DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 11| Maig 2021

RISCOS PER A LA SEGURETAT EN LA UTILITZACIÓ D'UNA XARXA WIFI PÚBLICA. CONSELLS EN LA SEUA UTILITZACIÓ

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

ÍNDEX

RISCOS PER A LA SEGURETAT EN LA UTILITZACIÓ D'UNA XARXA WIFI PÚBLICA. CONSELLS EN LA SEUA UTILITZACIÓ

Vos convidem a traslladar-nos les temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Les peticions hauran de dirigir-se a:

Diputació de València
Dpt. de Protecció de Dades
i Seguretat de la Informació

Pl. de Manises, 4 – 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONS

Si desitges subscriure't a la nostra publicació accedeix al següent enllaç

INTRODUCCIÓ

Fins fa pocs anys, la idea d'interconnectar dispositius tecnològics estava lligada a la clàssica distribució d'una xarxa d'ordenadors cablejada que ens permetia, d'una banda, tindre accés a un servidor, normalment de dades i per un altre, a Internet. Hui dia, aquesta concepció ha canviat radicalment. L'ús de la tecnologia sense fil s'ha estés de tal manera que ningú concep un sistema en el qual, per a connectar-se, siga necessari fer ús de cables. Ens trobem immersos en una era sense fil en la qual dispositius com a ordinadors personals, telèfons intel·ligents o tauletes i elements IoT poden arribar a estar interconnectats entre si sense necessitat de fer ús del cable, a través d'ones electromagnètiques, incorporant aquesta capacitat de manera nativa, sense necessitat d'afegir-la artificialment. L'aparició de la xarxa sense fil s'entén com una extensió d'una xarxa d'ordinadors interconnectats físicament, per cable, amb un únic objectiu: proporcionar llibertat de moviments evitant haver de situar-se en una ubicació física determinada a l'hora de connectar-se als recursos que puga oferir una organització. Però malgrat els avantatges que puga oferir aquesta funcionalitat, no està exempta de riscos associats al seu ús, que s'hauran d'analitzar i tindre en compte en qualsevol organització a l'hora de configurar polítiques i mesures que els mitiguen o minimitzen i que al seu torn, garantisquen la seguretat de les comunicacions.

Definirem xarxa sense fil, com aquella formada per dispositius capaços d'intercomunicar-se entre si o amb una altra xarxa (com a Internet), sense necessitat d'elements físics que les connecten com poden ser els cables. Tenint en compte que existeixen molts tipus de xarxes sense fils la diferència de les quals radica en aspectes com l'arquitectura, tecnologia o estàndards de comunicació entre altres, en aquesta guia ens centrarem en les més esteses, les Xarxes d'Àrea Local Sense fils, conegudes com WLAN (en anglés, *Wireless* Local Àrea *Networks*) o xarxes wifi.

Com hem evidenciat, el principal avantatge de comptar amb un mecanisme de xarxa sense fil és l'absència de cables i, per tant , l'absència de preocupacions per l'estat, manteniment i organització d'aquests.

No obstant això, un dels principals inconvenients associats a aquesta mena de connectivitat és la naturalesa oberta i accessible d'aquesta, la qual cosa la converteix en una tecnologia més vulnerable que el cable. A més, a causa d'interferències de senyal i altres factors, com, per exemple, els ambientals, podria veure's afectada la velocitat de navegació o fins i tot la pròpia disponibilitat del senyal. En resum, la tecnologia wifi permet donar servei a diversos usuaris que podran connectar-se quan així ho desitgen i en qualsevol lloc on arribe el senyal, mentre que amb el cable només podrà connectar-se aquell que faça ús d'aquest cable en el lloc habilitat.

"…UN DELS PRINCIPALS INCONVENIENTS ASSOCIATS A AQUESTA MENA DE CONNECTIVITAT ÉS LA NATURALESA OBERTA I ACCESSIBLE D'AQUESTA, LA QUAL COSA LA CONVERTEIX EN UNA TECNOLOGIA MÉS VULNERABLE QUE EL CABLE"

RISCOS DE LA XARXA WIFI PUBLICA

Quan ens connectem a una xarxa wifi-pública desconeixem qui és l'administrador o quines mesures de seguretat utilitza per a impedir accions malintencionades d'altres usuaris connectats i, per tant, podem exposar-nos sense necessitat a una sèrie de riscos que descriurem a continuació.

Robatori de dades transmeses:

Si la connexió la realitzem sense contrasenya, la qual cosa coneixem com una xarxa "oberta", les dades que transmetem poden ser llegits per qualsevol, tant l'administrador com altres usuaris que es troben connectats a la xarxa.

La informació està exposada a qualsevol que sàpiga com llegir-la, i per a això no és necessari tindre uns coneixements tècnics molt elevats.

Si el sistema ens demana una contrasenya i apareix un cadenat, com a "xarxa protegida", la informació es transmet de forma xifrada. No obstant això, això està condicionat pel sistema de seguretat utilitzat i la contrasenya triada. De menor a major seguretat, els sistemes són WEP, WPA i WPA2. 

Mai hem de connectar-nos a una xarxa WEP ja que s'ha demostrat que és vulnerable i que la seua seguretat equival a una xarxa oberta (sense contrasenya).

Robatori de dades emmagatzemades en el nostre equip

En formar part d'una xarxa pública en la qual existeixen altres usuaris connectats, el nostre dispositiu està exposat i visible als altres usuaris presents en aquesta.

Per tant, som susceptibles de rebre qualsevol tipus d'atac des d'un d'aquests equips connectats.

Infecció dels dispositius

En connectar-nos a una wifi aliena, un usuari malintencionat connectat a la mateixa xarxa podria tractar d'infectar el nostre equip amb alguna mena de virus.

És important mantindre sempre el nostre equip actualitzat amb les últimes actualitzacions de seguretat per al sistema operatiu i per a les aplicacions que tinguem instal·lades.

Equips intermediaris malintencionats

Un usuari malintencionat connectat a la xarxa podria configurar el seu equip per a fer d'intermediari de la comunicació entre nosaltres i el servei (per exemple, *Facebook*) modificant o eliminant la informació intercanviada, que passaria a través del ciberdelincuente.

El hacker "innocent"

En un moment donat, podem sentir la temptació de connectar-nos a una xarxa aliena oberta o protegida utilitzant eines de *hacking* wifi. No obstant això, aquesta pràctica constitueix un ús il·lícit de serveis de tercers que pot tindre conseqüències legals.

A més, pot donar-se el cas que aqueixa xarxa wifi no present contrasenya o siga especialment fàcil de hackejar precisament per a atraure víctimes a ella i així robar les dades a l'usuari entremaliat.

RECOMANACIONS BÀSIQUES

Mai hem d'utilitzar xarxes wifi no de confiança per a accedir a serveis on s'intercanvie informació sensible: informació bancària, recursos corporatius, correu electrònic o accés a les xarxes socials.

Hem d'evitar l'ús de qualsevol servei en el qual la informació transferida tinga un component important de privacitat. Encara que podem utilitzar les xarxes públiques per a altres accions, com llegir notícies en periòdics en línia o mirar la previsió del temps, no oblidem que la major part dels dispositius mantenen un procés de sincronització contínua, per la qual cosa el risc continua existint.

Si ho pots evitar, no et connectes a xarxes sense fils obertes. Les xarxes públiques poden posar-nos en perill. Tant l'administrador com algun dels usuaris connectats poden utilitzar tècniques per a robar-nos informació.

Mantindre sempre l'equip actualitzat, amb l'antivirus instal·lat correctament i si és possible, fer ús d'un tallafocs.

Si ens connectarem, és preferible accedir a una xarxa amb seguretat WPA o WPA2. Les xarxes obertes i amb seguretat WEP són totalment insegures.

No inicies sessió (usuari/contrasenya) en cap servei mentre estigues connectat a una xarxa pública. Evita realitzar transaccions bancàries, compres en línia o qualsevol altra tasca que supose l'intercanvi de dades privades des de xarxes wifi-públiques.

Deshabilitar qualsevol procés de sincronització del nostre equip si usaràs una xarxa pública.

Després de la connexió, eliminar les dades de la xarxa memoritzats pel nostre equip. Transaccions bancàries, compres en línia o qualsevol altra tasca que supose l'intercanvi de dades privades des de xarxes wifi-públiques.

"DESPRÉS DE LA CONNEXIÓ, ELIMINAR LES DADES DE LA XARXA MEMORITZATS PEL NOSTRE EQUIP"

PAUTES A TINDRE EN COMPTE EN PROTECCIÓ DE DADES

A continuació, a fi de minimitzar l'exposició indesitjada de dades de caràcter personal, es relacionen unes pautes bàsiques:

1. Tingues en compte la privacitat com una de les característiques desitjables a l'hora de triar un navegador i les aplicacions que instal·les i utilitzes en els teus dispositius. A causa de la constant evolució d'aquests productes has de consultar les últimes anàlisis que es publiquen sobre ells.
2. Evita instal·lar aplicacions innecessàries en el teu navegador, això minimitzarà els riscos.
3. Mantingues actualitzat el teu navegador per a gaudir de les últimes tecnologies de protecció antirastreig.
4. Si el navegador disposa de protecció avançada anti-rastrege/seguiment, activa o mantingues activada aquesta configuració. Aquestes opcions permeten diversos nivells de protecció, tria el nivell més elevat i que, alhora, s'ajuste a les teues preferències. En tot cas, si així ho consideres, pots habilitar l'opció per a enviar als llocs web el senyal "*Do not track*" , indicant el teu desig de no ser rastrejat.
5. Sospesa la utilitat de tindre dos navegadors diferents instal·lats, un amb una configuració més restrictiva i un altre configurat amb majors permisos. D'aquesta manera, si les configuracions anteriors t'impedeixen accedir a algun servei concret, pots continuar accedint a aqueix servei amb l'altre navegador minimitzant l'exposició de les teues dades.
6. Pots configurar el navegador de tal manera que en tancar-se s'eliminen les *cookies*. Si aquesta mesura et resulta incòmoda per a navegar en els teus llocs favorits, pots optar per esborrar-les manualment cada cert temps.
7. Evita en la mesura del possible iniciar sessió en el navegador, identificant-te amb un usuari, o almenys, evita que la sessió es mantinga oberta de manera indefinida.
8. Si el navegador no disposa de protecció avançada anti-rastrege/seguiment, es poden instal·lar extensions que realitzen aquesta funció. No obstant això, instal·la únicament aquells que oferisquen garanties. En general, instal·lar programari de tercers en el navegador pot introduir riscos.
9. Configura les opcions del teu dispositiu perquè, si així ho desitges, no s'utilitze l'identificador de publicitat per a crear perfils o mostrar anuncis personalitzats basats en la localització o el perfil.
10. Revisa i configura les opcions de personalització, perfils i publicitat d'aquelles aplicacions, serveis i xarxes socials que utilitzes.

"SOSPESA LA UTILITAT DE TINDRE DOS NAVEGADORS DIFERENTS INSTAL·LATS, UN AMB UNA CONFIGURACIÓ MÉS RESTRICTIVA I UN ALTRE CONFIGURAT AMB MAJORS PERMISOS. D'AQUESTA MANERA, SI LES CONFIGURACIONS ANTERIORS T'IMPEDEIXEN ACCEDIR A ALGUN SERVEI CONCRET, POTS CONTINUAR ACCEDINT A AQUEIX SERVEI AMB L'ALTRE NAVEGADOR MINIMITZANT L'EXPOSICIÓ DE LES TEUES DADES"

MATERIAL COMPLEMENTARI

- "Resolució de procediment A/00251/2018 instruït per l'Agència Espanyola de Protecció de Dades." Consulta aquest enllaç.
- Recomanacions de seguretat en xarxes WI-FI corporatives, per CN-CERT. Consulta aquest enllaç.
- Infografia recomanacions per a minimitzar els riscos que el seguiment en l'activitat de navegació pot tindre, per l'Agència Espanyola de Protecció de Dades. Consulta aquest enllaç.
- Decàleg bàsic de seguretat per CN-CERT. Consulta aquest enllaç.
- Seguretat en xarxes wifi per INCIBE. Consulta aquest enllaç.
- Resolució d'arxiu, referents a l'Ajuntament de Barcelona per Autoritat Catalana de Protecció de Dades (APDCat). Consulta aquest enllaç.
- Guia "Privacitat i seguretat en internet", elaborada per l'AEPD i l'OSI. Consulta aquest enllaç.

NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) Protecció de Dades avala que Interior monitore xarxes socials per a detectar faules sobre la Covid-19.**

  L'Agència Espanyola de Protecció de Dades (AEPD) ha avalat que el Ministeri de l'Interior monitore les xarxes socials per a detectar les faules i *'fake news'* relacionats amb la Covid-19, un assumpte pel qual diversos partits de l'oposició van demanar explicacions després d'informar-se d'aquesta labor policial en roda de premsa en Moncloa durant el primer estat d'alarma decretat al març de 2020.

  Consulta la informació en aquest enllaç.

- **El Ple dona llum verda al Projecte de Llei orgànica de protecció integral a la infància i l'adolescència enfront de la violència i el remet al Senat, que recull la disponibilitat d'un canal de denúncia de continguts il·lícits amb la finalitat de garantir la protecció en Internet.** Consulta la notícia en aquest enllaç.

- **El Comité Europeu de Proteccion de dades adopta un dictamen sobre el projecte de decisió d'adequació del Regne Unit.** El 14 d'abril de 2021, el Comité Europeu de Proteccion de dades ("EDPB") va anunciar que havia adoptat la seua Opinió sobre el projecte de decisió d'adequació del Regne Unit emesa per la Comissió Europea el 19 de febrer de 2021. La decisió d'adequació s'adoptarà formalment si és aprovada pels Estats membres de la UE actuant a través del Consell Europeu.

  Consulta la notícia en aquest enllaç.