beveiliging tegen stroompieken, bijv. bij blikseminslag of met opzet veroorzaakte stroompieken?

Fysieke bescherming

2.20. Staan de kritische computer- en communicatiefaciliteiten ver genoeg van vaste faciliteiten die bijzonder kwetsbaar zijn voor brand, explosies of gevaarlijke lekkages?

2.21. Staan de kritische computer- en communicatiefaciliteiten ver genoeg van openbare parkeerplaatsen, straten en andere locaties waar gemakkelijk een bom tot ontploffing kan worden gebracht?

2.22. Wordt kritische computer- en communicatieapparatuur uit de buurt gehouden van gewone ramen die als toegang zouden kunnen dienen voor granaten, bommen, geweervuur of microgolfwapens?

2.23. Staan de noodstroomgeneratoren ver genoeg van openbare parkeerplaatsen, straten en andere locaties waar gemakkelijk een bom tot ontploffing kan worden gebracht?
2.24. Zijn kritische elektronische systemen die belangrijke doelwitten vormen afgeschermd met metaal dat bestand is tegen aanvallen met niet-nucleaire elektromagnetische wapens? *
2.25. Is er een veilige laad- en loszone, die fysiek gescheiden is van het datacentrum, zodat het vervangen of aanvullen van apparatuur geen mogelijkheid biedt voor toegang door onbevoegden of explosieven?
2.26. Worden elektronische apparatuur, onderdelen en andere leveringen fysiek geïnspecteerd voordat ze naar het datacentrum worden gebracht om na te gaan of er niet mee geknoeid is?

Route 3: Fysieke nevenproducten

3.01. Zijn documenten met gevoelige informatie beveiligd tegen printen wanneer dat niet noodzakelijk is? *
3.02. Zijn er voldoende strenge procedures om de toegang van onbevoegden tot geprinte documenten met gevoelige informatie te beperken?
3.03. Staat in het beveiligingsbeleid van de onderneming in welke opbergmiddelen geprinte documenten met gevoelige informatie moeten worden opgeslagen?
3.04. Zijn er voldoende strenge procedures voor het veilig vernietigen van geprinte documenten?
3.05. Wordt erop gelet dat hergebruik en recycling van papier niet ten koste gaat van de veiligheid van geprinte documenten met gevoelige informatie?
3.06. Zijn er voldoende strenge beleidsregels en procedures voor het gebruik van verwijderbare magnetische media, zoals USB-sticks etc.?
3.07. Zijn er voldoende strenge procedures om de toegang van onbevoegden tot back-up media te beperken?
3.08. Zijn er voldoende strenge procedures voor het goed inventariseren van cd-roms en USB-sticks etc. die gevoelige informatie bevatten?
3.09. Is er een vaste procedure voor het registreren van opslagmedia die uit de inventaris worden verwijderd, zodat de verantwoordelijke medewerkers eerst controleren dat ze zijn verwijderd om te worden afgevoerd, ten tweede dat ze op de juiste manier zijn vernietigd of leeg gemaakt en ten derde dat de fysieke restanten fysiek zijn vrijgegeven?
3.10. Zijn er voldoende strenge procedures voor het veilig vervoeren van verwijderbare opslagmedia die naar andere plaatsen moeten worden gebracht?

3.11. Zijn er procedures om te zorgen dat geheugenmedia, zoals hard drives, tapes, flash drives en zip disks grondig overschreven worden voordat ze worden vrijgegeven voor andere doeleinden?
3.12. Zijn er voldoende strenge procedures voor het veilig vernietigen of opschonen van geheugenmedia, zoals hard drives, tapes, flash drives en zip disks, wanneer ze niet meer worden gebruikt?
3.13. Zijn er voldoende strenge procedures voor het opschonen van geheugenmedia die vanwege de garantie worden vervangen of worden verkocht aan het publiek of worden geschonken aan goede doelen?
3.14. Worden gebruikte cd-roms met gevoelige informatie op de juiste manier vernietigd (niet alleen gebroken) voordat ze worden afgevoerd?

Gebied 2: Kwetsbare plekken in softwaretoegang

Route 4: Authenticatie van identiteit

Authenticatiebeleid

4.01. Worden informatiesystemen beschermd met primaire authenticatiemechanismen, zoals gebruikersnamen en wachtwoorden?
4.02. Wordt de toegang van elke gebruiker tot applicaties op het systeem beperkt tot de applicaties die voor die gebruiker nodig en geschikt zijn?
4.03. Vindt er voor applicaties die toegang geven tot gevoelige informatie extra authenticatie van de gebruiker plaats?
4.04. Maakt het systeem gebruik van geavanceerde authenticatiemechanismen zoals biometrische kenmerken, *two-factor tokens* of *challenge exchanges* voor kritische applicaties of gevoelige informatie?
4.05. Zijn terminals en softwaresystemen zodanig ingesteld dat gebruikers opnieuw moeten inloggen na een periode van inactiviteit of wanneer een andere voorziening aangeeft dat de medewerker de terminal heeft verlaten?
4.06. Zijn de verbindingen met kritische systemen die op afstand benaderd kunnen worden via een of meer van deze authenticatiemechanismen voor deze systemen gereserveerd of vindt er encryptie op plaats?
4.07. Wanneer er gebruik wordt gemaakt van geavanceerde authenticatie voor de toegang, wordt deze technologie dan overal gebruikt in de hele onderneming?
4.08. Is er een procedure om de rechten voor *two-factor tokens* en *smart cards* snel in te trekken, zodra deze gecompromitteerd zijn?
4.09. Is er een alarm dat een signaal afgeeft zodra geprobeerd wordt gebruik te maken van een geblokkeerd *two-factor token* of een *smart card*? *

4.10. Wanneer gebruik wordt gemaakt van biometrische kenmerken, is er dan ook nog een pincode nodig om de identiteit te verifiëren?
4.11. Wanneer gebruik wordt gemaakt van biometrische kenmerken, vinden er dan live scans of andere controles plaats om te na te gaan of er echt een levende persoon wordt gecontroleerd? *
4.12. Kan de onderneming zo nodig toegang krijgen tot de data en applicaties die gewoonlijk worden beveiligd met behulp van persoonlijke *two-factor authenticatie*, bijv. op basis van biometrische kenmerken? *

Monitoring van toegang en pogingen daartoe

4.13. Is het beleid dat alle toegangspogingen worden geregistreerd, of ze succesvol zijn of niet, met name voor applicaties met kritische functies of waarin gevoelige informatie is opgeslagen?
4.14. Worden alle wijzigingen die de systeembeheerder uitvoert op wachtwoorden geregistreerd en gecontroleerd?
4.15. Wordt elke uitbreiding van toegangsrechten geregistreerd en gecontroleerd?
4.16. Is er een alarm dat waarschuwt wanneer gebruik wordt gemaakt van het algemene root-level of beheerdersniveau (bijv. van de domeinbeheerder)?
4.17. Worden alle toegangsregistraties weggeschreven naar een niet-overschrijfbare schijf of ander vast medium waar zelfs de systeembeheerder niets op kan veranderen? *
4.18. Worden geslaagde authenticaties gecontroleerd zodat de toegang correct en passend verloopt?
4.19. Wordt geprobeerd geslaagde toegangspogingen op ongebruikelijke tijdstippen en/of tijdens de nacht te achterhalen en te onderzoeken?
4.20. Worden herhaalde mislukte toegangspogingen tot applicaties tijdig onderzocht?
4.21. Zijn er automatische alarmen en verdedigingsmaatregelen om gewelddadige aanvallen op de inlogmechanismen te blokkeren en worden die ingeschakeld bij meervoudige inlogpogingen, ook al gebeuren ze verspreid over een langere tijd en met verschillende gebruikersidentiteiten?

Beheer van wachtwoorden en biometrische kenmerken

4.22. Bevat het ondernemingsbeleid veilige procedures voor de afgifte van wachtwoorden?
4.23. Schrijft het beleid een minimumlengte voor wachtwoorden voor, waarbij wordt rekening gehouden met de rol van de gebruiker en hoe lang de wachtwoorden voor de desbetreffende systemen mogen zijn?

4.24. Worden binnen de organisatie ontwikkelde applicaties beschermd met wachtwoorden met een minimum en maximum aantal karakters?
4.25. Worden hogere eisen gesteld aan de wachtwoorden, bijv. combinaties van diverse soorten karakters of karakters gekozen uit grote karaktersets?
4.26. Wordt voorkomen dat wachtwoorden door middel van leesbare tekst worden verzonden, bijv. via e-mail of instant messaging?
4.27. Zijn werknemers verplicht hun wachtwoorden volgens een vast schema te wijzigen?
4.28. Wordt voorkomen dat werknemers eerdere wachtwoorden kunnen gebruiken zodra ze hun wachtwoord volgens schema moeten wijzigen?
4.29. Stelt het beleid voldoende eisen aan wachtwoorden voor netwerkapparatuur, zoals routers en switches?
4.30. Zijn er maatregelen genomen om diefstal van wachtwoorden of de al dan niet gecodeerde bestanden waarin de wachtwoorden worden opgeslagen te voorkomen?
4.31. Gaat er een alarm zodra een bestand waarin wachtwoorden zijn opgeslagen ontvreemd wordt? *
4.32. Is er een procedure om wachtwoorden snel en veilig te veranderen wanneer deze mogelijk gecompromitteerd zijn?
4.33. Schrijft het beleid voor dat wachtwoorden onmiddellijk worden geblokkeerd zodra een medewerker wordt ontslagen, ontslag neemt of met pensioen gaat?
4.34. Worden applicaties op servers en werkstations regelmatig gecontroleerd op ongebruikte accounts of accounts van voormalige medewerkers en worden deze accounts opgeheven of worden er nieuwe wachtwoorden aan toegewezen?
4.35. Is er een strenge registratieprocedure voor biometrische kenmerken, waardoor er een hoge mate van zekerheid bestaat dat de vastgelegde gegevens worden ontvangen van de juiste persoon?
4.36. Worden de biometrische kenmerken van een gebruiker zodra ze zijn vastgelegd bewaard op een veilige locatie die bestand is tegen sabotage en diefstal?
4.37. Beschikken de onderneming en haar leveranciers over een plan voor het vervangen van gesaboteerde biometrische informatie met alternatieve informatie? *
4.38. Schrijft het beleid procedures voor, voor het vernietigen van biometrische informatie zodra deze niet langer nodig is?

Beheer van encryptiesleutels en digitale certificaten

4.39. Worden encryptiesleutels op een veilige manier gecreëerd en wordt daarbij gebruik gemaakt van goedgekeurde industriële methoden?

4.40 Worden de decryptieprocedures los van de inlogprocedures geactiveerd en zijn er andere wachtwoorden voor nodig?
4.41. Wordt het genereren van encryptiesleutels geregistreerd in een sabotagebestendig bestand en worden daarbij ook de identiteit van de uitvoerende werknemer en het tijdstip vastgelegd?
4.42. Worden encryptiesleutels en digitale certificaten op zo'n manier verspreid dat diefstal wordt voorkomen?
4.43. Worden encryptiesleutels op een veilige manier opgeslagen en wordt daarbij gebruik gemaakt van goedgekeurde industriële methoden?
4.44. Worden encryptiesleutels op een veilige manier vernietigd en wordt daarbij gebruik gemaakt van goedgekeurde industriële methoden?
4.45. Is er een snelle en effectieve methode voor het verwijderen van gesaboteerde encryptiesleutels?
4.46. Zijn er periodieke en betrouwbare procedures voor het archiveren van privé encryptiesleutels en de bijbehorende wachtwoordzinnen voor afzonderlijke gebruikers?
4.47. Als privé encryptiesleutels worden bewaard, worden ze dan gearchiveerd op een met een wachtwoord beveiligde en versleutelde plaats om sabotage of diefstal te voorkomen?
4.48. Worden archieven met privé encryptiesleutels en de bijbehorende sleutels voor wachtwoordzinnen bewaard wanneer ze niet langer actief gebruikt worden, zodat eerder versleutelde bestanden zo nodig kunnen worden opgevraagd?
4.49. Omschrijft het ondernemingsbeleid procedures voor het gebruik van op digitale certificaten gebaseerde authenticatiemechanismen?
4.50. Worden kopieën van de privésleutels van digitale certificaten opgeslagen op een met een wachtwoord beveiligde en versleutelde plaats waar ze opgevraagd kunnen worden, maar diefstal voorkomen wordt?
4.51. Zijn systemen met geïnstalleerde certificaten voorzien van voldoende beveiligingsmaatregelen die diefstal van de privé sleutels van deze certificaten beletten?
4.52. Geldt er een procedure waardoor gecompromitteerde privésleutels van digitale certificaten snel kunnen worden ingetrokken?
4.53. Gelden er vervaltermijnen voor encryptiesleutels en digitale certificaten?

Bewaking van de authenticiteit van documenten

4.54. Worden documenten met daarin bedrijfsinformatie of opinies van de onderneming geconverteerd naar een formaat die niet eenvoudig kan worden gewijzigd voordat ze elektronisch buiten de onderneming worden verspreid?

4.55. Worden documenten digitaal ondertekend wanneer ze worden geconverteerd in een formaat die niet eenvoudig kan worden gewijzigd?

4.56. Worden de digitale handtekeningen op belangrijke documenten regelmatig gecontroleerd om na te gaan of ze inderdaad zijn gecreëerd door de persoon van wie ze afkomstig lijken te zijn?

4.57. Worden belangrijke e-mails verzonden met behulp van een applicatie die hun inhoud een hashwaarde geeft en voorziet van een digitale handtekening zodat de inhoud en de identiteit van de afzender niet eenvoudig kunnen worden gemanipuleerd?

4.58. Worden bevestigingen van ontvangst van belangrijke e-mails verzameld en opgeslagen in een bestand waaruit blijkt dat ze de geadresseerde hebben bereikt?

Route 5: Applicatierechten

Aanpassing van rechten

5.01. Worden de fabrieksinstellingen voor de beveiliging op software en hardware gewijzigd voordat ze geactiveerd worden?

5.02. Heeft de onderneming officieel kritische classificaties toegekend aan de belangrijke of op grote schaal gebruikte softwareapplicaties?

5.03. Wordt de toegang tot kritische applicaties beperkt tot gebruikers binnen de onderneming die ze werkelijk nodig hebben?

5.04. Heeft de onderneming haar informatiebestanden formeel geclassificeerd naar gevoeligheid?

5.05. Wordt de toegang tot gevoelige gegevens beperkt tot gebruikers binnen de onderneming die ze werkelijk nodig hebben?

5.06. Is het recht gegevens te wijzigen of te importeren in documenten of databases beperkt tot werknemers die dat daadwerkelijk moeten doen bij hun normale werkzaamheden.

5.07. Is het recht uitvoer van gevoelige informatie te produceren, zoals het printen of gebruik ervan als bijlage bij e-mails beperkt tot gebruikers van wie dat tot hun taken en verantwoordelijkheden behoort?

5.08. Zijn de rechten op root- en beheerniveau beperkt tot degenen die ze werkelijk nodig hebben?

5.09. Worden de rechten op root- en beheerniveau beheerd en gecontroleerd?

5.10. Wordt geregistreerd hoe de goedkeuring verloopt om mensen toegang te verschaffen tot virtuele private netwerken?
5.11. Wordt geregistreerd hoe de goedkeuring verloopt om mensen op afstand toegang te verschaffen tot modems?
5.12. Is er een procedure om vast te leggen en te achterhalen welke rechten gelden voor elke afzonderlijke werknemer?
5.13. Worden de rechten met betrekking tot softwareapplicaties van individuele werknemers gecontroleerd en aangepast zodra hun werkzaamheden sterk veranderen?
5.14. Geldt er een procedure voor het verwijderen en controleren van het verwijderen van rechten zodra ze niet meer nodig zijn?

Algemene controle op rechten

5.15. Wordt werknemers belet gevoelige informatie te bewaren op lokale opslagmedia, zoals diskettes, cd-roms of USB-sticks, tenzij dit voor zakelijke doeleinden nodig is? *
5.16. Worden de applicaties gemonitord om na te gaan of gevoelige informatie wordt geprint, opgeslagen of gedownload zonder dat noodzakelijk is? *
5.17. Worden lokaal opgeslagen bestanden met kritische gegevens altijd versleuteld bewaard wanneer ze niet gebruikt worden? *
5.18. Kan een geldige gebruiker bestanden met gevoelige gegevens uploaden of downloaden van het ene systeem naar het andere, wanneer dit niet de bedoeling is?
5.19. Worden alle uploads van bestanden met gevoelige gegevens gemonitord en geregistreerd?
5.20. Worden alle uploads van versleutelde gegevensbestanden gemonitord en geregistreerd?
5.21. Zijn er maatregelen om geldige gebruikers te beletten uitvoerbare bestanden te downloaden naar hun systeem zonder ze eerst te laten scannen op schadelijke software?
5.22. Wanneer werknemers gevoelige informatie kunnen opslaan op een lokale drive, wordt dit dan gemonitord en geregistreerd? *
5.23. Heeft een geldige gebruiker toegang tot bronnen op andere systemen zonder extra wachtwoorden en/of validatie met IP-adres?
5.24. Wanneer een dienstverlenende applicatie uit concurrentieoverwegingen vertrouwelijk moet blijven, is deze dan alleen voor vertrouwd personeel toegankelijk via het web en niet voor het algemeen publiek?

Route 6: Validatie van input

6.01. Worden de karakters die in de wachtwoordvelden worden getypt afgeschermd zodat omstanders ze niet kunnen lezen?
6.02. Is er een programma voor het controleren van wachtwoorden zodra ze worden gecreëerd om te waarborgen dat ze voldoen aan de eisen voor wachtwoorden zoals omschreven in het beveiligingsbeleid van de onderneming?
6.03. Zijn alle invoervelden in een applicatie beperkt tot passende karakters en uitdrukkingen? (In velden voor een sofinummer zouden bijvoorbeeld alleen cijfers en streepjes toegestaan moeten zijn.)
6.04. Zijn alle invoervelden in een applicatie beperkt tot een passende minimum- en maximumlengte? (In velden voor een sofinummer zouden bijvoorbeeld slechts 9 cijfers toegestaan moeten zijn.)
6.05. Zijn de regels voor de invoervelden beperkend genoeg, zodat er geen uitvoerbare instructies ingevoerd kunnen worden?
6.06. Gelden er beperkingen voor de gegevensvelden voor de database die overeenkomen met de beperkingen in de velden in de gebruikersinterface, zodat er direct in die database geen onjuiste gegevens en uitvoerbare instructies kunnen worden ingevoerd?
6.07. Worden de gegevensvelden die zelden hoeven te worden gewijzigd “read-only" gemaakt, zodra vastgesteld is dat de gegevensinvoer correct is?
6.08. Is er een geschikte procedure om een gegevensveld dat read-only is gemaakt te corrigeren onder bijzondere omstandigheden en die correctie te controleren?
6.09. Zijn de foutmeldingen zo vormgegeven dat ze geen informatie laten zien over de interne opzet en configuratie van de software?
6.10. Zijn de herstelfuncties uitgeschakeld om te voorkomen dat ze toegang bieden en informatie laten zien over de interne opzet en configuratie van de software?
6.11. Zijn de servicepoorten voor kritische applicaties zo geconfigureerd dat gegevens die buiten de juiste operationele parameters voor die applicaties vallen worden uitgefilterd? *
6.12. Zijn er stresstests uitgevoerd op de servicepoorten die gebruikt worden door kritische applicaties zodat ze niet gevoelig zijn voor overlopende buffers op het niveau van de servicepoorten?
6.13. Zijn er vooraf ingestelde parameters voor de invoeren voor kritische processen, zodat pogingen tot invoeren die buiten die parameters vallen geblokkeerd worden of bevestigd moeten worden vanuit een andere bron? *

Route 7: Passende gedragspatronen

7.01. Is er een alarm dat waarschuwt zodra er blijkbaar gegevens worden ingevoerd door werknemers in hoeveelheden of verdeeld op een wijze die niet passen bij hun normale werkpatroon? *

7.02. Is er een alarm dat waarschuwt zodra toegang wordt verkregen tot ongebruikelijke hoeveelheden bestanden of in een volgorde die niet passen bij de normale werkpatronen? *

7.03. Is er een alarm dat waarschuwt zodra er bij internettransacties sprake is van ongebruikelijke combinaties van klantidentiteiten, factuur- en leveringsadressen? *

7.04. Zijn er vaste procedures voor het controleren van aanpassingen en wijzigingen in besturingssystemen om te zorgen dat wijzigingen die bij elkaar horen dat ook inderdaad doen? *

7.05. Wordt geprobeerd geslaagde toegangspogingen op ongebruikelijke tijdstippen en/of gedurende de nacht te achterhalen en te onderzoeken, wanneer computers onopgemerkt processen zouden kunnen uitvoeren zonder dat daar toestemming voor is gegeven? *

7.06. Is het mogelijk situaties te ontdekken waarin valse gegevens of instructies worden ingevoerd zonder dat daarbij sporen worden achtergelaten? *

7.07. Is de database zo opgezet dat gevoelige informatie niet kan worden overschreven zonder dat de wijzigingen daarna nauwkeurig worden gearchiveerd, voorzien van het desbetreffende tijdstip? *

7.08. Is er een mechanisme voor het monitoren en loggen van alle wijzigingen in kritische databases?

7.09. Worden de logs van wijzigingen in kritische databases regelmatig geanalyseerd op ongebruikelijke toegangspatronen, ongebruikelijke tijdstippen en frequenties? *

7.10. Wanneer wijzigingen in gegevens worden gelogd, wordt de log dan regelmatig geanalyseerd op ongebruikelijke wijzigingspatronen in de databases? *

7.11. Worden systeem- en beveiligingslogs zo bewaard dat ze worden beschermd tegen wijzigingen of wissen zodra ze zijn opgeslagen?

7.12. Bevat het systeem *honey tokens*, die bestaan uit nepdocumenten of nepaccounts waarmee gelogd kan worden of en wanneer iemand er toegang toe heeft? *

7.13. Is er een automatisch proces voor het monitoren van systemen zodra er tekenen zijn dat er mogelijk valse informatie is ingevoerd? *

7.14. Is er een automatische quarantainefunctie voor systemen die mogelijk zijn besmet met valse gegevens zonder dat ze afgesloten worden? *

Gebied 3: Kwetsbare plekken in netwerken

Route 8: Permanente netwerkverbindingen

Integriteit van netwerkverbindingen

8.01. Is het netwerk zelf beveiligd met authenticatieprocedures naast de beveiliging van de systemen op het netwerk?

8.02. Zijn er maatregelen getroffen om te voorkomen dat systemen zonder toestemming eenvoudig kunnen worden aangesloten op het netwerk?

8.03. Wordt het netwerkverkeer regelmatig gemonitord om vast te stellen wat de normale gebruikspatronen zijn?

8.04. Wordt het netwerkverkeer regelmatig gemonitord op illegale communicatiekanalen?

8.05. Zijn de netwerkcomponenten zo geconfigureerd dat de kritischer verkeerscategorieën, zoals instructies voor procesbesturing, voorrang krijgen boven minder kritische categorieën, zoals e-mail?

8.06. Zijn er redundante communicatieverbindingen voor kritische systemen?

8.07. Is er redundantie in extreem kritische netwerken wat betreft de *switching fabric*?

8.08. Wanneer gevoelige informatie via, naar of vanuit het netwerk wordt verzonden, wordt de transmissie dan door middel van encryptie beschermd tegen afluisteren of wijzigen?

8.09. Bepaalt het ondernemingsbeleid welk type gegevenscommunicatie versleuteld moet worden en welke technologieën daarbij moeten worden gebruikt?

8.10. Worden virtuele netwerkverbindingen gebruikt om veilige communicatie met partnernetwerken mogelijk te maken?

8.11. Zijn er beveiligingsvereisten vastgesteld voor niet-versleutelde netwerkverbindingen buiten de partnernetwerken?

8.12. Als er gebruik wordt gemaakt van al dan niet draadloze *Voice over IP* (VoIP) voor zeer gevoelige communicatie, wordt de transmissie dan versleuteld?

Integriteit van netwerkcomponenten

8.13. Moet elke router, switch, server, elk werkstation en alle andere informatieapparatuur voldoen aan minimale veiligheidseisen om te mogen worden aangesloten op het netwerk?

8.14. Worden netwerk softwarecomponenten bij het opstarten automatisch getest op wijzigingen in de beveiligingsconfiguraties die zijn aangebracht sinds het systeem voor het laatst werd gestart, en indien er wijzigingen worden aangetroffen, wordt de systeembeheerder dan automatisch daarvan op de hoogte gesteld? *

8.15. Worden legitieme systemen die geen grotere netwerkconnectiviteit vereisen buiten de grotere netwerken gehouden?
8.16. Wordt het netwerk regelmatig gecontroleerd op systemen waarvoor geen toestemming is?
8.17. Indien op software gebaseerde Voice over IP telefoons worden gebruikt voor gevoelige communicatie, zijn de systemen dan beveiligd tegen *voice loggers*? *
8.18. Zijn er tests uitgevoerd om na te gaan of kritische systemen niet te snel offline kunnen raken door grote hoeveelheden gegevens of verkeer, wat bijv. bereikt kan worden door een *denial-of-service* aanval?
8.19. Is er een mechanisme om kritische componenten automatisch opnieuw te starten, bijv. webserverapplicaties, wanneer andere applicaties diverse malen geen verbinding met hen tot stand kunnen brengen en de systeembeheerder te melden dat dit gebeurd is?
8.20. Maken kritische systemen gebruik van redundante domeinnaam systeem servers (DNS) om de gevolgen van onderbrekingen van die service vanuit een bron te beperken?
8.21. Zijn er maatregelen genomen om domeinnaam systeem servers (DNS) te monitoren op aanvallen waarmee verzoeken worden gerouteerd naar lokaties waarvoor geen toestemming is?
8.22. Vinden er *vulnerability scans* of penetratietests plaats op kritische systemen voordat ze worden aangesloten op de bedrijfsnetwerken?
8.23. Vinden regelmatig *vulnerability scans* of penetratietests plaats op kritische systemen binnen de bedrijfsnetwerken?
8.24. Vinden *vulnerability scans* of penetratietests plaats op alle internetgerichte of klantgerichte systemen en applicaties voordat ze op het netwerk worden geplaatst?
8.25. Vinden regelmatig *vulnerability scans* of penetratietests plaats op alle internetgerichte of klantgerichte systemen en applicaties die op het netwerk zijn aangesloten?

Draadloze verbindingen en modems

8.26. Zijn er duidelijke regels die streng gehandhaafd worden voor het tot stand brengen en gebruiken van draadloze verbindingen met de interne netwerken?
8.27. Draait er regelmatig een *wireless analyzer* om eventuele zonder toestemming op het netwerk aangesloten draadloze randapparatuur op te sporen?
8.28. Worden infrarood-, bluetooth- en draadloze verbindingen met printers uitgeschakeld zodra ze niet nodig zijn voor bedrijfsdoeleinden?

8.29. Wanneer draadloze technologie, zoals een draadloos LAN, bluetooth of draadloos USB, wordt gebruikt voor gevoelige informatie, worden er voor de verbindingen dan krachtige encryptietechnologieën gebruikt?
8.30. Worden de standaard PIN's voor bluetooth apparatuur gewijzigd voordat ze in gebruik worden genomen?
8.31. Als er draadloze technologie wordt gebruikt voor een kritisch netwerk, is het signaal dat de aanwezigheid van een netwerk aangeeft dan uitgeschakeld?
8.32. Wanneer er gebruik wordt gemaakt van draadloze netwerktechnologie, worden de gezamenlijke encryptiesleutels dan regelmatig gerouleerd?
8.33. Wanneer er gebruik wordt gemaakt van draadloze netwerktechnologie, wordt de toegang tot de draadloze verbindingen dan beperkt tot apparatuur waarvoor toestemming is?
8.34. Schrijft het ondernemingsbeleid procedures voor, voor modems binnen de infrastructuur van de onderneming?
8.35. Gelden er voor de toegang tot goedgekeurde modems veiligheidsmaatregelen, zoals herhaal- en doorschakeldetectie?
8.36. Vinden er intern regelmatig *war-dialing* campagnes plaats om niet-goedgekeurde modems op te sporen die via inbellen toegankelijk zijn?
8.37. Worden de telefooncentrales van de onderneming regelmatig gecontroleerd op pogingen om niet-goedgekeurde modems op te sporen met behulp van *war-dialing* aanvallen van buitenaf?

Firewalls, inbraakdetectie en preventie systemen

8.38. Beschikt de onderneming over lijsten met ingaande en uitgaande verkeersbestemmingen en verkeerscategorieën die de firewalls mogen passeren?
8.39. Zijn de firewalls van de onderneming zo geconfigureerd dat alleen het verkeer op de goedgekeurde lijsten hen kan passeren?
8.40. Is er een procedure voor het goedkeuren van wijzigingen in de *rule sets* die het verkeer definiëren dat de firewalls mag passeren?
8.41. Zorgt de onderneming ervoor dat de lijsten met verkeer dat de firewalls mag passeren regelmatig herzien worden om rekening te houden met veranderingen in de verkeersbehoeften van de onderneming?
8.42. Zijn regelmatige controles van de firewalls bij de onderneming verplicht om na te gaan of de *rule sets* juist en zonder wijzigingen zijn geïmplementeerd?
8.43. Worden beveiligingslogs voor firewalls zo bewaard dat voorkomen wordt dat ze gewijzigd of gewist worden?

8.44. Worden de beveiligingslogs voor firewalls regelmatig gecontroleerd op niet-toegestaan verkeer?
8.45. Worden er firewalls gebruikt om kritische systemen te beschermen tegen toegang door onbevoegd intern personeel?
8.46. Houdt de onderneming uitgebreide toegangscontrolelijsten bij voor haar routers en ook van de gebruikte internet protocol (IP) adressen en poortnummers?
8.47. Zijn regelmatig controles van de routers bij de onderneming verplicht om na te gaan of de toegangscontrolelijsten juist zijn geïmplementeerd?
8.48. Zorgt de onderneming ervoor dat de toegangscontrolelijsten voor haar routers regelmatig gecontroleerd worden, zodat rekening wordt gehouden met veranderingen in de verkeersbehoeften van de onderneming?
8.49. Worden er binnen het netwerk inbraakdetectie- en/of –preventiesystemen gebruikt?
8.50. Worden de meldingen van inbraakdetectiesystemen voortdurend gemonitord?
8.51. Worden de *signatures* op inbraakdetectie- en preventiesystemen regelmatig bijgewerkt?
8.52. Worden de beveiligingslogs voor inbraakdetectie- en inbraakpreventiesystemen regelmatig bekeken op afwijkende patronen?
8.53. Worden beveiligingslogs voor inbraakdetectie- en inbraakpreventiesystemen zo bewaard dat voorkomen wordt dat ze gewijzigd of gewist worden?

Filters

8.54. Worden er webfilters gebruikt om het uploaden van vertrouwelijke informatie naar *web-based* e-mailapplicaties zoveel mogelijk te beperken? *
8.55. Worden er webfilters gebruikt om het uploaden van gevoelige informatie naar online opslagportalen en *contact directory portals* (zoals Linkedin) zoveel mogelijk te beperken? *
8.56. Worden er webfilters gebruikt om het verzenden van gevoelige informatie via portalen voor elektronische ansichtkaarten zoveel mogelijk te beperken? *
8.57. Filtert de onderneming de downloads van medewerkers vanaf het internet aan de hand van hun takenpakket? *
8.58. Maakt de onderneming gebruik van contentfilters om vijandige Active X, JavaScript en Java Applets op te vangen?
8.59. Filtert de organisatie de inhoud van alle bijlagen die via e-mail worden verzonden, zodat de verzending van gevoelige informatie wordt geblokkeerd of ontdekt? *

8.60. Filtert de organisatie alle uitvoerbare (*executables*) bestanden uit die als bijlagen bij een e-mail zijn gevoegd?
8.61. Worden er e-mailfilters gebruikt om het verzenden van vertrouwelijke informatie aan externe derden te beperken, tenzij er toestemming voor is en de informatie versleuteld is? *
8.62. Filtert de onderneming de inhoud van alle instant messages (IM) die mogelijk gevoelige informatie bevatten? *
8.63. Voorziet de onderneming gevoelige documenten van een digitaal watermerk zodat content filters ze makkelijker kunnen herkennen? *
8.64. Filtert de organisatie de inhoud van alle uitgaande transmissies via file transfer protocol (FTP) of trivial transfer protocol (TFTP), zodat de verzending van gevoelige informatie wordt geblokkeerd of ontdekt?
8.65. Beperkt de onderneming SNMP-verzoeken (Simple Network Management Protocol) bij de internet gateway?
8.66. Beperkt de onderneming interne SNMP-verzoeken van niet-toegestane systemen tot kritische servers en netwerkvoorzieningen?
8.67. Past de onderneming bij de internet gateways filtering toe op inkomend en uitgaand verkeer?
8.68. Past de onderneming bij de perimeter routers filtering toe op inkomend en uitgaand verkeer om misbruik met behulp van pseudo IP adressen te beletten?
8.69. Past de onderneming tussen verbindingen met partnernetwerken filtering toe op inkomend en uitgaand verkeer?
8.70. Worden met behulp van firewall- of routerrules niet-toegestane uitgaande verbindingen van publieksgerichte systemen zoals webservers belet?

Route 9: Intermitterende netwerkverbindingen

Telecommunicatiekwesties

9.01. Maken werknemers die thuiswerken gebruik van computers met firewalls, virusbescherming, security patches, software voor VPNs en andere beveiligingsvoorzieningen die de onderneming geschikt acht?
9.02. Krijgen ambulante werknemers gestandaardiseerde computervoorzieningen die voorzien zijn van de beveiligingsmaatregelen om gevoelige data te beschermen bij verlies of diefstal van de computer en voldoen die ook aan de overige beveiligingsvereisten van de onderneming?
9.03. Schrijft het ondernemingsbeleid beveiligingsvereisten voor, voor inbelverbindingen naar het bedrijfsnetwerk of VPN?

9.04. Schrijft het ondernemingsbeleid beveiligingsvereisten voor, voor draadloze modems en draadloze breedbandverbindingen op lokaties elders?
9.05. Maken telewerkers gebruik van twee-factor authenticatie om toegang te krijgen tot het bedrijfsnetwerk?
9.06. Moeten telewerkers gebruikmaken van VPN-verbindingen om toegang te krijgen tot het bedrijfsnetwerk?
9.07. Wordt bij gebruik van web-based VPNs informatie over de sessie van de computer waarmee de sessie gestart werd grondig verwijderd?
9.08. Vindt er extra monitoring plaats van verbindingsactiviteiten op afstand om te compenseren dat er in andere opzichten minder toezicht op is?

Onregelmatige verbindingen bij werknemers en partners

9.09. Worden laptops, opslagmedia of andere apparatuur die met regelmaat tijdelijk op het netwerk worden aangesloten voor onderhoud, streng gecontroleerd?
9.10. Worden laptops, opslagmedia of andere apparatuur die met regelmaat tijdelijk op het netwerk worden aangesloten voor software-updates, streng gecontroleerd?
9.11. Worden infrarood-, bluetooth- en draadloze verbindingen op laptops en pda's uitgeschakeld zodra ze niet nodig zijn voor bedrijfsdoeleinden?
9.12. Worden interne microfoons en camera's op laptops uitgeschakeld binnen kritische zones?
9.13. Wanneer gevoelige informatie op laptops moet worden opgeslagen, wordt deze dan versleuteld?
9.14. Worden alle laptops die door externe leveranciers en aannemers tijdelijk op het bedrijfsnetwerk van de onderneming worden aangesloten gecontroleerd op virussen, wormen en andere schadelijke software?
9.15. Worden de activiteiten gevolgd die worden verricht met laptops die door externe leveranciers en aannemers tijdelijk op het bedrijfsnetwerk worden aangesloten?
9.16. Schrijft het ondernemingsbeleid beveiligingseisen voor, voor pda's, smartphones, USB-drives, Ipods, digitale camera's en andere apparatuur die op het bedrijfsnetwerk kan worden aangesloten?
9.17. Als verwijderbare media zijn toegestaan, wordt het gebruik ervan dan gemonitord? *
9.18. Indien pda's of smartphones zijn toegestaan, hanteert de organisatie beperkingen wat betreft de gevoelige informatie die er naartoe mag worden gedownload?

9.19. Moet gevoelige informatie die tijdelijk op een pda of smartphone moet worden opgeslagen worden versleuteld?
9.20. Indien pda's of smartphones zijn toegestaan, zijn ze dan voorzien van anti-virusapplicaties?
9.21. Indien pda's of smartphones zijn voorzien van anti-virussoftware, vinden er dan regelmatig updates plaats van de *definition files*?

E-Commerce verbindingen

9.22. Als er zakelijke transacties plaatsvinden via het internet, worden er dan gegevens van de klant en van zijn computer verzameld ter ondersteuning van de authenticatie van de transactie?
9.23. Is er een systeem waarmee klanten kunnen controleren of ze op de officiële website van de onderneming zijn waarmee ze zaken willen doen?
9.24. Wordt de klantverificatie voor elektronische transacties beschermd tegen automatische aanvallen door middel van een illustratie of *audio playback* met een patroon dat alleen door mensen kan worden herkend? *
9.25. Wordt bij zakelijke transacties waarmee grote bedragen gemoeid zijn gebruik gemaakt van authenticatie met behulp van digitale certificaten, two-factor tokens of andere authenticatiemechanismen?
9.26. Wanneer voor zakelijke transacties gebruik wordt gemaakt van digitale certificaten, worden deze dan afgegeven door een door de bedrijfstak goedgekeurde autoriteit?
9.27. Als er voor zakelijke transacties gebruik wordt gemaakt van digitale certificaten, is er dan een systeem om te controleren of de transactie werkelijk plaatsvindt met het systeem waarvoor het certificaat is afgegeven? *
9.28. Zijn er mechanismen ingesteld om te voorkomen dat opdrachten of instructies bij zakelijke transacties via het internet worden gewijzigd?
9.29. Is er een mechanisme om e-commerce sessies automatisch af te breken na enige tijd van inactiviteit?
9.30. Worden gevoelige klantgegevens, zoals creditcardnummers en persoonlijke identificeerbare gegevens (*identifiers*) door andere systemen behandeld dan het systeem waarmee de webtransactie zelf plaatsvindt?
9.31. Zijn klantwebsites voorzien van software die elke site automatisch in de oorspronkelijke toestand terugzet, zodra pogingen tot manipulatie/aanpassen worden gedaan?
9.32. Worden de webportalen voor elektronische transacties vaker gecontroleerd op de beveiliging dan andere informatiesystemen van de onderneming?

Route 10: Netwerkonderhoud

Netwerkdocumentatie

10.01. Bestaan er gedetailleerde overzichten van de topologie van het bedrijfsnetwerk, zodat alle verbindingsroutes kunnen worden achterhaald?

10.02. Als deze topologieoverzichten bestaan, staan er dan ook de gebruikte service paden en protocollen op?

10.03. Is gecontroleerd of de informatie van de netwerktopologie klopt en of alle componenten en verbindingen binnen het netwerk er inderdaad op staan?

10.04. Is er een plattegrond of geografische kaart waarop precies staat waar de netwerkkabels liggen?

10.05. Worden alle documenten met overzichten van netwerktopologieën en de fysieke opzet streng beveiligd tegen toegang door onbevoegden?

10.06. Zijn alle kabels en apparatuur in de kabelkasten en op andere locaties voorzien van fysieke labels daar waar ze misschien opnieuw geconfigureerd moeten worden?

10.07. Zijn er labels voor apparatuur aan zowel de voor- als de achterzijde van hun behuizing om het risico dat ze door incorrect of onbedoeld opnieuw worden geconfigureerd te beperken?

Richtlijnen en normen voor de beveiliging

10.08. Is er een systeem voor het volgen van softwarepatches en –updates en het registreren van berichten dat ze nodig zijn, de aangekondigde releasedatum en de data waarop ze werkelijk ontvangen worden?

10.09. Worden de juiste personen binnen de organisatie gewaarschuwd bij nieuwe kwetsbare plekken, zodat ze maatregelen kunnen treffen voor de tijd tussen het moment waarop ze werden ontdekt en het tijdstip waarop de juiste patch of update wordt geïnstalleerd?

10.10. Zijn er procedures voor het implementeren van softwarepatches en updates waardoor het risico van slecht functioneren wordt beperkt door testen vooraf, zorgvuldig gekozen tijdstippen voor de installatie en noodprocedures om de laatst bekende goede status snel te herstellen?

10.11 Worden de beveiligingsinstellingen en –configuraties opnieuw gecontroleerd zodra patches en upgrades zijn geïnstalleerd of ze niet per ongeluk zijn gereset naar minder veilige of standaardinstellingen?

10.12. Is er een standaardprocedure om te controleren of de opgespoorde softwarepatches en -updates inderdaad tijdig en op de juiste wijze zijn geïnstalleerd?
10.13. Worden de standaard beveiligingsinstellingen van de leverancier op systemen gewijzigd voordat ze in het netwerk worden geïntegreerd?
10.14. Is er beleid voor het beperken en monitoren van het gebruik van management tools op afstand waarmee systemen kunnen worden bestuurd van buiten het bedrijfsnetwerk?
10.15. Heeft de organisatie overeenkomsten met leveranciers waarin zij een specifiek betrouwbaarheidsniveau en service voor het netwerk garanderen?
10.16. Zijn er procedures voor *rate-limiting* van het verkeer zodat het netwerk niet bezwijkt onder extreme belastingen van de diensten?
10.17. Zijn er procedures voor het toevoegen van extra servers en omleiden van verkeer om te voorkomen dat kritische netwerkcomponenten bezwijken onder extreme belastingen van de diensten?
10.18. Is het gebruik van niet-versleutelde protocollen, zoals Telnet, FTP en SNMP voor het systeembeheer verboden volgens het ondernemingsbeleid, tenzij het systeem deze protocollen nodig heeft?
10.19. Wanneer voor het beheer van de systemen niet-versleutelde protocollen nodig zijn, zijn de bijbehorende verbindingen zo ingesteld dat ze na een bepaald tijd opgeheven worden?
10.20. Zijn alle servers en werkstations geconfigureerd volgens een gespecificeerde beveiligingsstandaard?
10.21. Zijn alle netwerkcomponenten zoals routers en switches geconfigureerd volgens een gespecificeerde beveiligingsstandaard?
10.22. Zijn alle firewalls en inbraakdetectiesystemen geconfigureerd volgens een gespecificeerde beveiligingsstandaard?
10.23. Is het beheer op afstand van routers, switches en andere netwerkcomponenten beperkt tot internet protocol (IP) adressen waarvoor toestemming is?
10.24. Is de logische toegang tot managementinterfaces voor beveiligingscomponenten (bijv. firewall, IDS, enz.) beperkt tot alleen geautoriseerde systemen of internet protocol (IP) adressen?

Systeem- en beveiligingslogs

10.25. Worden wijzigingen van de configuratie van alle kritische servers gelogd?
10.26. Worden wijzigingen van routers en switches gelogd?

10.27. Worden wijzigingen van de configuratie van firewalls en inbraakdetectiesystemen gelogd?
10.28. Is *syslog* ingeschakeld op kritische servers en wordt de informatie naar een systeem op afstand gelogd?
10.29. Is *syslog* ingeschakeld op routers en switches en wordt de informatie naar een systeem op afstand gelogd?
10.30. Is *syslog* ingeschakeld op draadloze netwerk toegangspunten en wordt de informatie naar een systeem op afstand gelogd?

Gebied 4: Kwetsbare plekken in de automatisering

Route 11: Sensors en besturingssystemen op afstand

11.01. Is er een algemene kaart waarop alle communicatiepaden waarlangs de besturingssystemen verbonden zijn correct zijn weergegeven?
11.02. Worden alle documenten waarop de logische toegangsroutes tot besturingssystemen vermeld zijn streng bewaakt tegen toegang door onbevoegden?
11.03. Zijn alle besturingssystemen die niet met internet behoeven te worden verbonden geïsoleerd van internet?
11.04. Worden alle verbindingen tussen besturingssystemen en internet regelmatig beoordeeld om te bepalen of ze echt nodig zijn?
11.05. Zijn alle besturingssystemen geïsoleerd van het bedrijfsnetwerk als er geen dringende noodzaak is voor een verbinding?
11.06. Als een besturingssysteem niet van het bedrijfsnetwerk geïsoleerd kan worden, wordt het dan beschermd met zeer beperkende firewalls en inbraakdetectiesystemen?
11.07. Wordt erop gelet dat indringers geen duidelijk gelabelde schematische overzichten van de fysieke processen en de systemen voor het beheer ervan te zien kunnen krijgen?
11.08. Zijn de adressen en commandocodes voor componenten van het besturingssysteem, zoals op afstand bestuurde switches en kleppen zodanig toegekend of opnieuw toegekend dat ze niet te makkelijk te raden of te achterhalen zijn? *
11.09. Zijn er voorzieningen, zoals alarmen op afstand, om door te geven dat er fysiek gemanipuleerd wordt met sensors op afstand zodat er valse meldingen ontstaan?
11.10. Zijn de sensors op afstand zo opgezet of gewijzigd dat het moeilijk is hen fysiek zo te manipuleren dat ze valse gegevens doorgeven? *

11.11. Zijn zeer kritische besturingsvoorzieningen toegankelijk via een tweede besturingskanaal, zodat toegang mogelijk blijft als dat niet lukt via het eerste kanaal?
11.12. Zijn er extra sensorsets waarmee kritische processen worden bewaakt met behulp van een andere meettechniek zodat een verkeerde melding van de eerste sensorset snel wordt ontdekt? *
11.13. Als sensors op afstand communiceren via een gsm-, satelliet- of andere draadloze verbindingen, zijn er maatregelen genomen om te voorkomen dat de verzonden informatie gemanipuleerd kan worden? *
11.14. Zijn er plannen en procedures voor het geval dat kritische draadloze links overbelast raken?
11.15. Indien terminals op afstand geschikt zijn voor wachtwoorden of encryptie en de vereiste operationele snelheid het toelaat, wordt daar gebruik van gemaakt?
11.16. Zijn alle nieuwe terminals op afstand en andere apparaten voor besturing op afstand die op het netwerk worden geïnstalleerd voorzien van te wijzigen wachtwoorden of herprogrammeerbare authenticatiemechanismen?
11.17. Worden alle periodiek geautomatiseerde transmissies van kritische controlegegevens waarbij snelheid geen rol speelt beschermd met encryptie?
11.18. Zijn alle kritische systeemcomponenten zo geconfigureerd dat ze hun klok regelmatig afstemmen met een veilige tijdbron?
11.19. Zijn alle componenten binnen het netwerk zo gesynchroniseerd dat ze allemaal dezelfde tijd, tijdzone en datum gebruiken?
11.20. Wordt de klok van buitengewoon kritische systeemcomponenten regelmatig aangepast via verschillende bronnen, zodat vervalsing of manipulatie van de communicatie met een tijdbron wordt ontdekt? *
11.21. Zijn er voldoende alarmen om de beheerders te waarschuwen wanneer kritische processen buiten de normale parameters voor veilig functioneren dreigen te raken? *
11.22. Worden updates van de besturingssystemen van terminals op afstand op een veilige manier verzonden vanaf een veilige bron?
11.23. Wordt statusbevragingen aan terminals op afstand op een veilige manier verzonden vanaf een veilige bron?

Route 12: Backup-procedures

Backup-strategie

12.01. Worden backups gemaakt van de besturingssystemen, programma's en besturingsinformatie en de gegevens?

12.02. Worden er backups gemaakt van de gegevens met een frequentie die past bij de economische waarde ervan en de frequentie waarmee ze veranderen?
12.03. Worden de backupgegevens lang genoeg bewaard om een veilige kopie te garanderen wanneer de gegevens geleidelijk gedurende langere tijd worden gemanipuleerd op een wijze die moeilijk te ontdekken valt?
12.04. Worden er frequent backups gemaakt van alle logs van activiteiten die van belang kunnen zijn voor de beveiliging en worden ze opgeslagen in een vorm waarmee manipulatie voorkomen wordt?
12.05. Worden er regelmatig backups gemaakt van de configuraties van switches en routers?
12.06. Worden de backups van de logfiles van de toegang tot applicaties regelmatig opgeslagen op een veilige locatie?
12.07. Worden de logfiles van toegang tot applicaties lang genoeg bewaard zodat achterhaald kan worden waar geleidelijke datacorruptie vandaan komt?
12.08. Worden er meerdere backups gemaakt, zodat als er een verloren gaat of onbetrouwbaar wordt het systeem nog steeds hersteld kan worden?
12.09. Worden de backups regelmatig getest om te waarborgen dat ze leesbaar en betrouwbaar zijn?
12.10. Zijn er procedures voor de behandeling van backupgegevens waarmee gemanipuleerd is, met name tijdens een crisis? *
12.11. Worden backups regelmatig overgebracht naar een opslagmedium dat niet met het netwerk in verbinding staat?
12.12. Worden backups regelmatig overgebracht naar een fysieke locatie op afstand?
12.13 Worden cruciale backups die nog niet zijn overgebracht naar een locatie op afstand zo opgeslagen en gelabeld dat ze snel kunnen worden meegenomen bij een fysieke evacuatie?
12.14. Als verlies van backupinformatie gevaarlijk is voor de onderneming, worden backups dan opgeslagen op meer dan één locatie op afstand?

Veiligheid backups

12.15. Zijn er procedures voor verlies of diefstal van niet-versleutelde backup-tapes met daarop eigendoms- of gevoelige informatie?
12.16. Moeten de gegevens volgens de backup-procedure worden gecontroleerd op gevaarlijke codes zoals virussen en Trojan horses voordat de backup plaatsvindt? *
12.17. Als er een backup wordt gemaakt van gevoelige of vertrouwelijke informatie, wordt deze dan versleuteld tijdens de backup en in versleutelde vorm opgeslagen? *

12.18. Worden de voor de backup gebruikte encryptiesleutels bewaard op een veilige locatie en regelmatig gewijzigd zodat niet alle gegevens bekend worden wanneer een sleutel gemanipuleerd is? *
12.19. Worden de encryptiesleutels voor de backups, samen met een schema waarop staat waar en wanneer ze zijn gebruikt, op een veilige manier op een andere locatie bewaard? *
12.20. Wanneer de backup-kopieën fysiek worden verplaatst naar een locatie op afstand, worden ze dan in sabotagebestendige verpakkingen met een veilig transportmiddel verplaatst en tijdens het vervoer gevolgd? *
12.21. Zijn alle backupmedia tijdens de opslag beschermd tegen fysieke diefstal, ongeacht of ze ter plaatse of elders worden bewaard?
12.22. Zijn er veilige procedures voor vernietiging of hergebruik van backupmedia die niet meer nodig zijn, ongeacht of ze ter plaatse of elders zijn opgeslagen?
12.23. Als de kopie van de backup elektronisch naar een systeem op afstand wordt verstuurd, wordt de informatie dan versleuteld of via een speciaal veilig netwerk verzonden?

Gebied 5: Kwetsbare plekken onder menselijke beheerders

Route 13: Onderhoud van beveiligingsprocedures door personen

Training op het gebied van beveiliging

13.01. Worden alle werknemers periodiek getraind op het gebied van beveiligingsbeleid, waarbij voldoende wordt uitgelegd waarom dit belangrijk is?
13.02. Krijgen de werknemers de instructie hun laptops en andere draagbare informatieapparatuur in de gaten te houden of op een veilige plaats op te bergen wanneer ze deze buiten de werkplek gebruiken of vervoeren?
13.03. Krijgen de werknemers de instructie geen wachtwoorden te kiezen die bestaan uit persoonsgegevens die eventueel voor iedereen toegankelijk zijn?
13.04. Worden de medewerkers gewezen op het gevaar van het opslaan van wachtwoorden op onveilige plekken, zoals op plakbriefjes op hun werkplek?
13.05. Wordt de medewerkers geleerd welke soorten informatie die in de onderneming omgaan gevoelig zijn?
13.06. Wordt de medewerkers geleerd software die per post arriveert te wantrouwen, ook wanneer die lijkt te zijn verpakt en verzonden door vertrouwde leveranciers?
13.07. Worden de medewerkers getraind niet in te gaan op sociale druk via telefoon of internet waarbij geprobeerd wordt hun privé-informatie te ontfutselen of hen bepaalde nummer- of karakterreeksen te laten typen of draaien?

13.08. Worden de medewerkers er regelmatig aan herinnerd geen bestandtypes te downloaden die uitvoerbare codes kunnen bevatten, geen verdachte emails te openen en geen eigen software te installeren op de systemen van de onderneming?
13.09. Worden de medewerkers bewust gemaakt van de veiligheidsrisico's die ze kunnen lopen door op hun mobiele telefoon persoonlijke informatie op te slaan, met name identificatiegegevens?
13.10. Zijn de medewerkers erop gewezen dat ook massaal geproduceerde en massaal gedistribueerde software nog steeds gerichte schadelijke software kan bevatten?
13.11. Zijn de medewerkers, ook de hogere leidinggevenden, zich ervan bewust hoe gevaarlijk het is niet-gedocumenteerde netwerklinks te installeren die niet zijn goedgekeurd door het beveiligingspersoneel?
13.12. Worden alle medewerkers regelmatig getest op hun kennis van de beveiligingsprocedures en opkomende nieuwe risico's en gevaren?

Verantwoordelijkheid voor de beveiliging

13.13. Heeft elke medewerker het handhaven van de beveiliging van de onderneming in zijn functieomschrijving staan?
13.14. Zijn alle medewerkers verplicht overeenkomsten te ondertekenen op het gebied van vertrouwelijkheid en intellectuele eigendommen?
13.15. Worden alle externe aannemers, faciliteitmanagers, koeriers en onderhoudsbedrijven uitdrukkelijk geïnformeerd over het beveiligingsbeleid en de normen die op hun werkzaamheden van toepassing zijn?
13.16. Worden alle externe aannemers, faciliteitmanagers, koeriers en onderhoudsbedrijven contractueel gebonden aan het handhaven van dezelfde strikte beveiligingsrichtlijnen en -normen die de onderneming zelf gebruikt?
13.17. Verschijnen er op inlog- en authenticatieschermen mededelingen dat toegang of gebruik door onbevoegden wederrechtelijk is?
13.18. Is het de medewerkers verboden zonder toestemming eigen software te installeren op apparatuur van de onderneming?
13.19. Wordt in het beleid aangegeven hoe email, internet en instant messaging door de medewerkers mogen worden gebruikt?
13.20. Is het de medewerkers verboden hun pc's te laten gebruiken door andere medewerkers?
13.21. Is het de medewerkers verboden aan anderen hun wachtwoord door te geven?
13.22. Is het de medewerkers verboden persoonlijke identificatiemiddelen te gebruiken zoals badges en elektronische toegangspassen om andere medewerkers toegang te geven tot informatiefaciliteiten en -systemen?

13.23. Valt elk onderdeel van de informatieapparatuur die de onderneming bezit of huurt uitdrukkelijk onder de verantwoordelijkheid van een medewerker?
13.24. Is de aangewezen medewerker ook verantwoordelijk voor de algemene beveiliging van de apparatuur onder zijn hoede?
13.25. Worden er permanente labels of andere markeringen gebruikt waarmee andere medewerkers snel kunnen zien wie verantwoordelijk is voor een bepaald apparaat?
13.26. Worden de medewerkers voldoende aangemoedigd beveiligingsincidenten en slechte praktijken te melden, zonder daar de dupe van te worden?
13.27. Zijn de medewerkers aansprakelijk voor werkzaamheden die ze verrichten op het informatiesysteem en die in strijd zijn met het beveiligingsbeleid van de onderneming?

Beoordeling van de beveiliging

13.28. Worden het informatiebeveiligingsbeleid van de onderneming en de uitvoering ervan jaarlijks beoordeeld door een externe deskundige?
13.29. Is de opzet van de jaarlijkse beoordeling van het informatiebeveiligingsbeleid en de uitvoering ervan ruim genoeg om kwetsbare plekken in de fysieke faciliteiten en het gedrag van medewerkers te ontdekken?
13.30. Worden het informatiebeveiligingsbeleid van de onderneming en de uitvoering zorgvuldig gecontroleerd aan de hand van de erkende voorschriften en normen die gebruikelijk zijn in de bedrijfstak?
13.31. Worden de resultaten van de controle van de informatiebeveiliging analytisch genoeg bekeken zodat gebieden waarvoor andere of aanvullende maatregelen nodig zijn aan het licht komen?
13.32. Is er een betrouwbaar systeem voor het registreren en volgen van kwetsbare plekken die door medewerkers zijn opgemerkt, bij controles zijn ontdekt of door leveranciers of in de media zijn gemeld, zodat beveiligingspersoneel snel kan beschikken over een actuele lijst, waarop te zien is welke al zijn verholpen en waar nog oplossingen nodig zijn?
13.33. Worden herstelwerkzaamheden bij ernstige gebreken altijd tijdig uitgevoerd?
13.34. Worden herstelprogramma's voor recent ontdekte gebreken maandelijks gecontroleerd zodat er steeds snel vooruitgang wordt geboekt?
13.35. Worden de controles van de informatiebeveiliging met elkaar vergeleken zodat hogere leidinggevenden kunnen zien of er vooruitgang wordt geboekt op dit gebied?

Reactie op en behandeling van incidenten

13.36. Worden de verschillende strategieën voor cyberaanvallen gedetailleerd en gevarieerd genoeg beschreven aan de medewerkers zodat ze deze in een vroeg stadium kunnen herkennen en snel rapporteren?

13.37. Weten de medewerkers waar, binnen en buiten de onderneming, eventuele aanvallen gemeld moeten worden?

13.38 Beschikken medewerkers die toegang hebben tot zeer kritische systemen of faciliteiten over speciale toegangscodes waarmee ze duidelijk kunnen maken dat ze onder dwang handelen? *

13.39 Zijn er automatische detectiesystemen die op afstand stil alarm slaan wanneer deze dwangcodes worden gebruikt? *

13.40. Zijn er alternatieve communicatiekanalen beschikbaar wanneer de normale kanalen gecompromitteerd zijn?

13.41. Weten de medewerkers hoe ze systemen die gecompromitteerd zijn, moeten isoleren door ze van het netwerk af te koppelen?

13.42. Zijn er plannen voor het handmatig isoleren (in quarantaine plaatsen) en volgen van systemen die mogelijk zijn besmet met valse gegevens zonder dat ze afgesloten worden?

13.43. Is er een procedure voor het wijzigen van de isolatiegrenzen zodra betere informatie over de mogelijke besmetting beschikbaar wordt?

13.44. Weten de medewerkers hoe ze informatiesystemen die gecompromitteerd zijn, kunnen terugzetten in de laatst bekende goede staat?

13.45. Is er een mechanisme voor het achterhalen van de laatst bekende goede staat wanneer die al van een behoorlijke tijd terug stamt?

13.46. Als er andere systemen zijn ter vervanging van afgesloten systemen of systemen die door de aanval onbetrouwbaar zijn geworden: weten de medewerkers hoe ze daarop moeten overschakelen?

13.47. Weten de medewerkers waar ze aanvullende informatie en begeleiding kunnen krijgen bij voortdurende aanvallen?

13.48. Indien de onderneming zeer noodzakelijke diensten aan vaste klanten verleent: is er een lijst met klanten met de hoogste prioriteit?

13.49. Weten de coördinerende medewerkers hoe ze bewijsmateriaal voor forensisch onderzoek en strafrechtelijke vervolging moeten verzamelen en bewaren?

13.50. Vinden er regelmatig oefeningen plaats waarbij de coördinerende medewerkers alle fasen van de respons op een cyberaanval op een redelijk realistische manier doorlopen?

13.51. Worden medewerkers getraind hoe ze bij een ramp en herstelwerkzaamheden veilig om moeten gaan met opslagmedia en nevenproducten?
13.52. Hebben de coördinerende medewerkers de kans gekregen de noodprocedures te oefenen in gesimuleerde rampensituaties? *
13.53. Wordt er zowel na echte incidenten en oefeningen gediscussieerd over de opgedane ervaringen en de lering die eruit te trekken valt?

Route 14: Opzettelijke acties die de beveiliging bedreigen

Controle op achtergrond van medewerkers

14.01. Wordt de achtergrond nagetrokken van medewerkers met toegang tot hogere informatieniveaus, ook wanneer dit niet blijkt uit hun salarisniveau of functieomschrijving?
14.02. Wordt de achtergrond van een medewerker die tot een aanzienlijk hoger niveau van verantwoordelijkheid en toegang wordt bevorderd opnieuw nagetrokken?
14.03. Wordt de achtergrond nagetrokken van medewerkers die belast zijn met bijv. schoonmaak of onderhoud zoals conciërges?
14.04. Indien er merkbare veranderingen optreden in het persoonlijk of financieel gedrag van een medewerker met toegang tot kritische systemen, is er een discrete procedure voor een nieuwe achtergrondcontrole, waarbij snelle veranderingen in bijv. de kredietwaardigheid of plotselinge onverklaarde tekenen van welvaart kunnen worden opgemerkt? *
14.05. Worden de adresgegevens bijgehouden van voormalige werknemers die zeer goed op de hoogte waren van kritische systemen en procedures?

Controle op gedrag

14.06. Wordt informatie gewoonlijk alleen verspreid op basis van noodzakelijkheid (*need-to-know)* basis, waarbij waar nodig nog steeds informatie met verschillende disciplines wordt gedeeld en wordt gezorgd dat medewerkers weten waarom ze bepaalde dingen moeten doen?
14.07. Wordt een tweede werknemer ingeschakeld om kritische informatie te verifiëren voordat deze wordt ingevoerd?
14.08. Zijn de verantwoordelijkheden tussen medewerkers zo verdeeld dat een medewerker nooit kritische werkzaamheden kan verrichten zonder dat andere medewerkers daarvan op de hoogte zijn?
14.09. Beperkt de onderneming de toegang tot kritische systemen voor medewerkers vanuit locaties en op tijdstippen zonder toezicht?

14.10. Krijgt onderhoudspersoneel, zoals conciërges, alleen toegang tot zeer kritische zones onder directe begeleiding van beveiligingspersoneel?
14.11. Staat onderhoudspersoneel, zoals conciërges, ook in zones die minder kritisch zijn onder cameratoezicht?
14.12. Worden de fysieke en elektronische logs van medewerkers regelmatig gecontroleerd op patronen die niet gekoppeld lijken aan hun normale taken?
14.13. Worden mislukte inlogpogingen van eigen medewerkers regelmatig gecontroleerd?
14.14. Wordt voorkomen dat medewerkers toegang krijgen tot bestanden waaruit blijkt dat ze worden geobserveerd en of ze speciale aandacht hebben getrokken?
14.15. Moeten medewerkers regelmatig vrij nemen, zodat activiteiten die ze anders zouden kunnen verbergen aan het licht komen tijdens hun vervanging?
14.16. Zijn er maatregelen om te voorkomen dat medewerkers het terrein verlaten met gevoelige informatie op diskettes of USB-sticks? *

Betrekkingen met werknemers

14.17. Zijn eerlijkheid en vertrouwen belangrijker bij de behandeling van werknemers dan het aangrijpen van elke kans op winst of voordeel op korte termijn?
14.18. Zijn er geschikte regelingen voor medewerkers om hun klachten te uiten zonder daar de dupe van te worden en kunnen ze dan zien dat die serieus aangepakt worden?
14.19. Verlopen personeelsinkrimpingen op een manier die vijandige gevoelens onder voormalige werknemers tot een minimum beperkt?
14.20. Is er een procedure die het medewerkers mogelijk maakt pogingen van derden die hen dwingen de beveiliging te omzeilen te melden, zonder dat dit algemeen bekend wordt of wordt opgenomen in het personeelsdossier?
14.21. Als een medewerker grote persoonlijke problemen doormaakt, is het dan beleid zijn of haar verantwoordelijkheid voor kritische systemen en de toegang daartoe tijdelijk te beperken?

Gebied 6: Kwetsbare plekken in de levering van software

Route 15: Intern beleid voor software-ontwikkeling

Veilige procedures voor het ontwikkelen van nieuwe software

15.01. Zijn de stappen en procedures voor het intern ontwikkelen van software schriftelijk vastgelegd?

15.02. Voldoet de softwareontwikkeling aan richtlijnen gebaseerd op de beste beveiligingspraktijken in de bedrijfstak?
15.03. Moeten alle medewerkers van leveranciers en aannemers die betrokken zijn bij de softwareontwikkeling voldoen aan minimum beveiligingsvereisten?
15.04. Worden voorgestelde softwareontwerpen ook door beveiligingsdeskundigen beoordeeld op informatiebeveiliging voordat de alfa versies worden geproduceerd?
15.05. Is er een systeem om precies na te gaan welke medewerker of aannemer welke code heeft geschreven voor intern geproduceerde software?
15.06. Zijn alle programmeurs die aan softwareapplicaties werken ervan op de hoogte dat exact wordt bijgehouden wie welke code heeft geschreven?
15.07. Zijn er procedures voor het invoegen van codes tijdens de productie van software, zodat niemand de kans krijgt een deel van een code te veranderen behalve de programmeur die als verantwoordelijke geregistreerd is? *
15.08. Worden wijzigingen van de broncode bibliotheek (*source code library)* gecontroleerd en gevolgd, zodat de broncode controlemodule niet kan worden omzeild door iemand met de rechten van een beheerder? *
15.09. Wordt het commentaar bij elke sectiecode tijdens het schrijven bewaard, zodat andere ontwikkelaars en beveiligingsdeskundigen snel zien waar de secties voor ontworpen zijn?
15.10. Zijn er vooraf goedgekeurde codemodules die in nieuwe software kunnen worden gevoegd om standaardbeveiligingsfuncties uit te voeren, zoals authenticatie en encryptie?
15.11. Voorziet de onderneming ontwikkelaars van dummy gegevens zodat de applicaties die ontwikkeld worden niet hoeven te worden uitgeprobeerd op privé-, gevoelige of vertrouwelijke informatie?
15.12. Worden applicaties in ontwikkeling uitgeprobeerd in testomgevingen die volledig losstaan van de echte productieomgeving?

Beveiligingsfuncties integreren in nieuwe software

15.13. Wordt de applicatie in ontwikkeling zo opgezet dat deze gevoelige informatie die in een bestand of database moet worden opgeslagen versleutelt?
15.14. Wordt de applicatie in ontwikkeling zo opgezet dat deze gevoelige informatie die naar het lokale systeemregister moet worden weggeschreven versleutelt?
15.15. Wordt de applicatie in ontwikkeling zo opgezet dat deze gevoelige informatie die naar een vluchtig geheugen moet worden weggeschreven versleutelt?

15.16. Wordt de applicatie in ontwikkeling zo opgezet dat deze gevoelige informatie die naar een ander systeem moet worden verzonden versleutelt?
15.17. Wordt de applicatie in ontwikkeling zo opgezet dat deze gevoelige informatie die naar *cookies* moet worden weggeschreven versleutelt?
15.18. Wordt de applicatie in ontwikkeling zo opgezet dat zeer voorspelbare authenticatie- en encryptiecodes worden voorkomen?
15.19. Is de applicatie in ontwikkeling zo opgezet dat er een minimum aan privileges vereist is voor het uitvoeren van instructies?
15.20. Wordt bij applicaties in ontwikkeling de betekenis van codecomponenten afgeschermd waarmee kritische operaties moeten worden uitgevoerd?
15.21. Zijn kritische applicaties in ontwikkeling zo opgezet dat subcomponenten als *dynamic link libraries* worden geauthenticeerd om hun authenticiteit te waarborgen voordat ze worden gebruikt? *

Beveiligingstests op nieuwe software

15.22. Wordt door de onderneming ontwikkelde software onderworpen aan een codetest vanuit de beveiligingsoptiek, ongeacht of de productie uitbesteed was of intern heeft plaatsgevonden, voordat de definitieve versie wordt vrijgegeven voor gebruik? *
15.23 Worden de gebruikersaccounts die voor het testen van de software zijn gebruikt systematisch verwijderd voordat de software echt in gebruik wordt genomen?
15.24. Als er commentaren van ontwikkelaars op de *source code* zijn geïntegreerd en die tijdens het ontwikkelingsproces zijn blijven staan, worden ze dan handmatig verwijderd voordat het programma in gebruik wordt genomen?
15.25. Laat de onderneming deskundigen op het gebied van informatiebeveiliging de ontwikkelde software testen, ongeacht of deze intern of extern is geproduceerd?
15.26. Laat de organisatie deskundigen op het gebied van informatiebeveiliging regelmatig applicaties testen nadat ze in gebruik zijn genomen?

Route 16: Relaties met externe leveranciers

Passende relatie met leveranciers

16.01. Zijn de stappen en procedures voor de relatie met softwareleveranciers en externe ontwikkelaars schriftelijk vastgelegd?
16.02. Worden potentiële leveranciers en externe ontwikkelaars beperkt tot degenen van wie kan worden vastgesteld dat ze voldoen aan de normen voor informatiebeveiliging in de bedrijfstak?

16.03. Moeten leveranciers of gedetacheerde medewerkers op de hoogte worden gesteld van, of getraind in, het beveiligingsbeleid van de klant?
16.04. Zijn leveranciers of gedetacheerde medewerkers contractueel verplicht het beveiligingsbeleid van de klant na te leven?
16.05. Zijn medewerkers van leveranciers verplicht geheimhoudingsverklaringen te ondertekenen?
16.06. Zijn leveranciers op grond van serviceovereenkomsten verplicht de achtergrond van hun medewerkers te controleren voordat ze aan een klant worden toegewezen?
16.07. Als een applicatie door een derde leverancier is geleverd, kan de leverancier aantonen dat er maatregelen zijn getroffen om te waarborgen dat de applicaties geen achterdeurtjes heeft waarmee derden toegang kunnen verkrijgen?
16.08. Moeten softwareleveranciers schriftelijk verklaren dat hun code aan een strenge en grondige inspectie is onderworpen voordat deze voor gebruik is vrijgegeven?
16.09. Zijn softwareleveranciers verplicht zich garant te stellen voor het behoud en de bescherming van de broncode die gebruikt is voor de afgenomen (gekocht of onder licentie) applicaties?

Beheer van relaties met leveranciers

16.10. Zijn er betrouwbare kanalen voor het ontvangen van updates van elke softwareleverancier?
16.11. Is er een procedure om via internet of telefoon te controleren of een fysieke zending van de leverancier authentiek is?
16.12. Voorzien leveranciers fysieke zendingen van verpakkingen en labels die moeilijk te vervalsen of te saboteren zijn?
16.13. Wanneer er software updates moeten worden toegepast: is er een garantie dat deze adequaat zijn getest in de relevante softwareomgeving, voordat ze worden geïnstalleerd?
16.14. Zijn er voldoende beperkingen aan, en zit er een vervaldatum op, de toegangsrechten die de leveranciers nodig hebben om de software en updates te installeren?
16.15. Wordt regelmatig gecontroleerd of toegangsrechten van voormalige leveranciers en aannemers inderdaad zijn opgeheven zodra ze niet meer nodig waren?

16.16. Is het mogelijk het functioneren van het systeem te controleren tijdens het updateproces en het systeem terug te zetten in de laatst bekende goede staat wanneer een wijziging mislukt?
16.17. Beschikt de organisatie over processen om de toegang tot interne informatie door externe leveranciers of aannemers te beperken, controleren of monitoren? *
16.18. Beschikt de organisatie over processen om de toegang voor leveranciers, aannemers en ander extern personeel te identificeren en te beëindigen zodra toegang niet meer nodig is?
16.19. Wordt het komen en gaan van leveranciers vastgelegd en bewaakt, hetzij elektronisch, hetzij fysiek?
16.20. Zijn er procedures om te controleren of kopieën van vertrouwelijke informatie zijn vernietigd zodra de leveranciers de overeengekomen software hebben geleverd?
16.21. Worden de activiteiten van voormalige leveranciers of aannemers die in contact zijn geweest met kritische informatie of kritische systemen gecontroleerd op inbreuken op geheimhoudingsverklaringen?

Toestemming voor het gebruik van de US-CCU Checklist voor cybersecurity

De US-CCU Cyber-Security Check List, waarop het auteursrecht rust van US-CCU, mag kosteloos worden opgenomen in andere documenten, formats en software, maar alleen onder de volgende voorwaarden:

1. US-CCU ontvangt vooraf een voorbeeld van de beoogde publicatie en US-CCU bevestigt schriftelijk dat de publicatie voldoet aan deze richtlijnen van US-CCU.

2. Deze mededeling wordt op een duidelijk zichtbare plaats opgenomen in de inleiding, het colofon of toelichting die of dat in de publicatie wordt opgenomen.

3. Als er andere vragen op het gebied van cybersecurity worden opgenomen in de publicatie, dienen die van de US-CCU Cyber-Security Check List in vet of cursief of op een andere manier te worden weergegeven die hen duidelijk onderscheidt van het overige materiaal.

4. Alle vragen van de US-CCU Cyber-Security Check List dienen zonder uitzondering te worden opgenomen in de publicatie.

5. De oorspronkelijke formulering van de vragen van de US-CCU cybersecurity checklist wordt ongewijzigd overgenomen.

6. Het auteursrecht van US-CCU wordt erkend en op de omslag en titelpagina van de publicatie wordt nadrukkelijk vermeld dat het berust bij John Bumgarner en Scott Borg.

7. De datum van de gebruikte editie van de US-CCU Cyber-Security Check List wordt duidelijk vermeld op de omslag en titelpagina van de publicatie.

8. Gebruikers van de publicatie worden er bij dezen van in kennis gesteld dat de US-CCU Cyber-Security Check List direct en gratis voor het publiek verkrijgbaar is bij US-CCU.