DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

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

Butlletí N.º 20| Febrer 2022

PREVENCIÓ I GESTIÓ D'ATACS *RANSOMWARE*

I N D E X

PREVENCIÓ Y GESTIÓ D'ATACS *RANSOMWARE*

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades s Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

El *ransomware* és un tipus de *malware* (programari maliciós) que, en els últims temps, està creixent de manera exponencial. Aquest «segresta» els nostres recursos, impedint l'accés als mateixos -habitualment xifrant-los-, i sol·licita un rescat a canvi del seu alliberament.

El rescat se sol·licita, generalment, a través d'un missatge o una finestra que emergeix en el dispositiu afectat. És habitual que s'incloga un límit de temps per a pagar el rescat i que amenacen amb la destrucció total dels arxius segrestats o amb incrementar el valor del rescat si no es paga a temps. Així mateix, és comú que el rescat se sol·licite a través d'alguna moneda virtual com el Bitcoin. Un exemple de missatge podria ser el següent:

El *ransomware* pot afectar qualsevol usuari, negoci o activitat que puga pagar a canvi de la devolució de la seua informació. Aquest està afectant usuaris domèstics, negocis, sector públic i fins i tot a serveis crítics com a hospitals, causant pèrdues temporals o permanents d'informació, interrompent l'activitat normal, ocasionant pèrdues econòmiques per a restaurar els sistemes i fitxers i, en molts casos, també danys reputacionals.

En el present butlletí, us proposem una sèrie d'actuacions per a conéixer, previndre i mitigar aquesta amenaça.

EL *RANSOMWARE* «SEGRESTA» ELS NOSTRES RECURSOS, IMPEDINT L'ACCÉS ALS MATEIXOS -GENERALMENT XIFRANT-LOS- I SOL·LICITA UN RESCAT A CANVI DEL SEU ALLIBERAMENT.

QUÈ PODEMOS FER ELS USUARIS DELS SISTEMES D'INFORMACIÓ PER A EVITAR-HO?

Un gran nombre d'infeccions amb *ransomware* tenen lloc per mitjà d'atacs d'enginyeria social. Això és, els atacants enganyen els usuaris per a instal·lar el *malware*. El més habitual és que les infeccions es produïsquen per alguna de les següents vies:

- correu electrònic amb enllaços o adjunts maliciosos;
- escriptori remot exposat a Internet, amb credencials poc robustes i sense mecanismes de protecció;
- vulnerabilitats en el navegador web que faciliten la infecció en navegar per llocs maliciosos;
- dispositius externs infectats que es connecten als equips corporatius.

Per a evitar el *ransomware*, segueix aquestes **RECOMANACIONS:**


Mantingues actualitzats els sistemes operatius, navegadors i aplicacions.


Utilitza contrasenyes robustes.


Evita obrir adjunts o clicar enllaços en correus sospitosos no esperats o no sol·licitats.


Evita usar xarxes públiques.


Comprova que la pàgina web en la qual has entrat és una adreça segura. Per a això, ha de començar amb https:// i un xicotet cadenat tancat ha d'aparéixer en la barra d'estat del nostre navegador.

UN GRAN NOMBRE D'INFECCIONS *RANSOMWARE* TENEN LLOC PER MITJÀ D'ATACS D'ENGINYERIA SOCIAL. AIXÒ ÉS, ELS ATACANTS ENGANYEN ELS USUARIS PER A INSTAL·LAR EL *RANSOMWARE*.

UNA VEGADA MATERIALITZAT L'ATAC, COM ACTUEM?

1 NO PAGAR MAI EL RESCAT

- Pagar no garanteix que anem a tornar a tindre accés a les dades.
- Si paguem, és possible que siguem objecte d'atacs posteriors, perquè ja saben que estem disposats a pagar.
- Pot ser que sol·liciten una xifra major una vegada hàgem pagat.
- Pagar fomenta el negoci dels ciberdelinqüents.

2 APLICAR EL PROCEDIMENT DE GESTIÓ DE BRETXES DE SEGURETAT

La detecció per part d'un usuari dels sistemes d'informació de la Diputació de València d'un atac *ransomware* o de qualsevol altre succés que supose o poguera suposar un incident de seguretat haurà de ser **comunicat immediatament** per a valorar si pot catalogar-se com a "bretxa de seguretat de les dades personals".

Després de la comunicació, es recaptarà **informació útil** per a decidir quines mesures prendre i per a valorar la necessitat de notificar al centre de resposta a incidents de ciberseguretat, a l'autoritat de control en matèria de protecció de dades i, en el seu cas, als afectats. Així mateix, es valorarà la denúncia de l'incident a les Forces i Cossos de Seguretat de l'Estat perquè s'investigue l'origen del delicte. Així, es pot col·laborar en les labors de prevenció a altres entitats i en les accions per a capturar al ciberdelinqüent.

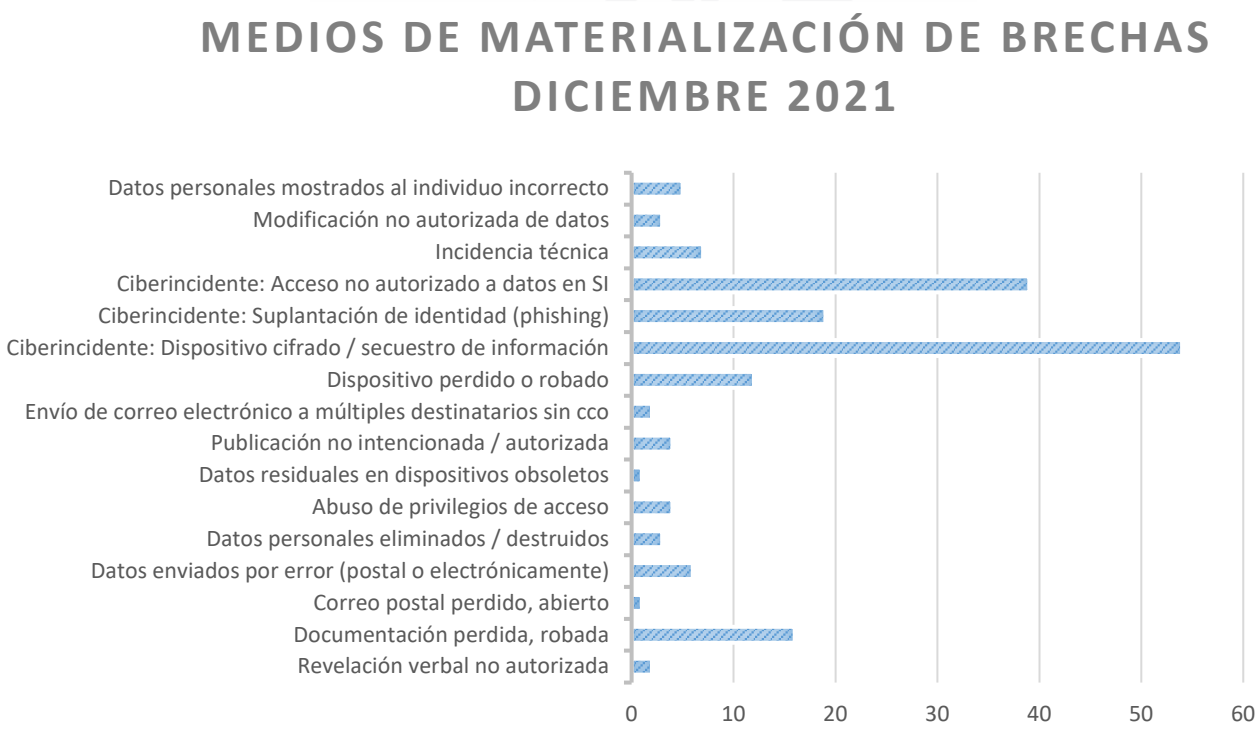
El **Delegat de Protecció de Dades (DPD)** ocuparà un paper molt rellevant, liderant el pla d'actuació en tots els seus aspectes. És important que el DPD siga consultat tan prompte s'haja detectat l'incident, la qual cosa implicarà que l'usuari que el detecte haja de comunicar-lo sense dilació. L'actuació del DPD tindrà especial rellevància en aquesta fase de comunicació perquè, entre les funcions que la normativa li atribueix, està la d'actuar com a punt de contacte entre el Responsable del tractament -la Diputació de València- i l'autoritat de control -l'AEPD-.

És important que es genere **documentació de tot el procés** de detecció, contenció i resposta, i que es custodien les evidències.

T'animem que revises el butlletí de protecció de dades remés el mes d'abril de 2021 (**Butlletí núm. 10: "Anàlisi, gestió i comunicació de les bretxes de seguretat en el context del RGPD".)**

L'USUARI DELS SISTEMES D'INFORMACIÓ DE LA DIPUTACIÓ QUE DETECTE UN *RANSOMWARE* O QUALSEVOL ALTRE SUCCÉS QUE SUPOSE O POGUERA SUPOSAR UN INCIDENT DE SEGURETAT, HAURÀ DE COMUNICAR-LO IMMEDIATAMENT A LA PERSONA DESIGNADA A ESTE EFECTE O, SI NO N'HI HA, AL RESPONSABLE DE LA INFORMACIÓ

L'Agència Espanyola de Protecció de Dades (AEPD) publica, amb periodicitat mensual, un informe que resumeix les principals característiques de les notificacions de bretxes de seguretat rebudes. En tots els informes publicats al llarg de 2021 han destacat les bretxes de seguretat provocades per ciberincidents consistents en el xifratge de dispositius i segrest de la informació (*ransomware*). En l'informe de desembre de 2021 -l'últim publicat fins hui-, l'Agència assenyala que les bretxes de dades personals causades per ciberincidents de tipus *ransomware* continuen sent les més notificades.



EN 2021, LA MAJOR PART DE LES BRETXES DE SEGURETAT NOTIFICADES A L'AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES VAN SER PROVOCADES PER AGENTS EXTERNS A LES ORGANITZACIONS, SENT ELS CIBERINCIDENTS PROVOCATS PEL SEGREST I XIFRATGE DE LA INFORMACIÓ (*RANSOMWARE*) ELS MÉS HABITUALS.

PODEN SANCIONAR A LA DIPUTACIÓ PER SER VÍCTIMA D'AQUESTA MENA D'ATACS?

En l'àmbit del sector públic, el Reglament (UE) 2016/679, de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD) permet als Estats establir les seues pròpies normes per a regular el seu règim sancionador. En el cas d'Espanya, la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD) contempla per a determinades categories de responsables o encarregats del sector públic la sanció de **APERCEBMENT**, acompanyada de les mesures que procedisca adoptar perquè cesse la conducta o es corregisquen els efectes de la infracció. Així mateix, ha de tindre's en compte el **DANY REPUTACIONAL** que la sanció causaria a l'entitat.

En cas de ser víctima d'un atac tipus *ransomware*, la Diputació de València podria ser sancionada per no comptar amb mesures tècniques i organitzatives adequades per a evitar o minimitzar l'impacte d'aquesta mena d'atacs, per no gestionar adequadament l'incident una vegada materialitzat el mateix o per no notificar la bretxa a l'autoritat competent o als interessats, segons la valoració del risc realitzada.

Com podem evitar la sanció?

- De manera **prèvia a l'incident**, hem de comptar amb **mesures tècniques i organitzatives per a evitar o minimitzar l'impacte**.
- Hem de seguir el **procediment** per a afrontar incidents d'aquest tipus.
- Amb **posterioritat a l'incident**, hem d'aplicar **mesures addicionals per a minimitzar l'impacte.**
- Hem de **denunciar els fets** davant les Forces i Cossos de Seguretat de l'Estat.
- Hem de **generar documentació de tot el procés** de detecció, contenció i resposta i custodiar les evidències davant una bretxa de seguretat.
- Hem de realitzar un **informe final sobre l'incident**.
- Hem de **notificar la bretxa a qui corresponga**, segons la valoració del risc realitzada.

EN CAS DE SER VÍCTIMA D'UN ATAC TIPUS *RANSOMWARE*, LA DIPUTACIÓ DE VALÈNCIA PODRIA SER SANCIONADA PER NO COMPTAR AMB MESURES TÈCNIQUES I ORGANITZATIVES ADEQUADES PER A EVITAR O MINIMITZAR L'IMPACTE D'AQUESTA MENA D'ATACS, PER NO GESTIONAR ADEQUADAMENT L'INCIDENT UNA VEGADA MATERIALITZAT EL MATEIX O PER NO NOTIFICAR LA BRETXA A L'AUTORITAT COMPETENT O ALS INTERESSATS, SEGONS LA VALORACIÓ DEL RISC REALITZADA.

MATERIAL COMPLEMENTARI

- Bretxes de seguretat: protegeix-te davant el *ransomware* (Blog AEPD). Consulta aquest enllaç.
- Bretxes de dades personals (AEPD). Consulta aquest enllaç.
- Informe de notificacions de bretxes de seguretat durant desembre de 2021 (AEPD). Consulta aquest enllaç.
- Expedient Nº: E/03575 (AEPD). Consulta aquest enllaç.
- Procediment Nº: E/01783/2020 (AEPD). Consulta aquest enllaç.
- Procediment Nº: E/08454/2019 (AEPD). Consulta aquest enllaç.
- Ajuda *ransomware* (Blog INCIBE). Consulta aquest enllaç.
- *Ransomware:* guia de aproximació (INCIBE). Consulta aquest enllaç.
- Que no et segresten l'ordinador: mesures per a evitar-ho (Blog INCIBE). Consulta aquest enllaç.
- Mesures de seguretat contra *ransomware* (CCN). Consulta aquest enllaç.
- "La meua organització ha sigut víctima d'un atac *ransomware,* ¿ com he d'actuar?" (Blog Associació Espanyola per a la Qualitat -AEC). Consulta aquest enllaç.

NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) sanciona a una entitat per implantar un sistema de control horari per reconeixement biomètric d'empremta dactilar sense haver realitzat prèviament una Avaluació d'Impacte.** El Consorci ESS Bilbao va decidir en 2019 implantar un sistema de fitxatge per reconeixement d'empremta dactilar. De la documentació obrant en l'expedient, l'AEPD no va trobar evidència de la realització de l'avaluació d'impacte de protecció de dades, per la qual cosa va sancionar a l'entitat amb prevenció, per una infracció de l'article 35 del RGPD.

Consulta la resolució en aquest enllaç.

- **La Secretaria d'Estat de Digitalització i Intel·ligència Artificial crea la web de la "Oficina de la Dada".** En 2020 es va crear l'Oficina de la Dada, dependent de la Secretaria d'Estat de Digitalització i Intel·ligència Artificial. Les seues principals línies estratègiques són les del disseny, coordinació i seguiment del model de referència arquitectònic per a fomentar la recol·lecta, gestió i intercanvi de dades públiques. En la nova web podràs trobar informació sobre aquest tema.

Consulta la web en aquest enllaç.

- **L'Autoritat Catalana de Protecció de Dades (APDCAT) emet un Dictamen sobre la conformitat amb la normativa de protecció de dades de l'ús del certificat COVID a Catalunya i el requeriment del DNI per part dels establiments.** Conclou l'autoritat que l'exigència del certificat COVID en els termes exposats i que han sigut autoritzats pel Tribunal Superior de Justícia de Catalunya, no pot considerar-se contrària a la normativa de protecció de dades personals. Igualment, quan siga exigible aquest certificat, l'exigència d'exhibició de l'anvers del DNI a l'efecte de verificar la identitat resultaria compatible i proporcionat d'acord amb la normativa de protecció de dades personals.

Consulta el Dictamen en aquest enllaç.