Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: ronald@eygendaal.com

De jacht op straling

In september 2025 arresteerde de politie twee 17-jarige Nederlandse jongens. Ze zouden in opdracht van Rusland hackopdrachten hebben uitgevoerd. Gewapend met WiFi-sniffers liepen de tieners langs cruciale gebouwen in Den Haag, zoals het Europol-kantoor en de Canadese ambassade, om WiFi-verkeer af te tappen.

Zeven jaar eerder, in 2018, probeerden vier Russische hackers vanaf een parkeerplaats in Den Haag in te breken in het WiFi-netwerk van de Nederlandse overheid. Ook zij werden gearresteerd.

Deze incidenten laten pijnlijk zien hoe kwetsbaar de radiostraling van WiFi is bij hoogrisico-objecten. In een tijdperk waarin draadloze communicatie centraal staat in ons IT-landschap, biedt LiFi (Light Fidelity) een revolutionaire oplossing. In plaats van radiogolven gebruikt LiFi zichtbare lichtgolven, infrarood of ultraviolet licht om data over te dragen, sneller en potentieel veiliger. LiFi lost echter niet alle stralingsproblemen op. Dit artikel belicht de LiFi-technologie, de beveiligingsvoordelen en -uitdagingen, organisatorische implicaties en de integratie met TEMPEST-mitigaties, inclusief toekomstperspectieven.

Wat is LiFi

LiFi is een technologie die gebruikmaakt van LED-lampen om gegevens via licht te verzenden. Deze lampen vormen de basis van LiFi, omdat ze miljarden keren per seconde aan en uit kunnen schakelen, onzichtbaar voor het menselijk oog, om digitale informatie in binaire vorm over te dragen.

Een fotodetector, zoals een fotodiode, ontvangt deze lichtsignalen en zet ze om in elektrische signalen die apparaten kunnen verwerken. De snelheid van LiFi varieert per situatie; in laboratoriumtests zijn snelheden tot 224 gigabit per seconde (Gbps) behaald, terwijl praktische toepassingen doorgaans lagere snelheden bieden, rond 3,5 Gbps of 30 Mbit/s bij commerciële systemen. LiFi opereert binnen het zichtbare lichtspectrum en vereist een directe zichtlijn tussen de zender (LED-lamp) en ontvanger.

Dit maakt dat het licht geen muren kan doordringen, wat zowel een beperking als een voordeel is, met name voor informatiebeveiliging.

Informatiebeveiliging en LiFi

Een van de grootste voordelen van LiFi op beveiligingsgebied is de fysieke beperking van licht. Omdat lichtsignalen niet door muren of ondoorzichtige objecten heen gaan, is het veel moeilijker voor onbevoegden om van buitenaf toegang te krijgen tot het netwerk. Dit in tegenstelling tot WiFi, waarbij radiogolven over lange afstanden en door fysieke barrières heen kunnen worden opgevangen, wat het risico op afluisteren vergroot.

Bovendien zorgt LiFi voor natuurlijke netwerkisolatie. In een kantooromgeving kan elke kamer een eigen LiFi-netwerk hebben, zonder interferentie of overlapping met andere ruimtes. Dit vermindert de kans op ongeautoriseerde toegang tot gevoelige gegevens.
LiFi kan worden gecombineerd met encryptietechnieken zoals AES (Advanced Encryption Standard) om de gegevensoverdracht nog verder te beveiligen. Sinds 2025 zijn er LiFi-producten op de markt met FIPS (Federal Information Processing Standard) 140-3-certificering, waardoor LiFi nog geschikter wordt voor high-security toepassingen. LiFi is gestandaardiseerd onder IEEE 802.11bb.

Uitdagingen op het gebied van beveiliging

LiFi-hacking is een relatief nieuw en complex onderwerp, mede door de unieke aard van de technologie. Omdat LiFi gegevens via lichtsignalen overdraagt, vereist hacking een directe zichtlijn naar de lichtbron, wat het moeilijker maakt dan bij WiFi. Toch zijn er potentiële kwetsbaarheden, zoals het onderscheppen van signalen met geavanceerde optische apparatuur als de zender niet goed is afgeschermd.

Manipulatie van LED-lampen, fotodetectors of netwerkverbindingen kan theoretisch ook toegang bieden tot het netwerk. Encryptie, zoals AES en fysieke beveiliging van de infrastructuur zijn cruciaal om deze risico's te minimaliseren. Tot nu toe zijn er weinig geregistreerde gevallen van succesvolle LiFi-hacks, maar onderzoek blijft nodig naarmate de technologie groeit.

In het huidige complexe en onvoorspelbare geopolitieke landschap neemt de kwetsbaarheid toe.

Een andere uitdaging is de integratie van LiFi in bestaande netwerkinfrastructuren. Veel organisaties vertrouwen op een combinatie van bekabelde en draadloze netwerken en het implementeren van LiFi vereist investeringen in nieuwe hardware, zoals LED-lampen en fotodetectors. Daarnaast moeten organisaties ervoor zorgen dat de software en protocollen die LiFi-netwerken ondersteunen, voldoen aan strenge beveiligingsnormen om kwetsbaarheden te minimaliseren.

Toekomstperspectieven

LiFi is momenteel operationeel, vooral in sectoren waar informatiebeveiliging van groot belang is. Onderzoekers werken aan innovaties, zoals het inzetten van meerdere lichtbronnen om de dekking te vergroten en de afhankelijkheid van een directe zichtlijn te verminderen, met aandacht voor roaming tussen verschillende LiFi-netwerken. Gebruikers willen immers naadloos van hun kamer via de gang naar een andere ruimte kunnen bewegen zonder connectieverlies.

Ook wordt er aan locatiebepaling gesleuteld; in LiFi-gebouwen kunnen LED-lampen dankzij de zichtlijn je positie bepalen, waardoor lampen buiten bereik niet hoeven te zenden of te ontvangen. Daarnaast worden hybride systemen onderzocht die LiFi en WiFi integreren om zowel snelheid als beveiliging te verbeteren. Bovendien wordt LiFi al toegepast in omgevingen waar radiogolven ongewenst zijn en elektromagnetische interferentie een probleem kan vormen; hier kan LiFi de oplossing bieden.

LiFi geeft organisatorisch gedoe

De introductie van LiFi zal ook organisatorisch voor aanzienlijke verandering zorgen. Er zijn namelijk al lichtarmaturen op de markt die LiFi ondersteunen, wat een nieuwe dimensie toevoegt aan de infrastructuur van kantoren en andere werkplekken. Dit roept de vraag op: zal de IT-afdeling dan ook verantwoordelijk worden voor de verlichting? Het integreren van verlichting en internettechnologie kan leiden tot een herdefiniëring van taken binnen organisaties. Dit zou betekenen dat IT-medewerkers mogelijk training nodig hebben om met deze hybride systemen om te gaan.

Tegelijkertijd kan het de samenwerking tussen afdelingen zoals facilitair management en IT versterken. Het is een ontwikkeling die zorgvuldige planning en aanpassing vereist om soepel te verlopen.

LiFi en TEMPEST

LiFi elimineert WiFi-radiostraling, maar andere apparaten blijven lekken. TEMPEST – het onbedoeld uitzenden van elektromagnetische signalen door monitoren, toetsenborden, kabels en servers – verraadt nog steeds toetsaanslagen, scherminhoud of verwerkte data. Na de Koude Oorlog lang als verouderd beschouwd, is deze dreiging weer springlevend.

In het huidige complexe en onvoorspelbare geopolitieke landschap – gekenmerkt door oplopende spanningen, verschuivende machtsverhoudingen en miljardeninvesteringen in veiligheid en defensie – neemt de kwetsbaarheid toe.

Het snel veranderende cybersecurity-landschap heractiveert oude gevaren zoals TEMPEST. Technologische vooruitgang heeft de risico's niet verkleind, maar juist verfijnd: moderne interceptietechnieken en groeiende spionageactiviteiten maken het mogelijk om deze zwakke straling op te vangen, van enkele meters tot honderden meters ver, afhankelijk van de gebruikte apparatuur.

Hybride aanvallen

Ook de toename van hybride aanvallen, zoals spionage en cyberoperaties, maakt de Tempest relevantie groter. Staten en niet-statelijke actoren, zoals hackersgroepen, kunnen Tempest technieken combineren met andere methoden zoals social engineering of netwerkhacks om toegang te krijgen tot gevoelige systemen.

Bouwkundige beveiliging

Bij de beveiliging tegen TEMPEST speelt bouwkundige beveiliging een belangrijke rol. Een Faraday-kooi is een afgeschermde ruimte die elektromagnetische straling blokkeert. Het bouwen van zo'n kooi is geen eenvoudige klus; het vereist precisie, planning en de juiste materialen. De kern ligt in het creëren van een volledig geleidende barrière zonder onderbrekingen, goed geaard, en in staat om de specifieke frequenties van TEMPEST-signalen – variërend van kHz tot GHz – te blokkeren.

De kooi mag geen openingen hebben groter dan een fractie van de golflengte van de signalen die je wilt blokkeren – voor GHz-frequenties betekent dit openingen kleiner dan een paar millimeter. Een spectrumanalyzer of EMF-meter is onmisbaar om na de bouw te controleren of de kooi daadwerkelijk werkt. Elk detail telt: een kleine kier, een slecht geaarde verbinding, of een vergeten naad, kan de hele afschermingmaatregelen ondermijnen. Lekken in de kooi worden vaak veroorzaakt door deuren en ramen. Zo dienen ramen bedek te zijn met geleidend gaas of folie en zorgt een slechte, geleidende afdichting rond deuren vaak voor lekkage.

Geen standaard kantooromgeving

Een standaard kantooromgeving is op zichzelf geen Faraday-kooi. Gebruikers hebben immers behoefte aan een bureau, een computer, netwerkverbinding, verlichting, verwarming en andere faciliteiten. Een standaard kantoor zal aangepast moeten worden naar een Faradaykooi.

Bij de inrichting van een dergelijke kantoor ruimte gelden echter specifieke TEMPEST-eisen die in acht moeten worden genomen. Zo is het bekend dat voedings en netwerkkabels zeer gevoelig zijn voor Tempest. Om elektromagnetische interferentie (EMI) en radiofrequentie-interferentie (RFI) te voorkomen, moeten deze kabels op de overgang tussen de externe omgeving en de afgeschermde ruimte (kooi) worden voorzien van Tempest filters ter bescherming. Maar ook alle elektrische apparaten in de kooi dienen voorzien te zijn van deze filters.

Een moderne kooi van Faraday is uitgerust met een intern LiFi-netwerk. LiFi maakt gebruik van lichtgolven voor datatransmissie, die niet door muren of ondoorzichtige objecten kunnen dringen. Hierdoor is het nagenoeg onmogelijk om het signaal buiten de afgeschermde ruimte te onderscheppen. De kabel die het LiFi-accesspoint in de kooi verbindt met de buitenwereld, moet worden voorzien van filters om de afscherming te waarborgen.

Meldingen en buitenbeveiliging

TEMPEST-straling lijkt op een radiosignaal, maar heeft een beperkt bereik. Buiten dit gebied vervaagt het signaal snel, net als een radio die geen ontvangst meer heeft.

Toch kunnen kwaadwillenden het signaal met geavanceerde technieken – zoals gevoelige ontvangers en richtantennes – alsnog onderscheppen. Het gebruik van richtantennes verhoogt echter het risico op ontdekking, bijvoorbeeld door een verdachte auto met antenne in de buurt van een beveiligde locatie.

Om dit te voorkomen, moet het terrein en de gebouwen rondom de beveiligde zone als één beveiligd gebied worden behandeld, vergelijkbaar met een kooi. Dit blokkeert de plaatsing van interceptieapparatuur. Maak gebruik van hekwerken, camera's, toegangspoorten en andere vormen van omtrekbeveiliging om volledige bescherming te garanderen.

Hoewel er nog geen publiek bekende incidenten zijn, wijzen verschillende signalen op hernieuwde interesse van statelijke actoren in TEMPEST. Denk aan de stijgende vraag naar interceptie-apparatuur, waargenomen busjes met antennes bij risicolocaties en de sterk toegenomen belangstelling voor TEMPEST-proof zonwering, anti-TEMPEST-folie en ander maatregelen.

Compliance en ISO 27002

TEMPEST verwijst naar een technisch fenomeen waarbij elektronische apparaten, zoals: monitoren, toetsenborden, kabels en servers, straling uitzenden die eenvoudig kan worden onderschept. In de ISO 27002-norm zijn diverse beheersmaatregelen opgenomen die betrekking hebben op interceptie. Zo richt control 7.12 Cabling security zich op het beveiligen van kabels tegen interceptie, terwijl control 8.12 Data leakage prevention eveneens interceptie adresseert. Door LiFi en TEMPEST-beveiligingsmaatregelen te implementeren, wordt voldaan aan deze ISO 27002-controls.

"Boevenvangers, de groeten…"

Referenties

https://www.nu.nl/tech/6067694/eu-legt-vier-russen-sancties-op-voor-hackaanval-op-opcw-in-den-haag.html

https://tweakers.net/nieuws/239652/politie-arresteert-17-jarigen-die-met-wifisniffer-voor-rusland-zouden-spioneren.html

https://www.signify.com/en-gb/our-company/news/press-releases/2025/20250611-signifys-trulifi-light-based-network-meets-highest-encryption-standards

https://www.hart4technology.nl/nl/tempest-beveiliging