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 31| Gener 2023

ENGINYERIA SOCIAL

Í N D E X

ENGINYERIA SOCIAL

EN L'ADMINISTRACIÓN PÚBLICA

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 i Seguretat de la Informació

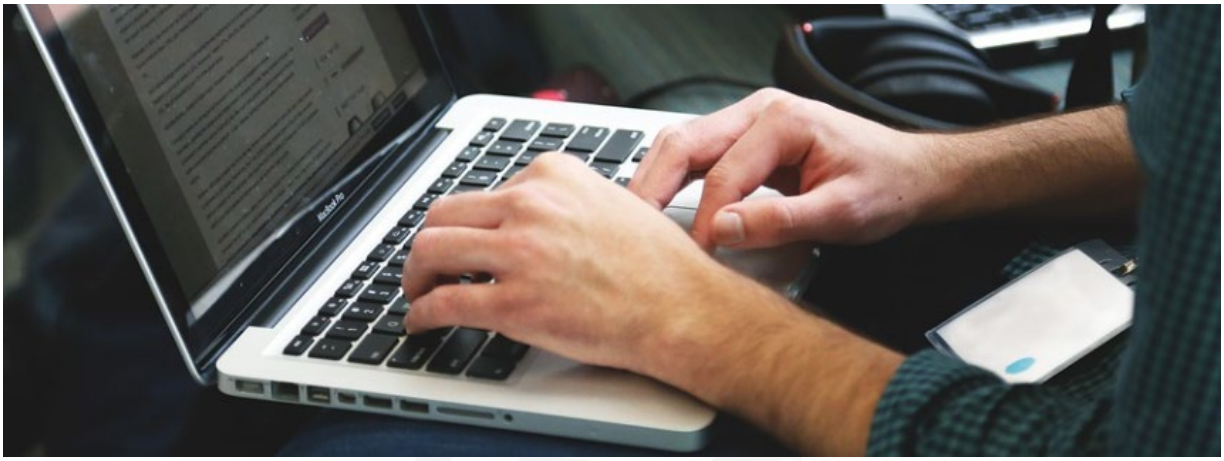
Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

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

INTRODUCCIÓ



Un dels principals pilars fonamentals de la protecció de les dades personals és la **seguretat en el tractament** d'aquestes dades. En particular, l'article 32 del Reglament General de Protecció de dades estableix que s'hauran d'aplicar "*mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc*".

Les mesures de seguretat protegeixen les dades personals de possibles atacs tecnològics, mitigant el risc que es materialitzen les amenaces a les quals es troben exposats. No obstant això, cal destacar que durant l'any 2022 el 82% de les bretxes tecnològiques van involucrar el **factor humà.**

Aquestes dades posen de manifest que la via més fàcil per a comprometre una organització de qualsevol tipus – inclòs el sector públic – és aconseguir que els seus propis usuaris legítims òbriguen portes als ciberatacantes o fins i tot executen directament les accions que el ciberatacant desitja. Per a aconseguir-ho, s'han desenvolupat **tècniques d'enginyeria social**.

A aquest efecte, en una de les publicacions de l'Agència Espanyola de Protecció de Dades, es defineix "enginyeria social" com "l'acció d'enganyar o fer xantatge a una persona perquè revele informació o emprenga una acció que puga usar-se per a comprometre o afectar negativament un sistema o, la qual cosa és el seu fi últim, una organització o un Estat".

En el present butlletí s'abordaran les diferents tècniques d'enginyeria social i les seues peculiaritats.

"ENGINYERIA SOCIAL: acció d'enganyar o fer xantatge a una persona perquè revele informació o emprenga una acció que puga usar-se per a comprometre o afectar negativament un sistema o, la qual cosa és el seu fi últim, una organització o un Estat".".

PRINCIPALS TÈCNIQUES D'ENGINYERIA SOCIAL

Pretexting

- Base de qualsevol atac d'enginyeria social
- Consisteix a elaborar un escenari/historia fictícia, on l'atacant tractarà que la víctima compartisca informació que, en circumstàncies normals, no revelaria.

Phishing

- Cerca "pescar" a les víctimes
- Amb caràcter general, s'empren correus electrònics amb arxius adjunts infectats o links a pàgines fraudulentes amb l'objectiu de prendre el control dels seus equips i robar-los informació confidencial.

Sextorsión

- Xantatge que busca amenaçar a la víctima amb distribuir suposadament contingut compromés d'ella als seus contactes (encara que no existisca aquest contingut), sinó accedeix a les peticions del ciberdelinqüent, generalment a realitzar un pagament.

Baiting

- Utilitza un esquer amb programari maliciós a la vista de les seues víctimes perquè ells mateixos infecten els seus dispositius.

Smishing

- És una variant del "phishing" però que es difon a través de SMS
- Es demana a l'usuari que telefone a un número de tarifació especial o que accedisca a un enllaç d'una web falsa.

Vishing

- Consisteix en trucades telefòniques mitjançant les quals l'atacant es fa passar per una organització o persona de confiança perquè la víctima revele informació privada.

Shoulder surfing	•Es basa a mirar "per damunt del muscle" •A l'atacant li n'hi ha prou amb observar el que escriu o té en pantalla un altre usuari per a obtindre informació molt útil.
Quid pro quo	•Es promet un benefici a canvi d'informació de caràcter personal. Solen ser compensacions en format regal (marxandatge, diners o accés gratuït a programes de pagament).
Dumpster diving	•Es refereix a l'acte de "ensumar en el fem" per a obtindre documents amb informació personal o financera.
Redes sociales	•Les tècniques d'engany més comuns a través de les xarxes socials són mitjançant cupons de descompte, jocs i concursos on l'usuari creu que pot guanyar alguna cosa.

Els ciberatacs basats en tècniques d'enginyeria social poden ser simples o complexos.

El primer grup utilitza solament el que es coneix com a *biaixos congnitius bàsics* i inherents a la naturalesa humana. Sobre la base d'estudis i investigacions, les persones prenem al voltant de 35.000 decisions de mitjana al dia, de les quals solament 91 són conscients. La resta les pren el cervell amb dreceres mentals o biaixos cognitius, entre els quals es troben fer o no "clic" en un enllaç *ransomware* que rebem per correu electrònic. Per exemple, el "efecte de veritat il·lusòria" provoca que, com al cervell li resulta més senzill processar informació que ha experimentat anteriorment, es tinga una sensació que ens pot portar a malinterpretar un senyal com un contingut vertader. D'aquesta manera, els ciberatacants poden realitzar atacs de phishing aprofitant aquest biaix. **La cultura de la ciberseguretat en el sector públic ha d'incorporar l'enfocament de pensar i revisar abans de fer clic en un enllaç.**

El segon grup s'ajusta a les peculiaritats de cada persona o organització. És el més perillós perquè sovint les mesures de seguretat tradicionals no són suficients per a detindre aquests atacs.

En conclusió, és molt rellevant la conscienciació i formació contínua dels empleats de les entitats públiques, perquè aquests ciberatacs poden comprometre informació personal dels ciutadans.

RESOLUCIÓ D'ARXIVAMENT D'ACTUACIONS ENFRONT D'UNA RECLAMACIÓ PER HAVER REBUT UN ATAC DE PHISHING

L'Agència Espanyola de Protecció de Dades (AEPD) - Expedient Núm.: E/06661/2021 - va procedir a l'arxivament de les actuacions després de la reclamació d'un particular a una notària per haver rebut mitjançant una adreça de correu electrònic desconeguda i un arxiu adjunt. En el cos del correu contenia el contingut literal de dos correus enviats per la Notaria amb la que va contractar serveis anteriorment i incloïa les seues dades personals.

En el present cas, de la documentació aportada per la NOTARIA en el curs d'aquestes actuacions d'investigació ***no es desprén que, amb anterioritat a la bretxa de seguretat, mancara de mesures de seguretat raonables en funció dels possibles riscos estimats.***

*La NOTARIA reconeix que la causa que ha pogut generar l'incident es deriva de l'actuació del malware "***MALWARE.1". Aquest malware es propaga per correu electrònic en descarregar-se arxius adjunts.*

Afig, no obstant això que, "no consta que ningú del despatx haguera obert aquests arxius adjunts".

*La NOTARIA identifica dos equips afectats per l'incident i expressa que per a solucionar l'incident "es va dur a terme una anàlisi de seguretat i neutralització del virus infectat fent-se ús de les eines específiques i programari antivirus-EmoCheck i ***MALWARE.1-Stopper-".*

Així mateix, no existeixen evidències que no haguera actuat de manera diligent una vegada coneguda la bretxa de seguretat, ni que les mesures adoptades amb posterioritat a l'incident ací analitzat no foren adequades.

Així, després de produir-se la bretxa de seguretat, la NOTARIA manifesta que ha reforçat les mesures de seguretat implantades:

- *Revisions informàtiques generals en l'àmbit del manteniment periòdic contractat.*
- *Actuacions d'avís i advertiment des de Gerència als empleats de la Notària davant circumstàncies similars que puguen estar produint-se, havent-se donat indicacions precises relatives a extremar les precaucions davant correus sospitosos, no havent-se de procedir a l'obertura dels seus arxius adjunts de cap manera..*
- *Revisions relatives a protecció de dades de caràcter personal, especialment tocant a la responsabilitat proactiva ("accountability") i a l'anàlisi i control de les medides tècniques i organitzatives implantades."*

Cal destacar la bona disposició de la NOTARIA en el sentit que, quan ha tingut coneixement de l'incident, ha posat en marxa les mesures oportunes per a evitar que es puga repetir en el futur. En conseqüència, l'AEPD va considerar que la NOTARIA havia adoptat totes les mesures que estaven a la seua disposició per a impedir i minimitzar l'impacte de la bretxa de seguretat ocorreguda.

MATERIAL COMPLEMENTARI

- Publicació de l'AEPD "Sense privacitat no hi ha ciberseguretat". Consulta la publicació en aquest enllaç.
- Infografia sobre tècniques d'enginyeria social publicada per OSI (Oficina de Seguretat de l'Internauta. Consulta la Infografia en aquest enllaç.
- Ciberconsells per als atacs de "phishing" publicat pel Centre Criptológico Nacional. Consulta la Publicació en aquest enllaç.

  Declaració sobre el paper d'un enfocament basat en el risc en la protecció de dades del Grup de Treball de l'article 29. Consulta la Publicació en aquest enllaç.

NOTÍCIES

- **L'AEPD imposa una sanció per infracció de l'article 5.1.f) (integritat i confidencialitat) i 5.2 del RGPD (responsabilitat proactiva)**

  El reclamant va detectar que el seu SIM no funcionava correctament i s'havien realitzat tranferencias sense el seu consentiment. Es devia al fet que el ciberatacante havia duplicat la seua targeta SIM.

  La companyia telefònica va al·legar que la pèrdua de disposició i control de les dades personals es produeix bé en un moment anterior a la seua participació (per exemple, mitjançant pràctiques de phishing o enginyeria social) o bé en un moment posterior a la seua participació, per la qual cosa considera que no se li poden atribuir.

  L'AEPD considera que en els procediments seguits per la companyia per a gestionar les sol·licituds de canvi de SIM s'identifiquen vulnerabilitats, constatant-se la falta de responsabilitat proactiva i la deficiència en les mesures de seguretat aplicades, la qual cosa constitueix una infracció dels principis bàsics de protecció de dades.

  Consulta la publicació en aquest enllaç.