Continuïteit begint in computerruimte

In de huidige 24/7-cultuur is beschikbaarheid de sleutel. De continuïteit van de onderneming is mede afhankelijk van de beschikbaarheid van faciliteiten, medewerkers en informatie. ICT-managers doen er veel aan om hun ICT te beveiligen tegen hedendaagse risico's die de 24/7-cultuur met zich meebrengt. Bij beveiliging denken ICT-managers in eerste instantie aan technische beveiligingsmaatregelen op netwerk- en systeemniveau, maar ze vergeten daarbij de fysieke beveiliging van computerruimten.

Water, vuur, inbrekers maar ook bliksem bedreigen de computerruimtes. Toch kunnen ICT-managers veel van deze bedreigingen het hoofd bieden door preventie en detectie en, als het kwaad al is geschied, een adequaat noodplan. Uitval kan worden veroorzaakt door brand, rook, sabotage, ondeskundig gebruik, gebruik door onbevoegden of inbraak en zelfs zaken als blikseminslag of wateroverlast komen voor. Om tegen dergelijke risico's bescherming te bieden, moeten bedrijven een aantal maatregelen nemen. Het is duidelijk dat constante kwaliteit van de maatregelen en eisen die voor computerruimten gelden van essentieel belang is. Behalve één of meerdere computerruimten moeten ook de ondersteunende technische ruimten zoals kabel invoerruimten worden beveiligd. In deze ruimten bevindt zich de apparatuur voor de ondersteunde processen. Uitval van een van deze ruimten kan vergaande gevolgen hebben zoals uitval van internet en telefonie en een falende dienstverlening. Dit artikel beschrijft een aantal van de maatregelen die meerdere risico's kunnen afdekken. Het artikel is niet uitputtend.

Algemene eisen

De eerste eisen die bedrijven aan computerruimten moeten stellen, lijken heel voor de hand liggend. Computerruimten liggen bij voorkeur niet aan de buitenzijde op de begane grond van een gebouw. Ook is het verstandig dat computerruimten niet beneden het maaiveld of op zolders worden gelokaliseerd omdat hierdoor de kans op vloeistofschade aanzienlijk toeneemt. Pijpleidingen en verwarmingsbuizen vormen een risico voor vloeistofschade. In principe mogen er geen vloeistoffen in of door de ruimte lopen en als dit niet te voorkomen is, moet onder de leidingen een aflopende opvangbak worden geplaatst die de vloeistof bij lekkage buiten de ruimte leidt. Vloeistofdetectoren op de vloer kunnen ervoor zorgen dat eventuele lekkages tijdig worden gesignaleerd.

Een computerruimte is in principe niet voorzien van ramen. Indien er wel ramen aanwezig zijn moeten deze voorzien worden van extra inbraakvoorzieningen, zonwerende folie of eventueel bouwkundige afscherming.

Om uitval van systemen te voorkomen is ook de toegankelijkheid van de ruimte van belang. Apparatuur gaat immers op de meest onmenselijke tijden kapot en technici moeten 24 uur per dag en 7 dagen in de week bij de apparatuur kunnen voor reparatie. Bedrijven moeten voorkomen dat technici door het gebouw moeten zwerven op zoek naar de computerruimten. Om dit te voorkomen moeten de computerruimten bij voorkeur via een algemene ruimte of gang bereikbaar en duidelijk herkenbaar zijn.

De doelstelling van toegangsbeveiliging is dat alle computerruimte(s) en 19 inch kast(en) waarin de apparatuur staat opgesteld, uitsluitend toegankelijk zijn voor personen die daar binnen het kader van hun functie werkzaamheden moeten verrichten. Men kan dit faciliteren met behulp van een toegangscontrolesysteem of met fysieke sleutels. Het belangrijkste is dat het toegangsbeheer controleerbaar, verifieerbaar en reproduceerbaar is. Vanuit zowel technisch als vanuit beveiligingsoogpunt is een goede projectering van computerruimten van cruciaal belang.

Bouwkundige beveiliging

Bij bouwkundige beveiliging wordt vaak gedachte aan hang- en sluitwerk. Echter in het kader van computerruimtes dient bij bouwkundige beveiliging ook de fysieke strekte van deuren, ramen, wanden vloeren en plafond te worden bekeken. Een ideale computerruimte is bij voorkeur een bouwkundig compartiment, met voldoende weerstand tegen braak, branddoorslag en brandoverslag. In de praktijk zien we dat de bouwkundige beveiliging nogal wat problemen geeft waardoor zowel de brandbeveiliging als de inbraakbeveiliging tekort worden gedaan.

Wanden worden vaak tussen de verhoogde computervloer en het verlaagde plafond geplaatst waardoor personen met kwade bedoelingen een tegel kunnen verwijderen uit de computervloer en onder de wand door kunnen kruipen. Ook in geval van brand is deze constructie funest en kan de brand in dit soort situatie gemakkelijk via het plafond, of onder de vloer, overslaan naar een andere ruimte. Een soortgelijke situatie doet zich voor bij het verlaagde plafond. Het is dus belangrijk dat wanden goed aansluiten aan de dragende vloer en het bovenliggende dragende plafond.

Ook kabelgoten vormen een veiligheidsrisico. De bekabeling moet bij voorkeur buiten het zicht door het gebouw worden gerouteerd omdat anders het gevaar ontstaat van sabotage en manipulatie van de kabels. In kelders, zolders en -parkeergarages kan de bekabeling door gesloten stalen kabelgoten worden gerouteerd die tevens brandgevaarlijke situaties voorkomen. Uiteraard dienen de kabeldoorvoeren brandwerend afgedicht te zijn.

"In de praktijk zien we dat de bouwkundige beveiliging nogal wat problemen geeft waardoor zowel de brandbeveiliging als de inbraakbeveiliging tekort worden gedaan."

Infrastructuur

Betrouwbare verbindingen tussen de computerruimte en de buitenwereld zijn in het kader van continuïteit van cruciaal belang. Vanuit deze optiek kunnen computerruimten best via meerdere wegen worden ontsloten naar de buitenwereld. Dit kan bijvoorbeeld door vanuit verschillende computerruimten verbindingen naar de openbare infrastructuur aan te leggen, waarbij deze verbindingen bij voorkeur op verschillende plaatsen het gebouw verlaat. Bij voorkeur wordt er gebruikgemaakt van openbare infrastructuur van verschillende providers.

Wanneer een bedrijf over meerdere vestigingen beschikt kan het een optie zijn per vestiging maar één aansluiting naar de openbare infrastructuur aan te leggen en de vestigingen onderling aan elkaar te knopen. Eisen voor infrastructuur dienen in een zo vroeg mogelijk stadium bekend te zijn, te meer omdat het procedé om graafvergunningen te verkrijgen in veel gevallen een langdurig traject kan zijn. Groot voordeel is dat men tegenwoordig op kantoor veel gebruikmaakt van de mobiele telefoon en dat er veel laptops voorzien van draadloos internet. Vanuit continuïteitsoptiek zijn we hierdoor dus minder afhankelijk geworden van de vaste telecom en internetinfrastructuur in en rond gebouwen.

Elektra-infrastructuur

ICT kan niet functioneren zonder stroom. In het kader van computerruimtes en continuiteit is het van belang om hier over na te denken. Bedrijven ondervinden gemiddeld 10 maal per jaar een computeruitval. De gemiddeld benodigde tijd om weer operationeel te zijn bedraagt 4 uur. De benodigde tijd om een netwerk weer operationeel te krijgen kan tot 48 uur oplopen.

Een bedrijf dient zich af te vragen hoelang de ICT-omgeving actief moet blijven bij uitval van het energienet? Welke maatregelen heeft u genomen? Heeft u een UPS of een noodstroomaggregaat staan? Of beide? Zo ja, test u deze wel eens? En als u een noodstroomaggregaat heeft staan, heeft u dan ook afspraken met een brandstofleverancier? Kunt u deze ook laten komen op zon- en feestdagen? Kortom een paar vragen die direct verbandhouden met een noodstroomaggregaat.

Vaak worden UPS en noodstroomaggregaat in vestigingsperspectief geplaatst en niet in bedrijfsperspectief.

Daarnaast speelt bij computerruimtes de vraag of we iets met bliksembeveiliging moeten doen. Door een indirecte inslag kan een overspanning of inductie in de computerruimte terechtkomen via datakabels, elektriciteitsvoeding, waterleidingen, bewapening van de betonconstructie van het gebouw etc. waardoor schade aan de apparatuur ontstaat. Er wordt aanbevolen om de hele ruimte te laten voorzien van overspanning en inductiebeveiliging.

Brandbeveiliging

Om brand in een vroegtijdig stadium te kunnen ontdekken, zijn gebouwen en ruimten voorzien van brandmeldinginstallaties.

Brandmeldingen worden doorgestuurd naar alarmcentrales of bewaakte meldposten die op hun beurt de brandweer alarmeren.
In computerruimten levert het nogal eens problemen op om de rook van een beginnende brand (ook wel smeulbrand genoemd) snel te detecteren. Dit wordt onder andere veroorzaakt door luchtstromen van airco's. Door de airco is er sprake van een verhoogde luchtsnelheid waardoor conventionele brandmelders niet of nauwelijks werken. Toch is het van cruciaal belang om brand snel te detecteren en werknemers te alarmeren. Een van de belangrijkste redenen hiervoor is de hoge schadeposten die ontstaan bij brand in computerruimten.
De zogenaamde aspiratiedetectiesystemen zijn in staat smeulbrand snel te detecteren. Een aspiratiedetectie kan worden gezien als een rookaanzuigsysteem dat monsters neemt van de lucht om die te testen op aanwezigheid van rook. De luchtmonsters worden met behulp van een pomp aangezogen via een leidingnetwerk in de computerruimte. Dit aanzuigen gebeurd vanaf de verschillende testpunten. In het aspiratiedetectiesysteem worden de luchtmonsters eerst gefilterd om stofdeeltjes en andere vervuiling te verwijderen. Vervolgens worden de proefmonsters in een detectiekamer gebracht, waar een lichtbron het monster test op aanwezigheid van rook. Dit testen gebeurt door het meten van de lichtverduistering. De waardes van de lichtverduistering kunnen liggen tussen 0,005 en 20%. Doordat de meeting instelbaar is ontstaat een grote mate van nauwkeurigheid van de detector. De resultaten van de metingen worden weergegeven op een controlepaneel of via een interface doorgegeven aan een brandmeldsysteem, waarna het mogelijk is om een ontruimingsalarm en een blusinstallatie aan te sturen.

Gasblusinstallaties

Gasblusinstallaties worden gebruikt om branden te blussen in computerruimten met hoogtechnologische en kostbare apparatuur waar verontreinigende blusinstallaties uit den boze zijn. Dit betekent dat wanneer er brand ontstaat er gas in de ruimte wordt geblazen waardoor het vuur geen zuurstof meer krijgt en dus niet meer kan uitbreiden en zelfs zal doven. Vanwege het gebruik van dit blusgas is het noodzakelijk om de ruimten vlak voor het blussen te ontruimen.

Sprinklerinstallaties

Het klinkt raar maar sinds een aantal jaren is het mogelijk om computerruimten te voorzien van sprinklerinstallaties. In het kader van de milieuregelgeving zijn hierover speciale afspraken gemaakt tussen de overheid enerzijds en de verzekeraars anderzijds. De computerruimten worden met water geblust, wat naast waterschade ook restschade geeft. Bedrijven die gebruikmaken van een sprinklerinstallatie in een computerruimte hebben een speciale verzekering nodig. Omdat er met water wordt geblust zijn er nog bijkomende risico's in verband met de in dit soort ruimtes aanwezige elektriciteit. Dit vraagt om specifieke procedures.

Watermist

In plaats van sprinklerinstallaties wordt de laatste jaren hoge druk watermist in computerruimten gebruikt. Doordat watermist elektrisch zeer slecht geleidend is en niet corrosief is, is het veilig bij gebruik in de aanwezigheid van elektrische apparatuur en kan het dus toegepast worden in computerruimten. Door het gebruik van watermist is het gevaar van een thermische schok op elektronische apparatuur niet aanwezig. Dit is een groot voordeel ten opzichte van CO_2. Er dient te worden vermeld dat watermist geen deeltjes of olieachtig residu achterlaat waardoor elektronische apparaten, computers, software, datafiles en andere communicatie apparatuur zouden kunnen beschadigen.

Conclusie

Zoals in de inleiding aangegeven is dit artikel verre van volledig. Duidelijk is dat computerruimten een cruciale rol spelen in de continuïteit van de ICT-dienstverlening. Helaas worden de genoemde onderwerpen nog wel eens onderbelicht waardoor de continuïteit van de ICT-dienstverlening onder druk komt te staan en dit terwijl de computerruimte met zijn infrastructuur de fundering vormt voor de 7/24 ICT-dienstverlening.

(Door Ronald Eygendaal)