PLATFORM VOOR CYBERSECURITY
CPNI.NL

Beveiliging van legacy procescontrolesystemen

op weg naar veilige procescontrolesystemen

Cybersecurity één publiek-private integrale aanpak

Inhoudsopgave

CPNI.NL
Versie 1.0 (15 februari 2012)

Auteurs:
Maarten Oosterink, CPNI.NL
Review en input:
Aad Dekker, Alliander
Paul Hendriks, Essent
Lhoussain Lhassani, Stedin
Mirsad Murtic, Yokogawa
Joost Roldaan, Heineken
Renny ter Veer, Waterleidingmaatschappij Drenthe
Martin Visser, Waternet
Wil Weterings, Schiphol Groep
Bart de Wijs, ABB

Auke Huistra, CPNI.NL
Eric Luiijf, TNO/CPNI.NL

Managementsamenvatting

Deze white paper beschrijft oplossingen die organisaties kunnen gebruiken om de beveiliging van legacy procescontrolesystemen op peil te brengen en te houden. In algemene zin bedoelen we met een legacy systeem een oude methode, technologie, computersysteem of applicatie die in gebruik is en blijft ondanks het feit dat er nieuwe technologieën of efficiëntere methoden voorhanden zijn.

Legacy systemen kenmerken zich doordat ze om een of meer redenen niet afdoende op gangbare wijze kunnen worden beveiligd tegen nieuwe dreigingen rond beschikbaarheid, integriteit of vertrouwelijkheid. Voorbeelden hiervoor zijn ontbrekende of onvolledige ondersteuning door de leverancier en afwezigheid van beveiligingsupdates. Ook verlies van (voldoende) kennis en kunde in de eigen organisatie, bijvoorbeeld door personeelsverloop, kan een oorzaak zijn.

Het is essentieel om de eigen omgeving goed te kennen. Daarbij is het van belang te weten elke procescontrolesystemen in de organisatie worden gebruikt en hoe belangrijk deze zijn voor de continuïteit van de bedrijfsprocessen. En welke kwetsbaarheden deze systemen bevatten.

In deze white paper komt een aantal mogelijke maatregelen aan bod om legacy procescontrolesystemen te beschermen tegen ongewenste invloeden op de beschikbaarheid, integriteit of vertrouwelijkheid van de informatie in deze systemen dan wel processen die ermee worden bestuurd. Een generiek antwoord bestaat niet. Elke situatie en elke organisatie kent haar eigen kwetsbaarheden en mogelijkheden om deze weg te nemen, te voorkomen of de kans op gevolgschade te verminderen.

Voor elke situatie past een unieke mix van maatregelen. Deze maatregelen moeten het resultaat zijn van een risicoanalyse, waarin een afweging wordt gemaakt op basis van de kans dat een bepaalde dreiging op zal treden, de impact die dit met zich mee kan brengen en de kosten of investeringen die nodig zijn om dit risico te verkleinen of weg te nemen.

De dreigingen waar systemen aan bloot staan en de kans dat een dreiging wordt uitgebuit, is onderhevig aan verandering. Het is verstandig om bestaande ICT procedures of audit-mechanismen te hanteren bij het regelmatig evalueren van de gekozen combinatie van maatregelen.

Definities

In dit document wordt de volgende definitie gehanteerd voor legacy procescontrolesystemen (verder ook aangeduid als legacy systemen) in relatie tot de beveiliging ervan:

Legacy systemen zijn systemen die niet volledig volgens gangbare methoden en technieken kunnen worden beveiligd en daardoor een hoger risico vormen voor de continuïteit, integriteit of vertrouwelijkheid van het bestuurde proces.

Voorbeelden van oorzaken voor het bestempelen van systemen tot legacy zijn:

- Ontbrekende (deel)ondersteuning door leverancier of gebrek aan reserveonderdelen
- Dalende kennis en kunde over systemen in de markt of eigen organisatie
- Onvoldoende beveiliging tegen fysieke of logische dreigingen uit de omgeving

Onder beveiliging verstaan we hierbij het beschermen tegen ongewenste invloeden op de beschikbaarheid, integriteit of vertrouwelijkheid van de systemen of de processen die ermee worden bestuurd.

Doelstellingen

Het doel van deze white paper is om een aantal oplossingen aan te dragen voor het beter beveiligen van legacy procescontrolesystemen en deze oplossingen in vogelvlucht te behandelen. Achterliggend doel is om management en andere beslissers binnen organisaties die met legacy systemen te maken hebben handvatten te bieden om beslissingen te nemen.

Kern

Bijna elke organisatie die procescontrolesystemen gebruikt, heeft te maken met verouderde maar vitale systemen en ontbrekende kennis of documentatie van die systemen. Maar ook met systemen waaraan men geen aanpassingen durft te doen uit angst voor de gevolgen.

Dit is een van de redenen waardoor de gangbare methoden en technieken om (informatie) systemen te beschermen niet (volledig) toepasbaar zijn.

Het resultaat is dat voor deze systemen een specifieke samenstelling van maatregelen moet worden gekozen. Dit hoeven niet altijd bijzondere of kostbare maatregelen te zijn. Voor de meeste systemen geldt dat via een bedrijfsbrede aanpak een verzameling van maatregelen kan worden vastgesteld. Hierbij kan worden gekozen uit een verzameling van mogelijke bouwstenen.

Voorbeelden hiervan zijn:
- De regelmatige installatie van beveiligingsupdates (patches)
- Opstellen en bekendmaken van beleid over gebruik van verwisselbare media
- Regelmatig maken van back-ups
- Hebben van sluitende supportcontracten
- Voor handen hebben van goede logische toegangscontrole (sterke wachtwoorden)

Kanttekening hierbij: hoewel systemen vaak vanwege hun leeftijd ‘legacy’ worden genoemd, hoeft dat niet meteen een probleem voor de beveiliging te zijn. Niet elk systeem heeft regelmatig updates nodig en een goed geteste back-up kan ook voor een oud systeem als vangnet dienen. Ook kan hier in het geval van een procescontrolesysteem zonder netwerkverbindingen of USB poorten minder strikt mee worden omgegaan.

Niet alleen leveranciers zijn verantwoordelijk voor het verdwijnen van ondersteuning en kennis over operationele systemen. Niet zelden zorgen reorganisaties of natuurlijk personeelsverloop voor verdamping van kennis in de eigen organisatie. Gebrek aan documentatie kan hierbij ook een rol spelen. Zeker bij systemen die zelden aandacht nodig hebben, en dat geldt voor veel procescontrolesystemen, is het kwaad geschied lang voordat men er erg in heeft.

De verzameling van bouwstenen waaruit beveiliging wordt opgebouwd is voor legacy systemen niet wezenlijk anders dan voor traditionele informatie- en communicatietechnologie (ICT) systemen. Net als in ICT omgevingen is het gangbaar om maatregelen te treffen op basis van afgewogen risicofactoren. Deze zouden het resultaat van een risicoanalyse moeten zijn, waarin een afweging wordt gemaakt op basis van de kans dat een bepaalde dreiging op zal treden, de impact die dit met zich mee brengt en de kosten of investeringen die nodig zijn om dit risico te verkleinen of weg te nemen. Meer informatie over risicoanalyse en process control security is te vinden in de good practice guide van CPNI getiteld: ‘Understanding the business risk’ *(bron: Centre for Protection of National Infrastructure UK)*.

Let op: een risicoanalyse is een momentopname. Dagelijks doen zich nieuwe dreigingen voor, die van invloed kunnen zijn op de manier waarop systemen moeten worden beveiligd om het risico acceptabel te houden. Het is belangrijk dat deze dreigingen zo vaak mogelijk worden geanalyseerd. En waar nodig veranderingen worden doorgevoerd in de manier waarop systemen worden beveiligd. Het is verstandig om hiervoor (bestaande) ICT procedures of audit-mechanismen te hanteren.

Het is de mix van maatregelen die het verschil moet maken. Selecteer daarbij de maatregelen volgens het 'defense-in-depth' principe. Dit houdt in dat één specifieke kwetsbaarheid door meer dan één maatregel wordt afgedekt. Meer informatie hierover staat in de good practice guide van het Amerikaanse Department of Homeland Security: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies *(bron: Department of Homeland Security US)*.

De meest voorkomende maatregelen worden kort in deze white paper behandeld. Het is echter onmogelijk om een volledig overzicht te bieden.

Maatregelen

Vervanging of upgrade

Vanuit het oogpunt van een informatiebeveiliger is vervanging van een legacy systeem vaak een logische optie. Maar beveiliging concurreert met bijvoorbeeld de kosten en de benodigde tijd die nodig zijn voor migratie. Een risicoanalyse moet dan uitsluitsel geven. Wanneer het risico goed inzichtelijk is en de maatregelen gedefinieerd, kan er een rest risico over blijven dat niet acceptabel is. Dat kan een motivatie zijn om versneld tot vervanging of upgrade van het legacy systeem over te gaan.

Hardening

Hardening is het inperken van een systeem tot het strikt noodzakelijke. Voor computersystemen en netwerkcomponenten betekent dit het verwijderen van onderdelen of toepassingen die niet noodzakelijk zijn. Hiermee wordt het aantal mogelijke kwetsbaarheden tot een minimum beperkt. Dit kan betekenen dat een ongebruikte netwerkpoort wordt uitgeschakeld of een ingebouwde webserver gedeactiveerd. Denk bij Windows systemen aan het verwijderen van niet noodzakelijke toepassingen zoals bureau-accessoires of Windows Mediaspeler. Denk bij Unix systemen aan het verwijderen of uit-schakelen van onnodige services zoals X11 of de Telnet daemon. Informatie over het veilig configureren van ICT systemen is te vinden op de website van de National Security Agency (NSA) *(bron: National Security Agency US)*. Ga ook na bij leveranciers of zij al specifieke diensten of oplossingen hebben georganiseerd die zorgen voor adequate hardening.

Fysieke markering en beperking van toegang

Voor veel systemen geldt dat logische beveiligingsmaatregelen, zoals het instellen van wachtwoorden of het beperken van gebruikers-rechten, kunnen worden omzeild als fysieke toegang tot systemen kan worden verkregen. Dan is veelal sprake van kwade opzet. Fysieke toegang kan worden voorkomen door kwetsbare systemen af te zonderen. Plaats ze achter slot en grendel, maar realiseer wel dat van sleutels vaak (te) veel exemplaren in omloop zijn.
Mensen kunnen ook onbedoeld problemen veroorzaken. Betrokkenen zijn zich vaak niet bewust van de gevolgen van hun handelingen voor specifieke (kwetsbare) systemen. Het markeren van systemen als kwetsbaar of kritisch/vitaal kan – hoe simpel ook – al een effectief middel zijn. Een dergelijke waarschuwing kan fysiek zijn, maar ook via login banners worden gebracht. Een duidelijke instructie die het risico van gebruik van een systeem duidt, kost weinig, maar kan incidenten voorkomen.

Beperken gebruikersrechten en logische toegang

In veel (oude) systemen wordt geen onderscheid gemaakt tussen soorten gebruikers, zoals bijvoorbeeld beheerders of gebruikers die slechts inzage in bepaalde meetwaarden hoeven te hebben. Waar in het verleden om goede (of slechte) redenen is gekozen geen onderscheid te maken, kan dit tegenwoordig vervelende gevolgen hebben. Zeker als systemen verbonden zijn via een netwerk of wanneer draagbare media worden gebruikt. Moderne malware, zoals virussen, Trojans en andere kwaadwillende software, is in staat om zich razendsnel een weg

te banen door systemen en netwerken. Meestal gebruikmakend van onnodig hoge rechten van gebruikersaccounts. Het uitdelen van nieuwe gebruikersrechten volgens het 'least privilege' principe kan een snelle verspreiding voorkomen. Ga hiervoor na welke voorzieningen het betreffende systeem biedt. Wellicht is nuttige functionaliteit (nog ongebruikt) voorhanden.

Het gebruik van een algemeen wachtwoord of een te eenvoudig wachtwoord, kan er voor zorgen dat mensen onbedoeld een kwetsbaar systeem gebruiken. Ook verregaande integratie in bestaande authenticatieomgevingen zoals een Active Directory kan er voor zorgen dat mensen onnodig toegang tot een systeem hebben. Daarmee kunnen zij bewust of onbewust een gevaar voor deze systemen vormen.

Wachtwoorden

Toegang tot systemen of bepaalde functionaliteit binnen systemen is veelal afgeschermd door wachtwoorden. Het is raadzaam om, indien mogelijk, persoonlijke gebruikersaccounts te gebruiken die voorzien zijn van niet eenvoudig te raden wachtwoorden. Daarnaast is het verstandig een routine te hebben voor het regelmatig wijzigen van deze wachtwoorden. Dit voorkomt bijvoorbeeld dat gebruikersaccounts die door meerdere personen worden gebruikt nog toegankelijk zijn voor personen die deze niet meer nodig hebben. Rond de vereiste complexiteit en frequentie van verandering van wachtwoorden is geen eenduidig antwoord te geven. Dit is afhankelijk van veel factoren, bijvoorbeeld andere aanwezige beveiligingsmaatregelen zoals fysieke beveiliging of sociale controle, en gevolgschade bij misbruik.

Netwerkcompartimentering en firewalls

Het zijn niet alleen gebruikers die direct van negatieve invloed op legacy systemen kunnen zijn. Met name oudere systemen kunnen onvoorspelbaar reageren op netwerkverkeer. Zelfs verkeer dat in kantooromgevingen als normaal wordt beschouwd, kan ongewenste uitwerking hebben op procescontrolesystemen. Deze systemen in een apart deel van het netwerk plaatsen kan uitkomst bieden. Al dan niet gecombineerd met het gebruik van een firewall. Speciaal voor kwetsbare systemen zijn er ook specialistische firewalls verkrijgbaar die het mogelijk maken deze toch veilig in een bestaande netwerkomgeving te gebruiken.

Reserveonderdelen in voorraad

Voor systemen die als 'end-of-life' zijn bestempeld door de leverancier, of waarvan de leverancier om andere redenen niet (tijdig) reserveonderdelen op locatie kan leveren, kan het verstandig zijn om zelf onderdelen inclusief de benodigde documentatie in voorraad te houden. Omdat onderdelen niet het eeuwige leven hebben, is het risico op falen ervan voor oudere systemen groter. De mate waarin leveranciers in staat zijn deze onderdelen te vervangen, lijkt omgekeerd evenredig met de leeftijd van systemen. Dat kan door gebrek aan onderdelen zijn, maar ook omdat medewerkers van de leveranciers onvoldoende bekend zijn met oude systemen. Met leveranciers kunnen afspraken worden gemaakt over het in consignatie houden

van reserveonderdelen. Ook kunnen deze zelf worden aangeschaft en in voorraad worden gehouden. Denk ook aan de vastlegging van benodigde configuratiegegevens en procedures.

Virtualisatie

In de ICT heeft virtualisatie een grote vlucht genomen. Moderne ontwikkelingen en legacy systemen lijken op het eerste gezicht niet samen te gaan. Toch biedt virtualisatie hier juist mogelijkheden. Zo biedt zogenaamde 'physical to virtual' (P2V) technologie mogelijkheden om fysieke (IT) systemen te 'kopiëren' naar virtuele systemen en daarmee naar moderne virtuele omgevingen. Hiermee kan de afhankelijkheid van oude en lastig vervangbare hardware worden voorkomen. Het biedt ook mogelijkheden voor back-up (snapshots) en restore, en daarmee verhoogde beschikbaarheid. Enkele leveranciers bieden een oplossing voor huidige systemen. Maar ook voor oudere systemen waarvoor ondersteuning ontbreekt, kan virtualisatie een goede oplossing zijn om de beschikbaarheid van systemen te verhogen.

Back-up en restore

Zoals eigenlijk voor alle systemen moet gelden, is een regelmatige back-up voor legacy systemen belangrijk. Afhankelijk van het betreffende systeem kan dit een volledige kopie van besturingssysteem en applicaties zijn, tot een dump van de applicatiecode uit een programmable logic controller (PLC). In geval van een legacy systeem is het raadzaam om voor elke wijziging een back-up te maken. Nog belangrijker dan de back-up zelf is het testen van de mogelijkheid om deze terug te zetten. Test of een back-up ook echt bruikbaar is wanneer deze nodig is. Maak hierover bijvoorbeeld afspraken met de leverancier. Bijkomend voordeel is dat beheerders of operators al weten wat ze moeten doen als het een keer echt nodig is. Dat kan kostbare tijd besparen. Een dergelijke test is ook een uitgelezen kans om configuraties en procedures te documenteren en te toetsen op juistheid.

Opnieuw inrichten

Sommige systemen zijn zo ingericht (of slecht gedocumenteerd) dat de integriteit in het geding is als gangbare beveiligingsoplossingen zoals antivirus of hardening worden toegepast. In uitzonderlijke gevallen kan het opnieuw inrichten van zo'n systeem of omgeving uitkomst bieden. Zo'n actie kan eventueel worden gecombineerd met een poging om van meer recente of courante hardware gebruik te gaan maken. Zo kan bijvoorbeeld worden onderzocht of een applicatie die door een leverancier alleen onder Windows 2000 wordt ondersteund, op een recentere versie van Windows te installeren is. Denk ook aan een combinatie van mogelijkheden, bijvoorbeeld door toepassing van virtualisatie. Zo kan een legacy applicatie op een schoon Windows 95 besturingssysteem worden geïnstalleerd die als virtuele machine in een Windows 2003 serveromgeving actief is, op moderne hardware. Let wel, meestal is opnieuw inrichten een zeer kostbare exercitie en is er altijd de kans dat het niet lukt. Toch kan het in sommige gevallen een bruikbaar hulpmiddel zijn.

Documentatie en organisatie

Bij de bescherming van legacy systemen wordt vaak vergeten om alsnog documentatie van het systeem aan te leggen als deze niet beschikbaar is. Het resultaat is dat de gedeeltelijke kennis die wordt opgedaan door mensen die het systeem onderhouden alsnog niet wordt geborgd. Het ontbreken van duidelijke normen of richtlijnen voor het beheer van systemen of de documentatie ervan, is één van de oorzaken. Een voorbeeld van een richtlijn die kan waken over adequaat beheer van documentatie is het definiëren van een onderhoudsproces. In zo'n proces kan aandacht worden gevraagd voor het bijwerken van documentatie.

De kwaliteit van het beheer van systemen is veelal afhankelijk van de persoonlijke kwaliteiten en opvattingen van individuen. Voor vitale systemen is dit niet verstandig. Deze afhankelijkheid kan worden weggenomen door duidelijke instructies te hanteren, verantwoordelijkheden te benoemen en toe te zien op de naleving van richtlijnen.

Bewustwording en training

Informatiebeveiliging staat of valt met de bewustwording van de mensen die erbij betrokken zijn. Dat is ook het geval voor legacy systemen. Mensen die zich bewust zijn van de extra risicofactoren die voor bepaalde systemen gelden, zullen zorgvuldiger te werk gaan. En daarmee kan onbewust verkeerd handelen worden voorkomen. Juiste training van medewerkers is het belangrijkste middel om tot betere bewustwording te komen. Denk bijvoorbeeld aan verplichte (online) training voordat men toegang krijgt tot procescontrolesystemen of specifieke legacy systemen.

Conclusie

De beveiliging van legacy procescontrolesystemen is op inhoud niet heel anders dan voor courante (IT) systemen. Beveiliging van informatiesystemen, waaronder ook procescontrolesystemen, begint met een risicoanalyse. Tijdens de risicoanalyse wordt gekeken naar risicofactoren. Deze worden gewogen volgens de formule: risico = kans x effect. Op basis hiervan kan een overweging worden gemaakt om het risico te accepteren of aanvullende maatregelen te nemen.

Kijken we naar legacy systemen, dan kunnen keuzes die in het verleden zijn gemaakt ons nu parten spelen. Soms is het verstandig om de bron van het probleem aan te pakken, bijvoorbeeld door het systeem van de grond af aan opnieuw op te bouwen. Dit kan problemen met onnodig hoge gebruikersrechten voorkomen en lost vaak instabiliteitsproblemen op, die worden veroorzaakt door ongecontroleerde installatie van extra software.

Meestal volstaan andere, minder kostbare maatregelen. Deze kunnen technisch zijn, zoals een andere inrichting van het netwerk waarop de legacy systemen zijn aangesloten of toepassing van firewalls. Maar deze kunnen ook procedureel zijn, bijvoorbeeld door invoering van een verplichte training voor het gebruik van de legacy systemen.

Zoals altijd begint het beschermen van legacy systemen met het verkleinen van de kans op een verstoring. Voor het verkleinen van deze kans is een aantal effectieve maatregelen beschikbaar.

Hardening zorgt ervoor dat het aantal punten waarop een systeem kwetsbaar is tot een minimum wordt beperkt. Training of een waarschuwing in de vorm van een duidelijke sticker zorgt ervoor dat gebruikers zich bewust zijn van een verhoogd risico bij het gebruik van deze legacy systemen.

De kans op verstoringen is nooit helemaal uit te sluiten. Een goed geteste back-up en goed geïnstrueerde beheerders beperken de schade van een dergelijke verstoring . Goede (geteste) procedures, documentatie en vastlegging van configuratiegegevens zijn hierbij essentieel. Denk ook aan een veilige en, in geval van nood, bereikbare plek om back-ups te bewaren. Als aanvullende maatregel kan het raadzaam zijn om zelf reserveonderdelen of complete (zo mogelijk voor geïnstalleerde en geconfigureerde) schaduwsystemen in voorraad te houden.

Meer informatie

Beschikbare bronnen en online (Engelstalige) documenten die meer informatie over dit onderwerp bieden:

Good practice guidelines afkomstig van CPNI UK:

http://www.cpni.gov.uk/advice/infosec/business-systems/scada/

Standards & References aangereikt door het Control Systems Security Program van het Amerikaanse Department of Homeland Security:

http://www.us-cert.gov/control_systems/csstandards.html

Guide to Industrial Control Systems (ICS) Security afkomstig van NIST, USA:

http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

SP99, Industrial Automation and Control Systems Security van de International Society of Automation, USA:

http://www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

Relevante literatuur

Referenties
Centre for Protection of National Infrastructure UK. (n.d.). PROCESS CONTROL AND SCADA SECURITY: GUIDE 1. UNDERSTAND THE BUSINESS RISK. Retrieved July 19, 2011, from CPNI.gov.uk:

http://www.cpni.gov.uk/documents/publications/2008/2008024-gpg_scada_business_risk.pdf

Department of Homeland Security VS. (n.d.). Recomended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Retrieved July 19, 2011, from Control Systems Security Program:

http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

National Security Agency. (n.d.). Security Configuration Guides. Retrieved July 12, 2011, from National Security Agency:

http://www.nsa.gov/ia/guidance/security_configuration_guides/

CPNI.NL
Postadres
Postbus 96864
2509 JG Den Haag

Bezoekadres
Oude Waalsdorperweg 63
2597 AK Den Haag

T 088 866 38 61
E info@cpni.nl
I www.cpni.nl