Rapport: Cyberweerbaarheid installateurs alarminstallaties

Gemaakt voor:
Techniek Nederland & OTIB

Gemaakt door:
Threadstone Cyber Security BV
René van Etten

ISSO Kennisinstituut voor bouw en installatietechniek
Arjan Schrauwen

Inhoudsopgave

Inhoudsopgave 2

Samenvatting 3

1 Inleiding 4

2 Methode 5

2.1 Deskresearch 5
2.2 Diepte Interviews 5
2.3 Toetsen resultaten ledenbijeenkomst 5

3 Resultaten 7

3.1 Deskresearch 7
3.1.1 Relevante normen, kaders, regels en wetten 7
3.1.2 De interne organisatie van de installateur in relatie tot de klant 7
3.1.3 Stakeholders 7
3.1.4 Vatbare informatie en systemen 11
3.1.5 Inschatting van de risico's 12
3.1.6 Impact voor eindklant 14
3.2 Conclusies 14

4 Aanbevelingen 16

4.1 Aanbeveling per relatie 16
4.2 Voorzet eindtermen installateur mbt cyberweerbaarheid 18
4.2.1 Installateur 18

BIJLAGE 1: normen, wetten en richtlijnen 21

BIJLAGE 2: Vragenlijst diepte-interviews 23

BIJLAGE 3: AANBEVELINGEN 32

Samenvatting

Het cyberweerbaar maken van ICT is steeds meer in het nieuws. Voorheen speelde dit zich voornamelijk af bij banken grote bedrijven en organisaties die bij falen de Nederlandse economie kunnen ontwrichten (zogenaamde kritische infrastructuren).

Afgelopen jaren zien we in toenemende mate ook aandacht voor vormen van cybercriminaliteit bij kleinere organisaties en consumenten, onder andere veroorzaakt door de opkomst van vormen van ransomware, hacking en phishing.

Gebouwinstallaties hebben nog beperkte aandacht. Dit is vreemd als men zich bedenkt dat toegang tot gebouwen steeds meer digitaal verloopt. Bij een hack is er een kans aanwezig dat een bedrijfsproces wordt stilgelegd of is er kans op inbraak. De installateur die beveiligingsinstallaties aanlegt en beheert speelt logischerwijs een grote rol in het cyberweerbaar maken van een gebouw. Maar wat is de stand van zaken met betrekking tot het cyberweerbaar maken van gebouwen? Wat is het huidige kennisniveau? Wat zijn ontwikkelgebieden op dit vlak?

Om hier inzicht in te krijgen hebben Techniek Nederland en Otib de volgende vragen bij ISSO en Threadstone neergelegd:

- Wat is de stand van zaken met betrekking tot cyberweerbaarheid bij alarminstallaties?
- Waar haalt de installateur kennis op omtrent cyberweerbaarheid?
- Welke kennis is nodig om alarminstallaties nu en in de toekomst cyberweerbaar te maken?
- Welke aanbevelingen zijn er voor de installateur te maken ten aanzien van cyberweerbaarheid?

Om deze vragen te beantwoorden zijn achtereenvolgens de volgende stappen doorlopen:

a. Deskresearch: welke normen en wetten zijn van toepassing? Waar kan de installateur invloed op uitoefenen met betrekking tot cyberweerbaarheid?
b. Diepte-interviews. Op basis van de resultaten uit het deskresearch zijn diepte-interviews gehouden bij fabrikanten, leveranciers, alarminstallateurs en PAC's.
c. De conclusies uit voorgenoemde stappen zijn gespiegeld aan de aanwezigen in de ledenbijeenkomst voor alarminstallateurs die aangesloten zijn bij Techniek Nederland
d. Vervolgens zijn aanbevelingen opgesteld alsmede een voorzet voor eindtermen van de toekomstige alarminstallateur ten aanzien van cyberweerbaarheid.

De conclusies zijn als volgt te formuleren:

a. Naast hardware/softwarematige beveiligingen is het vooral de organisatorische kant van het aanbrengen en beheren van alarminstallaties die aandacht behoeft met betrekking tot cyberweerbaarheid..
b. Belangrijkste partijen om een alarminstallatie cyberweerbaar op te zetten zijn: fabrikanten, verzekeraars, PAC's, medewerkers installateur, klanten en ICT'ers die verantwoordelijk zijn voor de infrastructuur bij de klant.
c. Klanten weten vaak niet de juiste vragen te stellen met betrekking tot cyberweerbaarheid.
d. Installateurs zijn zich goed bewust van hun rol in de keten vanwege borging proces (BORG/VEB/VRKI)
e. Op organisatorisch vlak is er een verbetering mogelijk op het gebied van wachtwoordbeheer en asset management.
f. De huidige certificeringen t.a.v. informatiebeveiliging, zoals de ISO27001, zijn momenteel te zwaar voor het merendeel van de installateurs.
g. Installateurs geven zelf aan dat er onvoldoende praktische kennis is op het gebied van ICT/draadloze systemen en de beveiliging daarvan.

1 Inleiding

Nederland heeft ca. 600 miljoen m2 gebruiksoppervlak aan utiliteitsgebouwen. Dit zijn vaak kantoorgebouwen, datacentra, ziekenhuizen, scholen en ook gebouwen waarin industriële bedrijfsprocessen worden aangestuurd.

Deze gebouwen zijn meestal op een bepaalde manier elektronisch beveiligd tegen inbraak en brand én bovendien vaak verbonden met het internet en gebouwbeheersysteem. Op deze wijze kan een gebouw op afstand worden bestuurd en bewaakt door beheerders en gebruikers van gebouwen. De verantwoording van het ontwerp, de aanleg, het gebruik en het onderhoud van deze systemen gebeurt in een samenwerkingsverband wat strekt van fabrikant/leverancier, ontwerper, installateur, facilitair manager tot gebouweigenaar. Een keten is zo sterk als de zwakste schakel. Een hack op een onderdeel van deze keten kan een elektronisch beveiligd gebouw en het aanwezige bedrijfsproces ernstig beschadigen.

Stelt u eens voor dat als gevolg van een slecht beveiligd systeem een brandbeveiligingsinstallatie niet in werking treedt bij een hoog kantoorgebouw? Of dat een datacenter niet gekoeld wordt? Of dat in een ziekenhuis de elektrische installatie uitvalt? Naast de directe effecten zoals uitval van systemen is de gevolgschade vaak niet te overzien.

Dergelijke systemen worden gerealiseerd en beheerd in een verticale samenwerking van ondernemingen. Deze partijen bestaan uit gebouweigenaren, ontwerpers van gebouwinstallaties, fabrikanten, installateurs, beveiligers van gebouwen en gebruikers. Deze partijen vormen dan ook de doelgroepen van dit project. In het geval van een calamiteit of dreiging is het vaak moeilijk vast te stellen welke partijen welke verantwoording dragen, welke acties er nodig zijn en door wie deze het beste uitgevoerd kunnen worden.

Bedrijven zijn individueel naar oplossingen van de problemen rond digitale beveiliging aan het zoeken. ISSO, Techniek Nederland en OTIB zijn gezamenlijk een project gestart om centraal kennisopbouw en –overdracht te doen over de specifieke problematiek van het verhogen van de cyberweerbaarheid van installaties. Doelstelling is met die kennis bedrijven te informeren over de inrichting van weerbare installaties. Daarnaast wordt de kennis gebruikt om werknemers op te leiden met als doel een verbetering van de cyberweerbaarheid van gebouwen te realiseren.

Dit project heeft niet tot doel om al concrete tooling aan te leveren. Het is bedoeld om een inzicht te geven in wat de branche kan doen om – in brede zin – de digitale weerbaarheid te verbeteren. Beveiligingsinstallaties zijn echter een eerste stap. De installatiebranche wil duurzaam werken aan het verhogen van de cyberveiligheid van alle typen installaties. De gekozen methodiek in de toekomst voor bijvoorbeeld gebouw- en klimaatbeheersing, betaalsystemen en energievoorziening.

Dit rapport beschrijft de activiteiten, uitkomsten en conclusies van dit project. Hierbij wordt ook een voorzet gegeven van de eindtermen die nodig zijn om cyberweerbaarheid door de installateur alarminstallaties in goede banen te leiden.

2 Methode

Binnen dit onderzoek zijn achtereenvolgens de volgende activiteiten uitgevoerd:
a. Deskresearch
b. Verdieping middels ‘diepte interviews’
c. Presentatie en enquête tijdens ledenvergadering
d. Rapportage

2.1 Deskresearch

Deze heeft zich gericht op het krijgen van een beeld van de huidige situatie. Om dit beeld helder te krijgen is gewerkt aan de volgende vragen:
- Welke normen, kaders, wetten en regels zijn er t.a.v. cybersecurity / informatiebeveiliging waar een installateur mee van doen heeft?
- Welke stakeholders zijn er rond de gehele ‘lifecycle’ van een installatie?
- Welke informatie en systemen zouden ‘gehackt’ kunnen worden of vatbaar kunnen zijn voor incidenten op het gebied van informatiebeveiliging?
- Wat is het risico en de potentiële impact?
- Welke vragen moeten we stellen bij de diepte-interviews?

Op basis van alle informatie die in de deze fase is opgehaald is een vragenlijst opgesteld die gebruikt is bij de diepte interviews. De vragenlijst is terug te vinden in bijlage 2.

2.2 Diepte Interviews

Er zijn een tiental gesprekken gevoerd bij installateurs van alarminstallaties, fabrikanten van alarminstallaties en Particuliere Alarm Centrales (PAC’s) waar de installateurs veel mee te maken hebben in hun dagelijks werk. Deze interviews hebben een open karakter gehad, waarbij niet echt een hele duidelijke vragenlijst is doorgenomen. Op basis van een leidraad met vragen (zie bijlage 2) is een gesprek gevoerd en zijn punten doorgesproken met de partijen.

De volgende gesprekken zijn gevoerd:

Organisatie	**Rol geinterviewde**	**Aantal**
Installateur > 250	Directeur	1
Installateur < 100	Directeur	3
Installateur < 100	Monteur	1
Installateur < 100	Adviseur en werkvoorbereider	1
PAC		1
Fabrikant		1
n.v.t.	Onafhankelijk adviseur	1
Totaal		**9**

Uiteindelijk zijn de resultaten van deze gesprekken op onderstaande wijze ingedeeld:
- Relaties
  - Relatie tussen installateur en eindklant
  - Relatie tussen installateur en ICT beheerder
  - Relatie tussen installateur en PAC
  - Relatie tussen installateur en fabrikant
- Organisatie van de installateur
  - Interne organisatie van de installateur
  - Medewerkers
  - Certificeringen, normeringen en wet- en regelgeving
- De installaties
  - Advies en plaatsing
  - Onderhoud
  - Werken met oudere installaties

2.3 Toetsen resultaten ledenbijeenkomst

De resultaten van deze interviews zijn vervolgens in een aantal stellingen opgezet die bij de ledenvergadering van de alarminstallateurs van Techniek Nederland op 6 juni 2019 zijn voorgehouden. De aanwezigen konden vervolgens middels een groene of rode kaart aangeven in welk antwoord ze zich het beste konden vinden. De resultaten van de diepte interviews en de stemming op de ledenvergadering is in dit rapport opgenomen in bijlage 3.

3 Resultaten

3.1 Deskresearch

3.1.1 Relevante normen, kaders, regels en wetten

Installateurs van alarminstallaties gebruiken een aantal normen en richtlijnen volgens welke er wordt gewerkt. Hierbij moet gedacht worden aan de BORG regeling en de VEB regeling (normen voor installateurs van alarminstallaties), de VRKI (richtlijn) en de – meer algemene - ISO27001 (voor informatiebeveiliging). De wet Particuliere Beveiligingsbedrijven en Recherchebureaus (Wpbr) is specifiek van toepassing op bedrijven die zich bezighouden met installatie van alarminstallaties.
In de BORG/VEB en VRKI wordt bovendien verwezen naar een aantal normeringen, zoals de NEN-EN 50131 en NEN-EN 50136 die specifiek zijn opgezet voor (installateurs van) alarminstallaties. Ook de IEC62443 (Industriële automatsering en controle systemen, IACS) is van toepassing.
Hiernaast geldt algemene wetgeving, zoals de wet Wet Beveiliging Netwerk- en informatie systemen (Wbni). Tenslotte is recent de wet Computercriminaliteit III en de AVG in 2018 van toepassing geworden.
In bijlage 1 is een korte beschrijving opgenomen per regeling, norm, richtlijn of wet.

3.1.2 De interne organisatie van de installateur in relatie tot de klant

In de VRKI is vastgelegd waaraan een installatie moet voldoen en welke middelen moeten worden ingezet om de eigendommen van de eindklant te beschermen. Er is niet vastgelegd op welke wijze de installateur e.e.a. installeert, welke eisen de installateur stelt aan (ingehuurde) medewerkers en op welke wijze de eigen organisatie met informatie, risico's en dreigingen moet omgaan. Hiervoor is de Borg en de VEB richtlijn vastgelegd.
Elke installateur zal voor haar eigen organisatie moeten bepalen op welk niveau ze zich op dit moment bevind en in hoeverre men kan verbeteren t.a.v. informatiebeveiliging. Dit zal mede afhankelijk zijn van de klantengroep van de installateur (bij leveranciers van bijvoorbeeld de overheid wordt de eis voor leveranciers om te voldoen aan de ISO27001 certificering steeds groter).

3.1.3 Stakeholders

Belanghebbenden kunnen invloed uitoefenen op de cyberweerbaarheid van de bedrijven in de installatiebranche. Enerzijds kunnen de belanghebbenden eisen stellen aan het bedrijf in de installatiebranche (de beveiligingsinstallateur), anderzijds kan de beveiligingsinstallateur van invloed zijn op belanghebbende, doordat de installateur eisen stelt aan de belanghebbende. Daarom kan er onderscheid gemaakt worden tussen drie groepen belanghebbende, namelijk:

1. Belanghebbende die eisen stellen aan beveiligingsinstallateur;
2. Belanghebbende waar beveiligingsinstallateur eisen aan stelt;
3. Belanghebbende die eisen stellen en waar eisen aan worden gesteld.

In onderstaand overzicht zijn de stakeholders vermeld die vanuit de desk-research het meest relevant worden geacht. De stakeholders zijn ingedeeld in de volgende categorieën:

	Stakeholders	**Omschrijving**
1	(Brancheorganisaties) Directe gebruikers	Eindgebruiker van dienst, proces of product
2	(Brancheorganisaties van) Voorwaarde scheppende organisaties / opdrachtgevers	Organisaties die de voorwaarden bepalen waaraan het product of dienst moet voldoen (bijv. opdrachtgevers). Wetmatige voorwaarden worden door wetgevende instanties bepaald (zie 9).
3	(Brancheorganisaties van) Adviserende organisaties	Organisaties die andere belanghebbenden inhoudelijk kunnen adviseren (bijv. ingenieursbureaus, adviesbureaus, consultancy).
4	(Brancheorganisaties van) Uitvoerende / toepassende / dienstverlenende organisaties	Organisaties die het product gebruiken / toepassen in hun dienstverlening naar de eindgebruiker toe (installateur, maar ook aannemers).
5	(Brancheorganisaties van) Producenten / leveranciers van hoofdproduct	Hoofdproducent / hoofdleverancier van de producten die worden gebruikt door uitvoerende, dienstverlenende organisaties.
6	(Brancheorganisaties van) Producenten / leveranciers van aanhangende producten en diensten	Producenten / leveranciers van producten of diensten die in de productketen voorkomen en/of aanbieders van aanvullende diensten.
7	(Brancheorganisaties van) Distributeurs van hoofdproduct	Distributeurs en inkoopkanalen via wie de installateur (4) de Producten inkoopt
8	Onderzoek- en kennisinstellingen	Instellingen die zonder direct commercieel belang kennisleverancier zijn of onderzoek verrichten. Bijv. onderwijsinstellingen, laboratoria, onderzoeksinstellingen.
9	Controlerende instanties	Bijv. inspectiediensten, certificeringinstellingen
10	Wetgevende instanties	Overheden
11	Contextbepaler groter geheel	Organisaties (bijv. stichtingen, platforms) die op generieke wijze betrokken zijn.

3.1.3.1 Belanghebbende die eisen stellen aan de beveiligingsinstallateur

Stakeholder	**Categorie**	**Mate van belang**	**Mate van invloed**	**verwachtingen, eisen en wensen**
Klanten[1]	1	Hoog	Hoog	Juist werkende installaties, goede service
Techniek Nederland	4	Laag	Middel	Belangenbehartiging voor de installateur
VEB	4	Laag	Middel	Belangenbehartiging voor de installateur
Nederlandse Veiligheidsbranche	4	Laag	Middel	Belangenbehartiging voor de installateur
VEBON-NOVB	4	Laag	Middel	Belangenbehartiging voor de installateur
Stichting ISSO	8	Middel	Laag	Voorziet installateur van benodigde kennis en kwaliteitsrichtlijnen
Stichting OTIB	8	Middel	Laag	Voorziet medewerkers van installateur van scholing
Opleidingscentra	8	Middel	Laag	Voorziet medewerkers van installateur van scholing
TVVL	8	Middel	Laag	Platform waar leden kennis ontwikkelen, delen en overdragen.
Autoriteit Persoonsgegevens (AP)	9	Laag	Middel	Installateur moet zich houden aan de AVG
Ministerie van Justitie en Veiligheid	10	Laag	Laag	Zorgen voor een veilig en rechtvaardige maatschappij, toezien op wet PBR

[1] Zakelijk of particulier, enkel of in samenwerkende vorm (bijvoorbeeld in de vorm van een VVE, bedrijfsverzamel-gebouw of winkelcentrum en eigenaar, beheerder of gebruiker)

Ministerie van Economische Zaken en Klimaat	10	Laag	Laag	Zorgen voor een duurzaam, ondernemend Nederland
Centrum voor Criminaliteitspreventie en Veiligheid (CCV)	11	Laag	Middel	Samenwerkingsverband waarbij standaards zoals BORG en VRKI opgezet en onderhouden worden
Verbond van Verzekeraars	2	Laag	Middel	Verbeterde Risico Klasse Indeling (VRKI)
Verzekeraars	2	Middel	Hoog	Individuele verzekeraar van de klantomgeving
NEN	2	Laag	Middel	NEN normeringen, o.a. NEN-EN 50131, NEN-EN 50136, NEN-EN 50518, NPR 8136, NEN8131 en NEC 79
Politie	2	Laag	Middel	Politie Keurmerk Veilig Wonen (PKVW)
Stichting Kwaliteit voor Installaties Nederland (KvINL)	9	Middel	Middel	Certificerende instelling, o.a. verantwoordelijk voor bepaling van de BRL 6020 normering.
KIWA	9	Middel	Middel	Certificerende instelling
SKG-IKOB	9	Middel	Middel	Certificerende instelling voor hang- en sluitwerk (buiten scope?)
FME	3	Laag	Middel	Belangenbehartiging voor technologische industrie

3.1.3.2 Belanghebbenden waar eisen aan worden gesteld door de beveiligingsinstallateur

Stakeholder	**Categorie**	**Mate van belang**	**Mate van invloed**	**verwachtingen, eisen en wensen**
Fabrikanten van beveiligingsinstallaties, camera's, sloten etc. (m.n. via FME)	5	Hoog	Laag	Juist en eenvoudig werkende installaties, goede garantie en service
Inkoopkanalen van apparatuur (Technische unie, Rexel etc.)	7	Middel	Middel	Service, advies
Ontwikkelaars van software en apps die ingrijpen op de beveiligingsinstallaties, bijvoorbeeld gebouwbeheersystemen.	6	Middel	Middel	Goed en veilig werkende apps
IT-leveranciers (Infra)	6	Hoog	Middel	Goed en veilig werkende verbindingen
Leverancier communicatieverbindingen	6	Hoog	Laag	Goed en veilig werkende verbindingen

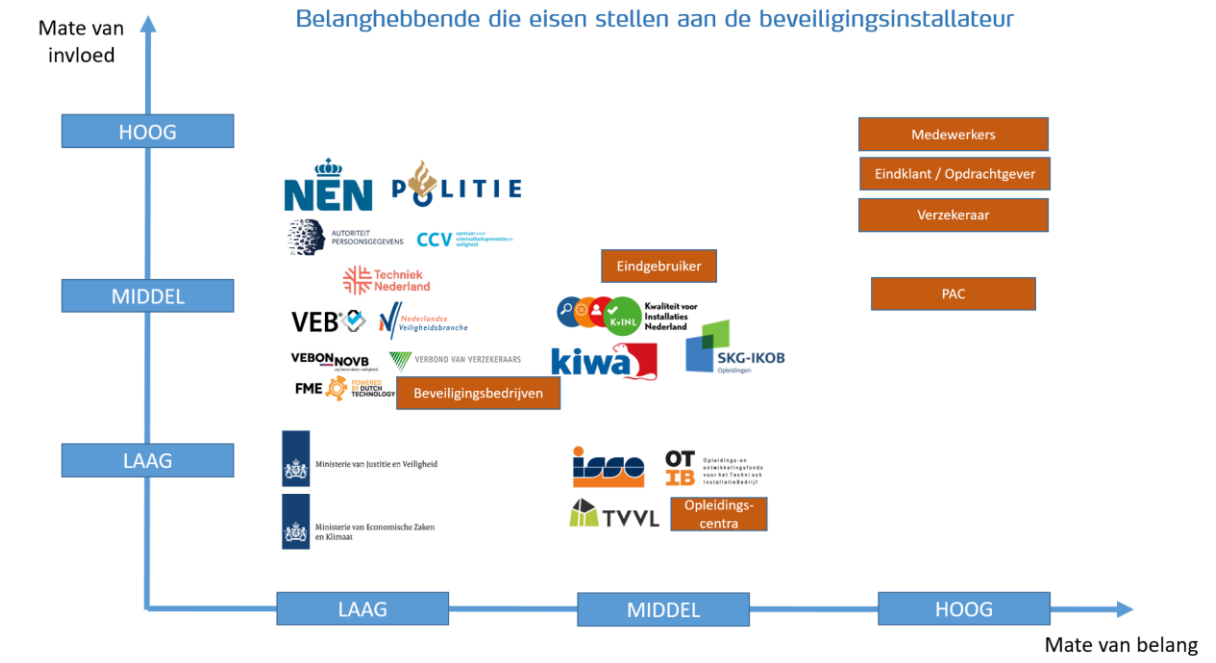
3.1.3.3 Belanghebbenden die eisen stellen aan de beveiligingsinstallateur én waar eisen aan worden gesteld door de beveiligingsinstallateur

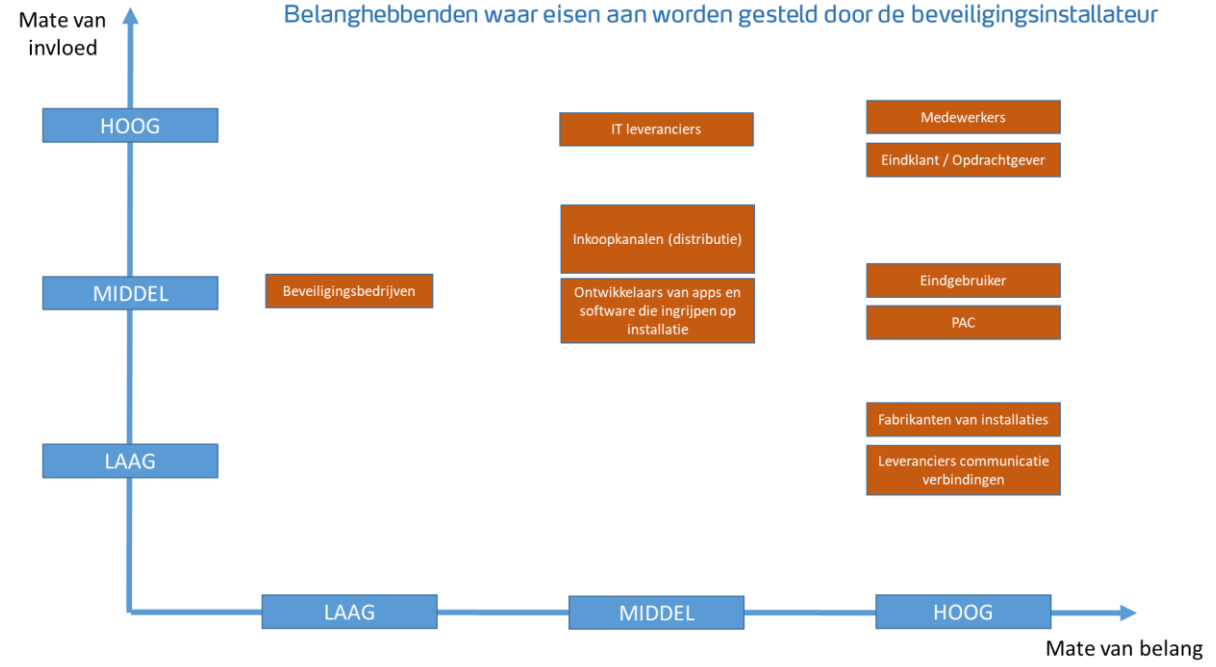
Stakeholder	**Categorie**	**Mate van belang**	**Mate van invloed**	**verwachtingen, eisen en wensen**
Eindgebruikers van de apparatuur (personen)	1	Middel	Middel	Installatie moet eenvoudig werken, serviceniveau installateur moet goed zijn
		Hoog	Middel	Eindgebruikers moeten weten hoe de installatie werkt en volgens de voorschriften gebruiken
Alarm Receiving Centre (ARC) of Particuliere Alarm Centrales (PAC)	6	Hoog	Middel	Configuratie en installatie moet juist zijn
		Hoog	Middel	Alarmmeldingen moeten tijdig en juist opgevolgd worden richting eindklant
Medewerkers van beveiligingsinstallateur	5	Hoog	Hoog	Goed werkgeverschap (incl. primaire en secundaire arbeidsvoorwaarden)

		Hoog	Hoog	Levering van arbeid en kennis
Beveiligingsbedrijven / bewakingsdiensten	6	Laag	Middel	Installatie die juist werkt
		Laag	Middel	Op een juiste en tijdige wijze oppakken van meldingen die vanuit PAC's komen
Hoofdaannemers, resellers	4	Hoog	Hoog	Juist werkende installaties, goede service
		Hoog	Hoog	Betaling van uitgevoerde werkzaamheden

3.1.4 Mate van invloed en belang stakeholders, visueel weergegeven

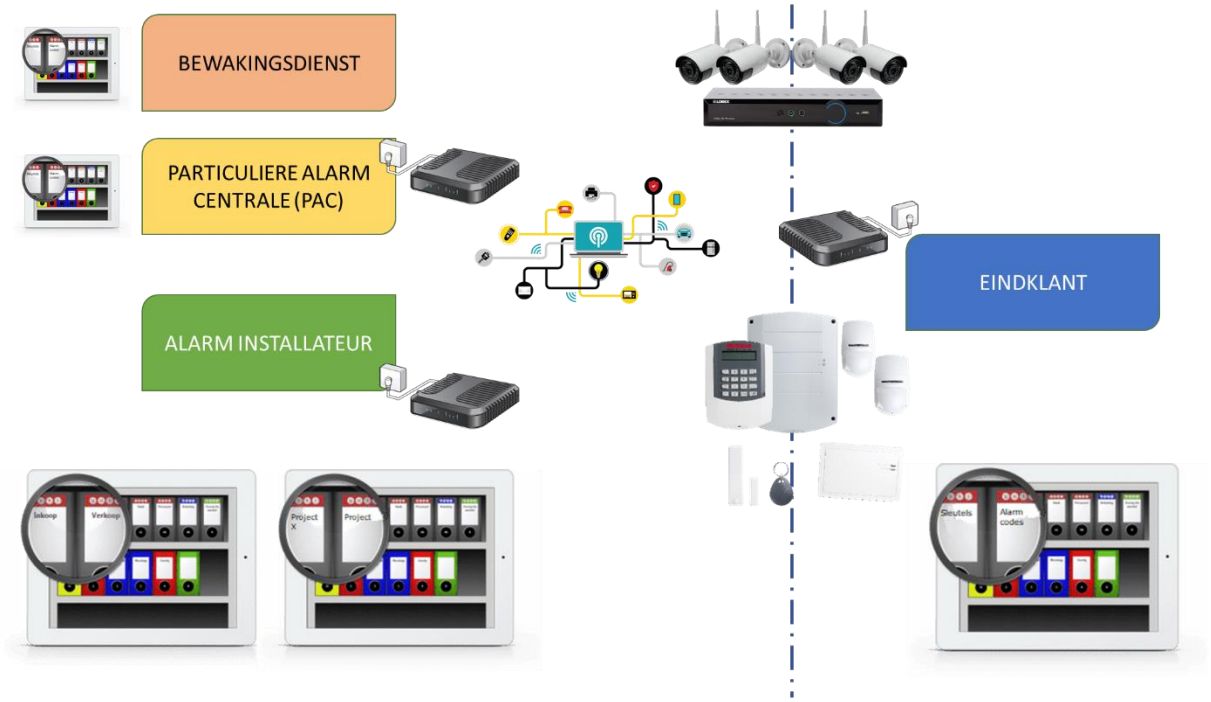
In onderstaande afbeeldingen zijn de mate van invloed en de mate van belang van de beveiligingsinstallateur en haar stakeholder visueel weergegeven.





3.1.5 Vatbare informatie en systemen

In het onderzoek is m.n. gekeken op welke wijze de installateur van de alarm- en camera-installaties zich beter weerbaar kunnen maken tegen vormen van cybercriminaliteit en verstoringen in de informatiebeveiliging. Dit behelst de totale lifecycle van de alarm- of camera installatie, inclusief alle daaraan verbonden beleid, standaards, processen, procedures, handleidingen etc.
Om te weten op welke wijze de installateur zijn digitale weerbaarheid kan verbeteren, is inzicht nodig in de 'assets' (middelen) die de installateur in zijn bezit heeft of beheerd in de volledige levenscyclus van een installatie (en daarvoor/daarna). Dit gaat dus verder dan de installatie zelf, ook een projectdossier, een alarmcode etc. vallen onder de 'assets'.
Voor het werken met de alarminstallaties is een lijst opgezet van 'assets'. Ditzelfde is gedaan voor camera's en specifieke assets die voor de installateur, eindklant, Particuliere Alarm Centrale (PAC) en bewakingsdienst van toepassing zijn.



Voor de alarminstallaties zijn de volgende 'assets' gedefinieerd:

- Alarmcentrale, eventueel met externe koppelingen (bijv. RS-232 etc.);
- Sensoren en detectoren (magneetcontacten, trilcontacten, bewegingsmelders, glasbreuk, hitte/rook etc.)
- Alarmgevers (sirenes met licht en/of geluid, mistgeneratoren etc.)
- Bedienpanelen/kaartlezers incl. sleutels, passen, afstandsbedieningen etc.
- Noodstroomvoorziening
- Verbinding(en) tussen alarmcentrale en PAC (primair en evt. secundair)
- Verbinding tussen alarmcentrale en installateur
- Verbinding tussen alarmcentrale en alarmgevers
- Verbinding tussen alarmcentrale en sensoren en detectoren

Voor de camera systemen zijn de volgende 'assets' gedefinieerd:

- Camera's
- Systemen t.b.v. opslag van de data die van camera's afkomt (recorder)
- Verbinding tussen camera's en opslagsysteem
- Apps die op afstand verbinding maken met opslagsysteem

Assets t.b.v. de installateur

- De organisatie
- Projectdossier inclusief tekeningen, codes etc.
- Uitgegeven procescertificaat, beveiligingscertificaat, opleveringsbewijs (van alarminstallatie en bouwkundige beveiliging)
- Mogelijkheden tot inloggen op afstand op de centrale met codes, procedures etc. daaromheen
- (ingehuurde) medewerkers van de installateur
- Auditor

- Ontwikkelaar van apps en systemen die gekoppeld worden aan alarmcentrales of camera systemen etc. (denk aan gebouwbeheer etc)

Assets t.b.v. de eindklant
- De te beschermen goederen, inventaris en informatie
- Dossier met beheer van uitgegeven en ingetrokken sleutels (sleutelbeheer)
- Dossier met beheer van uitgegeven en ingetrokken alarmcodes (alarmcodebeheer)
- Ontvangen procescertificaat, beveiligingscertificaat, opleveringsbewijs (van alarminstallatie en bouwkundige beveiliging)
- Beheerder van alarmcentrale en/of camera systemen
- HR afdeling voor uitgifte en inname van sleutels, codes en toegang
- Eindgebruikers

Assets t.b.v. PAC en bewakingsdienst
- Projectdossier met gegevens over eindklant, installateur en alarminstallatie
- Mogelijkheden tot inloggen op afstand op de centrale met codes, procedures etc. daaromheen?
- Medewerkers PAC en/of bewakingsdienst

Overige assets zijn voor de installateur buiten beschouwing gelaten.

Uit bovenstaande lijst blijkt dat de assets waar de installateur op enigerlei wijze mee te maken heeft veel verder gaat dan de alarminstallatie, de camera's en de te beschermen goederen, inventaris en informatie. Vanuit de optiek van informatiebeveiliging zal per asset bekeken moeten worden wat de risico's zijn t.a.v. beschikbaarheid, integriteit en vertrouwelijkheid (de zogenaamde BIV classificatie[1]).

Het bepalen van de risico's gebeurt volgens onderstaande algemene formule:

Risico = kans x impact (3.1)

3.1.6 Inschatting van de risico's

Om het proces om risico's in te schatten voor de eindklanten wordt door installateurs veelvuldig de VRKI gebruikt. Op basis van eenvoudig te begrijpen model (gebaseerd op de 'attractiviteit' van de te bewaken zaken/inboedel) wordt een risicoklasse bepaalt, op basis waarvan vervolgens een aantal beveiligingsmaatregelen worden geadviseerd.
Een dergelijk model is voor informatiebeveiliging (nog) niet in aanwezig. De installateur zal per situatie moeten bekijken wat de kans van een dreiging is op de eerder beschreven assets. Op basis van de kans en de mogelijke impact kan vervolgens een risico worden bepaald en kan worden besloten welke maatregelen getroffen moeten worden om een risico – indien nodig – te verminderen/mitigeren, te vermijden, te accepteren of over te dragen.

De installateur zal per asset moeten kijken welke dreigingen er zijn, wat de kans is dat een dreiging werkelijkheid wordt en wat de impact is bij calamiteiten. Op basis daarvan kunnen de juiste maatregelen worden getroffen.

3.1.6.1 Het bepalen van de kans van een dreiging

Ten aanzien van digitale dreigingen geldt dat het bepalen van de kans lastig en zeer afhankelijk van de (klant)situatie bepaald kan worden. Gesteld kan worden dat een installateur die werkt voor klanten uit onderstaande lijstje, de kans op hacking en cyberinbraak groter is.
- klanten die zelf veel zaken met 'attractieve waarde' in hun pand hebben (te denken valt uiteraard aan juweliers, maar ook particulieren met auto-, kunst- of antiekcollecties etc.);
- klanten die werken in/voor kritische infrastructuren;
- klanten die zelf veel informatie verwerken;
- klanten die gevoelige of bijzondere (persoons)gegevens verwerken;
- klanten die veel werken met octrooien, patenten etc;
- (semi)-overheden, gevangenissen etc.

[1] https://nl.wikipedia.org/wiki/BIV-classificatie

3.1.6.2 Impact bepalen

De impact van een verstoring wordt bepaald aan de hand van de BIV-classificatie (Beschikbaarheid, Integriteit en Vertrouwelijkheid). E.e.a. is volgens de theorie als volgt te definiëren[1]:
Beschikbaarheid (Continuïteit): informatie moet beschikbaar en toegankelijk zijn. Classificatie gaat in op de mogelijke gevolgen als informatie, of een informatie set, niet beschikbaar is.
Integriteit (Betrouwbaarheid): Het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Goed beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens voor een gedefinieerde groep gerechtigden is cruciaal voor de integriteit van informatie. Classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig is of niet actueel is.
Vertrouwelijkheid (Exclusiviteit): De bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Classificatie gaat in op de mogelijke gevolgen wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.

Grofweg hebben we tijdens de deskresearch een aantal voorbeelden uitgewerkt van mogelijke impact bij calamiteiten voor:

- De kantoorautomatisering (KA) van de installateur;
- De werking van de alarminstallaties;
- de situatie van de eindklant.

Deze worden hieronder beschreven.

3.1.7 Impact op kantoorautomatisering (KA) van de installateur

Mogelijke impact op administratieve processen komt voort uit de ‘reguliere’ Kantoor Automatisering (KA) die bij de installateurs wordt gebruikt. De impact van beveiligingsissues heeft m.n. betrekking op de eigen organisatie, maar kan ook escaleren naar impact op gegevens van klanten en uiteindelijk zelfs naar de opgeleverde alarminstallaties met alle mogelijke gevolgen van dien.

Beschikbaarheid

- Systemen met informatie over klantgegevens, offerte/orderadministratie, financiële administratie, projecten, planning, afgegeven certificaten, standaards, service/support administratie, procedures etc. zijn niet (meer) beschikbaar.

Integriteit

- Gegevens van klanten met bijvoorbeeld inloggegevens, tekeningen etc. raken aangetast;
- Informatie van reeds afgegeven certificaten raken aangetast;
- Standaards en procedures rond de installatie van alarminstallaties worden aangetast.

Vertrouwelijkheid

- Standaards en procedures rond inrichting van installaties komen op straat te liggen;
- Klantgegevens met inlogcodes en bijvoorbeeld tekeningen etc. komen op straat te liggen;
- Beheerdersgegevens (denk daarmee ultimum aan inloggegevens van alarminstallaties) komen op straat te liggen.

3.1.8 Impact op de werking van alarminstallaties

Dit hoofdstuk gaat in op mogelijke inbreuken op de alarminstallatie zelf, inclusief verbindingen, detectoren, alarmgevers etc.

Beschikbaarheid

- Alarminstallatie(s) is/zijn niet beschikbaar;
- Detectoren en sensoren geven geen signalen door aan alarminstallatie(s);
- Sabotagebescherming werkt niet;
- Meldingen worden niet doorgegeven aan alarmgevers (sirenes, mistsystemen etc.);
- Meldingen worden niet doorgegeven aan PAC.

Integriteit

- Gegevens in de alarminstallatie(s) blijken niet juist, te denken aan gegevens van beheerder, gebruikers, zones, detectoren/sensoren, alarmgevers, sabotagewerking, logs etc.;

[1] https://nl.wikipedia.org/wiki/BIV-classificatie

- Gegevens in de alarminstallatie(s) blijken te worden gerouteerd waardoor meldingen niet meer juist worden verwerkt. Denk hierbij aan routering van informatie van sensoren/detectoren die hun meldingen niet meer kunnen afgeven of waardoor de alarminstallatie haar meldingen niet meer kan afgeven aan alarmgevers of PAC.

Vertrouwelijkheid
- Gegevens in de alarminstallatie(s) blijken (bewust of onbewust) op straat te liggen;
- Opgeleverde systemen blijken niet te voldoen aan de wetgeving (m.n. AVG);
- Hoofdbeveiligingscode van installateur van alarmsystemen blijken op straat te liggen (in hoeverre wordt er één hoofdbeveiligingscode gebruikt voor alle systemen)?

3.1.9 Impact op de situatie van de eindklant

De impact/schade bij verstoringen in de beschikbaarheid, integriteit of vertrouwelijkheid zal per klantsituatie verschillen (de alarminstallatie van een organisatie die onderdeel uitmaakt van de kritische infrastructuren in Nederland zal bij verstoring een andere impact hebben dan bij een gemiddeld MKB bedrijf of consument).

De installateur zal dan ook samen met de eindklant moeten bepalen wat de impact is als er verstoring optreedt. Zoals aangegeven gebeurt deze risico inschatting voor de alarminstallaties zelf veelal aan de hand van de VRKI (bij relatief kleinere klantomgevingen). Aan de hand hiervan kan bepaald worden welke maatregelen moeten worden genomen om tot een passend beveiligingsniveau te komen. Bij omgevingen met een hogere attractiviteit wordt er een aparte risicobeoordeling uitgevoerd i.s.m. de verzekeraar.

In onze optiek zal er niet alleen naar de waarde gekeken moeten worden van de te beschermen activa zoals in de VRKI is opgenomen, maar zal ook bijvoorbeeld naar zaken gekeken moeten worden zoals:
- Als door verstoring van het alarmsysteem medewerkers niet meer naar binnen kunnen, wat is dan het productiviteitsverlies;
- Wat zijn de kosten van vervanging of herstel van de alarmcentrale zelf;
- Wat is de waarde van informatie die zich binnen het te beschermen object bevinden (wordt hierop goed doorgevraagd?);
- Treedt er schade aan goodwill/reputatie of imago op als er een verstoring optreedt en is deze te kwantificeren?

3.2 Conclusies

In het traject bleek al snel dat er in feite twee ‘stromingen’ zijn die van belang zijn t.a.v. informatiebeveiliging, namelijk:
1. De te leveren en onderhouden alarminstallatie – inclusief alles daaromheen zoals bekabeling, verbindingen, sensoren, detectoren, alarmgevers etc. etc. – én, - wellicht nog wel belangrijker:
2. De organisatorische kant (interne organisatie, afspraken met betrokken partijen etc.).

Gebleken is dat er veel stakeholders betrokken zijn in het proces van advisering tot en met oplevering en onderhoud van alarminstallaties. De belangrijkste partijen in het proces zijn:
- de fabrikanten
- verzekeraars,
- Particuliere Alarm Centrales (PAC’s),
- medewerkers van de installateur,
- de klanten en
- de ICT’ers die verantwoordelijk zijn voor de klants infrastructuur.

Met al deze partijen wordt informatie uitgewisseld. Informatie die in handen van kwaadwillenden al snel kan leiden tot bijvoorbeeld vormen van (digitale) inbraak of die door foute omgang kunnen leiden tot onveilige systemen. De gevolgen kunnen voor de installateurs en haar klanten groot zijn. Of de installateurs goed met crisissituaties om kunnen gaan is niet bekend; het overgrote merendeel van de benaderde installateurs heeft namelijk geen crisisplan. Door de samenwerking in een keten is in feite daarmee een risico voor alle partijen aanwezig.

Het continue streven naar verbetering op het gebied van informatiebeveiliging in de gehele keten zal belangrijker worden.

Uit de interviews blijkt dat eindklanten niet genoeg naar de wijze vragen waarop installateurs zorgen voor (hun eigen) informatiebeveiliging. Veelal hebben ze daarvoor ook onvoldoende kennis (ze weten niet de juiste vragen te stellen). Juist daar ligt in een kans door aan te tonen dat installateurs serieus werk maken van informatiebeveiliging en daarmee de kwalitatief mindere partijen in offertetrajecten al beter weten uit te sluiten.

Installateurs lijken zich over het algemeen goed bewust van hun rol in de keten. Het proces rond het adviseren en opleveren van alarminstallaties is op veel punten geborgd door bijvoorbeeld regelingen als de BORG en VEB (t.b.v. de interne organisatie van de installateur) en instrumenten zoals de VRKI (om een risico inschatting te kunnen maken bij de eindklant en daarop het advies te kunnen uitwerken). Er gaat daardoor dan ook veel goed. Ten aanzien van informatiebeveiliging zijn er echter ook verbeteringen mogelijk. Met name op organisatorisch vlak (bijvoorbeeld omgang met alarmcodes door monteurs cq binnen de organisatie van de installateur, asset management (bij welke klant staat welke installatie met welke versie etc.) is nog veel onduidelijk of wordt nog niet goed opgepakt. Een ISO2700x certificering is voor de meeste installateurs in het MKB een te zware ‘last’. Dit heeft alles te maken met hun concurrentiepositie. Doordat certificering van alarminstallaties niet altijd verplicht is (m.n. in de onderkant van de markt, zoals bij particulieren en MKB), wordt veelal op prijs geconcurreerd. Dit kan de kwaliteit van het opgeleverde werk en de algemene kwaliteit van de installateur onder druk zetten. Ook basisbehoeften rond informatiebeveiliging die een installateur eigenlijk geregeld zou moeten hebben kunnen daardoor onder druk komen te staan. We zijn van mening dat in de BORG en VEB regeling en VRKI richtlijn een aantal basale eisen t.a.v. informatiebeveiliging missen die een installateur wel op orde zou moeten hebben (bijvoorbeeld de onderhoudsrichtlijnen van de BORG regeling stammen uit 2000). De gehele branche zal profiteren van verbeteringen op het gebied van informatiebeveiliging in deze richtlijnen en regelingen.

Door technische wijzigingen in de laatste jaren (met name op het gebied van de verbindingen van de alarmcentrales via bijvoorbeeld WiFi en het openbare internet) is (algemene) ICT kennis steeds belangrijker geworden. De installateurs geven zelf aan dat deze kennis nog onvoldoende aanwezig is, dat nieuwe krachten die van school komen eigenlijk meer praktische kennis mee zouden moeten nemen en dat de kennis bij het bestaande personeel onvoldoende wordt opgebouwd door te weinig aansluiting van kennisinstituten met de praktijk. Hiervoor is het belangrijk dat de eindtermen meer gaan aansluiten; de vraag van de installateurs is met name om meer praktische kennis mee te geven.

4 Aanbevelingen

4.1 Aanbeveling per relatie

Per relatie en situatie zijn op basis van deskresearch, interviews en gesprekken met stakeholders een aantal aanbevelingen op te stellen. Hieronder volgte een opsomming van deze aanbevelingen. Een meer uitgewerkt versie is terug te vinden in bijlage 3.

Relatie installateur – Eindklant

- Zorg er voor dat klanten bewuster omgaan met informatiebeveiliging en bij projecten dus ook meer gaan vragen over de informatiebeveiliging is geregeld. De betere installateurs kunnen zich hierdoor ook beter profileren en onderscheiden.
- Andere mogelijkheid is om informatiebeveiliging (nog) meer onderdeel uit te laten maken van de VEB/BORG en VRKI certificering en in de markt duidelijker te communiceren wat de voordelen zijn van het werken met een gecertificeerd installateur.

Relatie installateur – ICT beheerder

- Zorg er voor dat afstemming tussen installateur en ICT beheerders meer gestandaardiseerd verloopt en dat ICT beheerders bewuster omgaan met de informatiebeveiliging van alarminstallaties. De juiste werking van installaties is sterk afhankelijk van hun werkzaamheden.

Relatie installateur – PAC

- Zorg voor een gestandaardiseerde overdracht tussen installateur en PAC, die bij voorkeur via een digitaal portaal verloopt. Ook het plaatsen van een centrale in testmodus zou gedigitaliseerd kunnen/moeten (?) verlopen met duidelijke eisen t.a.v. autorisatie en authenticatie.
- Voor het gebruik van Apps dienen – zeker door monteurs – de juiste beveiligingsvoorschriften te worden gebruikt.

Relatie installateur - leverancier/fabrikant

- Ideaal loopt het proces tussen uitlevering van installaties tussen fabrikant, installateur, netwerkbeheerder, PAC en eindklant digitaal. Zo weten alle partijen welke maatregelen zijn getroffen en kan de kwaliteit in de gehele keten verbeterd worden.
- Als dit ondoenlijk is, kunnen fabrikanten meer gaan eisen dat centrales geregistreerd worden (bij voorbeeld in het kader van fabrieksgarantie) zodat bekend is waar de installaties zich bevinden en welke installateur e.e.a. heeft aangelegd.
- Security en privacy by design/default moet een verplichting zijn/worden voor alle alarminstallaties die op de markt worden gebracht. Er zal nader onderzoek moeten worden gedaan in hoeverre fabrikanten hiertoe op dit moment verplicht zijn en welke verplichtingen daar op dit moment voor gelden.

Interne organisatie van de installateur

- In de VEB- en BORG regeling wordt m.n. gekeken naar de wijze waarop installaties opgeleverd moeten worden. In onze optiek zou informatiebeveiliging van de organisatie van de installateur (inclusief beleid, medewerkers, techniek, procedures etc.) in deze regelingen meer/prominenter meegenomen kunnen/moeten worden
- Het is wenselijk dat er standaardisatie komt inclusief duidelijke procedures (die gebruiksvriendelijk zijn voor zowel eindklant als monteur). Deze moeten voor kleinere installateurs minder zwaar zijn dan de eisen/richtlijnen uit de ISO2700x, maar zwaarder dan wat nu gebruikt wordt en ingaan op zowel beleid/organisatie, techniek als menselijk handelen/bewustzijn.
- Ondersteun installateurs in het opzetten van een crisisplan zodat áls er in de branche iets fout gaat, bedrijven ook weten wat ze moeten doen.
- In workshops kan ook eens nagespeeld worden wat er allemaal bij een crisis komt kijken. Dit gaat veel verder dan techniek en gaat ook verder dan alleen de installateur (ook een PAC, fabrikant of klant kan te maken krijgen met vormen van cybercriminaliteit die impact heeft op de installateur).

Gebruik van wachtwoorden

- Zorg voor een duidelijke levenscyclus van wachtwoorden van installaties van klanten (van aanmaak tot vast en incidenteel onderhoud en beëindiging van de relatie met klant/medewerkers). Hierbij zal gekeken moeten worden naar juiste autorisatie (rechten) en authenticatie (identificatie). M.n. voor kleinere installateurs denken we dat het handig is om hier bepaalde tooling voor aan te leveren cq ze te wijzen op tooling die in de markt voorhanden is.

Medewerkers van de installateur

- Bekijk in hoeverre het mogelijk is om training op te zetten rond informatiebeveiliging. In onze optiek zou dit zich enerzijds moeten richten op de installaties die opgeleverd worden, maar anderzijds ook heel duidelijk gericht op de interne organisatie van de installateur (informatiebeveiliging op de KA omgeving). Controleer verder in hoeverre in de eindtermen informatiebeveiliging in voldoende mate is opgenomen.
- Het is wenselijk dat er standaardisatie komt inclusief duidelijke procedures. Deze moeten voor kleinere installateurs minder zwaar zijn dan de eisen/richtlijnen uit de ISO2700x, maar zwaarder dan wat nu gebruikt wordt en ingaan op zowel beleid/organisatie, techniek als menselijk handelen/bewustzijn. Een in-dienst, wijzig functie en uit-dienst procedure horen hier nadrukkelijk bij.

Certificeringen

- Het is wenselijk dat er standaardisatie komt inclusief duidelijke procedures. Deze moeten voor kleinere installateurs minder zwaar zijn dan de eisen/richtlijnen uit de ISO2700x, maar zwaarder dan wat nu gebruikt wordt en ingaan op zowel beleid/organisatie, techniek als menselijk handelen/bewustzijn. Een in-dienst, wijzig functie en uit-dienst procedure horen hier nadrukkelijk bij.

Advies en plaatsing van installaties bij klanten

- In de risico-inventarisaties wordt m.n. gekeken naar de fysieke waarde van spullen. Er wordt zover bekend geen rekening gehouden met bijvoorbeeld de waarde van data. In onze optiek zou dit opgenomen moeten worden in de VRKI.
- Zet in de VRKI een aantal eisen op t.a.v. informatiebeveiliging, bijvoorbeeld gericht op DDoS aanvallen, hacking van installaties etc. Inmiddels is in de VRKI wel een hoofdstuk opgenomen omtrent alarmtransmissie. Verder onderzocht moet worden in hoeverre de verbindingen t.b.v. onderhoud zijn opgenomen – of opgenomen moeten worden – in de VRKI.
- Zeker bij middelgrote installaties kan een kwaliteitsslag gemaakt worden door de oplevering – en controle op juiste werking + informatiebeveiliging – door een andere persoon te laten plaatsvinden cq een verplichte audit te laten uitvoeren. Dit is nu (nog) geen onderdeel van de VEB- en BORG regeling.
- T.a.v. het werken met camera systemen in relatie tot de AVG kan er een aparte flyer of document opgezet worden, zodat de eindklant i.s.m. zijn installateur hier ook eenvoudig naar kan handelen.
- Zorg voor een duidelijke procedure omtrent de wijze waarop afscheid genomen wordt van een klant en welke verplichtingen dan gelden t.a.v. het behouden van dossierinformatie (o.a. bewaartermijnen, omgang met back-ups van installaties etc.).

Onderhoud van installaties bij klanten

- De voorschriften voor onderhoud van de BORG regeling stammen uit 2000. Informatiebeveiliging is hier nog niet in opgenomen en we adviseren om deze te herzien, waarbij rekening is gehouden met alle punten die te maken hebben met informatiebeveiliging.
- Zorg er voor dat het nalopen van logging onderdeel gaat vormen van het onderhoud óf dat er automatisch acties worden uitgevoerd op het moment dat zich uitzonderingssituaties voordoen.
- Zet een duidelijke (minimale) procedure op waarin wordt aangegeven op welke wijze er op afstand ingelogd kan/mag worden.

Werken met oudere installaties

- Informatiebeveiliging is niet alleen van de 21e eeuw. Er ligt nu meer nadruk op, omdat vrijwel alles aan het internet wordt gekoppeld en daardoor ook nieuwe dreigingen ontstaan. Bekijk ook voor oudere installaties welke impact informatiebeveiliging heeft of kan hebben.

4.2 Voorzet eindtermen installateur mbt cyberweerbaarheid

Installateur

Taak:

- Adviseren van klanten mbt alarminstallaties,
- Het maken van ontwerpen van alarminstallaties,
- Het aanleggen en programmeren van alarminstallaties,
- Het beheren en onderhouden van alarminstallaties,
- Het opbouwen van dossiers voor beheer,
- Het bijhouden van dossiers.

Deeltaak

Eindtermen deeltaken

De kandidaat kan irt cyberweerbaarheid:		BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	Klant adviseren mbt alarminstallaties			X	X	X	X	X
2.	Een alarminstallatie ontwerpen				X		X	X
3.	Een alarminstallatie aanleggen en programmeren	X	X	X		X	X	
4.	Een alarminstallatie beheren en onderhouden	X	X	X		X		
5.	Een dossier voor beheer opbouwen			X	X		X	X
6.	Een dossier voor beheer bijhouden	X	X	X			X	X
7.	Continu kennis bijspijkeren mbt cyberweerbaarheid			X	X	X	X	X

BB: Basisberoepsgerichte leerweg

De basisberoepsgerichte leerweg (bbl) is een opleidingsrichting binnen het voorbereidend middelbaar beroepsonderwijs (vmbo). Deze richting is bestemd voor leerlingen die meer op de praktijk zijn ingesteld.

KB: Kaderberoepsgerichte leerweg

De kaderberoepsgerichte leerweg (kblw) is een opleidingsrichting binnen het voorbereidend middelbaar beroepsonderwijs (vmbo). Deze leerweg is voor leerlingen die het liefst kennis opdoen door met praktijk bezig te zijn.

De benaming verwijst naar het feit dat de leerlingen bezig zijn met een opleiding die in haar geheel gericht is op een functie binnen het kader van de gekozen sector. De leerling doet examen in vier algemene vakken en een beroepsgericht vak of programma met een omvang van 960 uur.

GL: Gemengde leerweg

De gemengde leerweg (GL) is een van de vijf leerwegen in het Nederlands vmbo. Deze leerweg is bedoeld voor leerlingen die op zich weinig moeite hebben met studeren, maar zich ook al gericht willen voorbereiden op bepaalde beroepen.
De benaming ‘gemengde leerweg’ betekent dus een vermenging van zowel theoretisch als praktisch onderwijs.

TL: Theoretische leerweg

De theoretische leerweg is de algemeen vormende leerweg van het vmbo.

(bron: Wikipedia, Min van OCW)

Bij de niveau’s MBO 3, MBO4 en MBO 4+ moet men denken aan een monteur beveiligingsinstallaties (MBO 3), een technicus Beveiligingsinstallaties (MBO 4), een adviseur beveiliging (MBO 4+) en een TB Mechanische beveiliging (MBO 4+).

Uitwerking deeltaak (irt cyberweerbaarheid) 1:”Klant adviseren mbt alarminstallaties”

	In dit verband kan de kandidaat:	BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	De behoeften van de klant in beeld brengen				X		X	X
2.	De klant helpen de juiste vragen te stellen				X		X	X
3.	De klant de juiste oplossing te bieden				X		X	X
4.	Een advies uitbrengen en offerte opstellen			X	X		X	X

Uitwerking deeltaak (irt cyberweerbaarheid) 2:"Een alarminstallatie ontwerpen"

	In dit verband kan de kandidaat:	BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	Een bestaande situatie in beeld brengen				X	X	X	
2.	Een principeontwerp maken				X		X	X
3.	Een concept voorleggen aan de klant				X		X	X
4.	Het uitdetailleren van het goedgekeurde principeontwerp			X	X	X	X	X
5.	Het bespreken van het ontwerp met de klant				X		X	X

Uitwerking deeltaak (irt cyberweerbaarheid) 3:"Een alarminstallatie aanleggen en programmeren"

	In dit verband kan de kandidaat:	BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	De juiste materialen bestellen		X	X	X	X	X	
2.	Het juiste gereedschap gebruiken	X	X	X		X	X	
3.	Het werkgebied van de aan te leggen installatie voorbereiden (werkruimte creeren)	X	X	X		X	X	
4.	Overleggen met de klant van de te ondernemen werkzaamheden (wat gaat de installateur doen, waar en op welke wijze, binnen welke termijn)	X	X	X		X	X	X
5.	De alarminstallatie op een goede en nette manier aanleggen	X	X			X	X	
	De alarminstallatie op een goede en nette manier programmeren	X	X	X		X	X	
6.	Wijzigingen tijdens de aanleg bijhouden	X	X			X	X	
7.	Revisiedocumenten opstellen		X	X	X	X	X	X
8.	De gerealiseerde installatie overdragen aan de klant (wachtwoorden, aandachtspunten, advies gebruik)		X	X	X		X	X
9.	Het werkgebied weghalen en netjes achterlaten	X	X	X		X	X	
10.	De installatie overdragen/in beheer opnemen aan een PAC			X	X		X	X
11.	Praktische aanbevelingen mbt ICT uitvoeren in de te realiseren installatie	X	X	X		X	X	X

Uitwerking deeltaak (irt cyberweerbaarheid) 4:"Een alarminstallatie beheren en onderhouden"

	In dit verband kan de kandidaat:	BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	Een alarminstallatie onderhouden	X	X	X		X	X	
2.	Storingen verhelpen		X	X		X	X	
3.	In dossier van installatie aantekeningen maken mbt onderhoud/storing		X	X		X	X	
4.	Een advies voor verbetering/aanpassing opstellen		X	X	X	X	X	X
5.	Een advies geven aan de klant over gebruik van de installatie		X	X	X	X	X	X
6.	Overleggen met PAC			X	X	X	X	X
7.	(Software)updates doorvoeren van installaties		X	X		X	X	
8.	Klanten informeren over potentiële dreigingen en hiervoor oplossingen aandragen			X	X		X	X

Uitwerking deeltaak (irt cyberweerbaarheid) 5:"Een dossier voor beheer opbouwen"

	In dit verband kan de kandidaat:	BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	Een beheercyclus voor de installatie opstellen				X		X	X

	(hard- en softwareupdates)							
2.	Het revisiedossier up to date houden				X		X	X
3.	Een systeem opstellen/gebruiken voor het beheer van verschillende installaties				X		X	X
4.	Goed wachtwoordenbeheer opstellen				X		X	X
5.	Verbeteringen kunnen aandragen voor een beter beheer				X		X	X

Uitwerking deeltaak (irt cyberweerbaarheid) 6:"Een dossier voor beheer bijhouden"

|In dit verband kan de kandidaat:		BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	Het revisiedossier up to date houden			X		X	X	
2.	Klanten informeren over het tijdig wijzigen van wachtwoorden.			X	X	X	X	X
3.	Klanten informeren over het doorvoeren van updates			X	X	X	X	X
4.	Verbeteringen kunnen aandragen voor een beter beheer				X		X	X

Uitwerking deeltaak (irt cyberweerbaarheid) 7:" Continu kennis bijspijkeren mbt cyberweerbaarheid"

|In dit verband kan/is de kandidaat:		BB	KB	GL	TL	MBO3	MBO4	MBO4+
1.	Ontwikkelingen bijhouden en relateren aan eigen werkzaamheden (technisch, hacks, nieuws)				X		X	X
2.	Op de hoogte van potentiële dreigingen en kan hierop anticiperen				X		X	X
3.	Voorstellen doen voor het volgen van geschikte trainingen/workshops/cursussen/opleidingen om het eigen werk goed te kunnen blijven uitvoeren.				X		X	X
4.	Praktische aanbevelingen doen mbt ICT en draadloze systemen				X		X	X

BIJLAGE 1: Normen, wetten en richtlijnen

Korte omschrijving	Lange omschrijving	Laatst bekende publicatiedatum	Regeling, norm, wet of richtlijn
BORG regeling	De BORG-regeling is een keurmerk waarin eisen worden gesteld aan het beveiligingsbedrijf en zijn ontwerp, maar ook aan de uitvoering van dit ontwerp en het onderhoud daarvan. Het kan gezien worden als kwaliteitssysteem. Het Centrum Criminaliteitsbeheersing en Veiligheid (CCV) heeft de verantwoordelijkheid voor de kwaliteitsontwikkeling en beheer van de BORG-regeling. Het CCV is een samenwerkingsverband tussen overheid, bedrijfsleven en eindgebruiker. Het CCV voert deze verantwoordelijkheid niet zelf uit. Dat is uitbesteed aan Certificatie-instellingen (CI's). Een CI beoordeelt dus de erkende BORG-beveiligingsbedrijven en mag deze bedrijven ook certificeren.	1 november 2018	Regeling
VEB kwaliteitsregeling	Kwaliteitssyteem vergelijkbaar met de BORG regeling, maar onder beheer van de Vereniging Erkende Beveiligingsbedrijven (VEB).	26 maart 2009	Regeling
BRL6020 beoordelingsrichtlijn	Richtlijn die is opgezet door KvINL (onafhankelijk beheerder van kwaliteitsrichtlijnen) in opdracht van Uneto-VNI.	15 september 2015	Richtlijn
VRKI	Verbeterde Risicoklassenindeling, eigendom van het Verbond van Verzekeraars en wordt uitgegeven en beheerd door het Centrum Criminaliteitsbeheersing en Veiligheid (CCV). Instrument waarmee een globale risico-inschahting van diefstal en inbraak kan worden gemaakt. Op basis van deze inschatting bepaalt het instrument de beveiligingsmaatregelen.	1 mei 2018	Instrument (Richtlijn)
ISO27001:2013	ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. Met ISO 27001 certificering kan een organisatie laten zien dat het voldoet aan alle eisen rondom informatiebeveiliging	December 2015	norm
Wpbr	De Wet particuliere beveiligingsbedrijven en recherchebureaus stelt eisen aan beveiligingsbedrijven en recherchebureaus, de opleidingen in de branche, bevat waarborgen voor de betrouwbaarheid van het personeel, regelt het toezicht door de politie en de klachtbehandeling door beveiligingsorganisaties. Ook zijn er specifieke regels voor particuliere alarmcentrales en geld- en waardetransport. Naast deze wet is er onderliggende regelgeving.	4 juli 2013	Wet
NEN 8131	NEN 8131 geeft regels voor het ontwerp, de uitvoering, bediening, inbedrijfstelling, onderhoud en de kwaliteit van inbraak- en overvalalarmsystemen (I&OAS) die in gebouwen zijn geïnstalleerd. De eisen en aanbevelingen van deze norm zijn gebaseerd op de Europese normen zoals opgesteld door CLC/TC79 Alarm systems. Deze norm verwijst naar de normenreeks NEN-EN 50131 en andere relevante normen.	1 mei 2014	Norm
IEC62443	Wereldwijde norm voor de beveiliging van industrële automatisering en controle systemen (IACS systemen). Het IEC 62443 normenkader is voor de operationele technologie (OT), wat de ISO 27000 serie is voor de informatietechnologie (IT). De IEC ontwikkelt wereldwijde normen onder de vlag van de World Standards Cooperation, waar de ISO en	2019	Norm

	ITU lid van zijn.		
Wet beveiliging netwerk- en informatie systemen (Wbni)	Deze wet regelt een meldplicht van incidenten en een zorgplicht (treffen van beveiligingsmaatregelen). M.n. gericht op organisaties in vitale infrastructuren en digitale dienstverleners	9 november 2018	Wet
Wet computercriminaliteit III	Wet waarmee Justitie en politie nieuwe bevoegdheden krijgen om computercriminaliteit beter te bestrijden.	1 maart 2019	Wet
AVG	De Algemene verordening gegevensbescherming (AVG) is een privacywet die geldt in de hele Europese Unie (EU).	25 mei 2018	Wet

BIJLAGE 2: Vragenlijst diepte-interviews

Vragenlijsten t.b.v. project weerbaarheid alarminstallateurs

4 februari 2019 – Versie 0.1
Concept

Referentie : Vragenlijsten t.b.v. project weerbaarheid alarminstallateurs Techniek Nederland / OTIB

Inleiding

Voor het project weerbaarheid installateurs zullen een aantal interviews worden georganiseerd. Na deze interviews zal een enquête worden opgezet die over een bredere doelgroep kan worden verspreid om zo een goed beeld te krijgen van waar de installateurs staan, tegen welke problemen en uitdagingen ze aanlopen en op welke mogelijke manieren ze geholpen kunnen worden.
Om te voorkomen dat de enquêtes in een bepaalde richting worden geduwd, zijn de vragen die er toe doen zo ‘open’ als mogelijk gehouden. Bij het interview kan vervolgens bijlage 1 respectievelijk bijlage 2 gebruikt worden om diepgang in het gesprek te krijgen.
Voor alle partijen daarnaast is een aparte set van een kleine 20 vragen bijgevoegd dat een algemeen beeld geeft over de informatiebeveiliging.

Vragenlijst voor fabrikant, installateur (advies, realisatie en onderhoud) en PAC

1. In wat voor organisatie bent u werkzaam (meerdere antwoorden mogelijk)?
   - Fabrikant van alarm installaties of aanverwante apparatuur;
   - Advies en/of ontwerp van alarminstallaties (adviseert);
   - Installateur van alarminstallaties (realiseert);
   - Beheer en onderhoud van alarminstallaties (onderhoud);
   - Particuliere Alarm Centrale (PAC);
   - Afnemer/eindgebruiker van alarminstallaties.

2. Kunt u aangeven hoe groot uw organisatie is (in FTE)?
   - 1 tot 4 medewerkers;
   - 5 tot 10 medewerkers;
   - 11 tot 50 medewerkers;
   - 51 tot 100 medewerkers;
   - 101 tot 250 medewerkers;
   - Meer dan 250 medewerkers.

3. Wat is uw functie/rol binnen de organisatie (meerdere antwoorden mogelijk)?
   - Eindverantwoordelijke (directeur, management)
   - (advies bij) verkoop (verkoper, sales consultant, accountmanager etc.)
   - Consultant (monteur, technisch consultant etc.)
   - Overig, namelijk….

---

4. In hoeverre en op welke wijze krijgt u van eindklanten of installateurs vragen die betrekking hebben op informatiebeveiliging en/of de beveiliging van installaties?

5. In hoeverre vindt u dat u een ‘zorgplicht’ naar uw afnemers heeft t.a.v. informatiebeveiliging en op welke wijze geeft u hier invulling aan?

6. Welke maatregelen treft u t.a.v. de beveiliging van de alarminstallaties die door uw organisatie worden gemaakt, ontworpen, geplaatst en/of onderhouden?

7. Op welke wijze houdt u uw kennis rond informatiebeveiliging (in relatie tot alarminstallaties) up-to-date?

8. Op welke wijze gebruikt u richtlijnen en certificeringen zoals de ISO27001, IEC 62443, VRKI en de BORG / BRL6020?

9. Leven er bepaalde vragen omtrent informatiebeveiliging / cybersecurity van uw alarminstallaties en op welke wijze zou u hierin geholpen kunnen/willen worden?

Vragenlijst voor eindklanten

1. Kunt u aangeven hoe groot uw organisatie is (in FTE)?
   - 1 tot 4 medewerkers;
   - 5 tot 10 medewerkers;
   - 11 tot 50 medewerkers;
   - 51 tot 100 medewerkers;
   - 101 tot 250 medewerkers;
   - Meer dan 250 medewerkers.

2. Wat is uw functie/rol binnen de organisatie (meerdere antwoorden mogelijk)?
   - Eindverantwoordelijke bij aanschaftraject
   - Verantwoordelijke voor beheer van installatie
   - Eindgebruiker
   - Overig, namelijk….

---

3. In hoeverre en op welke wijze heeft u bij de aanschaf van uw alarminstallatie informatiebeveiliging en/of cybersecurity meegenomen?

4. Op welke wijze zorgt u ervoor dat alarmcodes, tags, sleutels en evt. andere middelen die gebruikt worden bij de alarminstallaties niet in verkeerde handen vallen (gedurende de gehele ‘life-cycle’ van deze middelen)?

5. Leven er bepaalde vragen omtrent informatiebeveiliging / cybersecurity van uw alarminstallaties en op welke wijze zou u hierin geholpen kunnen/willen worden?

Algemene vragen m.b.t. informatiebeveiliging (gericht op administratie en organisatie)

Organisatie

- Is er een persoon of afdeling duidelijk verantwoordelijk voor informatiebeveiliging?
- Heeft u met uw leveranciers/onderaannemers duidelijke afspraken gemaakt omtrent informatiebeveiliging en is e.e.a. vastgelegd en zo ja, op welke wijze?
- Krijgen medewerkers training op het moment dat ze in dienst komen m.b.t. informatiebeveiliging?
- In hoeverre heeft u standaards en procedures rond informatiebeveiliging gedocumenteerd/vastgelegd en hoe zorgt u er voor dat iedereen zich hieraan houdt?
- Heeft u documentatie van uw eigen IT omgeving
- Wat gebeurt er als een medewerker in dienst komt, van functie wijzigt of vertrekt (is er een duidelijke in- en uit-dienst procedure waarin aandacht is voor informatiebeveiliging)?
- In hoeverre heeft u een crisis- of incidentenplan binnen uw organisatie?
    - Weten medewerkers bij wie incidenten gemeld moeten worden?
    - Worden incidenten vastgelegd?
    - Wordt er na een incident onderzoek gedaan hoe het incident heeft kunnen ontstaan, hoe ernstig de gevolgen zijn en wat er gedaan kan worden om tot verbetering te komen?
    - In hoeverre wordt direct bekeken of een beveiligingsincident gemeld moet worden (bij instanties, klanten, leveranciers etc.)?

Technisch

- Op welke wijze heeft u deze laptops en/of andere systemen beveiligd (denk aan updates, antivirus, backup, encryptie, fysieke beveiliging etc.)?
- Mag er binnen uw organisatie gewerkt worden met mobiele/externe datadragers (USB sticks etc.) of cloudoplossingen zoals dropbox etc.?
- Op welke wijze heeft u de back-up en restore van uw eigen data geregeld? Is deze afgestemd op de eisen van uw organisatie (RPO/RTO)? In hoeverre controleert u met regelmaat de back-up van uw eigen data op juiste werking en volledigheid?
- In hoeverre worden alle acties die in de administratieve processen van de administraties worden uitgevoerd gelogd? Hoe wordt vervolgens omgegaan met de logbestanden?

Specifieke administratie van informatie die betrekking heeft op alarminstallaties

- Op welke wijze worden tekeningen, installatieschema's, documentatie, instellingen, alarmcodes etc. bewaard op laptops of andere systemen?
- Op welke wijze heeft u de AVG wetgeving geregeld, bijvoorbeeld t.o.v. camerasystemen die u adviseert, levert, installeert, onderhoud of gebruikt?

Budget

- Heeft u een apart budget voor informatiebeveiliging en kunt u aangeven hoe groot dit budget is in percentage van de omzet?
- In hoeverre is dit budget bepaald a.h.v. risico's die zijn onderkend binnen uw organisatie?
- Is dit budget op enigerlei wijze meegenomen bij het advies, installatie, onderhoud of afname van de alarminstallatie?

Verdieping bij vragen voor fabrikant, installateurs (advies, realisatie en onderhoud) en PAC

Leverancierskant (fabrikant, installateurs – advies, realisatie en onderhoud - en PAC)

4. In hoeverre en op welke wijze krijgt u van eindklanten of installateurs vragen die betrekking hebben op informatiebeveiliging en/of de beveiliging van installaties?

    - Kunt u bijvoorbeeld aangeven welke vragen u afgelopen periode hieromtrent heeft gekregen en wat hier vervolgens mee heeft gedaan?

5. In hoeverre vindt u dat u een 'zorgplicht' naar uw afnemers heeft t.a.v. informatiebeveiliging en op welke wijze geeft u hier invulling aan?

    - Wat doet u om hieraan te voldoen?
    - Heeft u een beveiligingsbeleid dat periodiek getoetst wordt?
    - Heeft u bijvoorbeeld een IEC 62443 en/of ISO27001 certificering?
    - Laat u uw organisatie regelmatig toetsen op informatiebeveiliging?

6. Welke maatregelen treft u t.a.v. de beveiliging van de alarminstallaties die door uw organisatie worden gemaakt, ontworpen, geplaatst en/of onderhouden?
   Denk hierbij aan:
    - Security/privacy by design?
    - In hoeverre stelt ú de eisen aan de apparatuur, verbindingen etc. die geadviseerd/gebruikt worden?
        - Welke eisen stelt u zoal?
    - Weet u waar de door u geproduceerde of geleverde systemen zich bevinden?
        - Hoe houdt u dit bij?
    - Heeft u goed inzichtelijk waar (gevoelige) gegevens van uw klanten of installaties zich bevinden?
        - Hoe krijgt u dit inzicht en op welke wijze houdt u dit bij?
    - Voert u risico-inventarisatie uit?
        - Op welke momenten doet u dit?
        - Op welke wijze bepaalt u de waarde van assets (bijvoorbeeld aanschafwaarde, boekwaarde, vervangingswaarde, rekening houden met data/informatie en reputatie/imago etc.)?
    - Hoe wordt omgegaan met gebruikersnamen en wachtwoorden?
        - Is er een hoofdwachtwoord?
            - Hoe wordt hier mee omgegaan?
            - Is het verplicht om dit Instellen bij oplevering (op enige wijze afgedwongen J/N)?
            - Is dit voor elke installatie gelijk?
            - Moet dit periodiek gewijzigd worden?
            - Hoe wordt e.e.a. vastgelegd en bijgehouden?
            - Wat gebeurt er bij vertrek van medewerkers?
        - Zijn er mogelijkheden tot meerweg authenticatie?
    - Op welke wijze vindt de instructie bij oplevering plaats?
        - Instructie bij oplevering aan alle medewerkers of 1 medewerker van eindklant?
        - Wijzen op potentiële risico's bij ingebruikname?
        - Wordt er bij oplevering een controle uitgevoerd op informatiebeveiliging (bijvoorbeeld verwijderen van gegevens, tekeningen etc. van systemen etc.)?
        - Op welke wijze worden evt. certificaten uitgereikt?
    - Op welke wijze vindt onderhoud en begeleiding na installatie plaats?
        - Op welke wijze wordt e.e.a. overgedragen naar andere afdelingen, klant of andere organisaties (bijv. PAC)?

        - Op welke wijze voert u dit uit (op afstand/lokaal, anders)?
        - Updaten van software van installaties?
            - Frequentie?
            - Door wie?
        - Worden er periodiek backups van installaties gemaakt?
            - Hoe wordt hier mee omgegaan (waar opgeslagen)?
        - Worden alle acties in de installaties gelogd?
            - Hoe wordt vervolgens omgegaan met de logs?
        - Worden er periodieke controles, bijvoorbeeld op gebruikers die niet meer bestaan of gebruikers die teveel rechten hebben, uitgevoerd?
        - Wordt er periodiek een controle van de technische beveiliging, bijvoorbeeld via een pentest, uitgevoerd?
    - Wat gebeurt er als een klant vertrekt?

7. Op welke wijze houdt u uw kennis rond informatiebeveiliging (in relatie tot alarminstallaties) up-to-date?
    - Vakbladen
    - Trainingen (intern of extern)
    - Begeleiding van externe consultants
    - Anders/overig….

8. Op welke wijze gebruikt u richtlijnen en certificeringen zoals de ISO27001, IEC 62443, VRKI en de BORG / BRL6020?

    - Hoe goed werkt dit? Mist u bepaalde aspecten? Wat doet u meer/minder/anders t.o.v. deze richtlijnen? Zijn er andere richtlijnen die u gebruikt?

9. Leven er bepaalde vragen omtrent informatiebeveiliging / cybersecurity van uw alarminstallaties en op welke wijze zou u hierin geholpen kunnen/willen worden?

Verdieping bij vragen voor eindklanten

Afname (eindgebruiker)

3. In hoeverre heeft u bij de aanschaf van uw alarminstallatie informatiebeveiliging en/of cybersecurity meegenomen?
    a. Welke vragen heeft u hieromtrent gesteld?
    b. Alleen gericht op de installatie zelf of ook op de organisatie van de leverancier, installateur en/of onderhoudspartijen?
    c. Op welke wijze heeft dit meegewogen in de beoordeling bij aanschaf?
    d. Heeft u e.e.a. ook gecontroleerd?

4. Op welke wijze zorgt u ervoor dat alarmcodes, tags, sleutels en evt. andere middelen die gebruikt worden bij de alarminstallaties niet in verkeerde handen vallen (gedurende de gehele ‘life-cycle’ van deze middelen)?
    a. Zijn er standaard procedures voor in-dienst, uit-dienst, wijzig functie?
    b. Wordt e.e.a. vastgelegd in een logboek?
    c. Op welke wijze worden de codes en informatie rond uitgegeven ‘assets’ bewaard (en vernietigd)?
    d. Controleert u met enige regelmaat de instellingen van de installaties (bijvoorbeeld op gebruikers die niet meer bestaan of gebruikers die teveel rechten hebben)?
    e. Doet u dit in overleg met uw installateur/onderhoudsorganisatie?
    f. Wat gebeurt er met de uitkomsten?
    g. Bent u weleens verhuisd en zo ja, wat is er toen gedaan om het gebruik van de alarminstallatie af te sluiten?

5. Leven er bepaalde vragen omtrent informatiebeveiliging van uw alarminstallaties en op welke wijze zou u hierin geholpen kunnen/willen worden?

BIJLAGE 3: Aanbevelingen

Relatie Installateur – Eindklant

Resultaat diepte-interview

Onderwerp	Onze bevinding (in algemeenheid)
Vragen van eindklanten over de wijze waarop de installateur de beveiliging omgaat met informatiebeveiliging	De vraag komt nog beperkt vanuit de markt. Bij grotere trajecten (bijvoorbeeld aanbestedingen) wordt e.e.a. wel meegenomen, maar m.n. bij particulieren en MKB organisaties is er vrijwel geen vraag en lijkt de keuze vooral bepaald te worden door prijs en reputatie. Reputatie wordt versterkt doordat installateurs in hun uitingen het lidmaatschap van brancheverenigingen (m.n. VEB, VEBON-NOVB en Techniek Nederland) en evt. VEB/BORG-certificering gebruiken. Aan de andere kant lijken eindklanten zich onvoldoende bewust van het verschil van een VEB/BORG- en niet VEB/BORG-gecertificeerd installateur omdat in het lagere segment ook weinig naar deze certificering wordt gevraagd.
Bewustzijn bij eindklanten	Eindklanten lijken zich onvoldoende bewust van de (online) gevaren die digitalisering met zich hebben meegenomen. Met name voor het werken met apps en draadloze netwerken zou het bewustzijn omhoog kunnen cq moeten.

Enkele citaten uit diepte-interviews

...Bij bestek / aanbesteding bij grotere (overheids-) opdrachten levert opdrachtgever veelal tekeningen met exacte verwachtingen aan. Hier ligt juist een risico...

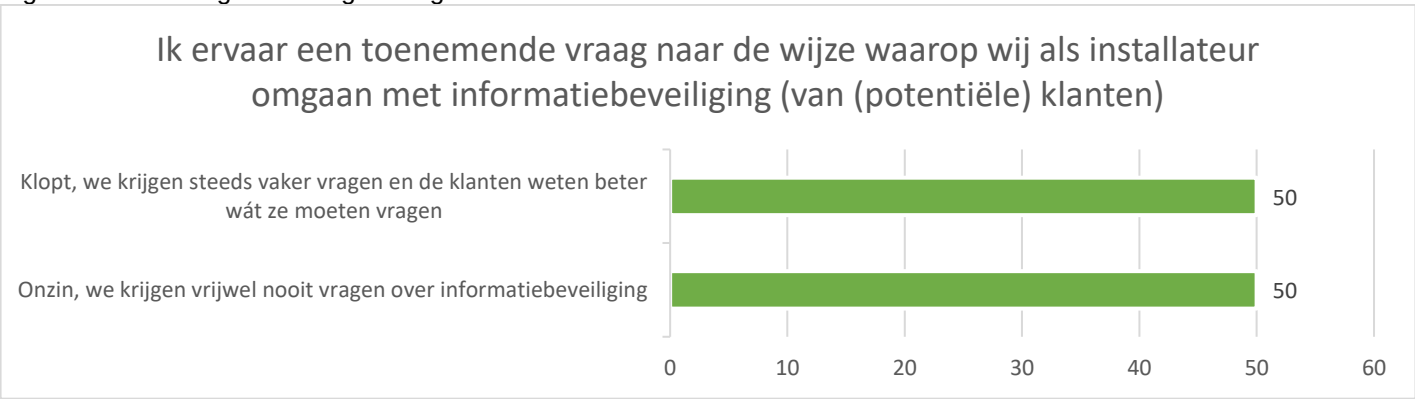
...Klant / particulier bepaalt op welke plaats de sensoren worden geplaatst...

...Apps van de installaties worden zonder toegangscodes op telefoons geplaatst. Hierdoor is het mogelijk om een centrale uit te schakelen op het moment dat je je BUITEN het beveiligd gebied van de centrale bevindt...

...Pasjes met codes liggen op de alarmcentrale...

...Er is alleen een tag nodig om een installatie uit te schakelen. Als de tag dus verloren of gestolen raakt kan een kwaadwillende zo naar binnen...

Ingebrachte stelling ledenvergadering



Onze aanbeveling(en)

1.	Zorg er voor dat klanten bewuster omgaan met informatiebeveiliging en bij projecten dus ook meer gaan vragen over de informatiebeveiliging is geregeld. De betere installateurs kunnen zich hierdoor ook beter profileren en onderscheiden.
2.	Andere mogelijkheid is om informatiebeveiliging (nog) meer onderdeel uit te laten maken van de VEB/BORG en VRKI certificering en in de markt duidelijker te communiceren wat de voordelen zijn van het werken met een gecertificeerd installateur.

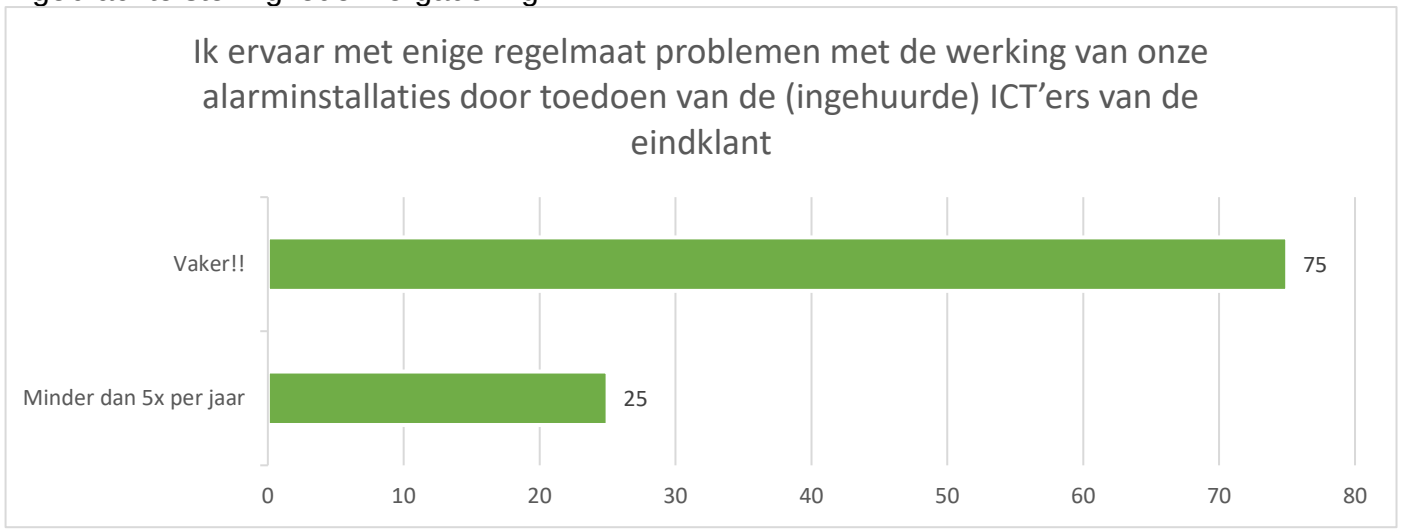
Relatie Installateur – ICT beheerder

Onderwerp	Onze bevinding (in algemeenheid)
Afstemming met ICT beheerders	De relatie met (externe) ICT afdelingen van opdrachtgever is belangrijk bij het openzetten van poorten op firewall/router systemen, aanmaken van netwerksegmenten op switches, draadloze netwerken t.b.v. camera systemen, VPN verbindingen om in te kunnen loggen op afstand, gebruik noodstroomvoorziening op netwerkapparatuur etc. etc. De wijze waarop de wensen/eisen met ICT beheerders wordt afgestemd is echter veelal niet gestandaardiseerd en gebeurt bovendien niet altijd op een goed beveiligde manier (bijvoorbeeld via E-mail). Gevolg is dat voor partijen niet duidelijk is wat er van elkaar wordt verwacht, wat beveiligingsrisico's kan opleveren.

Citaat uit diepte-interviews

... ICT partij verwijderd de UPS waar modem en/of switch op is aangesloten of controleert deze niet periodiek op juiste werking. Gevolg is dat bij een stroomstoring de installatie geen meldingen richting PAC kan doen...

Ingebrachte stelling ledenvergadering



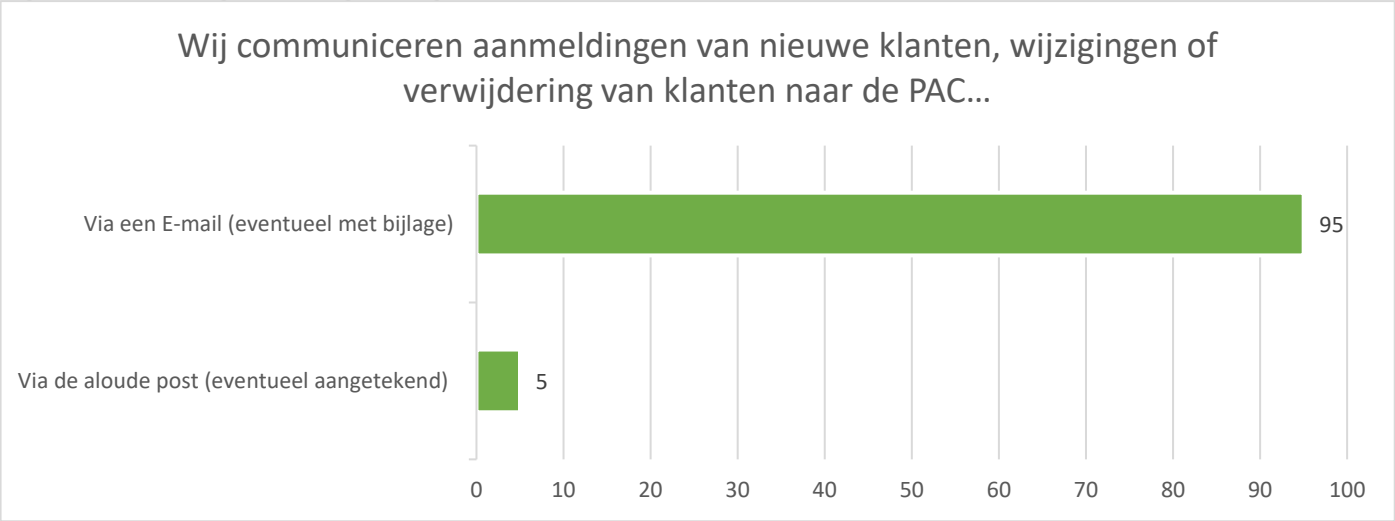
Onze aanbeveling(en)

1.	Zorg er voor dat afstemming tussen installateur en ICT beheerders meer gestandaardiseerd verloopt en dat ICT beheerders bewuster omgaan met de informatiebeveiliging van alarminstallaties. De juiste werking van installaties is sterk afhankelijk van hun werkzaamheden.

Relatie Installateur – PAC

Onderwerp	Onze bevinding (in algemeenheid)
Afstemming met PAC	De wijze van overdracht van informatie van installateur richting PAC verloopt veelal niet gestandaardiseerd. Er zijn PAC's die apps hebben ontwikkeld, waardoor monteurs eenvoudiger bij installaties kunnen komen voor het onderhoud. Deze apps geven in gebruik ook weer beveiligingsrisico's waar rekening mee gehouden dient te worden.

Ingebrachte stelling ledenvergadering



Onze aanbeveling(en)

1.	Zorg voor een gestandaardiseerde overdracht tussen installateur en PAC, die bij voorkeur via een digitaal portaal verloopt. Ook het plaatsen van een centrale in testmodus zou gedigitaliseerd kunnen/moeten (?) verlopen met duidelijke eisen t.a.v. autorisatie en authenticatie.
2.	Voor het gebruik van Apps dienen – zeker door monteurs – de juiste beveiligingsvoorschriften te worden gebruikt.

Enkele citaten uit diepte-interviews

…Gegevens worden via E-mail in een Excel bestand van installateur naar PAC gestuurd (incl. gegevens eindklant, pasnummers, promnummer etc.)…

…Apps worden zonder toegangscode of 2-weg authenticatie op telefoons van monteurs geïnstalleerd. Als de telefoon 'open' staat kun je dus eenvoudig bij alle centrales/installaties van klanten komen…

Opmerkingen bij de ledenvergadering

Er zou een extra optie bij moeten komen, "Via een inlog een portal bij de PAC"
Via de post = niet te hacken, dus het meest veilig?

Relatie Installateur – leverancier / fabrikant

Onderwerp	Onze bevinding (in algemeenheid)
Afstemming met leverancier / fabrikant	Fabrikanten voelen zich verantwoordelijk voor het veilig aanleveren en houden van hun apparatuur. Om bijvoorbeeld wijzigingen in de installaties (bijvoorbeeld firmware updates etc.) uit te voeren is er een sterke afhankelijkheid van de installateur. Indien de dienstverlening van installateurs onvoldoende is dan kan dit negatieve impact hebben op de fabrikant. Daardoor is een dreiging voor de kleinere installateurs dat fabrikanten/importeurs meer de regie naar zich zullen toetrekken en zullen gaan samenwerken met een aantal grotere spelers (waardoor ze ook minder afhankelijk zijn van de kwaliteit van een individuele installateur). Oplossingen waarbij niet alleen het product wordt geleverd, maar een totaaloplossing. Dit laatste kan grote invloed hebben op de rol van de installateur. De fabrikant weet veelal niet goed waar installaties zijn geplaatst. Installateurs hebben op hun beurt moeite om een lijst op te leveren van een bepaald type installatie met een bepaalde versie firmware. Hierdoor kan de support onvoldoende zijn op het moment dat er in een kort tijdsbestek kritische updates moeten worden geïnstalleerd. Uit de interviews is gebleken dat de meeste installateurs alleen updates van firmware uitvoeren tijdens het jaarlijkse onderhoud (sommige installateurs nemen de firmware updates niet mee in het jaarlijks onderhoud of kiezen er voor om updates helemaal niet te installeren in verband met mogelijke problemen in de werking van de installatie na installatie van een update). Het niet installeren van laatste firmware kan forse risico's met zich meebrengen t.a.v. informatiebeveiliging.
Security by design / default van installaties en apparatuur	Er is een toenemende aandacht voor informatiebeveiliging in de alarmcentrales die worden geleverd. In combinatie met het IP protocol kunnen nog wel verbeteringen worden doorgevoerd. Leveranciers zijn steeds meer bezig met security by design/default. Hierdoor worden gebruikers verplicht om bijvoorbeeld bij de eerste keer inloggen een wachtwoord te wijzigen. Dit is echter zeker nog niet bij alle apparatuur het geval waardoor er toch altijd een menselijke factor blijft.

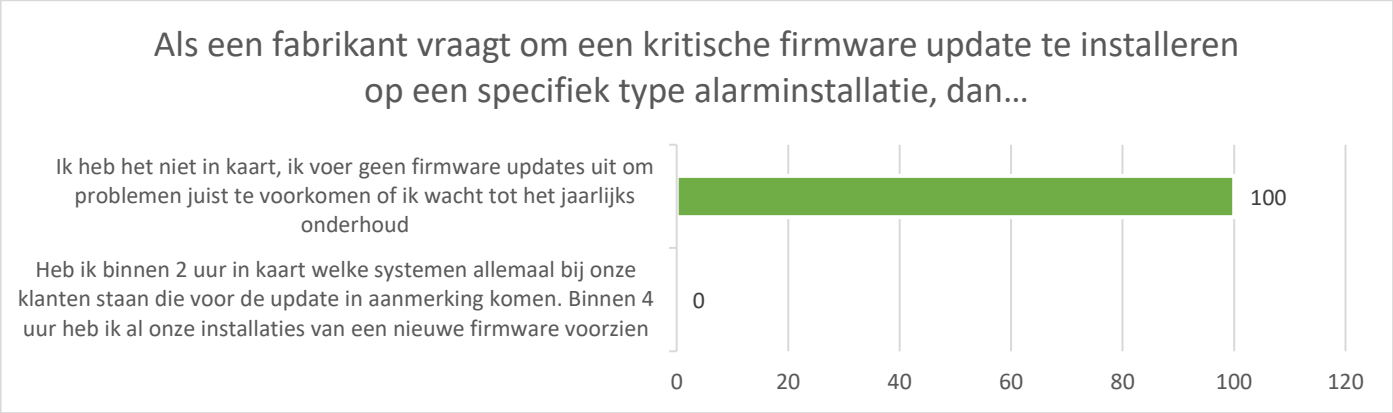
Enkele citaten uit diepte-interviews

…Bij beveiligingslekken waarschuwt de fabrikant de installateur om het beveiligingslek te repareren. Mocht de installateur in gebreke blijven dan krijgt de installateur een x aantal waarschuwingen. Als de installateur dan nog in gebreke blijft, dan trekt de fabrikant haar verantwoordelijkheid terug…

….er is bijvoorbeeld geen automatische 'one-touch provisioning' mogelijk en WAN IP nummers komen niet op een blacklist na x foutieve inlogpogingen….

…Bij grotere organisaties kun je met een PIN code van 4 cijfers tegen de grenzen aanlopen. Bij een organisatie van bijvoorbeeld 250 personen is 1 op de 4 codes juist…

Ingebrachte stelling ledenvergadering



Onze aanbeveling(en)

1.	Ideaal loopt het proces tussen uitlevering van installaties tussen fabrikant, installateur, netwerkbeheerder, PAC en eindklant digitaal. Zo weten alle partijen welke maatregelen zijn getroffen en kan de kwaliteit in de gehele keten verbeterd worden.
2.	Als dit ondoenlijk is, kunnen fabrikanten meer gaan eisen dat centrales geregistreerd worden (bij voorbeeld in het kader van fabrieksgarantie) zodat bekend is waar de installaties zich bevinden en welke installateur e.e.a. heeft aangelegd.
3.	Security en privacy by design/default moet een verplichting zijn/worden voor alle alarminstallaties die op de markt worden gebracht. Er zal nader onderzoek moeten worden gedaan in hoeverre fabrikanten hiertoe op dit moment verplicht zijn en welke verplichtingen daar op dit moment voor gelden.

Opmerkingen bij de ledenvergadering

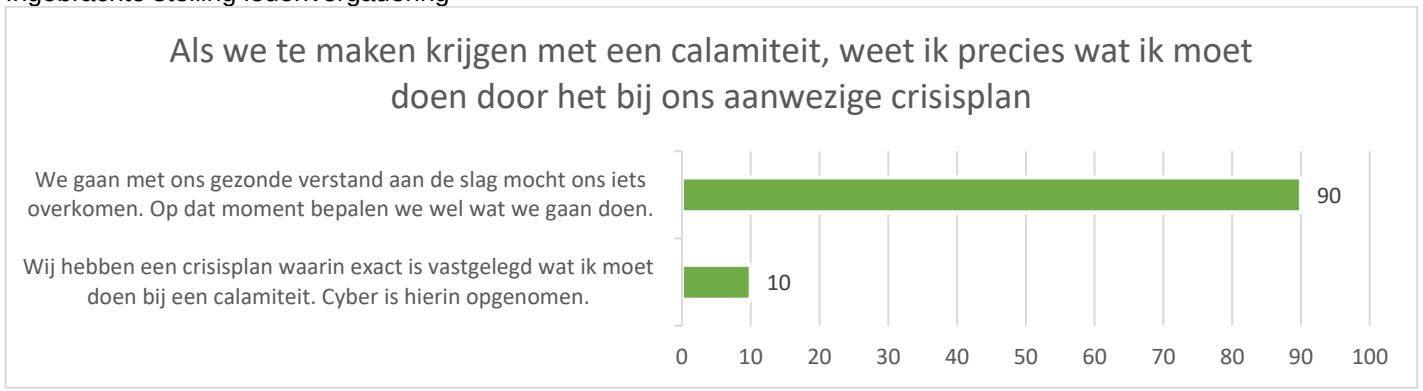
Updates van de fabrikanten zijn vaak inhoudelijk niet juist

Merk/type weten installateurs vaak wel, maar niet versie/serienummer van installaties

Interne organisatie van de installateur

Onderwerp	Onze bevinding (in algemeenheid)
Informatiebeveiliging interne organisatie	Over het algemeen zien we een groot verschil in volwassenheid op het gebied van informatiebeveiliging, afhankelijk van de installateur. Dit verschil wordt m.n. bepaald door de klantengroep die bediend wordt, of het adviseren, plaatsen en onderhouden full-time business is (of er bij wordt gedaan) en hoe groot de organisatie van de installateur is (hoe meer klanten afhankelijk zijn van informatiebeveiliging en hoe groter de installateur, hoe groter het bewustzijn rond informatiebeveiliging). Grotere installateurs zijn ISO27001 gecertificeerd, daarmee bezig of hebben bewust keuzes gemaakt om daar nog niet aan te voldoen. Bij kleinere organisaties zien we dat informatiebeveiliging nog veelal in CMM-level 1 tot 3 bevindt (dat dingen ad-hoc gebeuren, dat niet veel beschreven is – geen beleid, procedures, incidentenplan of continuïteitsplan) en dat er duidelijke verbeteringen kunnen worden doorgevoerd. Vrijwel alle partijen die we hebben geïnterviewd hebben hun processen inmiddels geheel of grotendeels gedigitaliseerd. Monteurs werken met tablets of laptops waarmee ze verbinding kunnen maken met het netwerk of waarop ook informatie wordt opgeslagen. Informatie die wordt opgeslagen – zoals tekeningen, configuratiebestanden en back-ups van de installaties etc. etc. worden op het netwerk van de installateur opgeslagen, waarmee deze netwerken extra aantrekkelijk worden voor gerichte aanvallen.
Incidenten en crisisplan	Bij de meeste installateurs is geen – of een zeer beperkt - crisisplan aanwezig. Gevolg is dat bij een hack op bijvoorbeeld het interne netwerk van de installateur niet bekend is welke stappen er genomen moeten worden en dat het bewustzijn over wat er allemaal bij een komt kijken onvoldoende is.

Ingebrachte stelling ledenvergadering



Enkele citaten uit diepte-interviews

… Laptops monteurs zijn niet versleuteld. Beleid is dat er zo min mogelijk data op deze systemen komt te staan, maar of dat ook werkelijk gebeurt is de vraag. Er wordt gewerkt met een bepaalde versie van antivirus, maar deze verstoort het proces regelmatig, waardoor hij af en toe wordt uitgezet…

…Meerweg authenticatie wordt niet ingezet (in de vorm dat je iets moet hebben/weten), maar er moeten wel diverse verschillende wachtwoorden worden ingegeven voordat je bij systemen kunt komen (om bijvoorbeeld bij back-up bestanden van installaties te komen moet je eerst inloggen op een werkplek, daarna een VPN opzetten met wachtwoord, daarna inloggen op de PC die daarvoor aanwezig is, daarna een shell opstarten en vervolgens is een code van de klant nodig)…

…Tijdelijk kan het zijn dat tekeningen, codes etc. worden uitgeprint of opgeschreven. Veelal is het bewustzijn aanwezig om na projecten deze informatie te vernietigen…

…Er is geen crisisplan. Wel een keer te maken gehad met ransomware…

…Bij een inbraak/incident worden we er wel bij geroepen om te kijken waarom het alarm niet is afgegaan of om het systeem uit te lezen. Het komt nogal eens voor dat de detector door de klant is afgeplakt…

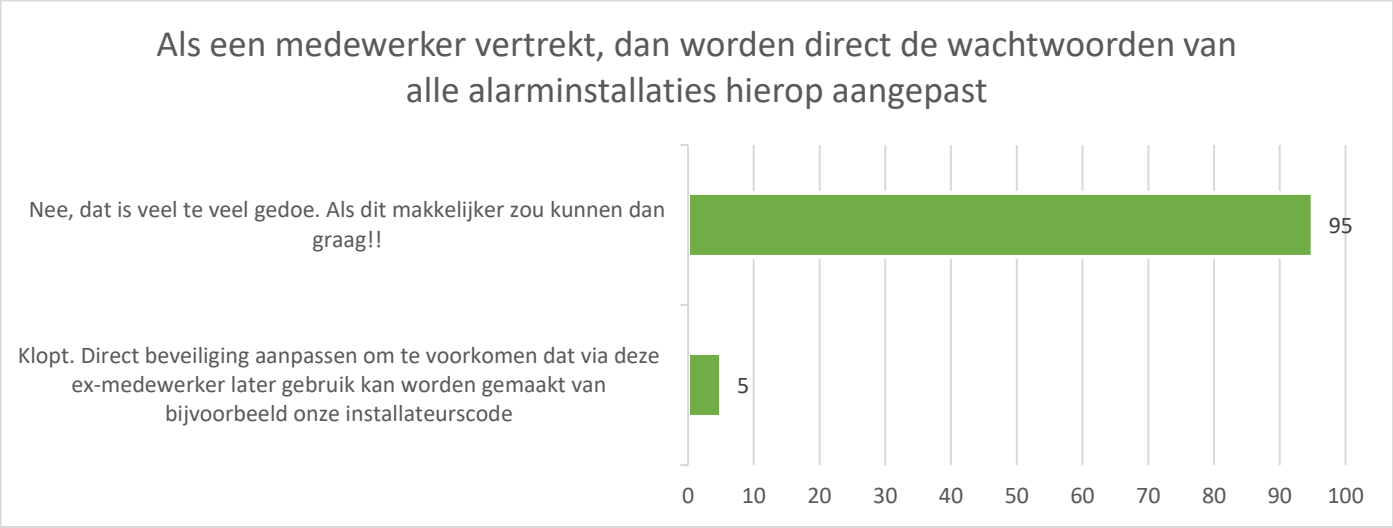
Onze aanbeveling(en)

1.	In de VEB- en BORG regeling wordt m.n. gekeken naar de wijze waarop installaties opgeleverd moeten worden. In onze optiek zou informatiebeveiliging van de organisatie van de installateur (inclusief beleid, medewerkers, techniek, procedures etc.) in deze regelingen meer/prominenter meegenomen kunnen/moeten worden
2.	Het is wenselijk dat er standaardisatie komt inclusief duidelijke procedures (die gebruiksvriendelijk zijn voor zowel eindklant als monteur). Deze moeten voor kleinere installateurs minder zwaar zijn dan de eisen/richtlijnen uit de ISO2700x, maar zwaarder dan wat nu gebruikt wordt en ingaan op zowel beleid/organisatie, techniek als menselijk handelen/bewustzijn.
3.	Ondersteun installateurs in het opzetten van een crisisplan zodat áls er in de branche iets fout gaat, bedrijven ook weten wat ze moeten doen.
4.	In workshops kan ook eens nagespeeld worden wat er allemaal bij een crisis komt kijken. Dit gaat veel verder dan techniek en gaat ook verder dan alleen de installateur (ook een PAC, fabrikant of klant kan te maken krijgen met vormen van cybercriminaliteit die impact heeft op de installateur).

Gebruik van wachtwoorden

Onderwerp	Onze bevinding (in algemeenheid)
Wachtwoorden van installaties	De omgang met wachtwoorden wordt voor installateurs als lastig ervaren. Veelal wordt er 1 installateurscode gebruikt voor alle installaties. Andere installateurs zijn wat verder en gebruiken geautomatiseerde tooling voor het beheren van verschillende wachtwoorden (wachtwoordmanagers). Belangrijkste bij dit punt is natuurlijk dat hier een grote afhankelijkheid van medewerkers ligt. Als ze kwaadaardige intenties hebben, kunnen ze altijd codes van installaties achterhouden. Zie ook 'Medewerkers installateur'. Overigens is het werken met wachtwoorden hier nader toegelicht, maar kunnen ook voor het werken met verbindingen en firewalls van klanten/derden, het werken met draadloze verbindingen, het werken met Apps etc. etc. dit soort aanbevelingen worden gemaakt.

Ingebrachte stelling ledenvergadering



Onze aanbeveling(en)

1.	Zorg voor een duidelijke levenscyclus van wachtwoorden van installaties van klanten (van aanmaak tot vast en incidenteel onderhoud en beëindiging van de relatie met klant/medewerkers). Hierbij zal gekeken moeten worden naar juiste autorisatie (rechten) en authenticatie (identificatie). M.n. voor kleinere installateurs denken we dat het handig is om hier bepaalde tooling voor aan te leveren cq ze te wijzen op tooling die in de markt voorhanden is.

Enkele citaten uit diepte-interviews

...Er wordt 1 wachtwoord voor alle installaties gebruikt...
...Dit wordt gedaan middels een installateurstool voor aangesloten systemen. De tool kan de code periodiek aanpassen of als medewerkers weggaan. Hierop wordt in trainingen gewezen...
...Alleen bij hogere beveiligingseisen (m.n. grotere klanten) kan er pas worden ingelogd nádat de klant zijn code heeft ingegeven of de PAC de installatie in test-modus heeft gezet...
...Binnen de organisatie zijn afspraken gemaakt, zoals het niet noteren van codes van klanten, een manier om met wachtwoorden te werken waarbij elke klant toch een uniek wachtwoord heeft. Standaard wachtwoorden worden direct gewijzigd etc...
...Geïnterviewde weet dat andere installateurs veel minder veilig werken en bijvoorbeeld 1 code hanteren voor alle centrales. Hij kent zelfs een aantal van deze codes van concurrenten...

Opmerkingen bij de ledenvergadering

Er is een verschil tussen programmeercodes installateur en gebruikerscodes

Geheimhoudingsverklaring medewerker gebruiken

Medewerkers van de installateur

Onderwerp	Onze bevinding (in algemeenheid)
Onderaannemers	Bij de geïnterviewde personen wordt er zelden gewerkt met onderaannemers. In de gevallen dat het gebeurt wordt de uiteindelijke inbedrijfstelling over het algemeen door de installateur uitgevoerd.
Kennisopbouw	Kennisopbouw bij medewerkers vindt over het algemeen plaats door zelfstudie (zelf ook uitzoeken) en producttrainingen van fabrikanten. Het belang van de ICT component lijkt in de opleidingen op dit moment onvoldoende aanwezig. Er zijn geen trainingen gericht op informatiebeveiliging of je moet naar ISO2700x trainingen gaan. Over het algemeen zijn de producttrainingen opgezet ter ondersteuning van het product en wordt algemene kennis rond informatiebeveiliging gemist. M.n. bij oudere medewerkers is er weinig cursusmateriaal of begeleiding aanwezig om ze te instrueren t.a.v. de digitale informatie/netwerken. Bij jongere medewerkers wordt er al steeds meer aandacht voor gegeven in de opleidingen, al wordt er ook aangegeven dat de eindtermen nog te weinig kennis rond digitale netwerken (IP-gebaseerd) bevatten.
In dienst	Alle installateurs die we hebben geïnterviewd vragen een verklaring van vertrouwelijkheid aan bij de politie bij in-dienst treden (deze gaat verder dan een VOG verklaring). Hiernaast is er in het arbeidscontract / personeelshandboek de nodige artikelen voor geheimhouding, boetebeding etc. De afhankelijkheid – m.n. bij kleinere installateurs – van ethisch werkende medewerkers is enorm groot. Er blijft altijd een risico dat monteurs geïntimideerd of verleid worden om codes of informatie af te staan.
Uit dienst	Bij het uit dienst treden worden veelal mondelinge/schriftelijke verwijzingen gemaakt naar de artikelen rond geheimhouding dit bij het in-dienst treden zijn aangegaan. Bij kleinere installateurs worden verder geen wijzigingen doorgevoerd in installateurscodes etc. (wel worden sleutels/pasjes ingeleverd, wordt een evt. VPN afgesloten en wordt de laptop ingenomen).

Enkele citaten uit diepte-interviews

...Er wordt bij de arbeids-overeenkomsten duidelijk afgesproken wat wordt verwacht omtrent geheimhouding etc...

...Nieuwe medewerkers worden veelal in het diepe gegooid en krijgen direct toegang tot de systemen en daarmee alle wachtwoorden, codes etc...

...Veel aspecten omtrent Cyber Security en (informatie)beveiliging zijn terug te voeren op het gedrag van de mens in plaats van de techniek. Hier zou meer aandacht voor moeten zijn...

...Kennisopbouw gebeurt door beursbezoeken, lectuur en informatie vanuit leveranciers...

...Er komt wel informatie van leveranciers, maar dit is niet vanuit een cyber security oogpunt. Cursussen/trainingen die raakvlakken hebben met cyber security worden wel door leveranciers verzorgd...

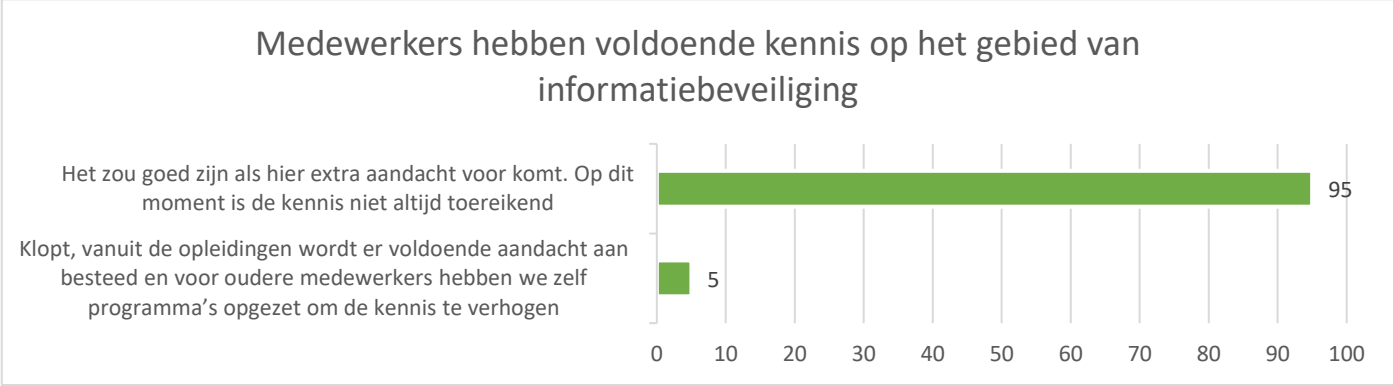
...Bij uit-dienst wordt door de advocaat apart een brief gestuurd waarin de afspraken nog eens op papier worden gezet rond geheimhouding etc...

...Op het moment dat iemand uit dienst gaat wordt de toegang tot de VPN ontnomen...

Opmerkingen bij de ledenvergadering

- Zowel bij oudere medewerkers als instromers schiet de kennis rond informatiebeveiliging te kort
- Meer opleiden voor algemene kennis over installaties over IP - IOT, hoeft niet specifiek over beveiliging te gaan
- Technische specificaties komen gedetailleerd van opdrachtgevers: die zou je moeten kunnen toepassen
- Opleiding MBV (??) schiet te kort (m.n. meer praktijk opnmemen en het niet te theorethisch maken).

Ingebrachte stelling ledenvergadering



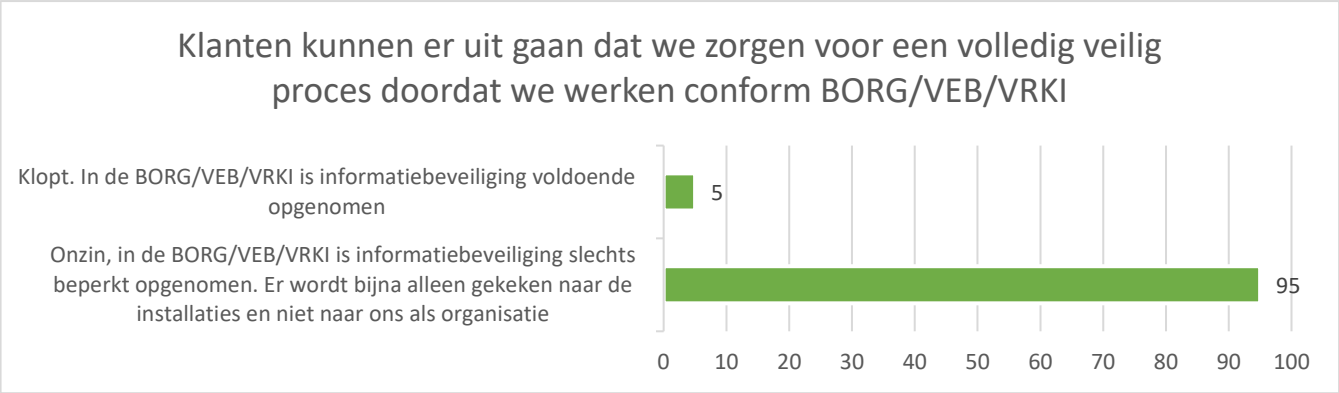
Onze aanbeveling(en)

1.	Bekijk in hoeverre het mogelijk is om training op te zetten rond informatiebeveiliging. In onze optiek zou dit zich enerzijds moeten richten op de installaties die opgeleverd worden, maar anderzijds ook heel duidelijk gericht op de interne organisatie van de installateur (informatiebeveiliging op de KA omgeving). Controleer verder in hoeverre in de eindtermen informatiebeveiliging in voldoende mate is opgenomen.
2.	Het is wenselijk dat er standaardisatie komt inclusief duidelijke procedures. Deze moeten voor kleinere installateurs minder zwaar zijn dan de eisen/richtlijnen uit de ISO2700x, maar zwaarder dan wat nu gebruikt wordt en ingaan op zowel beleid/organisatie, techniek als menselijk handelen/bewustzijn. Een in-dienst, wijzig functie en uit-dienst procedure horen hier nadrukkelijk bij.

Certificeringen

Onderwerp	Onze bevinding (in algemeenheid)
certificeringen	Installateurs die wij hebben geïnterviewd zijn BORG gecertificeerd en werken volgens de VRKI richtlijnen. Daarnaast wordt er regelmatig gewerkt conform ISO 9001 (algemene kwaliteitsnormering). Grotere installateurs zijn bekend met of werken volgens ISO2700x. Vanuit de interviews wordt aangegeven dat de BORG regeling afgelopen jaren is verzwakt, waardoor het eenvoudiger is om aan de eisen te voldoen. In de VEB en BORG regelingen is informatiebeveiliging slechts beperkt opgenomen.

Ingebrachte stelling ledenvergadering



Onze aanbeveling(en)

1.	Neem informatiebeveiliging (nog meer) op in zowel de VEB, BORG als de VRKI. Dit zal zich zowel op de projecten en het onderhoud van de alarminstallaties als de interne organisatie – incl. omgang van digitale gegevens – moeten toespitsen.

Opmerkingen bij de ledenvergadering

- Relatie opdrachtgever – installateur – verzekeraar: wie is waar voor verantwoordelijk en levert wat?

Enkele citaten uit diepte-interviews

… CP komt voor het middensegment uit met de VRKI; wordt als te summier gezien om klanten goed te kunnen bedienen. Organisatorische zaken worden gemist…

…in de 30 jaar dat geïnterviewde werkt als installateur heeft zich slechts 1x een BORG controle plaatsgevonden…

…Richtlijnen van de BORG zijn in de praktijk veelal niet haalbaar (m.n. de eisen aan medewerkers)…

…Sommige verzekeraars verzekeren zonder dat er een BORG gecertificeerde centrale is opgeleverd…

…Er is vrijwel geen handhaving en/of controle omtrent BORG gecertificeerde installateurs en installaties. Als er een controle is, dan kan de installateur zélf aangeven welke installaties gecontroleerd moeten worden…

…Het is te eenvoudig om zich staande te houden als installateur. Er zijn te weinig prikkels om beter werk te leveren, uitzonderingen daargelaten. Zolang er geen 'rode kaart' getrokken wordt richting onvoldoende presterende installateurs zal er volgens ondervraagde niet veel veranderen…

…BORG certificaten van de opgeleverde installatie worden alleen uitgegeven als de klant daarom vraagt. Dit heeft er ook mee te maken dat installateurs over het algemeen niet verantwoordelijk zijn voor het bouwkundige deel (dit onderdeel is verplicht voor BORG certificering)…

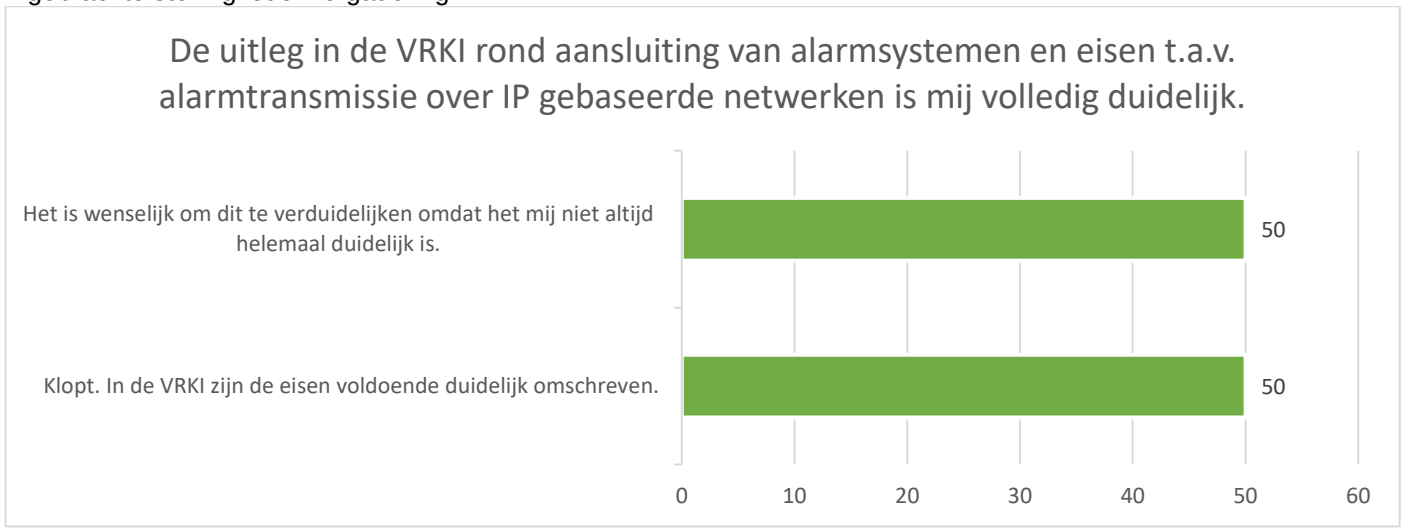
Advies en plaatsing van installaties bij klanten

Onderwerp	Onze bevinding (in algemeenheid)
Risico beoordeling	Over het algemeen vindt risico classificatie plaats conform VRKI. Bij grotere omgevingen volstaat de VRKI niet en wordt in samenspraak met partijen (m.n. verzekeraar, klant en installateur) bepaald aan welke eisen de installatie moet voldoen.
Eisen	Op basis van de risico beoordeling wordt bepaald welke maatregelen worden getroffen t.a.v. informatiebeveiliging. In onze optiek worden er in de VRKI slechts beperkte eisen gesteld die betrekking hebben op informatiebeveiliging. De werking van het internet is voor IP gebaseerde installaties enorm groot.
Oplevering van projecten en uitleg aan eindklant	Instructie aan eindklanten gebeurt veelal mondeling door de monteur, tezamen met het invullen van het opleverdocument. Doordat de installaties per situatie verschillen zijn de handleidingen die worden overgedragen in de meeste gevallen de algemene handleidingen van de installaties (vanuit de fabrikant). De eindklant zal deze zelf moeten vertalen naar gebruikers handleidingen. Vooral bij kleinere installaties vindt geen onafhankelijke controle plaats door een derde persoon (op juiste werking en informatiebeveiliging). Bij oplevering van camera systemen wordt in veel gevallen onvoldoende uitleg gegeven aan de eindklant over de relatie van installatie tot zijn rechten en verplichtingen i.v.m. de aangescherpte wetgeving (AVG).
Vertrek van een klant	Op het moment dat een klant vertrekt wordt de installateurscode gewijzigd naar de default instelling en aangeleverd aan de klant, zodat hij deze kan afstemmen met de nieuwe installateur. Het dossier met tekeningen, back-ups van installaties, evt. andere codes etc. blijven veelal op het bedrijfsnetwerk van de installateur aanwezig.

Enkele citaten uit diepte-interviews

... Single- of dual path verbinding wordt bepaald a.h.v. VRKI (ter voorkoming van evt. DDoS aanvallen)...
...Installaties worden zo opgezet dat werken met VPN tunneling en whitelisting van IP nummers verplicht is...
... data gaat alleen als 'outbound- verkeer' vanuit de centrale naar PAC/Organisatie. Bij hogere beveiligings-eisen worden dedicated verbindingen gebruikt...
...IP gebaseerde centrales worden niet altijd 'gepolled', of dit vindt slechts 1x per 24 uur plaats. Bij centrales waarbij geen 2e verbinding is wordt hierbij een beveiligings-risico gelopen op het moment dat verbindingen wegvallen...
...Het is op dit moment moeilijk voor een installateur in te schatten hoe hackersproof een installatie is...
...Slechts 1 medewerker bij eindklant is op de hoogte van de werking van de installatie...
...Er is geen duidelijke procedure of uitleg over de wijze waarop de eindklant juist en veilig moet omgaan met codes ...
... Er is eigenlijk geen uitleg over verwerking van data (bijvoorbeeld bewaartermijnen) van geplaatste camera systemen....
...Dossiers, back-ups van installaties etc. blijven nog lange tijd aanwezig op het netwerk van de installateur...

Ingebrachte stelling ledenvergadering



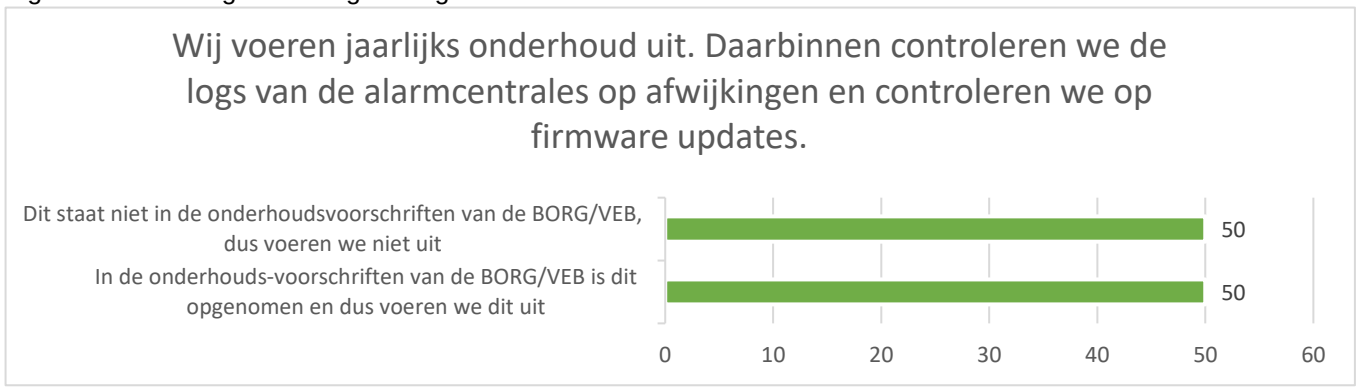
Onze aanbeveling(en)

1.	In de risico-inventarisaties wordt m.n. gekeken naar de fysieke waarde van spullen. Er wordt zover bekend geen rekening gehouden met bijvoorbeeld de waarde van data. In onze optiek zou dit opgenomen moeten worden in de VRKI.
2.	Zet in de VRKI een aantal eisen op t.a.v. informatiebeveiliging, bijvoorbeeld gericht op DDoS aanvallen, hacking van installaties etc. Inmiddels is in de VRKI wel een hoofdstuk opgenomen omtrent alarmtransmissie. Verder onderzocht moet worden in hoeverre de verbindingen t.b.v. onderhoud zijn opgenomen – of opgenomen moeten worden – in de VRKI.
3.	Zeker bij middelgrote installaties kan een kwaliteitsslag gemaakt worden door de oplevering – en controle op juiste werking + informatiebeveiliging – door een andere persoon te laten plaatsvinden cq een verplichte audit te laten uitvoeren. Dit is nu (nog) geen onderdeel van de VEB- en BORG regeling.
4.	T.a.v. het werken met camera systemen in relatie tot de AVG kan er een aparte flyer of document opgezet worden, zodat de eindklant i.s.m. zijn installateur hier ook eenvoudig naar kan handelen.
5.	Zorg voor een duidelijke procedure omtrent de wijze waarop afscheid genomen wordt van een klant en welke verplichtingen dan gelden t.a.v. het behouden van dossierinformatie (o.a. bewaartermijnen, omgang met back-ups van installaties etc.).

Onderhoud van installaties bij klanten

Onderwerp	Onze bevinding (in algemeenheid)
Onderhoud en wijzigingen	Bij alle geïnterviewde personen zijn onderhoudscontracten een belangrijke bron van inkomsten. In vrijwel alle gevallen wordt er een jaarlijks onderhoud uitgevoerd op de centrale waarbij m.n. de werking van alle componenten wordt gecontroleerd. Niet alle installateurs kijken bij het jaarlijkse onderhoud ook naar informatiebeveiliging (bijvoorbeeld of er nieuwe firmware is uitgekomen voor de installaties). Belangrijke firmware wijzigingen worden ook niet altijd doorgevoerd. Als alles goed werkt kunnen wijzigingen in software/firmware vervelende gevolgen hebben (uitval of storingen). Tussentijdse eenvoudige wijzigingen – bijvoorbeeld het toevoegen of verwijderen van een gebruiker – gebeurt veelal op afstand. De wijze waarop deze wijzigingen worden afgestemd tussen eindklant en installateur gebeurt veelal ad-hoc via E-mail of telefoon. Hier ligt in onze optiek een belangrijk beveiligingsrisico. In de onderhoudscontracten is niet altijd expliciet vastgelegd dat installateurs ook op afstand kunnen inloggen. In principe wordt dit in (mondeling) overleg met de klant ingesteld (maar niet schriftelijk vastgelegd).
Back-ups	Back-ups van installaties worden gemaakt en bij veel installateurs opgeslagen op het netwerk.
Logging	Logging op afwijkingen vindt beperkt plaats. Op de installaties worden zelf logs bijgehouden en ook op andere componenten (bijvoorbeeld VPN verbindingen) kan logging worden geplaatst. Logs worden bij de kleinere installateurs alleen nagekeken op het moment dat er vragen zijn (dan kan het dus ook voorkomen dat op dat moment gemerkt wordt dat logging niet goed werkt).
Inloggen op afstand	Er wordt veelvuldig gebruik gemaakt van mogelijkheden om installaties volledig op afstand te kunnen beheren. Hiervoor worden verschillende systemen ingezet. We hebben niet gekeken naar de beveiliging van deze individuele systemen, maar zien in het proces wel issues m.b.t. informatiebeveiliging.

Ingebrachte stelling ledenvergadering



Enkele citaten uit diepte-interviews

… Bij het uitvoeren van onderhoud op afstand dient de klant eerst zijn beheerderscode in te voeren. Daarna kan er onderhoud worden uitgevoerd door Organisatie. Rechten voor het uitvoeren van onderhoud (gebruikers, codes etc.) ligt in principe bij klanten zelf, maar kan ook aan Organisatie worden uitbesteed…

…Bij het onderhoud (1x per jaar) wijzigen we het installateurswachtwoord...

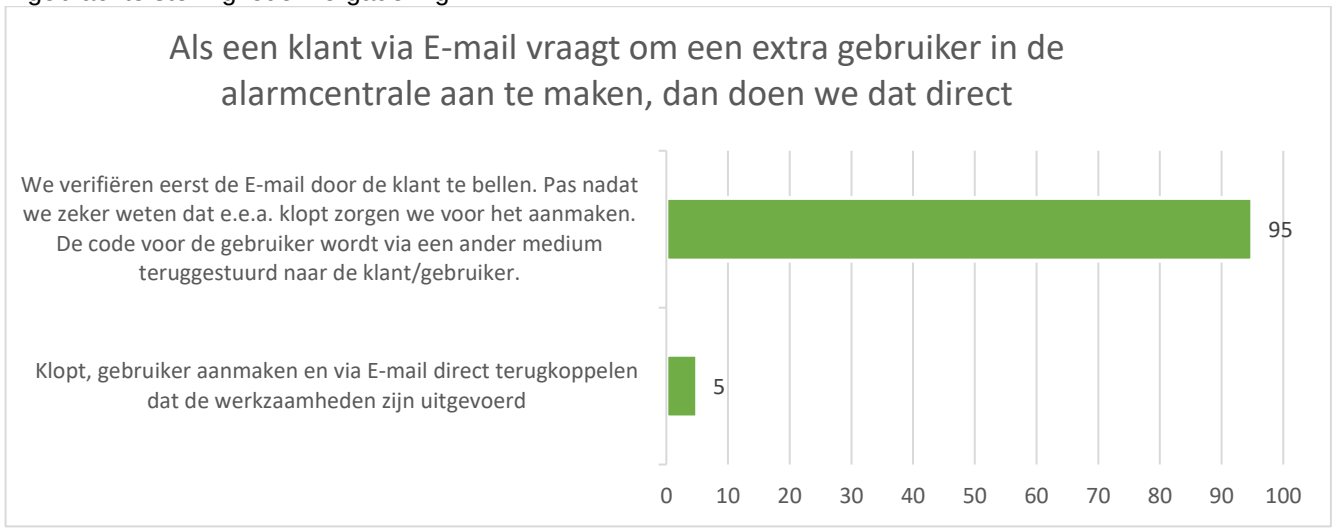
…Zeker niet elke klant heeft een onderhoudscontract. Hierdoor kan het best zijn dat centrales, detectoren, sensoren etc. niet goed meer functioneren zonder dat de klant of installateur dat weet…

…Voordat gestart wordt met onderhoud wordt veelal eerst een back-up gemaakt van de installatie. Deze back-up bestanden komen uiteindelijk op het netwerk van de installateur (maar blijven ook wel eens achter op laptops van monteurs)…

… Logging op installaties gebeurt automatisch. We lopen deze logs niet na op afwijkingen…

… Er worden apps voor installateurs gebruikt zijn waarop je zonder 2FA kunt inloggen en waar geen wachtwoordbeleid – buiten het eenmalig instellen van een complex wachtwoord - op deze systemen staan. Nadat je bent ingelogd krijg je toegang tot alle klanten en installaties die bij klanten zijn geplaatst…

Ingebrachte stelling ledenvergadering



Onze aanbeveling(en)

1.	De voorschriften voor onderhoud van de BORG regeling stammen uit 2000. Informatiebeveiliging is hier nog niet in opgenomen en we adviseren om deze te herzien, waarbij rekening is gehouden met alle punten die te maken hebben met informatiebeveiliging.
2.	Zorg er voor dat het nalopen van logging onderdeel gaat vormen van het onderhoud óf dat er automatisch acties worden uitgevoerd op het moment dat zich uitzonderingssituaties voordoen.
3.	Zet een duidelijke (minimale) procedure op waarin wordt aangegeven op welke wijze er op afstand ingelogd kan/mag worden.

Werken met oudere installaties

Onderwerp	Onze bevinding (in algemeenheid)
Oudere installaties	Voor oudere centrales was informatiebeveiliging van ondergeschikt belang. We zijn tijdens de interviews tegen een aantal punten aangelopen die betrekking hebben op de beveiliging van oudere centrales.

Ingebrachte stelling ledenvergadering
Geen stelling ingebracht.

Onze aanbeveling(en)

1.	Informatiebeveiliging is niet alleen van de 21e eeuw. Er ligt nu meer nadruk op, omdat vrijwel alles aan het internet wordt gekoppeld en daardoor ook nieuwe dreigingen ontstaan. Bekijk ook voor oudere installaties welke impact informatiebeveiliging heeft of kan hebben.

Enkele citaten uit diepte-interviews

... Oudere centrales hebben het probleem dat daar direct met laptops op aangesloten kan worden, waarna je het wachtwoord kan wijzigen en – zonder de centrale aan te passen naar default settings – je wijzigingen in de centrale kan doorvoeren of kan uitlezen.. I.s.m. de eindklant zal hiervoor wel eerst de centrale opengemaakt moeten worden wat een alarm zal veroorzaken....

...Oudere centrales hebben daarnaast het probleem dat er default downloadcodes worden gebruikt. Met port-forwarding kun je eigenlijk eenvoudig op dit soort centrales binnenkomen. Vooral bij partijen die alarmcentrales er een beetje 'bij' deden is dit een risico...

...Het was bij veel oudere centrales mogelijk om in te stellen dat een centrale na inloggen op afstand automatisch terugbelde op jouw nummer waarna onderhoud uitgevoerd kon worden. Met IP is het mogelijk om whitelisting van IP nummers te gebruiken, maar uiteraard moet dit alles wel ingesteld staan op de centrale en/of firewall...