Om design av ett högsäkerhets serverrum (Klass 1)

av Glenn Larsson (2005)

InfoSäk D, KY - Enköping

På uppdrag av Magnus Andersson, Office Data

(*Konverterad till **PDF** 2008-Dec-01*)

Inledning:

Syftet med detta dokument är att ta reda på och sammanställa dom krav som ställs på ett modernt högsäkerhets serverrum (SR). Begränsningar har gjort till ett klass 1 serverrum då det var den högsta klassen och den mest intressanta att skriva om. Även en del förlängningar har gjorts för att öka säkerheten till en ännu högre nivå. Serverrummet är i exemplet ämnat att vara ett högsäkerhetsklassat serverrum för ett stort internationellt företag.

Syftet med ett säkert serverrum är att skydda företagets information, investeringar och personal ifrån stöld, brand, översvämning, informationsläckage, sabotage, driftstörningar och annat som kan påverka företagets överlevnad.

Det fysiska skyddet utgörs utav följande punkter:

- **Accesskontrol**, i fallet nedan så används lås, dörrar och biometri för att förhindra obehöriga att komma in i serverrummet.
- **Brandskydd**: Serverrummets väggar utgörs av ett kompositskydd (främst gips) som reducerar möjligheterna att brand kan penetrera rummet. Dessutom så finns ett brandlarm i rummet kopplat direkt till ett brandsläcknings system baserad på Argonit som fyller rummet på kort tid och låter personalen lämna området under lugna förhållanden.
- **Skydd för utrustning**: Datorutrustningen är rackmonterade i SS/EN1047-2 [**2**] klassade skåp som förhindrar stöld, brand, gas, fukt och vätska att förstöra utrustningen. Skåpet har dessutom kylning.
- **RÖS skydd** [1]: Serverrummet är avskärmat ifrån EM strålning, kablaget är avskärmat, ström och kommunikationskablage in/ut ur lokalen har linjefilter. Väggarna är dessutom ljudisolerade.
- **Övervakning/detektering**: Serverrummet, Fastigheten och Huset är övervakat via kamera. Även sensorer som varnar för gas, vätska, fukt och brand finns installerade.
- **Respons:** ett vaktbolag finns på platssom även har personal på plats för kort responstid. Brand släcks automatiskt med ett automatiserat system för brandsläcknings, samt driftspersonal finns på plats 24 H/Dygn för att lösa andra problem på plats.
- **Informationskydd**: Systemet gör backuper och dessa tas om hand via personalen som deponerar kopior i ett SS/EN1047-2 klassat mediaskåp. Även kopior tas av en 3’e parts service provider som inte personalen har tillgång till.

[**1**] Se Appendix B

[**2**] Se Appendix C

Vilka krav ställs då på ett klass 1 Serverrum?

- Rummet ska uteslutande användas för datordrift, endast behörig personal har tillträde till datorrummet.
- Åtkomst till rummet ska autentiseras via kodkort, helst en biometrisk lösning.
- Alla enheter ska monteras i ett godtagbart låsbart datorskåp [**2**].
- Datorutrustningen ska separeras ifrån övrig el i huset och ha egen strömförsörjning ifrån ställverket och egna säkringar.
- Kommunikationskablar ska vara särskillda ifrån strömkablar så att inga störningar uppstår.
- Utrustningen ska ha en UPS som klarar driften i så lång tid som specificerats av systemägaren, det ska även finnas en reservkraft (t.ex Diesel generator) med en separat ström tillförsel till rummet.
- Utrustningen ska kylas av en redundant kylanläggning i en jämn temperatur på 22’ (C) [**1**]. Kylanläggningen ska även ha redundant strömförsörjning.
- Alla enheter ska vara rackmonterade.
- Det ska finnas en kontaktlista med personal som kan/ska tillkallas vid incidenter, t.ex nätverkstekniker och säkerhetsansvarig.
- Underhåll och funktionskontroll av systemfunktionen ska ske regelbundet [**1**].
- Dörren ska alltid vara låst, Låset till SR ska uppfylla kraven i **SS 200:3**.
- Lokalen får ej vara skyltat att det är ett SR.
- Det ska finnas larm som varnar när Fukt, Temperatur är inte håller dom angivna specifikationerna (För fukt är detta 85% [**1**], Temperaturen > 40’ (C)) eller om brand uppstår i lokalen, och brandvarnaren ska ha partikel detektering, inte rök detektering.
- Inget brännbart material får finnas i serverrummet.
- Alla elektriska installationer ska vara över golvnivå.
- Ett godkännt skåp för lagring av backuper ska finnas [**2**] utanför lokalen.
- Ingångar till huset ska övervakas av vaktbolag (med kamera eller vakt), även SR ska övervakas med kameror (realtidsövervakning).
- Ett fast monterat brandsläckningssystem ska finnas i lokalen.

[**1**] Rekommendation ifrån *Coromatic Datorsäkerhet AB*,
Privat seminarium om design av serverrum.

[**2**] Ska uppfylla kraven i **SS/EN1047-2**

Min design av serverrumet och hur det fungerar:

(En bild över serverrummet återfinns i **Appendix A**)

- Ett kompositskal byggs runt serverrummet. (Gips och Aluminium) Gipset skyddar emot brand och Aluminiumskalet reducerar RÖS. Gips valdes före betong då det är lätt att riva/bygga med om serverrummet behöver byggas ut, Aluminium valdes för samma orsak. I dagsläget så har serverrummet tillräckligt med expansionsmöjligheter.

- Kameraövervakning sker av huset (ingångar, parkeringar osv) och valda kritiska punkter (trapphus) samt serverrummet i realtid. Kamera övervakningen ska även ha IR kapabilitet ifall att strömmen till belysning avbryts.

- Ett vaktbolag (SECURITAS) övervakar fastigheten med personal på plats för kort responstid i fall att incident skulle uppstå. (t.ex fysiskt intrång)

- 2 st leverantörer av internet (ADSL, separata ingångar) i fall att den ena går ner. Kablarna dras ifrån 2 olika telestationer.

- 2 st leverantörer av elkraft, Båda leverantörerna har var sin ingång och leverar ifrån 2 olika infrastrukturer (t.ex under marken och via kabel över marken).

- Linjefilter installeras på all kommunikation och strömkabel för reduktion av RÖS.

- 2 st UPS installeras för redundans av ström. Det interna strömförsörjningssystemet tar kraft ur båda dessa UPS.

- Allt kablage är avskärmad med aluminium för att minimera störningar/RÖS. Kablaget är monterat i tak och separerat för sig, t.ex kommunikationskabel separat ifrån strömförsörjning.

- Kommunikationskabel ut/in ur serverrummet kopplas optiskt igenom väggen (Fiberoptik eller Optokopplare) för att reducera RÖS. (går kabeln sönder så kan den leda signal rakt in i aluminium höljet och göra om skyddet till en antenn)

- Reduntant kommunikationskabel går emellan serverskåpen som tillåter att servrarna kan replikera information mellan varandra i realtid.

- Datorutrustning rackmonteras (för ordningens skull) i SS/EN1047-2 klassade säkerhetsskåp med kylning (fläktar) pg av att väggarna är av gips som innebär att vätska kommer därför att läcka ut vid brand. Kylningen ska ha jämn temperatur och ska precisions kyla utrustningen.

- Ett larm varnar för abnormala halter av Gas/Fukt/Vätska som kan skada utrustningen/personalen.

- Ett brandlarm med partikelavkänning är kopplat direkt till ett gassläckningssystem med argonit finns monterat i rummet. Argongasbehållare är inlåsta i annat rum. Leveranssystemet för gasen är rör som ej leder ström för att reducera RÖS.

- En kontaktlista med personal vid incidenter finns fastmonterad på väggen vid dörren.

- Dörr brandklassad EI60/120 och som har ett godkännt lås enligt SS 200:3, samt automatiskt dörrstängare som håller dörren stängd.

- Biometrisk autentikering vid dörren som reagerar på tumavtryck och tummens värmesignatur.

- Installationsgolvet är ESD säkert (förhindrar statisk elektricitet) så ingen klimatkontroll behövs utanför skåpen. Dessutom är det utrustat med halkskydd.

- Backupskåp som uppfyller SS/EN1047-2 finns på *utsidan* av serverrummet.

<u>Saker som ej syns på bilden men sker:</u>

- Backup’s sker även via VPN till 3’e part för skydd ifrån administrativ personal.

- Belysningen i rummet tar ström ur valfri UPS.

- Friskluft Intag/Utlopp är avskärmade ifrån obehörig åtkomst (inhägnat område)

- All utrustning är monterad minst 30 cm up ifrån installationsgolvet.

- Alla kablar är monterade i monterings skenor på väggar och tak. Inga kablar ligger/hänger löst.

- Inga manualer (papper) finns tillgängliga i serverrummet

- Serverrummet är ej skyltat att det är ett sådant.

- Policys utformas för teknisk personal som ska ha tillgång till rummet så att de vet sina ansvarsområden.

- ”Recovery/Restore” instruktioner ska finnas i närheten av serverrummet. Detta ska dessutom övas 1 gång i kvartalet av ansvarig personal på laborationsutrustning.

- Utrustningen som används i serverrummet testas och utrustas med lämpligt filter för att reducera RÖS ytterligare.

- All utrustning ska inventeras med minst följande uppgifter Tillverkare, Typ av utrustning, Antal, eventuella Serienummer för att underlätta vid förlust av utrustning.

- All utrustning i serverrummet stöldskyddsmärks enligt praxis ifrån Svenska Stöldskydds Föreningen.

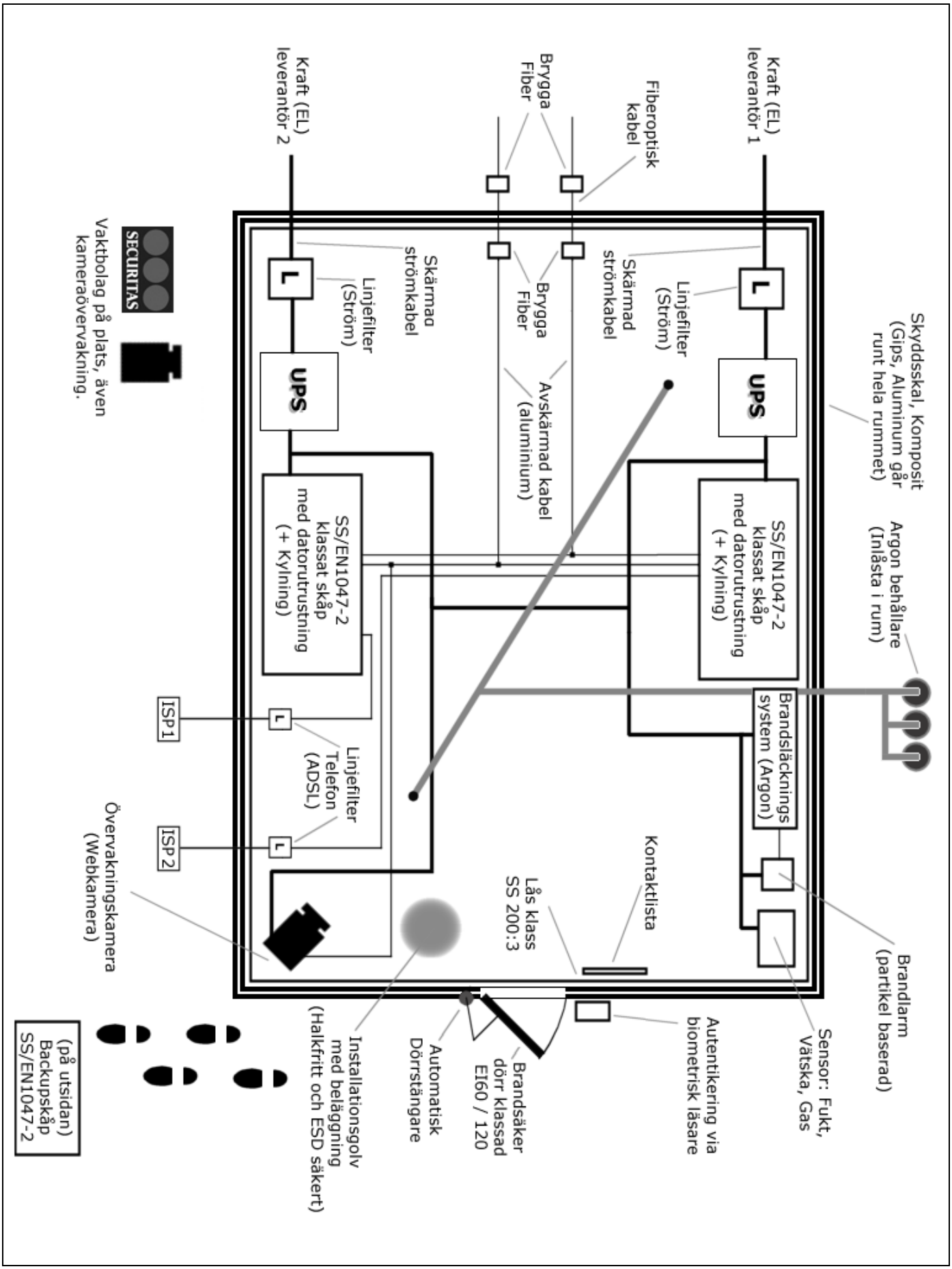
- Kritisk utrustning i serverrummet som kan bli föremål för angrepp ska plomberas så att intrång i hårdvaran lätt märks.

- Skyddsronder/Certifieringar ska utföras av säkerhetsansvarig regelbundet 1 gång per månad samt vid slumpartat tillfälle under samma månad.

- Alla besök In/Ut ur serverrummet ska loggas för spårbarhet av säkerhetsansvarige.

- Roller enligt Keyholder/Key shares defineras så att åtkomsten kan begränsas. Roller som t.ex hårdvara, larm kan defineras upp så att ingen enstaka individ kan få tillgång till allt. Huvudnycklar till allt ska inte existera, inte ens för den säkerhetsansvarige.

Appendix A: layout av serverrummet.



Appendix B: Om RÖS.

-"Vad är RÖS och varför ska jag bry mig"?

RÖS är signaler som röjer information igenom t.ex induktans, magnetism (t.ex crosstalk) eller elektronisk strålning. Detta gör informationsstöld väldigt lätt för en angripare - varför bryta sig in i ett system och riskera åka fast då denne kan stå 2 kilometer bort med en mottagare och titta på vad du gör på din datorskärm?

[**3**] beskriver källor som genererar RÖS som följande:

___

"a. (U) Functional Sources. - Functional sources are those designed for the specific purpose of generating electromagnetic energy. Examples are switching transistors, oscillators. signal generators, synchronizers, line drivers, and line relays.

b. (C) Incidental Sources (U). - Incidental sources are those which are not designed for the specific purpose of generating electromagnetic energy. Examples are electromechanical switches and brush-type motors. The sources of compromising emanations may include all electromechanical and electronic equipment and systems used to process national security information. In determining the extent of compromising emanations, and the necessary countermeasures to be applied, equipment must be considered individually and as components of a system. Any circuit processing national security information may be a source of compromising emanations, and installations using individually suppressed equipments and systems could be sources of compromising emanations unless proper installation and maintenance procedures are utilized.
...
When CE are radiated, they might leave the Controlled Space (CS) along signal, phone or powerlines, through conductive structures such as steel beams and water pipes, or as direct radiation from the source. The signals need not be of great magnitude to be compromising because receiving instruments with which they can be intercepted can make use of even a small amount of energy..."

___

Vad den ovanstående texten beskriver:

Elektroniska källor som är designade för ett specifikt ändamål som att generera elektromagnetisk (EM) energi. Exempel inom IT världen som genererar detta är transistorer (processorer), oscillatorer (klockningen). Incidenta källor är källor som inte var designade för att generera elektromagnetisk energi, t.ex elektromagnetiska switchar (reläer) och elektriska motorer (backuprobotar, hårddiskar).

Källorna för kompromitterande strålning (RÖS) kan inkludera all elektromekanisk och elektronisk utrustning som nyttjas i verksamheten, för att kunna bestämma spridningen av RÖS och dom nödvändiga motmedlen som ska sättas in, så måste varje komponent sättas granskas som både en enskild komponent och som en komponent av ett större system.

Vilken komponent som helst i systemet kan vara en källa för RÖS och tyngd läggs på proper installation, drift & underhållsrutiner. När RÖS uppstår så kan signalen lämna det säkrade området via signal (t.ex datornätverk), telenätet eller strömnätet, via elektriskt ledande strukturer som stålbalkar eller (metalliska) vattenledningar, signalerna behöver inte vara starka för att kunna plockas up av ett instrument på utsidan.

Kunskap vi får fram av den publikt tillgängliga dokumentationen som direkt går att applicera i designen av ett serverrum (SR):

- Själva väggarna i SR ska vara överlappande skivor med ett av följande (ström)ledande material *Stål*, *Koppar*, *Aluminium* [**2**]

- Utrustning som är designat för mer än ett ändamål (av olika signifikans för säkerheten) bör vara testad och certifierad av lämplig myndighet/organistion för att garantera skydd emot RÖS.

- Mobiltelefoner och annan privat kommunikationsutrustning måste störas ut så de ej går att bruka i SR.

- Om telefoni (Modem/ISDN/ADSL) måste finnas i SR, så ska dessa utrustas med signalfilter som skyddar emot RÖS, t.ex lågpass filter för rösttrafik på modem. (se: [**1**] Sektion **4.6.3.1**)

- All strömförsörjning ska utrustas med linjefilter innanför rummet, kablage som därefter leder utåt ur SR ska avskärmas så inte att dessa åter igen plockar upp RÖS.

- Ett UPS system eller ett linjefilter är i sig inte tillräckligt bra för att filtrera bort all genererad RÖS, utan specifika filter bör tillverkas och installeras på varje enhet som genererar RÖS.
  (se: [**1**] Sektion **4.7.2.1.**)

- All datortrafik in/ut ur serverrummet ska gå via fiber. En brygga nätverk-till-fiber ska finnas på insidan och en brygga för fiber-till-nätverk ska finnas på utsidan av serverrummet. Bryggorna får inte befinna sig på samma sida av väggen.

- Om ekonomin tillåter så ska fiberoptisk kabel användas i så stor utsträckning som det går. Även om större delen av nätverket i SR skulle byggas i fiber så ska trafiken fortfarande ha filtrerats innan det lämnar rummet, för även om Optisk kabel inte kan plocka upp RÖS så kan RÖS ha plockats upp av metallisk kabel *innan* den blev bryggad till fiber.

- Kablage ämnade för bruk inom SR får inte lämna SR under några som helst omständigheter.

- Trådlösa LAN (Wireless) får överhuvudtaget inte användas i nätverket.

- All elektronisk utrustning i SR måste jordas på ett korrekt sätt (separat avskärmad kabel till jord) så att inte felande utrustning blir en källa för RÖS. Kablage som ska användas ska vara avskärmade med aluminiumfolie. (Se: [**1**] sektion **4.4.1.**)

- Utformningen av serverrummet får ej underlätta att RÖS sprids via den närliggande fysiska strukturen i huset. Närliggande struktur av elektriskt/EM

ledande material (balkar osv) måste avskärmas så att RÖS inte transporteras vidare ifrån SR. (se [**3**], sektion **1-3.**)

- Leveranssystem med gas, t.ex brandsläckning och friskluft intag ska vara av icke elektriskt/EM ledande material så inte RÖS kan spridas via dessa. In/utloppet för dessa system ska vara på ett skyddat och övervakat område.

- Då RÖS även innefattar akustik så ska även väggarna i SR ska vara fullt ljudisolerade ifrån omvärlden. Detta kan reduceras med ett ljudabsorberande material i väggen.

- Fönster ska naturligtvis inte finnas i serverrummet.

Notera: Dessa punkter är baserade på källorna, sunt förnuft, kvalificerade gissningar och en stänk paranoia.

Källförteckning - RÖS:

[1**]** **"NSTISSAM TEMPEST/2-95 - RED/BLACK INSTALLATION GUIDANCE"**

(2005 Jan 19) http://cryptome.org/nsa-tempest.htm

[2**]** **"*Electronic Protection*"**

(2005 Jan 22) http://www.cs.nps.navy.mil/people/faculty/rowe/eprotect.htm

[3**]** **"*Nacsim 5000*"**

(2005 Jan 19) http://cryptome.org/nsa-tempest.htm

Appendix C: Det som testas (*) i EN1047

(*) Övriga krav som kan ställs på skåpen enligt standarden refereras till normen **SS/EN 1047-2** som är den aktuellaste versionen av normen.

Skåp certifierade enligt *EN 1047* har testats enligt följande: [**1**]

- **Värme**

  1 090°C värme tillförs från tre håll samtidigt. Temperaturen i skåpet får inte öka till mer än 55° C. Temperaturnivån då datamedia förstörs är cirka 60° C. Datorer i drift havererar vid cirka 70° C.

- **Vattenånga**

  Datamedia och datorer tål i kombination med värme inte mer än 85 % relativ luftfuktighet. I tegel och betong finns cirka 2% kristalliskt bundet vatten som vid brand frigörs och på grund av den höga temperaturen genast övergår till vattenånga under tryck.

- **Gaser**

  Absolut gastäthet. Korrosiva brand- och rökgaser är ett mycket allvarligt hot mot både datamedia och datorer. Detta ställer mycket höga krav på gastätheten.

- **Falltest**

  När skåpet upphettats tas det ut ur ugnen och släpps omedelbart ner från 9,15 meter på en bädd av grovt grus. Skåpet ställs sedan tillbaka i ugnen där det får stå i ytterligare 40 minuter varefter ugnen stängs av. Testet avbryts inte förrän temperaturen i skåpet är den samma som omgivningstemperaturen. Skåpet måste under hela detta förfarande bibehålla nämnda gränsvärden.

- **Magnetism**

  Universitetet i Köln har testat och godkänt VDMA 24991 / EN1047 som fullgott skydd mot magnetism.

- **Fysiskt våld och tillträde**

  Utöver VDMA 24991 / EN1047 har Lampertz-skåpen dessutom testats mot fysiskt våld och fysiskt tillträde. Universitetet i Aachen samt Tysklands officiella testcenter har tagit fram de testförfaranden som används.

[**1**] *CDAB* (2005 Jan 23)

http://www.cdab.se/fysisk/normer.htm