UN PAS MÉS EN EL SERVEI WIFI: SEGURETAT A LA XARXA DE BIBLIOTEQUES

Lissette Castillo (Bibliotecària)

Grelda Ortiz (Bibliotecària)

1.Introducció

Amb la proliferació dels smartphones i altres dispositius mòbils, les empreses tecnològiques (Apple, Nokia, et al.) han volgut facilitar la tecnologia wireless, connexió a la Xarxa Internet sense fils, coneguda com a wifi. Es així com la Wi-Fi Alliance promou l'ús del protocol estàndard IEEE 802.11 a xarxes inal·làmbriques d'àrea local (Castro, 2005) i que qualsevol dispositiu dins del abast de la senyal es pugui connectar a la Xarxa.

Les xarxes de biblioteques no son alienes a aquesta tecnologia (Serrano-Muñoz, 2011)[1], i moltes ofereixen el Servei de connexió wifi a les seves instal·lacions si els usuaris volen connectar-se a la xarxa Internet. El problema de seguretat ve que internet va ser creada dins del entorn universitari, sense tenir en compte amenaces externes, els pirates informàtics es dediquen des de a robar contrasenyes de xarxes socials fins i tot a robar les dades de les targetes de crèdit. Per tant ens preguntem: com de segur és aquest servei? Per a una empresa, és més senzill, només cal contractar serveis tipus Rogue Mobile App o Cybertrack, i regular o restringir nous aparells que s'afegeixen a les seves xarxes. Però, per les xarxes wifi de les biblioteques, siguin de la tipologia que siguin, no ho és pas. Molts usuaris porten els seus propis aparells: ordinadors portàtils, iPads, smartphones, i tots ells volen poder connectar- se a la xarxa Internet (Wolff, 2015). Si bé es cert que les biblioteques fem un control d'accés (autentificació d'usuaris), la senyal wifi sense encriptar[2] pot ser escoltada[3] per qualsevol cracker dins del abast de la senyal wifi de la mateixa biblioteca; inclús un atacant pot aixecar un punt d'accés amb el mateix nom que el punt d'accés wifi real de la biblioteca, i que enganyi aixi a alguns usuaris perquè es connectin a ell en comptes de connectar-se a la biblioteca. Un cop fet això, es possible atacar els usuaris, permetent que aquest atacant pugui accedir sense autorització a equips connectats a aquesta xarxa. Es clar, la biblioteca tampoc vol que qualsevol persona faci servir els recursos de la mateixa biblioteca per a usos aliens als del servei.

El nostre pòster busca donar a conèixer aquest perill de seguretat tant als gestors d'aquestes wifis

2.Metodologia

[1] Les biblioteques han desenvolupat aplicacions mòbils com ara catàlegs, aplicacions de geolocalització es a dir biblioteques de butxaca- per a dispositius mòbils.

[2] La senyal wifi ofert per la Universitat de Barcelona està sense encriptar, per això recomanen fer servir la wi-fi de Eduroam, que sí està encriptada. <http://bloctic.ub.edu/eduroam-o-wifiub/> . [Data de consulta: 25 de novembre 2015]

[3] Dins de l'argot informatics es coneix com "sniffer" quan els atacants poden escoltar tots els continguts accredits pels usuaris, tot i no poder interactuar amb ells.

Farem servir les estadístiques d'ús de la wifi de les biblioteques de Barcelona dels últims anys per mostrar el creixement d'ús de Internet amb aparells externs a les biblioteques i sobre els quals no es té control.

A més, buscarem a diversos mitjans de comunicació -Diaris i revistes- per extreure casos de mal ús d'aquest servei a les biblioteques.

3.Resultats

3.1. Estadístiques d'ús de Internet via wifi a les biblioteques

Any	2011	2012	2013	2014
Usuaris servei wi-fi en usuaris acumulats (Xarxa de Biblioteques Municipals de la Província de Barcelona)	1.152.783	1.308.439	1.592.258	1.880.849
Usuaris servei wi-fi (Xarxa Biblioteques de Barcelona)	--	--	--	657.126

Hem fet servir aquestes estadístiques per ser públiques[4] i ser la xarxa amb més usuaris integrats.

3.2. Casos reals d'atacs de pirates a les biblioteques

Any	2011	2014	2015
Atacs reals	1	1	1

Hem fet servir el buscador Google per trobar aquests casos[5], utilitzant termes com "library data breach", o "library account hacked".

4.Conclusió

La responsabilitat és de tots, biblioteques i usuaris. Cada vegada son més els usuaris que utilitzen els seus dispositius mòbils per accedir a dades personals i corporatives a través de connexions wi-fi gratuïtes com les que s'ofereixen a les biblioteques. Molts d'aquests dispositius personals no compleixen amb els nivells de seguretat mínims, per la qual cosa es converteixen en punts d'accés

5.Propostes

[4] Memòria 2014 Diputació de Barcelona; i les Estadístiques 2014 de la xarxa de Biblioteques de Barcelona.

[5] Els articles que parlen dels casos relacionats amb atacs a biblioteques en son 3: Programador de 24 anys accedeix al sistema informàtic del Massachusetts Institut of Technology MIT sense autorització. <https://gigaom.com/2011/07/19/aaron-swartz-hacked-mit-library/> ; Spotify - un "repositori musical en línia" va ser atacada al 2014, van haver de demanar als seus usuaris que canviessin les contrasenyes. <http://thehackernews.com/2014/05/spotify-hacked-urges-android-users-to.html> ; i el cas del compte de Facebook de l'American Library Association va ser hackejada el 7 de setembre 2015. <http://americanlibrariesmagazine.org/blogs/the-scoop/alas-facebook-account-was-hacked-and-youll-never-guess-what-happened-next/> . [Data de consulta: 25 de novembre 2015]

Pot ser difícil trobar l'equilibri entre seguretat i accés a Internet dins de les xarxes de biblioteques. I encara més amb tecnologies noves que encara estan canviant. Les biblioteques i els seus usuaris han de seguir unes pautes de seguretat informàtica per tal de minimitzar els accessos no autoritzats als seus recursos:

5.1. Per a les xarxes de biblioteques que ofereixen el servei wifi:

- Facilitar als usuaris de wifi de les biblioteques una guia amb consells per evitar que els pirates obtinguin les seves dades
- Comptar: la xarxa de biblioteques ha de saber quins aparells es connecten i funcionen dins la seva xarxa local
- Aïllar els usuaris entre si, de forma que puguin conectar-se a internet pero no puguin interactuar uns contra els altres, i d'aquesta forma es pot evitar que usuaris maliciosos puguin atacar d'altres usuaris de la mateixa biblioteca
- Monitoritzar – amb el hardware adequat- també l'aparició d'altres punts d'accés amb el mateix nom que el de la biblioteca i alertar als usuaris en cas de detectar-ne algun amb aquestes característiques
- Configurar: donar als usuaris informació -en forma de guia a la pàgina del servei wifi per exemple- de quines son les claus per configurar els seus aparells per tenir un mínim de seguretat quan es connecten a la xarxa Internet via wifi
- Formació d'usuaris: explicar als usuaris de la seva co-responsabilitat en l'ús del servei wifi
- Repetir tot el procés: estar al dia en seguretat informàtica

5.2. Per als usuaris finals del servei wifi:

- Actualitzacions: periòdicament han d'actualitzar totes les apps, software, i sistemes operatius al dispositius
- Evitar accedir a pàgines on us demanin usuari i contrasenya quan la connexió a Internet es via wifi
- Utilitzar contrasenyes segures, i a ser possible, fer servir la doble autentificació.
- Deshabilitar el wi-fi si no s'està utilitzant
- Utilitzar serveis d'encriptació o VPN (Xarxa Privada Virtual)

6.Bibliografía

Castro,Rodrigo."Avanzando en la seguridad de las redes WIFI" [en línia]. *Red Iris Boletín*, nº 73, setembre 2005. <https://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf> . [Data de consulta: 25 de novembre 2015]

Serrano-Muñoz, Jordi; et. al. “Implementació de web mòbil a les biblioteques”. *Item: revista de biblioteconomía i documentació*, 2011 núm 55, p. 121-134.

Wolff, Josephine. “Can Campus Networks ever be secure?” [en línia]. *The Atlantic*, octubre 2015. <http://www.theatlantic.com/technology/archive/2015/10/can-campus-networks-ever-be-secure/409813/> . [Data de consulta: 25 de novembre 2015]