



Elvira Dragstra is werkzaam bij advies- en projectmanagementbureau Merpa

*Van alle onderzochte apparaten garandeerde de fabrikant dat ze ook bij een omgevingstemperatuur van 35 °C zonder problemen functioneren.*

# Ergernissen en onzekerheid door gevoelige sensoren

## Zijn valse alarmmeldingen te voorkomen?

DETECTIE IS NOODZAKELIJK OM ONS VROEGTIJDIG TE ALARMEREN OVER ONEFFENHEDEN EN DREIGEND GEVAAR IN ONS DATACENTER. MAAR WAT ALS DE ALARMMELDINGEN DIE VOLGEN (TE) REGELMATIG VALS ZIJN EN DAARDOOR LEIDEN TOT ERGERNISSSEN EN ONZEKERHEID?

Midden in de nacht uit zijn bed worden geps't, omdat er een alarmerend bericht komt vanuit het datacenter, dat overkomt menig ict-manager. De manager stapt slaperig in de auto en snelt naar het datacenter toe. Maar wat schetst zijn verbazing, er is niets aan de hand! Alles draait uitstekend: de koelinstallaties draaien, de temperatuur en luchtvochtigheid zijn binnen de vastgestelde marges, er is geen stroomuitval en er is geen brand.

Hij loopt nogmaals een rondje langs de installaties en pas als hij er zeker van is dat alles in orde is, reset de manager het meldsysteem, sluit af en gaat terug naar huis om nog wat te slapen. Gelukkig, het was vals alarm. Alhoewel, gelukkig? De vraag is natuurlijk: Waar komt dan dat alarm vandaan?

### NIET TE ACHTERHALEN

Dit voorbeeld is gebaseerd op praktijksituaties. Soms heeft de ict-manager kunnen achterhalen waardoor de valse alarmen werden veroorzaakt en waar ze vandaan kwamen, maar in sommige gevallen ook niet.

Bij een alarm dat wel te achterhalen was, bleek uit de historie van het meldsysteem dat de bevochtigingsunit van de koelinstallatie af en toe vocht uitstootte, waardoor de luchtvochtigheid kort en hevig opliep tot boven

de ingestelde drempelwaarde. Hierdoor volgde er, terecht overigens, een alarm.

Nadat de instellingen van de bevochtigingsunit en drempelwaarden waren gewijzigd, leek de boosdoener gevonden. Maar nee, de valse alarmen bleven terugkomen, helaas vaak midden in de nacht. Ict-specialisten, maar ook onderhoudsmonteurs van de diverse installaties konden de veroorzaker(s) niet achterhalen en ook uitwisseling met een nieuw systeem, loste de alarmeringen niet op.

Na veel ergernissen, verloren tijd en moeite heeft deze situatie geresulteerd in verwijdering uit het datacenter van het meldsysteem met zijn accessoires (met uitzondering van de brandmelders). Wat is overgebleven, is de onzekerheid van wat komen gaat.

### VALSE ALARMMELDINGEN

Wat verstaan we onder valse alarmmeldingen? Onder valse alarmmeldingen verstaan we alarmen die in de praktijk geen gevaar of dreiging van gevaar vormen. Ze zijn daarom ongewenst. Regelmatig is niet te herleiden wie of wat het alarm heeft veroorzaakt of hoe het is veroorzaakt. Vaak hebben ze plaats op momenten waarop er geen gevaar kan zijn (geweest).

Deze meldingen gaan ons verstand te boven en brengen ergernissen en onzekerheid met zich mee. Een verhoging van de luchtvochtigheid is voor te stellen in de eerste uren nadat personen in of uit het datacenter zijn gelopen, maar niet midden in de nacht! De historie van de meldsystemen moet uitkomst bieden, maar doet in de meeste gevallen slechts melding van datum, tijdstip en type.

### TYPE VALSE ALARMMELDING

De meest voorkomende valse alarmmeldingen in het datacenter zijn afkomstig van brandmelders en temperatuur- en luchtvochtigheidopnemers en/of -sensoren.

De vraag is of valse alarmmeldingen zijn te voorkomen? Hiervoor is het van belang iets te vertellen over het ontstaan van (valse) alarmen.

Alarmen ontstaan als ingestelde drempelwaarden in het aangeschafte alarmsysteem worden bereikt via signalen vanuit geplaatste sensoren, opnemers en/of melders (en er dus gevaar wordt gedetecteerd). Hoe valse alarmmeldingen ontstaan, weten we voornamelijk uit de praktijk. De maatregelen die we kunnen nemen om zoveel mogelijk valse alarmmeldingen te voorkomen, hangen af voor het type valse alarmmelding.



## MAATREGELEN BIJ EEN TE HOGE OF TE LAGE TEMPERATUUR EN LUCHTVOCHTIGHEID

- 1 Stel de drempelwaarden van het meldsysteem zodanig in dat er voldoende marge is tussen de onder- en bovenwaarden, maar dat het toch veilig is. 30 en 70 °C en 30 en 85 % RLV (relatieve luchtvochtigheid) zijn maxima. Hiermee lijken we klaar te zijn, maar zo simpel ligt het niet. Het ontstaan van een alarm volgt uit communicatie tussen het systeem en de daarop aangesloten sensoren (zogenoemde detectoren). Zonder de laatste wordt er niet gedetecteerd en dus ook niets gemeld.
- 2 Voor correcte informatie is het dan ook van groot belang dat de sensoren juist zijn geplaatst. Als bijvoorbeeld een melding wordt vereist bij een te hoge temperatuur in de ruimte, dan worden in het datacenter vaak warmtesensoren geplaatst op plekken waar hotspots worden verwacht en/of bij de aanzuigzijde van de airconditioners. Dit lijkt logisch, maar de vraag is natuurlijk: heeft de klant hier wat aan en wat zijn de gevolgen ervan? De temperaturen in de ruimte fluctueren omdat, door communicatie tussen de airco's onderling en de bij hen ingestelde ruimtetemperatuur en luchtvochtigheidsgraad (RLV), zij af en toe even aanslaan om de temperatuur en de RLV weer op het peil te brengen van hun eigen instelling. Hierdoor detecteren de geplaatste warmte- en RLV-sensoren in de ruimte een piek op temperatuur en RLV. De sensoren geven dit door aan het meldsysteem en er volgt een alarm als de temperatuur of luchtvochtigheidsgraad buiten de ingestelde drempelwaarden van het systeem komt. Het gevolg is een vals alarm, maar zoals gezegd ook ergernis en onzekerheid omdat er niets aan de hand lijkt te zijn wanneer de gealarmeerde manager in het datacenter aankomt. Alles is weer terug naar normaal.
- 3 Als er zowel in de ruimte als nabij de bron wordt gemeten, kan dit erg verwarrend worden. De ruimtesensoren geven een gemiddelde door van de door hen gemeten temperaturen en RLV en wijken af van de gemeten waarden bij de bron(nen). Hoe moet de klant een alarmmelding nu interpreteren? Het is verstandiger een keuze te maken uit een van de twee mogelijkheden.
- 4 Zorg dat de instellingen van de koelunits binnen de drempelwaardes van het meldsysteem liggen, anders komen er (valse) alarmmeldingen van de apparaten zélf (lees: airco in storing).
- 5 Zorg dat de sensoren zich niet in de omgeving van de toegangsdeur bevinden. Dit geeft geheid problemen.
- 6 Zorg voor scheiding van warme en koude 'straten', zodat geen vermenging van koude en warme lucht plaatsheeft.
- 7 Zorg ervoor dat alarmmeldingen niet alleen per sms worden gestuurd. Niet alle providers sturen sms'jes direct door (soms pas uren later). Hierdoor kunnen alarmmeldingen veel later binnen komen dan het tijdstip waarop het probleem door het systeem is gedetecteerd. Midden in de nacht lijkt voor sommige providers de rustigste tijd om sms'jes door te sturen (weinig bel- en dataverkeer).
- 8 Zorg er ook voor dat meldingen goed te lokaliseren zijn voor degene bij wie de melding binnenkomt. Dit betekent per ruimte een up-to-datetekening waarop duidelijk alle apparaten en melders staan vermeld (genummerd en genaamd). Zowel de nummers als de namen moeten direct duidelijk maken waar de melding vandaan is gekomen. Voor meldkamers geldt dat er up-to-dategegevens moeten zijn van personen en/of instanties die bij een melding moeten worden benaderd. Kortom: duidelijkheid over wie wat moet doen bij een melding, voorkomt veel ergernissen en vooral missers!

## MAATREGELEN TEGEN EARLY WARNING BIJ BRANDMELDSYSTEMEN:



- 1 Zorg voor een schone en stofvrije ruimte, zodat er geen stofdeeltjes worden gedetecteerd die (valse) alarmen kunnen veroorzaken. Dozen die moeten worden uitgepakt, kunnen dan ook beter in het voorportaal of elders worden uitgepakt.
- 2 Een nieuw systeem moet wennen aan zijn nieuwe omgeving. Zorg daarom voor een nastelafpraak na een rustperiode van circa vier weken om het meldsysteem bij te regelen.
- 3 Wijzigingen in het datacenter, zoals bijplaatsing van koelunits, heeft invloed op het meldsysteem. Laat daarom een controle uitvoeren, nadat de wijziging heeft plaatsgehad.
- 4 Zorg ervoor bij testen of werkzaamheden in het datacenter, zoals onderhoud, dat degene(n) bij wie de melding binnenkomt, weet dat (valse) alarmen kunnen binnenkomen vanwege de werkzaamheden. Denk hierbij aan stof en trillingen bij boren en/of lassen, verhoging van RLV door in- en uitlopen van het datacenter.
- 5 Periodiek onderhoud is nodig om het systeem en melders schoon te maken en te testen op de juiste werking.
- 6 Zijn met deze maatregelen nu alle valse alarmmeldingen voorbij? Het antwoord is nee, valse alarmen zullen niet 100 % verdwijnen. De omgeving blijft aan veranderingen onderhevig en daardoor wat onvoorspelbaar. Ook staat de detectieapparatuur heel gevoelig ingesteld: tenslotte willen we in een zo vroeg mogelijk stadium worden geïnformeerd over dreigend gevaar.



## EEN ALARMSYSTEEM KIEZEN

Door het datacenter met alle toebehoren optimaal te bewaken en te beheren (te monitoren) en hiervoor iemand verantwoordelijk te maken, is er continu realtime-informatie beschikbaar over de status ervan. Hiermee heeft de manager een dreiging van gevaar in een zo vroeg mogelijk stadium op zijn netvlies. Voorwaarde is wel dat het systeem up to date wordt gehouden. Voor een juiste interpretatie moet elke wijziging in het datacenter, zoals uitbreiding, consolidatie of vervanging van ict-apparatuur en storage, aanpassingen aan koelinstallaties, ups'en, vermogens, in het systeem zijn opgenomen.

Er zijn veel meld- of alarmsystemen op de markt en bij een keuze van een systeem moet rekening worden gehouden met de volgende factoren:

- Niet elk willekeurig systeem is geschikt voor elke organisatie. Daarom moeten wensen en verwachtingen inzichtelijk zijn. Niet elk systeem is bijvoorbeeld flexibel en schaalbaar. Zo is het systeem van fabrikant x niet automatisch uitwisselbaar met het systeem van fabrikant y en is niet elk systeem uitbreidbaar bij de komst van een tweede of derde datacenter. Ook is niet elk systeem door meerdere personen vanaf verschillende locaties tegelijkertijd benaderbaar. Erg onhandig als datacenters verspreid liggen.
- Als diverse disciplines, zoals facilitair en ict, verschillende informatie nodig hebben uit het systeem, moet hiermee bij de keuze rekening worden gehouden.
- Is de software te integreren met de gekozen en gebruikte infrastructuur? Een platform waarin ook detectie en eventueel monitoring is opgenomen, is veel makkelijker te hanteren en te beheren dan een systeem met eigen software dat lokaal op een of meer pc's draait. Dit geldt zeker bij de aanwezigheid van meerdere datacenters.

**Wat moet de manager er zelf aan doen.**

**Welke acties worden van hem verwacht?**

- Wie gaat het systeem beheren en up to date houden? Is daar tijd voor gereserveerd?
- Wie verzorgt de instructie en opleiding van het gekozen systeem?
- Let bij de keuze op kosten van aanpassingen en wijzigen van software. Sommige systemen kunnen en mogen alleen door de fabrikant worden aangepast. De kosten van deze aanpassingen kunnen zeer hoog oplopen.
- Reserveer tijd om de verschillende systemen met elkaar te vergelijken en laat bij geavanceerde systemen eerst een pilot draaien om te zien hoe het systeem zich gedraagt en welke mogelijkheden het in zich heeft.
- Laat plaatsing en installatie door een vakkundige partij uitvoeren.
- Is de verkopende partij ook thuis als zich een probleem aandient? Dit type systemen wordt graag als sluitpost verkocht. Maar wordt er ook tijd gemaakt als er in het datacenter oneffenheden zijn?

## CONCLUSIE

Detectie en monitoring van het datacenter zijn belangrijke onderdelen van de beveiliging in een datacenter en behoeven dan ook apart aandacht. Wensen en verwachtingen moeten aansluiten bij de definitieve keuze van een alarmsysteem en de verkopende partij. Laat de plaatsing en installatie verzorgen door partijen die hierin zijn gespecialiseerd.

*Stel de drempelwaarden van het meldsysteem zodanig in dat er voldoende marge is tussen de onder- en bovenwaarden, maar dat het toch veilig is.*

advertentie

Amersfoort 9, 10, 11 juni  
Vilvoorde 16 juni

**kannegieter**  
delivering ict. sharing knowledge



## Duurzame ICT

Kannegieter Kennismarkt 2009

Kannegieter 50 jaar kennis

\* Stel uw eigen programma samen

\* Marktplaats met demonstraties

\* Deelname is GRATIS

\* Identieke dagen

www.kennismarkt.kannegieter.nl

technologie partners













alliance partners


