Universitat Oberta de Catalunya

uoc.edu

Protecció i gestió de la continuïtat de negoci davant un atac ransomware per a PIMEs.

Mònica Marcos Benítez
Màster universitari en Ciberseguretat i Privadesa
Privadesa

Albert Jové Canela
Cristina Pérez Solà

22/05/2022


Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

FITXA DEL TREBALL FINAL

Títol del treball:	*Protecció i gestió de la continuïtat del negoci davant un atac ransomware per a PIMEs*
Nom de l'autor:	*Mònica Marcos Benítez*
Nom del consultor/a:	*Albert Jové Canela*
Nom del PRA:	*Cristina Pérez Solà*
Data de lliurament (mm/aaaa):	*05/2022*
Titulació o programa:	*Màster Universitari en Ciberseguretat i Privadesa*
Àrea del Treball Final:	*Privadesa*
Idioma del treball:	*Català*
Paraules clau	*PIME, Ransomware*

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

En l'actualitat, i com a conseqüència de la pandèmia del Covid-19, l'ús de les tecnologies en espais vulnerables en l'àmbit del treball ha augmentat. Els ciberdelinqüents són conscients d'aquestes vulnerabilitats i aprofiten aquestes oportunitats per extreure'n benefici.

En el món empresarial trobem les petites i mitjanes empreses, PIMEs, les quals són empreses més vulnerables com a conseqüència de tenir poc pressupost i formació en seguretat en general i ciberseguretat en particular. Fent aquestes empreses molt interessants per als ciberdelinqüents.

Un atac que ha fet ressò en aquests últims anys és el que pren nom de ransomware, el qual és un malware que s'introdueix als dispositius de les empreses mitjançant la descarrega d'arxius arribats per mitjà de correus electrònics, entre d'altres, i que el seu objectiu és xifrar els arxius i dades de les empreses, demanant un rescat per a aquestes dades i així obtenir un benefici. Al mateix temps, els ciberdelinqüents amenacen amb fer públiques aquestes dades, les quals podrien ser sensibles i podent tenir conseqüències legals a part de les econòmiques i reputacionals, com a conseqüència d'haver estat atacades per aquest tipus de malware.

En aquest estudi, es vol poder fer arribar a les PIMEs la importància de reorientar una part dels seus pressupostos cap a la ciberseguretat, aplicant unes mesures de prevenció assequibles per evitar que siguin víctimes d'un atac ransomware, o, si són afectades per aquest, poder minimitzar l'impacte i conseqüències.

Abstract (in English, 250 words or less):

Nowadays, because of the Covid-19 pandemic, the use of technology in vulnerable workplaces has increased. Cybercriminals are aware of these vulnerabilities and take advantage of these opportunities to obtain benefits of it.

In the business world, we can find small and medium sized enterprises, SMEs, which are the most vulnerable companies as a consequence of having a small budget and training in security in general and cybersecurity in particular. Making these companies very interesting for cybercriminals.

An attack that has been heard in the recent years is the one called ransomware, which is a malware that is introduced into corporate devices by downloading incoming files via e-mail, among others, and that its goal is to encrypt the company files and data, requesting a ransom for that data and thus make a profit. At the same time, cybercriminals are threatening to release this data, which could be sensitive and could have legal as well as economic and reputational consequences, as a result of being attacked by this type of malware.

The aim of this study is to make SMEs aware of the importance of reorienting part of their budgets towards cybersecurity, applying affordable prevention measures to prevent them from being the victims of a ransomware attack, or, if they are affected by it, to be able to minimize the impact and consequences.

Índex

Llista de figures

Llista de taules

1. Introducció

1.1 Context i justificació del Treball

En aquests últims anys, en el que s'ha viscut un succés que ningú s'imaginava que tindria lloc, una pandèmia a nivell mundial, el Covid-19, ha obert les portes a què es produïssin més ciberdelictes i que el percentatge d'empreses afectades per aquests augmentés, com a conseqüència del canvi de la forma de treballar abans i després de l'inici de la pandèmia del Covid-19.

Segons l'informe de *Ciberpreparación 2021*[1] realitzat per la companyia Hiscox, el percentatge d'empreses que van patir un ciberatac mundialment ha augmentat del 38% al 43% en aquest darrer any. Per tant, es pot apreciar clarament la tendència que ha hagut aquests últims anys i que continua sent, un món on els ciberatacs són l'ordre del dia.

Si focalitzem més, i no abastim tan mundialment, a Espanya, tenint en compte tots els tipus d'empreses grans i petites, el percentatge de ciberatacs que s'han produït al 2021 ha estat d'un 43%, segons l'informe de l'empresa Hiscox [1].

Alguns d'ells han fet ressò en aquesta època de pandèmia com ara el ciberatac al Hospital Central d'Astúries[2] produït per un atac ransomware, que va comprometre el funcionament de la sanitat, la qual ja estava congestionada per la mateixa pandèmia.

A més a més, hi ha diferents tipus de ciberatacs[3] que es poden produir com ara dominis maliciosos, malware, etc però l'atac que més està escalant i convertint-se en més habitual avui en dia és el ransomware.

El ransomware és tipus de malware que restringeix l'accés a determinades parts o arxius del sistema operatiu infectat, ja que aquests han estat xifrats, i demana a l'empresa afectada un rescat per treure la restricció. Això pot tenir conseqüències reputacionals, econòmiques i jurídiques per a l'empresa que ha patit aquest atac.

A més, s'afirma que el 58% de les companyies que han estat afectades per aquest atac ransomware han acabat pagant el rescat[4]. I es que en aquests temps de pandèmia els ciberdelinqüents han vist l'oportunitat d'aprofitar les

[1] Hiscox. https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021
[2] La Vanguardia. https://www.lavanguardia.com/tecnologia/20211222/7947999/ataque-ransomware-compromete-funcionamiento-hospital-mas-importante-asturias-pmv.html
[3] Interpol. https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19
[4] El País. https://cincodias.elpais.com/cincodias/2021/04/20/fortunas/1618932032_554260.html

vulnerabilitats de les empreses, ja que la majoria no estaven preparades per treballar remotament pel que fa als aspectes de ciberseguretat.

Però si ens fixem bé, això no només afecta a les grans empreses sinó que també es veuen afectades les PIMEs, microPIMEs i autònoms, encara que aquestes notícies no apareixeran als telenotícies i no es farà gran ressò com a conseqüència de la seva petita escala. Segons el mateix estudi de l'empresa Hiscox, en aquest últim any s'ha produït un 49% de ciberatacs en les petites empreses. Un valor que no deixa indiferent tenint en compte que a Espanya les PIMEs representen el 99,8% de les empreses[5].

Aquestes dades posen sobre la taula que la ciberseguretat no és un aspecte a no tenir en compte en la gestió de les empreses avui en dia, sinó un aspecte imprescindible per poder dur a terme el seu negoci i per tant, que no es vegi interromput per un ciberatac, en concret el ransomware.

Patir aquest tipus de ciberatac, el problema no és només patir-lo sinó les conseqüències d'haver-lo patit. Havent de parar motors durant un temps fins no tenir la infecció ransomware, poden afectar greument als aspectes econòmics de l'empresa, la reputació de cara als clients com a conseqüència d'haver estat infectats per aquest tipus de malware i un altre aspecte molt important és la informació que els ciberdelinqüents hagin pogut extreure. Si aquestes eren dades sensibles dels clients o fins i tot la propietat intel·lectual de l'empresa afectada també haurà conseqüències jurídiques a tractar.

Per aquesta raó, les empreses estan reorientant els seus pressupostos cap a la ciberseguretat. Però aquests costos poden ser elevats per a petites o mitjanes empreses. A més, moltes d'aquestes empreses tenen el pensament de no ser objectius de ciberatacs com a conseqüència de la seva petita escala. Un raonament molt erroni, ja que aquestes empreses també són més vulnerables com a conseqüència tenir poca formació en seguretat en general i ciberseguretat en particular i de no tenir tant pressupost dirigit cap a aquesta. Fent-les molt vulnerables i interessant pels atacants.

Per tot el comentat anteriorment, en aquest treball realitzarem un estudi focalitzat en les PIMEs per a què puguin prevenir-se d'un atac ransomware i alhora també proporcionar un pla de continuïtat de negoci que sigui assequible econòmicament per a aquestes empreses, intentant minimitzar així els casos d'atacs i augmentar la supervivència de les PIMEs a aquest tipus d'atacs cibernètics.

[5] Ministerio de industria, comercio y turismo. https://industria.gob.es/es-es/estadisticas/Cifras_PYME/CifrasPYME-enero2022.pdf

1.2 Objectius del Treball

L'objectiu del treball és donar un model de solució econòmicament assequible per a PIMEs. Incloent-t'hi un model de prevenció i un pla de continuïtat de negoci davant d'un atac ransomware.

Podem llistar els objectius que s'assoliran en aquest treball:

- Conèixer a fons què és el Ransomware, el seu origen i quins tipus hi ha segons com actuen i com es propaguen.
- Exposar la importància de la conscienciació de protegir-se davant un atac ransomware a les PIMES.
- Definir la situació habitual d'una PIME, organització, formació, situació econòmica.
- Entendre com poden ser atacades les PIMEs mitjançant un anàlisi de les seves vulnerabilitats.
- Exposar l'impacte econòmic, reputacional i jurídic de patir un atac ransomware.
- Definir mesures de prevenció assequibles per a PIMES.
- Definir un pla de continuïtat del negoci assequible econòmicament per a PIMEs.
- Avaluar les conseqüències legals en cas que hagi una fuga d'informació.

1.3 Enfocament i mètode seguit

Per poder realitzar i assolir els objectius plantejats en el punt anterior i així poder resoldre el problema plantejat, en aquest treball s'utilitzarà una metodologia d'investigació explicativa.

La raó per la qual s'han triat aquesta metodologia és perquè creiem que pot ser la més adequada per a realitzar l'estudi del ransomware i recopilar totes les dades i informació sobre les PIMEs utilitzant fonts imparcials, objectives i fiables. D'aquesta manera assolirem el coneixement sobre què és el ransomware, quins vectors d'atac i d'infecció hi ha.

Dins de la metodologia d'investigació explicativa farem ús dels mètodes ja existents, els comparatius causals, podent, d'aquesta manera, observar similituds o diferencies entre diferents PIMES, trobant les causes comunes (vulnerabilitats) del perquè són atacades per ciberatacs ransomware i d'aquesta manera poder donar solució al problema. Podent explicar mètodes de prevenció i, per tant, conscienciar a les petites i mitjanes empreses a què s'exposen i que han de prendre acció.

També farem ús d'un mètode ja existent que és l'estudi longitudinal, on serà útil per poder realitzar el pla de continuïtat del negoci i veure com l'ús d'aquest en el temps en cas que l'empresa hagi estat infectada, pot en sortir-se'n de la millor manera possible. I al mateix temps, veure com evoluciona l'estat de l'empresa en aspectes econòmics, reputacionals i jurídics.

D'aquesta manera, haurem pogut entendre, comprendre i transmetre la situació de vulnerabilitat de les PIMEs davant atacs ransomware. Conscienciant a les PIMEs per a què prenguin accions davant aquesta mena de ciberatac i provenint-lis una metodologia apte per a elles.

1.4 Planificació del Treball

Per poder dur a terme la planificació del projecte, llistarem les tasques que es duran a terme durant la seva realització a la taula 1. Això ens ajudarà a planificar de forma correcte el treball de fi de màster i aconseguir entregar tot l'estudi en els temps estipulats.

PAC1. Pla de treball		
	Inici	Fi
1.1. Context i explicació del problema a resoldre	2022-02-20	2022-02-21
1.2. Objectius del Treball	2022-02-22	2022-02-23
1.3. Enfocament i mètode seguit	2022-02-23	2022-02-23
1.4. Planificació del Treball	2022-02-24	2022-02-26
1.5. Estat de l'art	2022-02-27	2022-02-27
1.6. Recursos necessaris i presupost del projecte	2022-02-28	2022-02-28
Entrega Pla de Treball (Fita)	2022-03-01	2022-03-01
	2022-02-20	**2022-03-01**

PAC2. Entrega de seguiment		
	Inici	Fi
2.1. Definició de ransomware, origen i tipologia	2022-03-02	2022-03-04
2.2. Conscienciació a les PIMES	2022-03-05	2022-03-08
2.3. Afectació de la pandèmia Covid - 19	2022-03-09	2022-03-12
2.4. Estudi vulnerabilitat PIMES	2022-03-12	2022-03-15
2.5. Mecanismes d'infecció d'un atac ransomware	2022-03-16	2022-03-19
2.6. Impacte de l'atac	2022-03-19	2022-03-22
2.7. Mesures preventives davant un atac ransomware pe	2022-03-23	2022-03-28
Entrega PAC2 (Fita)	2022-03-29	2022-03-29
	2022-03-02	**2022-03-29**

PAC3. Entrega de seguiment		
	Inici	Fi
3. Pla de contingència i continuïtat del negoci en cas d'in	2022-03-30	2022-04-01
3.1. Explicació de l'objectiu	2022-04-02	2022-04-04
3.2. Abast del pla de continuïtat	2022-04-05	2022-04-09
3.3. Descripció de la situació que s'ha de controlar	2022-04-10	2022-04-11
3.4. Llista de procediments i responsables d'aquests	2022-04-12	2022-04-14
3.5. Disparament d'alarma en cas d'infecció	2022-04-14	2022-04-15
3.6. Pla de resposta	2022-04-15	2022-04-17
3.7. Pla de suport	2022-04-16	2022-04-19
3.8. Pla de recuperació	2022-04-20	2022-04-23
3.9. Pla d'anàlisi i millora	2022-04-23	2022-04-25
Entrega PAC3 (Fita)	2022-04-26	2022-04-26
	2022-03-30	**2022-04-26**

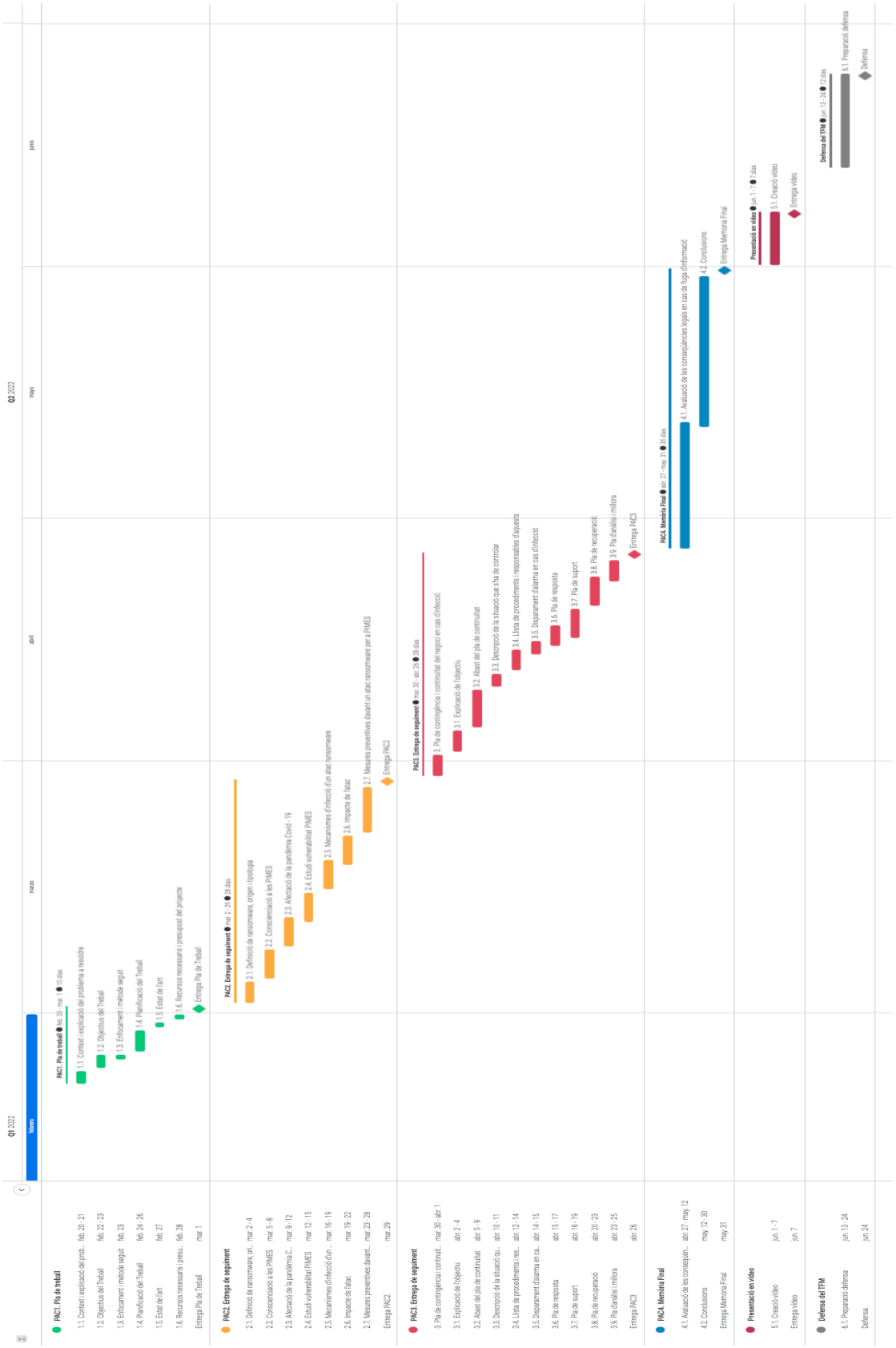
PAC4. Memòria Final		
	Inici	Fi
4.1. Avaluació de les conseqüències legals en cas de fu	2022-04-27	2022-05-12
4.2. Conclusions	2022-05-12	2022-05-30
Entrega Memoria Final (Fita)	2022-05-31	2022-05-31
	2022-04-27	**2022-05-31**

Presentació en vídeo		
	Inici	Fi
5.1. Creació vídeo	2022-06-01	2022-06-07
Entrega vídeo (Fita)	2022-06-07	2022-06-07
	2022-06-01	**2022-06-07**

Defensa del TFM		
	Inici	Fi
6.1. Preparació defensa	2022-06-13	2022-06-24
Defensa (Fita)	2022-06-24	2022-06-24
	2022-06-13	**2022-06-24**

Taula 1. Planificació de les tasques del Treball de Fi de Màster

1.4.1. Planificació temporal del Treball (Gantt)



Taula 2. Planificació temporal de les tasques

1.5. Estat de l'art

Cada cop més, com a conseqüència de les noves tecnologies i la situació de pandèmia, s'ha incrementat l'ús de les tecnologies en espais més vulnerables, com per exemple l'ús d'ordinadors personals, xarxes no segures, etc, fent incrementar també dels ciberatacs que es volen aprofitar d'aquestes vulnerabilitats i extreure'n un benefici.

En concret, l'atac ransomware no ha deixat de créixer segons l'estudi Ransomware Index Spotlight[6], tant en volum com en grau de sofisticació de les seves amenaces. Dels tipus més recents, poden realitzar atacs d'execució de codi de forma remota i altres poden explotar aplicacions webs i ser manipulades per a executar atacs de denegació de servei.

Els atacs amb aquest tipus de malware exigeixen el pagament d'un rescat per a recuperar els arxius o dades que han estat xifrades pel ransomware i que ara l'empresa afectada no hi té accés. Habitualment, avui en dia, demanen que el pagament es faci mitjançant criptomonedes o targetes de crèdit[7].

Tota aquesta situació, provoca que cada cop més hi hagi documentació existent sobre ciberatacs, i en concret també sobre el ransomware. Trobem per exemple *Una guia de aproximación para el empresario*[8] del Instituto Nacional de Ciberseguridad (INCIBE), on s'explica en què consisteix el ransomware com es poden protegir les empreses i què fer si els afecta. Es parla en aspectes generals però no es focalitza en les PIMEs.

Fent cerca, s'aprecia que molta informació que relacioni els ciberatacs amb les PIMEs no és el que més abunda. Tot i que segons el SSH TEAM Consulting[9], el cost mitjà d'un ciberatac en una petita empresa és de 75.000 euros[10] i que el 71% de les PIMEs d'Espanya ha estat víctima d'un ciberatac durant la pandèmia.

Per tant, és un àmbit que encara es pot explotar per a donar solucions a aquestes petites i mitjanes empreses que es troben més indefenses davant un atac ransomware per falta de formació en ciberseguretat i de pressupost destinat a aquest aspecte.

---

[6] Computing. https://www.computing.es/seguridad/informes/1129448002501/ransomware-vulnerabilidades-no-paran-de-crecer.1.html

[7] Malwarebytes. https://es.malwarebytes.com/ransomware/

[8] Ransomware. Una guia de aproximación para el empresario. Secretaría del estado de digitalización e intel·ligència artificial. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

[9] SSH TEAM Consulting. https://sshteam.com/

[10] ElPaís. https://cincodias.elpais.com/cincodias/2021/07/21/companias/1626821663_803769.html

Per aquesta raó, en aquest projecte s'intentarà acostar la informació sobre el ransomware a les PIMEs per a conscienciar-les i que puguin prendre accions per a no ser víctimes d'aquests tipus d'atac o, si el pateixen, que tinguin capacitat de recuperació i no impliqui el tancament de l'empresa.

1.6. Recursos necessaris i pressupost del projecte

Per poder realitzar el treball de final de màster, seran necessaris certs recursos a part de la planificació temporal exposada en l'apartat anterior. Aquests recursos tenen un cost associat de:

Recursos	Ús	Cost	Cost Total
Ordinador personal	Ordinador on es redactarà la memòria del projecte i es farà la cerca d'informació.	900€	900€
Connexió a Internet	Per a poder cercar informació es farà ús d'Internet	38€/mes	114€
Software d'edició de text	Ús de Microsoft Office (proporcionat per la UOC) per realitzar el treball de text	0€/mes	0€
Cost Total			1014€

Taula 3. Recursos i pressupost del projecte

2. Protecció i gestió del negoci davant un atac ransomware en PIMEs

Per a poder dur a terme l'estudi de prevenció i actuació davant un atac ransomware en PIMEs, i poder donar una solució assequible a aquest tipus d'empreses per a què puguin donar continuïtat al seu negoci després d'haver patit una infecció d'aquest tipus, primer de tot s'ha de saber contra que s'han de protegir aquestes petites i mitjanes empreses.

Primer es donarà l'explicació de què és el ransomware, quin és el seu origen i com ha evolucionat des del seu inici. A continuació, s'explicaran els diferents tipus de ransomware que existeixen, els diferents mecanismes d'infecció que utilitzen els atacants, és a dir els vectors d'atac existents i la forma en com operen, és a dir com xifren, etc.

Seguidament, es donarà conscienciació a les PIMEs sobre aquest tipus d'atac cibernètic, el ransomware, tenint en compte la seva situació com ara l'organització, formació i situació econòmica d'aquests tipus d'empreses. Podent realitzar un estudi de les diferents vulnerabilitats que poden tenir les PIMES, i com la pandèmia global del Covid-19 ha propiciat al increment d'aquest tipus d'atac i com els atacants s'han aprofitat d'aquestes noves vulnerabilitats per extreure'n un benefici.

A continuació, s'exposarà l'impacte tant econòmic, reputacional i jurídic que implicaria haver estat víctima d'un atac ransomware.

Finalment, es donaran a conèixer diferents mesures preventives davant un atac ransomware i un pla de contingència i continuïtat del negoci en cas d'incident.

2.1. Ransomware, un ciberatac en creixement

2.1.1. Definició, origen i evolució del ransomware

Si ens fixem amb el significat literal de la paraula ransomware, aquesta paraula està formada per la unió de dues d'angleses, *ransom*, que significa rescat, i *ware*, que significa producte.

El ransomware és un tipus de malware, en concret un software d'extorsió que es troba en constant evolució. Aquest xifra la informació dels dispositius de particulars o d'empreses impedint que hi puguin accedir, ja que les víctimes no tenen la clau per poder-les desxifrar, sinó que només l'atacant és qui la té.

Arribant a la seva finalitat de que les víctimes no puguin fer ús dels dispositius o dades xifrades fins que hagin pagat un rescat[11].

Per poder extorsionar de forma més intensa, els atacants xifraran dades crítiques de les víctimes, per exemple si es tracta d'una empresa els hi podrien xifrar informació confidencial del producte que ofereix aquella empresa o les bases de dades dels clients amb dades sensibles. Però aquests atacants poden no quedar-se esperant a què en algun moment la víctima pagui el rescat limitant-li només l'accés, sinó que també extorsionen a la víctima amenaçant-la de fer públiques les dades o d'eliminar tot allò al que ara no hi té accés en un cert període de temps. Posant més pressió a aquella empresa o usuari per a què realitzi el pagament del rescat, ja que a part de perjudici econòmic també hauria danys reputacionals o legals.

Aquest tipus de malware, pot utilitzar diferent vies per propagar-se i infectar. Algunes d'elles són mitjançant actualitzacions falses de software, campanyes de correu electrònic de *spam* i zones de descarrega de software no confiable. El que busquen els atacants és que l'usuari descarregui el contingut de l'arxiu adjunt infectat, si es mitjançant correu *spam*, o que seleccioni el *link* que portarà a la víctima a la pàgina web on se l'infectarà. Però aquesta màquina infectada, sinó s'aïlla de la xarxa, el ransomware es pot propagar per aquesta xarxa de l'empresa i infectar altres equips, obtenint així accés a més informació.

Però el ransomware no és un ciberatac que ha aparegut avui en dia, sinó que el primer ransomware data del 1989 [12]. En concret, el primer atac ransomware va ser realitzat pel seu inventor Joseph Popp. Un investigador que aprofitant la seva conferència mundial en l'Organització Mundial de la Salut, va distribuir disquets infectats amb aquest tipus de malware als assistents del congrés[13].

Aquest primer atac va comportar la pèrdua de fins una dècada d'investigació mèdica ja que tota la documentació havia estat bloquejada, denegant l'accés als arxius dels assistents que havien introduït al seu ordinador aquell disquet infectat.

A més a més, si seguim investigant en la historia i l'evolució del ransomware, ens podem adonar que aquest ha anat canviant el seu mode d'operació, podent diferenciant-lo en dues classes: bloqueig (ransomware-locker) i xifrat (ransomware-crypto).

[11] Kaspersky https://latam.kaspersky.com/resource-center/threats/ransomware
[12] RedesZone. https://www.redeszone.net/tutoriales/seguridad/ransomware-evolucion-historia/
[13] Imagen digital. https://www.dineroenimagen.com/2017-07-04/88422

El mode d'operació inicial del ransomware es basava en el bloqueig d'accés a l'ordinador, és a dir al sistema operatiu deixant una funcionalitat mínima. També es demanava un rescat per poder tornar a tenir accés a aquells arxius dins el sistema operatiu. Però usuaris amb cert coneixement es van adonar que era possible recuperar les dades, fent que l'efectivitat d'aquesta classe de ransomware fos menor comparat amb la classe de xifrat, fent que cada cop haguessin menys atacs d'aquesta mena.

En canvi, en l'actualitat, també podem trobar el ransomware basat en xifrar arxius o dades, provocant que l'usuari no pugui tenir accés a la informació dels seus dispositius, forçant a les víctimes a pagar el rescat en criptomonedes, per exemple, bitcoins, per a poder recuperar els arxius que havien estat xifrats, però proporcionant al atacant l'anonimat com a conseqüència que aquestes operacions no poden ser rastrejades.

Amb el transcurs del temps els atacs deguts al ransomware han anat incrementant, però podem observar que entre l'any 2014 i 2016, es va produir un creixement exponencial d'aquests atacs segons un article d'informació de l'institut tecnològic de Mèrida.

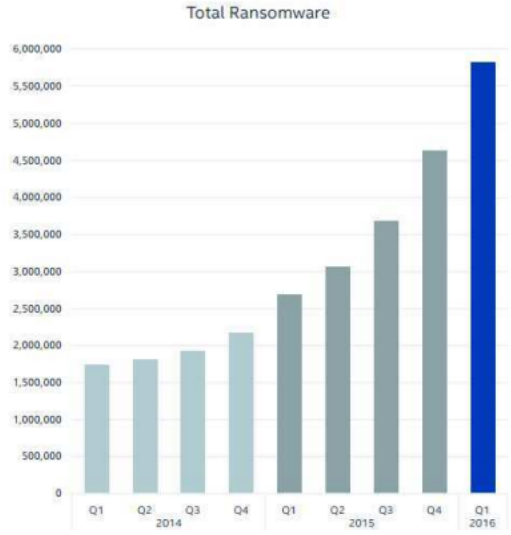


Figura 1. Nombre de mostres de ransomware entre 2014 i 2016 [14]

Un exemple d'atac global que va tenir lloc al maig del 2017 va ser l'atac ransomware WannaCry. Aquest és un exemple de ransomware xifrat que es va estendre a través d'ordinadors amb el sistema operatiu de Microsoft Windows, xifrant les dades de les víctimes i exigint un rescat d'entre 300 i 600 dólars amb bitcoins per a recuperar les dades. A més, els atacants amenaçaven en eliminar les dades si no feien el pagament en tres dies.

[14] Origen y evolución del cryptovirus Ransomware. https://www.academia.edu/32083196/ORIGEN_Y_EVOLUCI%C3%93N_DEL_CRYPTOVIRUS_RANSOMWARE

A més a més, també ha sorgit el Ransomware as a Service (RaaS), com a conseqüència que alguns ciberdelinqüents han fet evolucionar el concepte de ransomware convertint-lo en un esquema de distribució d'afiliats on el proveïdor del servei, la persona amb coneixements de programació, genera el malware, mentre que l'afiliat el distribueix i els dos obtenen beneficis dels atacs.

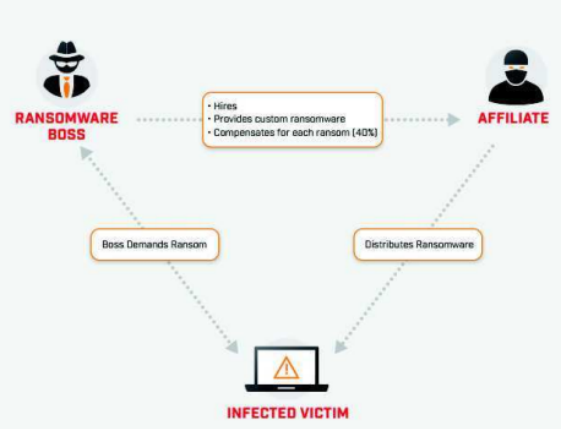


Figura 2. Sistema del RaaS [14]

2.1.2. Vectors d'atac

Com s'ha mencionat anteriorment, el ransomware utilitza diferents vies per poder infectar, les qual es poden anomenar vectors d'atac.

Entre els diferents vectors d'atacs existents els més utilitzats pels ciberdelinqüents per infectar mitjançant el ransomware són:

2.1.2.1. Phishing i enginyeria social

Un dels mètodes més empleats per a infectar a les víctimes amb ransoware, és mitjançant l'ús de correu electrònic el qual conté un arxiu maliciós.

L'objectiu és guanyar-se la confiança de les víctimes, ja siguin usuaris individuals o empreses, per a què així aquestes descarreguin l'arxiu adjunt o cliquin l'enllaç maliciós per així estendre la infecció per aquell dispositiu.

Però per aconseguir-ho, cada cop es fa ús d'informació més personalitzada i específica en el missatges dels correus electrònics per guanyar-se la confiança de la víctima que rep aquell correu, fent ús així de la enginyeria social[15], ja que els éssers humans tenim la tendència de

[15] Next Vision. Ciberseguridad Inteligente. https://nextvision.com/phishing-y-ransomware-tecnicas-de-ingenieria-social-que-ponen-en-riesgo-la-informacion-de-las-empresas/

confiar per naturalesa i els ciberdelinqüents ho aprofiten i enganyen a les víctimes.

A més, aquests arxius fraudulents poden ser difícils de distingir dels legítims, com a conseqüència que els atacants poden ocultar la veritable extensió de l'arxiu fent ús d'una configuració predeterminada de Windows [16]. Per exemple, si un arxiu te extensió .pdf, podria ser que la seva extensió completa realment fos pdf.exe.

Aprofitant el comentat anteriorment sobre l'enginyeria social, com a conseqüència d'aquesta confiança, també es produeixen suplantacions d'identitat de gran companyies d'administració pública i logística. Per concretar, en els últims anys han hagut diversos casos on es rebia un correu electrònic de l'empresa Correos on s'explicava que l'usuari tenia un paquet per a recollir i que descarregués la informació d'aquell enviament fent clic a un enllaç, tal i com es pot veure en la figura 3.

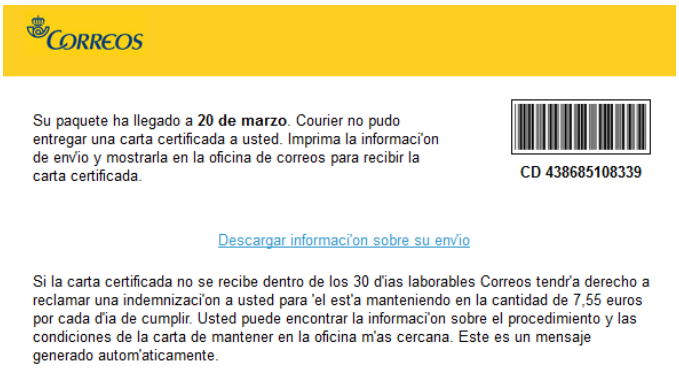


Figura 3. Correu electrònic suplantant a Correos [17]

O també suplantacions de companyies governamentals com ara l'Agencia Tributaria mitjançant un correu electrònic tal i com es mostra en la figura 4.

[16] SentinelOne. https://es.sentinelone.com/blog/7-common-ways-ransomware-can-infect-your-organization/

[17] Panda. MediaCenter. https://www.pandasecurity.com/es/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/

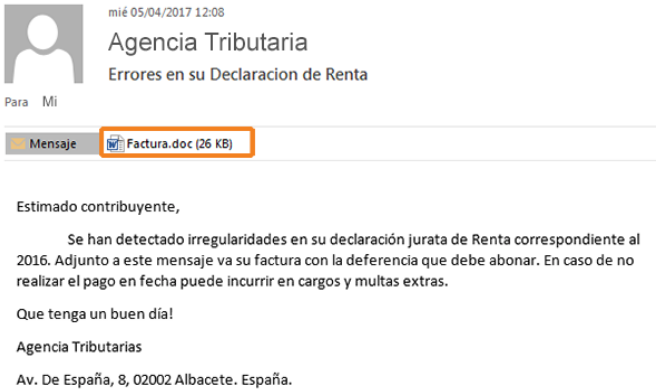


Figura 4. Correu electrònic suplantant l'Agencia Tributaria amb un arxiu maliciós [18]

2.1.2.2. Pàgines web malicioses

Un altre mètode d'infecció són les pàgines web malicioses o llocs webs que estiguin compromesos, ja que sigui fàcil introduir un codi maliciós.

Per infectar-se mitjançant aquest mètode, simplement l'usuari que acaba sent la víctima visita una pàgina web que sol visitar freqüentment. Però la diferència és que el lloc web compromès el redirigeix a una pàgina web maliciosa on se li demana fer una descarrega, per exemple, d'una versió nova d'algun navegador o reproductor multimèdia, però que realment se li està injectant el ransomware.

Aquest forma de redireccionar és bastant difícil de detectar si no s'analitza el codi subjacent de cada lloc web.

2.1.2.3. Protocol de escriptori remot (RDP)

El RDP (*Remote Desktop Protocol* en anglès) és un protocol d'escriptori remot de Microsoft [19] el qual proporciona funcions de pantalla i entrada remota a través de connexions de xarxa per a Windows. Actualment, la versió RDP només s'executarà mitjançant TCP/IP, i la connexió sol realitzar-se pel port TCP 3389.

Aquest protocol ha estat molt utilitzat sobretot en la pandèmia pel equips IT[20] per a poder accedir als ordinadors dels treballadors per

[18] Oficina de Seguridad del Internauta. https://www.osi.es/es/actualidad/avisos/2017/04/ahora-un-phishing-de-la-agencia-tributaria-quiere-secuestrar-tu-ordenador

[19] Microsoft. https://docs.microsoft.com/es-es/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

[20] IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2021/09/estos-son-los-tres-principales-vectores-de-ataque-del-ransomware

poder resoldre incidències de forma remota. Però segons el informe de Shodan[21] revela que 3.406.322 equips que estan connectats a la xarxa tenen aquest port obert, fet que ciberdelinqüents puguin aprofitar-ho mitjançant Shodan, trobar aquests dispositius i accedir així al servidor RDP fent ús de de força bruta. Un cop dins poden aconseguir els privilegis d'administrador, tenint així el control de la màquia i xifrar els arxius que desitgin.

2.1.2.4. Dispositius de memòria USB

Encara que aquest vector d'atac sigui més físic i no tant a distància, trobem que és important també destacar-lo i fer una breu explicació.

La raó és perquè la població està en constant moviment, va a aeroports, cafeteries, fires tecnològiques, etc. En tots aquests establiments podríem trobar-nos que alguna memòria USB oblidada per algú però que fos deixada expressament perquè la víctima amb la seva curiositat l'introduís al seu dispositiu, i al introduir-la el ransomware s'executaria immediatament, xifrant els arxius del dispositiu de la víctima.

2.1.2.5. Software vulnerable

Com s'ha comentat breument en l'apartat 2.1.1 d'aquest document, el maig del 2017 va tenir lloc l'atac ransomware WannaCry sobre ordinadors amb sistema operatiu Microsoft Windows. Aquest atac va aprofitar la vulnerabilitat d'aquest software per accedir als ordinadors connectats a la xarxa, xifrant així les dades de les víctimes.

Es recomana tenir la versió del sistema operatiu amb totes les actualitzacions existents per evitar problemes de vulnerabilitats conegudes. Al mateix temps, també es recomana tenir actualitzat qualsevol programari que se'n faci ús.

2.1.3. Tipus de ransomware

Avui en dia es coneixen diferent tipus de ransomware i segons un estudi realitzat per l'Institut Nacional de Ciberseguretat es pot classificar el ransomware en el següents tipus de menor a major importància: Hoax ransomware, scareware, bloquejadors de pantalla, ransomware xifrat i

[21] Shodan. https://www.shodan.io/search/report?query=remote+desktop

doxware. A continuació s'explicarà en què consisteix cada tipus de ransomware.

2.1.3.1. Hoax ransomware

La traducció del anglès de la paraula *hoax* significa engany. Per tant, com el propi nom indica, aquest tipus de ransomware consisteix en enganyar, simular que ha xifrat els arxius i no es té accés.

La forma de simular el xifrat es realitza mitjançant tècniques d'enginyeria social per extorsionar a la víctima i forçar-la a que pagui el rescat per poder recuperar les seves dades i que aquestes no siguin eliminades.
Però, realment el dispositiu no està compromès, si s'aconsegueix detectar aquest tipus de ransomware, senzillament no cal fer cas a les amenaces, per aquesta raó és el que té menys importància, però si es pot denunciar a les autoritats.

2.1.3.2. Scareware

Aquest tipus de ransomware consisteix en fer ús de l'esquer del fals software o programa de suport. La seva tècnica consisteix en fer saltar un anunci i informar sobre una suposada infecció per un virus, aportant una solució fàcil i ràpida, descarregant un programa de neteja de virus que quasi un sempre és un malware.

Senzillament, si apareix una mena d'anunci similar a l' entrar en una pàgina web visitada, només cal prestar atenció i no clicar a cap enllaç de l'anunci. L'únic problema que pot haver-hi és que el botó de tancament de la finestra pot ser fals i li estiguem donant a un enllaç per descarregar el malware.

2.1.3.3. Bloquejadors de pantalla

Els ransomware que són bloquejadors de pantalla consisteixen en fer que la víctima no pugui fer ús del seu dispositiu, bloquejant-li la pantalla, ja que se li mostra per pantalla completa un missatge mostrant les instruccions per desbloquejar el dispositiu.

En alguns casos, tal i com es pot observar en la figura 5, podien ser missatges fent-se passar per cossos de forces de seguretat en el que es demana un pagament per desbloquejar el dispositiu, però que òbviament aquest enviament de diners no arribaria a la policia sinó al ciberdelinqüent.

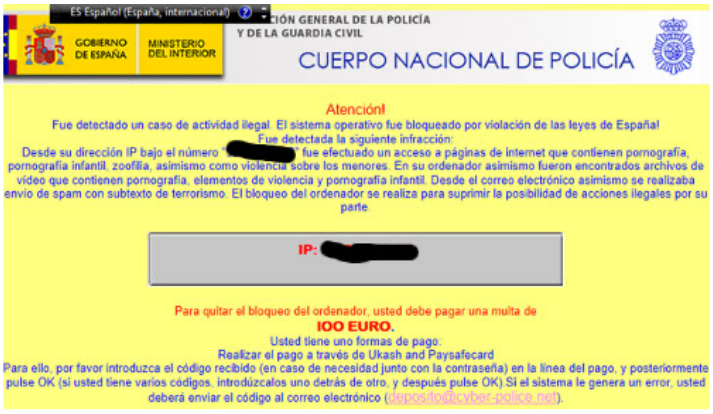


Figura 5. Exemple de pantalla bloquejant el dispositiu de la víctima[22]

En altres ocasions també podem trobar ransomware de bloqueig de pantalla que mostra un missatge on s'indica que diferents arxius han estat xifrats i indica el procés per recuperar-los. Però en realitat només bloqueja la pantalla i no han estat xifrats. Un exemple d'aquest tipus de bloqueig de pantalla el podem observar a la figura 6.

Figura 6. Exemple bloqueig de pantalla[23]

2.1.3.4. Ransomware de xifrat

El ransomware de xifrat ja no es tracta d'un atac que simula que han xifrat les nostres dades, tal i com fa el hoax ransomware. Aquest sí que xifra informació de dins del dispositiu de la víctima, i exigeix un rescat econòmic per a què l'usuari pugui recuperar les seves dades, però, realment no hi ha cap certesa que l'atacant li proporcioni

[22] Osi. https://www.osi.es/es/actualidad/avisos/2012/01/virus-muestra-un-falso-mensaje-del-cuerpo-nacional-de-policia

[23] Sensors Tech Forum. https://sensorstechforum.com/es/remove-noob-ransomware-restore-data/

quelcom a la víctima com per exemple amb la variant wiper que no retorna l'accés als arxius sinó que els elimina.

Per aquesta raó, el ransomware de xifrat és considerat com el més perillós de tots, segons l'Institud Nacional de Ciberseguretat.

2.1.3.5. Doxware

Aquest últim tipus de ransomware és el que aporta un benefici més ràpid als ciberdelinqüents com a conseqüència de fer ús de la tècnica *doxing*[24]. Aquesta consisteix en amenaçar a la víctima en fer públics els seus arxius personals, dades confidencials o converses emmagatzemades que ha xifrat l'atacant. És a dir, es tracta d'un ransomware que va més enllà del xifrat, xifra i amenacen fer públic allò xifrat podent fer comprometre a l'empresa si surt a la llum certa informació, tenint conseqüències legals.

La conseqüència i reacció que té aquesta amenaça cap a la víctima fa que aquesta es vegi sota més pressió, fent que acabi pagant el rescat, sent així un dels atacs més efectius econòmicament parlant per als ciberdelinqüents.

2.1.4. Ransomware as a service (RaaS)

A més, dels diferents tipus de ransomware als quals pot estar exposada una empresa o un usuari individual, avui en dia també podem trobar el que s'anomena Ransomware as a Service (RaaS) [25]. Aquest és un tipus d'atac que va augmentar significativament en el 2020.

El Ransomware as a Service és una classe de servei que ofereix kits de malware per poder dur a terme un atac ransomware.

Per tant, un grup de ciberdelinqüents desenvolupen un virus ransomware, el qual, com ja s'ha explicat en els apartats anteriors, xifrarà les dades de l'interior del dispositiu del usuari exigint un rescat a la víctima, i que el posaran a la venta al mercat negre, *dark web* en anglès. Això el que fa es que qualsevol persona, sense la necessitat de tenir coneixements tècnics, pot comprar-lo i el pot fer servir contra qui desitgi.

L'interessat en aquest servei simplement ha de pagar una subscripció mensual per poder fer ús del ransomware. La distribució del benefici obtingut pel

[24] Panda Security. https://www.pandasecurity.com/es/mediacenter/seguridad/doxware-evolucion-secuestros-digitales/
[25] Grupo Atico34. https://protecciondatos-lopd.com/empresas/ransomware-as-a-service-raas/

pagament del rescat pot ser de diferents maneres, en alguns casos l'afiliat es pot enduu des d'un 50% fins un 70% o, fins i tot, tot el benefici, com a conseqüència que alguns ciberdelinqüents només cobren per la creació del malware i l'ús del servei mitjançant la subscripció mensual, encara que el més habitual és que sigui un percentatge.

La diferència que trobem entre el ransomware i el RaaS és que qui duu a terme l'atac no és qui ha desenvolupat el malware, sinó que ho realitza qui ha contractat ell servei seguint els passos indicats pel desenvolupador. A més l'afiliat escull la víctima en funció del seu interès, principalment estratègic, per exemple una empresa competidora.

Aquest és el cas del ransomware Lockbit 2.0, que en el seu *dark web*, convida a formar part de la seva xarxa d'afiliats a que tinguin accés a xarxes corporatives o accés a informació interna que pogués ser d'utilitat. Per exemple si aquest servei ransomware l'utilitza una persona d'una empresa competidora, aquest pot tenir informació privilegiada de l'objectiu.

Per realitzar aquests tipus d'atac RaaS, els ransomwares més utilitzats són normalment el ransomware WannaCry, Sodinokibi, Satan, Egregor, Ryuk, Hostman, Encryptor, Alpha Locker, Netwaller, Cerber, Petya o FLUX, etc. Però en aquest 2021 un dels més utilitzats ha estat el ransomware Lockbit, i en aquest any ha sorgit el Lockbit 2.0, en la que els atacants han inclòs la funció de robar informació coneguda com *StealBit*, que permet descarregar automàticament i de forma molt ràpida els arxius de les víctimes al seu blog per a ser publicades. A més a més, es considera que conté el software de xifrat més ràpid (373MB/s)[26]. Per exemple, un cas real que va succeir el passat any 2021, l'empresa consultora multinacional Accenture va ser víctima d'un atac ransomware Lockbit 2.0. La companyia Cyble afirma que els ciberdelinqüents van robar 6TB d'informació de l'empresa, demanant un rescat de 50 milions de dòlars.

Un altre exemple seria el ransomware Sodinokibi, el qual va protagonitzar el rècord de la demanada de rescat més alta (10 milions de dòlars), es ven com a RaaS mitjançant un model de afiliació i comissió. Aquest explota la vulnerabilitat de Oracle WebLogic per poder accedir al dispositiu de la víctima, i un cop dins intenta adquirir drets d'administrador per accedir d'aquesta manera a tots els arxius sense restriccions. Per adquirir aquests dret d'administrador, ho farà mitjançant l'exploit CVE 2018-8453[27] basat en la vulnerabilitat d'elevació de privilegis de Windows quan el component Win32k no gestiona

[26]WeLiveSecurity. https://www.welivesecurity.com/la-es/2021/08/12/accenture-es-victima-de-ataque-del-ransomware-lockbit-2-0/
[27]Pandasecurity. https://www.pandasecurity.com/emailhtml/2007-CAM-RANSOMWARE-AD360-WG/2006-Report-Sodinokibi-ES.pdf

adequadament els objectes en la memòria. En la següent imatge podem apreciar la informació que INCIBE[28] dona sobre aquesta vulnerabilitat.

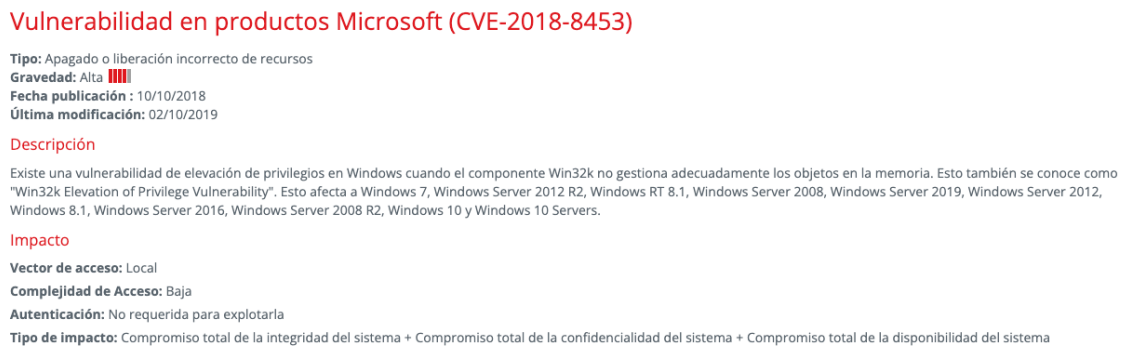


Figura 7. CVE 2018-8453

Després encripta les diferents dades mitjançant AES[29] i l'algoritme Salsa20[30]. L'AES s'utilitza per a encriptar els secrets de la sessió o dades que s'envien al servidor de control, mentre que les dades individuals s'encripten utilitzant la seguretat Salsa20. A més a més, el ransomware Sodinokibi utilitza un algoritme d'intercanvi crucial Diffie-Hellman[31] de corba el·líptica per a crear i intercanviar claus de xifrat. Per a què sigui més entenedor ens podem basar en el següent esquema que explica les diferents parts en que està formada el xifrat [27].

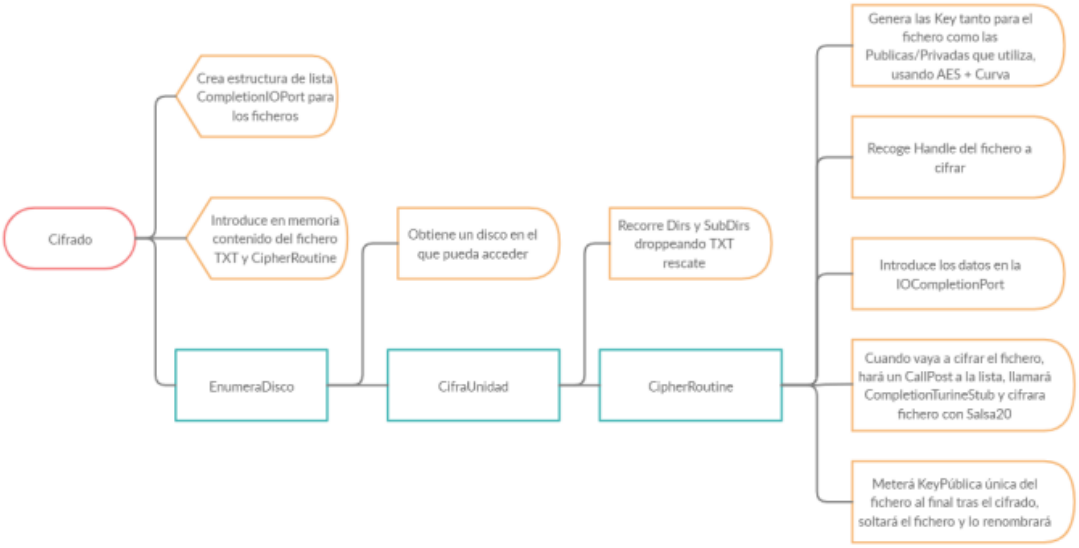


Figura 8. Esquema rutina de xifrat

[28] INCIBE-cert. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2018-8453
[29] Boxcryptor https://www.boxcryptor.com/es/encryption/
[30] Kripkit https://kripkit.com/salsa20/
[31] Grupo Atico34. https://protecciondatos-lopd.com/empresas/algoritmo-diffie-hellman/

2.2. Conscienciació sobre el ransomware a les PIMEs

Un cop explicat en els apartats anteriors el concepte de ransomware, els diferents vectors d'atac, els diferents tipus que hi ha i com ha evolucionat cap a Ransomware as a Service, és el moment d'introduir a les PIMEs i autònoms la importància d'estar conscienciats davant un atac ransomware, prendre les mesures preventives adequades per evitar l'impacte econòmic, reputacional o jurídic que comportaria un atac ransomware.

En els següents apartats exposarem l'entorn teòric i característiques de les PIMEs per entendre en quin entorn desenvolupen les seves activitats i quines limitacions econòmiques les caracteritzen. A més d'explicar breument la influència que ha tingut la pandèmia del Covid-19 en els atacs ransomware i com s'han pogut veure afectades aquest tipus d'empreses, podent extreure les diferents vulnerabilitats existents per poder aplicar unes mesures preventives.

2.2.1. Situació de les PIMEs

La definició de PIME s'especifica en l'annex I del Reglament (UE) nº651/2014 de la Comissió[32]. En aquest document, es defineixen el diferents tipus d'empresa que engloben les PIMEs i que es pot dividir entre micro, petita o mitjana empresa. En la taula 4 es mostra quan es considera que es cada tipus d'empresa segons el nombre de treballadors i el volum de negoci.

Categoría de empresa	Efectivos	Volumen de negocio	Balance general
Mediana	<250	<= 50 millones EUR	<= 43 millones EUR
Pequeña	<50	<= 10 millones EUR	<= 10 millones EUR
Micro	<10	<= 2 millones EUR	<= 2 millones EUR

Taula 4. Classificació PIMEs segons nombre de personal i volum econòmic

Per tant, com ja es conegut, una PIME té un nombre de treballadors reduït i el pressupost d'aquestes empreses no és molt elevat.

Aquestes característiques fan que invertiran més pressupost en l'execució del producte a comercialitzar que en ciberseguretat, ja que aquestes consideren que no són objectius de ciberatacs, però la realitat és totalment el contrari.

Tal i com s'ha comentat en l'apartat 1.1 d'aquest estudi, les PIMEs representen el 99,8% del teixit empresarial espanyol[33], les quals generen un percentatge de

[32] Gobierno de España. Ministerio de Industria, Comercio y Turismo. http://www.ipyme.org/es-ES/DatosPublicaciones/Paginas/DefinicionPYME.aspx

[33] Delfos. https://www.delfossistemas.com/ataque-ransomware-ciberamenaza-mas-comun-para-las-pymes/

feina del 60%. És a dir, que les PIMEs són una part molt important del motor econòmic d'Espanya. I pensar que per la seva mida no són objectius interessants pels atacants, és un error, ja que tenen més mancances en seguretat que les grans companyies i poden tenir carències de personal per poder-se defensar davant un atac ransomware. Segons un informe[34] del gegant del buscador, s'afirma que 8 de cada 10 PIMEs espanyoles no es consideren un objectiu atractiu per als ciberdelinqüents.

De fet, un estudi elaborat l'any 2021 per la companyia Hiscox, mostra que el 58% de les companyies que han rebut un atac ransomware han pagat el rescat, fent que els ciberdelinqüents inverteixin aquests beneficis per millorar els seus atacs, fent que aquesta situació no tingui fi.

2.2.2. Afectació Covid-19

La pandèmia global del covid-19, va trasbalsar ràpidament la forma de treballar de les empreses, independentment de la seva mida. Va comportar un confinament total de la població, fent que si les empreses volien continuar duent a terme el seu negoci, dins les possibilitats que tenien, els treballadors d'aquestes empreses havien de teletreballar, quan potser mai s'havia teletreballat en aquella empresa.

Els treballadors havien de treballar des de les seves cases amb ordinadors proporcionats per les empreses o, en molt casos, com les empreses no tenien ordinadors per poder proporcionar als treballadors, aquests van fer ús dels seus ordinadors personals. Però aquests aspectes haurien d'estar integrats en les polítiques de seguretat de l'empresa per poder combatre riscos corporatius com el frau, ciberdelictes i extorsió.

Tot aquest conjunt va aportar noves vulnerabilitats als sistemes de treball que els ciberdelinqüents podien aprofitar per extreure's un benefici, ja que tot es feia telemàticament.

L'ús de connexió remota (RDP) als ordinadors de les oficines, no fer ús de VPN en les PIMEs, va fer que en el 2021 l'atac ransomware fos la ciberamenaça més comú per a les PIMEs[30].

Per tant, per a què una PIME pugui estar preparada per defendre's d'un atac ransomware, necessita d'una inversió que durant molts anys no s'ha vist la necessitat, però en aquests dos últims anys, arrel de la pandèmia, ha fet obrir els ulls a les empreses.

[34] Businessinsider. https://www.businessinsider.es/ciberseguridad-pymes-claves-experto-google-949839

2.2.3. Estudi vulnerabilitats PIMEs

Segons l'informe Escudos[35] més de 300.000 PIMEs va patir ciberatacs, on s'advertia que la principal vulnerabilitat solen ser els errors humans. I es que mitjançant enginyeria social i *phishing*, per exemple, es com arriben molts dels arxius maliciosos que són el mitjà per realitzar el ransomware per xifrar dades confidencials de l'empresa i així poder-la extorsionar, demanant un rescat per desbloquejar altre cop els sistemes i evitar que totes aquestes dades, que han estat robades pels ciberdelinqüents, acabin a la *dark web*.

A part de l'error humà que pot existir en les PIMEs, com a conseqüència de les seves limitacions econòmiques, una altra vulnerabilitat que podem trobar és la falta formació dels treballadors en l'àmbit de la ciberseguretat per saber afrontar un ciberatac i minimitzar així la probabilitat de patir un atac ransomware en aquest cas.

Si seguim analitzant les possibles vulnerabilitats, ens adonem que avui en dia les PIMEs són el principal objectiu d'un atac ransomware com a conseqüència que si les comparem amb grans companyies, el nivell de seguretat és inferior en una PIME i manquen de recursos i personal per poder defendre's d'un atac.

Un altra vulnerabilitat a considerar és tenir un sistema d'autenticació dèbil, és a dir que les contrasenyes utilitzades no tinguin un nivell de seguretat alt o que no es canviïn i sempre es faci ús de les mateixes.

Si continuem analitzant, les PIMEs poden no tenir ben definides polítiques de control d'accés per accedir a certa informació. Fent que qualsevol usuari pugui entrar a informació confidencial o dades vulnerables fent que pugui haver una fuga d'informació que un ciberatacant pot aprofitar per introduir-se dins del sistema sent un usuari normal de treballador.

També podem trobar l'altre opció que sí que es demanin certs privilegis per accedir a certa informació de l'empresa, però si la PIME es atacada mitjançant injeccions SQL, aprofitant les vulnerabilitats de l'aplicació web per a enviar consultes de bases de dades no autoritzades, l'atacant pot entrar en el sistema, escalar privilegis i tenir accés a les dades confidencials podent-les xifrar i executar un atac ransomware.

[35] Noticias jurídicas. https://noticias.juridicas.com/conocimiento/tribunas/16792-riesgos-legales-del-teletrabajo-que-debemos-conocer/

2.2.4. Impacte d'un atac ransomware

Si una PIME es veu infectada per un ransomware, l'atacant xifrarà els arxius i les dades confidencials de la companyia i l'exigirà un rescat per poder recuperar aquestes dades abans que arribin a filtrar-se a la dark web, on si arribés, l'impacte que tindria sobre l'empresa seria molt negatiu. Podria afectar la reputació de la PIME i, en conseqüència, es veuria en possible risc la confiança dels clients cap aquesta empresa a més de les conseqüències econòmiques i jurídiques que podria patir la companyia si es filtrés informació amb dades personals.

Per tant, podem apreciar tres diferents tipus d'impacte que tindria l'atac ransomware sobre una PIME: econòmic, reputacional i jurídiquic.

L'impacte econòmic que comportaria un atac ransomware és que durant el temps que els arxius i dades estan xifrades, l'empresa no pot dur a terme el seu negoci ja que els ordinadors han estat infectats i al no tenir accés als arxius queden inoperatius. Per tant, l'operativa de l'empresa es veu obligada a estar paralitzada durant aquest període de temps, fent que no entrin guanys durant aquests impàs fins que es pugui restaurar tot al punt de partida abans de l'atac.

Un espai de temps que podria resultar indefinit si no es gestiona de forma correcta.

A més d'aquesta pèrdua econòmica com a conseqüència de tenir parat el negoci, se li ha de sumar la quantitat de rescat que pagarà la empresa, en cas que ho faci. Tot i això, no es recomana pas pagar el rescat ja que no hi ha cap seguretat de tornar a tenir accés a tots els arxius.

A més, l'empresa que pagués el rescat tindria més probabilitat de tornar a ser atacada pels ciberatacants, ja que han pogut apreciar que aquesta empresa tornaria a pagar el rescat.

L'impacte reputacional o d'imatge, que tindria com a conseqüència d'haver patit un atac ransomware, pot donar lloc a una imatge negativa de l'empresa ja que no ha estat capaç de protegir-se davant aquest tipus d'atac, i pot condicionar a la pèrdua de clients per la por a què torni a ser atacada, i tenint com a conseqüència una reducció de peticions per part dels clients.

Per últim, però no menys important, l'impacte jurídic que podia patir la PIME com a conseqüència d'aquest ciberatac són les sancions definides en el Regalment General de Protecció de Dades (RGPD), si hagués alguna fuga d'informació de caràcter personal, per exemple, o si a més aquestes dades a les que ha tingut accés el ciberdelinqüent són publicades o venudes a tercers,

les conseqüències pera l'empresa podrien ser més greus . A més d'incomplir els contractes amb els clients, penalitzacions per la no continuïtat dels serveis que poden oferir a tercers, etc.

El problema és que la majoria de PIMEs continua tenint el pensament reactiu, i només se n'adona de la necessitat d'un pla per protegir l'empresa tecnològicament un cop ja ha patit l'atac.

Podem concloure que l'impacte no és de poca importància, i el període de temps que el negoci està aturat pot prolongar-se en el temps, tenint un gran impacte econòmic que després pot costar afrontar. Aquest fet fa tenir una visió més clara dels beneficis de tenir una mesures preventives i un pla de continuïtat del negoci en cas d'infecció. És una inversió necessària que s'ha de realitzar cap a ciberseguretat, si volem que no afecti al negoci.

2.3. Mesures preventives davant un atac ransomware

Per tot el comentat en els apartats anteriors, és molt important que les empreses i sobretot les PIMEs, que poden tenir més dificultats de recuperació que les grans empreses, adoptin unes bones pràctiques preventives per evitar ser víctimes de ciberdelinqüents, i d'aquesta manera mantenir els sistemes de l'empresa per a què no siguin tècnicament vulnerables.

A continuació, s'exposaran un conjunt de mesures preventives que poden aplicar les PIMEs per prevenir-se d'un atac de tipus ransomware.

- Formació i conscienciació

  En una empresa, el motor del seu negoci són en gran part els seus treballadors. Sense ells, molt probablement l'empresa no podria existir ni realitzar el seu negoci. Però per a què aquest es pugui realitzar de forma òptima i no veure's afectat per un atac ransomware, és molt important dedicar uns recursos a la millora de la formació i conscienciació en matèria de ciberseguretat pels empleats.

  Per fer-ho, es poden fer campanyes de propagació explicant que és un atac ransomware, com es propaga i què poden fer els treballadors per evitar-ho.

A més a més, està a disposició de tot tipus d'empreses el kit de conscienciació d'INCIBE[36]. Un kit on els empleats poden accedir a recursos didàctics i eines d'entrenament per evitar incidents de ciberseguretat que poden afectar a l'empresa a la qual treballen, tenint així, el poder a les seves mans per poder evitar l'atac. I, un aspecte molt important pot ser utilitzat en PIMEs de qualsevol sector, ja que no es necessari tenir prèviament coneixements tècnics.

Figura 9. Kit conscienciació per empreses

- Còpies de seguretat periòdiques (*Backups*)

Una altra mesura preventiva davant un atac ransomware, i probablement una de les més importants, és realitzar còpies de seguretat periòdiques, *backups* en anglès, per poder recuperar la normalitat en l'empresa en el menor temps possible, restaurant així el negoci de l'empresa.

L'Institud Nacional de Ciberseguretat dóna unes recomanacions bàsiques que poden seguir les empreses pel que fa a còpies de seguretat. D'aquestes exposarem les que poden ser més factibles per a les PIMEs.

El que s'ha de tenir clar és que si es produís un atac ransomware, l'empresa es troba amb tres opcions: assumir que les dades s'han perdut, pagar el rescat o la última i la que té més sentit, recuperar les dades mitjançant una còpia de seguretat. Però només tenir una còpia no seria del tot segur ja que podria fallar. Per això la importància de la redundància i tenir més d'una còpia, INCIBE en recomana tres, en diferents discs durs o USB externs, que no estiguin connectats a la xarxa, per exemple, pot fer que l'activitat del negoci de la PIME no es vegi afectat pràcticament si se li produís un atac ransomware gràcies a aquesta mesura preventiva.

És important el fet que aquest disc dur o USB sigui extern i no estigui connectat a la xarxa de l'organització, ja que algun ransomware com ara el CryptoLocker que es capaç de recórrer les unitats de xarxa del equip,

[36] Incibe. Kit de conscienciación. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

podria infectar un USB connectat al sistema i fer que aquella còpia de seguretat no fos útil ja que quedaria inutilitzada.

Però per estar segurs que tenim unes còpies de seguretat útils en cas que es produís un atac, és important assegurar que funcionen correctament i sabríem com recuperar aquelles dades. Per aquesta raó, és important que cada un cert període de temps es revisin que aquestes còpies estan en bon estat.

- Navegació segura (VPN)

  Com s'ha comentat anteriorment en aquest estudi, la pandèmia del Covid-19 ha fet augmentar el teletreball i, en conseqüència, es realitzen connexions a la intranet de l'empresa o a l'equip corporatiu de l'empleat.

  Per evitar ser atacats, una altra mesura preventiva, indicada per a aquestes situacions és configurar la connexió remota (RDP) perquè només sigui accessible des de les xarxes privades virtuals (*Virtual Private Network*, VPN) i fent ús de dos factors d'autenticació.

  D'aquesta manera, els empleats de la PIME podran accedir als seus documents i navegar de forma segura, ja que les xarxes privades virtuals són un tipus de connexió de xarxa on les dades viatge xifrades i d'aquesta manera els atacants no poden veure el seu contingut.

- Mantenir software actualitzat

  Una altra mesura relativament senzilla, però que pot ajudar molt a prevenir un atac ransomware és tenir tots els tipus de software actualitzat, és a dir, tenir el sistema operatiu amb les últimes actualitzacions, farà que vulnerabilitats conegudes pels ciberatacants siguin arreglades i no puguin ser utilitzades per aquests per poder realitzar el ciberatac, i en conseqüència, que el sistema tingui menys vulnerabilitats.

  Però no només el sistema operatiu dels diferents ordinadors que es fan ús a l'empresa ha d'estar actualitzat a l'última versió, sinó també es recomana tenir actualitzats els navegadors web o qualsevol solució de seguretat. Per tant, la millor forma de tenir sempre tot tipus de software a l'última versió, és tenir la instal·lació d'actualitzacions configurada per a que es realitzi automàticament.

- Firewall

  Com segurament moltes empreses han d'oferir algun servei a través d'Internet als seus clients, aquestes han de donar accés als seus servidors als clients, per tant la xarxa s'ha d'obrir però de forma segura, sense desprotegir la resta de la xarxa de l'empresa.

  Una forma de prevenció és fer us de tallafocs o *firewall*, el qual és un sistema de seguretat que bloquejarà o permetrà l'entrada o sortida a la xarxa de l'empresa depenent les regles que es defineixin.

  Actualment, existeixen *firewalls* de codi obert [37], *open source* en anglès. Aquests solen ser gratuïts, d'alta eficiència i es poden fer servir per a ús corporatiu. Alguns d'aquests firewalls de codi obert que trobem són per exemple *pfSense* [38], *IPfire* [39] i *OpenSense* [40], entre altres. Per fer ús d'aquests, simplement s'ha de dirigir a la pàgina web d'aquests *firewalls* de codi obert i descarregar-se'l. Per tant, són una bona estratègia de prevenció per a PIMEs que proporcionen un servei però volen continuar protegint la xarxa.

- Zona desmilitaritzada (DMZ)

  Tot i que el *firewall* és un gran sistema de prevenció que controla qui pot accedir i qui no als servidors de l'empresa, pot ser que algun atacant aconsegueixi sobrepassar aquest *Firewall*. Si això succeeix tindria una afectació bastant greu, ja que l'atacant podria comprometre al servidor o altres dispositius que es trobessin a la xarxa de l'empresa.

  Per prevenir i evitar que succeeixi aquesta situació dins la PIME existeixen les xarxes DMZ, zona desmilitaritzada. Aquesta xarxa és una xarxa aïllada de la resta de la xarxa de la companyia. D'aquesta manera si algun ciberatacant aconsegueix passar el *firewall* i accedir als servidor que estan accessibles des d'Internet, si que tindrà accés a aquells servidors però no a la resta de la xarxa de l'empresa tal i com es pot apreciar en la figura 10.

[37] Geekflare. https://geekflare.com/es/best-open-source-firewall/
[38] pfSense. https://www.pfsense.org/download/
[39] IPFire. https://www.ipfire.org/
[40] OpenSense. https://opnsense.org/

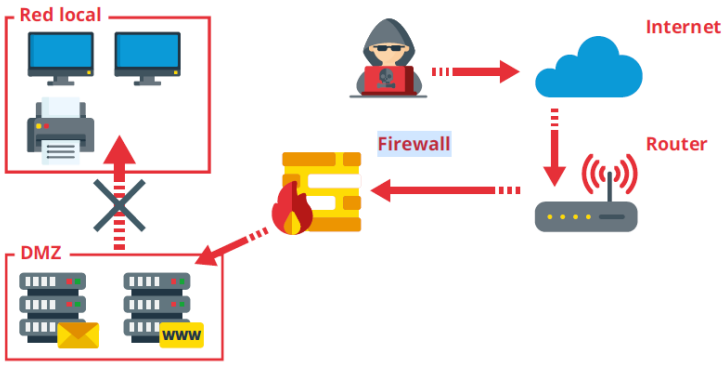


Figura 10. Esquema xarxa DMZ[41]

Per posar un exemple, els sistemes que haurien d'estar en una xarxa DMZ podrien ser els servidor de correu electrònic, els Servidors de Noms de Domini (DNS) i servidors VPN.

- Control d'accessos

Podem afegir el control d'accessos com a mesura preventiva que podria aplicar perfectament una PIME, evitant així que els treballadors tinguin més privilegis dels que necessiten.

Les mesures que englobarien tenir un control d'accés al sistema dins l'empresa serien tenir comptes amb privilegis limitats, contrasenyes robustes, autenticació de doble factor o múltiple factor (MFA) [42], definir el nombre màxim d'intents per accedir-hi al sistema, fer ús de *white list*[43] i tenir un accés controlat a les unitats de la xarxa[44]. A continuació, es detallarà breument el perquè fer ús de cadascuna d'aquestes mesures de prevenció de control d'accessos.

Tenir comptes amb privilegis limitats, significa que els treballadors de la PIME no facin ús de l'usuari Administrador i que facin ús de comptes d'usuari amb els permisos més limitats. Gràcies a aquesta mesura, en cas d'atac ransomware, i aconsegueix entrar en un dispositiu on l'usuari

[41] Incibe. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario
[42] Bit Life Media. https://bitlifemedia.com/2022/04/doble-factor-autenticacion-seguridad/#:~:text=El%20sistema%20de%20doble%20factor,un%20c%C3%B3digo%20de%20seguridad%20num%C3%A9rico.
[43] Grupo Atico34. https://protecciondatos-lopd.com/empresas/lista-blanca-gris-negra/#:~:text=En%20lugar%20de%20crear%20una,se%20demuestre%20que%20es%20aceptable.
[44] CCN-CERT. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

és administrador, l'atacant podria aconseguir el control de l'equip i de la resta transmetent-se per la xarxa de l'empresa.

Fer ús de contrasenyes robustes, les quals haurien de ser d'una longitud considerablement llarga i incloure majúscules, minúscules, números i símbols, a més de ser canviada amb una certa periodicitat, per exemple cada 3 mesos. La raó per la qual es útil aquesta mesura és que un atacant per obtenir la contrasenya d'un usuari ho sol realitzar mitjançant força bruta o mitjançant un atac per diccionari, és a dir fent ús de les contrasenyes més habituals, per exemple la contrasenya 1234. Si la PIME no fa ús de contrasenyes habituals o aquesta canvia cada cert període de temps reduirem la probabilitat que puguin atacar a l'empresa per mitjà d'aquesta vulnerabilitat.

Establir un nombre màxim d'intents per accedir al sistema, redueix el nombre d'atacs de força bruta i per diccionari que hem comentat anteriorment.

A més a més, de les contrasenyes robustes o limitar el nombre d'intents per poder accedir al sistema, també es pot fer ús de l'autenticació de doble factor o múltiple factor (MFA) quan s'intenta accedir als comptes des treballadors. Aquesta afegeix un nivell de seguretat més a l'accés dels comptes dels usuaris al tenir dos o més sistemes d'identificació diferents. Ja que si les credencials dels treballadors són robades o filtrades, si es té una autenticació de doble factor, pot contribuir a salvaguardar la informació.

Si la PIME en qüestió fa ús de polítiques *white list*, consisteix en crear unes llistes blanques amb les IPs dels equips que se'ls permet fer ús del servei. Per fer-ho s'ha de configurar correctament al firewall aquestes llistes blanques.

Finalment, l'última mesura de control d'accessos, tracta de tenir un accés controlat a les unitats mapejades de la xarxa. Si no es té aquesta mesura de control, en cas d'infecció el xifrat es produiria en totes les unitats de xarxa mapejades dins l'equip de la víctima. Però restringint els privilegis d'escriptura a la xarxa, l'impacte es veurà mitigat.

- Control de la instal·lació de programes

Per evitar que un treballador de manera no intencionada descarregui un programa infectat provinent de pàgines webs externes a l'empresa, s'ha d'introduir en les polítiques de la companyia on s'indiqui que els

treballadors no descarreguin ni instal·lin programes no permesos, filtrant la navegació i l'accés només a pàgines webs en les que es pot confiar.

Alguns sistemes operatius, com és el cas de Windows ja incorporen sistemes de protecció contra el ransomware. En la figura 11 es pot apreciar la protecció contra ransomware ja integrada.

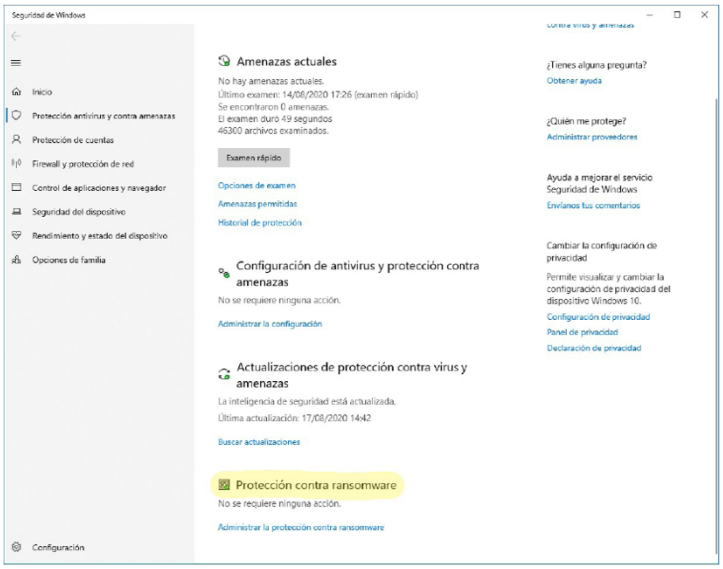


Figura 11. Protecció contra ransomware integrada a Windows 10

- Bona configuració del correu electrònic

Com ja s'ha comentat en parts anteriors d'aquest estudi, el correu electrònic és un dels principals mètodes d'infecció mitjançant la descarrega d'arxius maliciosos que pretenen ser d'algú de confiança però en realitat li estan suplantant la identitat. Per tant, aquí també té molta importància la conscienciació i formació dels treballadors per evitar que caiguin en aquesta trampa.

No obstant això, també és molt important tenir una bona configuració del correu electrònic que eviti que puguin succeir aquestes situacions. Per fer-ho, els servidors de correu electrònic han de:

- Activar un filtre de *spam*: D'aquesta manera s'evita que arribin al correu dels treballadors correus de *phishing*. En alguns casos, alguns proveïdors de domini ja porten un filtre *spam* que pot ser activat per a totes les direccions de correu electrònic de la companyia estalviant costos.

- Ús d'autenticació de correus entrants: D'aquesta manera s'evitarà la suplantació o *spoofing* de correus electrònics.

- Fer ús de previsualitzadors de documents d'Office: En d'obrir un document directament amb office fent servir macros, millor deshabilitar-les i fer us de les alternatives online.

- Escanejar el correu tant d'entrada com de sortida: Fent ús d'un antivirus per així l'empresa ser capaç de detectar arxius potencialment amenaçadors que poguessin comprometre a l'activitat de la companyia.

- Fer ús d'entorns virtuals: En cas que sigui estrictament necessari obrir algun arxiu sospitós, és recomana no fer-ho al dispositiu de l'empresa, on hi ha dades sensibles o confidencials de la companyia, sinó fer ús d'entorns virtuals com *Sandbox*[45] per a versions de Windows 10 i sinó es fa ús d'aquest sistema operatiu dins la PIME es pot fer ús de *Cuckoo*[46].

- Desactivar la visualització en format HTML: El format HTML permet als programes que han estat desenvolupats amb el llenguatge de programació *JavaScript* redirigir el navegador web a una pàgina maliciosa que infecti el dispositiu. Això s'ha de realitzar sobretot, en els comptes de correu que siguin crítiques o a disposició del públic per contactar amb l'empresa.

- Desactivar complements o extensions no utilitzades de navegadors

  Mantenir sempre els navegadors webs actualitzats a l'ultima versió per evitar tenir vulnerabilitats conegudes d'aquests navegadors i poder navegar de forma segura.

- Mostrar extensions de l'arxiu

  Una mesura preventiva, senzilla a realitzar però que pot ser molt útil per prevenir un atac ransomware, és mostrar les extensions dels arxius que reben per correu electrònic. Aquests poden ser arxius maliciosos, i és que alguns ransomwares com ara el CryptoLocker o CryptoTorrent[47] utilitzen fitxers amb dobles extensió, com ara.pdf.exe. Si el sistema del dispositiu de l'empresa no mostra l'extensió principal d'aquell fitxer, pot donar a creure que es tracta d'un arxiu pdf i no d'un executable. En la

[45] Digitaltrends. https://es.digitaltrends.com/computadoras/como-usar-windows-sandbox/
[46] Cuckoo. https://cuckoosandbox.org
[47] Medidas de seguridad contra ransomware. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

següent imatge es pot observar com mostrar les extensions de fitxers coneguts.

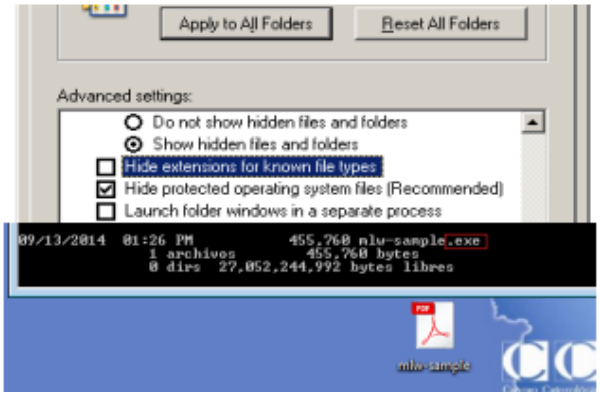


Figura 12. Mostrar extensió de fitxers coneguts

- Tenir un pla de continuïtat del negoci

  En les següents seccions d'aquest estudi a profunditzarem en la realització del pla de continuïtat del negoci. Però, evidentment, aquest s'ha de realitzar preventivament per així saber com actuar en cas d'incident.

  En aquest document s'ha de definir qui realitzarà la gestió de l'incident dins l'empresa, s'indicarà la documentació per saber quan és un estat d'activitat normal de negoci i quan s'ha sofert un incident. En cas d'haver sofert un, es classificarà l'incident segons el seu origen i criticitat. Aquest document ha de recollir els passos a seguir per a la recuperació de l'activitat, amb qui ha de contactar l'empresa per a saber com recuperar les dades, com podria ser ara contactar amb INCIBE-CERT[48].

  Finalment, recollirà la informació dels equips afectats, accions presses i resultats per poder detectar millores que es podrien realitzar en un futur.

[48] INCIBE-CERT. https://www.incibe-cert.es/respuesta-incidentes

3. Pla de contingència en cas d'infecció

En una empresa, independent del seu tamany, no només ha de tenir unes mesures de prevenció contra el ransomware, sinó també un pla de contingència que contingui les mesures adients per combatre la infecció i erradicar-la i així poder tenir una continuïtat del negoci.

Al cap i a la fi, per a qualsevol empresa, incloses les PIMEs, és important protegir els diferents processos del negoci mitjançant un conjunt de tasques que permetin recuperar l'empresa després d'un incident, com ara en el cas de ser infectat per un ransomware, en un impàs de temps que no comprometi la continuïtat de l'organització. Podent donar una resposta planificada, mitigant l'impacte que podria ocasionar la pèrdua d'informació.

En aquesta part de l'estudi, volem poder donar unes guies d'actuacions que haurien de realitzar les PIMEs en cas de ser afectades per un atac ransomware. D'aquesta manera tindran un pla de contingència assequible per a aquest tipus d'empresa i sabran com actuar en cas d'ocurrència d'atac ransomware, evitant pèrdues de temps i econòmiques innecessàries, permetent la continuïtat del negoci.

Per poder gestionar una situació d'aquestes característiques, ha d'estar dividida en quatre fases, segons el *Centro Criptológico Nacional* [49]: fase de preparació, fase de detecció, anàlisi i identificació, fase de contenció, mitigació i recuperació, i activitat post-ciberatac.

Figura 13. Fases pla de resposta a ciberincidents

En els següents apartats s'explicarà en què consisteix cada fase i quines accions s'hauran de duu a terme.

[49] Centro Criptológico Nacional. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

3.1. Fase de preparació

En aquesta fase de preparació, com bé el nom indica s'ha de preparar l'organització amb els mecanismes necessaris per poder recuperar-se en cas d'atac de la manera més ràpida possible.

En concret, per poder fer front a un incident de tipus ransomware, s'haurien de definir unes pautes a realitzar, basades en el document INCIBE [50]:

- Definir qui gestiona els incidents dins de l'empresa.
- La persona que gestioni els incidents haurà de comunicar a la direcció de l'empresa per saber l'estat de la situació.
- Definir el que s'entengui per activitat normal que permeti detectar incidents.
- Documentar amb qui s'ha de posar en contacte l'empresa al patir algun incident, com per exemple amb INCIBE-CERT de INCIBE, centre de resposta a incidents de seguretat.
- Definir l'existència d'una valoració de l'afectació de l'estat dels equips en cas d'incident.
- Tenir documentat els diferents clients de l'empresa i proveïdors que s'haurien de notificar en cas d'incident.

3.2. Fase de detecció, anàlisi i identificació

En aquesta fase, l'objectiu principal serà poder detectar l'amenaça, analitzar-la i classificar l'incident per poder dir la criticitat dels sistemes afectats segons el tipus de ransomware que sigui i del seu origen.

La correcta implantació de les mesures tant preventives, com les descrites en la fase de preparació, ajudaran a detectar les possibles escletxes de seguretat, tenint un procediment d'actuació en cas de detecció de l'amenaça i desencadenant els processos de notificació corresponents.

Primer de tot, en aquesta fase s'ha d'identificar, detectar, si a l'organització està tenint lloc un atac ransomware. Molts cops, però, el problema dels atacs ransomware és que es detecta que s'ha estat atacat per aquest ciberatac, quan

[50] INCIBE. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

els ciberatacants ja han demanant el rescat o els documents ja han estat xifrats. Per tant, podem apreciar que la velocitat de detecció és un factor molt important en aquest tipus de ciberamenaces, ja que una bona detecció a temps, fa que es pugui evitar l'extensió del ransomware dins de la xarxa de la PIME o, fins i tot, arribar abans de que tots els arxius crítics hagin estat xifrats.

Els indicis que ens indiquen que podem estar davant d'un ciberatac, provenen dels precursors i indicadors. Els precursors són indicis que indiquen que pot ocórrer un incident en el futur, mentre que un indicador és un indici de que un incident pot haver ocorregut o està ocorrent ara mateix. Alguns indicadors podrien ser l'alerta generada per un software antivirus, detecció d'un nombre importat de correus electrònics amb un contingut sospitós, etc.

A continuació de la fase de detecció ha d'haver una fase d'anàlisi i identificació. És a dir, en el moment que es detecti que l'empresa, en aquesta cas una PIME, ha estat o està sent atacada per un ransomware, s'ha de definir de quin tipus i criticitat és aquest ciberincident.

Segons la CCN-CERT hi ha diferents factors que s'han de considerar alhora de classificar els ciberincidents i poder així determinar la seva perillositat i prioritzar l'actuació sobre aquest.

Per classificar l'atac ransomware, es farà ús de la taula proporcionada per el CCN que es pot trobar en l'Annex I. Segons aquesta taula, el ransomware es pot classificar com a compromís de la informació. De tipus d'incident, es definiria com a modificació no autoritzada de la informació, tal i com es pot observar en la següent imatge.

Compromiso de la información	**Acceso no autorizado a información**	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.

Figura 14. Classificació ransomware dins dels ciberincidents

En el CCN-CERT també se'ns indica el nivell de l'impacte d'aquesta ciberincidència depenent de l'afectació d'aquesta. En l'Annex II es pot veure la taula on es defineix aquest nivell d'impacte.

Finalment, un cop s'ha detectat un ciberincident de tipus ransomware, s'ha analitzat i identificat la seva criticitat en funció de l'afectació que estigui tenint en l'empresa, es passarà a la fase de contenció, resolució i recuperació.

3.3. Fase de contenció, resolució i recuperació

- Contenció i comunicació

Si una PIME, desgraciadament es veu afectada per un atac ransomware i ha estat infectada per aquest malware, en la fase de contenció el primer que s'ha de realitzar és desconnectar els equips [51] de la xarxa, els quals es creguin infectats.

D'aquesta manera s'aconsegueix un aïllament de la resta d'equips que formen l'empresa, evitant així la propagació cap a altres elements de la companyia.

Aquest punt és molt important i, alhora fàcil de realitzar, simplement tirant del cable de xarxa aconseguiríem aquesta contenció, evitant per exemple que si ataqués a la PIME un ransomware Zcrypto [52], una mostra de criptocuc que xifra els arxius i es propaga per ell mateix cap a altres ordinadors i dispositius que es trobin a la xarxa sense fer ús de correu *spam* ni cap *exploit*. Aquest malware es copia a ell mateix als ordinadors connectats, així com als dispositius extraïbles i memòries USB per infectar a altres dispositius. Per a què no hagi dubtes, un *exploit* es qualsevol atac que aprofita alguna vulnerabilitat del sistema que, mitjançant una seqüència de codi per obtenir el control de ordinadors o robar dades.

Un altre aspecte dins de la fase de contenció que s'ha de tenir en compte és comprovar si el procés del malware encara se segueix executant localment. Si s'observa aquest comportament, es recomana matar el procés. Si no fos possible matar el procés, ho més senzill és apagar l'equip mitjançant el botó d'encendre i apagar físic.

Un cop contingut l'atac, el següent pas, tal i com s'ha comentat en la fase de preparació, s'haurà de notificar a la direcció de l'empresa per saber l'estat de la situació i, al mateix temps, notificar a les autoritats competents.

Evidentment, igual que és molt important la rapidesa de contenir el ransomware, també és molt important no trigar en notificar a les autoritats que s'ha produït un ciberatac de tipus ransomware per així tenir una ràpida resolució de l'incident i poder així minimitzar l'impacte que podria ocasionar.

Depenent el tipus d'organització que hagi estat atacada pel ransomware, haurà de notificar-ho a una autoritat o a una altra. En el cas que es tractés de un

[51] Periodico. https://www.elperiodico.com/es/activos/20210814/ataques-ransomware-protocolo-actuacion-pymes-11988884
[52] Kaspersky. https://www.kaspersky.es/blog/zcryptor-ransomware/8425/

organisme de govern haurà d'acudir al CCN-CER. En canvi, si es tracta d'una empresa privada a INCIBE-CERT.

En el cas de les PIMEs, les podem considerar una empresa privada, per tant, podran dirigir-se i notificar que han patit un atac ransomware al CERT de INCIBE.

INCIBE-CERT, com centre de resposta d'incidents de seguretat té com a funció, oferir suport tècnic i proporcionar informació per ajudar en la resolució del incidents relacionats amb ciberseguretat. També fa ús de tècniques de detecció primerenca d'incidents, notificant als afectats per a què puguin prendre mesures.

Un altre punt a tenir en compte quan es tracta d'un atac ransomware, és que dades personals de clients o proveïdors es poden haver vist afectades. Per tant, tal i com especifica l'article 33 del RGPD, el responsable del tractament de les dades ha de notificar en un màxim de 72h a Agència Espanyola de Protecció de Dades, en cas que les dades s'hagin vist exposades. Per fer-ho, simplement han d'anar a la pàgina web de *notificación de brechas de datos personales (art. 33 RGPD)* [53]

- Resolució i recuperació

En aquesta fase de resolució i recuperació, és molt important que la PIME tingui present que la forma de solventar aquesta situació no és pas pagant el rescat als ciberdelinqüents, ja que això no dona les garanties que l'empresa pugui recuperar la informació compromesa. Tanmateix, això només propiciaria a què els ciberdelinqüents, tornessin a atacar l'empresa com a conseqüència d'haver ja pagat un rescat anteriorment.
Per tant, mai s'ha de pagar un rescat d'aquesta mena.

L'objectiu que ha de tenir en ment la PIME és recuperar l'activitat del seu negoci en el menor temps possible, per així poder minimitzar les pèrdues econòmiques.

Per fer-ho INCIBE ens indica unes etapes per a poder solventar i recuperar l'activitat de l'empresa.

[53] Sede electrónica. https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/nbs/guiadoBrechasInicio.jsf

Figura 15. Etapes per recuperar l'activitat de l'empresa [47]

La primera part d'aquesta tàctica, consisteix en aïllar l'equip de la xarxa. Aquesta part ja s'ha realitzat en l'etapa de contenció, però en l'etapa de resolució en la que ens trobem ara podríem realitzar el canvi de contrasenyes de les comptes dels usuaris treballadors de la PIME, recordant que aquestes han de ser robustes i fortes i que cada cert període de temps, mínim un any, s'hauran de tornar a canviar.

La segona part que ens indica INCIBE es tracta de clonar completament el disc dur infectat. D'aquesta manera s'intenten recuperar les dades des del disc dur clon i no repercutir a l'original.

Per fer-ho, els passos a seguir serien: connectar el disc dur infectat a un altre equip, el qual estigui, evidentment, aïllat de la xarxa, i preparat per a dur a terme proves, utilitzat aquest equip de esclau i poder veure quina informació es pot salvar i poder realitzar la còpia de tot el disc. Quan es realitzi aquesta còpia, s'ha de tenir en compte de copiar els documents i dades sensibles, essencials i importants per al funcionament de l'empresa, però no pas executables que poguessin tornar a infectar l'equip.

Una altra opció podria ser extreure el disc dur afectat, però no clonar-lo. Simplement extreure'l i intercanviar-lo per un de nou, conservant el disc dur afectat com a proba o per si en un futur apareix una solució que permet desxifrar el contingut del disc i recuperar la informació.
La tercera part indicada per INCIBE tracta de desinfectar el disc dur clonat. Aquest pas és clau per poder després recuperar la informació que hi conté, ja que abans de recuperar les dades és molt important eliminar el ransomware. Per poder realitzar la desinfecció del disc dur o discs durs afectats, es necessitarà un antivirus o antimalware el qual estigui actualitzat, però abans seria interessant identificar la infecció del ransomware. Per fer-ho es pot fer ús de la pàgina web ID Ransomware [54], on s'ha d'introduir el missatge de rescat, l'arxiu encriptat o ambdues coses, sent capaç de detectar 1064 ransomwares diferents.

[54] ID Ransomware. https://id-ransomware.malwarehunterteam.com/

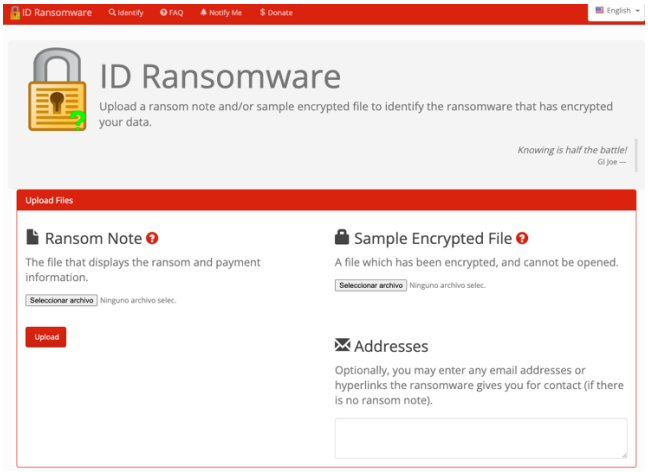


Figura 16. Identificació ransomware

Un cop introduïdes les dades demanades per la pàgina web, en uns segons identificarà el ransomware proporcionant diferents detalls com ara el nom de la família del ransomware, i si es coneixen tècniques per desxifrar els arxius o si actualment encara no n'hi ha.

Per exemple, si fos xifrat pel ransomware Qewe [Stop/Djvu] veuríem el següent:

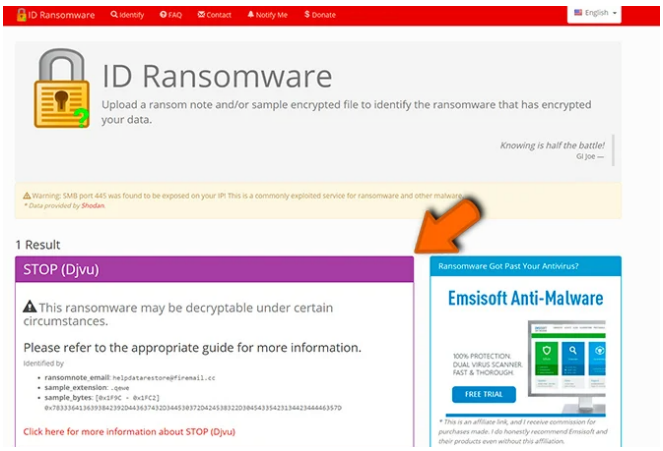


Figura 17. Identificació ransomware Qewe

Podem apreciar que si l'empresa fos infectada per aquest tipus de ransomware, probablement hauria forma de desxifrar les dades.

Per altra banda, si fos infectada pel ransomware.iso [Phobos], s'obtendria el següent missatge:

Figura 18. Identificació ransomware .iso

En aquest cas, veiem com ens diu que no es coneix cap forma de desxifrar les dades encriptades.

Al mateix temps no només hi ha una eina per identificar el tipus de ransomware, sinó que n'hi ha més. Una altra és l'eina *Crypto Sheriff* [55], de No More Ransom, oferta pel Centre Europeu de Ciberdelinqüència de la Europol. On també comprova els arxius que se li proporcionen, els quals són la nota de rescat i algun arxiu xifrat.

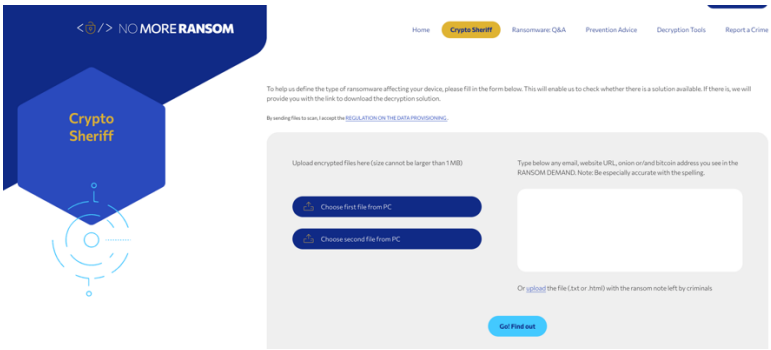


Figura 19. Crypto Sheriff

A més, si el *Crypto Sheriff* reconeix l'encriptat i té una solució, proporcionarà un enllaç per descarregar el programa de desxifrat que necessita.

Un cop tenim identificat el tipus de ransomware que ha pogut atacar la PIME, podem tractar de desinfectar els discs durs per així posteriorment restaurar el seu contingut. Per eliminar el malware ransomware, podem primerament comprovar si el malware s'ha eliminat a si mateix després de xifrar els arxius. Hi ha ciberdelinqüents que no volen que el seu software maliciós deixi pistes que puguin ajudar a crear eines per poder-lo desxifrar.

[55] No More Ransom. https://www.nomoreransom.org/crypto-sheriff.php?lang=en

L'altra opció, si el ransomware no s'ha esborrat a si mateix, és fer ús d'un antivirus o antimalware, per exemple Avast Free Antivirus [56], el qual pot detectar i eliminar molts tipus de programes ransomware de forma ràpida i senzilla.

Un cop arribats en aquest punt, coneixent el tipus de ransomware que ens ha afectat i, si es coneix, la forma de desxifrar els arxius, entrem al punt de recuperació i restauració dels equips per a què l'empresa pugui continuar amb el seu negoci.

Primer de tot, s'ha d'intentar recuperar les dades que havien estat xifrades. Un cop el disc ha estat desinfectat, s'han d'intentar recuperar les dades. Si s'ha fet ús de *Crypto Sheriff*, si existeix algun tipus de solució aquest ens informarà d'això, donant l'eina per poder desxifrar les dades, juntament amb un manual explicatiu de com utilitzar-la.

En cas que no existís cap solució per a recuperar les dades xifrades, el millor és guardar aquell dics dur afectat per si en un futur hagués alguna solució i poder llavors recuperar les dades.

L'altra opció, és restablir el sistema des d'una còpia de seguretat que no han estat afectades per l'atac ransomware. Per això, cal destacar la importància de realitzar còpies de seguretat de forma periòdica per poder assegurar una recuperació ràpida de l'activitat del negoci, afectant de la menor manera possible a l'economia de la PIME.

Per tant, un cop desinfectat l'equip, farem ús de la còpia de seguretat que tindrà l'empresa, gràcies a les mesures preventives que s'han comentat en aquest estudi, restaurant així l'equip a una versió anterior.

També podríem fer servir una altra opció, en cas que el sistema operatiu tingui *shadow copy* o *snapshot* [57], les quals mantenen còpies de versions anteriors dels diferents fitxers. És a dir, fer ús de les còpies de seguretat de Windows.

En aquest cas, s'ha de localitzar una còpia anterior a l'atac ransomware i restaurar els fitxers des de aquest punt anterior.

3.4. Fase d'aprenentatge i millora

Un cop recuperat el funcionament del negoci novament, és molt important, fer un bon anàlisi post atac i veure les millores que es poden realitzar per a reduir

[56] Avast Free Antivirus. https://www.avast.com/es-es/free-antivirus-download#mac
[57] WeLiveSecurity. https://www.welivesecurity.com/la-es/2017/09/26/shadow-copies-backup-windows-ransomware/

el risc que un atac d'aquestes característiques torni a succeir. Veure les vulnerabilitats que van aprofitar els ciberdelinqüents i fer un pla de millora contínua, avaluant el risc, la criticitat i el cost.

Al mateix temps, haver estat víctima d'un atac ransomware, posa sobre la taula les mancances en aspecte de ciberseguretat del conjunt d'empleats que formen l'empresa. Per això, recalquem en aquest estudi la importància de que les mesures preventives s'apliquin correctament, emfatitzant sobretot en la formació del personal en aspectes de ciberseguretat, on un tipus d'atac ransomware aprofita sobretot aquesta vulnerabilitat.

No obstant això, aquesta no és l'única forma de fer front a un atac ransomware, sinó tenir unes còpies de seguretat actualitzades, com hem vist també un aspecte molt important a mantenir al dia, ja que són necessàries per poder tornar a l'activitat del negoci en el menor temps possible.

Altres aspectes importants que ha de tenir la PIME, és l'activació de Firewall, antivirus, polítiques de control d'accessos, factors de doble autenticació o segmentació de la xarxa són mesures a tenir present en l'empresa i tenir-les actualitzades.

Per tant, per a una PIME, apostar per un equip de seguretat i invertir en aspectes de ciberseguretat és una necessitat. D'aquesta manera podran millorar en els àmbits de ciberseguretat i ser menys interessants per als ciberdelinqüents, com a conseqüència de estar preparades per a aquest tipus de situacions.

4. Conseqüències davant un atac ransomware

Com ja s'ha comentat al llarg d'aquest estudi, un atac ransomware pot tenir conseqüències reputacionals, econòmiques i jurídiques per a l'empresa que ha patit aquest atac, com a conseqüència del període d'inactivitat, els arxius sensibles compromesos, entre altres. Ja que depèn del temps que es trigui a recuperar l'empresa d'aquest tipus d'atac farà que l'impacte tant econòmic, com reputacional sigui major, si el temps de recuperació és major.

En aquest apartat tractarem aquestes conseqüències per poder mostrar a les PIMEs la importància d'invertir en seguretat informàtica i prendre accions per prevenir-se d'atacs com el ransomware i ser, d'aquesta manera, menys vulnerables als ulls dels ciberatacants.

Es tractarà de forma separada cada conseqüència en els següents apartats.

4.1. Conseqüències econòmiques

Tal com s'ha comentat en els apartats anteriors, quan una empresa, o en el nostre cas d'estudi una PIME, es veuen infectades pel malware ransomware, el primer a fer es contenir l'atac. Això significa que els dispositius de l'empresa romandran parats fins que es contingui i se solucioni l'atac, provocant una parada de l'activitat del negoci.

Com a conseqüència directa de l'aturada de l'activitat, tindrà repercussions econòmiques durant tot el temps d'inactivitat. Com major sigui aquest temps, major seran les pèrdues econòmiques.

Però les conseqüències econòmiques no només són degudes a l'aturada de les activitats econòmiques, sinó també al rescat pagat, en cas que es realitzi el pagament, o el cost de l'empresa consultora contractada per solucionar el problema de l'atac ransomware, entre d'altres.

S'ha fet referència al cost del pagament del rescat, ja que encara que en aquest estudi s'hagi comentat que no es recomana pas realitzar el pagament als ciberatacants, moltes empreses acaben pagant aquest rescat. La raó per la qual moltes empreses decideixen realitzar el pagament és perquè el temps que fa que l'activitat estigui aturada, suposa per a l'empresa unes pèrdues econòmiques massa elevades, fent que es replantegin duu a terme al pagament als atacants i poder tornar quan abans a l'activitat de negoci de l'empresa.

A més, segons un estudi elaborat per Sophos [58], més víctimes han pagat el rescat, d'un 26% l'any 2020 a un 32% l'any 2021. Però també s'afirma en aquest estudi que pagar el rescat només permet recuperar les dades parcialment, en concret el 65% de dades van ser restaurades després de pagar el rescat. Com s'ha dit en apartats anteriors, pagar el rescat no és una assegurança de recuperar les dades. En la següent taula es mostra els percentatges dels mètodes que van fer servir les empreses de l'estudi per recuperar les dades.

2020	2021	
26%	32%	Van pagar rescat per recuperar les dades
56%	57%	Van fer ús de còpies de seguretat per recuperar les dades
12%	8%	Van fer ús d'altres mètodes per recuperar les dades
94%	96%	Total d'empreses que van recuperar les dades

Taula 5. % empreses de la forma en com van recuperar les dades

Un altre aspecte a tenir en comte, és que el valor dels rescats, els qual no han parat d'augmentar en els últims anys. Una dada també interessant que se'ns mostra en aquest estudi és el cost mig del rescat. Aquest s'ha duplicat en l'any 2021. L'any 2020 el cost mitjà podia estar pels 260.000 euros, però al 2021 pot arribar fins a 500.000 euros.

Finalment, en aquest estudi també s'indica que les empreses que tenen un pla de recuperació i continuïtat del negoci, tenen menys probabilitats de patir una inactivitat del negoci greu com a conseqüència d'un atac ransomware, i que 4 de cada 5 empreses petites poden recuperar-se d'aquest tipus d'atac en 24 hores, si tenen aquests plans de recuperació.

Per acabar, però no menys important, la pèrdua de confiança dels clients de l'empresa, a part d'afectar reputacionalment, també afecta econòmicament, ja que si l'empresa que ha estat víctima del ransomware, aquesta no pot oferir el servei que donava als clients, quedant aquests descontents i perdent la confiança en l'empresa. Això pot provocar pèrdua de clients actuals, provocant menys ingressos, i també pèrdua de clients futurs.

[58] Sophos state of ransomware. https://assets.sophos.com/X24WTUEQ/at/wpkww9k8xsn3m7j2hrpw5ws/sophos-state-of-ransomware-2021-wpes.pdf

4.2. Conseqüències reputacionals

La reputació d'una companyia fa referència a la valoració que té el públic respecte aquesta. Bàsicament es basa en la publicitat que se'n fa de l'empresa, els productes que comercialitza i la visió que té el públic de la seva activitat.

Les conseqüències reputacionals no són un aspecte a tenir poc en compte, sinó tot el contrari i més avui en dia que si una notícia negativa afecta a una empresa, acabarà a les xarxes socials o altres plataformes on la gent s'assabentarà de ho ocorregut i serà comentada pels usuaris. Podent generar un impacte molt negatiu en la reputació de l'empresa afectada, podent arribar a ser tan crítica que danyi la imatge de l'empresa de forma permanent.

A més a més, en un atac ransomware, les dades personals de clients, treballadors o proveïdors poden quedar exposades, i en aquests casos els internautes no és quedaran callats davant una situació semblant, provocant al mateix temps una desconfiança sobre aquesta empresa entre els usuaris. Les opinions podrien girar al voltant de la falta de previsió i recursos de l'empresa cap a aquest tipus d'amenaces.

Si la gestió d'aquesta infecció per ransomware no és adequada, les conseqüències cauran en la reputació del negoci, sobretot si no es prenen mesures de forma ràpida i eficaç per fer front a l'atac.

I és que amb el desenvolupament d'Internet la reputació de les empreses ha agafat importància, fent que sigui el risc reputacional un dels més preocupants pels CEOs de les empreses. De fet durant el 2017 i 2018 el risc reputacional apareixia en el top 5 de riscos [59].

Per tant, el risc reputacional requereix una gestió i vigilància constant. Però moltes empreses es tracta com una gestió de crisis de comunicació, fent que s'actuï de forma reactiva enlloc de proactiva.

Sabent tot ho dit anteriorment, per estalviar-se una PIME els efectes més adversos, es necessari gestionar la reputació de la companyia en dos aspectes: investigació i monitorització [60].

La investigació consisteix en analitzar la reacció dels usuaris, analitzant quines han estat les seves opinions i comentaris que han difós per la xarxa en successos passats. D'aquesta manera és pot tenir una visió bastant acurada de com els usuaris veuen a l'empresa.

[59] La gestión de riesgos en el mundo digital. https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf
[60] NOA. https://noa.aon.es/ciberseguridad-e-impacto-reputacional/

Pel que fa a la monitorització, aquesta consisteix en saber que ocorre en l'actualitat, revisant també els comentaris i opinions que hi ha en aquest moment a la xarxa sobre la companyia. D'aquesta forma, es pot saber les reaccions que estan tenint els usuaris davant algun fet actual i prendre les mesures i dedicions necessàries per minimitzar l'impacte i evitar que els usuaris no perdin la confiança en l'empresa. Ja que, si no té bona reputació els clients actuals podrien no voler continuar amb els serveis proporcionats per la PIME, i alhora, no aconseguir nous clients en el futur, perillant seriosament la continuïtat del negoci.

4.3. Conseqüències jurídiques

En els anteriors apartats, s'ha tractat de les conseqüències econòmiques i reputacionals, mentre que en aquest tractarem les conseqüències jurídiques que poden comportar a una empresa que ha estat atacada per un atac ransomware podent donar lloc a delictes que comportin certes sancions.

Primer de tot, ens centrarem en les conseqüències que tindran els atacants com a conseqüència de dur a terme el ciberatac. Més en concret, les conductes típiques d'un atac ransomware són de delicte de danys i sabotatges que inclou el Codi Penal (CP) en l'article 264 [61]. En aquest article del Codi Penal, es castiguen les conductes que recauen sobre dades, programes informàtics o documents electrònics aliens, mentre que les que fan referència al funcionament normal d'un sistema informàtic aliè, se sancionen amb l'article 264 bis CP. Aquests delictes poden tenir penes de presó de sis mesos fins a tres anys.

A més a més, l'article 264.2 CP agreuja les penes en els fets delictius en el marc d'una organització criminal, quan s'hagin causat danys d'especial gravetat o afectin als interessos generals. En aquest cas s'especifica que es podria condemnar de dos a cinc anys de presó als ciberdelinqüents que han realitzat aquest atac. En aquest últim cas també comportaria una multa de deu cops el perjudici causat.

Però si que és veritat que poder condemnar als ciberdelinqüents pels delictes comesos no és una tasca fàcil, com a conseqüència que no és fàcil poder-los identificar a causa de les característiques d'Internet com ara la possibilitat d'anonimat, el seu caràcter descentralitzat, inexistència d'autoritats amb competències suficients per a controlar l'activitat que s'hi duu a terme.

[61] El País.
https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html

A continuació, ens centrarem en les afectacions jurídiques que pot patir una empresa que s'ha vist afectada per un atac ransomware, ja que els clients poden realitzar reclamacions a l'empresa, tenint en comte tant la responsabilitat civil contractual, com l'afectació de tercers com a conseqüència de l'extracció i la difusió de les dades.

Si ens centrem en els aspectes de responsabilitat civil contractual, aquests s'indiquen en l'article 1101 del Codi Civil, on s'estableix que queden subjectes a la indemnització dels danys i perjudicis causats els que en el compliment de les seves obligacions realitzen danys, negligència o morositat. És a dir, l'incompliment en el contracte entre empresa i client.

Mentre que l'afectació de tercers a causa de la sostracció de informació, pot quedar recollida en l'article 1902, on s'exposa que el que per acció o omissió causa danys a un altre, intervenint culpa o negligència està obligat a reparar el dany causat. És a dir que s'ha produït una responsabilitat civil extracontractual.

Per tant, l'empresa estaria causant danys a tercers com a conseqüència que les dades d'aquests han estat exposades, i això és el que la PIME ha d'evitar i fer ús de les mesures preventives esmentades en aquest estudi per poder evitar aquestes situacions.

En un atac ransomware, també s'ha de tenir en compte que en certes situacions les dades encriptades que els atacants poden difondre, podrien considerar-se com delictes de descobriment de la informació personal, si les dades afectades són de caràcter personal. Aquest aspectes es recullen en l'article 197.1 i 197.2 del Codi Penal [62]. Aquest article sanciona conductes que afecten als drets a la protecció de dades i als drets d'intimitat i de la pròpia imatge. En concret, se cita en l'article 197.1, que el que reveli secrets aliens, dels que tingui coneixement per raó del seu ofici o les seves relacions laborals, serà castigat amb una pena de presó d'un a tres anys i multa de sis a dotze mesos. Mentre que en l'article 197.2, s'esmenta que el professional que amb l'incompliment de la seva obligació de sigil o reserva, divulgui els secrets d'una altra persona, serà castiga i amb la pena de presó d'un a quatre anys, multa de dotze a vint-i-quatre mesos i inhabilitació especial per a aquella professió durant un temps de dos a sis anys.

A més, a part del Codi Penal, si es veiessin afectades dades personals, l'empresa podria cometre un error pel que fa a responsabilitat legal a causa de no complir ho establert en la Llei orgànica 3/2018, de Protecció de Dades Personals i Garantia de Drets Digitals (LOPDGDD). Aquesta llei estableix els requisits i obligacions en matèria de protecció de dades en empreses sobre

[62] Deloitte. https://www2.deloitte.com/es/es/pages/legal/articles/A-que-peligros-ciberneticos-se-enfrenta-un-despacho-de-abogados-Figuras-delictivas-frecuentes-y-riesgo-reputacional.html

com procedir amb la informació personal, així com els drets que afecten a usuaris i consumidors [63].

A part de la LOPDGDD, també trobem el Reglament General de Protecció de Dades (RGPD), el qual implementa els drets dels usuaris sobre les seves dades i protegeix el tractament i circulació de les dades personals [64]. Més en concret en l'article 34 del RGPD tracta que quan sigui probable que la violació de la seguretat de les dades personals impliqui un alt risc per als drets i llibertats de les persones físiques, el responsable del tractament la comunicarà al interessat sense dilació indeguda [65].

Per tant, la empresa, sense dilació, ha de comunicar l'atac ransomware que ha patit. Sinó, aquesta podria ser sancionada per l'Agència Espanyola de Protecció de Dades (AEPD). En la *Guía para la notificación de brechas de datos personales* [66], s'indica que conforme l'article 33 del RGPD, tan aviat com el responsable del tractament tingui coneixement de que s'ha produït una escletxa de dades personals ha d'efectuar la corresponent notificació a l'Autoritat de Control competent, quan sigui probable que l'escletxa constitueixi un risc pels drets i llibertats de les persones. En aquest cas, s'ha de realitzar sense dilació i com a màxim en les 72 hores següents, tenint en compte també les hores transcorregudes durant els caps de setmana i festius.

L'AEPD indica que com part del procés de gestió d'incidents, s'ha d'incorporar un procediment de notificació d'escletxes de dades personals per a la correcta aplicació del RGPD. És a dir, definir l'Autoritat de Control a notificar, definir quina persona notificarà a l'Autoritat de Control, aprovisionarà dels mitjans tècnics necessaris per a la notificació i assegurar el compliment del termini. Al mateix temps, definir també el procediment de comunicació als afectats, definint qui realitzarà la comunicació, com es comunicarà als afectats, quins canals i medis s'utilitzaran i quins detalls permetran comunicar de forma efectiva.

A continuació es mostra el procés de gestió d'escletxes de dades personals.

[63] Grupo Atico 34. https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/
[64] Diccionario Web. https://diccionarioweb.com/que-es-rgpd/
[65] GDPR text. https://gdpr-text.com/es/read/article-34/
[66] AEPD. https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

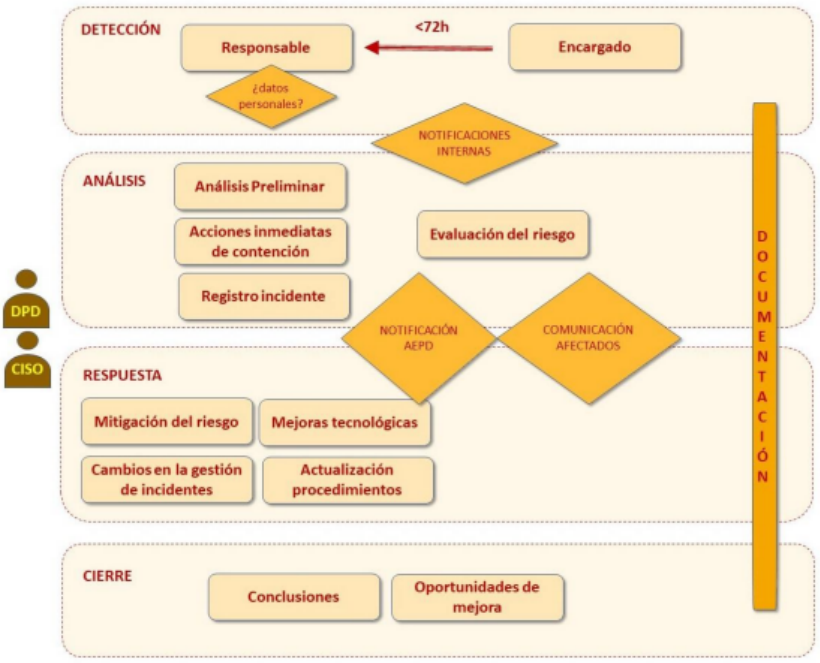


Figura 20. Procés de gestió d'escletxes de dades personals [64]

Finalment, tal i com s'ha comentat en diferents punts d'aquest estudi, no es recomana realitzar el pagament del rescat, però si l'empresa es veiés obligada a realitzar-lo com a cas extrem, es podria arribar a acusar a aquesta empresa de col·laborar en el finançament del terrorisme o blanqueig de capital, el qual comportaria a una exigència de responsabilitat per ajudar a afavorir una organització criminal, en aquest cas a la ciberdelinqüència.

5. Conclusió

Aquest projecte, s'iniciava amb la intenció de poder apropar més a les petites i mitjanes empreses, les PIMEs, una visió de la importància que té avui en dia per a una empresa d'aquestes característiques, ser conscient de com poden protegir-se o saber gestionar un atac ransomware, per poder així continuar amb el negoci amb les mínimes afectacions possibles.

Sobretot, tenint en compte com ha afectat la pandèmia del Covid-19 a fer major ús de tecnologies en espais vulnerables en l'àmbit del treball, i com al mateix temps el ciberatacants s'aprofiten d'aquesta situació per extreure'n un benefici.

Després d'haver realitzat aquest estudi, podem afirmar que el ransomware ha estat un dels principals ciberatacs en aquest últims anys afectats per la pandèmia i que continua afectant aquest 2022. Posant especial atenció a les petites i mitjanes empreses, les quals han experimentat una major afectació, ja que són més vulnerables, des del punt de vista del ciberdelinqüents.

Les PIMEs són més vulnerables en comparació a les grans empreses, com a conseqüència de tenir menys recursos econòmics, o cap, que poden destinar a la ciberseguretat i formació als empleats sobre aquesta, tal i com s'ha comentat en aquest estudi. Per aquesta raó, en aquest treball s'emfatitza a les PIMEs la importància de canviar aquesta situació i que s'introdueixi en l'empresa una formació contínua als treballadors sobre ciberseguretat i realitzar una gestió i planificació estratègica en aquest àmbit per així no ser tan vulnerables i disminuir el risc de ser atacades.

En aquest estudi, es fa èmfasis a les PIMEs per a què incloguin en la seu pla estratègic d'empresa unes mesures preventives de seguretat per evitar o reduir les possibilitats de patir l'atac ransomware. Donant elevada importància a la formació i conscienciació del personal de l'empresa, realitzar còpies de seguretat periòdiques, fer ús de navegació segura mitjançant VPN, mantenir el *software* actualitzat o una bona configuració del correu electrònic entre d'altres, poden evitar o reduir ser atacades per un ransomware.

Però no només es tracten mesures preventives, sinó que també es posa a disposició de les PIMEs un pla de contingència assequible per a aquest tipus d'empreses, per si en cas d'infecció, aquestes puguin ser capaces de combatre-la i erradicar-la en un període de temps que no comprometi a la continuïtat de l'empresa.

Definint les diferents fases que han de realitzar, com ara la fase de detecció, anàlisi i identificació de la infecció, així com les fases de contenció, resolució i recuperació d'aquesta infecció.

Però a més d'aquestes mesures, tant preventives com reactives, en aquest estudi també s'ha proporcionat conscienciació a les PIMEs sobre les conseqüències que pot arribar a patir l'empresa com a conseqüència d'haver-se vist afectada per un atac ransomware. Les conseqüències poden ser econòmiques, com a conseqüència de la inactivitat del negoci o el cost del rescat, reputacionals, com a conseqüència d'haver estat víctimes, futurs o actuals clients poden no voler continuar fent ús dels serveis de l'empresa tenint, per tant, una repercussió econòmica, i legals, poden arribar a ser multes o si es fan públiques dades personals i crítiques pot arribar a ser pena de presó. Per tant, podem dir que no es tracta d'un punt el qual no se li ha de donar importància, sinó ben bé el contrari, mostrant d'aquesta manera la importància de dur a terme dins de l'empresa unes mesures per evitar ser-ne víctima.

Finalment, l'últim pas, que es recomana en aquest estudi a les petites i mitjanes empreses, és no oblidar-se de realitzar la fase d'aprenentatge i millora. Haver pogut en sortir-se'n de l'atac ransomware, no significa oblidar-se'n, ja que podrien tornar a atacar l'empresa. És clau aprendre de les vulnerabilitats existents i prendre les mesures necessàries per evitar ser infectats de la mateixa manera, podent prendre accions pel futur.

Per concloure l'apartat de conclusions d'aquest estudi, és remarcable explicar els objectius que s'han assolit durant el seu procés.

Mitjançant un procés d'investigació s'ha pogut definir i conèixer què és el ransomware, el seu origen i els diferents tipus existents segons com actuen i com es propaguen, exposant diferents vectors d'atac.

A més, investigant diferents estudis estadístics, hem pogut veure la situació actual de les PIMEs, veient el percentatge d'atacs ransomware que han patit, com a conseqüència de les característiques d'aquest tipus d'empreses. Podent d'aquesta manera exposar la importància de la conscienciació a les PIMEs, exposant també els diferents impactes, econòmic, reputacional i jurídic a la que s'exposaran aquestes organitzacions a l'haver estat atacades per un ransomware.

També s'ha assolit l'objectiu de definir unes mesures de prevenció que siguin assequibles per les PIMEs, exposant diferents tècniques que no comportin un gran cost però si una eficàcia en àmbits de prevenció.

Al mateix temps, l'objectiu de definir un pla de contingència també s'ha assolit. Proporcionant a les PIMEs diferents tècniques reactives assequibles i eficaces.

Finalment, l'últim objectiu que ens havíem proposat i que s'ha assolit, ha estat avaluar les conseqüències legals en cas que hagi fuga d'informació. Per a aconseguir-ho, s'ha investigat diferents articles del Codi Civil i Penal Espanyol, així com la Llei orgànica 3/2018, de Protecció de Dades Personals i Garantia de Drets Digitals (LOPDGDD) i el Reglament General de Protecció de Dades (RGPD). Entenent i exposant les diferents conseqüències legals en que es poden veure afectats tant els ciberatacants, com l'empresa afectada.

6. Glossari

AES: Advanced Encryption Standard en anglès, és un dels algoritmes de xifrat per blocs més utilitzats i segurs que hi ha actualment.

Exploit: Qualsevol atac que aprofita alguna vulnerabilitat del sistema que, mitjançant una seqüència de codi per obtenir el control de ordinadors o robar dades.

Malware: Software hostil o intrusiu que duu a terme funcions no desitjades als dispositius infectats per aquest.

Phishing: Es refereix a l'enviament de correus electrònics que tenen l'aparença de provenir de fonts de confiança, però que en realitat pretenen manipular al receptor per robar informació confidencial.

PIME: Petita i mitjana empresa. Són empreses que tenen certa límitacions ocupacionals i financeres fixades per l'Estat. Micro empresa tindrà menys de 10 treballadors. Una petita empresa tindrà entre 10 i 49 treballadors. Una mitjana empresa tindrà menys de 250 treballadors.

RaaS: Ransomware as a Service en anglès, és una classe de servei que ofereix kits de malware per poder dur a terme un atac ransomware. Un grup de ciberdelinqüents desenvolupen un virus ransomware que el posaran a la venta a la *dark web* i l'interessat en aquest servei pagarà una quota per tenir aquest malware.

Ransomware: Es tracta d'un tipus de programa que restringeix l'accés a determinades parts o arxius del sistema operatiu infectat i demana un rescat per treure la restricció.

RDP: Remote Desktop Protocol en anglès, és un protocol d'escriptori remot de Microsoft el qual proporciona funcions de pantalla i entrada remota a través de connexions de xarxa per a Windows.

Shadow copy: Tecnologia inclosa en Microsoft Windows, capaç de crear còpies de seguretat fins i tot quan s'està fent ús dels arxius.

Spam: És qualsevol forma de comunicació no sol·licitada que s'envia de forma massiva. La seva forma més freqüent es un correu electrònic de publicitat enviat a un gran nombre de direccions.

7. Bibliografia

[1] Hiscox. https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021. Data de consulta: 20/02/2022

[2] La Vanguardia. https://www.lavanguardia.com/tecnologia/20211222/7947999/ataque-ransomware-compromete-funcionamiento-hospital-mas-importante-asturias-pmv.html. Data de consulta: 21/02/2022

[3] Ministerio de industria, comercio y turismo. https://industria.gob.es/es-es/estadisticas/Cifras_PYME/CifrasPYME-enero2022.pdf. Data de Consulta: 21/02/2020

[4] Interpol. https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19. Data de consulta: 22/02/2022

[5] El País. https://cincodias.elpais.com/cincodias/2021/04/20/fortunas/1618932032_554260.html. Datade consulta: 22/02/2022

[6] INCIBE. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario Data de consulta: 20/02/2022

[7] Malwarebytes. https://es.malwarebytes.com/ransomware/ Data de consulta: 28/02/2022

[8] Ransomware. Una guia de aproximación para el empresario. Secretaría del estado de digitalización e intel·ligència artificial. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario Data de consulta: 28/02/2022

[9] SSH TEAM Consulting. https://sshteam.com/ Data de consulta: 28/02/2022

[10] ElPaís. https://cincodias.elpais.com/cincodias/2021/07/21/companias/1626821663_803769.html Data de consulta: 28/02/2022

[11] Kaspersky https://latam.kaspersky.com/resource-center/threats/ransomware Data de consulta: 02/03/2022

[12] RedesZone. https://www.redeszone.net/tutoriales/seguridad/ransomware-evolucion-historia/ Data de consulta: 02/03/2022

[13] Imagen digital. https://www.dineroenimagen.com/2017-07-04/88422 Data de consulta: 02/03/2022

[14] Origen y evolución del cryptovirus Ransomware. https://www.academia.edu/32083196/ORIGEN_Y_EVOLUCI%C3%93N_DEL_CRYPTOVIRUS_RANSOMWARE Data de consulta: 03/03/2022

[15] Next Vision. Ciberseguridad Inteligente. https://nextvision.com/phishing-y-ransomware-tecnicas-de-ingenieria-social-que-ponen-en-riesgo-la-informacion-de-las-empresas/ Data de consulta: 03/03/2022

[16] SentinelOne. https://es.sentinelone.com/blog/7-common-ways-ransomware-can-infect-your-organization/ Data de consulta: 04/03/2022

[17] Panda. MediaCenter. https://www.pandasecurity.com/es/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/ Data de consulta: 04/03/2022

[18] Oficina de Seguridad del Internauta. https://www.osi.es/es/actualidad/avisos/2017/04/ahora-un-phishing-de-la-agencia-tributaria-quiere-secuestrar-tu-ordenador Data de consulta: 05/03/2022

[19] Microsoft. https://docs.microsoft.com/es-es/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol Data de consulta: 05/03/2022

[20] IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2021/09/estos-son-los-tres-principales-vectores-de-ataque-del-ransomware Data de consulta: 05/03/2022

[21] Shodan. https://www.shodan.io/search/report?query=remote+desktop Data de consulta: 05/03/2022

[22] Osi. https://www.osi.es/es/actualidad/avisos/2012/01/virus-muestra-un-falso-mensaje-del-cuerpo-nacional-de-policia Data de consulta: 06/03/2022

[23] Sensors Tech Forum. https://sensorstechforum.com/es/remove-noob-ransomware-restore-data/ Data de consulta: 06/03/2022

[24] Panda Security. https://www.pandasecurity.com/es/mediacenter/seguridad/doxware-evolucion-secuestros-digitales/ Data de consulta: 06/03/2022

[25] Grupo Atico34. https://protecciondatos-lopd.com/empresas/ransomware-as-a-service-raas/ Data de consulta: 06/03/2022

[26] WeLiveSecurity. https://www.welivesecurity.com/la-es/2021/08/12/accenture-es-victima-de-ataque-del-ransomware-lockbit-2-0/ Data de consulta: 14/04/20222

[27] Pandasecurity. https://www.pandasecurity.com/emailhtml/2007-CAM-RANSOMWARE-AD360-WG/2006-Report-Sodinokibi-ES.pdf Data de consulta: 14/04/2022

[28] INCIBE-cert. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2018-8453. Data de consulta 14/04/2022

[29] Boxcryptor https://www.boxcryptor.com/es/encryption/ Data de consulta: 06/03/2022

[30] Kripkit https://kripkit.com/salsa20/ Data de consulta: 07/03/2022

[31] Grupo Atico34. https://protecciondatos-lopd.com/empresas/algoritmo-diffie-hellman/ Data de consulta: 07/03/2022

[32] Gobierno de España. Ministerio de Industria, Comercio y Turismo. http://www.ipyme.org/es-ES/DatosPublicaciones/Paginas/DefinicionPYME.aspx Data de consulta: 07/03/2022

[33] Delfos. https://www.delfossistemas.com/ataque-ransomware-ciberamenaza-mas-comun-para-las-pymes/ Data de consulta: 08/03/2022

[34] Businessinsider. https://www.businessinsider.es/ciberseguridad-pymes-claves-experto-google-949839 Data de consulta: 09/03/2022

[35] Noticias jurídicas. https://noticias.juridicas.com/conocimiento/tribunas/16792-riesgos-legales-del-teletrabajo-que-debemos-conocer/ Data de consulta: 10/03/2022

[36] Incibe. Kit de conscienciación. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html Data de consulta: 12/03/2022

[37] Geekflare. https://geekflare.com/es/best-open-source-firewall/ Data de consulta: 10/05/2022

[38] pfSense. https://www.pfsense.org/download/ Data de consulta: 10/05/2022

[39] IPFire. https://www.ipfire.org/ Data de consulta: 10/05/2022

[40] OpenSense. https://opnsense.org/ Data de consulta: 10/05/2022

[41] Incibe. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario Data de consulta: 14/03/2022

[42] Bit Life Media. https://bitlifemedia.com/2022/04/doble-factor-autenticacion-seguridad/#:~:text=El%20sistema%20de%20doble%20factor,un%20c%C3%B3digo%20de%20seguridad%20num%C3%A9rico Data de consulta: 14/04/2022

[43] Grupo Atico34. https://protecciondatos-lopd.com/empresas/lista-blanca-gris-

negra/#:~:text=En%20lugar%20de%20crear%20una,se%20demuestre%20que%20es%20aceptable. Data de consulta: 13/03/2022

[44] CCN-CERT. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html Data de consulta: 19/03/2022

[45] Digitaltrends. https://es.digitaltrends.com/computadoras/como-usar-windows-sandbox/ Data de consulta: 20/03/2022

[46] Cuckoo. https://cuckoosandbox.org Data de consulta: 20/03/2022

[47] Medidas de seguridad contra ransomware. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html Data de consulta: 23/03/2022

[48] INCIBE-CERT. https://www.incibe-cert.es/respuesta-incidentes Data de consulta: 25/03/2022

[49] Centro Criptológico Nacional. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html Data de consulta: 14/04/2022

[50] INCIBE. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario Data de consulta: 14/04/2022

[51] Periodico. https://www.elperiodico.com/es/activos/20210814/ataques-ransomware-protocolo-actuacion-pymes-11988884 Data de consulta: 15/04/2022

[52] Kaspersky. https://www.kaspersky.es/blog/zcryptor-ransomware/8425/ Data de consulta: 15/04/2022

[53] Sede electrónica. https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/nbs/guiadoBrechasInicio.jsf Data de consulta: 15/04/2022

[54] ID Ransomware. https://id-ransomware.malwarehunterteam.com/ Data de consulta: 16/04/2022

[55] No More Ransom. https://www.nomoreransom.org/crypto-sheriff.php?lang=en Data de consulta: 15/04/2022

[56] Avast Free Antivirus. https://www.avast.com/es-es/free-antivirus-download#mac Data de consulta: 15/04/2022

[57] WeLiveSecurity. https://www.welivesecurity.com/la-es/2017/09/26/shadow-copies-backup-windows-ransomware/ Data de consulta: 17/04/2022

[58] Sophos state of ransomware.

https://assets.sophos.com/X24WTUEQ/at/wpkww9k8xsn3m7j2hrpw5ws/sophos-state-of-ransomware-2021-wpes.pdf Data de consulta: 20/04/2022

[59] La gestión de riesgos en el mundo digital. https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf Data de consulta: 21/04/2022

[60] NOA. https://noa.aon.es/ciberseguridad-e-impacto-reputacional/ Data de consulta: 21/04/2022

[61] El País. https://cincodias.elpais.com/cincodias/2019/11/06/legal/1573063068_861999.html Data de consulta 22/04/2022

[62] Deloitte. https://www2.deloitte.com/es/es/pages/legal/articles/A-que-peligros-ciberneticos-se-enfrenta-un-despacho-de-abogados-Figuras-delictivas-frecuentes-y-riesgo-reputacional.html Data de consulta 23/04/2022

[63] Grupo Atico 34. https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/ Data de consulta: 23/04/2022

[64] Diccionario Web. https://diccionarioweb.com/que-es-rgpd/ Data de consulta: 24/04/2022

[65] GDPR text. https://gdpr-text.com/es/read/article-34/ Data de consulta 24/04/2022

[66] AEPD. https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf 24/04/2022

Annex I

CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES		
Clasificación	**Tipo de incidente**	**Descripción y ejemplos prácticos**
Contenido abusivo	**Spam**	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	**Sistema infectado**	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
Obtención de información	**Escaneo de redes (scanning)**	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	**Explotación de vulnerabilidades conocidas**	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	**Compromiso de cuenta con privilegios**	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.

Disponibilidad	**Robo**	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.
	DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	**Acceso no autorizado a información**	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	**Uso no autorizado de recursos**	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	**Criptografía débil**	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	**Otros**	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Annex II

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
CRÍTICO	Afecta apreciablemente a la Seguridad Nacional.
	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a una Infraestructura Crítica.
	Afecta a sistemas clasificados SECRETO.
	Afecta a más del 90% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios.
	El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
	Impacto económico superior al 0,1% del P.I.B. actual.
	Extensión geográfica supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
MUY ALTO	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
	Afecta a un servicio esencial.
	Afecta a sistemas clasificados RESERVADO.
	Afecta a más del 75% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios.
	El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
	Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.
	Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
	Daños reputacionales a la imagen del país (marca España).
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

ALTO	Afecta a más del 50% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona.
	Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual.
	Extensión geográfica superior a 3 CC.AA.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
MEDIO	Afecta a más del 20% de los sistemas de la organización.
	Interrupción en la presentación del servicio superior al 5% de usuarios.
	El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
	Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual.
	Extensión geográfica superior a 2 CC.AA.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
BAJO	Afecta a los sistemas de la organización.
	Interrupción de la prestación de un servicio.
	El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona.
	Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual.
	Extensión geográfica superior a 1 CC.AA.
	Daños reputacionales puntuales, sin eco mediático