TEMPEST

in fysieke IT infrastructuur

White Paper

Juli, 2026

DOOR

André Hiddink

Product manager IT

Cybersecurity wordt tegenwoordig vooral gelinkt aan software, netwerken en encryptie, maar één risico krijgt daarbij nog te weinig aandacht: de onbedoelde elektromagnetische straling die moderne IT-systemen afgeven. TEMPEST richt zich precies op dit vraagstuk, het beheersen van deze compromitterende emissies, zodat gevoelige informatie niet via de fysieke omgeving kan worden afgevangen.

Door de opkomst van krachtige hardware, steeds toegankelijkere detectietechnologie en strengere wet- en regelgeving zoals NIS2 en de Cyber Resilience Act, staat fysieke informatiebeveiliging weer volop in de belangstelling.

Dit whitepaper belicht de onderliggende principes, de praktische uitdagingen en de ontwerpkeuzes van TEMPEST-infrastructuur, en laat zien waarom afscherming vandaag actueler is dan ooit.

FRIEDHELM LOH GROUP

RITTAL

Inhoudsopgave

1. Inleiding – De terugkeer van een onzichtbare dreiging

Cybersecurity wordt vaak geassocieerd met software, encryptie, identity management en netwerksegmentatie. Maar onder die digitale lagen schuilt een fysiek fenomeen dat al sinds het ontstaan van elektronica bestaat: elke schakeling straalt elektromagnetische energie uit. Die straling is zwak, maar niet willekeurig. Ze draagt patronen die direct samenhangen met de interne activiteit van het apparaat. Een processor die rekent, een scherm dat ververst, een netwerkkaart die pakketten verstuurt ze laten allemaal een elektromagnetische vingerafdruk achter.

In de meeste omgevingen is dat geen probleem. Maar in sectoren waar informatieverlies onacceptabel is, vormt die vingerafdruk een risico. Niet via een hack, niet via een kabeltap, maar simpelweg door te luisteren naar wat een apparaat uitstraalt. Dat is precies waar TEMPEST richt zich op het beheersen van compromitterende elektromagnetische emissies. Het betreft geen commerciële standaard, een door de NAVO ontwikkelde set van richtlijnen die primair bedoeld is voor gebruik binnen overheidscontexten, zoals defensie, politie, inlichtingendiensten en diplomatieke omgevingen.

Hoewel TEMPEST zijn oorsprong heeft in de Koude Oorlog, is de relevantie vandaag groter dan ooit. Moderne IT omgevingen zijn sneller, dichter en complexer geworden. Servers bevatten meer cores, schakelen op hogere frequenties en genereren sterkere elektromagnetische patronen. Datacenters worden compacter, edge locaties brengen kritieke workloads naar plekken waar fysieke controle minder vanzelfsprekend is, en de middelen om signalen op te vangen van draagbare ontvangers tot drones zijn toegankelijker geworden.

Tegelijkertijd dwingt wetgeving zoals NIS2 en de Cyber Resilience Act organisaties om risico's integraal te beoordelen. Niet alleen digitale risico's, maar ook fysieke risico's die kunnen leiden tot verlies van vertrouwelijkheid. Daarmee keert TEMPEST terug als een volwaardige pijler binnen moderne cybersecurity. Niet als een exotische techniek, maar als een noodzakelijke laag in een wereld waarin informatie overal aanwezig is en waarin de grens tussen fysiek en digitaal steeds verder vervaagt.

Door de beschikbaarheid van betaalbare software defined radio's en de toegenomen rekenkracht van standaard IT systemen is de drempel voor het detecteren en analyseren van elektromagnetische signalen aanzienlijk verlaagd. Waar dergelijke technieken historisch voorbehouden waren aan staten, zijn zij tegenwoordig toegankelijker geworden, wat het dreigingsbeeld verder vergroot.

2. De oorsprong van TEMPEST en de ontwikkeling van normering

Het inzicht dat elektronische apparatuur onbedoeld informatie kan prijsgeven via elektromagnetische straling ontstond in de vroege periode van de Koude Oorlog. Onderzoek liet zien dat de elektromagnetische emissies van elektronische systemen konden worden opgevangen en geanalyseerd, en dat deze emissies correlatie vertoonden met interne systeemactiviteit. Daarmee werd duidelijk dat informatie kon worden afgeleid zonder fysieke toegang tot apparatuur en zonder interactie met het systeem zelf.

Uit deze ontdekking ontstond TEMPEST als beveiligingsdiscipline. TEMPEST is geen formeel acroniem, maar een codenaam die wordt gebruikt om het geheel aan maatregelen, ontwerpprincipes en testmethoden te beschrijven dat gericht is op het beheersen van zogenoemde compromitterende emanaties. Het doel van TEMPEST is het voorkomen dat elektromagnetische emissies functioneren als een onbedoeld informatiekanaal naar onbevoegde partijen.

Binnen de NAVO is TEMPEST vastgelegd in de NATO TEMPEST Documentation Set, waarvan SDIP 27 (Suppressing Compromising Emanations – Installation and Equipment) de centrale richtlijn vormt. Deze norm beschrijft op hoofdlijnen:

- hoe elektromagnetische informatielekken moeten worden beperkt,
- welke eisen gelden voor apparatuur en installaties,
- hoe afscherming, filtering en bekabeling moeten worden toegepast,
- en hoe testen en certificering plaatsvinden.

De inhoud van SDIP 27 is deels geclassificeerd, omdat zij inzicht geeft in kwetsbaarheden en afluistermogelijkheden. De norm mag uitsluitend worden ingezien en toegepast door overheidsinstanties en door hen erkende test- en certificeringslaboratoria. TEMPEST is daarmee geen open industriestandaard, maar een door de staat gecontroleerde beveiligingsdiscipline.

2.1 Evolutie van SDIP 27

Gedurende lange tijd was SDIP 27/2 de geldende versie van de norm. Deze was afgestemd op een IT-omgeving met relatief lage schakelsnelheden, minder geïntegreerde hardware en een dreigingsmodel waarin afluisterapparatuur groot, kostbaar en statisch was. De nadruk lag sterk op het afschermen van individuele apparaten, vaak via aangepaste of speciaal ontwikkelde hardware. Met de opkomst van moderne IT-architecturen — gekenmerkt door hogere schakelsnelheden, compactere hardware en complexere integratie — voldeed deze benadering steeds minder. Tegelijkertijd werd afluistertechnologie kleiner, mobieler en eenvoudiger inzetbaar. Deze ontwikkelingen maakten een herziening van de norm noodzakelijk.

Dit resulteerde in SDIP 27/3, de huidige generatie van de richtlijn. SDIP 27/3 verlegt de nadruk van individuele apparatuur naar het installatie- en infrastructuurniveau, waarbij de fysieke omgeving wordt beschouwd als de primaire beveiligingsgrens.

De onderstaande tabel beschrijft de ontwikkeling van SDIP 27 primair vanuit het perspectief van infrastructuur gebaseerde TEMPEST-oplossingen, zoals afgeschermde racks en installaties. Afhankelijk van het beveiligingsniveau, de operationele context en nationale voorschriften kunnen onder SDIP 27/3 nog steeds specifieke TEMPEST-gecertificeerde apparaten, aanvullende afscherming van apparatuur of zelfs afgeschermde ruimtes (shielded rooms) vereist zijn. Als onderdeel van de totale beveiligingsarchitectuur.

Aspect	SDIP-27/2	SDIP-27/3
Technologische context	Lagere schakelsnelheden, eenvoudiger systemen	Hoge frequenties, sterk geïntegreerde hardware
Dreigingsmodel	Grote, statische ontvangers	Mobiele ontvangers, draagbare middelen, drones
Focus van afscherming	Individuele apparatuur	Installatie en infrastructuur
Hardwarebenadering	Focus op aangepaste hardware	Infrastructuur gebaseerde inzet van COTS hardware
Rol van infrastructuur	Ondersteunend	Primair beveiligingsniveau
Praktische impact	Complexe hardware certificering	Flexibele inzet van moderne IT omgevingen

Tabel 1 – Ontwikkeling van SDIP 27

2.2 Aanvullende toelichting op normatieve reikwijdte en technische implicaties

Hoewel SDIP 27/3 de nadruk verlegt van individuele apparatuur naar het installatie en infrastructuurniveau, blijft één uitgangspunt ongewijzigd: de norm is uitsluitend van toepassing op IT apparatuur en complete installaties. Een rack kan daarom formeel niet worden geclassificeerd als TEMPEST A, B of C. De TEMPEST classificatie wordt altijd toegekend aan de totale operationele configuratie, waarin apparatuur, bekabeling, filtering en fysieke infrastructuur gezamenlijk worden beoordeeld. Het rack vormt daarin een essentieel onderdeel van de afschermende grens, maar is geen zelfstandig TEMPEST object.

De ideale vorm van TEMPEST validatie is het testen van de volledige installatie in de daadwerkelijke gebruiksconfiguratie. In de praktijk is dit zelden haalbaar. Moderne IT omgevingen bestaan uit snel wisselende hardware, variabele configuraties en componenten met korte productcycli. Het is daardoor niet realistisch om elke mogelijke combinatie van apparatuur en infrastructuur afzonderlijk te certificeren. Dit is precies de reden waarom SDIP 27/3 de nadruk legt op infrastructuur als primair beveiligingsniveau: een stabiele, reproduceerbare fysieke grens die onafhankelijk is van de specifieke hardware die binnen die grens wordt geplaatst.

In dit kader is het belangrijk een veelvoorkomend misverstand te adresseren. TEMPEST risico's worden soms vergeleken met mobiele telefonie, maar dat is technisch onjuist. Een mobiele telefoon is een actieve zender die bewust radiosignalen uitstuurt met een gedefinieerde modulatie en bandbreedte. Servers en netwerkapparatuur doen dat niet. De elektromagnetische emissies van digitale systemen zijn onbedoelde bijproducten van kloksignalen, datalijnen en voedingen. Juist in die onbedoelde emissies kunnen patronen aanwezig zijn die correleren met interne datastromen. TEMPEST richt zich niet op radiocommunicatie, maar op het voorkomen dat dergelijke patronen

op afstand kunnen worden opgevangen en geïnterpreteerd. Dit onderscheid verklaart waarom afscherming op infrastructuurniveau noodzakelijk blijft, ook wanneer de gebruikte apparatuur zelf geen radiozender is.

Juridische disclaimer

Rittal levert geen TEMPEST geclassificeerde racks. Wij leveren infrastructuuroplossingen die het mogelijk maken een installatie te realiseren die op een gewenst TEMPEST niveau kan worden geconfigureerd en getest. De TEMPEST classificatie wordt uitsluitend toegekend aan de volledige installatie, conform de toepasselijke SDIP 27 richtlijnen.

2.3 Betekenis voor moderne IT omgevingen

De verschuiving die met SDIP 27/3 is ingezet, heeft belangrijke consequenties. In plaats van afscherming in de hardware zelf te realiseren, wordt de beveiliging geconcentreerd in de fysieke infrastructuur: racks, doorvoeren, voedingen en constructies. Hierdoor kan standaard commerciële IT hardware worden toegepast binnen een gecontroleerde TEMPEST omgeving, zonder ingrijpende aanpassingen aan de apparatuur en zonder verlies van vendorondersteuning.

Hiermee is TEMPEST geen historisch specialisme, maar een actuele beveiligingslaag die aansluit bij moderne IT architecturen en hedendaagse eisen aan informatiebeveiliging. Deze infrastructuurgerichte benadering vormt de basis voor de verdere hoofdstukken over EMC, elektromagnetische emissies en TEMPEST racks als gecontroleerde fysieke grens.

3. COTS, MOTS en NOTS: strategieën voor hardware in een TEMPEST omgeving

Voordat wordt ingegaan op de technische aspecten van TEMPEST en de manier waarop elektromagnetische emissies beheerst worden, is het belangrijk om eerst stil te staan bij de strategische keuzes rondom hardware en infrastructuur. De wijze waarop IT-systemen worden opgebouwd, bepaalt namelijk in grote mate waar en hoe afscherming gerealiseerd kan worden. Binnen TEMPEST-omgevingen zijn hierin drie benaderingen te onderscheiden: het gebruik van standaard commerciële hardware (COTS), aangepaste standaardhardware (MOTS) en volledig maatwerkoplossingen (NOTS). Deze keuzes verschillen fundamenteel in kosten, flexibiliteit en beheersing van elektromagnetische emissies, en vormen daarmee het uitgangspunt voor het verdere ontwerp van een veilige IT-infrastructuur.

De drie categorieën kunnen als volgt worden samengevat:

Type	Beschrijving	Kosten	Flexibiliteit
COTS	Standaard commerciële hardware, geen aanpassingen	Laag	Hoog
MOTS	Aangepaste standaardhardware met extra shielding	Middel	Laag
NOTS	Volledig maatwerk, speciaal ontwikkeld	Zeer hoog	Zeer laag

Tabel 2

COTS hardware vereist geen enkele fysieke aanpassing. Er worden geen behuizingen aangepast, geen extra filters geplaatst en geen voedingen vervangen. De apparatuur blijft volledig ondersteund door de leverancier, inclusief garantie en firmware updates. De afscherming wordt volledig verzorgd door het TEMPEST rack, waardoor hardware refreshes eenvoudig blijven en geen nieuwe certificering nodig is. MOTS hardware vraagt om gedeeltelijke aanpassingen, zoals extra metalen shielding, aangepaste kabeldoorvoeren

of filters op I/O poorten. Dit leidt tot hogere kosten, verlies van garantie en een afhankelijkheid van maatwerk bij elke hardware update. NOTS hardware gaat nog verder: volledig custom PCB design, speciale behuizingen en maatwerkvoedingen. Dit is extreem kostbaar, heeft lange doorlooptijden en wordt alleen toegepast in zeer specifieke militaire scenario's.

De voordelen van COTS worden daardoor snel duidelijk:

- Hardware innovatie gaat te snel voor MOTS en NOTS om bij te houden.
- Support, garantie en firmware updates blijven behouden.
- Kosten blijven laag, zowel in aanschaf als in lifecycle.
- COTS sluit aan op moderne IT architecturen zoals virtualisatie, cloud en GPU acceleratie.
- COTS voldoet aan NIS2 en CRA eisen zonder aanvullende hardware aanpassingen.
- Hardware kan vrij worden vervangen zonder nieuwe TEMPEST certificering.

TEMPEST racks spelen hierin een cruciale rol. Ze maken het mogelijk om standaard hardware veilig te gebruiken door de afscherming te verplaatsen van de hardware naar de infrastructuur. Door waveguides, gaskets en powerfilters worden alle mogelijke lekpaden gecontroleerd, terwijl de thermische prestaties behouden blijven ondanks lagere perforatie. Het rack wordt daarmee de fysieke beveiligingslaag, terwijl de hardware standaard, flexibel en toekomstbestendig blijft.

De essentie is dat COTS in combinatie met TEMPEST racks de enige strategie is die betaalbaarheid, flexibiliteit en veiligheid combineert. Het maakt TEMPEST toepasbaar in moderne IT omgevingen zonder de beperkingen van maatwerkhardware, en vormt daarmee de logische keuze voor vrijwel alle hedendaagse organisaties. Deze aanpak vormt de basis voor de verdere technische uitwerking. In het volgende hoofdstuk wordt toegelicht waarom traditionele EMC-benaderingen hiervoor onvoldoende zijn.

4. Waarom EMC niet genoeg is

Om deze infrastructuurgerichte benadering te begrijpen, is het eerst nodig om het verschil tussen EMC en TEMPEST nader te bekijken. Toen elektronische apparatuur in de jaren zestig en zeventig breder werd ingezet, ontstond de behoefte om te voorkomen dat apparaten elkaar zouden storen. Dat leidde tot het vakgebied EMC: elektromagnetische compatibiliteit. EMC richt zich op het beperken van ongewenste emissies zodat apparatuur betrouwbaar blijft functioneren, en op het beschermen van apparatuur tegen externe storingsbronnen. Het doel is stabiliteit en voorspelbaarheid van elektronische systemen in een gedeelde omgeving.

Waar elektromagnetische interferentie (EMI) zich richt op het beperken van storing tussen systemen, richt TEMPEST zich expliciet op de mogelijkheid dat deze emissies informatie bevatten. Het gaat niet om de aanwezigheid van een signaal, maar om de betekenis die daaruit kan worden afgeleid.
Op het eerste gezicht lijkt EMC sterk op TEMPEST. Beide disciplines gebruiken metalen behuizingen, geleidende pakkingen, filters, afgeschermde kabels en gecontroleerde doorvoeren. Maar de overeenkomst is slechts oppervlakkig.
De onderliggende doelstellingen verschillen fundamenteel, en precies daar ontstaat het misverstand dat in veel organisaties nog steeds leeft: dat EMC gecertificeerde apparatuur automatisch veilig zou zijn tegen afluisteren. Dat is niet zo.

EMC kijkt naar de hoeveelheid ruis die een apparaat produceert. Zolang de totale emissie onder een bepaalde drempel blijft, wordt het apparaat als 'compatibel' beschouwd. Het gaat om het voorkomen van storing, niet om het beschermen van informatie. Een EMC test beoordeelt of een apparaat geen hinder veroorzaakt voor andere apparatuur en of het zelf voldoende robuust is tegen externe invloeden. De inhoud van de emissie de informatie die erin verborgen kan zitten speelt geen enkele rol.

TEMPEST kijkt juist naar die inhoud. Waar EMC ruis als een ongewenst bijproduct ziet, beschouwt TEMPEST ruis als een potentieel kanaal waarlangs informatie kan ontsnappen. Een signaal dat voor EMC irrelevant is omdat het te zwak is om storing te veroorzaken, kan voor een aanvaller waardevol zijn als het correleert met interne activiteit. Een processor die schakelt, een cryptografische module die sleutels verwerkt, een netwerkinterface die pakketten verstuurt al deze activiteiten laten patronen achter in het elektromagnetische spectrum.

Daarom is EMC geen bescherming tegen afluisteren en is TEMPEST een noodzakelijke aanvullende laag.

5. Hoe digitale activiteit verandert in elektromagnetische informatie

Om te begrijpen waarom TEMPEST vandaag nog steeds relevant is, moet je terug naar de basis van digitale elektronica. Elke digitale schakeling of het nu een processor, geheugenmodule, netwerkinterface of grafische kaart is werkt door elektrische signalen te laten wisselen tussen twee toestanden. Die wisselingen zijn niet alleen elektrische gebeurtenissen binnen een chip; ze veroorzaken ook kleine elektromagnetische verstoringen in de omgeving.

Wanneer een transistor schakelt, verandert de stroom door een geleider abrupt. Die verandering creëert een elektromagnetisch veld dat zich als een golf door de ruimte kan verspreiden. Hoe sneller de schakeling, hoe hoger de frequentie van die golf. Moderne processoren schakelen miljarden keren per seconde. Dat betekent dat ze een complex patroon van elektromagnetische emissies genereren dat direct samenhangt met wat ze op dat moment doen.

Die emissies zijn zwak, maar niet willekeurig. Ze vormen een soort elektromagnetische vingerafdruk van de interne activiteit. Een cryptografische module die sleutels verwerkt, een server die een databasequery uitvoert, een netwerkkaart die pakketten verstuurt al deze activiteiten laten herkenbare patronen achter in het elektromagnetische spectrum.

Daarom is TEMPEST geen historisch overblijfsel, maar een discipline die juist in moderne IT omgevingen aan belang wint.

TEMPEST kan worden beschouwd als een vorm van side channel analyse, waarbij niet het systeem zelf wordt aangevallen, maar informatie wordt afgeleid uit fysieke bijwerkingen van elektronische processen. Deze benadering maakt gebruik van signalen die niet bedoeld zijn voor communicatie, maar die wel correleren met interne activiteit.

De relatie tussen elektromagnetische emissies en informatie is al decennia bekend. Klassieke demonstraties tonen aan dat beeldscherminformatie op afstand kan worden gereconstrueerd uit elektromagnetische straling, een fenomeen dat bekendstaat als Van Eck phreaking. Ook moderne digitale interfaces blijven hierbij relevante emissiebronnen.

6. Perforatie: het spanningsveld tussen thermiek en afscherming

Perforatie vormt een van de meest kritische ontwerpkeuzes binnen TEMPEST infrastructuur. In conventionele datacenters zijn sterk geperforeerde deuren en panelen gebruikelijk, vaak met een open oppervlak van 70 tot 85 procent. Deze hoge perforatiegraad faciliteert luchtstroming en vereenvoudigt thermisch ontwerp, maar staat haaks op effectieve elektromagnetische afscherming.

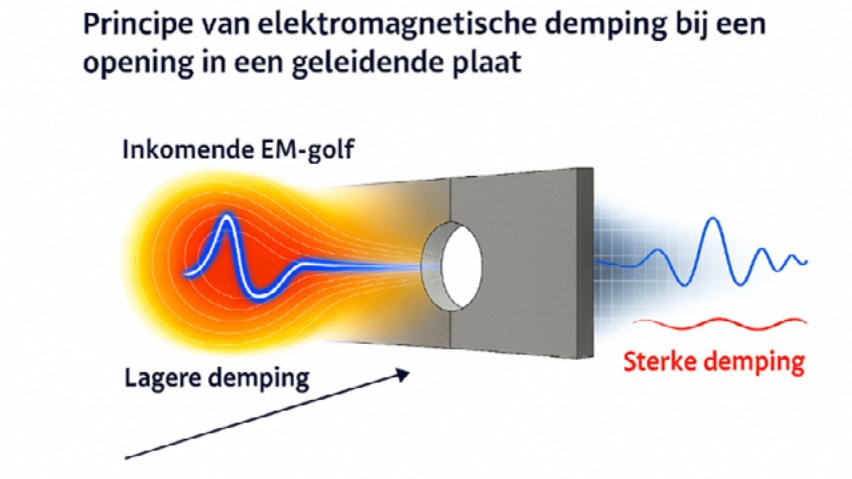
Vanuit TEMPEST perspectief vormt elke opening in een geleidende barrière een potentieel lekpad. Dit geldt niet alleen voor grote openingen, maar ook voor relatief kleine perforaties, zeker wanneer de betrokken elektromagnetische emissies zich in het hoogfrequente domein bevinden. Moderne IT apparatuur genereert emissies over een breed frequentiespectrum, waarbij juist de hoge frequenties bepalend zijn voor het risico op compromitterende emanaties.

6.1 Elektromagnetische interactie met een perforatie

Het effect van perforatie kan het best worden begrepen door te kijken naar de interactie tussen een elektromagnetisch veld en een enkele opening in een geleidende plaat. Daarbij is het cruciaal om te benadrukken dat elektromagnetische demping niet pas in de opening zelf ontstaat, maar reeds optreedt wanneer het veld het metalen oppervlak nadert.
Zodra een elektromagnetisch veld een geleidende plaat benadert:

- worden veldlijnen herverdeeld en weggedrukt,
- ontstaan oppervlaktestromen die een tegenveld opwekken,
- en wordt een aanzienlijk deel van de energie gereflecteerd.

Het gat in de plaat fungeert in dit proces niet als actieve demper, maar als koppelpunt. Slechts een sterk verzwakte veldcomponent kan door de opening koppelen. Deze koppeling verloopt via het waveguide below cutoff principe: de opening gedraagt zich als een korte golfgeleider waarvan de afmetingen kleiner zijn dan de relevante golflengtes, waardoor geen voortplantende golf kan ontstaan en het veld in de opening exponentieel afneemt.



Afbeelding 1 – Elektromagnetische interactie met een enkel perforatiegat

Principeweergave van elektromagnetische demping bij een opening in een geleidende plaat. Het elektromagnetische veld wordt reeds bij nadering van het metaal verzwakt door reflectie en veldannulatie. Slechts een sterk gedempte component koppelt door de opening, waarna aan de achterzijde een zwak restveld overblijft.

6.2 Gatdiameter en effectieve demping

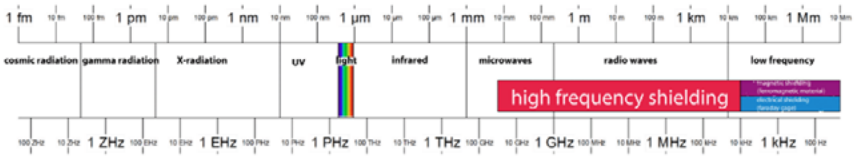
De mate van koppeling door een opening wordt in belangrijke mate bepaald door de gatdiameter. Perforaties met een diameter van bijvoorbeeld circa 3 mm zijn effectief omdat hun afmetingen aanzienlijk kleiner zijn dan de golflengte van de hoogfrequente emissies die moderne IT systemen produceren.
Hierdoor ligt de afsnijfrequentie van de opening ver boven het relevante emissiespectrum.
Concreet betekent dit:

- geen voortplantende elektromagnetische modus in het gat,
- een snel uitdovend (evanescent) veld in de opening,
- en een sterke verzwakking van het veld aan de achterzijde.

Door veel van dergelijke kleine perforaties toe te passen, ontstaat een constructie die thermisch functioneel blijft, maar elektromagnetisch gezien robuust afschermt. De demping wordt niet bereikt door één dominante opening, maar door het gemiddelde effect van vele zeer zwakke koppelingen.

6.3 Frequentiedomein en beperkingen van civiele normen

Om te begrijpen waarom perforatie ontwerp zo bepalend is, moet het worden geplaatst in het context van het elektromagnetisch spectrum. Civiele normen zoals EN 50147 1 bestrijken slechts een deel van dit spectrum en zijn primair ontwikkeld voor gecontroleerde meetomgevingen, zoals anechoïsche kamers in testlaboratoria.



Afbeelding 2 – Elektromagnetisch spectrum en civiele normen

Deze norm:

- beschrijft meetprocedures, geen afdwingbare grenswaarden voor operationele omgevingen,
- gaat uit van nagenoeg gesloten constructies,
- en houdt geen rekening met de vele functionele openingen die kenmerkend zijn voor datacenters, zoals ventilatie, voeding, datakabels en koeling.

Zoals in afbeelding 2 zichtbaar is, vallen de emissies van moderne IT apparatuur voornamelijk in het hoogfrequente bereik (MHz–GHz en hoger). In dit domein worden golflengtes kort en wordt het fysieke ontwerp van platen, perforaties en doorvoeren bepalend voor de afscherming. Algemene EMC normen zijn hiervoor onvoldoende richtinggevend.

6.4 Ontwerpimplicaties voor TEMPEST racks

De combinatie van hoge frequenties en korte golflengtes verklaart waarom TEMPEST racks bewust een beperkte perforatiegraad hanteren, doorgaans in de orde van 30–35 procent. Dit percentage is geen arbitraire norm, maar het resultaat van een afweging tussen:

- voldoende thermische capaciteit voor moderne IT apparatuur,
- en effectieve elektromagnetische demping over het relevante frequentiespectrum.

Koeling in een TEMPEST omgeving kan daarom niet worden gerealiseerd door simpelweg meer open oppervlak, maar vereist gecontroleerde luchtpaden, doordachte perforatie geometrie en een integraal ontwerp van rack en ruimte. Perforatie is daarmee geen detail, maar een structureel bepalende factor in de effectiviteit van TEMPEST infrastructuur. Zij verbindt thermiek, elektromagnetica en beveiliging tot één ontwerpvraagstuk en onderstreept waarom afscherming binnen SDIP 27/3 primair op infrastructuurniveau wordt gerealiseerd.

7. Koeling in TEMPEST infrastructuur

Moderne IT systemen worden gekenmerkt door een steeds hogere vermogensdichtheid. Processoren, geheugenmodules en accelerators produceren aanzienlijk meer warmte dan eerdere generaties hardware, terwijl racks compacter en dichter worden opgebouwd. In een standaard datacenter wordt deze warmte afgevoerd via open luchtstromen, sterk geperforeerde panelen en actieve ventilatie. In een TEMPEST omgeving is deze aanpak niet zonder meer toepasbaar.

Vanuit elektromagnetisch perspectief is een volledig gesloten, massieve kast ideaal. Een dergelijke constructie minimaliseert emissies en vereenvoudigt afscherming. Thermisch is een gesloten kast echter onhoudbaar. Zonder actieve warmteafvoer loopt de interne temperatuur snel op tot niveaus die de betrouwbaarheid, prestaties en levensduur van de apparatuur negatief beïnvloeden. Koeling is daarmee geen optionele voorziening, maar een ontwerpdwang binnen elke TEMPEST infrastructuur.

7.1 Het spanningsveld tussen koeling en afscherming

Elke vorm van koeling introduceert, direct of indirect, fysieke openingen. Luchtinlaten, uitlaten, ventilatoren of warmtewisselaars brengen noodzakelijke doorgangen met zich mee. Vanuit TEMPEST perspectief vormen deze doorgangen potentiële elektromagnetische lekpaden. Het spanningsveld tussen thermiek en afscherming is daarmee een centraal ontwerpvraagstuk.

De uitdaging is niet het volledig vermijden van openingen, maar het beheersen en controleren ervan. Koeling moet mechanisch mogelijk zijn, terwijl elektromagnetische emissies binnen de beveiligde zone blijven. Dit vereist een integraal ontwerp waarin thermische maatregelen vanaf het begin TEMPEST bewust worden meegenomen.

Dit betekent dat thermische optimalisatie zonder elektromagnetische afweging direct kan leiden tot nieuwe lekpaden.

7.2 Overzicht van koelconcepten binnen TEMPEST racks

Binnen TEMPEST omgevingen worden verschillende koelstrategieën toegepast. Deze strategieën verschillen in thermische capaciteit, complexiteit en impact op de afscherming, maar hebben gemeen dat zij expliciet zijn ontworpen om elektromagnetische lekpaden te beheersen.

Koeling via perforatie
Perforaties in deuren en panelen maken luchtstroming mogelijk en ondersteunen passieve of geforceerde luchtkoeling. Zoals beschreven in hoofdstuk 5 is de geometrie van deze perforaties bepalend voor hun elektromagnetische gedrag. Correct ontworpen perforaties dragen bij aan warmteafvoer, terwijl zij elektromagnetisch functioneren als sterk gedempte openingen.

Actieve ventilatie met ventilatoren
Ventilatoren verhogen de luchtverplaatsing binnen het rack en maken hogere warmtelasten mogelijk. In TEMPEST racks worden ventilatoren toegepast als onderdeel van een gecontroleerde constructie, bijvoorbeeld in combinatie met dieptewerking, geleidende structuren of afgeschermde behuizingen. De ventilator zelf is daarmee geen vrij “open gat”, maar een geïntegreerd onderdeel van het afschermconcept.

EMC en TEMPEST geschikte ventilatiemodules
Speciaal ontworpen ventilatiemodules combineren luchtverplaatsing met elektromagnetische demping. Deze oplossingen vormen een brug tussen thermische efficiëntie en afscherming, en worden toegepast waar hogere luchthoeveelheden nodig zijn zonder de afscherming te verzwakken.

Vloeistofgekoelde oplossingen (LCU / CW)
Liquid Cooling Units (LCU) en koelwater gebaseerde oplossingen voeren warmte af zonder grote luchtvolumes door het rack te verplaatsen. Hierdoor neemt de afhankelijkheid van perforatie en ventilatie af. Deze benadering verschuift het ontwerpvraagstuk naar leidingen, koppelingen en warmtewisselaars, die op hun beurt TEMPEST bewust moeten worden uitgevoerd.

In de praktijk worden deze koelconcepten vaak gecombineerd. Afhankelijk van rackopbouw, warmtelast en infrastructuur kan, afhankelijk van configuratie en randvoorwaarden, koelcapaciteit tot circa 8 kW per rack worden gerealiseerd, mits thermisch en elektromagnetisch ontwerp integraal worden benaderd.

7.3 Koeling als randvoorwaarde voor TEMPEST ontwerp

Koeling kan binnen TEMPEST infrastructuur niet als een losstaand probleem worden beschouwd. Iedere thermische maatregel heeft directe gevolgen voor elektromagnetische afscherming, en omgekeerd. Succesvolle TEMPEST implementaties erkennen koeling als een primaire ontwerpparameter en integreren thermiek, perforatie, ventilatie en afscherming tot één samenhangend systeem.

Dit onderstreept dat TEMPEST geen “nee tegen koeling” betekent, maar “ja tegen koeling, mits gecontroleerd”. Alleen door deze integrale benadering is het mogelijk om moderne, hoog vermogen IT omgevingen te combineren met effectieve bescherming tegen compromitterende elektromagnetische emanaties.

8. Waveguides, afgeschermde interfaces, gaskets en powerfilters: de stille bewakers van afscherming

In de voorgaande hoofdstukken is uiteengezet waarom openingen in een TEMPEST rack onvermijdelijk zijn en hoe elektromagnetische demping fysisch tot stand komt. Koeling, bekabeling en voeding vereisen mechanische doorgangen, maar deze mogen nooit ongecontroleerd functioneren. Binnen een TEMPEST omgeving ligt de uitdaging dan ook niet in het vermijden van openingen, maar in het zodanig uitvoeren van deze openingen dat zij elektromagnetisch geen lekpad vormen.

Een TEMPEST rack lijkt op het eerste gezicht op een reguliere serverkast, maar bij nadere beschouwing blijkt het een zorgvuldig geconstrueerd systeem waarin elke doorgang expliciet onderdeel is van het afschermconcept. Niet massieve panelen alleen bepalen de effectiviteit van de afscherming, maar juist de manier waarop noodzakelijke functies worden toegelaten. Waveguides, gaskets en powerfilters vormen hierin de sleutelcomponenten en fungeren als de stille bewakers van de afscherming.

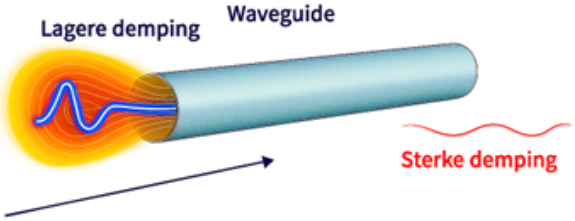
8.1 Waveguides en het orgelpijp principe

Waveguides worden toegepast om fysieke doorgangen mogelijk te maken zonder elektromagnetische doorlating. Het betreft lange, smalle metalen buizen die lucht of glasvezel mechanisch laten passeren, terwijl elektromagnetische straling onder de afsnijfrequentie geen voortplantende modus kan vormen. Dit gedrag staat bekend als het waveguide below cutoff principe en wordt in de praktijk vaak aangeduid als het orgelpijp principe.

Hoewel elektromagnetische energie bij de ingang aan de buis kan koppelen, verhindert de geometrie van de waveguide dat het veld zich door de buis kan voortplanten. In plaats daarvan neemt de veldsterkte in de lengterichting exponentieel af. De mate van demping wordt bepaald door de verhouding tussen lengte en diameter: hoe langer de buis en hoe kleiner de diameter, hoe groter de demping. Hierdoor kan een noodzakelijke mechanische doorgang worden gerealiseerd zonder dat deze fungeert als een effectief elektromagnetisch transmissiepad.

Waveguides worden in TEMPEST racks specifiek toegepast voor de invoer van glasvezel. De glasvezel is niet geleidend en transporteert geen elektromagnetische energie. De elektromagnetische beheersing ligt daarom volledig in de geometrie van de waveguide, die voorkomt dat de opening als lekpad fungeert.

Essentieel is dat verschillende typen verbindingen verschillende risico's introduceren en daarom niet met één uniforme maatregel kunnen worden beheerst. Elke doorgang vereist een specifiek afgestemde oplossing.



Afbeelding 3 – Waveguide ("orgelpijp") en lengte/diameter effect

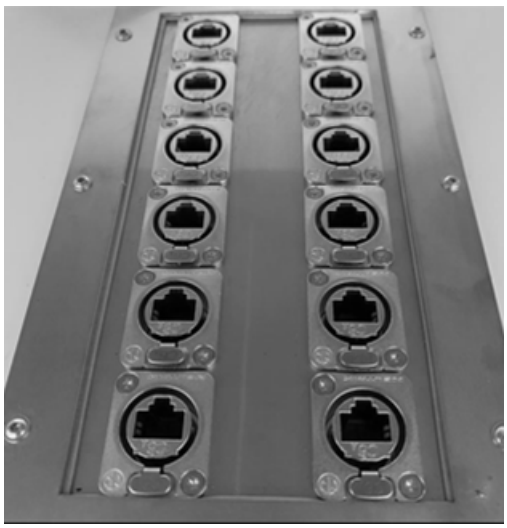
Een lange, smalle buis functioneert als waveguide onder afsnijfrequentie. Door de verhouding tussen lengte en diameter kan geen voortplantende elektromagnetische modus ontstaan en neemt het veld in de lengterichting exponentieel af.

8.2 Gecontroleerde koperinvoer via adapterplaten

Naast glasvezelverbindingen worden in IT omgevingen ook koperen verbindingen toegepast, bijvoorbeeld voor ethernet (RJ45). Vanuit TEMPEST perspectief vormt koper een fundamenteel ander risico dan glasvezel. Koperen kabels zijn elektrisch geleidend en kunnen zelf elektromagnetische energie koppelen en transporteren. Hierdoor is geometrische demping, zoals toegepast bij waveguides, voor koper niet voldoende.

Bij koperen verbindingen moet het risico worden beheerst op interface niveau. Dit wordt gerealiseerd door gebruik te maken van afgeschermde adapterplaten, waarin elke RJ45 poort afzonderlijk mechanisch en elektrisch is geïntegreerd in een metalen constructie. De adapterplaat maakt volledig elektrisch contact met de rackbehuizing en zorgt ervoor dat de afscherming van de kabel naadloos overgaat in de afscherming van het rack.

Door deze opzet wordt voorkomen dat koperen dataverbindingen functioneren als antenne of elektromagnetisch lekpad. De datafunctie blijft behouden, terwijl de fysieke scheiding tussen het interne, gecontroleerde domein en de externe omgeving expliciet wordt afgedwongen. De scheiding tussen glasvezel en koperinvoer is daarmee een bewuste en noodzakelijke ontwerpkeuze binnen TEMPEST infrastructuur.



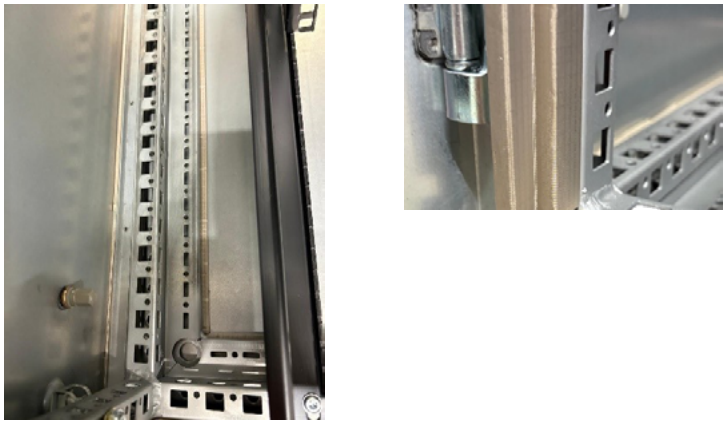
Afbeelding 4 – Afgeschermde RJ45 adapterplaat voor koperen dataverbindingen

Metalen adapterplaat met afzonderlijk afgeschermde RJ45 interfaces.
De elektrische continuïteit tussen connector, kabelafscherming en rackbehuizing voorkomt dat koperen netwerkverbindingen functioneren als elektromagnetische lekpaden, terwijl functionele datacommunicatie behouden blijft.

8.3 Gaskets en elektrische continuïteit

Naast doorvoeren vormen naden en bewegende delen intrinsiek zwakke punten in iedere afschermconstructie. Overgangen tussen panelen en deuren moeten mechanisch kunnen functioneren, maar mogen elektromagnetisch geen onderbreking veroorzaken. Geleidende gaskets vervullen hierin een cruciale rol.

Gaskets zorgen voor elektrisch continu contact tussen aangrenzende metalen delen, ook bij trillingen, thermische uitzetting en herhaald openen en sluiten. Zonder deze geleidende afdichting zouden zelfs zeer smalle spleten kunnen functioneren als elektromagnetische lekpaden, met een disproportionele impact op de totale afscherming. Binnen een TEMPEST rack zijn gaskets daarom geen afwerkingsdetail, maar een essentieel onderdeel van het beveiligingsconcept.



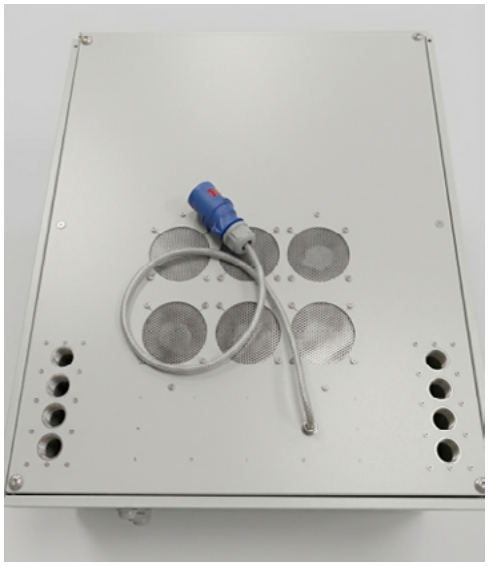
Afbeelding 5 – Afscherming met gaskets

Geleidende gasket toegepast tussen bewegende delen van een TEMPEST rack. De gasket waarborgt elektrische continuïteit tussen panelen en deuren en voorkomt dat naden functioneren als elektromagnetische lekpaden.

8.4 Powerfilters en voedingsinvoer

Ook de voedingslijn vormt een potentieel pad voor elektromagnetische lekkage. Zonder aanvullende maatregelen kan hoogfrequente elektromagnetische energie via de netaansluiting het rack verlaten. Powerfilters voorkomen dit door hoogfrequente componenten te blokkeren, terwijl de gewenste laagfrequente voedingsenergie (50 of 60 Hz) wordt doorgelaten.

Door powerfilters als integraal onderdeel van het rack uit te voeren, wordt de voedingsinvoer opgenomen in het totale afschermconcept. Net als bij waveguides en gaskets is de powerfilter geen losstaand element, maar onderdeel van een samenhangend systeem waarin alle doorgangen gecontroleerd zijn uitgevoerd.



Afbeelding 6 – Powerfilter en ventilatie

Gecombineerde toepassing van powerfiltering en gecontroleerde ventilatie. Het powerfilter laat uitsluitend laagfrequente voedingsenergie toe en blokkeert hoogfrequente componenten. Ventilatie wordt gerealiseerd zonder directe elektromagnetische doorbraak.

Samen zorgen waveguides, gaskets en powerfilters ervoor dat een TEMPEST rack functioneel kan blijven zonder concessies te doen aan de afscherming. Zij maken het mogelijk om lucht, kabels en energie toe te laten, terwijl compromitterende elektromagnetische emanaties binnen de gecontroleerde omgeving worden gehouden.

9. Het TEMPEST rack als gecontroleerde fysieke grens

Binnen een TEMPEST omgeving vervult het rack een fundamenteel andere rol dan in een traditioneel datacenter. Waar een standaard serverrack primair is ontworpen voor mechanische ondersteuning en luchtgeleiding, fungeert een TEMPEST rack als actieve beveiligingsgrens. Het rack vormt de fysieke scheiding tussen een gecontroleerde omgeving waarin gevoelige digitale verwerking plaatsvindt en een omgeving die als potentieel ongecontroleerd moet worden beschouwd.

Deze grenswerking is noodzakelijk omdat moderne IT apparatuur onvermijdelijk elektromagnetische emissies genereert. Processoren, geheugen, netwerkinterfaces en voedingscircuits schakelen op hoge snelheden en produceren elektromagnetische velden die zich niet beperken tot de interne elektronica. Zonder expliciete afscherming zouden deze emissies buiten het rack detecteerbaar blijven en kunnen fungeren als onbedoeld informatiekanaal.

Het TEMPEST rack is daarom ontworpen als een integraal afschermsysteem, niet als een verzameling losse onderdelen. De mate waarin emissies worden onderdrukt, wordt uitgedrukt in shielding effectiveness, doorgaans gemeten in decibel (dB). Deze demping is nooit het resultaat van één enkel paneel of component, maar van het samenspel tussen alle constructieve elementen van het rack.

Daarbij zijn met name van belang:

- de elektrische continuïteit van metalen panelen;
- het afdichten van naden en deuren;
- de gecontroleerde uitvoering van kabel- en luchtdoorvoeren;
- en filtering van voedings- en signaalpaden.

Zodra één van deze elementen tekortschiet, ontstaat een lekpad dat de effectiviteit van de totale afscherming ondermijnt. In die zin is een TEMPEST rack slechts zo sterk als zijn zwakste overgang.

Deze infrastructuurgerichte benadering sluit aan op SDIP 27/3, waarin de focus is verschoven van het aanpassen van individuele apparaten naar het beveiligen van de fysieke omgeving als geheel. Hierdoor wordt het mogelijk om standaard commerciële IT hardware (COTS) veilig toe te passen binnen een gecontroleerde TEMPEST infrastructuur. Het rack wordt daarmee het primaire beveiligingsobject, terwijl de hardware flexibel en toekomstbestendig blijft.

De effectiviteit van deze grens wordt bepaald door de correcte uitvoering van alle doorgangen, zoals beschreven in het voorgaande hoofdstuk.

10. Waar TEMPEST wordt ingezet

TEMPEST wordt toegepast in omgevingen waar het verlies van vertrouwelijke informatie onacceptabel is, ongeacht of dat verlies ontstaat door digitale aanvallen of door het onderscheppen van elektromagnetische emanaties. Hoewel de techniek zijn oorsprong heeft in militaire en inlichtingenoperaties, is het toepassingsgebied de afgelopen jaren verbreed door strengere wetgeving, hogere dreigingsniveaus en de toenemende waarde van digitale informatie. TEMPEST is daarmee niet langer een niche discipline, maar een strategische beveiligingslaag voor organisaties die afhankelijk zijn van de integriteit en vertrouwelijkheid van hun IT infrastructuur.

Traditioneel wordt TEMPEST ingezet bij defensie, inlichtingendiensten en diplomatieke posten, waar het onderscheppen van informatie directe gevolgen kan hebben voor nationale veiligheid. In deze omgevingen worden TEMPEST racks gebruikt om commandosystemen, cryptografische apparatuur, communicatieplatformen en analyseomgevingen af te schermen. Ook politie en veiligheidsdiensten passen TEMPEST toe, bijvoorbeeld in forensische labs, interceptiekamers en operationele commandoruimtes waar gevoelige data wordt verwerkt.

Daarnaast groeit de toepassing in civiele sectoren. Kritieke infrastructuur zoals energie, water, telecom en luchtvaart verwerkt steeds meer digitale informatie die, wanneer onderschept, kan worden misbruikt voor sabotage of spionage. Ook strategische R&D omgevingen, zoals high tech bedrijven, chipfabrikanten en onderzoeksinstituten, gebruiken TEMPEST racks om intellectueel eigendom te beschermen tegen industriële spionage. In deze sectoren is het risico niet alleen nationaal, maar ook economisch: het uitlekken van ontwerpdata, algoritmes of prototypes kan directe impact hebben op concurrentiepositie en innovatiekracht.

In de praktijk is de toepassing van TEMPEST binnen niet-overheidsorganisaties echter veelal gekoppeld aan een formele overheids- of defensiebehoefte. Organisaties uit de industrie, onderzoeksinstellingen en commerciële contractanten kunnen in aanraking komen met TEMPEST-eisen wanneer zij

werkzaamheden uitvoeren in het kader van nationale veiligheidsbelangen of defensieprogramma's. In dergelijke situaties vloeit de noodzaak voor TEMPEST doorgaans voort uit contractuele beveiligingseisen, accreditaties of formele ondersteuning door een bevoegde overheids- of militaire instantie. Een onderneming die bijvoorbeeld deelneemt aan een programma zoals de F-35 kan een gerechtvaardigde operationele reden hebben om TEMPEST-maatregelen toe te passen, maar deze noodzaak vloeit in de regel voort uit de beveiligingseisen van de opdrachtgever, de operationele context en de van toepassing zijnde accreditatie-eisen.

De reden dat TEMPEST racks hier zo goed passen, is dat ze een gecontroleerde fysieke grens creëren zonder dat de IT omgeving hoeft te worden aangepast. Organisaties kunnen blijven werken met standaard COTS hardware, moderne datacenterarchitecturen en snelle hardware refreshes, terwijl de fysieke laag wordt beschermd tegen ongewenste emanaties. Dit maakt TEMPEST toepasbaar in omgevingen waar flexibiliteit, schaalbaarheid en lifecycle beheer essentieel zijn. Het rack wordt daarmee een strategisch instrument: een manier om gevoelige informatie te beschermen zonder de operationele IT omgeving te verstoren.

Door de combinatie van strengere wetgeving, toenemende dreigingen en de groeiende waarde van digitale informatie wordt TEMPEST steeds vaker gezien als een noodzakelijke laag binnen een bredere beveiligingsarchitectuur. Het is niet langer alleen een maatregel voor militaire bunkers of geheime kamers, maar een praktische oplossing voor elke organisatie die wil voorkomen dat informatie onbedoeld de fysieke omgeving verlaat

In deze context is het risico niet alleen technisch of operationeel, maar ook economisch van aard.

11. NIS2, CRA en de terugkeer van fysieke beveiliging

De introductie van NIS2 en de Cyber Resilience Act (CRA) heeft de manier waarop organisaties naar cybersecurity kijken fundamenteel veranderd. Waar beveiliging jarenlang vooral werd gezien als een software en netwerkvraagstuk, verplichten deze nieuwe kaders organisaties om risico's integraal te beoordelen inclusief de fysieke laag. Daarmee komt een discipline als TEMPEST opnieuw in beeld, niet als niche techniek, maar als een noodzakelijke aanvulling op moderne beveiligingsarchitecturen.

NIS2 legt de nadruk op het beschermen van essentiële en belangrijke entiteiten tegen verstoringen, sabotage en datalekken. Daarbij wordt expliciet gekeken naar de volledige keten: van digitale processen tot fysieke infrastructuur. Organisaties moeten aantonen dat zij maatregelen nemen om informatie te beschermen tegen alle vormen van ongeautoriseerde toegang, inclusief het onderscheppen van elektromagnetische emanaties. Dit betekent dat de fysieke omgeving waarin IT apparatuur draait racks, ruimtes, kabeldoorvoeren, voedingen onderdeel wordt van de beveiligingsbeoordeling.

De CRA gaat nog een stap verder door leveranciers verantwoordelijk te maken voor de veiligheid van hun hardware gedurende de volledige lifecycle. Apparatuur moet veilig worden ontworpen, veilig worden geleverd en veilig blijven door middel van updates en onderhoud. Dit maakt het gebruik van aangepaste of maatwerkhardware (MOTS en NOTS) problematisch: elke aanpassing aan een apparaat kan invloed hebben op garantie, firmware ondersteuning en compliance. COTS hardware daarentegen blijft volledig

binnen de standaard lifecycle van de leverancier, waardoor updates, patches en beveiligingsverbeteringen gegarandeerd blijven.

TEMPEST racks sluiten naadloos aan op deze nieuwe realiteit. Door de afscherming te verplaatsen van de hardware naar de infrastructuur, kunnen organisaties standaard COTS apparatuur blijven gebruiken zonder dat dit ten koste gaat van veiligheid of compliance. Het rack wordt de gecontroleerde grens die voorkomt dat elektromagnetische informatie de beveiligde zone verlaat, terwijl de hardware zelf volledig vendor supported blijft. Dit maakt het mogelijk om te voldoen aan NIS2 eisen voor fysieke beveiliging én aan CRA eisen voor lifecycle veiligheid, zonder de IT omgeving complexer of duurder te maken.

De combinatie van COTS hardware en TEMPEST racks biedt daarmee een toekomstbestendige oplossing die past binnen de wettelijke kaders en tegelijkertijd aansluit op de snelheid waarmee moderne IT omgevingen evolueren. In een tijd waarin regelgeving steeds strenger wordt en de dreigingen steeds geavanceerder, vormt deze aanpak een pragmatische en effectieve manier om zowel digitale als fysieke risico's te beheersen.

Hiermee wordt de fysieke IT infrastructuur, waaronder racks en doorgangen, expliciet onderdeel van de beveiligingsverantwoordelijkheid.

12. Conclusie – waarom TEMPEST opnieuw onmisbaar is

TEMPEST is geen historisch overblijfsel, maar een moderne beveiligingslaag die inspeelt op de realiteit van vandaag: hogere schakelsnelheden, complexere hardware, toegankelijkere afluistertechnologie en strengere wetgeving. Waar klassieke beveiligingsmaatregelen zich richten op de digitale laag, adresseert TEMPEST juist de fysieke laag de plek waar digitale activiteit onvermijdelijk verandert in elektromagnetische informatie.

Dit whitepaper laat zien dat TEMPEST geen verzameling losse maatregelen is, maar een integraal ontwerpkader. Openingen in een IT infrastructuur zijn onvermijdelijk vanwege koeling, bekabeling en voeding, maar vormen pas een risico wanneer zij ongecontroleerd worden uitgevoerd. Door fysieke principes te begrijpen en openingen expliciet te ontwerpen via perforatie, waveguides, afgeschermde interfaces, gaskets en powerfilters wordt functionaliteit mogelijk zonder concessies te doen aan afscherming.

Door de beveiligingsgrens te verplaatsen van het individuele apparaat naar de infrastructuur ontstaat een schaalbare, betaalbare en toekomstbestendige aanpak die aansluit bij moderne IT omgevingen. Het TEMPEST rack fungeert daarbij als gecontroleerde fysieke grens waarin thermiek, mechanica en elektromagnetica samenkomen. In die zin markeert TEMPEST opnieuw de scheidingslijn tussen wat binnen moet blijven en wat nooit ongecontroleerd naar buiten mag treden.

Voor meer informatie met betrekking
tot dit onderwerp:

André Hiddink
Product Manager IT

E-mail: ahiddink@rittal.nl

FRIEDHELM LOH GROUP

Rittal B.V.
Hengelder 56 • Postbus 246 • 6900 AE Zevenaar
Tel.: 0316 59 16 60 • Fax: (0316) 52 51 45
E-mail: sales@rittal.nl • www.rittal.nl

RITTAL