Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Zicht op risico's van legacysystemen

Een self-assessmentmethode om de risico's van (vitale) legacysystemen in kaart te brengen

Handreiking | versie 1.1| 17 augustus 2023

Inleiding

Nederland is in hoge mate afhankelijk van het goed functioneren van ICT.[1] Incidenten met ICT-systemen kunnen grote maatschappelijke gevolgen hebben. De zogenaamde 'legacysystemen' verdienen hierbij bijzondere aandacht. Dit zijn systemen die gebouwd zijn met technologie die niet of nauwelijks meer wordt ondersteund door leveranciers en/of de eigen organisatie.

Veel van deze legacysystemen draaien al jaren uitstekend. Ze zijn ogenschijnlijk betrouwbaar en incidenten hebben zich al jaren niet voorgedaan. De keerzijde is dat het systeem zo oud is dat personeel en leveranciers niet langer de kennis hebben om dit systeem te onderhouden. Daardoor is er onvoldoende kennis binnen de organisatie aanwezig om een incident of probleem op te lossen, wanneer dat zich voordoet.

Daarnaast zijn veel legacysystemen inmiddels gekoppeld aan andere systemen of aan het internet. Deze systemen en de beveiliging ervan zijn oorspronkelijk niet ontworpen voor deze koppelingen. Hierdoor zijn legacysystemen kwetsbaarder voor stroringen of kwaadaardige activiteiten zoals sabotage of spionage. Kortom: qua beschikbaarheid, integriteit en vertrouwelijkheid zijn legacysystemen in vergelijking met modernere systemen kwetsbaarder en daarmee onveiliger.

Als het gaat om systemen bij organisaties in vitale sectoren kan deze kwetsbaarheid grote gevolgen hebben, zowel voor de eigen organisatie als voor de maatschappij. Het is dan ook van belang dat organisaties zich bewust zijn van de risico's die zich kunnen voordoen en dat zij beschikken over strategieën om risico's te verkleinen.

Om organisaties hierbij te helpen is dit self-assessment ontwikkeld. Met het doorlopen van dit self-assessment krijgt u inzicht in de kwetsbaarheden van een systeem. Het self-assessment geeft voorts inzicht in de kans op incidenten en de impact van verstoringen en levert input voor beslissingen over de toekomst: is een systeem aan vervanging toe of kunnen de kwetsbaarheden door relatief eenvoudige ingrepen worden weggenomen? Het self-assessment kan zowel door ICT- als security-experts worden gebruikt, maar biedt ook management een hulpmiddel om het benodigde inzicht te krijgen om investeringsbeslissingen te nemen. Het self-assessment beperkt zich tot een vooraf geselecteerde legacysysteem in een organisatie. Vaak werken deze systemen binnen complexe informatieketens die de organisatiegrens overstijgen. Een volledige risicoanalyse op de gehele informatieketen is aan te raden, maar ligt buiten de scope van dit self-assessment.

[1] Onder ICT verstaan we in dit kader naast gegevensverwerkende systemen ook industriële controlesystemen (ICS/SCADA) en aan SCADA gerelateerde protocollen zoals Profinet, FieldBus, ModBus, ProfiBus en CAN.

De uitkomsten van het self-assessment kunnen wel input leveren voor overleg binnen de organisatie en voor overleg met ketenpartners, leveranciers en overheden over verder onderzoek naar en opties voor het managen van risico's van legacysystemen.

Dit self-assessment is een hulpmiddel om op eenvoudige en laagdrempelige wijze inzicht te krijgen in de kwetsbaarheden en om u handelingsperspectief te bieden voor het zo veilig mogelijk maken van uw vitale legacysystemen. Het staat u vrij om het self-assessment naar eigen inzicht aan te passen op uw specifieke situatie.

Doelgroep

CISO's, security specialisten en IT specialisten

Doel van het self-assessment

Besluitvorming over legacysystemen vraagt strategische aandacht.

Voor het nemen van een verantwoorde investeringsbeslissing over een legacysysteem is het belangrijk dat u een objectief beeld krijgt van de risico's die uw organisatie loopt met de legacysystemen. Bij een laag risico kunt u beslissen tot handhaven van het systeem en blijven monitoren of de kwetsbaarheid toeneemt. Blijkt het risico hoog te zijn dan kan u beslissen tot ingrijpendere maatregelen zoals de volledige vervanging van het systeem. Naast het risico dat het systeem zelf met zich meebrengt, zult u ook moeten beoordelen hoe het risico zich verhoudt tot de belangen van uw organisatie. Door een afweging te maken tussen de belangen van de organisatie in relatie tot het risico dat het legacysysteem zelf met zich meebrengt kunt u weloverwegen besluit nemen ten aan zien van de te volgen strategie. Vervanging van een legacysysteem is vaak een risicovol en meerjarig traject dat directe strategische besturing vraagt.

De rol van het management

Het is goed om bij de strategische besluitvorming over de toekomst van informatiesystemen regelmatig geïnformeerd te worden over de risico's van legacysystemen. U kunt daarbij de volgende stappen overwegen:

1. Beslis op directieniveau over het regelmatig uitvoeren van het self-assessment als onderdeel van uw besluitvormingsproces over strategische investeringen in kritische informatiesystemen.
2. Bepaal in overleg met de proces- en systeemeigenaren voor welke systemen het self-assessment zinvol is. Dit is geen wet van Meden en Perzen, maar een collegiale inschatting voor welk systeem of voor welke systemen het self-assessment zinvol kan zijn.
3. Geef opdracht aan een team ICT- en security-experts om het self-assessment uit te voeren en de uitkomsten in termen van een onderbouwd risicoprofiel te rapporteren.
4. Laat u op basis van de uitkomsten van het self-assessement adviseren over de te volgen koers voor de toekomst van het systeem. Is een systeem aan vervanging toe of kunnen de kwetsbaarheden door relatief eenvoudige ingrepen worden weggenomen of is het risico acceptabel?

Wanneer het self-assessment gebruiken?

Voor welke organisaties?

Het self-assessment is geschreven voor (grotere) organisaties met legacysystemen.

Voor welke systemen?

Het self-assessment is toepasbaar op alle soorten ICT-systemen, ongeacht hun functie (informatieverwerking, procesbesturing), soort (frontend of backend, client, applicatie, platform, besturingssysteem, hardware, netwerk/middleware of combinatie daarvan), technologie (bijvoorbeeld programmeertaal), ontwerper of leverancier. Hoewel ook personele en fysieke beveiliging van belang zijn voor de veiligheid van ICT-systemen, wordt in dit self-assessment alleen ingegaan op aan de ICT-gerelateerde kwetsbaarheden. Ook ligt de nadruk op kwetsbaarheden en beveiligingsopties die specifiek zijn voor legacysystemen bijvoorbeeld het niet beschikbaar hebben van goede updates.

Dit self-assessment is bedoeld voor het verkrijgen van inzicht in de kwetsbaarheid van één systeem. Onder een systeem wordt hier verstaan een ICT-product en de daarmee samenhangende onderdelen. Een systeem kan uit meerdere onderdelen bestaan, zoals combinaties van hard- en software of systemen die samen één of meerdere bedrijfsfuncties ondersteunen.

Als u meerdere (vitale) legacysystemen heeft, kunt u voor ieder van deze systemen het self-assessment uitvoeren. Als bij de uitvoering van het self-assessment blijkt dat het niet mogelijk is om één gelijkluidend antwoord te geven voor verschillende delen van het systeem, kies er dan voor om het self-assessment voor maar één deel of voor elk van de delen apart uit te voeren.

Zicht op onveilige legacysystemen

Om tijdig te kunnen besluiten om verbeteringen in de beveiliging door te voeren zouden organisaties van al hun systemen in beeld moeten hebben wanneer de vertrouwelijkheid, beschikbaarheid en/of integriteit van hun systemen bedoeld of onbedoeld in het geding komen. Met andere woorden: wanneer een systeem onveilig wordt. Daarnaast dient ook helder te zijn welke van deze systemen legacysystemen zijn.

Het is vervolgens nuttig om gestructureerd in kaart te brengen hoe veilig het legacysysteem is en welke opties reëel zijn om de belangen van de bedrijfsvoering – en zeker voor vitale organisaties ook de samenleving – te borgen. Concreter zouden systeemeigenaren in ieder geval over moeten gaan tot nadere analyse als meerdere van de onderstaande situaties aan de orde zijn:

- Het systeem ondersteunt vitale processen voor de eigen organisatie, andere organisaties of de maatschappij.
- Het systeem verwerkt vertrouwelijke informatie (denk bijvoorbeeld aan gegevens die vallen onder de Wet bescherming persoonsgegevens).
- Het systeem kent koppelingen met andere systemen.
- Het systeem is gebouwd met niet meer ondersteunde technologie.
- Incidenten met het systeem op het gebied van vertrouwelijkheid, beschikbaarheid of integriteit nemen toe en kunnen niet goed meer worden opgelost.

- Het onderhoud van het systeem lijkt 'kunst- en vliegwerk' te zijn geworden.
- Documentatie over het systeem ontbreekt.
- Voor het systeem cruciale medewerkers verlaten de organisatie.
- Er hebben zich grote ICT- of organisatieveranderingen rondom het systeem voorgedaan.
- Externe ondersteuning van het systeem of het aantrekken van nieuwe, eigen medewerkers voor de ondersteuning van het systeem is problematisch geworden.
- Specialisten horen van steeds meer hacks of hiccups op vergelijkbare systemen bij andere organisaties.

Deze situaties zijn indicaties dat de veiligheid van een legacysysteem niet zonder meer gewaarborgd is en dat het raadzaam is om het systeem verder te onderzoeken.

Dit self-assessment is bedoeld als een hulpmiddel bij het nader onderzoeken van het systeem, het bespreken van de (on)veiligheid van een systeem binnen de organisatie en het nemen van beslissingen over de toekomst van het systeem.

Het verdient aanbeveling dit self-assessment periodiek uit te voeren voor alle legacysystemen om zo een actueel beeld te houden. Ook alle systemen die volgens medewerkers onveilig zouden kunnen zijn, kunnen met dit self-assessment verder worden onderzocht.

Het self-assessment

Als er een beeld is van de legacysystemen binnen de organisatie en er is een keuze gemaakt voor welke systemen het self-assessment wordt uitgevoerd, is het van belang om bij de uitvoering de volgende factoren in het oog te houden:

- Management commitment.
  Stel vast wie de eigenaar van het legacysysteem is. Dit is degene die eindverantwoordelijk is en besluiten kan nemen. Zorg voor duidelijke afspraken met het senior management over het belang van het self-assessment, de inzet van resources en de wijze van terugkoppeling en verder behandeling van het self-assessment.
- Organiseer de uitvoering.
  Stel vast wie het proces van het self-assessment gaat begeleiden (procesbegeleider). De eigenaar van het legacysysteem kan deze taak delegeren. De procesbegeleider zorgt ervoor dat alle relevante functionarissen woorden betrokken. Naast ICT- en security-specialisten is het ook verstandig om de gebruikers van het systeem te betrekken en bijvoorbeeld de functionarissen die de contacten onderhouden met leveranciers. Het verdient de aanbeveling om het self-assessment met alle relevante functionarissen gezamenlijk doorlopen. Zo kan de benodigde dialoog gevoerd worden en kunnen medewerkers elkaar's input verrijken waardoor een completer beeld ontstaat. Indien nodig kunt u het self-assessment opsplitsen in meerdere sessies. Verzamel alle documentatie en leg gesprekken en besluiten vast.
- Periodiek herhalen.
  Het self-assessment is bedoeld als een zogenaamde 'learning loop' (Plan-Do-Check-Act): voer het assessment eens in de zoveel tijd uit en verbeter zo de veiligheid van uw systemen steeds verder. En bedenk dat wat nu nog geen legacy is, dat over een aantal jaren waarschijnlijk wel zal zijn. Het self-assessment kan daarom ook kennis en bewustzijn genereren die maakt dat u bij het inkopen of aanpassen van nieuwe systemen toekomstige legacyproblemen voor kunt zijn. Integreer het self-assessmnet in het lifecyclemanagement van uw organisatie.

Onderdelen van het self-assessment

Het self-assessment bestaat uit drie onderdelen:

1. Het bepalen van de veiligheid;
2. Het bepalen van de impact van verstoringen;
3. Het bepalen van het risicoprofiel en de mitigatie strategie.

In de volgende hoofdstukken worden de drie onderdelen uitgewerkt. De vragen en de uitleg van de bijbehorende scores kunt u terugvinden in het gelijknamige Excelbestand.

Deel 1 – Bepalen veiligheid

De veiligheid van een legacysysteem wordt bepaald door technische aspecten, maar ook door de context rondom het systeem. Is het systeem beveiligd tegen actuele aanvallen, zijn er voldoende maatregelen getroffen om te voorkomen dat mensen die niets in het systeem te zoeken hebben toch toegang hebben en zijn er voldoende mogelijkheden om het systeem up-to-date te houden en aan te passen naar actuele eisen en wensen? Maar ook: zijn er nog mensen binnen de organisatie die weten hoe het systeem werkt en wat er moet gebeuren als het systeem crasht?

In dit eerste deel van het self-assessment is een aantal vragen opgenomen dat u helpt inzicht te krijgen in de veiligheid van het systeem. Deze fase eindigt met een samengevat beeld van de veiligheid van het systeem voor het (senior) management.

Vragen

In het self-assessment staan vragen waar een score aan gegeven kan worden. Hoe lager de score bij de vragen in dit deel van het assessment, hoe groter de kans dat het legacysysteem niet veilig is.

Deze score geeft ook een indicatie over de waarschijnlijkheid dat verstoringen kunnen optreden.

Soms kan een zwakke beheersmaatregel in het ene onderdeel gecompenseerd worden door een sterke beheersmaatregel in een ander onderdeel. Probeer bij de beantwoording van de vragen wel zo veel mogelijk per onderdeel een score te geven zonder daarbij reeds compenserende maatregelen mee te wegen. Bij het opstellen van het totaalbeeld kan vervolgens met behulp van wegingsfactoren of door het geven van een toelichting aangegeven worden in welke mate lage scores op het ene onderdeel gecompenseerd worden door een hogere score in een ander onderdeel.

Waarschijnlijkheid van het optreden van verstoringen

Hoewel ervoor is gekozen om in het self-assessment geen specifieke vragen over de waarschijnlijkheid van verstoringen van het systeem op te nemen, verdient dit onderwerp wel de aandacht. In algemene zin is het uiteraard zo dat hoe lager uw systeem in dit hoofdstuk heeft gescoord op veiligheid, hoe groter de kans is dat verstoringen optreden.

Verstoringen kunnen het gevolg zijn van toeval of onbewuste fouten van medewerkers. Ook bij een moedwillige verstoring is het soms toeval dat juist uw organisatie en niet een andere organisatie het doelwit wordt van bijvoorbeeld criminelen. Omdat internet gekoppelde systemen automatisch worden gescand en afgetast is de dreiging van infectie via het internet een permanent aanwezige dreiging. Daarom is bij systemen die direct en indirect aan internet gekoppeld zijn de waarschijnlijkheid van verstoring aanzienlijk en moet de weerbaarheid passend zijn.

Juist vitale organisaties vormen een interessant doelwit voor zware criminelen, terroristen en buitenlandse inlichtingendiensten. Dit zijn tegenstanders hebben veel technische middelen om verstoringen te veroorzaken. Hierdoor is de waarschijnlijkheid van verstoring van belangrijke systemen van vitale organisaties dus hoger.

De waarschijnlijkheid van verstoringen is en blijft een inschatting, waarbij de werkelijkheid positiever of negatiever kan uitpakken. Als zich met regelmaat incidenten voordoen of wanneer er sprake is van een duidelijke toename van incidenten, kan dit erop wijzen dat het systeem onveiliger wordt. Andersom is een systeem waarmee nauwelijks incidenten zijn niet per se veilig. Aanwezige kwetsbaarheden kunnen immers ineens leiden tot (ernstige) verstoringen.

Toelichting vragen deel 1

Hieronder worden onderwerpen waar de vragen die in deel 1 van het self-assessment betrekking op hebben, toegelicht.

Vraag 1 – Ontwikkeling

Om eventuele kwetsbaarheden in de beveiliging te kunnen repareren of additionele beveiligingsmaatregelen aan te kunnen brengen, dient de software van zowel de clientomgeving en de applicatieomgeving als onderliggende componenten aangepast te kunnen worden. Om wijzigingen in het systeem op een gecontroleerde wijze aan te brengen, te testen, te accepteren en op gecontroleerde wijze in productie te kunnen brengen, is het aanwezig zijn van een gescheiden ontwikkel-, test-, acceptie- en productieomgeving (OTAP) een vereiste.

In legacysystemen is het systeemontwerp soms weinig gestructureerd en is het niet ongebruikelijk dat delen van de businessfunctionaliteit hard gecodeerd in de software zijn vastgelegd. Wanneer er niet voldoende kennis of documentatie van het ontwerp en de functionaliteit van de applicatie aanwezig is, neemt het vermogen tot aanpassing van de applicatie af en komt het herstellend vermogen bij verstoringen in gevaar.

Vraag 2 – Governance

Voor de governance en het beheer van alle systemen is het noodzakelijk dat de hiervoor benodigde taken, rollen en bevoegdheden eenduidig belegd zijn binnen de eigen organisatie en dat hierover, zo nodig, goede afspraken zijn gemaakt met de leverancier.

Vraag 3 – Lifecyclemanagement

Het is van belang om continu kritisch te kijken naar de legacysystemen binnen de organisatie en zorg te dragen voor een goed doordacht lifecycle management.

Vraag 4 – Incidenten

Het aantal incidenten dat zich inmiddels heeft voorgedaan bij het systeem, geeft een indicatie over de betrouwbare werking van dat systeem. Dit neemt niet weg dat ook een systeem waar zich geen eerdere incidenten hebben voorgedaan ineens kan falen.

Vraag 5 – Beheer

De kennis over het systeem kan verwateren naarmate een systeem langer in gebruik is. Dit kan zowel binnen de eigen organisatie als bij de leverancier gebeuren. Hierdoor is het lastiger om adequaat beheer in te richten voor het systeem. Dit heeft gevolgen voor de weerbaarheid van het systeem. Wanneer de beschikbare beheerkennis bij specialisten afneemt, neemt het belang van voldoende en actuele documentatie alleen maar toe. Daarnaast is het hebben van de vereiste documentatie een goede indicator van de kwaliteit van het beheer. Van belang is hierbij een goede afstemming tussen de operationele beheertaken en de tactische beheertaken.

Vraag 6 – Wijzigingen

Het aantal wijzigingen in een systeem en de mate waarin een systeem wordt gebruikt waarvoor het ooit bedoeld is, zegt iets over kwetsbaarheid. Regulier (adaptief en

correctief) onderhoud verlaagt de kwetsbaarheid van het systeem. Grootschalige aanpassingen en het toevoegen van extra functionaliteiten waar het systeem niet voor gemaakt is en niet op berekend is kan de kwetsbaarheid verhogen.

Vraag 7 – Externe ondersteuning

Hoe afhankelijker een systeem is van externe partijen (leveranciers of ICT-dienstverleners), hoe beter de afspraken moeten zijn over onderhoud en beheer. Afspraken gelden met name voor het tijdig oplossen van beveiligingslekken en het snel reageren op kritische en beveiligingsincidenten. Wanneer de ondersteuning van het systeem door de externe partijen wegvalt ontstaat er vanzelfsprekend een kwetsbare situatie. Afspraken dienen dus ook oog te hebben voor toekomstige situaties.

Vraag 8 – Beveiliging

Onderdelen van systemen die via een intranet of het internet te benaderen zijn, dienen regelmatig onderzocht te worden op kwetsbaarheden. Het inventariseren van kwetsbaarheden in de beveiliging vergt diepgaande specialistische kennis van zowel informatiebeveiliging als van de gebruikte protocollen, technologieën en algoritmen. Wanneer het systeem kwetsbaarheden in de beveiliging bevat, dienen deze spoedig gerepareerd te worden middels patches of systeemaanpassingen.

Naarmate de tijd verstrijkt, verouderen beveiligingsalgoritmen, protocollen en technologieën of worden er onoplosbare kwetsbaarheden gevonden. Protocollen die tien jaar geleden breed worden toegepast, zijn vandaag onveilig.

Legacysystemen zijn ontworpen met de kennis die toen beschikbaar was ten aanzien van beveiliging. Gevolg hiervan is dat ze vaak niet bestand zijn tegen actuele aanvalstechnieken. Vaak zijn legacysystemen niet in staat om modernere beveiligingsmaatregelen zoals multifactor authenticatie of het verlenen van veilige toegang op afstand toe te passen. Als een legacysysteem encryptiemogelijkheden biedt, bestaat de kans dat de geboden technologie, algoritmen en gebruikte sleutellengtes niet meer volstaan.

Vraag 9 – Koppelingen

De mate waarin het systeem wordt blootgesteld aan dreigingen is in belangrijke mate afhankelijk van de koppelingen die het systeem heeft met andere systemen in de organisatie en buiten de organisatie.

Hoewel het gebruik van internet voor een of meerdere van deze koppelingen het dreigingsniveau aanzienlijk doet toenemen, kunnen ook interne koppelingen en koppelingen met andere organisatie bedreigingen vormen.

Toegang tot het systeem via de diverse koppelingen moet zo veel mogelijk beperkt worden tot uitsluitend die gebruikers en systemen waarvoor de koppeling bedoeld is. Gebruikers van de koppelingen dienen zich te authentiseren en het netwerkverkeer over de koppeling dient beveiligd te zijn tegen ongewenste modificatie of afluisteren. Ook dient de beschikbaarheid van de koppelingen beschermd te zijn tegen uitval van netwerkcomponenten en eventuele aanvallen gericht op de beschikbaarheid van het systeem.

Bij legacysystemen is er tijdens het ontwerp en de implementatie veelal geen rekening gehouden met actuele aanvalstechnieken. Waardoor deze systemen daar mogelijk kwetsbaarder voor zijn.

Vraag 10 – Uniciteit

Enkelvoudig uitgevoerde (unieke) systemen zijn vatbaarder voor dreigingen en kwetsbaarheden. Er is bij enkelvoudige systemen vaak onvoldoende redundantie en externe ondersteuning beschikbaar. Redundantie van het systeem (‘dubbel uitvoeren’) of alternatieve werkwijzen en ‘workarounds’ in de bedrijfsprocessen wanneer

het systeem uitvalt kunnen de afhankelijkheid in de organisatie van het systeem beperken.

Zeker als het gaat om PLC's (Programmable Logic Controllers), embedded en/of procesbesturingssystemen (ICS/SCADA) in de industrie is er vaak geen uitwijk mogelijk (immers: één onderdeel met één proces). Daarnaast is het uitvoeren van ketentesten zeer complex bij dergelijke systemen: legacy-software gedraagt zich onvoorspelbaar als het wordt geconfronteerd met nieuwe testtechnieken, met als risico dat het systeem (onherstelbaar) beschadigd wordt.

Vraag 11 – Client

In legacysystemen is het niet ongebruikelijk dat de server-login credentials op de client opgeslagen worden. Het gevolg is dat de kans bestaat dat deze credentials worden ontvreemd en misbruikt worden voor ongeautoriseerde toegang tot de server.

Daarnaast is het in legacysystemen ook niet ongebruikelijk dat er, bijvoorbeeld om performanceredenen, (gevoelige) bedrijfsinformatie op de client wordt opgeslagen. Wanneer deze clientomgeving niet afdoende beveiligd is of bijvoorbeeld middels een verloren of gestolen laptop buiten de invloed van de organisatie raakt, bestaat het risico dat er informatie uitlekt en mogelijk misbruikt wordt.

Wanneer de client ontworpen, gebouwd en geïmplementeerd is zonder specifieke aandacht voor "veilig programmeren", kan er mogelijk, met aanvallen op bijvoorbeeld de gebruikersinterface, ongeautoriseerde toegang verkregen worden tot bedrijfsinformatie in het systeem. Bij het ontwerp en de bouw van de client dienen de in de industrie bekende programmeerfouten (zoals bijvoorbeeld beschreven in SANS 25[2]) die kwetsbaarheden kunnen veroorzaken vermeden te worden en dient de gebruikersinterface getest te worden op het weerstaan van de aanvallen gebaseerd op in de industrie bekende kwetsbaarheden (zoals onder andere beschreven in de OWASP-top 10[3]). Wanneer er voor de toegangsbeheersing tot bedrijfsinformatie wordt vertrouwd op beveiligingsmaatregelen in de clientsoftware, dan dient voorkomen te worden dat er toegang tot de server verkregen kan worden met andere tools of software dan de bedoelde clientsoftware.

Vraag 12 – Applicatie

Het aanwezige autorisatiemodel dient te voorzien in implementatie van het "need-to-know" principe. Dit principe houdt in dat iedere gebruiker toegang krijgt tot die informatie die nodig is voor de uitvoering van zijn of haar taken en niet meer dan dat. In legacy-applicaties is het aanwezige autorisatiemodel niet altijd voldoende fijnmazig om dit principe te kunnen realiseren. Om de beheers inspanning te beperken zijn soms niet alle aanwezige mogelijkheden in het autorisatiemodel benut om tot een voldoende fijnmazige inrichting van de autorisaties te komen.

Voorts is het in legacysystemen niet ongebruikelijk dat er voor toegang tot de database volledig wordt vertrouwd op de aanwezige beveiligingsmaatregelen in de client of de applicatie. Hierdoor kan er mogelijk buiten de applicatie om directe toegang tot de database verkregen worden.

Wanneer de programmabibliotheken waar de applicatie uit opgebouwd is niet afdoende beveiligd zijn tegen ongeautoriseerde aanpassingen, kunnen de applicatiefunctionaliteit en eventuele beveiligingsmaatregelen ongewild aangepast worden, waardoor inbreuken op de beveiliging kunnen optreden.

[2] Top 25 Software Errors | SANS Institute

[3] OWASP Top Ten | OWASP Foundation

Vraag 13 – Systeemsoftware

Onder systeemsoftware wordt verstaan software zoals besturingssystemen, databases, middleware enzovoorts.

Leveranciers geven vaak geen updates meer uit voor legacysystemen en de daarbij behorende systeemsoftware. Als gevolg daarvan worden kwetsbaarheden in de beveiliging van deze systeemsoftware mogelijk niet meer (tijdig) gerepareerd. Hierdoor zal de mate van kwetsbaarheid van het systeem als geheel over de tijd toenemen. Wanneer de bedrijfsinformatie op het niveau van de systeemsoftware niet specifiek is afgeschermd, bestaat het risico van ongeautoriseerde toegang tot bedrijfsinformatie vanuit de beheer-of systeemomgeving.

In sommige legacysysteem software zijn de mogelijkheden voor toegangsbeheersing tot het "file system" en het "job entry system" niet optimaal of lastig te configureren. Hierdoor ontstaat het risico van ongeautoriseerde toegang op bestandsniveau of kunnen ongeautoriseerde processen gestart worden.

Vraag 14 – Hardware

Wanneer de hardware vanwege kostenafwegingen of vanwege een beperkte beschikbaarheid van vervangende hardware niet tijdig vervangen wordt, ontstaan risico's ten aanzien van de beschikbaarheid van het systeem. En wanneer er sprake is van beperkte beschikbaarheid van vervangende hardware of de benodigde hardware geheel niet meer leverbaar is, ontstaan risico's ten aanzien van de continuïteit van het systeem.

Voorts bestaat de mogelijkheid dat er ten tijde van bouw voor de beveiliging is vertrouwd op aanwezige hardwarematige of infrastructurele voorzieningen, die inmiddels gewijzigd zijn waardoor eerdere aannames aangaande de beveiliging niet meer valide zijn. Zo kan er bijvoorbeeld ooit vertrouwd zijn op een fysieke verbinding met een domme terminal, maar is het systeem inmiddels via een IP-koppeling op het netwerk beschikbaar gemaakt. Ook zit heeft consequentie voor de beveiliging.

Bepalen veiligheidsprofiel

Op basis van de vragen in deel 1 kunt u een samengevat en overzichtelijk beeld schetsen van het veiligheidsprofiel van een legacysysteem om het (senior) management te informeren.

Voor ieder van de 14 onderdelen van het veiligheidsprofiel kunnen de scores op de verschillende vragen gemiddeld worden. Hierdoor ontstaat per onderdeel een totaalscore tussen 1 en 5. De resultaten van het self-assessment worden ook weergegeven in een radardiagram. Vanzelfsprekend wegen niet alle onderdelen van het veiligheidsprofiel even zwaar. De organisatie staat vrij om zelf wegingsfactoren voor de verschillende onderdelen aan te geven.

Op het moment dat blijkt dat u op meerdere onderdelen een score behaalt van 3 of lager dan is het raadzaam te overwegen de veiligheid van het systeem te verbeteren. Indien slechts op één of enkele onderdelen een kwetsbaarheid is aangetroffen, dan verdient het aanbeveling de aandacht te concentreren op deze onderdelen en daar gerichte verbeteringen in aan te brengen. Een kwetsbaarheid in één of enkele onderdelen van het systeem hoeft immers nog niet te betekenen dat het gehele systeem kwetsbaar is. Hoe lager de veiligheid van het systeem, hoe groter de kans op het optreden van een verstoring. Ook hier is het verstandig het self-assessment te bezien binnen de context van het risicomanagementproces.

Deel 2 – Impact van verstoringen

Voor de vraag in hoeverre de onveiligheid van een systeem een risico opleveren is het ook van belang de vraag te stellen welke maximale impact een verstoring van het systeem heeft op de maatschappij. Daarom kijken we in dit onderdeel naar de impact van de verstoring van het systeem. De exacte aanleiding voor de verstoring doet wat dit betreft niet ter zake. We gaan uit van een 'all hazard benadering', waarbij alleen de maximale impact voor de maatschappij wordt bezien. Bij de beantwoording van de vragen kunt u dan ook voor het gemak uitgaan van volledige uitval of grootste inbreuk op de vertrouwelijkheid of integriteit.

Met dit onderdeel van het self-assessment kunt u het geheel van effecten inschatten, inclusief de effecten op andere ICT-systemen, de rest van de eigen organisatie, de directe impact op de maatschap- pij en keteneffecten op andere organisaties. Bij een backend systeem lijkt de directe impact van een verstoring op de buitenwereld op het eerste gezicht beperkt. Om de impact van een dergelijk systeem in te schatten kunt u bij de beantwoording van deze vragen het 'domino-effect' meenemen. Schat hierbij in wat de schadelijke impact is van aantasting van andere (ICT-)systemen als direct en onvermijdelijk gevolg van aantasting van het onderzochte legacysysteem.

Bij het invullen van dit onderdeel van het self-assessment kan informatie nodig zijn van andere afdelingen dan de ICT-afdeling. Hou daar ook rekening mee wanneer u aan de start van het self-assessment bepaald welke mensen u wilt betrekken bij het assessment. Het verdient de aanbeveling deze mensen te betrekken bij het gehele proces zodat zij een duidelijk beeld hebben van het betreffende legacysysteem en de mogelijke onveiligheden.

Toelichting vragen deel 2

De maximale impact van een verstoring kan bestaan uit verschillende factoren. Voor dit self-assessment zijn deze factoren vertaald naar een aantal vragen. De factoren worden hieronder toegelicht. Hoe lager de score op een vraag is, hoe groter het belang van het systeem en hoe groter de impact bij een verstoring.

Vraag 15 – Kosten van gevolgschade

Aantasting van een systeem kan gevolgschade met zich meebrengen, zowel voor de organisatie zelf als voor de maatschappij. Volledige uitval (landelijk) van een vitaal systeem kan leiden tot flinke financiële schade bij de organisatie en zelfs tot faillissement, met alle gevolgen van dien. Ook kan uitval leiden tot schadeclaims van gebruikers (burgers). Bij deze vraag wordt gekeken naar de geschatte kosten van volledige uitval van het systeem.

Vraag 16 – Verstoring van het dagelijks leven

Hierbij moet worden gekeken hoeveel en voor hoe lang eigen medewerkers of burgers in de samenleving ernstig worden gestoord om hun normale activiteiten te ondernemen. Daarbij kan worden gedacht aan het kunnen werken binnen de vitale organisatie die het betreft, naar werk of naar school gaan, telefoneren, internet gebruiken.

Vraag 17 – Maatschappelijk onrust

Hierbij wordt gekeken naar in welke mate en hoe lang Nederlanders boos of bang zijn. Hierbij kan ook worden gekeken naar (ernstige) aantasting van het vertrouwen in de organisatie. Denk hierbij bijvoorbeeld aan het door hacks verliezen van data en ernstige schendingen van privacy van burgers.

Vraag 18 – Doden en gewonden

Hierbij wordt gekeken naar in welke mate bij verstoringen van een systeem doden of gewonden vallen. Denk hierbij bijvoorbeeld aan de gevolgen die zich kunnen voordoen bij verstoringen van systemen bij kerncentrales, vergiftiging van het drinkwater door moedwillige verstoringen in de waterzuivering etc.

Samengevat beeld van de impact

Op basis van de bovenstaande vragen kunt u een samengevat beeld schetsen van de impact van een verstoring van het systeem om het senior management te informeren. Voor ieder van de 4 factoren om de impact te bepalen kunnen de scores op de verschillende vragen gemiddeld worden.

Deel 3 – Risicoprofiel en risicomitigatie

Dit onderdeel geeft u een handreiking voor het bepalen van het risicoprofiel van het legacysysteem en het bepalen van mogelijke strategieën om risico's te mitigeren. Onder risicoprofiel wordt verstaan de hoogte van het risico op basis van het veiligheidsprofiel uit onderdeel 1 en de impact uit onderdeel 2.

Bepalen risicoprofiel

Op basis van de scores op de vragen uit onderdeel 1 en 2 kan het risicoprofiel van het legacysysteem worden opgesteld. Zoals al eerder aangegeven staat het u vrij om bepaalde wegingsfactoren aan scores mee te geven die een goede weergave zijn voor uw organisatie.

De totaalscores voor het veiligheidsprofiel van het legacysysteem kan zijn:

1. Niet/onbekend
2. Zeer beperkt
3. Beperkt
4. Voldoende
5. Ruim voldoende/ niet relevant

Hoe lager de score, hoe onveiliger het legacysysteem waarschijnlijk is.

De totaalscores voor impact lopen ook van 1 tot en met 5. Waarbij de impact bij een score van 1 het hoogst is.

De scores kunnen geplot worden op onderstaand schema waardoor een overall beeld ontstaat van het legacysysteem; het risicoprofiel. Een hoge score op het veiligheidsprofiel en de impact, leidt tot een zeer laag risicoprofiel. Andersom leidt een lage score tot een zeer hoog risicoprofiel.

In totaal zijn er 5 risicoprofielen:

ZL – Zeer laag

L – Laag

M – Midden

H – Hoog

ZH – Zeer hoog.

Risicoprofiel legacysysteem:

Impact					
5	M	L	L	ZL	ZL
4	M	M	L	L	ZL
3	H	M	M	L	L
2	H	H	M	M	L
1	ZH	H	H	M	M
	1	2	3	4	5 **Veiligheid**

Op basis van het risicoprofiel kunt u een risicoafweging maken en bepalen welke strategie u gaat inzetten voor het betreffende legacysysteem.

Bij de risicoafweging zet de (management)verantwoordelijke(n) het risico van het legacysysteem af tegen de overige doelen van de organisatie en de nadelen (ook de kosten) van opties om de onveiligheid van het systeem te verminderen.

Als het risico laag is of er een nieuwe versie of een vervanger van het systeem verwacht wordt dan kan het risico geaccepteerd worden. Overwegingen die daarbij een rol spelen zijn:

- Is het maatschappelijk verantwoord en aanvaardbaar om het risico te accepteren?
- Valt het risico binnen de grenzen van een wettelijke verplichting?
- Zijn er voldoende financiële reserves om eventueel op incidenten te reageren?

Als het risico acceptabel is (zeer laag/ laag), is het niet noodzakelijk om direct mitigerende acties te (laten) nemen. Hierbij is het wel zaak om het risico door de verantwoordelijke leiding te laten vastleggen en accepteren (eigenaarschap en accountability) en vervolgens continu te monitoren.

Bij een risicoprofiel midden zal (senior) management een afweging moeten maken over de te volgen mitigatiestrategie. Naast een inschatting van het risico wordt ook bepaald in welke mate het risico als acceptabel wordt gezien en welke kosten gemaakt kunnen worden om de risico's te mitigeren.

Bij een hoog of zeer hoog risico zal een passende mitigatiestrategie moeten worden opgesteld en uitgevoerd om het risico minstens terug te brengen naar een acceptabel niveau. De voortgang van de strategie moet worden gemonitord. Ook rapportage hierover aan het (senior) management is raadzaam zodat zij in staat zijn de juiste besluiten te nemen en waar nodig bij te sturen.

Voor alle legacysystemen geldt dat het raadzaam is om de (management)aandacht voor het legacysysteem ook te houden na het self-assessment, waardoor het legacysysteem periodiek wordt meegenomen in rapportages, onderzoeken, beheerbudgetten, overleggen etc. Dit voorkomt onaangename verrassingen in de toekomst.

Mogelijke mitigatiestrategieën

De onderstaande strategieën zijn voor legacysystemen denkbaar, al kunnen sommigen niet passen bij het specifieke systeem dat wordt bekeken. De strategieën staan gerangschikt van minst ingrijpend naar meest ingrijpend. Dit is waarschijnlijk ook in volgorde van oplopende kosten en van op korte termijn tot slechts op langere termijn te realiseren. Bij alle mitigatiestrategieën zal bepaald moeten worden hoeveel de desbetreffende strategie bijdraagt aan het verminderen van de risico's en welke kosten daarvoor redelijkerwijs gemaakt kunnen worden.

Detectie

Door aanvullende detectiemaatregelen te nemen, kan er sneller gereageerd worden op verstoringen. Denk hierbij aan actieve, softwarematige monitoring van het systeem

Beheer

Verder kunt u de kans op incidenten verminderen door een aantal randvoorwaardelijke en beheersmatige zaken op orde te brengen en te houden. Denk hierbij aan zaken als:

- Kennis: voer een beleid gericht op het behouden of opbouwen van kennis van het legacysysteem en de gebruikte technologieën. Koester de mensen die deze kennis nog bezitten, zorg voor een tijdige overdracht en vastlegging van deze kennis en neem zo nodig mensen die deze kennis (nog) bezitten (opnieuw) in dienst. Als u het beheer heeft uitbesteed, zult u nog steeds veel over het systeem moeten weten. Dit zowel om adequaat te reageren op incidenten als om bij verdere ontwikkeling of vervanging van het systeem op veiligheid te kunnen sturen.
- Ondersteuning: communiceer proactief met uw leverancier over de periode waarover u nog ondersteuning van het systeem en de gebruikte technologieën mag verwachten en maak hier goede afspraken over. Stel u op de hoogte van de bij de leverancier nog aanwezige kennis en de kwaliteit van de ondersteuning die u nog geboden wordt.
- Eigenaarschap: zorg voor eigenaarschap in de business. Enerzijds door voor systemen eigenaren aan te wijzen en anderzijds in de vorm van een verantwoordelijke functionaris die toezicht houdt op de beheerprocessen, waaronder change-, configuratie-, incident- en patchmanagement.

- Business – IT afstemming: zorg ervoor dat verdere ontwikkeling en gebruik van het systeem goed worden meegenomen in de ontwikkeling van plannen en besluitvorming van de business afdelingen, andere IT-projecten, het (senior) management etc. Voorkom dat het systeem onveiliger wordt door omgevingsveranderingen.

Respons

Het risico kunt u tevens verminderen door u goed voor te bereiden op een adequate incidentrespons. Denk hierbij aan het opstellen van een incidentresponsplan waarin alle belangrijke aspecten zijn geadresseerd, het inrichten van een incidentresponsteam met de benodigde kennis en mandaat en het testen en actueel houden van het responsplan en het oefenen met alle betrokkenen. Dit geldt uiteraard niet alleen voor legacysystemen.

Herstel

Een andere mogelijkheid is het voorbereiden van de technische randvoorwaarden voor herstel, zoals back-up en restore, reserve-hardware, tools om het systeem te benaderen etc.

Afschermen

Een andere strategie is het inzetten op afscherming van het systeem. Beperk de toegang tot het systeem tot het hoogstnoodzakelijke, schakel onnodige functies en poorten op de systemen uit, pas veilige configuratiebaselines toe, breng de laatste patches aan etc. Daarnaast kunt u de netwerktoegangspaden beperken tot uitsluitend die toegangspaden die nodig zijn voor de legitieme gebruikers van het systeem en deze toegangspaden beschermen middels zaken als ACL's, firewalls en/of een DMZ.

Opdelen

Om de potentiële impact van verstoringen te verkleinen, kunt u het systeem (of delen daarvan) opdelen (zoneren) in afzonderlijke delen.

Beschermen

Nog een andere strategie is het verhogen van de bescherming van het systeem. Dit kan op verschillende manieren:

- Virtuele patches: breng extra bescherming aan door upstream in de toegangspaden naar de systemen firewalls en/of gateways op de applicatielaag op te nemen die voor het systeem relevante aanvallen filteren c.q. blokkeren.
- Virtualiseren: migreer het systeem naar een virtuele serveromgeving om de afhankelijkheid van specifieke hardware te verminderen.
- Isoleren: scherm het systeem als geheel af door er op applicatieniveau een veilige "wrapper" omheen te bouwen, via welke alle koppelvlakken kunnen verlopen.

Upgraden

U kunt ook overwegen het risico te verminderen door vervanging van de kwetsbare operating systemen, protocollen, technologieën en algoritmen en het geschikt maken van de applicatie voor de gemoderniseerde infrastructuur (upgraden). In deze strategie worden delen van het systeem of het hele systeem op een hoger veiligheidsniveau gebracht.

Uitfaseren

Faseer delen van het systeem uit door de functionaliteit die afhankelijk is van kwetsbare componenten onder te brengen in andere (veilige) systemen.

Procesherontwerp

Herontwerp bedrijfsprocessen zodanig dat de noodzaak voor delen van het systeem komt te vervallen en delen van het systeem uitgezet kunnen worden. Hierbij kan worden gedacht aan het anders uitvoeren van primaire functies van het systeem, maar ook aan het niet meer als deel van het systeem laten uitvoeren van aansturings-, rapportage- of controleprocessen.

Vervangen

Bouw het systeem volledig opnieuw op basis van moderne technologie en voorzie het systeem van passende beveiligingsmaat- regelen. Naast het vervangen van het systeem kunt u ook delen van het systeem (bijvoorbeeld een bepaalde hardwarelaag) of rand- apparatuur vervangen.

Besluitvorming

Op basis van de uitkomsten van het self-assessment in combinatie met de hierboven genoemde mitigatiestrategieën, kunt u (senior) management een goed beeld geven hoe de risico's te beheersen. Door bewust na te denken over de toepasbaarheid van de strategieën in relatie tot risico's en kosten, wordt het eenvoudiger voor het (senior) management om een goede beslissing te nemen over het legacysysteem.

Bij het nemen van een besluit door het (senior) management kunnen de volgende factoren een rol spelen:

- Risico-acceptatie: voor het maken van een goede afweging is het van belang te bepalen hoeveel risico de organisatie wil en kan lopen. Bij deze overwegingen kunnen compliance, wet- en regelgeving, media-aandacht bij incidenten, relaties met klanten, afnemers en overheden een rol spelen.
- Planvorming: is er een realistisch plan en is er voldoende capaciteit, kennis en kunde beschikbaar voor de uitvoering,
- Risico van transitie: vooraf moet worden vastgesteld of de huidige risico's daadwerkelijk hoger zijn dan de risico's na uitvoering van de mitigatiestrategie.
- Transitieperiode: welke maatregelen er ook gekozen worden, het (senior) management moet goed in beeld hebben welke tussentijdse maatregelen getroffen worden en wat hier voor nodig is (mensen en middelen).
- Nieuwe technologieën: een inschatting van de kans dat zich in de nabije toekomst nieuwe technologieën aandienen die makkelijkere strategieën mogelijke maken, kan behulpzaam zijn bij de vraag welke maatregelen passend zijn. Daarbij moet ook in ogenschouw genomen welke tussentijdse maatregelen nodig zijn.
- Afbouwproces: als verwacht kan worden dat de bedrijfsprocessen die het systeem uitvoert of ondersteunt in de voorzienbare toekomst door de organisatie zullen worden gestoptof afgebouwd, kan dit een reden zijn om ondanks de onveiligheid en het risico geen verregaande maatregelen te nemen. Ook hierbij moet in ogenschouw worden genomen of tussentijdse (lichtere) maatregelen genomen moeten worden.

Tot slot

Geen enkel systeem staat op zichzelf. Doordat de maatschappij steeds meer gedigitaliseerd is, zijn systemen steeds meer met elkaar verbonden. Dit geldt ook voor legacysystemen. Om een goed beeld te krijgen van de risico's die uw organisatie als geheel loopt is het verstandig een gedegen risicomanagementproces in te richten waarin u periodiek op strategisch, tactisch en operationeel niveau kijkt naar de risico's die u loopt. Dit stelt u in staat de belangen of kroonjuwelen van uw organistie goed te beschermen en prioriteiten te stellen om te komen tot een passend niveau van weerbaarheid voor uw organisatie. Dit self-assessment kan een intergraal onderdeel vormen van het risicomanagementproces van uw organisatie.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl
Augustus 2023