cesicat

SEGURETAT I PROTECCIÓ EN LA MISSATGERIA INSTANTÀNIA

Índex

Qui fem aquesta guia

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya

Donar suport a la protecció de les infraestructures crítiques TIC nacionals

Promocionar un teixit empresarial català sòlid en seguretat TIC

Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

Introducció

I aquesta guia, per a qui és?

Aquesta guia va dirigida a totes aquelles persones que utilitzen habitualment sistemes de missatgeria instantània, incloent clients específics (Windows Live Messenger, Google Talk, Yahoo! Messenger, ICQ, ...), el xat integrat en diverses xarxes socials (Facebook xat, xat de Tuenti), o d'altres programes amb un objectiu inicial diferent però que implementen un sistema d'aquest tipus (skype, steam,...).

3.1 Abast de la guia

En aquest document es proporcionen continguts dirigits a persones que no tenen un coneixement avançat d'informàtica o de seguretat de la informació.

Aquesta guia no pretén ser exhaustiva ni cobrir totes les mesures i les funcionalitats de seguretat possibles, sinó cobrir-ne les més bàsiques i les que el CESICAT considera imprescindibles per a un ús segur dels sistemes de missatgeria instantània.

La guia intenta tractar la missatgeria des d'un punt de vista genèric, sense especificar programes o serveis concrets. Gairebé totes recomanacions exposades es poden aplicar a la majoria dels serveis de missatgeria utilitzats actualment. No obstant, es tractaran de manera més específica les opcions disponibles a les xarxes de missatgeria més utilitzades i populars.

3.2 Aspectes legals i normatius

- Limitació de responsabilitat de CESICAT
- Suplantació d'identitat

4.1 Riscos

En aquest primer apartat s'exposen els riscos de seguretat associats amb l'ús habitual d'un servei de missatgeria instantània, o el que és el mateix, les possibles conseqüències negatives per descuidar o no aplicar un conjunt de recomanacions i bones pràctiques de seguretat.

4.1 Infecció de l'equip

La infecció de l'equip amb algun tipus de codi maliciós (*malware*) pot ser la conseqüència més greu que pot patir l'ordinador.

Actualment les famílies de codi maliciós més utilitzades tenen com a objectiu final permetre l'atacant accedir remotament a l'equip infectat, monitoritzar les seves accions i utilitzar-lo per realitzar atacs a tercers. Com a conseqüència, gran part de les accions realitzades poden tenir com a resultat un perjudici econòmic directe per a l'usuari i un benefici per al ciberdelinqüent.

La missatgeria instantània s'ha convertit en una via més per arribar a difondre codis maliciosos, tot aprofitant que les mesures de detecció/protecció necessàries en els elements de seguretat (antivirus, antiinundació -*anti-spamming*-,...) per a aquests tipus de comunicacions no són tan habituals com per a la protecció del correu electrònic.

4.2 Suplantació d'identitat

La suplantació d'identitat és una de les conseqüències més habituals dels atacs contra els serveis de missatgeria instantània.

Normalment aquests serveis no s'utilitzen per dur a terme activitats especialment importants en les quals la suplantació d'identitat provoqui un dany econòmic directe, com ara un frau. No obstant això, aquest tipus d'incidents pot facilitar informació a un possible atacant que pot ser utilitzada per dur a terme altres tipus d'atacs o per provocar greus perjudicis a la imatge de l'usuari. Aquest fenomen és especialment habitual en casos d'assetjament i discriminació social entre adolescents.

4.3 Fuita o robatori d'informació

La revelació d'informació privada o sensible a tercers no desitjats suposa un risc important pel fet que normalment els serveis de missatgeria instantània no permeten l'usuari estar realment segur de qui és la persona que està a l'altra banda del canal.

En moltes ocasions els usuaris proporcionen en els seus missatges d'estat, o en el seu propi sobrenom, informació que pot ser considerada com a privada. S'ha de tenir present que la informació visible en aquests dos camps pot acabar a mans de terceres persones que l'usuari no havia considerat. La llista de contactes pot arribar a ser tan extensa que és impossible recordar i ser conscient de tots i cadascun dels contactes que hem anat afegint. Finalment, el robatori d'informació pot produir-se de forma activa per part d'un atacant per mitjà de diversos mecanismes que es detallen a l'apartat 4.2.

4.4 Pèrdua d'accés i d'informació

Qualsevol atacant que tingui accés a les credencials d'accés pot utilitzar-les per entrar i canviar la contrasenya, de manera que l'usuari legítim ja no podria utilitzar-la, tot perdent l'accés a la seva identitat al servei de missatgeria instantània.

Per a molts usuaris és possible que aquest perjudici sigui més important que perdre el carnet d'identitat o la targeta de crèdit, per la dificultat que hi ha a la majoria d'aquests serveis per desactivar el compte perdut o manllevat, o per tenir l'opció -com a mínim- de notificar de forma segura als nostres contactes que s'ha deixat d'utilitzar una identitat i que la persona que la està fent servir no som nosaltres.

Cal tenir en compte que perdre tota la llista de contactes que tenim registrats pot ser una pèrdua irreparable. La majoria de vegades no hi ha una còpia de seguretat d'aquesta informació.

A més, si el compte utilitzat és comú en d'altres serveis disponibles a la xarxa (com en el cas de Windows Live, Yahoo! o Google), la pèrdua d'accés pot comportar una pèrdua d'informació important, correus electrònics, calendari, fotografies o altres dades associades que estiguin emmagatzemats en aquest tipus de serveis.

Una variant de tipus d'atac que pot comportar el risc de pèrdua d'accés i d'informació és el segrest del compte d'usuari. L'atacant extorsiona l'usuari amb la finalitat de treure'n un benefici.

Amenaces

En aquest apartat es detallen les amenaces principals que es podrien materialitzar pels riscos exposats a la secció anterior.

4.2.1 Contrasenyes febles

La majoria de serveis de missatgeria instantània utilitzen un duet -usuari i contrasenya- per identificar unívocament l'usuari i proporcionar accés al servei. Com en qualsevol sistema d'aquest tipus, i especialment en aquells en què l'identificador es comparteix amb molta gent o directament es fa públic, la fortalesa del sistema d'autenticació recau sobre la complexitat de la contrasenya.

Una contrasenya fàcil d'endevinar (noms i dates relacionables amb l'usuari, paraules existents en el diccionari,...), o fàcil d'extreure tot fent proves (contrasenyes curtes), és una de les conductes més habituals que faciliten el robatori de les credencials d'accés.

Una altra via possible per obtenir la contrasenya són els sistemes de recuperació de contrasenya en cas que l'usuari no la recordi. Alguns d'aquests sistemes són febles en el seu disseny i obliguen l'usuari a contestar preguntes secretes les respostes de les quals poden ser senzilles de conèixer.

4.5 Sessions sense tancar

La majoria dels clients d'accés als serveis de missatgeria inclouen la funcionalitat d'accés automàtic. Aquesta opció recorda la contrasenya de l'usuari amb la finalitat de no introduir-la cada vegada que s'inicia una sessió al servei.

Aquesta opció, que proporciona comoditat d'usabilitat, es converteix en una amenaça important en màquines d'ús compartit. L'escenari més senzill perquè un atacant pugui aconseguir accés a un compte aliè és el d'ordinadors d'ús compartit o públic (cibercafès, biblioteques,...) on un usuari ha activat l'opció de "recordar compte", "recordar contrasenya" i/o "inici automàtic". En accedir posteriorment un altre usuari es trobaria la sessió oberta, en moltes ocasions involuntàriament, amb l'accés obert a tota la informació i la possibilitat de poder suplantar l'usuari anterior. Això és aplicable tant a serveis de missatgeria basats en un programa client com a aquells que utilitzen una interfície web.

Finalment tenim atacs més elaborats en serveis basats en plataforma web, com ara els de fixació de sessió i segrest de sessió, aquest últim mitjançant intercepció de tràfic i robatori de la galeta (cookie) variable que s'emmagatzema localment.

4.5.1 *Phishing*

Els atacs de *phishing* afecten sobretot els serveis de missatgeria que es basen en sistemes de tipus web. Consisteixen en pàgines falses que intenten imitar i suplantar el proveïdor del servei amb l'objectiu que l'usuari introdueixi voluntàriament, sota engany, les seves credencials d'accés en un sistema controlat per un atacant.

En molts casos aquest tipus de pàgines no pretenen suplantar directament el proveïdor, però sí intenten fer creure l'usuari que estan associats al servei, utilitzant un disseny similar i oferint funcionalitats addicionals, gairebé sempre falses, com pot ser la possibilitat de saber qui té l'usuari a la seva llista de contactes o qui ha visitat el seu perfil.

Aquesta última amenaça estaria a mig camí entre l'atac de phishing i l'enginyeria social que s'explica a continuació.

4.5.2 Enginyeria social

L'enginyeria social és una classificació molt àmplia que inclou qualsevol atac on l'atacant, mitjançant l'engany o la persuasió, aconsegueix que l'usuari legítim realitzi inconscientment accions que faciliti el compliment de l'objectiu final de l'atacant. Alguns exemples són:

- Executar un programa o obrir un document maliciós.
- Visitar una pàgina web maliciosa.
- Comunicar el seu usuari i contrasenya voluntàriament.
- Proporcionar informació confidencial o restringida.

4.6 Codi maliciós

El codi maliciós és el que comunament es coneix com a "virus", encara que el terme més genèric que englobaba altres tipus de programaris maliciosos seria el mot anglès "*malware*". Aquests programes s'instal·len sense coneixement de l'usuari i actuen directament en el seu perjudici mitjançant el robatori d'informació, de diners o utilitzant els seus recursos (el seu ordinador i la seva connexió a Internet) per realitzar activitats il·legals.

Entre els múltiples mecanismes d'infecció de l'equip la missatgeria instantània és un més. Les vies principals en aquest cas són:

- Vulnerabilitats associades als clients de missatgeria.
- Enllaços o arxius maliciosos enviats com a correu brossa i propagats pel mateix virus als contactes que té la víctima.

4.7 Programari de publicitat (*adware*) i programari espia (*spyware*)

Aquesta categoria d'amenaces engloba un tipus de programes que, com els codis maliciosos (*malware*), s'instal·len als ordinadors dels usuaris sense el seu coneixement. Es poden introduir mitjançant la instal·lació d'un programa legítim o mitjançant enganys que provoquen que un usuari poc atent els instal·li voluntàriament. No arriben a creuar la frontera de codi maliciós com els virus, els troians, els cucs i d'altres categories de programari maliciós (*malware*), però normalment extreuen un benefici mitjançant l'explotació de la informació dels usuaris o mostrant publicitat. En la majoria d'ocasions aquest tipus de programes poden resultar perjudicials per al funcionament normal del sistema, i en molts casos resulten bastant difícils d'eliminar definitivament.

Un dels formats més habituals de programari espia (spyware) en missatgeria instantània són els complements per als programes clients que suposadament milloren les seves funcionalitats, afegeixen continguts atractius (icones, emoticones,...) o eliminen publicitat.

4.8 Correu brossa (*spam*)

Igual que els serveis similars com el correu electrònic o la telefonia, on l'identificador d'un usuari (adreça de correu, número de telèfon) es difon de manera més o

menys pública, és possible que es rebin missatges no desitjats amb publicitat o contingut perillós.

De vegades als missatges no desitjats en xarxes de missatgeria instantània també reben el nom d'"*spim*", derivat de les paraules en anglès *spam* (correu electrònic no desitjat o correu brossa) i "*instant messaging*" (missatgeria instantània).

4.9 Intercepció de trànsit

Com qualsevol servei que transmeti informació a través de la xarxa, la missatgeria instantània és susceptible de ser atacada per mitjà de l'escolta o la intercepció de trànsit. El risc és més gran en xarxes sense fils, sobretot les que s'utilitzen de forma pública (cibercafès, biblioteques, etc.), on qualsevol usuari que estigui connectat a la xarxa (o fins i tot sense estar-ho) rep tota la informació difosa a través d'ella.

4.9.1 Robatori d'informació amb accés local a l'equip

Finalment cal preveure la possibilitat que un atacant tingui accés a l'equip que l'usuari utilitza per accedir a la missatgeria instantània. Una intrusió local o remota permet robar informació emmagatzemada localment com ara credencials d'accés o fitxers de registre que inclouen les converses que s'han intercanviat amb la resta de contactes.

Encara que l'accés a un compte de missatgeria pot semblar secundari davant d'una intrusió completa al nostre equip, cal tenir en compte que per a un atacant robar la contrasenya d'aquests serveis pot significar tenir accés a la informació i al compte de forma prolongada en el temps, o fins i tot segrestar-la. Com s'ha comentat a l'apartat de Riscos, el valor de la informació associada al compte, encara que no estigui emmagatzemada a l'ordinador, pot tenir gran importància per a l'usuari.

Recomanacions

5.1 Programari

El primer pas per accedir a un servei de missatgeria instantània és triar i instal·lar el programari. Si el servei de missatgeria té un client específic, a l'hora de realitzar la seva descàrrega de la xarxa és molt important assegurar-nos que es realitza des del lloc web de l'empresa proveïdora del servei. És recomanable anar amb compte amb els resultats de la consulta de qualsevol cercador perquè els primers enllaços poden estar manipulats per oferir una descàrrega que no sigui la versió autèntica.

Hi ha la possibilitat d'utilitzar clients de tercers, opció interessant quan tenim més d'un compte en diferents serveis d'un mateix tipus. Per a aquests casos hi ha clients multi protocol no oficials, que són perfectament vàlids, però cal assegurar-se que són legítims. Amb aquesta finalitat es pot utilitzar alguna pàgina de descàrregues de programari gratuït que inclogui valoracions dels usuaris o alguna relació de clients coneguts[1]. Alguns proveïdors de missatgeria instantània com Facebook ofereixen la seva pròpia llista de clients compatibles[2].

5.1 Connexió segura amb el servidor

En el moment de configurar el client de missatgeria instantània el consell més bàsic és el d'utilitzar sempre una connexió segura amb el servidor, d'aquesta manera la informació viatjarà de forma xifrada per la xarxa i s'enviarà únicament al servidor legítim. Això impedeix que un atacant que escolti el tràfic el pugui entendre o pugui suplantar el servidor necessari per proporcionar el servei, modificant el tràfic a la seva voluntat.

En la majoria de clients oficials no és possible canviar aquesta opció i l'usuari està sotmès a la configuració per defecte que ha triat el proveïdor. No obstant aquest

1. http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients
2. https://www.facebook.com/sitetour/chat.php

fet, els clients de tercers que suporten múltiples protocols són normalment més flexibles i permeten que l'usuari configuri aquesta opció. Pot aparèixer amb diversos noms com "connexió segura amb el servidor", "connexió xifrada" o directament amb el nom del protocol utilitzat, com ara "SSL/TLS".

El xifrat és imprescindible per enviar les credencials d'identificació, i així està implementat en la majoria de serveis de missatgeria. Una mica menys habitual és que s'apliqui per a la resta de la comunicació, encara que és l'única forma d'assegurar que les converses no les pot escoltar un atacant.

En el cas d'accedir per mitjà d'un client web, la confidencialitat de la sessió i les converses ve donada per l'ús de l'HTTPS/SSL al connectar-se al lloc web. Cal assegurar-se que l'adreça a la qual s'accedeix comença per HTTPS, que el certificat és vàlid i que no provoca cap error.

5.2 No emmagatzemar les contrasenyes

Una opció extremadament important a l'hora de configurar el programa client o quan s'accedeix per mitjà d'un client web és desactivar l'opció d'emmagatzematge de la contrasenya en local.

És realment necessari desmarcar l'opció "guardar contrasenya" o "connectar automàticament" quan es fa servir un ordinador d'ús compartit o públic, en cas contrari, qualsevol usuari que accedeixi després a l'equip podrà utilitzar aquest compte.

És igual de recomanable fer-ho en ordinadors d'ús privat, evitarem que un atacant que aconsegueixi accés a l'equip, físicament o remotament, pugui robar les credencials emmagatzemades a l'ordinador.

Aquest risc és especialment important perquè molts programes client emmagatzemen la contrasenya sense xifrar.

5.3 Opcions de privacitat

Altres opcions rellevants des del punt de vista de la seguretat són les relatives a la privacitat, que resulten especialment importants en serveis associats a xarxes socials que inclouen la funcionalitat de compartir fotos o un altre tipus d'informació.

Alguns exemples de les opcions que es poden trobar en aquest tipus de programari són:

- Iniciar i connectar automàticament en encendre l'equip. A més del risc comentat a l'apartat anterior, l'ús d'aquesta opció té implicacions de privacitat, doncs els contactes de l'usuari podran saber amb exactitud quan es troba utilitzant l'equip.
- Indicar activitat de teclat i ratolí. Això pot indicar exactament quan l'usuari es troba davant de l'equip.
- Emmagatzemar registre de converses. Amb aquesta opció totes les converses intercanviades amb els contactes queden enregistrades, normalment en un format accessible a qualsevol que utilitzi l'equip o a un atacant que aconsegueixi accedir-hi.
- Mostrar foto de perfil. Pot ser útil desactivar l'opció de mostrar una foto de perfil a tots els contactes.
- No admetre missatges de persones que no siguin contactes donats d'alta, per evitar el correu brossa (*spam*) i els atacs d'enginyeria social.

Activar la protecció antivirus per a missatgeria

La majoria d'antivirus amb protecció en temps real inclouen l'opció d'analitzar els missatges instantanis a la recerca de contingut maliciós per inspecció d'enllaços o arxius rebuts. És recomanable comprovar que aquesta opció es troba activada i és compatible amb el servei de missatgeria utilitzat. Per descomptat, cal mantenir l'antivirus actualitzat en versió i firmes.

Contactes

La gestió dels contactes pot semblar irrellevant des del punt de vista de la seguretat, però si tenim la resta d'opcions correctament configurades el fet de mantenir fora de la llista de contactes un possible atacant és una barrera molt efectiva.

Algunes recomanacions bàsiques són:

- No admetre missatges de persones fora de la llista de contactes. D'aquesta manera evitarem rebre missatges no desitjats que en molts casos poden incloure enllaços o fitxers perillosos.
- No admetre contactes desconeguts. Si un desconegut intenta afegir l'usuari als seus contactes sense un motiu aparent és probable que es tracti d'algun tipus de contingut brossa (*spam*), atac o intent de frau.
- Comprovar que el contacte és qui diu ser, si és possible mitjançant un mitjà que no sigui Internet (telèfon, trobada personal).
- No publicar l'identificador en llocs públics, evitant així que qualsevol pugui intentar afegir l'usuari als seus contactes.

Enllaços web

Actualment els enllaços web maliciosos són la via d'entrada més comú del programari maliciós (*malware*) per infectar els equips. La missatgeria instantània és una via més per fer arribar a l'usuari aquests enllaços i aconseguir que els obri amb un navegador. Si el navegador o algun dels seus complements són vulnerables, el *malware* s'instal·larà a l'ordinador.

Les principals recomanacions relatives als enllaços rebuts són:

- Desconfiar de qualsevol enllaç, especialment dels que provinguin de desconeguts.
- Compte amb enllaços procedents de contactes coneguts però que van acompanyats d'algun missatge en un altre idioma o que s'envien aïlladament sense estar emmarcats en una conversa. Cal comprovar sempre, abans de clicar, que el contacte ha enviat l'enllaç voluntàriament.
- No refiar-se del text de l'enllaç, pot semblar que porta a un lloc legítim però podria portar-nos a un web maliciós.
- Compte amb els enllaços curts (bit.ly, go.gl, etc.) que s'han tornat molt populars arran del seu ús a les xarxes socials. Podem expandir i saber a on ens porten utilitzant eines específiques com el LongURL[3].
- En cas de dubte hi ha eines que permeten avaluar el grau de perillositat d'un determinat enllaç, com

3. http://longurl.org/

per exemple el VirusTotal[4], el SafeBrowsing de Google[5] o l'URLVoid[6], que comprova l'enllaç en diversos llocs alhora.

- Sospitar especialment d'enllaços a descàrregues d'arxius, que poden incloure un codi maliciós.

Arxius rebuts

Igual que en el cas dels enllaços web, els arxius rebuts per missatgeria instantània són una via habitual d'infecció. A continuació s'ofereixen algunes recomanacions bàsiques a l'hora d'avaluar la perillositat dels fitxers rebuts:

- Analitzar manualment amb l'antivirus si no està activada la protecció en temps real per a la missatgeria. Si l'arxiu és sospitós es pot enviar a algun servei de la xarxa com VirusTotal, on s'escaneja de forma paral·lela a múltiples motors d'antivirus.
- No s'ha de confiar en l'antivirus com a única protecció. Recordeu que la principal mesura de seguretat és el sentit comú de l'usuari.
- Sospitar d'arxius no sol·licitats. Cal comprovar que el contacte ha enviat l'arxiu voluntàriament.
- Revisar a consciència el nom dels arxius i sobretot la seva extensió. No val refiar-se de la icona que ens mostra el sistema per al fitxer. Els fitxers més perillosos són els executables (.exe, .com, .pif, .vbs,...), però també els documents (PDF, DOC, PPT,...), encara que fins i tot els aparentment més inofensius, com imatges o vídeos, poden resultar molt perillosos.

Altres recomanacions

En els apartats anteriors s'han exposat les recomanacions més importants i que són aplicables a qualsevol servei de missatgeria. En aquesta secció es tracten algunes mesures de seguretat addicionals que no són aplicables en tots els casos.

5.4 Xifrat extrem a extrem (OTR)

L'opció de connexió segura amb el servidor comentada a l'apartat 5.1.1 proporciona autenticació i confidencialitat amb el proveïdor del servei. No obstant això, si l'usuari necessita un nivell de confidencialitat extrem a extrem i assegurar-se que la persona que està a l'altra banda és qui diu ser, pot utilitzar una capa de seguretat addicional proporcionada per un programa o complement extern per a aquest objectiu.

L'exemple més popular és el protocol OTR (*Off the Record*) basat en un algoritme de clau simètrica (AES) i la funció resum (*hash*) (SHA-1). A més d'implementar autenticació i xifrat, afegeix dues característiques addicionals que no existeixen als sistemes habituals de comunicació segura basats en criptografia asimètrica: confidencialitat directa (*forward secrecy*) i autenticació negable.

Existeixen diverses implementacions d'aquest protocol, per exemple de forma nativa o en forma de complements per a diversos clients de missatgeria, que permeten utilitzar aquest sistema gairebé en qualsevol servei de missatgeria.

5.5 Denunciar el segrest de comptes dels teus contactes

Alguns serveis de missatgeria instantània han inclòs la funcionalitat de notificar el robatori del compte d'un dels teus contactes o el seu ús fraudulent per enviar correu brossa (*spam*) o difondre programari maliciós (*malware*). D'aquesta manera, si diversos usuaris denuncien un compte robat, el proveïdor portarà a terme les accions per cercar la solució pertinent. Si l'usuari legítim encara posseeix el control del compte se li demanarà que canviï la contrasenya, i en cas que no, si és possible identificar se li proporcionarà els mitjans per a recuperar-la.

5.6 Videotrucada

Encara que no es tracti estrictament de missatgeria instantània aquesta funcionalitat està inclosa en molts d'aquests serveis. Hi ha diferents recomanacions a tenir en compte, principalment les que tenen relació amb la privacitat:

- Desactivar l'opció d'acceptar trucades de vídeo automàticament. Això evitarà que un contacte pugui establir una trucada de vídeo sense que l'usuari s'assabenti, per exemple perquè no es troba en aquest moment davant l'equip.
- Tapar físicament la càmera web quan no s'estigui utilitzant, per exemple amb un tros de cinta adhesiva, evitant així que es puguin realitzar gravacions sense l'autorització de l'usuari. Múltiples famílies de troians avui dia inclouen aquesta funcionalitat. Alguns models inclouen una llum que s'encén quan la càmera està funcionant, però encara que té una funció similar, és menys efectiu que la protecció física.
- Vigilar el lloc des d'on es realitzen les videotrucades i el que es pot veure a través de la càmera. En funció de la confiança que es tingui amb l'altra part es pot, sense voler, mostrar alguna informació que és preferible mantenir com a privada. És molt fàcil gravar les imatges per estudiar-les detingudament amb posterioritat.

5.7 Registre d'accessos

Diversos proveïdors de missatgeria instantània, especialment aquells que tenen el compte associat a d'altres serveis, permeten accedir a un registre d'activitat del compte. Això permet detectar activitat estranya, com l'accés des d'adreces IPs desconegudes o en hores que l'usuari sap que no hi ha accedit. Una altra característica relacionada i altament desitjable és que el proveïdor permeti tancar remotament qualsevol altra sessió que s'hagi deixat oberta per equivocació.

Alguns proveïdors apliquen determinats filtres de detecció que permeten alertar l'usuari sobre activitat il·lícita. No obstant això, l'usuari pot consultar aquesta informació si detecta activitat sospitosa, com missatges de correu brossa (*spam*) enviats en nom seu als seus contactes.

4. http://www.virustotal.com/
5. http://www.google.com/safebrowsing/diagnostic?site=www.sitioacomprobar.com
6. http://www.urlvoid.com/

Conclusions

La missatgeria instantània ofereix funcionalitats que no tenen altres sistemes de comunicació, però també és una via més d'exposició als riscos existents a Internet. La majoria d'amenaces són similars a les existents en altres serveis de la xarxa, com el correu electrònic o la navegació web. Per tant, les recomanacions bàsiques són les mateixes:

- Informar-se sobre els riscos i les amenaces i aplicar el sentit comú per evitar l'enginyeria social.
- Conèixer les característiques i les funcionalitats de seguretat, i configurar els programes de forma adequada.
- Mantenir els programes i els antivirus actualitzats amb la finalitat de tancar possibles forats de seguretat.
- Desconfiar de fitxers i enllaços, especialment dels no sol·licitats o dels enviats per desconeguts.

Glossari

SSL/TLS: conjunt de protocols que permeten negociar els mecanismes de transferència segura d'informació i intercanviar les claus entre les parts. És el sistema més utilitzat en les comunicacions a través de xarxes insegures, per exemple per a l'accés segur a llocs web mitjançant la seva integració amb HTTP, el que s'anomena com HTTPS.

Criptografia de clau simètrica: algorismes d'ofuscació de la informació en els quals tant el procés de xifrat com el de desxifrat utilitzen la mateixa clau, coneguda tant per l'emissor com pel receptor de la informació.

Criptografia de clau asimètrica: algorismes d'ofuscació de la informació on cada participant en un intercanvi d'informació té un parell de claus complementàries, una de pública i una altra de privada. La informació que es xifra amb una d'elles només es pot desxifrar amb la seva parella. D'aquesta forma és possible proporcionar, a més de confidencialitat, autenticació i integritat.

Certificat digital: és un document digital mitjançant el qual un tercer confiable (una autoritat de certificació) garanteix la vinculació entre la identitat d'un subjecte o entitat (per exemple el nom, l'adreça, el domini d'un web, o altres aspectes d'identificació) i una clau pública.

Confidencialitat directa (*forward secrecy*): cada missatge es xifra amb una clau única. Aquesta propietat assegura que el trencament d'una clau en el futur, gràcies a l'augment de capacitat de procés dels ordinadors, no permetrà desxifrar automàticament totes les converses.

Autenticació negable: els participants d'una conversa poden autenticar les altres parts però, un cop finalitzada, qualsevol pot manipular el registre de manera que ningú pot demostrar davant un tercer allò que ha dit un participant. Aquesta és una característica bàsica en les converses privades cara a cara i que permet conservar l'anonimat a un participant si així ho desitja.

Referències i enllaços web

[1] ***Using Instant Messaging and Chat Rooms Safely.*** US-CERT Cyber Security Tip ST04-011.
http://www.us-cert.gov/cas/tips/ST04-011.html

[2] **Recomendaciones a usuarios de Internet. Agencia Española de Protección de Datos**
http://www.usuariosteleco.es/Novedades/Documents/agpd_guia_recomendaciones_internet.pdf

[3] ***Securing Instant Messaging. Symantec***
http://www.symantec.com/avcenter/reference/secure.instant.messaging.pdf

[4] **Virus en la mensajería instantánea. Microsoft**
http://www.microsoft.com/es-es/security/pc-security/antivirus-im.aspx

[5] **Comparativa de clients de missatgeria instantània. Wikipedia**
http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients

[6] **Instant Messaging Security Concerns and Recommended Best Practices. Francis J. Reiss, SANS Security Essentials GSEC Practical Version**
http://www.giac.org/paper/gsec/2980/instant-messaging-security-concerns-recommended-practices-security-essentials-gsec-pr/104990

[7] ***Understanding Instant Messaging (IM) and its security risk. Sujata Chavan, SANS Institute InfoSec Reading Room.***
http://www.sans.org/reading_room/whitepapers/protocols/understanding-instant-messaging-im-security-risks_1239

cesicat

Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat