Bescherming tegen dreigingen van buitenaf

EN 1047-2 biedt concept voor ict-beveiliging

Tussen een marketeer en de ict-manager van een middelgrote organisatie heeft het volgende gesprek over de beveiliging van het datacenter plaats.

Marketeer: *'Is uw datacenter goed beveiligd tegen inbraak en schades van buitenaf?'*

Ict-manager: *'Ja hoor, ons datacenter is goed beveiligd!'*

Marketeer: *'Kunt u vertellen hoe het datacenter is beveiligd?'*

Ict-manager: *'Ja hoor. Voordat u ons datacenter kunt betreden is er een voorportaal met sluis, voorzien van een elektronisch pasjessysteem, er hangen meerdere camera's en we hebben bewegingssensoren rondom ons datacenter aangebracht.'*

Marketeer: *'Heeft u ook aan andere beveiliging gedacht, zoals bescherming tegen hitte en/of brand, water en stroomuitval?'*

Ict-manager: *'Vanzelfsprekend, wij hebben in ons datacenter een early-warning branddetectiesysteem gekoppeld aan een automatische blusgasinstallatie voorzien van inerte gas, dus goed voor het milieu hè! We hebben hoeklijnen aangebracht onder de airconditioners tegen waterlekkage. We hebben een no-breaksysteem en bovendien zijn alle technische installaties redundant uitgevoerd, zodat bij uitval van één machine een andere met dezelfde capaciteit de functie van de eerste direct overneemt. Om statische elektriciteit te voorkomen hebben we ook nog bevochtiging laten aanbrengen.'*

Marketeer: *'Fijn om dit allemaal te horen mijnheer, maar hoe is het met de wanden en muren van uw datacenter gesteld. Zijn deze ook beveiligd tegen schade van buitenaf?'*

Ict-manager: *'Hoezo? De wanden en muren zijn 60 minuten brandwerend en zijn gemaakt van beton, daar komt toch niemand en niets doorheen?'*

BOUWBESLUIT

In de meeste programma's van eisen (PvE) of bestekken wordt uitgebreid aandacht besteed aan alle aspecten van beveiliging: de bouwkundige, elektrotechnische en koeltechnische aspecten, detectie en doormeldingen, en beheer en onderhoud. Dat deze eisen zijn gebaseerd op bouweisen conform het Bouwbesluit is niet of nauwelijks bekend bij de eigenaars of eindgebruikers die deze programma's (laten) opstellen voor de bouw van hun nieuwe datacenter. Dat daarmee de beveiliging van hun datacenter na de oplevering niet zo goed op orde is als zij denken, komt pas aan het licht wanneer er bijvoorbeeld in de ruimte naast de computerruimte brand uitbreekt. Dan blijkt dat de luchtvochtigheid in de computerruimte zeer snel en zeer hoog oploopt en dat door alle kieren rook naar binnenkomt.

BIJ BRAND

In een gebouw met betonnen wanden F90 (conform het Bouwbesluit) zullen bij een bevlamming van 1.100 °C buiten het datacenter de temperaturen in het datacenter na 90 minuten tot circa 200 °C zijn opgelopen. De luchtvochtigheid zal bij dezelfde bevlamming na 90 minuten boven de 100 % zijn opgelopen.

Deze 'schijnbeveiliging' blijkt ook als er zomaar water op de vloer ligt, waarvan niemand weet waar het vandaan komt. Op hetzelfde moment constateert de monteur van de koffieautomaat dat er een probleempje is met de watertoevoer en dat dit door een loodgieter moet worden opgelost. Hij weet namelijk alles over de koffieautomaat, maar gaat niet over de watertoevoer. Na de komst van de loodgieter blijkt dat de storing een gevolg is van een lek waardoor het water niet in de koffiebekers stroomt, maar al een aantal dagen in het datacenter! Toeval? Helemaal geen toeval. Het datacenter is op dit punt dus niet zo goed beveiligd als de eindgebruiker dacht. Hij vraagt zich af hoe dat kan? Zijn datacenter voldoet toch aan de bouweisen conform het Bouwbesluit?

Ja hoor, bouwkundig voldoet het datacenter aan de bouweisen, maar deze garanderen niet de veiligheid van het datacenter voor schade van buitenaf (lees: schade door ongelukjes in aangrenzende ruimten van het datacenter). Deze eisen zijn opgesteld ter bescherming van personen en zeggen iets over instortingsgevaar, maar niets over het behoud van de ict-apparatuur en daarmee het waarborgen van de continuïteit van de bedrijfskritische processen! Hiervoor zijn andere eisen opgesteld die zijn vastgelegd in de EN 1047-2. In deze norm staan de maximumwaarden van temperatuur en luchtvochtigheid gegeven, waaraan de ict-apparatuur mag worden blootgesteld (tabel 1).

	MAXIMUM-TEMPERATUUR	MAXIMUM RELATIEVE LUCHTVOCHTIGHEID (RLV)
Ict-apparatuur	70 °C	85,00 %
Datatapes	50 °C	85,00 %

Tabel 1.
Maximumwaarden van temperatuur en luchtvochtigheid voor ict-apparatuur vastgesteld in de EN 1047-2.

Elvira Dragstra is werkzaam bij advies- en projectmanagementbureau Merpa in Bleiswijk.

Omdat de bouweisen in het Bouwbesluit de ict-apparatuur onvoldoende zullen beveiligen tegen schade van buitenaf, zal iets anders moeten worden ondernomen om de ict-apparatuur te beschermen en daarmee de continuïteit van de kritische bedrijfsprocessen te waarborgen. Een van de mogelijkheden is een bouwconcept voor ict security te (laten) ontwerpen conform EN 1047-2.

Bouweisen zijn opgesteld ter bescherming van personen en zeggen iets over instortingsgevaar, maar niets over het behoud van uw ict-apparatuur.

Conform de EN 1047-2 is een aantal bouwconcepten ontwikkeld en op de markt gebracht die de kritische ict-apparatuur beschermen tegen schades van buitenaf. Deze bouwconcepten hebben met elkaar gemeen dat zij gedurende een x-periode hoge temperaturen, bijvoorbeeld veroorzaakt door brand buiten de ruimte, én vocht, bijvoorbeeld veroorzaakt door bluswater of lekkage buiten de ruimte, uit het datacenter weren zodat deze geen gevolgen hebben voor de werking en levensduur van de ict-apparatuur in het datacenter. Kortom, opdat er geen sprake is van uitval en/of storingen van ict-apparatuur.
Eindgebruiker en eigenaar moeten zich ervan bewust zijn dat ook de hardwarefabrikanten zich in hun specificaties van ict-apparatuur beroepen op de maxima, zoals gegeven in de EN 1047-2. Met andere woorden garanties op de correcte werking van ict-apparatuur gelden niet als blijkt dat de moederboarden ervan aan té hoge temperaturen zijn blootgesteld. In de meeste gevallen zal voor die tijd een alarm zijn afgegeven en zal de apparatuur zichzelf hebben uitgeschakeld. Maar in beide gevallen betekent het uitval van de ict-apparatuur.

OM WELKE SCHADE GAAT HET?

- Brand en/of hitte: 70 % van de branden ontstaat buiten het datacenter, slechts 30 % binnen in het datacenter.
- Vocht, water en/of damp: door (blus)water en/of waterlekkage.
- Rook en/of corrosieve gassen: door brand en blussing in aangrenzende ruimten.
- Inbraak en/of ongeoorloofde toegang.
- Magnetische velden en trillingen: door zware machines net buiten het datacenter of bijvoorbeeld een spoorbaan vlak naast het gebouw waarover circa viermaal per uur een trein rijdt.
- Stof door (ver)bouw buiten het datacenter en/of het gebouw of anderszins.
- Blikseminslag.

VERSCHILLEN IN BOUWCONCEPTEN

Zoals gezegd bestaan er verschillende bouwconcepten voor ict-security die onderling een aantal verschillen kennen. Een belangrijk verschil zit in de maxima aan temperaturen en de luchtvochtigheid die bij een bevlamming buiten het datacenter, binnen in het datacenter kan ontstaan, en de garanties die daarop worden afgegeven door de fabrikant. Bij het ene concept wordt een maximumtemperatuur van 40 °C en een relatieve luchtvochtigheid (RLV) van 60 % gegarandeerd en bij een ander concept 60 °C en RLV 80 %. Bij sommige concepten wordt helemaal niets gegarandeerd.
Deze verschillen komen voort uit het bouwontwerp, het gekozen bouwmateriaal, de wijze waarop de verschillende bouwonderdelen met elkaar worden verbonden en de wijze

BESCHERMING TEGEN BRAND

BESCHERMING TEGEN BRAND VOLGENS HET BOUWBESLUIT

bouweis: betonnen wand (DIN 4102 F90)
bevlamming: 1.100 °C
temperatuur na 90 minuten: 200 °C
relatieve vochtigheid na 90 minuten: >100 %

BESCHERMING TEGEN BRAND VOLGENS BOUWCONCEPT VOOR ICT-BEVEILIGING (EN-1047 2)

bevlamming: 1.100 °C
temperatuur na 90 minuten: maximaal 60 °C
relatieve vochtigheid na 90 minuten: <70 %

BESCHERMING TEGEN (BLUS)WATER

Wanneer u bedenkt dat bij een blussing meer dan 1.600 liter water per minuut wordt gebruikt, zult u begrijpen dat een groot deel van dit water door betonnen wanden, plafonds en dergelijke heen komt en mogelijk binnen het datacenter terecht zal komen.

waarop tests door onafhankelijke keuringsinstanties hebben plaatsgehad (als deze al zijn uitgevoerd). Bij sommige concepten zijn namelijk alleen de losse wanden getest, maar niet het totaalconcept met wanden, hoeken, dak en vloer, terwijl verbindingen en hoeken nu juist de kwetsbaarste plekken zijn. Om teleurstellingen achteraf te voorkomen is het dan ook van groot belang kennis te nemen van de uitgevoerde tests, voordat de keus van een bouwconcept wordt gemaakt.

Een tweede, belangrijk verschil zit in het aantal minuten waarop de garanties worden afgegeven. Bij het ene concept geldt een brandwerendheid van 120 minuten en bij een ander concept geldt dit voor slechts 60 minuten.

Het derde verschil zit 'm in het aantal facetten waarvoor het bouwconcept bescherming biedt. Biedt het concept behalve bescherming tegen temperatuur, RLV en vocht, ook bescherming tegen blikseminslag, magnetische velden en trillingen?

AANDACHTPUNTEN BIJ KEUZE BOUWCONCEPT

De vraag is natuurlijk waarop de eindgebruiker of eigenaar moet letten, wanneer hij een bouwconcept voor ict-beveiliging gaat kiezen. In de allereerste plaats zal de eigenaar of eindgebruiker zich moeten afvragen hoe lang continuïteit wordt vereist binnen de organisatie en wat de gevolgen en kosten zijn van uitval van de bedrijfskritische processen bij een x aantal minuten binnen de organisatie.

Ook zal hij een inschatting moeten maken welke schades kunnen worden verwacht. (Als de waterleidingen van het gebouw direct boven het datacenter lopen, is een risico van waterlekkage natuurlijk groter dan als de waterleidingen zich ver van het datacenter bevinden.)

PRIJS-PRESTATIEVERHOUDING

Op basis van de resultaten van deze exercitie kan de eigenaar of eindgebruiker een eerste selectie maken uit de bouwconcepten. Vervolgens kunnen de resterende bouwconcepten worden beoordeeld op de normen waaraan ze voldoen en de garanties die worden afgegeven door de fabrikant (uniek is Lampertz met haar verzekerde concepten voor 50 miljoen euro). Daarnaast zijn de uitgevoerde tests (hoe en waarop is getest) van belang en de verborgen 'gebreken' in het concept. Bijvoorbeeld hoe worden kabeldoorvoeren geopend en gedicht, hoe brand- en inbraakwerend is het overdrukrooster wat door de fabrikant wordt geleverd, hoe kan iets aan de wanden worden bevestigd zonder dat dit boorgaatjes in de wanden tot gevolg heeft en nog meer van dergelijke. Als laatste, maar een niet onbelangrijk aspect, moet het kostenplaatje van het concept passen in het budget en moet de prijs-prestatieverhouding juist zijn.

Conform de EN 1047-2 is een aantal bouwconcepten ontwikkeld en op de markt gebracht die de kritische ict-apparatuur beschermen tegen schade van buitenaf.