Auteurs: Jessica Maes is Programmamanager Versterken Cyberweerbaarheid in de Watersector, bereikbaar via jessica.maes@minienw.nl. Rik van Dijk is onderzoeker bij het NCSC en houdt zich daar onder andere bezig met vraagstukken rondom IACS-security en het duiden van kwetsbaarheden. Hij is bereikbaar via rik.vanDijk@ncsc.nl.

Patchmanagement in OT-omgevingen

Een rondgang langs de Infrastructuur & Waterstaat (I&W) sectoren

Patchen, patchen, patchen… patchen. Het advies dat menig securityspecialist geeft aan organisaties zodat ze beter in staat zijn om zich te verweren tegen aanvallers. Het snel patchen van kwetsbaarheden is voor IT-systemen een beproefde methode om snel en efficiënt kwetsbaarheden in systemen te verhelpen en de systemen zo weerbaarder te maken. Maar is dat patchen wel zo eenvoudig in industriële omgevingen met veel operationele technologie?

Steeds meer kaders en normen schrijven voor dat je het patchen op een goede manier hebt ingericht in je organisatie. Binnenkort wordt er in Europees verband besloten over een nieuwe versie van de Europese Directive on security of network and information systems (de NIS Directive (1), ook wel NIB-richtlijn genoemd). Hiermee zal waarschijnlijk de zorgplicht voor organisaties, ook met betrekking tot patchmanagement verder worden uitgebreid.

In OT-omgevingen kan het patchen van je systemen maanden kosten, is downtime onacceptabel en moet je 100% zeker zijn dat de nieuwe update geen onveilige situaties creëert. Allemaal afwegingen waar beheerders van industriële automatisering en controlesystemen (Industrial Automation and Control Systems, IACS) dagelijks mee te maken hebben. Op 24 maart 2022 gingen we in gesprek met de sectoren binnen I&W over verplichtingen, best practices en handvatten voor het patchen van IACS-systemen in de watersector.

Tijdens het webinar werd deelnemers gevraagd of zij wisten welke eisen er gesteld werden aan patchmanagement binnen hun organisatie. 70% van de deelnemers gaf aan dat ze dit niet wisten. Ook gaf 64% van de deelnemers aan dat zij erg veel moeite ervaren om kwetsbaarheden in hun systemen te identificeren. Deze uitkomsten geven aan dat het patchmanagement binnen deze doelgroep nog niet zo gemakkelijk gerealiseerd wordt. Het patchproces, van het identificeren van kwetsbaarheden tot het doorvoeren van de patch, is ingewikkeld en verdient meer aandacht. Om meer duidelijkheid te verschaffen beschrijven we hieronder welke aanpak helpt bij patchen in industriële omgevingen.

Hoe pak je dat aan, risicogericht patchen?

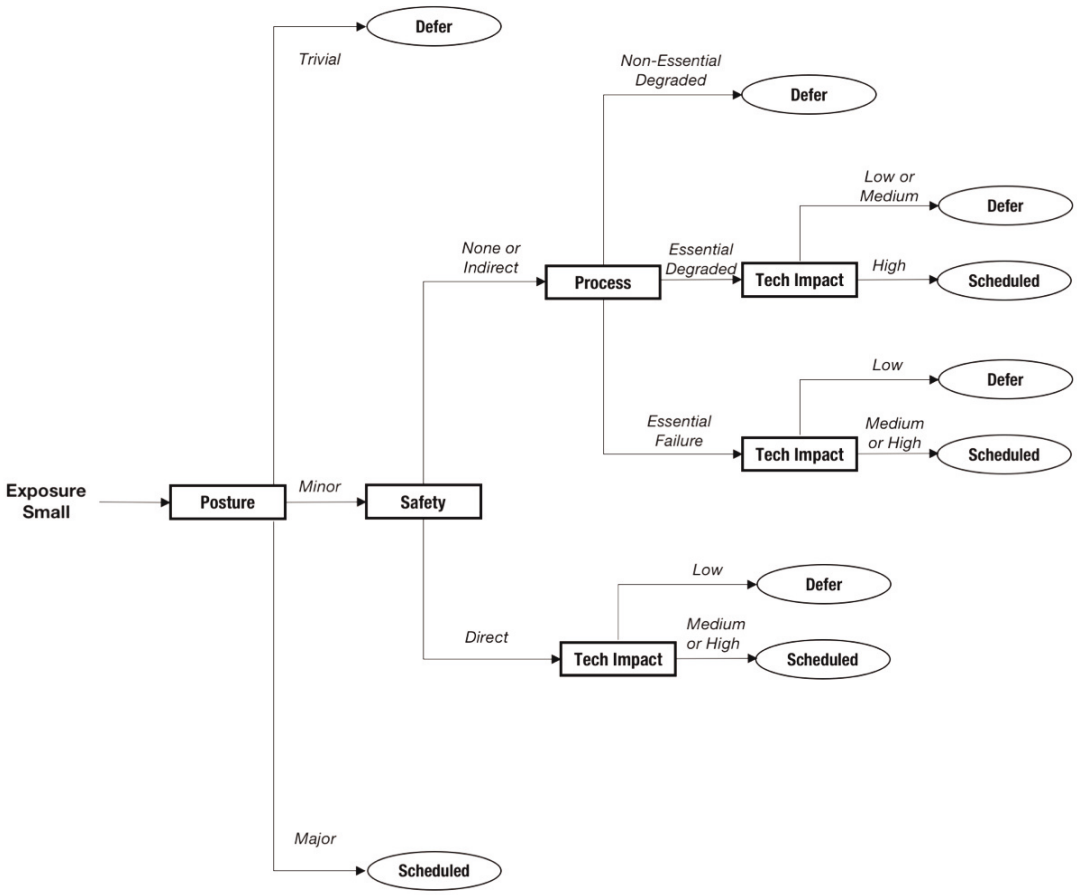
Verschillende standaarden bieden handvatten aan organisaties om hun patchmanagement in te richten. Voor IACS is de meest bekende standaard de IEC 62433 (2). De standaard gaat uit van een risk based approach voor organisaties om hun patchmanagement te doen. Dit houdt in, dat het organisaties aanmoedigt om wel of niet te patchen op basis van een eigen risicoafweging. De IEC 62433 biedt een workflow om patches binnen IACS-omgevingen uit te rollen. Per stap geeft de standaard een aantal handvatten.

Figuur 1 - IEC 62443 workflow. Bron: IEC 62443 2-2.

Om een goede risicoafweging te maken is het belangrijk dat de organisatie goed in beeld heeft welke assets er zijn (assetmanagement), welke componenten, systemen, soft- en hardware. Dit betekent niet enkel de naam en versie van het systeem maar veel meer. IEC 62433 biedt een goed overzicht welke informatie over het systeem verzameld moet worden. Leer het systeem kennen en documenteer dat goed. Daarbij is het belangrijk een duidelijk proces te hebben voor het verzamelen en bewaren van de juiste informatie over de kwetsbaarheid.

Vulnerability scannen heet hangijzer

Vulnerability scannen in IACS-omgevingen is (terecht) een heet hangijzer. Iedereen kent een verhaal waarbij een actieve scan ervoor zorgde dat een proces werd ontregeld. Veel IACS, zeker de oudere systemen, kunnen instabiel gedrag vertonen na een actieve scan. Toch is dat geen reden om scanning helemaal uit te sluiten. Vulnerability scanners kunnen veel toegevoegde waarde hebben; ze kunnen snel en efficiënt kwetsbaarheden identificeren. Bekijk per systeem of het geschikt is om er een scan op uit te voeren. Overleg met de leverancier en vergeet dit ook niet toe te voegen aan de documentatie over het systeem. Het aanschaffen van een vulnerability scanner is ook in IACS-omgevingen zeker het overwegen waard.



Figuur 2 - De SSVC-methode. Bron: first.org (4).

Vervolgens kan met de verzamelde informatie de risicoafweging gemaakt worden. Voor het bepalen van het risico zijn altijd twee elementen belangrijk: impact en kans. In het geval van het patchen in IACS moet niet alleen de vraag worden gesteld: welk risico introduceert een kwetsbaarheid in een IACS, maar ook wat is het risico dat de patch zelf met zich meebrengt? Wat voor kwetsbaarheid verhelpt de patch precies en op welke manieren kan dit uitgebuit worden? Zijn er misschien mitigerende maatregelen voorhanden? Ook het bepalen van de aard van het risico dat een kwetsbaarheid introduceert in het systeem is niet eenvoudig. Hoe meer kennis de organisatie heeft verzameld in de eerdere stap, hoe gemakkelijker de afweging kan worden gemaakt.

De organisatie kan dan een snelle triage doen via bijvoorbeeld een methode als Stakeholder Specific Vulnerability Categorization (SSVC) (3) van Carnegie Mellon. Dit biedt de uitvoerder een korte beslisboom met daarin een aantal vragen die het risico van een kwetsbaarheid verduidelijken. Het begeleidt de gebruiker naar een antwoord dat aansluit op de eigen organisatie.

Daarna kan worden overgegaan op een uitgebreidere risicomethode. Hiervoor biedt de CSIR 3.0 (5) van Rijkswaterstaat een aantal concrete handvatten. Via de RAMSHEEP-methode (6), waarbij ook aandacht voor de impact op de veiligheid en betrouwbaarheid van het aangestuurde proces belangrijk is, kan een uitvoerder een

In OT-omgevingen kan het patchen van je systemen maanden kosten.

goede risico-inschatting van de kwetsbaarheid op het systeem en het aangestuurde proces maken. Een andere strategie die duidelijkheid verschaft is om een Bowtie methode (7) te gebruiken om de invloed van de kwetsbaarheid op de bestaande controls inzichtelijk te maken.

Mocht uit de analyse komen dat patchen de beste strategie is, bereid het management erop voor dat de patch niet morgen al is doorgevoerd of dat de patch kostbaar is om door te voeren. Hier komen we zo op terug. Als laatste volgt een uitgebreid testproces waar de patch eerst wordt uitgerold op test- of niet-kritieke systemen voordat de patch op belangrijkere systemen geplaatst wordt.

Het patchproces is tijdrovend en kost flinke capaciteit omdat de organisatie er zeker van moet zijn dat de patch geen problemen oplevert voor het systeem en de processen die het aanstuurt of monitort. Een duidelijke rolverdeling, waarbij iedereen weet welke taak en rol hij of zij oppakt, wanneer er een kwetsbaarheid met een hoog risico wordt geïdentificeerd, is essentieel. Het kost tijd om in te richten maar scheelt achteraf een hoop tijd en geld elke keer dat een kwetsbaarheid moet worden verholpen.

De businesscase

Zoals gezegd: in tegenstelling tot IT-systemen is patchen voor IACS niet altijd de meest logische keuze. De beslissing om te patchen moet voortkomen uit een goede risicoanalyse en hierbij een gewogen kosten- en batenanalyse. Voor deze beslissing is uiteindelijk het bestuur verantwoordelijk. Vergeet als verantwoordelijke niet te hameren op de laatste stap in de workflow: verificatie en vastleggen.

Het helpt om de argumenten – voor het wel of niet patchen van een systeem – toe te lichten en vast te leggen door termen te gebruiken die de taal van de organisatie en het management reflecteren. Wat voor impact kan een kwetsbaarheid hebben op de bedrijfsvoering? Wat zijn de kosten voor het verhelpen van die kwetsbaarheid? Hoeveel tijd kost het verhelpen en hebben we de juiste kennis in huis? Management, OT-Specialisten en patchmanagers moeten om de tafel om deze onderwerpen te bespreken en om taalbarrières te slechten.

Om een goede businesscase te bouwen moet dan ook geen sprake zijn van taalverwarring tussen de uitvoerders en het management. Dit betekent dat beide partijen de tijd moeten nemen om elkaars werelden te begrijpen. Besteed hierbij aandacht aan het duidelijk uitleggen van het afwegingsproces dat een uitvoerder maakt. Eerdere genoemde middelen zoals een Bowtie kunnen helpen om het afwegingsproces ook voor anderen inzichtelijk te maken.

Duidelijkheid in taal tussen de verschillende stakeholders binnen de organisatie maken het beslissingsproces rondom het oplossen van kwetsbaarheden gemakkelijker en dragen bij aan een beter begrip tussen management en uitvoerders met betrekking tot de risico's waar de organisatie mee te maken heeft.

Hoe nu verder?

Zoals eerder benoemd is het patchen van IACS een ingewikkeld en tijdrovend proces. De focus zou moeten liggen op het maken van een goede risicoafweging. Uitvoerders hebben weinig aan stoere uitspraken en silver bullets. Deelnemers aan het webinar gaven aan dat zij behoefte hebben aan praktische handvatten en middelen. Soms zijn deze praktische richtlijnen er al, zoals de CSIR 3.0 waar ook het patchmanagement uitvoerig in wordt beschreven.

Als we het patchmanagement in IACS serieus nemen, moeten we begrip tonen voor de complexe werkelijkheid en tegelijkertijd handreikingen doen om de stappen die moeten worden doorlopen te vergemakkelijken. Dit artikel biedt een aantal eerste stappen die gezet kunnen worden maar volgende stappen zijn absoluut noodzakelijk. Daarom investeert het NCSC in verder onderzoek naar het vergemakkelijken van het patchmanagement in OT-omgevingen en werkt zij samen met I&W om organisaties bewuster te maken van het belang van risicogericht patchen.

Referenties

(1) https://digital-strategy.ec.europa.eu/en/policies/nis-directive
(2) https://en.wikipedia.org/wiki/IEC_62443
(3) GitHub - CERTCC/SSVC: Stakeholder-Specific Vulnerability Categorization
(4) https://www.first.org/
(5) csir-34-definitief-concept-20210914.pdf (cip-overheid.nl) en
https://www.magazinesrijkswaterstaat.nl/zakelijkeninnovatie/2022/01/cybersecurity
(6) https://repository.tudelft.nl/islandora/object/uuid:bfeae01d-cfbc-4749-bf2c-531fc7d802d0
(7) https://www.cgerisk.com/knowledgebase/The_bowtie_method