

30 seconden, niet 30 minuten: beveiligingsupdates met één druk op de knop



Hoe KEB de update-eis van de CRA vereenvoudigt met NOA

De Cyber Resilience Act (CRA) treedt eind 2027 in werking en brengt aanzienlijke veranderingen mee voor de machinebouwsector. De focus ligt op het beoordelen van de cyberbeveiliging van producten en processen, met als doel het systematisch dichten van beveiligingsgaten. Zo vereist de CRA onder andere dat producten beveiligingsupdates standaard automatisch installeren — met een duidelijke opt-out-mogelijkheid, en met ruimte voor afspraken tussen fabrikant en gebruiker over het juiste installatiemoment. Maar hoe kan aan deze eis worden voldaan als er honderden controllers, omvormers en machines moeten worden bijgewerkt? In dit artikel leggen we uit hoe het open automatiseringsplatform NOA updates binnen enkele seconden implementeert.

Waarom zijn beveiligingsupdates voor producten met digitale componenten zo belangrijk in de Cyber Resilience Act?

Over het algemeen zijn software-updates belangrijk omdat ze bijdragen aan systeemstabiliteit door bugfixes te bieden en ongeplande downtime te voorkomen. Ze breiden ook het scala aan functies uit, waardoor nieuwe use cases met machines kunnen worden geïmplementeerd. Maar updates zijn vooral noodzakelijk als het gaat om cyberbeveiliging – en de CRA houdt hier ook rekening mee.

Tegenwoordig duiken er voortdurend nieuwe beveiligingslekken op, of worden bestaande lekken ontdekt door hackers. Dit maakt het des te belangrijker om regelmatig updates uit te voeren die deze kwetsbaarheden dichten. Dit helpt om gerichte aanvallen op industriële systemen te voorkomen, bijvoorbeeld door middel van ransomware of sabotage. Dergelijke aanvallen leiden tot hoge kosten, stilstand en zelfs machinestoringen – bijvoorbeeld wanneer machines worden overgenomen door de aanvaller. Het doel is daarom om het aanvalsoppervlak te verkleinen door componenten, bibliotheken en protocollen up-to-date te houden. OT-systemen zijn bijzonder cruciaal. Ze hebben vaak lange levenscycli en zijn een specifiek doelwit omdat ze zelden worden gepatcht. Daarom hebben ze speciale bescherming nodig. Hier komt NOA om de hoek kijken.

Hoe werkt het installeren van updates bij NOA?

NOA biedt gebruikers drie handige manieren om updates te installeren. In de on-premise-modus krijgt de gebruiker toegang tot het NOA-apparaat – zoals het Embedded Automation Device C6 Compact 3 – via een HTTP-interface (Ethernet). Hiervoor moet de laptop op hetzelfde netwerk zitten als het NOA-apparaat. Het voordeel is dat de software rechtstreeks via de App Manager in NOA kan worden gedownload, zodat de gebruiker aan zijn laptop kan blijven werken.

Een andere optie is de cloud. De cloudoplossing van NOA Portal wordt gebruikt om toegang te krijgen tot het apparaat, en de update wordt handig vanuit de cloud geïnstalleerd. De laptop en het NOA-apparaat hoeven niet op hetzelfde netwerk te zitten. Het proces is bijzonder eenvoudig: open een browser, ga naar het NOA Portal en start de updates met één klik – dat is alles.

Updates kunnen ook via een VPN worden geïnstalleerd, zelfs als de gebruiker zich niet op het lokale netwerk van het NOA-apparaat bevindt, mits het apparaat een internetverbinding heeft. Met de NOA Connect-app kan de gebruiker een VPN-verbinding opzetten met het NOA-apparaat en toegang krijgen tot andere apparaten op hetzelfde netwerk. Software-updates – die bijvoorbeeld vooraf op de laptop zijn gedownload – kunnen vervolgens op de apparaten binnen het netwerk van het NOA-apparaat worden geïnstalleerd.

Hoe zou de alternatieve aanpak eruitzien zonder NOA om aan de update-eisen van de CRA te voldoen?

Dat hangt af van het apparaat en de beschikbare interfaces – dat wil zeggen of er een cd-station, USB-poort, Ethernet-poort en internettoegang aanwezig zijn. Daarnaast zijn opslagmedia zoals USB-sticks of SD-kaarten vereist. Dit is onhandig, omdat het fysieke toegang tot het apparaat vereist en het opslagmedium elke keer handmatig moet worden ingevoegd. Natuurlijk is het ook mogelijk om software naar de laptop te downloaden en deze vervolgens te installeren. Dit kost echter veel tijd, omdat de laptop herhaaldelijk verbinding moet maken met het betreffende apparaat. Hier kan NOA de processen aanzienlijk vereenvoudigen – met slechts een paar klikken start de update voor alle apparaten.

Waarschijnlijk is een van de grootste obstakels het grote aantal apparaten dat geüpdatet moet worden...

Precies, want in productieomgevingen is het niet ongebruikelijk dat gebruikers honderden units hebben die beveiligingsupdates moeten ontvangen. Met het NOA-portaal wordt het proces bijzonder efficiënt dankzij de functie Fleet Management. Fleet Management geeft gebruikers een volledig overzicht van alle apparaten in het veld of in productie. Deze kunnen worden beheerd in het NOA-portaal, en updates kunnen voor de volledige vloot apparaten worden gestart. Eenmaal ingelogd op het NOA-portaal, is slechts zes keer klikken nodig om de update te starten. Dit verkort de benodigde tijd van 30 minuten – bij een traditionele update met een opslagmedium – tot slechts 30 seconden. Zoals je ziet, duren traditionele updatemethoden veel te lang. Daardoor worden ze in de praktijk niet consequent gebruikt en krijgt kwetsbaarheidsbeheer niet de juiste aandacht. Alleen software zoals NOA maakt consistent kwetsbaarheidsbeheer mogelijk.

Welke update-intervallen kunnen gebruikers verwachten?

Hier maken we onderscheid tussen beveiligingsupdates en productupdates voor nieuwe functies, stabiliteitsverbeteringen, enzovoort. Beveiligingsupdates worden uitgevoerd in overeenstemming met de CRA-richtlijnen. Daartoe hebben we op productniveau kwetsbaarheidsbeheer geïmplementeerd. We monitoren continu de software die we op de markt hebben gebracht, met behulp van een Software Bill of Materials (SBOM) die we genereren tijdens het releaseproces van de software. Dit betekent dat we weten welke eigen en externe componenten in onze software zijn opgenomen. We vergelijken onze software met databases van bekende kwetsbaarheden om te bepalen of een van onze vrijgegeven softwareversies beveiligingskwetsbaarheden bevat. Op basis hiervan leveren we beveiligingsupdates zodra er een beveiligingslek wordt ontdekt. In overeenstemming met de CRA rapporteren wij deze bevindingen vervolgens aan de relevante autoriteit.

Bron: [30 seconden, niet 30 minuten: beveiligingsupdates met één druk op de knop](#)

Over ons

Marsman Elektronica en Aandrijvingen - De toekomst in besturings- en automatiseringstechnologie

Onze kernactiviteiten zijn:

- Procesautomatisering en visualisatie
- Motion control technologie
- Asynchrone motoren, synchrone motoren en servomotoren (wisselstroom)
- Borstelmotoren, borstelloze motoren, servomotoren, motoren met geïntegreerde elektronica en frameloze motoren (gelijkstroom)
- Diverse opties voor vertragingskasten, feedback, remmen, koppelingen en accessoires
- Klantspecifieke aanpassingen en speciale ontwerpen

Onze partners:

KEB Automation | KEB Antriebstechnik | Württembergische Elektromotoren (WEG) | KOSTAL Drives Technology | PMW Dynamics | Kählig Antriebstechnik GmbH | ADVANCED Motion Controls

[Marsman Elektronica en Aandrijvingen](#)