Kapteynstraat 1, SBIC - Building suite 220 / 2201 BB Noordwijk

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Position paper CVNL inzake Client Side Scanning

Aanleiding

Via chat-apps wordt veel illegale inhoud, waaronder online kinderporno, verspreid. Dat is een probleem en moet worden aangepakt. Momenteel wordt binnen de Europese Commissie een wetsvoorstel voorbereid om de verspreiding van online kinderporno, child sexual abuse material ofwel CSAM, tegen te gaan. Onderdeel van het huidige voorstel is een zogeheten detectiebevel. Op basis hiervan kunnen (tech)bedrijven onder voorwaarden worden verplicht om hun diensten te scannen op de aanwezigheid van materiaal van online seksueel kindermisbruik, zodat dit kan worden doorgeleid naar de opsporingsdiensten. Client-side scanning, waarbij de inhoud van chatberichten van burgers op hun telefoon wordt gecontroleerd, is volgens Cyberveilig Nederland wel degelijk een aantasting van end-to-end encryptie (verder E2EE) en heeft negatieve gevolgen voor de cybersecurity van Europa.

Negatieve gevolgen Client Side Scanning voor cyberveiligheid van Europa

We hebben hier verschillende technische en ethische standpunten en argumenten voor. Hieronder volgen de belangrijkste:

1. **Schending van het basisprincipe van vertrouwelijkheid**
   De kern van E2EE is dat alleen de verzender en de ontvanger de inhoud van de communicatie kunnen ontsleutelen en lezen. Client-side scanning doorbreekt dit principe omdat het gegevens toegankelijk maakt op het apparaat voordat ze versleuteld zijn of nadat ze ontsleuteld zijn. Dit ondermijnt de vertrouwelijkheid die E2EE belooft, wat een fundamentele pijler is voor veel beveiligingsoplossingen.

2. **Creëren van nieuwe aanvalsvectoren**
   Door een systeem toe te voegen dat berichten op een apparaat scant, creëer je een nieuwe aanvalsvector waar misbruik van gemaakt kan worden. Malware, hackers of kwaadwillende partijen kunnen mogelijk de client-side scanning-mechanismen misbruiken om toegang te krijgen tot gegevens die anders beschermd zouden zijn. De aanwezigheid van zo'n mechanisme vergroot de oppervlakte van mogelijke kwetsbaarheden, waardoor cybercriminelen of statelijke actoren meer kans krijgen om gevoelige informatie te onderscheppen of te manipuleren.

3. **Vertrouwen in software integriteit wordt ondermijnd**
   Client-side scanning vereist dat software op het apparaat van de gebruiker in staat is om de inhoud van berichten te lezen en analyseren. Dit staat haaks op ontwikkelprincipes zoals privacy- en security-by-design en -default. Dit kan het vertrouwen in de integriteit van software ondermijnen. Cybersecurity-experts waarschuwen vaak tegen systemen die een "achterdeur" kunnen bieden naar gebruikersgegevens, omdat zelfs goedbedoelde monitoringsoftware kwetsbaar kan zijn voor misbruik.

4. **Inconsistentie met 'zero-trust' modellen**
   Veel cybersecuritystrategieën zijn gebaseerd op het 'zero-trust' principe, dat stelt dat geen enkele entiteit, zelfs interne systemen, volledig vertrouwd mag worden. Client-side scanning vereist echter dat gebruikers vertrouwen op de software of dienst die de scanning uitvoert, wat in strijd is met het idee dat alle componenten als potentieel onbetrouwbaar moeten worden beschouwd. Dit kan leiden tot een groter risico als een kwaadwillende partij, zoals cybercriminelen of statelijke actoren, toegang krijgt tot de scanfunctionaliteiten.

5. **Verzwakking van algehele beveiliging**
   De sector waarschuwt vaak dat het verzwakken van één aspect van beveiliging, zoals encryptie, een domino-effect kan veroorzaken voor andere beveiligingssystemen. E2EE is een hoeksteen van digitale beveiliging voor persoonlijke communicatie, financiële transacties, en veel andere toepassingen. Als client-side scanning eenmaal wordt geïntroduceerd, kan dit de weg vrijmaken voor verdere verzwakking van beveiligingsstandaarden, wat een algehele erosie van digitale veiligheid veroorzaakt.

6. **Risico op massatoezicht en misbruik**
   Vanuit een privacy- en ethisch perspectief waarschuwt de cybersecuritysector vaak voor de gevaren van massatoezicht. Client-side scanning kan worden gezien als een

vorm van geautomatiseerde surveillance op grote schaal. Hoewel het in eerste instantie bedoeld kan zijn voor specifieke doelen, zoals het bestrijden van kindermisbruik, kan het systeem gemakkelijk worden uitgebreid naar bredere vormen van monitoring door overheden of bedrijven, wat een serieuze inbreuk vormt op burgerrechten en privacy. De maatschappelijke impact weegt dan ook niet op tegen de beoogde resultaten.

7. **Internationale precedentwerking**
   De cybersecuritysector wijst ook op het risico dat als één land of een groep landen client-side scanning afdwingt, dit een precedent schept voor andere regeringen om vergelijkbare of zelfs uitgebreidere surveillancesystemen in te voeren. Dit zou kunnen leiden tot een wereldwijde verzwakking van encryptie en digitale rechten, waarbij landen met minder strenge privacywetten de technologie voor bredere surveillancedoeleinden zouden kunnen inzetten.

8. **Verlies van vertrouwen door gebruikers**
   Client-side scanning kan leiden tot een verlies van vertrouwen van gebruikers in digitale diensten. Gebruikers kiezen vaak voor platforms die E2EE bieden juist vanwege de beloften van privacy en beveiliging. Als zij het gevoel krijgen dat hun berichten niet langer privé zijn, kan dit het vertrouwen in die diensten ondermijnen en hen ertoe aanzetten andere, potentieel minder veilige communicatiemiddelen te gebruiken.

9. **De burgerrechten van de inwoners van de EU worden geschonden**
   De EU slaat onterecht bevonden meldingen blijvend op. De AVG schrijft voor dat verwerkingen bewaard mogen blijven tot het doel van de verwerking is bereikt. Als een melding onterecht is, is het doel voor opsporen van terechte meldingen bereikt (de melding is immers onterecht bevonden) en de persoonsgegevens moeten dan terstond verwijderd worden. Ook is niet duidelijk of er mogelijkheden zijn tot een rectificatie als een false positive wordt gedetecteerd? Er staan geen harde voorwaarden voor autoriteiten om een klacht of verzoek tot intrekking meteen op te volgen. Ook is onduidelijk of er een beroepscommissie is waar de burger laagdrempelig verweer kan uiten. De gang naar de rechter en/of overheid dwingt een burger tot het in de arm nemen van een advocaat, waardoor directe en indirecte kosten plus derving zullen ontstaan. De kans dat daar binnen een redelijke termijn iets van terugkomt is, afgaande op ervaring met de overheid, niet gegarandeerd, zie onder andere het Toeslagenschandaal.

Kortom: De cybersecuritysector beschouwd client-side scanning als een directe bedreiging voor de integriteit en veiligheid van end-to-end encryptie. Tenslotte zijn er ook nog de ernstige, destructieve gevolgen voor de burgerrechten van inwoners van de Europese Unie.