Continuïteit begint in

De continuïteit van een onderneming is mede afhankelijk van de beschikbaarheid van faciliteiten, medewerkers en informatie. ICT-managers doen er veel aan om hun werkveld te 'beveiligen' tegen risico's die de 24/7-cultuur met zich meebrengt. Hierbij vergeten zij vaak de fysieke beveiliging van computerruimten. In dit artikel een aantal maatregelen om risico's af te dekken. Ronald Eygendaal *

Water, vuur, inbrekers en bliksem. Allemaal bedreigingen voor computerruimten. Maar ICT-managers kunnen veel van deze bedreigingen het hoofd bieden door preventie en detectie en een adequaat noodplan. Behalve één of meerdere computerruimten moeten ook de ondersteunende technische ruimten zoals kabelinvoerruimten en noodaggregaatruimten worden beveiligd. Uitval van een van deze ruimten kan vergaande gevolgen hebben, zoals uitval van communicatiesystemen en netwerkverbindingen en een falende dienstverlening.

Algemene eisen

Computerruimten liggen bij voorkeur niet aan de buitenzijde op de begane grond van een gebouw. Ook is het verstandig dat ze 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. Als dit niet te voorkomen is, moet onder de leidingen een aflopende opvangbak worden geplaatst die bij lekkage de vloeistof buiten de ruimte leidt. Vloeistofdetectoren op de vloer kunnen eventuele lekkages tijdig signaleren.
Een computerruimte is in principe niet voorzien van ramen. Als er toch ramen zijn, moeten deze worden voorzien van extra inbraakvoorzieningen, zonwerende folie of eventueel bouwkundige afscherming.
Technici moeten 24 uur per dag en zeven dagen in de week bij de apparatuur kunnen voor reparatie. Om te voorkomen dat technici in het gebouw moeten gaan zoeken naar de computerruimten, moeten deze ruimten bij voorkeur via een algemene ruimte of gang bereikbaar en duidelijk herkenbaar zijn.
De doelstelling van toegangsbeveiliging is dat alle computerruimte(n) en 19 inch kast(en) waarin de apparatuur staat opgesteld, uitsluitend toegankelijk zijn voor personen die daar uit hoofde van hun functie werkzaamheden moeten verrichten. Men kan dit faciliteren met een pasjessysteem of met fysieke sleutels. Het toegangsbeheer moet controleerbaar, verifieerbaar en reproduceerbaar zijn.

Bouwkunde

Bij bouwkundige beveiliging wordt vaak gedacht aan hang- en sluitwerk. Maar ook de fysieke sterkte van deuren, ramen, wanden vloeren en plafond dient te worden bezien. In het Bouwbesluit van 1992 zijn de begrippen 'weerstand tegen branddoorslag en brandoverslag' geïntroduceerd. Deze beogen dat een beginnende brand tot een bepaalde omvang beperkt blijft. Men gaat daarom uit van zogenoemde 'brandcompartimenten'. Doel hiervan is een eventuele brand te beperken tot één of meer brandcompartimenten.
De eis 'weerstand tegen branddoorslag en brandoverslag 'wordt uitgedrukt in minuten: 20, 30 of 60 minuten. De weerstand moet worden bepaald via de NEN-norm 6068.
In de praktijk blijkt het juist interpreteren van de voorschriften nogal wat problemen te geven waardoor zowel de brandbeveiliging als de inbraakbeveiliging te kort wordt gedaan. Wanden worden vaak tussen de verhoogde computervloer en het verlaagde plafond geplaatst waardoor kwaadwillenden een tegel kunnen verwijderen uit de computervloer en onder de wand door kunnen kruipen. Ook in geval van brand is deze constructie funest; brand kan dan gemakkelijk via het plafond of onder de vloer overslaan naar een andere ruimte.
Een soortgelijke situatie doet zich voor bij het verlaagde plafond. Wanden moeten dan ook goed aansluiten op de dragende vloer en het bovenliggende dragende plafond.
De bekabeling moet bij voorkeur buiten het zicht door het gebouw worden geplaatst, 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 waarmee tevens brandgevaarlijke situaties worden voorkomen. Uiteraard dienen de kabeldoorvoeren brandwerend afgedicht te zijn.

Infrastructuur

Betrouwbare verbindingen tussen de computerruimte en de buitenwereld zijn in het kader van continuïteit van cruciaal belang. Vanuit deze optiek kunnen computerruimten het beste 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

computerruimte

foto: EvoSwitch

Computerruimten spelen een cruciale rol in de continuïteit van de ICT-dienstverlening

op verschillende plaatsen het gebouw verlaten. Zo biedt KPN een dergelijke dienst onder de naam cityring. Wanneer een bedrijf over meerdere vestigingen beschikt, kan het een optie zijn per vestiging een aansluiting naar de openbare infrastructuur aan te leggen en de vestigingen onderling per staalverbinding aan elkaar te knopen. Bedrijven kunnen een bedrijfsnummer aanvragen bij de OPTA. Bedrijfsnummers, ook wel 088-nummers of nomadische nummers genoemd, geven de mogelijkheid aan bedrijven die over meerdere locaties met verschillende netnummers verspreid zijn, onder één nummerblok bereikbaar te zijn. Diverse providers bieden voor deze diensten een webinterface aan waarmee direct wijzigingen in de routering kunnen worden doorgevoerd. De klant kan dit geheel zelfstandig doen. Groot voordeel vanuit continuïteitsoptiek is dat in geval van nood al het telefoonverkeer binnen tien minuten naar andere nummers kan worden doorgezet. Uiteraard dienen er dan op een andere locatie van het bedrijf voldoende telefoonnummers en werkplekken beschikbaar te zijn. Overigens kan men bij diverse marktpartijen telefonie-uitwijk inkopen, waardoor de noodzaak voor voldoende telefoonnummers en werkplekken komt te vervallen.

Elektra-infrastructuur

Bedrijven ondervinden gemiddeld tien maal per jaar een computeruitval. De gemiddeld benodigde tijd om weer operationeel te zijn bedraagt vier uur. De benodigde tijd om een netwerk weer operationeel te krijgen kan tot 48 uur oplopen.
Een bedrijf dient zich af te vragen hoe lang de ICT-omgeving actief moet blijven bij uitval van het energienet. Wat gebeurt er bijvoorbeeld als een straal- »

verbinding uitvalt? Nemen dan de continuïteitsrisico's voor andere vestigingen toe?
Ook de migratie naar VoIP kan een reden zijn om naar de stroomvoorziening te kijken. Vaak kunnen via inline poweroplossingen VoIP-telefoons stroom krijgen, maar niet altijd.
Mochten UPS en noodstroom geen uitkomst bieden, dan kan een slim gebruik van bedrijfsnummers of telefonie-uitwijk aan te bevelen zijn.
Een Nood Stroom Aggregaat (NSA) moet regelmatig worden getest. En zijn er afspraken gemaakt met een brandstofleverancier? Vaak worden UPS en noodstroomaggregaat in vestigingsperspectief geplaatst en niet in bedrijfsperspectief.
Door een indirecte blikseminslag kan een overspanning of inductie in de computerruimte terechtkomen via datakabels, elektriciteitsvoeding, waterleidingen, bewapening van de betonconstructie van het gebouw et cetera. Aanbevolen wordt de gehele computerruimte te laten voorzien van overspanning en inductiebeveiliging.

Betrouwbare verbindingen tussen de computerruimte en de buitenwereld zijn in het kader van continuïteit van cruciaal belang

Brandbeveiliging

In computerruimten levert het nogal eens problemen op om de rook van een beginnende brand 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.
De zogenoemde aspiratiedetectiesystemen kunnen smeulbrand snel detecteren. Een aspiratiedetectie kan worden gezien als een rookaanzuigsysteem dat luchtmonsters neemt om deze te testen op de aanwezigheid van rook. In het aspiratiedetectiesysteem worden de luchtmonsters eerst gefilterd om stofdeeltjes en andere vervuiling te verwijderen. Vervolgens worden de proefmonsters in een detectiekamer getest door het meten van de lichtverduistering. De waardes hiervan kunnen liggen tussen 0,005 en 20 procent. Doordat de meting instelbaar is, ontstaat een grote mate van nauwkeurigheid van de detector.
Globaal bekeken zijn er twee automatische blusmethoden voor computerruimten: gasblusinstallaties en sprinklerinstallaties. Gasblusinstallaties worden gebruikt om branden te blussen in computerruimten met hoogtechnologische en kostbare apparatuur waar verontreinigende blusinstallaties uit den boze zijn. Bij brand wordt er gas in de ruimte 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.
Het is 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, hetgeen 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 ruimten aanwezige elektriciteit. Dit vraagt om specifieke procedures.
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 haar infrastructuren de fundering vormt voor de 7/24 ICT-dienstverlening.

Bronnen

» *White paper computerruimten Versie 1.5 Getronics PinkRoccade feb. 2006*
» *Fysieke Netwerkbeveiliging begint in computerruimte, Telecommagazine november 2003* «

Ronald Eygendaal is werkzaam als Security Consultant bij Getronics PinkRoccade en heeft meer dan vijftien jaar ervaring in beveiliging, fraudeonderzoeken en informatiebeveiliging in het bijzonder. Hij is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN)

Samenvatting

» Bedrijven ondervinden **gemiddeld tien maal per jaar** een **computeruitval**.
» Behalve één of meerdere computerruimten moeten ook de **ondersteunende technische ruimten** zoals kabelinvoerruimten en noodaggregaatruimten worden beveiligd.
» Computerruimten liggen bij voorkeur niet aan de buitenzijde op de begane grond. **Pijpleidingen en verwarmingsbuizen** vormen een **risico voor vloeistofschade**.
» De **ramen** van een computerruimte moeten worden voorzien van **extra inbraakvoorzieningen, zonwerende folie** of eventueel **bouwkundige afscherming**.
» Technici moeten **24 uur per dag** en **zeven dagen in de week** bij de apparatuur kunnen voor reparatie.
» Bij computerruimten moet ook de **fysieke sterkte** van deuren, ramen, wanden vloeren en plafond worden bezien.
» Aanbevolen wordt de hele computerruimte te laten voorzien van **overspanning** en **inductiebeveiliging**.