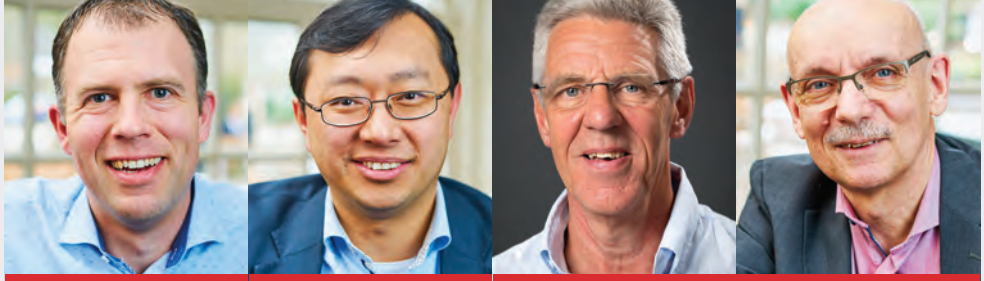
Achter Het Nieuws

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

Client Side Scanning: middel zoekt toepassing

Twee jaar geleden nam Apple het initiatief om de apparatuur van haar gebruikers actief te gaan controleren op (in eerste instantie) kinderporno. Experts (en heel veel medewerkers) waarschuwden massaal voor de risico's. Het resulteerde in een flinke deuk in het privacy-imago van het bedrijf, dat in 2021 de plannen snel op de lange baan schoof. Sinds het initiatief van Apple passeert Client Side Scanning regelmatig de revue en wordt er door voor- en tegenstanders druk gelobbyd. Hoe kijken de redactieleden naar CSS? Is dit de heilige graal om terrorisme, zware criminaliteit en plaatjes van kindermisbruik voor eens en voor altijd de nekslag toe te dienen? Of een privacy-nachtmerrie die ervoor zorgt dat niemand meer onbezorgd een babyfoto maakt met zijn telefoon?



Daar waar we de Facebooks van onze wereld inmiddels volop aan het verketteren zijn om hun verwerpelijke volgsystemen die gebruikt worden om geld te verdienen, viert het controleren van de samenleving voor opsporingsdoeleinden hoogtijdagen. Heel begrijpelijk. De halve wereld leeft inmiddels in zijn devices. En toegang tot dat gedrag biedt bijna ongelimiteerde mogelijkheden. De toegang tot die data is er momenteel wel. Maar vorderen of hacken is omslachtig, kostbaar en daardoor vooral nuttig om in te zetten bij personen die je al op de radar hebt. Daarmee mis je dus een enorme groep aan potentiële criminelen en terroristen die je via CSS eenvoudig inzichtelijk kunt maken. En laten we eerlijk zijn: wie wil kindermisbruik nu niet de wereld uit helpen? Tegen dat doel valt toch weinig in te brengen? Helaas grossieren we met elkaar ook in de voorbeelden waar een nobele toepassing die voor 'doel één' de wetgever passeert, in de loop der tijd wordt ingezet voor doeleinden waar initieel nooit draagvlak voor zou zijn geweest. Onze redactieleden reflecteren op het surveillancemechanisme dat al zoveel tongen heeft losgemaakt.

Maarten Hartsuijker

Als informatiebeveiliger wil je natuurlijk altijd tot in de puntjes weten hoe je gegevens worden verwerkt en wat je kunt doen om te borgen dat ze niet weglekken. Vanuit die verantwoordelijkheid is Client Side Scanning (CSS) een ongrijpbare zwarte doos. Eentje die wellicht begint als een heel klein doosje met een heel specifiek doel, maar die voor je het weet is uitgegroeid tot het 'manusje van alles' op de endpoints. Je hebt hierbij geen idee of dit 'manusje' besluit om jouw bedrijfsgeheimen door te sturen, of besluit ze ongemoeid te laten. En zowel dat besluit als de ontvanger van deze data kan daarbij ook nog eens afhankelijk zijn van het land waar een medewerker zich bevindt of geregistreerd heeft. Een bedreiging als deze verwacht je op sommige plekken op de wereld (en is vaak een reden om aan zakelijke devices reisvoorwaarden te koppelen), maar toch niet in Europa?

Zo nu en dan hoor ik in de discussie over client Side Scanning (CSS) iemand de opmerking maken dat de digitale wereld net als de fysieke samenleving niet wetteloos mag zijn. Ook weer niets tegenin te brengen. Maar deze valse tegenstelling suggereert ook dat CSS noodzakelijk is om een digitaal handhavingsgat op te vullen dat er in-real-life niet is. En dat is natuurlijk niet het geval, want in onze fysieke wereld kunnen we (gelukkig) op heel veel plekken onbespied onszelf zijn.

Laten we het eens omkeren en ervan uitgaan dat alle apparaten over een decennium onder 24x7 controle staan en dat kindermisbruik verhuisd is naar de achterkamertjes. Hoe zouden we het vinden als aannemers na oplevering van ons huis de sleutel zouden houden. Gewoon 'om af en toe even een handhaver binnen te laten om in de achterkamer te kijken of er niets geks gebeurt'? Of (veel efficiënter): dat aannemers je huis bij oplevering van camera's zouden voorzien met de opmerking: ze filmen alleen alles hoor. De beelden van wat je thuis doet gaan nergens heen. Tenzij je iets doet waarvan we denken dat het niet in de haak is natuurlijk, maar dat is bij jullie toch niet het geval!?

Ik zie aan deze maatregel dan ook vooral risico's kleven. Terwijl ik vermoed dat het digitale gedrag waar we terecht iets tegen willen doen heel eenvoudig een laagje dieper ondergronds kan en zal gaan.

Fook Hwa Tan - Het algemeen belang boven het individueel belang: de complexiteit van Client Side Scanning

In een tijd waarin technologie en privacy steeds meer met elkaar in conflict lijken te komen, is het cruciaal om een grondige afweging te maken tussen het algemeen belang en het individueel belang. Het recente debat rondom Client Side Scanning (CSS), zoals geïnitieerd door Apple, legt deze uitdaging bloot. Terwijl voorstanders beweren dat CSS een krachtig wapen kan zijn tegen terrorisme, zware criminaliteit en kindermisbruik, waarschuwen critici voor de potentieel verwoestende impact op onze privacy en de mogelijkheid tot misbruik door overheden en andere instanties.

Het is belangrijk om te erkennen dat de motivatie achter CSS nobel is. Het opsporen en bestrijden van kinderporno en ernstige criminele activiteiten is een doel dat niemand kan betwisten. Echter, het invoeren van dergelijke technologieën vereist een diepgaande overweging van de risico's en gevolgen voor onze samenleving.

Het belangrijkste argument voor CSS is de potentiële effectiviteit ervan bij het bestrijden van ernstige misdaden. Het systeem zou automatisch verdachte inhoud kunnen detecteren zonder dat deze informatie ooit de cloud of servers van een bedrijf verlaat. Dit zou een belangrijke stap kunnen zijn in de strijd tegen kindermisbruik en terrorisme. Het is echter van cruciaal belang om ervoor te zorgen dat deze technologie met de hoogste mate van nauwkeurigheid werkt en dat er strikte waarborgen zijn om valse positieven te voorkomen.

Aan de andere kant van het spectrum zijn de zorgen over privacy en mogelijke misbruiken van CSS. Het is begrijpelijk dat mensen bezorgd zijn over het feit dat hun gegevens en persoonlijke communicatie kan worden gescand, zelfs als het doel nobel lijkt te zijn. Het creëren van een technologische infrastructuur die potentieel kan worden misbruikt om privéberichten af te tappen of bedrijfsgeheimen te stelen, is een zorgwekkend vooruitzicht.

Daarom is het van essentieel belang dat er strikte en onafhankelijke controlemechanismen worden ingevoerd om misbruik van CSS te voorkomen. Deze controles moeten gebaseerd zijn op transparantie, verantwoording en naleving van strenge juridische normen. Bovendien moet de implementatie van CSS onderworpen zijn aan voortdurende beoordeling en evaluatie om ervoor te zorgen dat het systeem niet afdwaalt van het oorspronkelijke doel.

Het algemeen belang moet altijd worden afgewogen tegen het individueel belang, maar het mag niet ten koste gaan van onze fundamentele rechten en vrijheden. We moeten voorkomen dat we in een samenleving terechtkomen waarin privacy volledig ondergeschikt wordt aan veiligheid. Een balans moet worden gevonden, en deze balans vereist voortdurende discussie en reflectie, niet alleen door bedrijven als Apple, maar ook door overheden, experts en de samenleving als geheel.

Uiteindelijk moeten we ervoor zorgen dat CSS niet wordt gebruikt als een middel om onze privacy te ondermijnen of om inbreuk te maken op onze fundamentele rechten. De weg naar een veiligere samenleving mag niet leiden tot een surveillancestaat waarin niemand meer vertrouwelijk kan communiceren. We moeten zorgvuldig navigeren in dit complexe landschap en blijven streven naar een evenwicht tussen het algemeen belang en het individueel belang, terwijl we onze waarden en vrijheden hoog in het vaandel houden.

Leo van Koppen - CSS-wetgeving een opmaat naar Chinese surveillance?

Client Side Scanning lijkt een nobel initiatief van Apple. De mooie doelstelling ervan onderschrijven we allemaal. Het bestrijden van kindermisbruik verdient de hoogste prioriteit, maar met CSS geraken we toch wel in een heel lastig dilemma: kindermisbruik oftewel criminaliteit bestrijden ten koste van de privacy van de burger. Dat dilemma aanpakken vereist een grondige analyse en een beschouwing vanuit veel invalshoeken. In mijn reactie wil ik, in de wetenschap dat

Ik ben van mening dat CSS, zoals nu in Europees verband wordt voorgesteld een enorme inbreuk is op de privacy van de burger

ik niet volledig ben, op een aantal ervan reflecteren.
Op dit moment van schrijven ligt het voorstel in Brussel en op het moment van verschijnen van dit artikel zal duidelijk geworden zijn hoe de wetgeving eruit zal gaan zien. In het voorstel dat nu voorligt ter bestrijding van kinderporno wordt gesproken over drie vormen van scannen: 1. Scannen op bestaande afbeeldingen d.m.v. hashes, 2. Scannen van nieuwe afbeeldingen en 3. Scannen van grooming , beiden via AI. Deze technieken zijn overigens afwijkend van de technieken die Apple wil toepassen. Europa wil dus een eigen implementatie van CSS gaan doen.

Is de methodiek wel waterdicht? Is de gebruikte methode zodanig betrouwbaar dat er geen of tenminste een heel laag percentage false positives ontstaat? De gevolgen van false positives zouden kunnen leiden tot het aanklagen en wellicht ook (publiekelijk) veroordelen van onschuldige mensen. Dat kan een enorme impact hebben. In het verlengde van false positives moet je ook kijken naar de false negatives. Wat als de crimineel een werkwijze vindt om het systeem te ontduiken wat me overigens in het geheel niet ondenkbaar voorkomt.

Kan de stroom aan meldingen goed afgehandeld worden? Een dergelijk systeem genereert een enorme hoeveelheid meldingen, deze komen dan op een locatie (een speciale afdeling van Interpol) binnen. Is men a. in staat om deze stroom te verwerken, zijn er voldoende mensen beschikbaar die dit werk kunnen en willen uitvoeren, en b. is het bekijken van dit soort beelden werk dat een persoon kan volhouden? We kennen inmiddels de verhalen van de mensen die dit voor Facebook en het voormalig Twitter hebben verricht.
Wat kan een mogelijk gevolg zijn? Stel dat de CSS zal worden ingevoerd, hoe eenvoudig is het dan om het systeem te gebruiken voor een ander goed doel, bijvoorbeeld belastingfraude opsporen of Covid-ontkenners te volgen e.a. Het is een kleine moeite om naast de database met bekende kinderporno een tweede of derde toe te voegen voor het scannen en opsporen van andersoortige criminaliteit of ongewenst gedrag. De techniek maakt het mogelijk, dus waarom zouden we het (in tijd van nood) niet gebruiken?

Proportionaliteit? Staat een dergelijke maatregel, die zo'n inbreuk heeft op de privacy, wel in verhouding tot de opsporing van de criminelen en het uitbannen van kinderporno? De groep mensen die een privacy inbreuk ervaren is vele en vele malen groter dan de groep criminelen die er mee kan worden opgespoord.

Ik ben van mening dat CSS, zoals nu in Europees verband wordt voorgesteld een enorme inbreuk is op de privacy van de burger, dat het een opmaat kan zijn naar surveillance praktijken zoals we die van China kennen en dat het resultaat is dat we een ambtelijk monster gecreëerd hebben waarmee we meer leed bij burgers veroorzaken en heel weinig criminelen zullen vangen omdat zij andere wegen en middelen zullen vinden om deze maatregel te ontwijken.

Conclusie, NIET DOEN!

Chris de Vries - Neem de 'Big Tech' hun macht af!

Client Side Scanning roept bij onze redacteuren veel op, getuige de omvang van hun reacties dat het gebruikelijke woordenaantal overschrijdt. Daarbij gaan ze allen in op de onwenselijke neveneffecten, die het nastreven van de goede (nobele) doelen onoverkomelijk lijken te volgen. Tussen de regels door lees je: 'de weg naar hel is geplaveid met goede bedoelingen'. Godfried Bomans schreef eens dat veel futurologen of schrijvers van toekomstromans meestentijds pessimisten zijn. Dat, omdat zij de flexibiliteit en veerkracht van de mens onderschatten. Zijn onze redacteuren dan ook pessimisten? Neen! Het bespreekbaar maken van reële (be)dreigingen is de taak van elk kritisch levend mens, die werkelijk deel uitmaakt van de samenleving waarin hij leeft, woont en werkt. En het woord 'werken' hier bewust op de laatste plaats. Zij geven hierbij adem aan de gedachte dat een rationeel goed verdedigbaar besluit, terdege op sociale gronden zou moeten kunnen worden afgewezen.

'...He was walking down the white-tiled corridor, with the feeling of walking in sunlight, and an armed guard at his back. The long hoped-for bullet was entering his brain. … He had won the victory over himself. He loved Big Brother'

Benieuwd

De redactie van IB-Magazine is benieuwd naar jullie reacties en mening. Tag ook collega's en vakgenoten en nodig ook hen uit te reageren.

Dat daarbij de mening van de gewone mens zwaarder weegt dan die van politici, ambtenaren, die mogelijk (!?) dienstbaar zijn aan de (industriële/economische) oligarchen. Uit de Griekse taal: oligos (weinig of klein) en archein (heersen, regeren) en neen, oligarchen komen niet alleen in Rusland voor.

Ik verwijs graag naar dit nummer van IB-Magazine waarin het interview met Winn Schwartau, de spreker van de bijeenkomst van PvIB in mei van dit jaar. Winn is een specialist op het terrein van Cybersecurity & Cyberwar.

Eén van zijn belangrijkste waarschuwingen luidde dat het doel van Big Tech bedrijven is: winst behalen door vorming van een wereld (`terraforming') waar er geen oog is voor privacy en waarbij de menselijke conditie bepaald wordt door het vertellen van verhalen; die de werkelijkheid verdraaien (`reality distortion'), zaken veranderen en dat met het oog op gedragsmodificatie door inbezitname van de menselijke geest (`absorption of minds'). Zijn actie suggestie: **neem de 'Big Tech' hun macht af!**

Ik ben het dus met mijn collega's eens dat Client Side Scanning een groot gevaar vertegenwoordigt, maar dat niet alleen vanwege het misbruik van techniek, maar ook de inherente overgave van privacy (lees: de meest persoonlijke data) aan Big Tech bedrijven, die het voor de levensstandaard van hun eigenaren misbruiken om de mens ongemerkt te manipuleren op een nog nooit geziene schaal. Diezelfde mens ook nog eens in extase denkend: *'...He was walking down the white-tiled corridor, with the feeling of walking in sunlight, and an armed guard at his back. The long hoped-for bullet was entering his brain. … He had won the victory over himself. He loved Big Brother.'* George Orwell, 1984. Ik wens innig dat dit doembeeld niet de werkelijkheid zal zijn voor onze (achter)kleinkinderen!

NB.: Ik heb de gebruikelijke limiet ook overschreden.