Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Kies een berichtenapp voor uw organisatie

Openbare apps worden gebruikt voor interne communicatie

Factsheet FS-2017-03 | versie 1.1 | 31 augustus 2017

Veel zakelijke communicatie verloopt via berichtenapps[1]. Het zakelijk gebruik van openbare berichtenapps brengt risico's met zich mee. Dit heeft consequenties voor de organisatie en het delen van informatie. De beveiliging van de gebruikte berichtenapps voldoet vaak niet aan het beveiligingsbeleid voor interne communicatie.

Het NCSC adviseert te onderzoeken welke berichtenapp het geschiktst is voor uw organisatie. Maak daarna een risicoafweging die de beveiligings- en gebruikerseisen in acht neemt. Tref eventueel aanvullende maatregelen.

[1] Een berichtenapp is een online communicatiedienst voor de smartphone, bijvoorbeeld WhatsApp, Signal en Telegram. Via een app wisselt men informatie uit. Deze factsheet gaat niet in op instant messaging (IM) zoals Slack en Extensible Messaging and Presence Protocol (XMPP).

Achtergrond

Het gebruik van berichtenapps, zoals het delen van vertrouwelijke zakelijke informatie, brengt risico's met zich mee. Deze factsheet beschrijft de belangrijkste risico's bij het gebruik van berichtenapps. De factsheet heeft als doel om informatiebeveiligers een risicoafweging te laten maken welke berichtenapp het meest geschikt is voor de organisatie. Het NCSC beveelt organisaties aan om gedegen onderzoek te doen naar een veilige berichtenapp die voldoet aan het interne beveiligingsbeleid. Het NCSC doet geen onderzoek naar de beveiliging van berichtenapps.

Doelgroep

Informatiebeveiligers van middelgrote tot grote organisaties.

Aan deze factsheet hebben bijgedragen:

De Belastingdienst , NRG (Nuclear Research & Consultancy Group) en Rabobank.

Wat is er aan de hand?

Berichtenapps zijn vaker het platform om snel met elkaar te communiceren.

Berichtenapps worden steeds vaker gebruikt als communicatiemiddel. Een van de redenen is dat berichtenapps gebruiksvriendelijk en binnen handbereik zijn. Dit gebruiksgemak leidt tot efficiënter samenwerken en contact onderhouden met collega's en klanten. Veel berichtenapps zijn beschikbaar voor meerdere besturingssystemen. Zij zijn vaak op de smartphone en soms via de laptop benaderbaar. In veel gevallen zijn berichtenapps gratis en gemakkelijk te installeren. Bovendien is de betreffende berichtenapp algemeen bekend en gebruiken veel collega's en klanten dezelfde app. Deze apps staan in tegenstelling tot de vaak beperkte functionaliteiten van door de organisatie geboden middelen.

Het gebruik van berichtenapps kent risico's.

Diverse risico's spelen bij het gebruik van berichtenapps. De voornaamste is dat data op andere locaties terecht komen dan van te voren beoogd. De verkeerde persoon ontvangt, per abuis, vertrouwelijke gegevens. Er kan dan sprake zijn van een datalek. Daarnaast kan het telefoonnummer niet meer in bezit zijn van de persoon waar de informatie wel voor bedoeld was.

Organisaties en medewerkers staan niet altijd stil bij de risico's van berichtenapps.

Communiceren via berichtenapps voor zakelijke doeleinden brengt risico's met zich mee. Het is aan de organisatie om een situatie te creëren waarin medewerkers bewust gebruik maken van een berichtenapp die zoveel mogelijk voldoet aan het interne beveiligingsbeleid. De risico's voor de organisatie hebben betrekking op de locatie van de data, wie toegang heeft en welke partijen de data kunnen opvragen. Data komen, bijvoorbeeld door het koppelen van databases na een fusie of overname, bij andere partijen of op een andere locatie terecht. Data vallen mogelijk onder een andere jurisdictie als data buiten de landgrenzen zijn opgeslagen.

Wat kan er gebeuren?

Voor de organisatie is het van belang om in kaart te brengen in hoeverre bovenstaande risico's van toepassing zijn op de organisatie. De risicoafweging is mede afhankelijk van het volwassenheidsniveau van de organisatie en de impact die het risico kan vormen. Indien sprake is van Mobile Device Management (MDM) spelen sommige risico's wellicht geen of een minder belangrijke rol. Bij MDM kan de organisatie een app in een container plaatsen en zelf beheren. Bepaal aan de hand van onderstaande risico's of en in welke mate deze gelden voor de organisatie.

Het integraal uploaden van contactlijsten naar servers van een app-ontwikkelaar.

Gedurende de installatie van de berichtenapp kan een pop-up verschijnen of deze app toegang mag verkrijgen tot het telefoonboek. In sommige gevallen kan dit gunstig zijn, omdat de app meteen alle contacten overneemt en de gebruiker gemakkelijk een chat kan starten. De telefoonnummers van de contacten uit het telefoongeheugen zijn in dat geval wel geüpload naar de servers van de app-ontwikkelaar. Dan zijn telefoonnummers uit de smartphone ook elders opgeslagen. De vraag is in hoeverre dit een risico vormt voor de organisatie. Indien in het telefoonboek personen staan met een gevoelige functie of geheim nummer, is dit wellicht een risico. Bovendien zijn dan telefoonnummers van collega's of klanten gedeeld met een derde partij. Die personen weten zelf niet dat derden in het bezit zijn gekomen van hun gegevens. Denk hierbij aan wet- en regelgeving zoals privacybeleid, overeenkomsten en geheimhoudingsverklaringen die de organisatie ondertekend heeft met partners. Deze overeenkomsten kunnen bijvoorbeeld vereisen om klantgegevens niet aan derden te verstrekken.

Gedrags- en gebruikersdata staan elders opgeslagen en zijn opvraagbaar voor derden.

Bij het versturen van berichten in een berichtenapp worden op de achtergrond vaak gedrags- en gebruiksgegevens meegezonden. Uit deze gegevens is te herleiden wie contact heeft gehad met wie, op welk tijdstip, waar en hoe vaak. Ook de status en de profielfoto kunnen onderdeel uitmaken van deze gegevens.[2] Daarnaast kunnen deze gegevens op servers buiten Nederland opgeslagen zijn, waardoor een andere jurisdictie van toepassing is. Derden hebben dan de mogelijkheid om ongevraagd de data te delen of in te zien. Buitenlandse inlichtingendiensten kunnen deze gegevens opvragen, omdat deze opgeslagen staan op servers die binnen hun jurisdictie vallen.

Andere partijen inzage hebben in de inhoud van de communicatie.

Als encryptie onvoldoende is toegepast op het netwerkverkeer dan kunnen partijen het netwerkverkeer onderscheppen en de inhoud van berichten meelezen. De actoren buitenlandse inlichtingendiensten en criminele organisaties beschikken over de motivatie en middelen om netwerkverkeer te onderscheppen.

Vertrouwelijke gegevens kunnen terechtkomen op servers buiten het netwerkbeheer van de organisatie.

Op het moment dat de berichtenapp is geïnstalleerd, kan data al verzonden zijn naar een externe server. Daarnaast verschilt per berichtenapp of en hoe lang berichten op de server staan.

[2] Zie verder https://veiliginternetten.nl/themes/draadloos-internet/situatie/berichtendiensten/mijn-locatie-zichtbaar-whatsapp/.

De server kan overal ter wereld staan. De organisatie heeft niet het beheer over deze server en ook geen zicht op de data die naar de server zijn verzonden. Uw organisatie is afhankelijk van de beveiliging van een derde partij waar geen overeenkomst mee gesloten is.

Juridische en organisatorische risico's

Organisaties dienen vertrouwelijk om te gaan met (persoons)gegevens en voldoende passende organisatorische en technische maatregelen te hebben getroffen om data te beschermen. Vertrouwelijke data die buiten de organisatie terecht komen, kunnen leiden tot reputatie- en imagoschade. Verlies van vertrouwen in de organisatie of het product en boetes zorgen voor financiële schade. In sommige gevallen kunnen boetes bij datalekken worden opgelegd. Houd rekening met juridische vereisten die gelden voor het openbaar maken van schriftelijke communicatie en het vastleggen van verkeersgegevens of inhoud van communicatie in uw sector. Dergelijke vastleggingen kunnen nodig zijn vanwege interne (kwaliteits)reviews of toezichthouders die inzicht willen verkrijgen in verkeersgegevens.

Wat adviseert het NCSC?

Maak een risicoafweging of een berichtenapp gewenst is en past bij de organisatie.

Elke organisatie is anders. Daarmee verschilt ook het niveau van risicoacceptatie. Het ene bedrijf heeft geen kader en staat het gebruik van alle berichtenapps toe. Een andere organisatie vraagt zich af welke berichtenapp het veiligst is om te gebruiken. Een derde organisatie ontwikkelt, beheert en distribueert intern een eigen berichtenapp. De mate van volwassenheid van de organisatie bepaalt in hoeverre de genoemde risico's acceptabel en van toepassing zijn voor de organisatie. Daarnaast is het per organisatie verschillend of en hoe MDM is ingericht. De genoemde risico's geven handvatten om berichtenapps te (laten) onderzoeken[3] [4] en de resultaten naast het huidige beveiligingsbeleid te leggen. Deel de resultaten met samenwerkingspartners en houd rekening met de hoge omloopsnelheid van diverse berichtenapps en de aangeboden functionaliteiten. Het gezamenlijk (laten) onderzoeken van berichtenapps geeft inzage in de risico's. Een gedegen onderzoek geeft antwoord op welke berichtenapp het geschiktst is voor de organisatie, of dat het ontwikkelen en zelf beheren van een app het enige alternatief is. Kies voor de berichtenapp die zoveel mogelijk voorziet in de beveiligingseisen zoals vermeld in het beveiligingsbeleid voor interne communicatie en andere interne richtlijnen.

[3] Zie voor een overzicht van apps en hun beveiliging: https://www.eff.org/node/82654 (laatst geupdate in april 2016).
[4] https://toolbox.bof.nl/adviezen/whatsapp-alternatief/ (gepubliceerd in april 2015).

Evalueer het interne beveiligingsbeleid op het gebruik van berichtenapps.

Onderzoek of het interne beveiligingsbeleid voldoende van toepassing is op het gebruik van berichtenapps. Bekijk het huidige beleid en beoordeel kritisch of dit toepasbaar is voor berichtenapps als interne communicatie. Vul het beleid aan met specifieke eisen voor het gebruik van berichtenapps indien het huidige beleid onvoldoende ingaat op de risico's bij het gebruik van berichtenapps in de organisatie.

Onderzoek welke berichtenapp voldoet aan het beveiligingsbeleid voor een acceptabel restrisico.

Het interne beveiligingsbeleid is leidend voor het gebruik en de keuze van een berichtenapp. Onderzoek per berichtenapp wat de gebruikersvoorwaarden, beveiligingsmaatregelen en functionaliteiten zijn. Beoordeel of deze factoren in voldoende mate overeenkomen met het interne beleid. Als dit onvoldoende is, breng in kaart wat de afwijkingen zijn en neem aanvullende maatregelen. Kies een berichtenapp die zoveel mogelijk voldoet aan de bestaande beleidsnormen, zodat het restrisico laag is en de aanvullende maatregelen tot een minimum beperkt blijven.

Tref eventuele aanvullende maatregelen.

Nadat het beveiligingsbeleid is gecontroleerd, geëvalueerd en onderzoek is gedaan naar een berichtenapp, is de huidige set maatregelen van belang. De reeds geïmplementeerde technische en organisatorische maatregelen dienen de risico's voldoende af te dekken. Indien de genomen maatregelen niet afdoende zijn, neem dan compenserende maatregelen om de restrisico's te beheersen. Het is hierbij ook relevant hoe de organisatie gebruik maakt van MDM. [5]

Aanvullende beveiligingsmaatregelen voor berichtenapps zijn:

- Installeer alleen berichtenapps vanuit een erkende appstore.
- Zoek naar een berichtenapp die niet de contactgegevens/het telefoonboek uploadt naar de server.
- Creëer een intern of besloten adresboek/contactlijst van de organisatie om te gebruiken in de app.
- Kies een app die voorziet in het vaststellen van de authenticiteit van het communicatiekanaal (bijvoorbeeld scannen van QR-code ter verificatie).
- Stel een toegangbeperkende maatregel (bijv. pincode) in voor het gebruik van de berichtenapp.
- Gebruik alleen berichtenapps waarbij end-to-end encryptie ingeschakeld is.
- Kies een berichtenapp die encryptie gebruikt op basis van opensource technieken, welke controleerbaar is en onderdeel uitmaakt van een beveiligingsaudit.

[5] Zie https://www.ncsc.nl/actueel/factsheets/factsheet-velig-gebruik-van-smartphones-en-tablets.html.

- Kijk of de opslaglocatie afgeschermd is op de smartphone, waarbij de data (foto's, sleutelmateriaal, berichten) versleuteld zijn opgeslagen.
- Kies voor zelf verwijderende berichten.
- Kies een berichtenapp die data nooit opslaan of direct verwijderen van de server zodra het bericht is afgeleverd.
- Pas autorisatiebeheer toe op chatgroepen.

Blokkeren is beheersintensief en ineffectief

Het weren van berichtenapps op smartphones is geen adequate maatregel. Er verschijnen dagelijks nieuwe berichtenapps en het blokkeren van (onveilige) berichtenapps vergt veel capaciteit. Het bieden van een goed onderzochte berichtenapp heeft dan meer effect dan het proberen te blokkeren van alle berichtenapps.

Schenk aandacht aan de distributie van de app.

Het is van belang om het implementeren van de gewenste berichtenapp met voldoende aandacht te doen, zodat het medewerkers aanmoedigt de berichtenapp te gaan gebruiken. Maak het gemakkelijk om de gekozen berichtenapp uit te rollen binnen de organisatie. Bied bijvoorbeeld de berichtenapp gratis aan met eventueel een gebruiksinstructie of push deze naar de smartphones van medewerkers. Daarbij kunt u de app reeds instellen met de juiste veiligheidsinstellingen zodat veilig gebruik meteen van toepassing is.

Handelingsperspectief

- Maak een risicoafweging of een berichtenapp het juiste communicatiemiddel is voor de organisatie.
- Controleer het huidige beveiligingsbeleid en evalueer of deze toepasbaar is op het gebruik van berichtenapps en vul aan waar nodig.
- Verricht onderzoek naar berichtenapps die zo veel mogelijk voldoen aan het interne beveilingsbeleid.
- Voer een risico- en maatregelenanalyse uit bij het gebruik van een berichtenapp.
- Breng in kaart wat de risicovolle scenario's zijn voor de organisatie.
- Identificeer welke maatregelen zijn geïmplementeerd in de gekozen berichtenapp.
- Beoordeel de effectiviteit van deze maatregelen.
- Beschrijf de ontbrekende en/of falende maatregelen.
- Maak inzichtelijk welke restrisico's bestaan.
- Accepteer de restrisico's of neem aanvullende maatregelen om de restrisico's te mitigeren.

Tot slot

De organisatie is verantwoordelijk om risico's, die optreden bij het gebruik van berichtenapps in de zakelijke communicatie, te beheersen. Het aantal berichtenapps stijgt en het gebruik blijft toenemen. Het is van belang om de risico's rondom het gebruik van berichtenapps binnen uw organisatie in kaart te hebben gebracht. Neem organisatorische en technische maatregelen die verband houden met het interne beleid. Medewerkers gaan bewuster berichtenapps gebruiken als zij op de hoogte zijn van de risico's. Het voorkomen van privacyschending, datalekken of bedrijfsspionage vanwege een berichtenapp in uw organisatie is van groot belang.

Kies bewust voor het gebruik van een berichtenapp!

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-03 | versie 1.1 | 31 augustus 2017