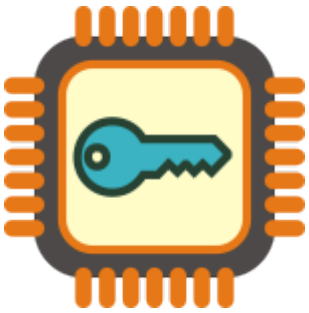
Wat is er aan de hand bij Medicom op KPN CyberCentrum Flevoland?



De gebruikers van het huisartsinformatiesysteem(HIS) Medicom hebben twee dagen achtereen een mail van de leverancier PharmaPartners gehad die vragen oproept. Er zijn performance-problemen waardoor de snelheid, waarmee Medicom werkt achteruit loopt. Die lijken te maken te hebben met firewall-problemen. Dit HIS werkt in de vorm van clusters van huisartsen en apotheken die met elkaar regulier samenwerken. Deze clusters worden voor PharmaPartners gehost door een datacentrum van KPN in Almere. In 2011 ging PharmaPartners over van een groot aantal servers in Apeldoorn bij het datacentrum van Getronics naar het KPN CyberCentrum Flevoland. Daar werden de servers gevirtualiseerd en werd met name het dagelijkse systeembeheer een stuk makkelijker.

Eerste melding

Op 7 juli werd aan de gebruikers van Medicom gemeld dat er actuele performanceproblemen waren. Blijkbaar hadden huisartsen en apothekers gemeld dat de snelheid van hun systeem terugliep. Er is toen een herstart van de firewall gedaan waarop de situatie wel wat verbeterde, maar niet voldoende. Daarna zijn de gevirtualiseerde servers herstart. Na die herstart was er een verbetering, maar nog geen optimale toestand.

Tweede melding

Op 8 juli krijgen de gebruikers een nieuwe melding dat de performance op het gewenste niveau gekomen was, maar dat de belasting van de firewall toch weer begon op te lopen. Om die reden wordt in de nacht van 8 op 9 juli een extra firewall geïnstalleerd om opnieuw traagheid te voorkomen.

Overwegingen

Bij de eerste melding is het nog voorstelbaar dat er sprake is van een soft- of hardwareprobleem van Medicom zonder dat er sprake is van compromitteren van systemen van buitenaf. Na de tweede melding, die van het installeren van een extra firewall, dringt zich toch de gedachte op dat er sprake is van een eventuele cyberaanval. Immers, als er hard aan de deur gerammeld wordt, zet je er ook een extra slot op. Het KPN Cybercentrum Flevoland is niet uitsluitend de host van Medicom, maar kent zeer vele klanten. Bij een cyberaanval op een dergelijk centrum is het voorstelbaar dat de firewalls van subsystemen het gigantisch druk hebben om de toegang van reguliere gebruikers mogelijk te maken naast het afslaan van aanvallers. Het plaatsen van een extra firewall kan het reguliere gebruik dan ook verbeteren.

Wat er precies gaande is, wordt meestal niet aan de buitenwacht gemeld.

Het zal dus voorlopig gissen blijven.

Wordt mogelijk vervolgd.

W.J. Jongejan