

	Systeemdokumentatie Titel : Risico afweging VRI Informatiebeveiliging Auteur : E. Bish / H. Hoets Datum : 19 maart 2021 Versie : 1.0
--	--

Risico afweging Verkeer Regel Installaties i.h.k.v. Informatiebeveiliging

Auteurs:

E. Bish	Sr. Adviseur en projectleider systemen
H. Hoets	Sr. Adviseur Verkeer Regel Installaties

	Systeemdokumentatie Titel : Risico afweging VRI Informatiebeveiliging Auteur : E. Bish / H. Hoets Datum : 19 maart 2021 Versie : 1.0
---	--

Management samenvatting

Dit document beschrijft de meest voor de hand liggende bedreigingen voor de correcte werking van Verkeer Regelinstallaties in de context van Informatiebeveiliging.

De mogelijke impact en mitigerende maatregelen worden op hoofdlijnen benoemd.

In het kader van Informatiebeveiliging wordt gesteld dat manipulatie door een kwaadwillende op het niveau van de TLC, bijvoorbeeld door de elektrische ingangen te beïnvloeden, het beschadigen van detectielussen of het veroorzaken van lampstoringen, weliswaar ongewenst gedrag van de VRI kan veroorzaken maar dat de impact beperkt blijft tot lokale uitval van deze enkele VRI. Er ontstaat geen onveilige verkeerssituatie en deze status is direct zichtbaar in de besturingsapplicatie (VBS suite van applicaties) en wordt continue gelogd. Bij deze aanname hoort ook de aanname dat de systeemkast gesloten is en zich in correcte staat bevindt. Grote schades zoals aanrijdingen of brand vallen buiten deze risico afweging.

De mitigerende maatregelen betreffen het voldoende fysiek robuust uitvoeren van de straatkast, het fysiek beschermen van de apparatuur en bekabeling in de kast en het gebruik van logische beschermingsmiddelen.

	Systeemdocumentatie Titel : Risico afweging VRI Informatiebeveiliging Auteur : E. Bish / H. Hoets Datum : 19 maart 2021 Versie : 1.0
--	--

Versie historie

Historie

Versie	Status	Wijzigingen	Auteur	Datum
1.0 concept	Initiële versie	Initieel document	E. Bish	30 januari 2021
1.0	Uitgave	Van concept naar uitgave	E.Bish	19 maart 2021

Distributie

Naam	Organisatie	Rol
E. Bish	Verkeer en Openbare Ruimte	Adviseur en Projectleider Systemen
H. Hoets	Verkeer en Openbare Ruimte	Adviseur Verkeer Regel Installaties
R. Hartman	Verkeer en Openbare Ruimte	Adviseur Verkeer Regel Installaties
E. Breems	Verkeer en Openbare Ruimte	Security Officer cluster Ruimte en Economie
E. Folten	Verkeer en Openbare Ruimte	Asset manager Verkeer Regel Installaties

	Systeemdokumentatie Titel : Risico afweging VRI Informatiebeveiliging Auteur : E. Bish / H. Hoets Datum : 19 maart 2021 Versie : 1.0
--	--

Inhoudsopgave

Risico afweging Verkeer Regel Installaties i.h.k.v. Informatiebeveiliging	1
Management samenvatting	2
Versie historie.....	3
Inhoudsopgave	4
Systeemcomponenten	5
Fail-safe gedrag	6
Risico's, impact en mitigatie.....	6

	Systeemdokumentatie Titel : Risico afweging VRI Informatiebeveiliging Auteur : E. Bish / H. Hoets Datum : 19 maart 2021 Versie : 1.0
--	--

Systeemcomponenten

Een Verkeer Regel Installatie (VRI) bestaat uit een metalen systeemkast die in de openbare ruimte is geplaatst nabij het kruispunt dat actief geregeld moet worden. De VRI bestaat op hoofdlijnen uit een Traffic Light Controller (TLC) voor het verwerken van elektrische ingangssignalen, het tonen van het juiste lichtbeeld voor het besturen van het verkeer op basis van een starre regeling of een voertuig afhankelijke regeling. De wijze van regelen wordt op afstand over het besturingsnetwerk of lokaal op basis van een klok ("week automaat") bepaald door het selecteren van een specifieke vooraf gedefinieerde regeling. De uitgangssignalen van de TLC worden bewaakt zodat onjuiste of ongewenste lichtbeelden niet getoond kunnen worden. Indien door een verstoring een onjuist beeld getoond zou moeten worden, dan worden alle lichten gedoofd of worden alle richtingen op geel knipperen gezet waardoor de weggebruiker weet/ziet dat nu gewoon de wegenverkeerswet van toepassing is.

In het kader van Informatiebeveiliging wordt gesteld dat manipulatie door een kwaadwillende op het niveau van de TLC, bijvoorbeeld door de elektrische ingangen te beïnvloeden, het beschadigen van detectielussen of het veroorzaken van lampstoringen, weliswaar ongewenst gedrag van de VRI kan veroorzaken maar dat de impact beperkt blijft tot lokale uitval van deze enkele VRI. Er ontstaat geen onveilige verkeerssituatie en deze status is direct zichtbaar in de besturingsapplicatie (VBS suite van applicaties) en wordt continue gelogd. Bij deze aanname hoort ook de aanname dat de systeemkast gesloten is en zich in correcte staat bevindt. Grote schades zoals aanrijdingen of brand vallen buiten deze risico afweging.

De ingangssignalen zijn:

- Detectielussen in het wegdek
- Drukknoppen op de masten
- Detectiecamera's
- Prioriteitsaanvragen van het openbaar vervoer en nood & hulpdiensten via korte afstandsradio (KAR)
- Detectiesignalen zoals brugopeningen, brandweeringrepen, aanmelden van de tram
- Lokale bediening vanaf het console
- Besturing over het IP netwerk d.m.v. het IVERA protocol
- Management van het apparaat via CCOL command line, WebGui, FTP etc. over het IP netwerk.
- Detectiesignalen van nabij gelegen VRI's over de koppelkabel.
- Voor een iVRI: ETSI berichten
- Seriële poorten

De uitgangssignalen zijn:

- Lichtgroepen
- Logging Data (VLOG bestanden, VLOG stream, NV bestanden etc)
- Status informatie in de vorm van trigger signalen

- Status informatie van de fasebewaking
- Voor een iVRI: ETSI berichten
- De grafische interface (WebGui) toont de actuele status van het geregelde kruispunt. Na aanmelden is het mogelijk om systeeminstellingen op te vragen of te wijzigen.

Fail-safe gedrag

Onder normale omstandigheden wordt op basis van de centrale klok in de VBS besturingsapplicatie elke VRI op de ingestelde momenten op de juiste regeling (CPxx) gezet. Wanneer besturing op afstand om wat voor reden dan ook niet lukt, dan valt de TLC terug op de lokaal aanwezige systeemklok voor het op het gewenste moment activeren van de juiste regeling. Dit kan hooguit een sub-optimale verkeersdoorstroming tot gevolg hebben, maar kan niet tot onveilige situaties aanleiding geven. Onvolledige of onjuiste lichtbeelden kunnen niet getoond worden. De fasebewaker grijpt dan in en zet de installatie op geel knipperen of schakelt deze uit.

Risico's, impact en mitigatie

Onder de aanname dat manipulatie van de elektrische ingangen hooguit lokale uitval van de VRI kan veroorzaken en geen terugwerking op het besturingsnetwerk kan hebben zijn elektrische storingen op de in- en uitgangspoorten van de TLC geen risicofactor voor het besturingsnetwerk of een bedreiging in het kader van Informatiebeveiliging.

De risicoafweging in het kader van Informatiebeveiliging beperkt zich dus tot de componenten in de systeemkast en beïnvloeding van de werking van de TLC over het besturingsnetwerk. De volgende meest voor de hand liggende risico's kunnen worden benoemd:

Risico	Beschrijving	Impact	Mitigatie
Ongeloofwaardige regeling.	Op afstand of lokaal verstarring van een specifiek lichtbeeld door 1 of meerdere rijrichtingen permanent op rood te zetten. Uiteindelijk zullen weggebruikers dit lichtbeeld als foutief interpreteren en door rood gaan rijden (rood licht negatie) en dat zorgt voor onveiligheid op de weg.	Ongevallen zijn tenminste aanleiding tot imagoschade, maar kunnen ook verdergaande juridische consequenties hebben.	Algehele bescherming van de systeemkast en de verbindingen van de systeemkast met het datacenter. Zowel fysieke als logische beschermingsmaatregelen treffen. Geautomatiseerde monitoring zodat onjuist of ongewenst gedrag snel wordt opgemerkt en opgevolgd kan worden.

Verkeer ontregelen	Manipulatie van het gedrag van meerdere VRI's tegelijkertijd door beïnvloeding vanuit het besturingsnetwerk. Indien dit zich zou voordoen dan kan een verkeerschaos ontstaan en kan op grote schaal roodlicht negatie ontstaan en dat is een bron voor onveilige en gevaarlijke situaties op de weg.	Ongevallen zijn tenminste aanleiding tot imagoschade, maar kunnen ook verdergaande juridische consequenties hebben.	Algehele bescherming van de systeemkast en de verbindingen van de systeemkast met het datacenter. Zowel fysieke als logische beschermingsmaatregelen treffen. Geautomatiseerde monitoring zodat onjuist of ongewenst gedrag snel wordt opgemerkt en opgevolgd kan worden.
Datastroom onbetrouwbaar	Het aftappen van de datastroom van- en naar de VRI. De datastroom kan privacy gevoelige elementen bevatten en de data, in het bijzonder VLOG, wordt als bewijslast voor ongeval analyses gebruikt. Datalek. In het geval van een iVRI kunnen de ETSI berichten die door het systeem verwerkt worden onder specifieke omstandigheden als privacy gevoelig aangemerkt worden	De integriteit van de datastroom dient geborgd te worden voor een betrouwbare werking van het systeem en om de integriteit van de log bestanden of log stream te kunnen garanderen.	Communicatie uitsluitend over encrypted channels. Bij voorkeur toepassen van end-to-end encryptie op basis van TLS. Afscherming (beveiliging) van het endpoint zowel logisch als fysiek om de private key voor de TLS sessies maximaal te beschermen. Private keys niet exporteerbaar maken. Monitoring van de RIS interface van een iVRI systeem.
Klok manipulatie/drift	Wanneer de systeemklok niet goed gesynchroniseerd wordt of niet correct is ingesteld dan wordt	Bij ernstige klokafwijkingen is communicatie met de VRI niet meer mogelijk.	De systeemklok periodiek geautomatiseerd synchroniseren met een atoomklok referentie vanuit het

	de informatie in de VLOG stroom grotendeels onbruikbaar en is geen betrouwbare bron meer voor (ongeval) analyses. Indien de systeemklok niet correct is ingesteld of extreem grote drift vertoond, dan kunnen TLS sessies ongeldig worden en is communicatie met de VRI over een beveiligd kanaal niet meer mogelijk. Een relatief kleine afwijking in de orde van seconden van de klok kan de werking van een groene golf voor de weggebruikers verstoren.	Bij geringe afwijkingen kan functieverlies optreden of neemt de betrouwbaarheid van de VLOG data af. Indien VLOG data niet betrouwbaar geleverd kan worden, dan kan niet aan de verplichting worden voldaan om data te leveren voor ongeval analyses. Analyses vanuit een verkeerskundig standpunt zijn minder nauwkeurig te maken.	besturingsnetwerk. (stratum1) Zowel datum als tijd synchroniseren. Geautomatiseerde monitoring op klok afwijkingen.
Verlies aan controle door overbelasting	De TLC bevat een systeembord met beperkte systeembronnen. Een bewuste Denial-of-Service (DoS) aanval of een software fout van de centrale besturingssoftware kan het systeem overbelasten. Bij eerdere tests is gebleken dat een klein aantal gelijktijdige sessies met valide data en protocollen al de besturing op	Verlies van controle op afstand. Mogelijk worden de cyclus tijden van de VRI niet meer betrouwbaar gehaald. Verlies van logging data en status informatie.	Firewall systeem voor de TLC plaatsen met intrusion detection & mitigation mogelijkheden. Strikte filtering op uitsluitend noodzakelijke protocollen. Regelset van de firewall inregelen op basis van IP naar IP communicatie in plaats van op netwerk naar netwerk communicatie.

	afstand onmogelijk kan maken. De TLC kent meerdere interfaces en die zijn allen gevoelig voor overbelasting.		Geautomatiseerde monitoring van de firewall zodat afwijkend gedrag wordt gedetecteerd en kan worden opgevolgd door de Servicedesk van de opdrachtgever en/of de leverancier van de VRI. Geautomatiseerde integriteitscontrole op de VLOG datastroom aan de kant van de opdrachtgever.
Geen inherente bescherming ("self-defence")	Het besturingssysteem van de TLC bevat geen eigen bescherming tegen ongewenst of foutief netwerkverkeer. Hierdoor staan er meer systeempoorten open dan strikt noodzakelijk.	Functie en/of prestatieverlies van de VRI.	De TLC dient maximaal afgeschermd te worden met fysieke en logische beschermingsmiddelen. Automatische doormelding en Logging van niet-standaard gedrag. Systeem hardening.
Digitale identiteiten	De configuratie van de TLC kan plaatsvinden via console sessies of door middel van de grafische interface. Deze interface is beveiligd met een enkelvoudig wachtwoord en is niet gekoppeld aan een rol. Het is een alles of niets situatie. Het gebruik van een single-factor authenticatie op basis van een pincode van 4	Identiteitsfraude, toegang tot systeeminstellingen voor niet-geautoriseerde personen.	Definieer meerdere gebruikersrollen op alle componenten die lokaal of over het netwerk een interface bieden. Definieer tenminste een administrator rol en een alleen lezen rol. Toon alleen informatie passend bij de rol. Gebruik een sterk wachtwoord beleid of maak gebruik van centrale authenticatie.

	cijfers geeft erg weinig bescherming.		Verleen alleen toegang wanneer dat noodzakelijk is voor het uitvoeren van werkzaamheden. Beperk de groep mensen die toegang hebben tot een noodzakelijk minimum.
Ongeautoriseerde toegang	Bij geopende systeemkast is het op verschillende manieren mogelijk misbruik te maken van het systeem.	Ongewenst gedrag of uitval van de installatie. Onbetrouwbare logging data. Aftappen van data. Plaatsing van "rogue device". (= An unauthorized device accesses the system, manipulating it or providing incorrect data to system operators.) Aftappen van de elektriciteit aansluiting.	De straatkast moet fysiek zeer robuust zijn uitgevoerd, voorzien van deugdelijke sloten met bijbehorend sleutelplan, automatische doormelding op alle segmenten. Geen actieve ongebruikte netwerkaansluitingen in de kast. Fysieke afscherming van bekabeling en aansluitingen. Laat geen aanwijzingen in de kast achter die een malafide gebruiker informatie geven over de configuratie of het netwerk (bijvoorbeeld stickers, systeemdokumentatie, mobiele gegevensdragers etc.). Gebruik geen DHCP of andere automatische configuratie protocollen als dat niet noodzakelijk is. Verklein het "attack surface" door hardening

			van de TLC, firewall en andere aanwezige componenten.
Menselijke fouten en ongecontroleerde wijzigingen	Mensen kunnen fouten maken en goed bedoeld wijzigingen aan het systeem doorvoeren die een negatieve invloed hebben op het systeem.	Ongewenst gedrag of uitval van de installatie. Onbetrouwbare logging data. Lekken van data.	Beperk toegang tot de installatie tot een kleine groep gecertificeerde medewerkers. Voer alleen wijzigingen door op een gestructureerde en gecontroleerde wijze. Indien Ad-hoc werkzaamheden moeten worden uitgevoerd, voer dan altijd achteraf een controle uit op functionele en beveiliging aspecten. Standaardiseer de opbouw van de installatie.
Weersinvloeden	In de zomer kan de temperatuur in de straatkast hoog oplopen. In andere seizoenen kan vocht of kou de werking van de apparatuur beïnvloeden. Er kan zich vuil of stof ophopen in de straatkast.	Ongewenst gedrag of uitval van de installatie. Besturing op afstand niet mogelijk. Geen status of logging informatie.	Robuuste straatkast voorzien van passieve ventilatie en vorstbescherming. Gebruik alleen datacommunicatie apparatuur van industriële kwaliteit die geschikt is voor een groot temperatuurbereik en uitgerust met passieve koeling. Bewaak de interne temperatuur van de componenten d.m.v. het SNMP protocol of met aparte

Systeemdocumentatie

Titel :
 Risico afweging VRI Informatiebeveiliging

Auteur : E. Bish / H. Hoets
 Datum : 19 maart 2021
 Versie : 1.0

			temperatuursensoren met een automatische tool. Inspecteer op periodieke basis de conditie van de straatkast en de componenten die zich daarin bevinden.