oktober 2008 nummer 6

INFORMATIEBEVEILIGING

Een blik achter de schermen van Cyber Storm II

ENISA, een nadere kennismaking

SELinux: access control op basis van least privilege

Fysieke beveiliging van computerruimtes nader bekeken

Deel 3: RBAC - een procesbenadering

PvIB
Platform voor InformatieBeveiliging

http://creativecommons.org/licenses/by-sa/3.0/nl/

ib

Continuïteit begint in computerruimte

Auteur: Ronald Eygendaal > 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).

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 computerruimtes.

Water, vuur, inbrekers, maar ook bliksem vormen een bedreiging voor computerruimtes. Toch kunnen ICT-managers veel van deze kwaden het hoofd bieden door preventie en detectie en, als het kwaad al is geschied, middels 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 zal duidelijk zijn dat constante kwaliteit van de maatregelen en eisen die voor computerruimtes gelden van essentieel belang zijn.

Behalve één of meerdere computerruimtes moeten ook de ondersteunende technische ruimten zoals kabel invoerruimten en noodaggregaatruimten worden beveiligd. In deze ruimten bevindt zich de apparatuur voor de ondersteunende processen. Uitval van één van deze ruimten kan vergaande gevolgen hebben zoals uitval van communicatiesystemen en netwerkverbindingen en een falende dienstverlening. Preventief kan bijvoorbeeld worden besloten faciliteiten zoals de stroomvoorziening meervoudig aan te bieden ter reductie van het risico.

Dit artikel beschrijft een aantal maatregelen die meerdere risico's kunnen afdekken. Het artikel is niet uitputtend en volledig. Overigens staat ook hier de tijd niet stil. Een trend in de industrie lijkt op dit moment het ontstaan van grote datacenters die veel van de zaken die hier aan bod komen, kunnen aanbieden voor een groot aantal afnemers. Die doorkijk naar de (nabije) toekomst willen we u niet onthouden en die is door het verhaal heen geweven. Dit alles doet niets af aan de principes die opgaan voor computerruimtes.

Algemene eisen

De eerste eisen die bedrijven aan computerruimtes moeten stellen, lijken heel voor de hand liggend. Computerruimtes liggen bij voorkeur niet aan de buitenzijde op de begane grond van een gebouw. Ook is het verstandig dat computerruimtes 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 bij lekkage de vloeistof 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.

Was vroeger de praktijk dat een bedrijf een eigen rekencentrum had, tegenwoordig is het shared managed datacenter 'hot'. Enerzijds mogelijk door toegenomen miniaturisatie van componenten en anderzijds door schaalvergroting toe te passen en meerdere klanten vanuit één site te hosten. Typische datacenters ontstaan zo op grote industrieterreinen.

Om uitval van systemen te voorkomen is ook de toegankelijkheid van de ruimtes 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. Het liefst voorkomen we echter dat technici door het gebouw gaan zwerven op zoek naar de computerruimtes. Om dit te voorkomen, moeten de computerruimtes bij voorkeur via een algemene ruimte of gang bereikbaar en duidelijk herkenbaar zijn. Preventief kan men een hardware opstelling al voorzien van redundante componenten die remote kunnen worden 'omgestoken' zodat menselijke handelingen zoveel mogelijk achterwege kunnen blijven. Servers zijn in hoge mate uitwisselbaar tegenwoordig.

De doelstelling van toegangsbeveiliging is dat alle computerruimtes en 19 inch kasten 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 behulp van een pasjessysteem of met fysieke sleutels. Het belangrijkste is dat de toegang beheersbaar en controleerbaar is. Dit heeft ook gevolgen voor de organisatie van de aanbieder van de dienstverlening. Ofwel er moet iemand on site aanwezig zijn om toegang te verlenen ofwel er zal iemand op aanvraag wijzigingen in de verbindingen moeten aanbrengen zodat een uitgevallen server vervangen wordt.

Bouwkunde

Bij bouwkundige beveiliging wordt vaak gedacht aan hang- en sluitwerk. Echter in het kader van computerruimtes dient bij bouwkundige beveiliging ook de fysieke sterkte van deuren, ramen, wanden, vloeren en plafond te worden bezien. Een ideale computerruimte is bij voorkeur een bouwkundig compartiment, met voldoende weerstand tegen branddoorslag en brandoverslag. 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 zogenaamde 'brandcompartimenten'. Doel hiervan is wanneer er in een gebouw brand uitbreekt deze brand te beperken. De eis 'weerstand tegen branddoorslag en brandoverslag' wordt uitgedrukt in minuten: twintig, dertig of zestig minuten. Hiervoor is de NEN-norm 6068 opgesteld.

In de praktijk zien we dat het juist interpreteren van de voorschriften nogal wat problemen geeft waardoor zowel de brandbeveiliging als de inbraakbeveiliging tekortschieten.

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 slaat in dit soort situaties gemakkelijk via het plafond of onder de vloer over naar een andere ruimte.

Een soortgelijke situatie doet zich voor bij het verlaagde plafond. Het is dus belangrijk dat wanden goed aansluiten op 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.

Een andere mogelijkheid, juist goed mogelijk bij de bredere toepassing van 19 inch kasten, is de bekabeling vanuit een beschermde goot van boven of beneden te laten komen en af te werken in de kasten. Op deze wijze is de bekabeling niet meer separaat toegankelijk terwijl het optisch een veel beter - netter - beeld geeft dan de spaghetti die vroeger nog wel eens uit kasten placht te puilen. Omdat de bekabeling desnoods remote kan worden geschakeld, vermindert ook de behoefte aan fysieke toegang tot de ruimte.

Infrastructuur

Betrouwbare verbindingen tussen de computerruimte en de buitenwereld zijn in het kader van continuïteit van cruciaal belang. Vanuit deze optiek kunnen computerruimtes 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 op verschillende plaatsen het gebouw verlaten. KPN biedt bijvoorbeeld een dergelijke dienst onder de naam cityring. 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 per straalverbinding aan elkaar te knopen. Eisen voor infrastructuur dienen in een zo vroeg mogelijk stadium bekend te zijn, te meer omdat het procedé om vergunningen voor graafwerkzaamheden te verkrijgen in veel gevallen een langdurig traject kan zijn.

Sinds 2004 is het voor bedrijven mogelijk om speciale bedrijfsnummers bij de OPTA aan te vragen. 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 (bijvoorbeeld 088-660xxxx) bereikbaar te zijn. Het bedrijfsnummer begint altijd met 088-. Het maakt daarbij niet uit waar het bedrijf zich in Nederland bevindt.

Diverse providers bieden voor deze diensten een webinterface aan. Met deze webinterface kunnen direct wijzigingen in de routering worden doorgevoerd. De klant kan dit geheel zelfstandig doen. Groot voordeel vanuit continuïteitsoptiek is dat in geval van nood al het telefoonverkeer eenvoudig en snel (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 of in ieder geval minder zwaar weegt.

Elektra-infrastructuur

ICT kan niet functioneren zonder stroom. In het kader van computerruimtes en continuïteit is het van belang om hierover na te denken. Bedrijven ondervinden gemiddeld tien maal per jaar een stroomuitval. 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? Denk bijvoorbeeld aan straalverbindingen die u in gebruik heeft. Wat gebeurt er nu als deze uitvallen? Nemen dan

de continuïteitsrisico's voor andere vestigingen toe?

Ook de migratie naar VoIP kan een reden zijn om eens grondig naar de stroomvoorziening te kijken, immers een VoIP telefoon heeft stroom nodig. Vaak kunnen via inline power oplossingen VoIP telefoons stroom krijgen, maar niet altijd. Mochten UPSen en noodstroom geen uitkomst bieden, denk dan eens aan het slim gebruiken van bedrijfsnummers of telefonie-uitwijk.

Nog even terug naar het Nood Stroom Aggregaat (NSA), heeft u ook zo'n ding staan? Test u het aggregaat wel eens? En heeft u afspraken met een brandstofleverancier? Kortom een paar vragen die direct verband houden met een NSA.

Moeten we iets aan bliksembeveiliging doen? Als gevolg van een inslag kan een overspanning of inductie in de computerruimte terechtkomen via datakabels, elektriciteitsvoeding, waterleidingen, bewapening van de betonconstructie van het gebouw et cetera waardoor schade aan de apparatuur ontstaat.
Aanbevolen wordt het gehele datacenter te laten voorzien van overspanning- en inductiebeveiliging. Zeker voor grotere gebouwen, bijvoorbeeld wanneer ze het hoogste gebouw in de omgeving zijn, is het aan te bevelen aan de buitenkant bliksemafleiding aan te brengen. Zorg er dan wel voor dat de koperen leiding niet makkelijk toegankelijk is, vanwege diefstalgevaar.

Brandbeveiliging
Om brand in een vroegtijdig stadium te kunnen ontdekken, zijn gebouwen en ruimten voorzien van brandmeldinstallaties. Brandmeldingen worden doorgestuurd naar alarmcentrales of bewaakte meldposten die op hun beurt de brandweer alarmeren.

In computerruimtes 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 computerruimtes.

De zogenaamde aspiratie-detectiesystemen zijn in staat smeulbrand snel te detecteren. Een aspiratiedetectie kan worden gezien als een rookaanzuigsysteem dat monsters neemt van de lucht om deze te testen op aanwezigheid van rook De luchtmonsters worden met behulp van een pomp aangezogen via een leidingnetwerk in de computerruimte. Dit aanzuigen gebeurt vanaf de verschillende testpunten. In het aspiratie-detectiesysteem 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 procent. Doordat de meeting instelbaar is, ontstaat een grote mate van nauwkeurigheid van de detector.

De resultaten van de metingen worden weergegeven via een controlepaneel of via een interface doorgegeven aan een brandmeldsysteem. Waarna het mogelijk is om een ontruimingsalarm en een gasbuisinstallatie aan te sturen. Door een tijdige melding is een ordelijke ontruiming van de ruimten mogelijk voordat wordt overgegaan tot blussen.

Globaal bekeken zijn er twee automatische blusmethodes voor computerruimtes, namelijk: gasblusinstallaties en sprinklerinstallaties.
Gasblusinstallaties worden gebruikt om branden te blussen in computerruimtes 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.

Het klinkt raar, maar sinds een aantal jaren is het mogelijk om computerruimtes te voorzien van sprinklerinstallaties. In het kader van de milieuregelgeving zijn hierover speciale afspraken gemaakt tussen de overheid enerzijds en de verzekeraars anderzijds. De computerruimtes 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 ruimten aanwezige elektriciteit. Dit vraagt om specifieke procedures.

Conclusie
Zoals in de inleiding aangegeven, is dit artikel verre van volledig. Duidelijk is dat computerruimtes 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. Dit terwijl de computerruimte met zijn infrastructuren de fundering vormt voor de 24/7 ICT-dienstverlening.

Bronnen

- *White paper computerruimtes Versie 1.5, Getronics PinkRoccade, feb. 2006.*
- *Fysieke Netwerkbeveiliging begint in computerruimte, Telecommagazine, november 2003.*
- *Afbeeldingen zijn afkomstig van http://flickr.com*