A : Auke Vleerstraat 6D
7521 PG Enschede
T : 053-7503070
F : 053-7503071

I : www.quarantainenet.nl
E : info@quarantainenet.nl
B : NL89 RABO 0317 2867 14
KvK : 08135536

Quarantainenet
NETWORK MANAGEMENT AND SECURITY

ISO 27001 met Qmanage

Inclusief NEN 7510, BIR, BIG, BIWA en IBI

Versie 1.2
Auteur drs.ir. Frank van den Hurk
Site http://www.quarantainenet.nl

Quarantainenet is NEN 7510:2011 en ISO/IEC 27001:2013 gecertificeerd.

DEKRA gecertificeerd
Kwaliteit
NEN 7510
www.dekra-seal.com

DEKRA gecertificeerd
Kwaliteit
ISO/IEC 27001
www.dekra-seal.com

Inhoudsopgave

1 Inleiding

Steeds meer organisaties worden vanuit wetgeving of een ander normenkader geacht te zorgen voor beveiliging van hun informatiesystemen in de breedste zin van het woord. De standaard die hiertoe vaak geïmplementeerd wordt, is ISO 27001: Code voor informatiebeveiliging. Hierop zijn een aantal doelgroep-specifieke standaarden gebaseerd:

- Zorg: NEN 7510 opgesteld
- Gemeenten: Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Provincies: Interprovinciale Baseline Informatiebeveiliging (IBI)
- Waterschappen: Baseline Informatiebeveiliging Waterschappen (BIWA)
- Rijksoverheid: Baseline Informatiebeveiliging Rijksdienst (BIR)

Vel doelgroep-specieke standaarden komen voort uit de zeer gevoelige gegevens die verwerkt worden: patiëntgegevens of persoonlijke gegevens van grote groepen burgers. Vanwege het belang van deze gegevens is extra aandacht voor informatiebeveiliging noodzakelijk.

Qmanage is in staat om een belangrijk deel van de aanbevolen technische maatregelen uit deze normen op een kosteneffectieve en eenvoudig te implementeren manier voor uw organisatie (deels) in te vullen. Dit informatieblad vertelt u, geclusterd per thema uit de norm, waar Qmanage u kan helpen op weg naar certificering.

Een belangrijke stap in het voldoen aan deze standaarden is de risico-inventarisatie. Uit deze risico-inventarisatie blijkt vaak dat de belangrijkste dreigingen van binnenuit het netwerk komen. Daarom moet er relatief veel prioriteit worden gegeven aan een risicobehandelplan dat dit risico afdekt. De in dit document genoemde maatregelen, waarbij Qmanage een belangrijke rol speelt bij de invulling, zijn de belangrijkste pijlers in dit risicobehandelplan.

Dankzij de detectiecomponent van Qmanage is het toepassen van Qmanage niet alleen een invulling voor de in dit document genoemde maatregelen, maar tevens een probaat middel om de effectiviteit van een aantal andere maatregelen te meten.

Bij de nummering van de hoofdstukken en paragrafen is uitgegaan van NEN-ISO/IEC 27002:2007 en NEN 7510:2011. De citaten uit deze normen zijn in groene kaders weergegeven. Op een aantal plaatsen bestaan er minimale tekstuele afwijkingen tussen NEN-ISO/IEC 27002:2007 en NEN 7510:2011. In deze gevallen is de tekst uit NEN 7510:2011 opgenomen als citaat.

9 Fysieke beveiliging en beveiliging van de omgeving

9.2.3 Beveiliging van kabels

9.2.3.d

Gebruik duidelijk identificeerbare markeringen op kabels en apparatuur om fouten bij bewerking te voorkomen, zoals het per ongeluk 'patchen' van de verkeerde netwerkkabels.

Qmanage voorkomt dat er verkeerde patches aangelegd worden: de kabel an sich is niet meer relevant, omdat de netwerkconfiguratie op basis van het aangesloten apparaat automatisch aangepast wordt indien nodig.

9.2.3.e

Gebruik een gedocumenteerde patchlijst om de kans op fouten te verminderen.

Met Qmanage beschikt u real-time over een up-to-date patchlijst: u heeft altijd inzicht in welk apparaat op welke switchpoort en in welk VLAN is aangesloten. Daarmee is het handmatig bijhouden van patchlijsten niet meer noodzakelijk en kan er vrijelijk gepatcht worden.

9.2.3.f.5

Het gebruik van detectievoorzieningen en fysieke inspectie om ongeautoriseerde apparatuur die op de bekabeling is aangesloten, op te sporen.

Qmanage voorziet in de detectie van en ingrijpen bij het aansluiten van ongeautoriseerde apparatuur: ongeautoriseerde apparatuur wordt automatisch afgezonderd van de rest van het netwerk.

10 Beheer van communicatie- en bedieningsprocessen

10.2.2 Controle en beoordeling van dienstverlening door een derde partij

NB: Onderstaande rol van Qmanage is op dit onderdeel van de norm alleen van toepassing indien het beheer (een deel van) de op het netwerk aangesloten apparatuur is uitbesteed aan een derde partij.

10.2.2.c

Dit vereist tussen de uitbestedende organisatie en de derde partij een relatie en een proces voor het beheer van de dienstverlening om informatie te verstrekken over informatiebeveiligingsincidenten en beoordeling van deze informatie door de derde partij en de organisatie waar vereist volgens de overeenkomsten en enige ondersteunende richtlijnen en procedures.

De detectiecomponenten van Qmanage, in combinatie met de uitgebreide rapportagemogelijkheden, vormen een uitstekende bron om incidenten te bespreken met de partij die verantwoordelijk is voor beheer en beveiliging van (een deel van) de op het netwerk aangesloten apparatuur. Op basis hiervan kunnen er indien nodig verbeterslagen gemaakt worden. Dankzij Qmanage als onafhankelijke detectiebron in het netwerk wordt voorkomen dat het monopolie op de informatiebronnen voor de rapportage van informatiebeveiligings-incidenten bij de (derde) partij ligt, die ook zelf verantwoordelijk is voor beheer en beveiliging.

10.4.1 Maatregelen tegen kwaadaardige programmatuur

10.4.1

Er behoren maatregelen te worden getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en andere kwaadaardige programmatuur en er behoren geschikte maatregelen te worden getroffen om het risicobewustzijn van de gebruikers te vergroten.

Qmanage beschikt over een scala aan detectiecomponenten. Deze componenten kunnen diverse vormen van virussen en andere kwaadaardige software herkennen. Het is vervolgens mogelijk om automatisch en real-time tegenmaatregelen te nemen om verdere verspreiding te voorkomen.

Tevens wordt er binnen Qmanage veel aandacht besteed aan het vergroten van het risicobewustzijn van de gebruikers. Zo worden gebruikers van eigen apparatuur (BYOD) bij het aanmelden op het netwerk gewezen op het belang van een goede virusscanner en worden ze in het geval van virusbesmettingen aanvullend gewezen op te nemen maatregelen om herhaling te voorkomen.

10.6.1 Maatregelen voor netwerken

10.4.1

Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

Doordat Qmanage enkele belangrijke onderdelen op het gebied van netwerkbeheer automatiseert, waaronder het toewijzen van VLAN's, worden fouten bij handmatige toewijzing van VLAN's voorkomen. Dit verhoogt de bescherming tegen bedreigingen significant. Het wordt immers onmogelijk dat een switchpoort 'per ongeluk' nog in een VLAN stond terwijl dat niet meer het geval zou moeten zijn, of dat een niet voor het betreffende VLAN geautoriseerd apparaat wordt aangesloten op een switchpoort.

10.6.2 Beveiliging van netwerkdiensten

10.6.2.a

Technologie toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, encryptie en netwerkverbindingscontrole.

Qmanage verzorgt authenticatie op netwerkniveau: een apparaat of gebruiker krijgt alleen toegang tot het VLAN waarvoor het apparaat of gebruiker is geauthenticeerd.

10.6.2.c

Procedures voor het gebruik van netwerkdiensten om de toegang tot netwerkdiensten of toepassingen, waar nodig, te beperken.

Door de toegang tot bepaalde netwerkdiensten of toepassingen te beperken tot specifieke VLAN's, kan in combinatie met de geautomatiseerde netwerksegmentering van Qmanage worden bewerkstelligd dat alleen apparatuur waarvoor dit wenselijk is toegang heeft tot specifieke netwerkdiensten of toepassingen.

11 Toegangsbeveiliging

11.1.1 Toegangsbeleid

11.1.1.g

Beheer van toegangsrechten in een (gedistribueerde) netwerkomgeving, waarbij rekening wordt gehouden met alle beschikbare typen verbindingen.

Qmanage zorgt voor automatische VLAN-toewijzing op basis van twee concepten: de rol van een apparaat of gebruiker (met bijbehorende rechten) in combinatie het type en de locatie van de netwerkverbinding. Zo'n locatie kan een plek op het bedrade netwerk zijn, onderverdeeld in gebouw, SER of zelfs switchpoort, of een 'plek' op het draadloze netwerk, onderverdeeld per SSID. Op een centrale plaats in Qmanage wordt de matrix van deze combinaties beheerd. Van daaruit wordt het gekozen beleid automatisch toegepast op de gehele, al dan niet gedistribueerde, netwerkomgeving.

11.2.1 Registratie van gebruikers

11.2.1.e

Gebruikers verplichten een verklaring te ondertekenen waarin ze aangeven de voorwaarden voor de toegang te begrijpen.

Indien gebruikers met een eigen device (BYOD) toegang krijgen tot (een deel van) het netwerk, stelt Qmanage u in staat deze gebruikers gebruikersvoorwaarden te laten accepteren voordat toegang tot het netwerk wordt verleend. Deze acceptatie wordt uiteraard geadministreerd, zodat later terug te zoeken is wanneer de betreffende gebruiker de gebruiksvoorwaarden heeft geaccepteerd.

11.4.3 Identificatie van netwerkapparatuur

11.4.3

Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren.

Qmanage identificeert aangesloten devices en wijst op basis van deze identificatie automatisch het juiste netwerksegment toe. Hierbij is het tevens mogelijk om locatiegebonden beperkingen op te leggen.

11.4.5 Scheiding van netwerken

11.4.5

Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

Een methode voor het beveiligen van grote netwerken is het opsplitsen van de netwerken in afzonderlijke logische domeinen, bijvoorbeeld het interne netwerkdomeinen van een organisatie en externe netwerkdomeinen, die elk wordt beschermd door een afgegrensd beveiligd gebied. Er kan een getrapte verzameling beheersmaatregelen worden toegepast in verschillende logische netwerkdomeinen om de beveiligingsomgevingen van het netwerk verder te scheiden, bijvoorbeeld openbaar toegankelijke systemen, interne netwerken en kritische bedrijfsmiddelen. Definieer de domeinen aan de hand van een risicobeoordeling en de verschillende beveiligingseisen binnen elk van de domeinen.

(…)

Overweeg het splitsen van draadloze netwerken van interne en particuliere netwerken. Omdat de grenzen van draadloze netwerken niet goed zijn gedefinieerd, is in dergelijke gevallen een risicobeoordeling aan te bevelen om de beheersmaatregelen (bijvoorbeeld krachtige authenticatie, cryptografische methoden en frequentiekeuze) te identificeren die nodig zijn om de scheiding van netwerken in stand te houden.

Qmanage segmenteert het netwerk in afzonderlijke logische netwerken (VLAN's). Binnen Qmanage worden de verschillende domeinen gedefinieerd bijvoorbeeld openbaar toegankelijke systemen, interne netwerken en kritische bedrijfsmiddelen, waarna deze gekoppeld worden aan de benodigde VLAN's. Daarbij is onderscheid te maken op basis van het type en de locatie van de netwerkverbinding, waarbij op het bedrade netwerk onderverdeeld kan worden per gebouw, SER of zelfs switchpoort, en op het draadloze netwerk onderverdeeld kan worden per SSID.

11.4.6 Beheersmaatregelen voor netwerkverbindingen

11.4.6

Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen.

Qmanage beperkt de toegangsmogelijkheden voor gebruikers tot het VLAN waarvoor ze conform het toegangsbeleid geautoriseerd zijn.

11.4.7 Beheersmaatregelen voor netwerkroutering

11.4.7

Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.

Qmanage kan bijdragen aan genoemde beheersmaatregel door het vereenvoudigen van de benodigde tijd en moeite hiervoor. Door onderscheid te maken tussen groepen op VLAN-niveau, kan de routering op basis van deze groepen worden ingericht in plaats van op basis van individuele apparaten.

11.6.2 Isoleren van gevoelige systemen

11.6.2

Systemen met een bijzonder hoge gevoeligheid waar het gaat om vertrouwelijkheid en/of om beschikbaarheid en/of om integriteit behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.

Gevoelige systemen kunnen individueel of in (kleine) groepen in een specifiek VLAN worden geplaatst door middel van Qmanage, waardoor ongeautoriseerde toegang vanuit andere delen van het netwerk eenvoudig te voorkomen is.

11.7.1 Draagbare computers en communicatievoorzieningen

11.7.1

Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

(…)

Instrueer personeel dat draagbare computerapparatuur gebruikt, om hen bewust te maken van de extra risico's van deze manier van werken en van de noodzakelijke beheersmaatregelen.

Qmanage is ontworpen om het Bring Your Own Device-aspect van dergelijke draagbare apparatuur beheersmatig te trivialiseren. Bovendien zorgt Qmanage er dankzij automatische netwerksegmentatie, detectie en isolatie voor dat risico’s die bij BYOD horen worden geminimaliseerd.

Daarnaast wordt er binnen Qmanage veel aandacht besteed aan het vergroten van het risicobewustzijn van eigen apparatuur. Bij het aanmelden op het netwerk worden deze gebruikers gewezen op de extra risico's van deze manier van werken en van de noodzakelijke beheersmaatregelen.

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen

12.5.4 Informatielekken

12.5.4

Het voorkomen van alle mogelijke geheime communicatiekanalen is gezien het inherente karakter ervan moeilijk, zo niet onmogelijk. De benutting van dergelijke kanalen wordt echter vaak in gang gezet door Trojaanse paarden. Het nemen van maatregelen tegen Trojaanse paarden vermindert daarom het risico van gebruik van geheime communicatiekanalen.

Een deel van de detectie van Qmanage is specifiek gericht op het detecteren van virussen en andere kwaadaardige software die een verbinding naar buiten opzet. Het is vervolgens mogelijk om automatisch en real-time tegenmaatregelen te nemen om het verder lekken van informatie te voorkomen.

12.6.1 Beheersing van technische kwetsbaarheden

12.6.1.g.3

verhoogde controle om werkelijke aanvallen te ontdekken.

De detectiecomponenten van Qmanage waarschuwen u als er als gevolg van een technische kwetsbaarheid werkelijke aanvallen op uw netwerk plaatsvinden.

13 Beheer van informatiebeveiligingsincidenten

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

13.1.1

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Qmanage kan uitgebreid rapporteren over incidenten op het gebied van virussen en andere kwaadaardige software.

13.2.1 Verantwoordelijkheden en procedures

13.2.1.b

Laat naast de gebruikelijke continuïteitsplannen de procedures ook de volgende aspecten omvatten:

1) analyse en identificatie van de oorzaak van het incident;
2) inperking;
3) zo nodig planning en implementatie van corrigerende maatregelen om herhaling te voorkomen;
4) communicatie met degenen die worden getroffen door of zijn betrokken bij het herstel van het incident;
5) rapporteren van de genomen maatregelen aan de desbetreffende autoriteit;

Qmanage voorziet in de volgende aspecten:

1) Detectie van het incident, waarbij informatie ten bate van verdere analyse van het incident beschikbaar is.
2) Inperking van het incident door op basis van vooraf vastgelegd beleid automatisch of handmatig de bron van het incident op het netwerk te isoleren.
3) Communicatie met de gebruiker van het geïsoleerde systeem, zodat direct duidelijk is waarom het systeem op dat moment geen toegang heeft tot het netwerk.
4) Rapportage over incidenten, waardoor trends zichtbaar worden en zo nodig planning en implementatie van corrigerende maatregelen om herhaling te voorkomen geëffectueerd kunnen worden.

13.2.2 Leren van informatiebeveiligingsincidenten

13.2.2

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gevolgd.
Gebruik de informatie verkregen uit het beoordelen van informatiebeveiligingsincidenten om terugkerende of zeer ingrijpende incidenten te identificeren.

Qmanage is een belangrijke bron voor het inzichtelijk maken van de (terugkerende) problematiek rondom virussen en andere kwaadaardige software. Daarnaast zorgt Quarantainenet er voor dat de kennis die is opgedaan bij beveiligingsincidenten bij één van haar klanten gebruikt wordt voor het verbeteren van de beveiliging bij al haar klanten.

13.2.3 Verzamelen van bewijsmateriaal

13.2.3

Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Qmanage kent uitgebreide logging over zowel de wijze waarop een persoon zich door het netwerk heeft bewogen, als over de wijze waarop een incident zich ontwikkeld heeft.

Conclusie

Als u binnen uw organisatie bezig bent met ISO 27001, NEN 7510, BIR, BIG, BIWA of IBI, kan de implementatie van Qmanage een belangrijke bijdrage leveren aan een deel van de geadviseerde beheersmaatregelen. Qmanage is de oplossing voor netwerkbeheer en netwerkbeveiliging van Quarantainenet, die al in ruim 100 organisaties succesvol en eenvoudig geïmplementeerd is.

Wilt u met Quarantainenet in gesprek om te kijken of Qmanage u kan helpen bij de invulling van ISO 27001, NEN 7510, BIR, BIG, BIWA of IBI? Neem dan contact op met Quarantainenet, telefoon 053-7503070.