

## LiFi voor high-security omgevingen

In 2014 publiceerde ik het artikel “Security met LiFi”. Sindsdien heeft de ontwikkeling van LiFi een flinke vlucht genomen. In een tijdperk waarin draadloze communicatie een centrale rol inneemt in ons dagelijks leven, introduceert LiFi (Light Fidelity) een vernieuwende aanpak door gegevens over te dragen via licht. In plaats van de radiogolven die traditionele WiFi benut, maakt LiFi gebruik van zichtbare lichtgolven, infrarood of ultraviolet licht, wat resulteert in hoge snelheden en mogelijk veiligere datatransmissie. Dit artikel gaat dieper in op de technologie achter LiFi en belicht hoe deze bijdraagt aan informatiebeveiliging, met een focus op de voordelen, uitdagingen en toekomstige mogelijkheden.

### 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 het gebied van informatiebeveiliging is de fysieke beperking van licht. Omdat lichtsignalen niet door muren of ondoorzichtige objecten heen kunnen, is het veel moeilijker voor onbevoegden om toegang te krijgen tot het netwerk van buitenaf. 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 een natuurlijke netwerkisolatie. In een kantooromgeving kan elke kamer bijvoorbeeld een eigen LiFi-netwerk hebben, zonder interferentie of overlapping met andere ruimtes. Dit vermindert de kans op



ongeautoriseerde toegang tot gevoelige gegevens. Daarnaast kan LiFi worden gecombineerd met encryptietechnieken zoals AES (Advanced Encryption Standard) om de gegevensoverdracht nog verder te beveiligen, wat het een sterke oplossing maakt voor omgevingen waar veiligheid essentieel is, zoals banken, defensie en overheidsinstellingen. Sinds dit jaar zijn er LiFi-producten op de markt met FIPS 140-3-certificering, waardoor LiFi nog geschikter wordt voor high-security toepassingen.

### 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. 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 toe-

gepast 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.

### Conclusie

LiFi biedt een revolutionaire benadering van draadloze communicatie met aanzienlijke voordelen op het gebied van informatiebeveiliging. De fysieke beperkingen van lichtsignalen maken het een veiliger alternatief voor WiFi in omgevingen waar gegevensbescherming cruciaal is. Hoewel er uitdagingen zijn, zoals de afhankelijkheid van een directe zichtlijn en de kosten van implementatie, maken de hoge snelheden en inherente beveiligingsvoordelen LiFi tot een veelbelovende technologie voor de toekomst. Naarmate de technologie zich verder ontwikkelt, zal LiFi waarschijnlijk een belangrijke rol spelen in het vormgeven van veilige, snelle en efficiënte communicatienetwerken.

---

*Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België.*

Bron en foto: Ronald Eygendaal

