

31-5-2024

Versie: 1.0

ANALYSERAPPORT

Projectgroep

ICTAISc3

Docent

[Redacted]

School en Opleiding

Windesheim Zwolle HBO-ICT Software Engineering, Business IT Management & Infrastructure Design & Security

Student

Bark, Ivan (s1169347)

[Redacted]

Geen vertrouwelijke behandeling gewenst.

Versiebeheer

Versie	Datum	Omschrijving	Opmerkingen
0.1	01-03-2024	Eerste opzet	n.v.t.
0.2	03-03-2024	Probleemanalyse & Risicoanalyse	Eerste opzet Probleemanalyse & Risicoanalyse
0.3	05-03-2024	Onderzoeken	Eerste concept voor onderzoeken wetgeving en risico's

Distributie

Naam	Functie	Versie	Datum toezending	Reden toezending
	Docent	0.3	19-03-2024	Verkrijgen feedback
	Docent	1.0	31-05-2024	Oplevering

Inhoudsopgave

Inleiding	3
1. Wetgevingsanalyse	4
1.1. Aanpak.....	4
1.2. Onderzoeksvragen.....	4
1.3. Resultaat	5
1.3.1. Wetgeving rondom beveiliging	5
1.3.2. Wetgeving rondom beveiliging essentiële organisatie	7
1.3.3. Requirements beveiliging	9
1.4. Discussie	10
1.4.1. Conclusie.....	10
1.4.2. Discussie	10
2. Probleemanalyse	11
2.1. Aanpak.....	11
2.2. Resultaat	12
2.2.1. Ontregeling kantoorautomatisering	12
2.2.2. Risico op hack	13
3. Risicoanalyse	14
3.1. Aanpak.....	14
3.2. Resultaat	14
3.2.1. Risico beschrijving	14
3.2.2. Risico's	16
3.2.3. Matrix	16
4. Requirementanalyse	17
4.1. Aanpak.....	17
4.2. Resultaat	17
Bibliografie	18

Inleiding

Winfra vital verzorgt de levering van gas en elektriciteit aan klanten in Noordwest Overijssel. De infrastructuur van Winfra vital wordt gezien als een vitale infrastructuur dat met uitval grootschalige maatschappelijke ontwrichting kan veroorzaken, hierdoor is het van belang dat de veiligheid hiervan nauwlettend in de gaten wordt gehouden.

Inlichtingendiensten hebben gewaarschuwd dat vitale infrastructuren steeds meer aandacht krijgt van overheidsactoren. Deze actoren zijn instaat om niet alleen de technische zwakheden te verkennen, maar richten zich ook op kantoorautomatisering en het personeel. Door een snelle digitalisering van deze sector is een structurele aanpak van cybersecurity vereist namelijk: security by design.

In het analyserapport worden verschillende analyses uitgevoerd. Het gaat hierbij om de volgende analyses:

- Wetgevingsanalyse
- Probleemanalyse
- Risicoanalyse
- Requirementsanalyse

Door bovenstaande analyses uit te voeren wordt er een beter beeld geschetst voor de wetten, problemen en risico's die van invloed zijn op Winfra Vital, dit wordt verder uitgewerkt in de requirementsanalyse. De wetgevingsanalyse is een analyse om de wetgeving van cybersecurity in kaart te brengen, dit zijn de wetten waar Winfra Vital zich aan moet houden als een vitale infrastructuur. De probleemanalyse wordt gedaan vanuit de casus, risicoanalyse en de wetgevingsanalyse. De risicoanalyse maakt gebruik van de bevindingen uit de probleemanalyse en de wetgevingsanalyse en geeft input aan de requirementsanalyse. De requirementsanalyse maakt gebruik van de bevindingen uit bovenstaande analyses om tot verschillende requirements en principes te komen die worden meegenomen binnen het project.

1. Wetgevingsanalyse

1.1. Aanpak

De betreffende analyse wordt uitgevoerd doormiddel van een literatuurstudie. Er zal gebruik worden gemaakt van het internet met websites zoals de rijksoverheid om actuele wetboeken in te zien. Zoektermen die, onder andere, zijn gebruikt zijn: “wetgeving cybersecurity”, “wetgeving digitale beveiliging” en “wetten cybersecurity”.

1.2. Onderzoeksvragen

Om goed in kaart te brengen aan welke verplichtingen gehouden moet worden bij de uitvoering van dit project is er een analyse uitgevoerd naar wetgeving rondom cybersecurity. Voor deze analyse is de volgende hoofdvraag opgesteld:

1. Aan welke wetten moeten wij ons houden voor de implementatie van beveilig maatregelen aan een essentieel bedrijf?

Voor het beantwoorden van de hier bovenstaande hoofdvraag zijn er een aantal deelvragen opgesteld. Door het beantwoorden van deze deelvragen wordt er voldoende informatie verzameld om de hoofdvraag te kunne beantwoorden. Het gaat om de volgende deelvragen:

1. Welke wetten gelden algemeen voor het beveiligen van een bedrijf?

Deze deelvraag geeft inzicht over de wetten, met betrekking tot beveiliging, die gelden voor alle bedrijven.

2. Aan welke wetten moet een essentiële organisatie zich houden qua beveiliging?

Deze deelvraag geeft inzicht over de wetten, met betrekking tot beveiliging, die specifiek gelden voor essentiële organisaties. Winfra Vital is een essentiële organisatie.

3. Welke requirements moet een essentiële organisatie implementeren qua beveiliging?

Deze deelvraag geeft inzicht over de requirements, met betrekking tot beveiliging, die essentiële organisaties moeten implementeren om te voldoen aan de eerder gevonden wetten.

1.3. Resultaat

1.3.1. Wetgeving rondom beveiliging

In dit hoofdstuk zal er onderzocht worden welke wetten er zijn en waar rekening mee gehouden moet worden als bedrijf op het gebied van beveiliging. Het gaat hier om bedrijven in het algemeen en niet vitale of specifieke sectoren. Wetgevingen op het gebied van essentiële organisaties zal besproken worden in het volgende hoofdstuk.

De volgende deelvraag zal behandeld worden: Welke wetten gelden algemeen voor het beveiligen van een bedrijf?

NIS- en NIS2-richtlijnen

Een groot deel van de Nederlandse en Europese wetgevingen rondom cyberbeveiliging zijn gericht op vitale/essentiële organisaties. Daarentegen zijn digitale dienstverleners, bijvoorbeeld clouddiensten, zoekmachines, etc, nu ook opgenomen in deze wetten. Dit is van toepassing op de Europese NIS- en NIS2-richtlijnen. Deze richtlijnen zijn in Nederland geïmplementeerd als de Wet beveiliging netwerk- en Informatiesystemen (Wbni) (Rijksinspectie Digitale Infrastructuur, n.d.). Belangrijke punten die de Wbni omvat zijn de zorg- en meldplicht. (Rijksoverheid, 2018)

Deze richtlijnen en wetgevingen gelden voornamelijk voor vitale sectoren en worden daarom verder in het volgende hoofdstuk toegelicht.

Algemene Verordening Gegevensbescherming (AVG)

Op het moment dat een organisatie persoonsgegevens verwerkt, moet deze organisatie rekening houden met de AVG. De AVG zorgt ervoor dat er verantwoordelijk met persoonsgegevens wordt omgegaan. (Autoriteit Persoonsgegevens, n.d.)

De AVG omvat een aantal basisprincipes bij het verwerken van persoonsgegevens, daarnaast omvat het een aantal privacyrechten en plichten.

Verantwoordingsplicht

Organisaties moeten zich verantwoorden en aan kunnen tonen dat er verantwoordelijk omgegaan wordt met persoonsgegevens. De AVG kent een aantal basisprincipes waar organisaties zich aan moeten houden. De verantwoordingsplicht houdt in dat organisaties aan tonen dat ze zich hieraan houden. De basisprincipes zijn als volgt:

1. Rechtmatigheid, behoorlijkheid en transparantie
2. Doelbinding
3. Dataminimalisatie
4. Juistheid
5. Opslagbeperking
6. Vertrouwelijkheid en integriteit

Deze basisprincipes zorgen voor transparantie en rechtvaardig gebruik van de gegevens. Ook worden en niet meer gegevens verwerkt dan noodzakelijk.

(Autoriteit Persoonsgegevens, n.d.)

Maatregelen

Naast de rechten en plichten omvat de AVG ook een aantal verplichte maatregelen die uitgevoerd moeten worden. De maatregelen die de AVG concreet beschrijft zijn als volgt:

- Het bijhouden van een verwerkingsregister.
- De uitvoering van een “data protection impact assessment” (DPIA) bij het verwerken van persoonsgegevens met een hoog privacyrisico.
- Voor datalekken die niet gemeld hoeven te worden moet er een datalekregister worden bijgehouden.
- Het kunnen aantonen van toestemming van de betrokkene voor het verwerken van hun gegevens.
- Een privacyverklaring opstellen.

(Autoriteit Persoonsgegevens, n.d.)

Privacyrechten

Naast de hierboven genoemde plichten en maatregelen van organisaties hebben mensen rechten met betrekking tot de verwerking van hun gegevens. De AVG brengt een uitbreiding van deze rechten.

- Recht op het verwijderen van gegevens: naast dat de gegevens bij de organisatie worden verwijderd kan er geëist worden dat de organisatie de verwijdering doorgeeft aan externe organisaties die in het bezit zijn van de gegevens.
- Recht op dataportabiliteit: mensen hebben het recht om (onder bepaalde voorwaarden) hun persoonsgegevens in een standaardformat op te vragen.

(Autoriteit Persoonsgegevens, n.d.)

1.3.2. Wetgeving rondom beveiliging essentiële organisatie

In dit hoofdstuk wordt uitgelegd welke wetten essentiële organisaties zich aan moeten houden rondom beveiliging omdat ze essentieel zijn.

Rechten

Alle vitale aanbieders, ook als zij niet zijn aangewezen als AED of AAVA, hebben op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) recht op (Ministerie van Justitie en Veiligheid, z.d.):

- Bijstand van het Nationaal Cyber Security Centrum (NCSC) bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen;
- Informatie en adviezen van het NCSC over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen.

Plichten

AED's en AAVA's hebben naast deze rechten ook plichten op grond van de Wbni. AAVA's hebben naast de bovenstaande rechten de plicht:

- Incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende dienst direct te melden aan het NCSC;
- Inbreuken op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kunnen hebben ('bijna-ongelukken') voor de continuïteit van de verleende dienst direct te melden aan het NCSC.

AED's hebben naast bovenstaande rechten en plichten de plicht:

- Incidenten met aanzienlijke gevolgen voor de continuïteit van de dienstverlening bij de sectorale toezichthouder te melden;
- Passende technische en organisatorische maatregelen te nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen;
- Passende maatregelen te treffen om incidenten te voorkomen die de beveiliging aantasten van de voor de verlening van de dienst gebruikte netwerk- en informatiesystemen. Daarnaast hebben ze de plicht de gevolgen van dergelijke incidenten zo veel mogelijk te beperken.

Wetten/regels

Elektriciteits- en Gaswet: In Nederland regelt de Elektriciteits- en Gaswet de distributie, de levering, de productie en het transport van elektriciteit en gas. Deze wet stelt eisen aan de veiligheid, betrouwbaarheid en betaalbaarheid van energievoorziening.

Netcode Elektriciteit en Gas: De Netcode Elektriciteit en Gas zijn technische codes die regels bevatten voor het beheer en de exploitatie van elektriciteits- en gasnetwerken. Essentiële bedrijven in de gas- en elektriciteitssector moeten voldoen aan de eisen die in deze codes worden gesteld.

Autoriteit Consument & Markt (ACM): De ACM houdt toezicht op de energiemarkt en ziet erop toe dat energiebedrijven zich houden aan de regels met betrekking tot onder meer transparantie, tarieven en leveringsvoorwaarden.

Wet Informatie-uitwisseling Ondergrondse Netten (WION): Deze wet regelt de informatie-uitwisseling tussen partijen die graafwerkzaamheden uitvoeren en partijen die ondergrondse netwerken, zoals gas- en elektriciteitsleidingen, beheren. Hiermee willen ze schade voorkomen aan de netwerken.

Veiligheidsregels Gasinstallaties (VRGI): Voor gasinstallaties gelden specifieke veiligheidsregels, vastgelegd in de VRGI. Deze regels hebben betrekking op aanleg, ontwerp, inspectie en onderhoud van gasinstallaties.

Veiligheidsregels Elektrische installaties (NEN 1010): Voor elektrische installaties gelden veiligheidsregels die zijn vastgelegd in de NEN 1010. Deze regels hebben betrekking op het gebruik, de aanleg, het ontwerp, en het onderhoud van elektrische installaties.

Specifieke wetten

Elektriciteit wettelijke verplichtingen

- Artikel 16, lid 1, sub b: de netbeheerder heeft tot taak de veiligheid en betrouwbaarheid van de netten op de meest doelmatige wijze te waarborgen.
- Artikel 19 lid 1: een netbeheerder hanteert een doeltreffend kwaliteitsborgingssysteem voor de uitvoering van de o.g.v. deze wet aan hem toegekende taken en beschikt over een document waarin is aangegeven op welke wijze hij uitvoering geeft aan bovenstaande.
- Artikel 68, lid 1: plicht producent/leverancier om te bevorderen dat elektriciteit door henzelf en door afnemers op een doelmatige en milieu-hygiënische verantwoorde wijze wordt geproduceerd of bereikt.

Gas wettelijke verplichtingen

- Artikel 8, lid 1: een netbeheerder hanteert een doeltreffend kwaliteitsborgingssysteem (tevens veiligheid en betrouwbaarheid) voor de uitvoering van de hem toegekende taken en beschikt over een document waarin is aangegeven op welke wijze hij daaraan uitvoering geeft.
- Artikel 8a: meldplicht bij minister van EZK indien zich een voorval voordoet of heeft voorgedaan waardoor nadelige gevolgen voor de mens of het milieu zijn ontstaan of dreigen te ontstaan.
- Artikelen 10, 10a: beheerstaken op het gebied van gastransport en gasopslag; bv. Voldoende info verstrekken aan andere netbeheerders om te waarborgen dat transport en opslag m.b.v. zijn gastransportnet op een veilige en doelmatige wijze kan plaatsvinden (Artikel 10 lid 2, sub a).

1.3.3. Requirements beveiliging

Gebaseerd op best practices binnen de IT securitywereld, de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) en de Europese NIS-richtlijn (netwerk- en informatiesystemen) worden door ons requirements opgesteld.

1. Rapportageplicht
 - a. Incidenten moeten binnen hun respectievelijke timeframe gemeldt worden aan de toezichthouder, zoals bijvoorbeeld Autoriteit Persoonsgegevens (AP) in het geval van een datalek.
2. Toeganscontrole en authenticatie
 - a. Sterke toegangscontroles en multi-factor authenticatie voor toegang tot (kritieke) systemen en gegevens.
3. Incidentresponse
 - a. Faciliteer en onderhoud een uitgebreid uitgewerkt incidentresponseplan dat voldoet aan de eisen van de WBNI, en zorg voor regelmatige oefeningen.
4. Continue monitoring
 - a. Systemen voor continue monitoring van netwerkactiviteiten om op korte termijn potentiële beveiligingsincidenten te detecteren.
5. Classificatie informatiesystemen
 - a. Classificeer informatiesystemen op hun belang voor de continuïteit van essentiële diensten.
6. Kwetsbaarheidsbeheer
 - a. Voer regelmatige kwetsbaarheidsscans uit en zorg voor beheer van geïdentificeerde kwetsbaarheden.
7. Toezicht dienstverleners
 - a. Voer due diligence uit bij derde partijen die diensten of producten verlenen aan essentiële organisaties en zorg voor passende beveiligingsmaatregelen.
8. Bewaartermijnen.
 - a. Wettelijke betaaltermijnen voor gegevens en minimalisatie van de verzameling van persoonlijke gegevens tot het minimum.
9. Regelmatige audits en evaluaties
 - a. Regelmatige beveiligingsaudits om de effectiviteit van de beveiligingsmaatregelen te beoordelen.
10. Samenwerking met toezichthouders
 - a. Werk samen met toezichthouders en deel relevante informatie over de beveiligingsstatus en incidenten.

1.4. Discussie

1.4.1. Conclusie

Uit ons onderzoek blijkt dat bij het implementeren van beveiligingsmaatregelen voor een essentieel bedrijf verschillende wetten en richtlijnen van belang zijn.

In de eerste plaats zijn er algemene wetten en richtlijnen die gelden voor alle bedrijven. Denk hierbij aan de Algemene Verordening Gegevensbescherming (AVG), die specifieke eisen stelt aan de verwerking van persoonsgegevens. Dit omvat onder andere het bijhouden van een register van verwerkingsactiviteiten en het uitvoeren van een data protection impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico. Daarnaast regelt de AVG privacyrechten voor individuen, zoals het recht op gegevenswissing en het recht op dataportabiliteit.

Voor essentiële organisaties zijn er ook specifieke wetten en voorschriften die zich richten op de bescherming van vitale sectoren. Een voorbeeld hiervan is de Wet beveiliging netwerk- en informatiesystemen (Wbni), die richtlijnen bevat met betrekking tot zaken als rapportageplicht van incidenten, toegangscontrole en authenticatie, incident response planning, continue monitoring van netwerkactiviteiten, classificatie van informatiesystemen op basis van hun belang voor de continuïteit, kwetsbaarheidsbeheer en toezicht op dienstverleners.

Verder zijn er specifieke wetgevingen zoals de Elektriciteits- en Gaswet, de Netcode Elektriciteit en Gas, de Wet Informatie-uitwisseling Ondergrondse Netten (WION), de Veiligheidsregels Gasinstallaties (VRGI) en de Veiligheidsregels Elektriciteitsinstallaties (NEN 1010), die van toepassing zijn op essentiële bedrijven in de betreffende sector.

Kortom, bij het implementeren van beveiligingsmaatregelen voor een essentieel bedrijf moet er rekening worden gehouden met verschillende wetten en richtlijnen, zowel algemene als specifieke wetgevingen die gericht zijn op de bescherming van vitale sectoren. Daarentegen zijn er geen specifieke wetten aanwezig over hoe de maatregelen worden geïmplementeerd en welk technologieën worden gebruikt.

1.4.2. Discussie

Voor dit onderzoek is er gekeken naar wetgevingen en richtlijnen die gericht zijn op cybersecurity. Hoewel de belangrijkste wetten beschreven zijn hebben wij niet compleet rekening gehouden met een aantal nieuwe wetten die eraan komen. Er is hiervoor gekozen omdat deze wetten nog niet zijn beschreven in een wetboek en op het moment dus ook nog niet gelden. Een vervolgonderzoek zou hierop kunnen uitbreiden.

2. Probleemanalyse

2.1. Aanpak

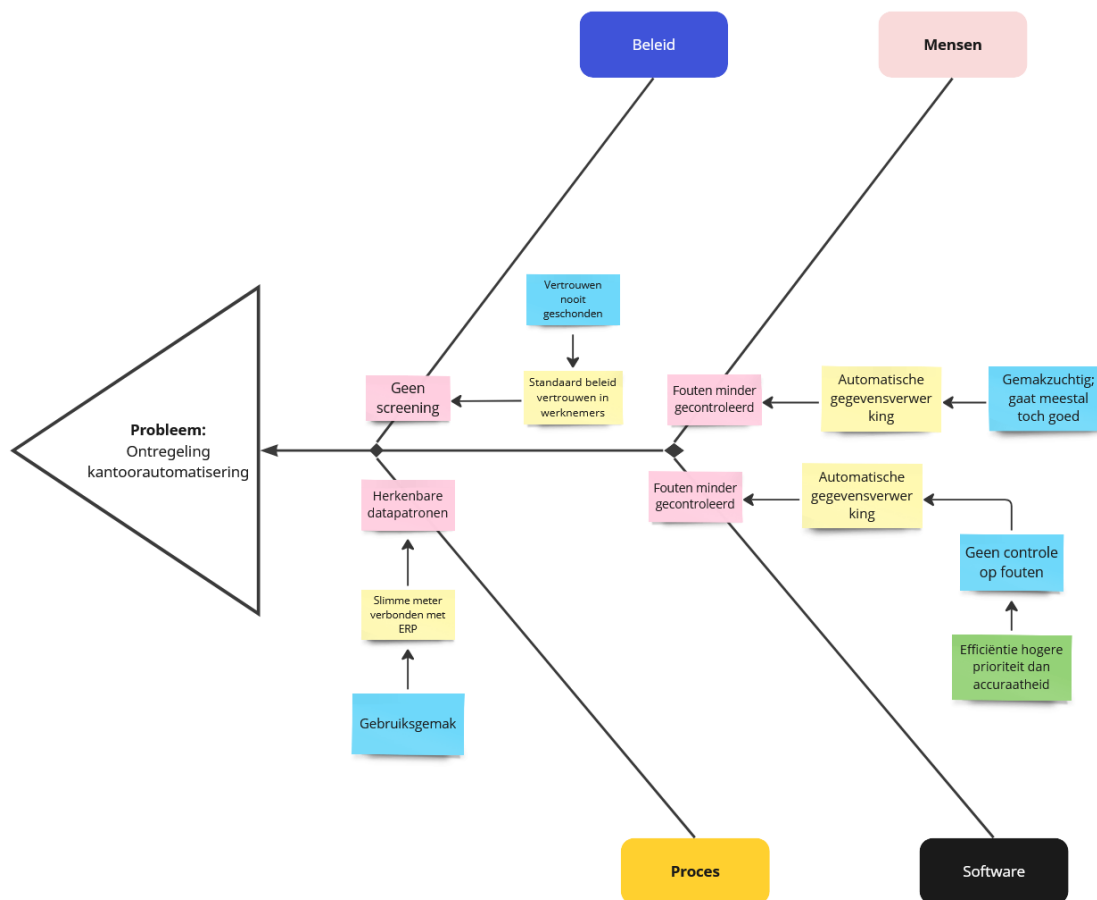
Om alle risico's in kaart te brengen dit project zullen wij gebruikmaken van een risicoanalyse met een aantal methodes om deze duidelijk te maken.

De Fishbone methode met 5 why's: Deze methode wordt toegepast om een breder en dieper beeld te creëren van het probleem. Je kan brainstormen over waar problemen zitten en visueel een "Fishbone" diagram maken om zo een concreet beeld te krijgen van waar het probleem zit. Het is een structurele manier van het bekijken naar problemen omdat je van voor naar achter werkt en de onderdelen in verschillende categorieën onderverdeelt.

De Fishbone methode gaat vaak samen met de 5 Why's. Zo kan er van een probleem een aftakking gemaakt worden met deze methode. Op een probleem vraag je door waarom iets is. Dat wordt over het algemeen 5 keer gedaan zodat de oorzaak van het probleem in kaart wordt gebracht. Dit wordt gedaan voor alle problemen die er zijn opgekomen tijdens het brainstormen.

2.2. Resultaat

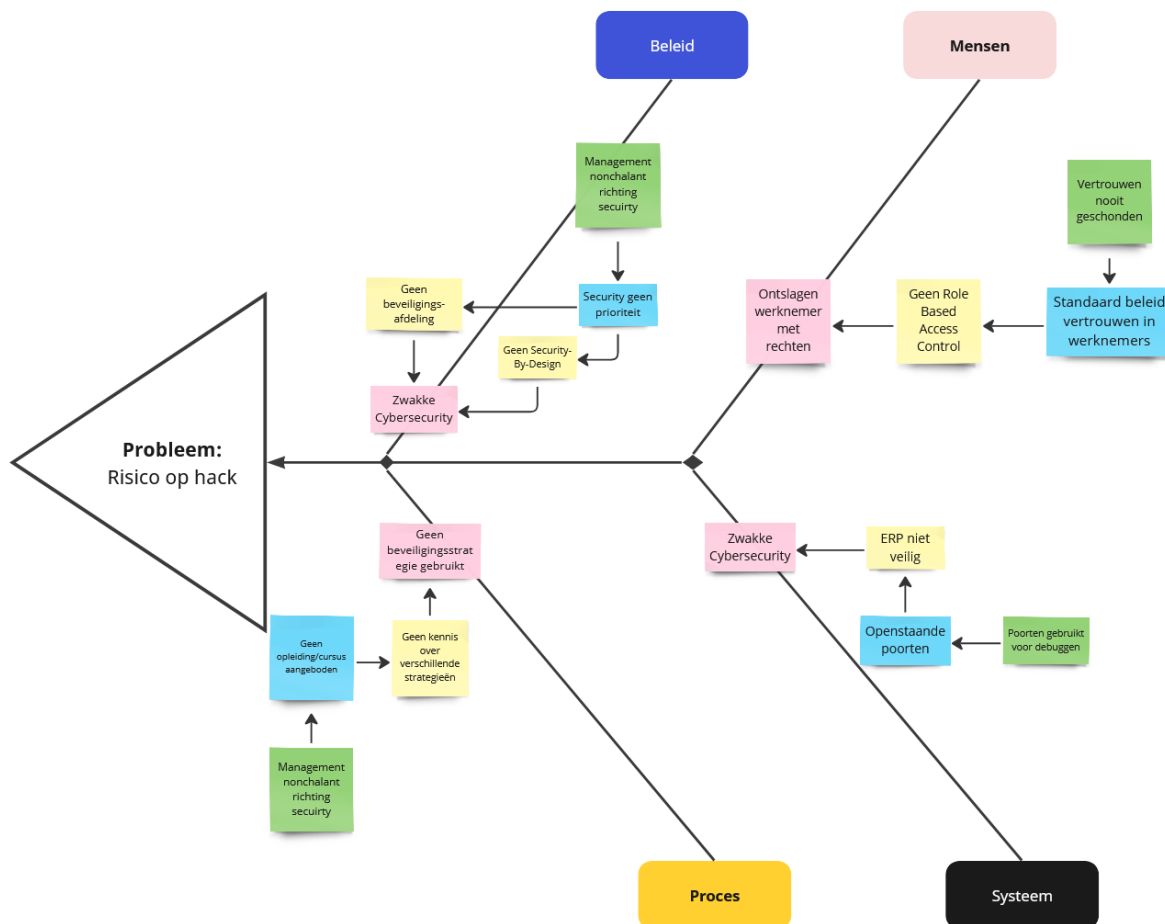
2.2.1. Ontregeling kantoorautomatisering



Figuur 2.1: Fishbone + 5 why's voor ontregeling kantoorautomatisering.

Een groot probleem wat kan voorkomen door overheidsactoren is het ontregelen van kantoorautomatisering. Aangezien het een automatisch proces is worden de fouten minder gecontroleerd door gemakzucht van de medewerkers ervanuit gaande dat het meestal toch goed gaat. Verder is een oorzaak die voor ontregeling van kantoorautomatisering kan zorgen dat de mensen niet gescreend worden, dit wordt gedaan omdat het vertrouwen nog niet is geschonden. Ook kunnen herkenbare datapatronen een oorzaak zijn omdat dit te manipuleren is.

2.2.2. Risico op hack



Figuur 2.2: Fishbone + 5 why's voor Risico op hack.

Het tweede probleem is een risico op een hack. Dit kan gebeuren door een inside threat, een ontslagen medewerker die wrok koestert naar het bedrijf en een account nog geldig heeft kan hiermee schade aanrichten. Ook kan een oorzaak zijn dat er geen gebruik wordt gemaakt van beveiligingsstrategieën aangezien er geen cursus is aangeboden hierover en het management het niet als hoogste prioriteit ziet. Verder kan een oorzaak zijn dat er zwakke cybersecurity is, oorzaken hiervan zijn dat er geen beveiligingsafdeling en security-by-design is doordat security geen hoge prioriteit heeft bij management.

3. Risicoanalyse

3.1. Aanpak

Literatuuronderzoek, met een risicomatrix. We hebben online een bron (Waalewijn & Paques, 2014) gebruikt om de verschillende risico's voor onze casus te bedenken. Deze risico's hebben we vervolgens gezamenlijk met onderbuikgevoel geclassificeerd op kans en impact. Deze classificatie hebben we in een matrix template (ProjectManager, 2024) gestopt om het zo overzichtelijk te maken.

3.2. Resultaat

3.2.1. Risico beschrijving

ERP kan gehacked worden door open debug-poort

De ERP bevat gegevens over de meterstanden van verschillende gebruikers. Gebruikers verbinden naar de ERP via een front-end website. Slimme meters zijn zelf direct verbonden met de ERP om zo hun standen door te geven.

Wanneer er een open debug-poort aanwezig is op de ERP, kunnen derden van deze poort gebruik maken om zo deze gegevens te bewerken. In het ergste geval zouden ze ook via deze poort toegang kunnen krijgen tot het interne netwerk van de ERP, wat voor grootschalige schade kan zorgen.

Datalek

Een datalek is een risico die de vertrouwelijkheid schaadt van het Netbeheer, de klantgegevens mogen niet gelekt worden. Verder is het wettelijk verplicht dat een datalek binnen 72uur gemeld wordt door Winfra Vital als vitale infrastructuur. Een datalek kan op verschillende manieren ontstaan, de volgende manieren worden in kaart gebracht:

- Malware
- Phishingaanval
- Insider Threat

Malware is software dat op het netwerken en systemen van Winfra Vital kan komen, malware heeft de mogelijkheid om een datalek te veroorzaken door de gegevens die bemachtigd zijn door te spelen naar derde partijen.

Phishingaanvallen zorgen voor toegang tot het netwerk waar het mogelijke data opstaat of toe bereikbaar is. Hierdoor is het mogelijk dat een datalek ontstaat.

Insider Threat is een risico dat optreedt wanneer een (ex)medewerker te veel rechten heeft gekregen dan wat hij/zij zou moeten hebben. Als deze (ex)medewerker kwaadaardige doeleinden heeft zou dit kunnen resulteren in een datalek.

DDoS aanval

Een DDoS aanval op puur de ERP is geen probleem, hiermee zijn alleen tijdelijk de gegevens niet meer invoerbaar. Echter wanneer de DDoS zich focust op de infrastructuur van het gas- en elektriciteitsnetwerk kan dit gigantische gevolgen hebben. Gehele bedrijven en/of meerdere

gebouwen zouden dan zonder stroom en/of gas komen te zitten. Voor bedrijven die echt niet zonder stroom kunnen kan dit grootte gevolgen hebben voor hun financiën.

Verkeerde input bij kantoorautomatiseringssysteem

Verkeerde input bij kantoorautomatiseringssysteem kan verschillende risico's met zich meebrengen. Het ontstaan van dit risico kan door menselijke fouten ontstaan maar ook door onduidelijke instructies of technische storingen. De risico's die de verkeerde input in dit systeem kan meenemen zijn:

- Gegevenscorruptie
- Vertrouwensverlies
- Kwetsbaarheden/achterdeuren

Gegevenscorruptie kan de integriteit van het systeem aantasten en dit kan leiden tot foutieve rapportages, onnauwkeurige analyses en besluitvormingen op basis van verkeerde informatie.

Vertrouwensverlies ontstaat wanneer klanten of belanghebbende foutieve informatie ontvangen van Winfra Vital als gevolg van de verkeerde input. Door foutieve informatie te ontvangen kan er argwaan ontstaan wat het imago van Winfra Vital schaadt.

Kwetsbaarheden/achterdeuren kunnen worden gebruikt wanneer de verkeerde input niet voldoende wordt gecontroleerd of audits op worden uitgevoerd. Als de kwaadwillende gebruikers door verkeerde input beveiligingscontroles kunnen ontzeilen kan dit leiden tot ongeautoriseerde toegang tot gevoelige gegevens.

Personeel chantage

Wanneer een persoon chanteerbaar is en deze een belangrijke functie heeft binnen de organisatie, kan die persoon zich gedragen als een Inside Threat. Zo'n persoon zou dan in staat zijn om werkzaamheden te saboteren, gevoelige informatie te delen of malware te installeren op een gevoelig systeem.

Malware

- **Ransomware**

Ransomware encrypt en/of lockt belangrijke systemen waardoor deze niet meer te gebruiken zijn. Dit kan resulteren in het niet meer kunnen leveren van stroom en/of gas.

- **Botnets**

Wanneer meerdere systemen zijn geïnfecteerd met botnets, kunnen deze een DDoS aanval van binnenuit uitvoeren waardoor belangrijke systemen niet meer te gebruiken zijn. Dit kan resulteren in het niet meer kunnen leveren van stroom en/of gas.

- **Spyware**

Met spyware kunnen hackers toegang krijgen tot login gegevens van admins, gevoelige data van systemen en goed inzicht krijgen in het netwerk architectuur. De informatie vanuit spyware kan benut en geëxploiteerd worden.

Natuurlijke omstandigheden

Fysieke schade kan o.a. veroorzaakt worden door: waterschade, brand, extreme temperaturen, heftige stormen enz. Het is belangrijk om rekening te houden met de wet van Murphy: "Als het mis kan gaan, gaat het een keer mis".

Phishing

Phishing is alleenstaand geen risico, gecombineerd met bovengenoemde risico's, zoals de verschillende malware, chantage en datalek, kan het wel een groot risico worden. Het is een tool om andere risico's te initialiseren/ waar te maken.

Insider Threat

Een persoon die zich voordoeft als gewone werknemer, maar stiekem werkt voor een kwaadaardige partij, kan verschillende risico's met zich meebrengen. Zo'n persoon zou bijvoorbeeld actief belangrijke systemen kunnen saboteren, of malware installeren. Ook zou zo'n persoon belangrijke gegevens met de kwaadaardige partij kunnen delen.

3.2.2. Risico's

Risico's	Kans	Impact
1. ERP kan gehacked worden door open debug poort	● ● ● ● ○	● ● ● ● ●
2. Datalek	● ● ● ○ ○	● ● ● ● ●
3. DDoS aanval	● ● ● ○ ○	● ● ● ● ○
4. Verkeerde input bij kantoorautomatiseringen systeem	● ● ● ● ○	● ● ● ○ ○
5. Personeel chantage	● ● ○ ○ ○	● ● ● ● ●
6. Malware	● ● ● ○ ○	● ● ● ● ●
7. Natuurlijke omstandigheden	● ● ○ ○ ○	● ● ● ● ○
8. Phishing	● ● ● ● ○	● ● ● ● ○
9. Inside Threat	● ● ● ○ ○	● ● ● ● ●

Tabel 1: Risico tabel als input voor de risico matrix met kans en impact.

3.2.3. Matrix

Risk Matrix		Severity				
		Insignificant	Minor	Moderate	Major	Sever
Likelihood	Almost Certain					
	Likely		4	4, 8	1, 8	1
	Possible				3, 6	2, 6, 9
	Unlikely				7	5
	Rare					

Figuur 3.1: Risico matrix voor de risico's die Winfra Vital loopt.

4. Requirementanalyse

4.1. Aanpak

De requirements analyse wordt gemaakt in een requirements tracability matrix, deze matrix zorgt ervoor dat er meer structuur blijft in de requirements. De requirements worden opgesplitst in principes, functionaliteiten en kwaliteiten. De kwaliteiten krijgen een type kwaliteit mee. De requirements worden geprioriteerd door de MoSCoW methode. Verder wordt er in het RTM neergezet welke testcase bij de verschillende requirements hoort.

4.2. Resultaat

Zie de requirements tracability matrix.

Bibliografie

Nationaal Cyber Security Centrum. (2024, February 19). Samenvatting NIS2-richtlijn. Over Het NCSC | Nationaal Cyber Security Centrum <https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-nis2-richtlijn>

Ministerie van Economische Zaken en Klimaat. (2018, September). Opgehaald van <https://open.overheid.nl/documenten/ronl-eb328ab6-d3ef-498d-87cf-ea12e33edbfa/pdf>

Ministerie van Justitie en Veiligheid. (sd). *Vitale aanbieders*. Opgehaald van <https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders>

privacy-web. (2017). Opgehaald van https://privacy-web.nl/wp-content/uploads/po_assets/556785.pdf

ProjectManager. (2024). *Risk Matrix Template for Excel*. Opgehaald van ProjectManager: <https://www.projectmanager.com/templates/risk-matrix-template-for-excel>

Waalewijn, D., & Paques, M. (2014, januari). *Digitale spionage en cybercriminaliteit groeiende dreiging voor de energiesector*. Opgehaald van Compact_: <https://www.compact.nl/articles/digitale-spionage-en-cybercriminaliteit-groeiende-dreiging-voor-de-energiesector-2/>