

Vijf essentiële lessen voor retailers met een wifihotspot

04-07-2017 12:26



Door Ryan Orsi

Director of product management bij [WatchGuard Technologies](#)

Wifi is anno 2017 de normaalste zaak van de wereld. Vrijwel iedereen draagt altijd minimaal één device met wifiverbinding bij zich. Volgens een onderzoek van Cisco zijn er in 2021 wereldwijd meer dan [540 miljoen publieke hotspots](#). De meeste retailers beseffen dan ook dat een draadloze hotspot tot de basisvoorzieningen van hun fysieke winkel behoort.

Het lijkt eenvoudig. Je plaatst een router, stelt een publiek netwerk beschikbaar en communiceert eventueel het wachtwoord op een duidelijke plek. Set and forget. Toch loop je als retailer op deze manier kansen mis. Een hotspot is namelijk in potentie zoveel meer dan slechts een toegangspoort tot het internet. En niet onbelangrijk: je stelt klanten bloot aan onnodige veiligheidsrisico's. Dit zijn de 'lessons learned' waarmee iedere retailer die zijn klanten gratis internet wil aanbieden zijn voordeel kan doen:

1. Gebruik een 'splash page' of captive portal, binnen de lijnen van de privacywetgeving

Veel organisaties gebruiken als portal voor hun hotspot een lijstje met algemene voorwaarden die gebruikers moeten accepteren. Dat is een gemiste kans. Dat verschaft weliswaar je klanten snel toegang tot gratis internet, maar je laat ook veel potentiële klantinformatie liggen.

Met aanpasbare portals en splash pages kun je waardevolle data verzamelen. Denk aan telefoonnummers en

profielen van sociale netwerken. Let hierbij wel op: de nieuwe Europese privacywetgeving die mei 2018 van kracht gaat (GDPR) legt strikte beperkingen op aan het verwerken van persoonsgegevens. Een telefoonnummer mag je bijvoorbeeld niet 'zomaar' opslaan en verwerken, het moet noodzakelijk zijn voor de dienstverlening die je aanbiedt.

Daarbij geldt de reden dat opgevraagde gegevens in de toekomst 'mogelijk waardevol' kunnen zijn voor marketing, niet als duidelijk vastomlijnd doel. Concretiseer het doel voor jezelf en gebruik het ook daarvoor. Denk bijvoorbeeld aan het gebruik van een telefoonnummer voor het sturen van een sms met een persoonlijke aanbieding. Communiceer bovendien dat doel helder met je klant en gebruik de persoonsgegevens nergens anders voor.

2. Bescherm je klanten tegen hackers

Openbare hotspots zijn aantrekkelijke jachtvelden voor wifihackers. Zonder fatsoenlijke securityvoorzieningen kunnen kwaadwillenden eenvoudig persoonlijke informatie van klanten onderscheppen. Denk aan creditcardgegevens, e-mail of wachtwoorden. Toch is draadloze security niet enkel een kwestie van het beschermen van je klanten. Goede voorzieningen beschermen ook je reputatie als retailer.

Hoe werkt wifisecurity precies? Een bekende methode is WIPS, ofwel Wireless Intrusion Prevention System. Deze oplossing beschermt draadloze netwerken tegen af luisterpraktijken. Het probleem: de meeste van die oplossingen zijn duur, en bovendien merken veel WIPS'en de hotspot van de burens al snel ontorecht aan als een vijandig toegangspunt, opgezet om jouw klanten te lokken en te misleiden. Als zo'n systeem een naburig netwerk ook nog ten onrechte blokkeert (een 'false positive'), kunnen daar vervelende, soms zelfs juridische consequenties aan [vastzitten](#).

Het goede nieuws is dat enterprise-grade wifibeveiliging niet meer enkel is voorbehouden aan de grootste bedrijven. Er bestaat nieuwe technologie die zo goed als alle 'false positives' voorkomt. Deze techniek kan devices en access points classificeren als 'betrouwbaar', 'naburig' of 'kwaadaardig' en daarop de maatregelen aanpassen.

Vervolgens is het belangrijk de compliance met de beveiligingsstandaard van de Payment Card Industry (PCI) te respecteren, zelfs al worden de vereisten ieder jaar strenger. Een onbeveiligd draadloos netwerk is nu eenmaal niet geschikt om betaalkaartgegevens over te versturen. Toch is compliance alleen niet genoeg om de veiligheid van je gasten te waarborgen. Zo is een van de voorschriften dat je ieder kwartaal de buurt verkent op kwaadaardige access points. Dat is natuurlijk veel te weinig. PCI-compliance is belangrijk, maar vul deze altijd aan met 24/7 WIPS-bescherming.

3. Bescherm je sales tegen e-commercereuzen

Het komt vast bekend voor: je klanten gebruiken je winkel als showroom en gaan vervolgens via jouw wifiverbinding op zoek naar de aanbieder die de laagste prijs vraagt. Gelukkig kun je veel engagementtechnieken gebruiken zodra klanten eenmaal bij je zijn aangemeld op het netwerk. Denk bijvoorbeeld aan een URL-interceptietool. Hiermee kun je bezoekers die prijzen vergelijken met die van andere aanbieders automatisch benaderen met bijvoorbeeld kortingscodes of op maat gesneden boodschappen. Ook hier geldt net als bij het verzamelen van persoonsgegevens dat je expliciet toestemming nodig hebt van de klant om zijn of haar surfgedrag te volgen.

Je kunt je wifinetwerk ook gebruiken als kanaal voor directe communicatie met de klant, bijvoorbeeld via sms of social media. Via het wifinetwerk verstuurd onderzoek en polls kun je je business- en marketingtactieken aanscherpen en tegelijkertijd laten merken dat je om de mening van je klant geeft.

4. Gebruik de wifistatistieken

Maar weinig retailers onderzoeken de statistieken van hun hotspot, terwijl daar een schat aan businessinformatie in verborgen ligt. Het is feitelijk de tegenhanger van je webanalytics, mocht je een website hebben uiteraard. Informatie over hoe lang klanten je winkel bezoeken, wat ze kopen, welke afdelingen ze wel of juist bezoeken: het zijn allemaal cruciale data voor het nemen van directe en langetermijnbeslissingen. Denk aan de optimalisatie van je winkellayout.

Ook hier heb je weer expliciete toestemming nodig van je klant. De privacywetgeving verbiedt het nadrukkelijk om klanten zonder toestemming en gerechtvaardigd doel op deze manier te volgen. De Autoriteit Persoonsgegevens [waarschuwde](#) retailers vorig jaar via een brief nog voor de consequenties en wees hen op de voorwaarden.

5. Schenk aandacht aan internetveiligheid voor kinderen

Natuurlijk is cybersecurity een belangrijk aspect, maar vergeet ook de veiligheid van kinderen niet. Bezoekers van alle leeftijden zouden probleemloos gebruik moeten kunnen maken van je hotspot. Dat betekent dat er geen ruimte is voor aanstootgevende en ongepaste content als geweld, porno of andere zaken die niet geschikt zijn voor kinderen.

Wat dit betreft kunnen we een voorbeeld nemen aan het Verenigd Koninkrijk. Zij hebben de organisatie [Friendly WiFi](#) in het leven geroepen, een instantie die gelegenheden keurt op veilig en gefilterd wifi. Je herkent winkels en horecazaken die dit aanbieden aan een goed zichtbaar Friendly WiFi-embleem.

Wifi kan een gamechanger voor je business zijn, op zowel een positieve als negatieve manier. Zonder goede securitymaatregelen is het aanbieden van een gastennetwerk vragen om problemen voor jezelf en je klanten. Aan de andere kant is een goed beveiligd en slim opgezet draadloos netwerk een waardevolle booster voor je marketing en sales en de klanttevredenheid.

Ryan Orsi