



Michael Theuerzeit • Lead
Consultant • Hudson Cybertec •
www.hudsoncybertec.com

'PATCHWINDOW'

In de procesindustrie draaien installaties volcontinu. Installaties kunnen vele maanden zonder onderhoudsstops, wat belangrijk is voor de continuïteit van een productie. Immers het opstarten van de installatie kost, net als het gecontroleerd en veilig stoppen ervan, vaak meerdere dagen. Het stilleggen van de productie is kostbaar en als de organisatie onderdeel uitmaakt van een ketenproces dan zijn daar zeer waarschijnlijk ook andere bedrijven direct bij betrokken omdat zij geen aanvoer meer krijgen, of zelf hun producten niet meer kwijt kunnen.

Het herstarten van een computer omdat deze 'gepatcht' is, is er dan ook niet bij. Binnen deze omgevingen moeten alternatieve 'patch'-strategieën worden bedacht, die passen binnen de volcontinue bedrijfsvoering van de organisatie. Dit is anders dan binnen een IT-omgeving, waar 's avonds, of desnoods in het weekend, een patchronde wordt gedraaid om alle 'operating systems' en applicaties weer up to date te maken.

Daarnaast speelt er binnen de OT iets anders: leveranciers van systemen dienen vooraf toestemming-patches goed te keuren. Als een organisatie dat niet doet, kan een leverancier niet garanderen dat bijvoorbeeld het SCADA-systeem blijft functioneren en zal deze wellicht zelfs geen ondersteuning geven op niet-goedgekeurde patches. Het is dus sowieso altijd wachten op goedkeuring en dan ook nog op een moment dat deze patches kunnen worden doorgevoerd. Voordat een patch dan ook maar in de buurt komt van de productie-omgeving wordt deze eerst dan ook in de testomgeving van de organisatie zelf geïnstalleerd en beproefd.

Bij Hudson Cybertec zien we soms dat klanten voldoende redundantie hebben in de gebruikte systemen omdat systemen als 'hot stand-by' draaien. Zij kiezen er na goedkeuring door de systeemleverancier en uitgebreid testen voor om eerst zo'n stand-by systeem te 'patchen' en deze na het testdraaien 'live' te maken. Op deze wijze is er altijd een draaiende omgeving om op terug te vallen. Draait het gepatchte systeem stabiel, dan kunnen andere systemen worden gepatcht. Indien er toch zaken aan het licht komen die een goede uitrol in de weg staan, wordt deze teruggedraaid. Op deze wijze worden patches gefaseerd uitgerold.

'PATCH'-STRATEGIEËN VEREIST

Andere klanten beschikken niet over deze redundantie en hebben daarom procedures ingericht om op een gestructureerde en verantwoorde wijze patches uit te kunnen rollen. Op welke manier er ook wordt gepatcht, het is van groot belang dat er goede afspraken zijn gemaakt binnen de organisatie zodat patch-procedures altijd veilig en verantwoord kunnen worden gevolgd, zonder dat de bedrijfscontinuïteit daar hinder van ondervindt.