## Feitelijke reactie Lydis

“Op zaterdag 16 september heeft Follow The Money een artikel geplaatst van Siem Eikelenboom en Sebastiaan Brommersma, waarin Yealink in een kwaad daglicht wordt gesteld. Lydis, als distribiteur van Yealink in de Benelux, heeft het artikel van Follow The Money geanalyseerd. Hieronder een aantal citaten uit het artikel, waaronder Lydis in het **PAARS**, haar reactie geeft op de aantijgingen van Follow The Money.”

Belangrijk om te weten is dat voor alle bedrijven, nimmer via Yealink-servers verloopt, wat betekent dat China en daarmee Yealink geen toegang en inzicht heeft in de communicatie.

Lydis heeft zich beperkt om hieronder de meest belangrijke opmerkingen te benoemen.

1. De belangrijkste boodschap die helder moet zijn, is: *‘Yealink beschikt niet over de communicatiedata van de apparatuur en kan dus anders dan is gesuggereerd ook geen data delen met de Chinese overheid.’*

2. Experts hebben slechts theoretisch naar geïsoleerde deelkwesties gekeken op basis van informatie van Hermans en daar op geoordeeld.

3. De experts hebben geen oordeel gevormd over de producten als geheel en de wijze waarop de producten gebruikt en geïmplementeerd worden. De presentatie van de expert conclusies moet dan ook worden afgedaan als "verdachtmakerij".

4. Verdenking wordt ondersteund door gebruik te maken van “oude” kwesties die al jaren opgelost zijn, en kwesties ten aanzien van producten die al jaren niet meer op de markt zijn.

5. Veel betrouwbare klanten, waaronder alle bekende providers in de Benelux, zoals Proximus, bevestigen de veiligheid van Yealink-producten. De producten worden grondig onderzocht door experts met behulp van pentests.

6. Onafhankelijke instituten zoals bijv. NetSPI, Spirent en Miercom hebben als experts op gebied van veiligheid, de producten en oplossingen van Yealink uitgebreid getest en komen tot de conclusie dat er "geen kwetsbaarheden" te vinden zijn.

Lydis team

# Reactie Lydis op artikel van Follow The Money over communicatieapparatuur van Yealink

De Nederlandse politie, ministeries, universiteiten, het Openbaar Ministerie, banken, ziekenhuizen, media en bedrijven actief binnen vitale sectoren gebruiken communicatieapparatuur van het Chinese bedrijf Yealink. Dit blijkt uit onderzoek van FTM in samenwerking met zakenkrant De Tijd.

Experts waarschuwen dat overheidsinstanties Yealink beter niet kunnen gebruiken.

**Reactie Lydis:** Een aantal veiligheidsexperts waarschuwden in het artikel naast 'bepaalde technische veiligheidsrisico's' ook over een in China onbekende wet over het feit dat 'Yealink is onderworpen aan de Chinese regels met betrekking tot de toegang van de data die het verzamelt.' **Lydis en Yealink willen benadrukken dat Yealink geen toegang heeft tot de communicatiedata.**

Helaas wordt er in het artikel een oordeel geveld op basis van fragmentarische informatie van Hermans. Er wordt geen oordeel gegeven op basis van de volledige oplossing en de positieve professionele tests, zoals die zijn uitgevoerd door NetSPI, Spirent en Miercom.

# Online vergaderen via Teams

Aan videoconferenties kun je ook met vaste telefoons deelnemen, mits die VoIP aankunnen: een verbinding via internet. Heide laat een demo zien van een zaaltje waar een dozijn mensen via Teams vergadert. De camera, die de meeting online toegankelijk maakt, zoomt automatisch in op wie het woord neemt. Ook hier zijn video en audio van topkwaliteit.

**Reactie Lydis:** In het artikel wordt ten onrechte alle apparatuur van Yealink over één kam geschoren. De producten die voor videovergaderingen worden gebruikt zijn allemaal Microsoft Teams "certified" en voldoen verplicht aan de veiligheid standaarden van Microsoft. ***Hier*** vind je de volledige eisen die Microsoft stelt aan alle fabrikanten die deze apparatuur maken. Deze Microsoft eisen gelden ook voor de telefoons die "Microsoft Teams certified" zijn.

Yealink verklaart ten aanzien van de Microsoft eisen:

Yealink's MTR and Teams phones are pre-installed with Microsoft's Teams app on the device. All Teams User Account & Teams Meeting Audio/Video Data are all in the Microsoft secure tunnel.

Regarding to Microsoft Teams data, "**No end-user data is transferred to, or accessible by, the Microsoft Teams (Rooms) device**."

Data van de Teams vergaderingen/telefoongesprekken kunnen dus niet naar China vloeien zelfs als China er om zou vragen want is er geen data om door te geven.

Volgens een woordvoerder van Microsoft zegt dat echter niets over veiligheid, zij hebben alleen de kwaliteit van de audio en video getest. 'In onze specificaties geven wij aan dat de fabrikanten van de devices verantwoordelijk zijn voor de beveiliging van de devices, de software en de firmware.'

- **Reactie Lydis:** Met deze beweringen wordt de lezer misleid. De link naar een Microsoft-pagina behandelt **USB-audio- en video devices**, zoals USB-headsets, speakers en camera's. De USB-apparaten zijn bedoeld voor thuiswerkplekken en vereisen een verbinding met een computer.

  Echter, het artikel van FTM richt zich op de Microsoft Teams Rooms-oplossingen voor vergaderruimtes, zoals Yealink MVC systemen en Android Meetingbars. Voor de Teams Rooms-oplossingen heeft Microsoft strikte specificaties opgesteld voor certificering. Deze oplossingen worden gebruikt om Teams-vergaderingen in vergaderruimtes te faciliteren.

  Yealink voldoet met al haar Microsoft Teams producten aan deze certificering van Microsoft omdat je alleen dan door Microsoft het stempel "certified" kan krijgen en mag voeren.

  De vereisten voor certificering omvatten:
  **Hardware-, software-, account- en netwerkbeveiliging.**

  Klik hier voor de volledige Microsoft security specificaties.

# De risico's van Chinese technologie

In juli 2021 nam de Chinese overheid nieuwe regels aan die in China opererende techbedrijven verplicht om kwetsbaarheden in hun software binnen 48 uur na ontdekking te melden.

**Reactie Lydis:** 'De juridische afdeling van Yealink heeft deze bewering uit het artikel gecontroleerd en geeft aan dat deze wetgeving in China niet bestaat, dit is echter ook niet relevant omdat Yealink anders dan bijvoorbeeld Chinese social media of autobedrijven geen data verzamelt. Er is dus niets om door te geven aan de overheid.

## De Chinese wet kan bedrijven dwingen achterdeurtjes en *bugs* in te bouwen, om de overheid toegang tot systemen te geven

Er is een tweede grond voor argwaan. China heeft strikte veiligheidswetten die technologiebedrijven verplichten om gebruikersgegevens over te dragen als de overheid dat vraagt. Dat geldt eveneens voor buitenlandse bedrijven die in China actief zijn. De wet kan Chinese bedrijven voorts dwingen achterdeurtjes en *bugs* in te bouwen, teneinde de overheid toegang tot systemen te geven.

In december 2020 waarschuwde het Amerikaanse ministerie van Binnenlandse Veiligheid voor het gebruik van Chinese hardware en digitale diensten, vanwege de strenge Chinese veiligheidswetten. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) waarschuwt al sinds 2010 voor de dreiging uit China.

In november 2022 publiceerden de inlichtingendiensten AIVD en MIVD met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) het tweede rapport Dreigingsbeeld Statelijke Actoren. Daarin staat dat China, Iran en Rusland een grote bedreiging voor de economische veiligheid vormen en een offensief cyberprogramma tegen Nederland en Nederlandse belangen voeren.

Dat roept de vraag op: hoe veilig is het om de producten van Yealink te gebruiken?

**Reactie Lydis:** De opmerking over de Chinese wetgeving komt een aantal malen terug in het artikel. ‘De juridische afdeling van Yealink heeft deze bewering uit het artikel gecontroleerd en geeft aan dat deze wetgeving in China niet bestaat!

Data van de telefoongesprekken met SIP telefoons kunnen niet naar China vloeien zelfs als China er om zou vragen want is er geen data om door te geven. Bij het gebruik van de apparatuur is er geen verbinding met een server van Yealink. Dit wordt bevestigd door experts van de providers die uitvoerig hebben onderzocht.

Op basis van positieve rapporten van bijv. experts als NetSPI, Spirent, Miercom zijn de producten veilig bevonden.

Als organisatie heeft Yealink onafhankelijke tests ondergaan en is gecertificeerd met ISO 27001 en SOC 1, 2, 3. Dit zijn harde feiten waarmee de conclusie "veilig" getrokken kan worden. Raadpleeg voor de certificeringen: https://www.yealink.com/en/trust-center/resources

# ‘Yealink kan door China worden gebruikt’

Een nieuwe VoIP-telefoon moet je eerst configureren. Daar hoef je zelf weinig voor te doen: zodra je hem aanzet, maakt hij contact met de servers van de fabrikant. Daar staat voor elk type toestel informatie met de juiste instellingen, plus de gegevens over je telefoonabonnement. ‘Al die informatie wordt ontsloten via de servers van de fabrikant,’ zegt Hermans. ‘Ook gevoelige informatie, zoals het serienummer van je telefoon en je gebruiksgegevens bij je telco-provider

**Reactie Lydis:** Alleen bij het voor de eerste keer instellen van de telefoon wordt er verbinding gemaakt met een RPS server, welke zich bevindt in Europa of de VS, afhankelijk van jouw locatie. De enige data die daarbij wordt overgedragen, is de locatie (URL) van de telefonie provider zoals bijv. Proximus of Vodafone, waar de instellingen voor het product

kunnen worden opgehaald. Het is technisch niet mogelijk om met de RPS server instellingen of firmware te laden in het product. De RPS server doet alleen maar een redirect naar de telefonie provider. De RPS server heeft als doel om de installatie te vergemakkelijken.

Zodra het product de instellingen van de telefonie provider ontvangen heeft, wordt automatisch in het product het verbinden met de RPS volledig uitgeschakeld. Dit kan niet weer door Yealink worden aangepast op afstand.

Er is dan vervolgens geen enkele verbinding meer met de RPS-server of andere server van Yealink.

De instellingen voor bijvoorbeeld, je telefoonnummer, gebruiksgegevens zijn opgeslagen op de server van de telefonieprovider!
Providers verzekeren hun klanten dat alle communicatiedata veilig is en dat Yealink hier geen toegang toe heeft.

De telefoons checken geregeld (en automatisch) of er nieuwe informatie in 'hun' provisioningsdocument staat.

**Reactie Lydis:** Dit is een direct proces tussen het product en het telefonie-platform van de provider (bijv. KPN, Proximus of Vodafone), zonder connectie met een Yealink-server of enige bemoeienis van Yealink-.

Ook Yealinks MeetingBar A20, een videoconferencing-product voor Microsoft Teams, zoekt bij firmware-updates contact met de servers van Yealink, constateerde cybersecurity-expert Matthijs Koot. Hij lichtte de MeetingBar voor FTM door.

**Reactie Lydis:** Helaas doet expert Matthijs Koot zijn bewering aan de hand van het domein " rpscloud.yealink.com" wat door het product wordt opgevraagd om de eerder genoemde RPS te benaderen. Het domein "rpscloud.yealink.com" is geregistreerd door Yealink bij een Chinese hosting maatschappij, maar de servers staan in Europa of VS. Het verband leggen tussen de registratie-organisatie van domein en dat het daardoor verdacht is, geeft grote vraagtekens bij deze bewering als je weet dat Yealink een Chinees bedrijf is.

Het verdere management van het product qua instellingen en firmware verloopt via het Microsoft Teams-platform en de Microsoft servers. Er is dan dus geen verdere verbinding met de RPS-server of andere server van Yealink. Voor het ophalen van firmware wordt dus geen contact gezocht met servers van Yealnk.

# ‘Zo is afluisteren een koud kunstje’

Naast de eventuele overheidsbemoeienis is er een ander probleem: de beveiligingsproblemen met de provisonering. Om dat proces veilig te laten verlopen, worden provisioningsdocumenten versleuteld naar telefoons verstuurd. Je kunt ze alleen ontgrendelen met een unieke sleutel, die op je eigen apparaat staat. Hermans ontdekte dat die voor alle telefoons van het bedrijf hetzelfde was, en dat Yealink die sleutel open en bloot had gepubliceerd in de software die het voor de provisioning gebruikt.

**Reactie Lydis:** ‘Veel betrouwbare klanten, waaronder alle bekende providers van de Benelux, bevestigen dat de Yealink-producten veilig zijn en dat de veiligheid ervan wordt aangetoond door verschillende ‘penetration test’-rapporten van gerenommeerde instanties zoals NetSPI, Spirent en Miercom.’ Bekijk alle pentest rapporten van Yealink *hier*.

*Pentest is een afkorting van ‘penetration testing’. Bij een Pentest gaan legale (ethische) hackers op realistische wijze de systemen onderzoeken. Zij kruipen als het ware in de huid van een kwaadwillende hacker. Net als een echte crimineel proberen ze op alle mogelijke manieren toegang te krijgen tot beveiligde gegevens.*

Lydis wil benadrukken dat het zodra één van de experts, die Follow The Money en De Tijd raadpleegden, dit jaar aan Yealink melding maakte dat beveiligingssleutels publiek waren, Yealink zijn ‘encryptietool ondanks dat de professionele providers het niet gebruiken, toch heeft aangepast zodat er geen standaardsleutel meer getoond wordt’.
Yealink nam de opmerking serieus en heeft zo spoedig mogelijk een nieuwe versie uitgebracht en haar klanten geïnformeerd. Belangrijk om te vermelden is dat telefonie providers (op wiens netwerk de Yealink producten functioneren) niet werken met de encryptietool. Zij zetten andere maatregelen in om de inhoud niet leesbaar te maken en het netwerk waar de producten actief zijn optimaal te beveiligen.

De genoemde kwetsbaarheid is dus wel aan de orde geweest maar in het geheel niet representatief voor het onderwerp van het artikel omdat deze kwestie voor grote bedrijven en overheden niet gespeeld kan hebben.

Yealink nam nog een tweede maatregel. Het versleutelde de firmware van een reeks oude en nieuwe telefoons, zodat die niet langer kon worden gelezen.

In de klantbrief van juli 2023 meldde Yealink ook deze stap, en benadrukte ditmaal dat dit probleem alleen speelde bij telefoons die niet meer worden verkocht, en dat er geen informatie van gebruikers was weggelekt.

‘Als firmware onleesbaar is, is dat een probleem,’ zegt cybersecurity-specialist Brenno de Winter. ‘Je kunt dan niet meer onafhankelijk controleren of producten veilig zijn en wat er allemaal in die software zit. Voor overheden die opereren in een gevoelige omgeving, zoals de politie en het OM, is het een *big deal* als ze apparaten met afgeschermde firmware gebruiken, want die kunnen de veiligheid van hun communicatie dan niet automatisch waarborgen.’

**Reactie Lydis:** Deze bewering is opvallend en wekt verwarring en argwaan op. Yealink geeft aan dat het versleutelen van de firmware noodzakelijk is om producten goed te beschermen. Het gaat hier over de firmware voor de SIP telefoon toestellen.

De firmware welke in de Benelux voor de SIP telefoons gebruikt wordt, is met deze wijziging in April 2023 gereleased voor alle klanten.
Yealink heeft Hermans uitgebreid geïnformeerd dat ze eigen Yealink software hebben gebruikt om de open source modules volledig te beschermen en te beveiligen.
Raadpleeg deze tests voor meer informatie over de veiligheid.
https://www.yealink.com/en/trust-center/resources

# Software uit de ‘digitale steentijd’

Hermans constateerde voorts dat bij Yealinks VoIP-telefoons standaard een netwerkpoort open staat. Volgens Koot, De Winter en Hermans is het openen van deze poort alleen in uitzonderingen nodig.

**Reactie Lydis:** Deze bewering is onjuist en onthult een gebrek aan kennis bij Hermans over hoe SIP-telefonie werkt.
Dat er bij SIP telefoon altijd een netwerkpoort openstaat is noodzakelijk voor het ontvangen oproepen en kunnen bellen. 'Als de provider ervoor kiest om de communicatie naar de telefoon via een andere poort te leiden, kan die standaardpoort worden gesloten met de juiste instellingen. Dit kan worden bevestigd door technische experts. Providers sluiten alle poorten die niet nodig zijn met instellingen in het product (vandaar dat dit ook ingesteld kan worden in de instellingen). Het is onjuist dit te bestempelen als een kwetsbaarheid. Het gebruik van deze poort is niet uniek voor Yealink-producten, maar wordt gebruikt door alle fabrikanten die SIP-telefoons aanbieden. Het gedrag van andere fabrikanten is hetzelfde als dat van Yealink.

---

Hermans doelt op de waslijst open source software die Yealink in veel producten heeft verwerkt. Een deel ervan is meer dan tien jaar oud; de oudste software stamt zelfs uit 2008: 'Dat is de digitale steentijd,' zegt Hermans. 'Bovendien bevat veel van die software bekende, kritieke kwetsbaarheden.'

**Reactie Lydis:** Belangrijk om te vermelden: Hermans heeft vergeten te vermelden dat Yealink haar eigen software heeft geschreven om de open source modules te beschermen en te beveiligen. Deze software zorgt ervoor dat de veiligheid van het complete product gegarandeerd is. Yealink heeft Hermans hier uitgebreid over geïnformeerd. Hermans heeft dit niet weersproken maar gebruikt een beoordeling van de onbewerkte open source modules om Yealink in een kwaad daglicht te stellen.

De tests van officiële testinstituten zoals Spirent, NetSPI en Miercom bevestigen dat het complete product veilig is. Raadpleeg deze tests voor meer informatie: https://www.yealink.com/en/trust-center/resources

Sommige daarvan stellen een kwaadwillende hacker in staat om producten op afstand te laten crashen, er kwaadaardige software op te zetten of toegang te krijgen tot potentieel gevoelige informatie.

**Reactie Lydis:** Deze bewering is niets meer dan "verdachtmakerij". Het is een theoretische stelling die niet wordt ondersteund door bewijs van de expert.
Maar de positieve tests van gerenommeerde instituten zoals Spirent, NetSPI en Miercom tonen aan dat het complete product veilig is.
Raadpleeg hen voor meer informatie:
https://www.yealink.com/en/trust-center/resources

De Winter**:** 'Verouderde software levert een verhoogd risico op, zeker wanneer het om bekende lekken gaat. Het is duidelijk dat het beheer van deze producten niet in lijn is met de normenkaders voor security die we in Nederland kennen. Yealink heeft dus een probleem met haar spullen. Maar wie daar als overheid gebruik van maakt, heeft minstens een even groot probleem. Je kunt een product met onderdelen waarop al 15 jaar geen onderhoud meer is gepleegd, simpelweg niet vertrouwen. Voor inlichtingendiensten en criminelen is dit een natte droom.'

**Reactie Lydis:** Duidelijk voorbeeld van een eenzijdige beoordeling van een deel van een product/oplossing.

Dat het complete product veilig is, bevestigen de positieve testen van bijv. Spirent, NetSPI en Miercom. Raadpleeg hiervoor:
https://www.yealink.com/en/trust-center/resources

Tussen 2011 en 2023 zijn er diverse kritieke kwetsbaarheden gevonden in de beveiliging van Yealinks producten. Twee ervan kregen de hoogste score in het Common Vulnerability Scoring System; kwetsbaarheden tussen de 9 en 10 zijn kritiek. Een selectie:

**Reactie Lydis:** Elke softwarefabrikant, heeft te maken met mogelijke verbeteringen in de software. Wij nodigen je uit om op https://cvedetails.com te kijken en zelf een oordeel te vormen over Yealink in vergelijking met andere fabrikanten.

Yealink scoort relatief positief op cvedetails en blijft voortdurend investeren in het verbeteren van hun producten en het vermijden van beveiligingsproblemen. Ze werken samen met experts van Netspi, Spirent en Miercom voor gedetailleerde onafhankelijke controles.

De claim over het model T38G is alleen al ongegrond, omdat de SIP-T38G in de Benelux nooit verkocht is door de officiële Yealink distributeurs.

# Klanten vertrouwen op certificaten

‘Het is duidelijk dat Yealink geen hoge prioriteit hecht aan beveiliging en technische expertise mist,’ stelt de internationaal hooggewaardeerde cryptograaf Bart Preneel (KU Leuven). 'In het licht van het grote aantal problemen zou ik dit eerder aan incompetentie wijten dan aan bewuste onveiligheid. Als je achterpoortjes wilt verbergen, kan dat veel subtieler.’

**Reactie Lydis:** Deze bewering is opmerkelijk en bevat een matige beargumentering.

De serieuze klanten en experts zoals NetSPI, Spirent en Miercom geven gecontroleerd een hoge waardering qua veiligheid van de producten. De onafhankelijke certificeringen ISO27001, SOC 1, 2, 3 bevestigen de kwaliteit van Yealink. Ondanks dat Yealink vaak duurder is dan de concurrentie, kiezen klanten bewust voor onze producten omwille van deze redenen.

Proximus zegt de VoIP-toestellen die het gebruikt te hebben getest, ‘in een laboratoriumomgeving om de netwerkactiviteit van het apparaat te controleren’. Ze vonden ‘geen enkele aanwijzing voor abnormaal gedrag’ ervan. ‘Ook het platform waarop de Yealink-apparatuur wordt gebruikt, hebben we vooraf onderworpen aan uitvoerige “penetratietesten” door een extern bedrijf.’

**Reactie Lydis:** Dit is de enige juiste manier om producten en fabrikanten onafhankelijk en grondig te beoordelen middels uitgebreide (pen)testen. Zoals alle professionele telefonieproviders over de hele wereld aangeven wordt de veiligheid beoordeeld door onafhankelijk en feitelijk te testen, in de telecommarkt worden hiervoor **pen testen** gebruikt.

## ‘Zelfs zonder die fout is het als overheidsdienst of groot bedrijf echter niet verstandig om apparatuur uit niet-bevriende landen te gebruiken’

Navraag bij TÜV Rheinland in Duitsland leert echter dat dit certificaat niet meer geldig is en dat Yealink het niet meer mag voeren. Yealink erkende eerder deze week tegenover FTM dat het certificaat eind augustus is vervallen. Desondanks refereert het daar op zijn website nog steeds aan.

**Reactie Lydis:** Belangrijk om te vermelden is dat het certificaat slechts kort geleden is verlopen, niet vanwege geconstateerde security-issues maar door tijdsverloop. Yealink is bezig het GDPR certificaat te vernieuwen, wat slechts een formaliteit zal zijn gezien hun focus op security.

Daarnaast is het een wettelijke verplichting om een goede beveiliging te hebben **maar niet om een dergelijk certificaat te hebben**. Gelukkig is de beveiliging van Yealink bevestigd door SOC3 en de pentest van NetSPI. Voor meer informatie, zie: https://www.yealink.com/en/trust-center/resources.

Cryptograaf Preneel sluit zich daarbij aan. ‘Als alle toestellen dezelfde gedeelde geheime sleutel hebben of hadden, is dat een ernstige ontwerpfout of configuratiefout. Het maakt het beheer van de toestellen uiteraard eenvoudiger, maar het is zeer onveilig. Zelfs zonder die fout is het als overheidsdienst of groot bedrijf echter niet verstandig om apparatuur uit niet-bevriende landen te gebruiken,’ waarschuwt hij.

**Reactie Lydis:** Belangrijk om te weten: er wordt een conclusie getrokken op basis van onvolledige informatie van Hermans, waarbij simpelweg wordt genegeerd dat de encryptietool niet wordt gebruikt door providers/carriers/professionals op de markt ondanks dat dit herhaaldelijk door Lydis / Yealink gecommuniceerd is aan Hermans

Daarnaast lijken we blind te zijn voor de herkomst van producten uit "bevriende" landen. Bijna alle (mobiele) telefoons en videotoepassingen

worden in China geproduceerd, zelfs voor producten uit "bevriende" landen (bijna 93% wordt geheel of gedeeltelijk in China geproduceerd, inclusief merken uit Europa en de VS).

Het lijkt ons verstandig om, net zoals veel serieuze klanten doen, te vertrouwen op de veiligheid en bruikbaarheid van producten die zijn getest en gecertificeerd door gerenommeerde instanties zoals NetSPI, Spirent en Miercom, en die voldoen aan ISO27001 en SOC 1, 2, 3 normen. Het is belangrijk om communicatie apparatuur hiermee te beoordelen en niet met een tunnelvisie of met vooringenomen standpunten te oordelen.