Delictes informàtics

recopilació de les dades i preservació de la cadena de custòdia

Jornada de Seguretat Informàtica i protecció de dades a les Policies Locals

(Seu Federació Catalana de Municipis)
16 de Maig de 2018

Laura Mora i Aubert

Víctimes de delictes informàtics

ASPERTIC

Particulars

Empreses/institucions

Delictes/Conflictes a particulars

Tipus habituals de cyber-delictes
- Extorsió
- Ciber-Assetjament
- Ciber-bullying (entorns educatius o laborals)
- Robatori

Assetjadors/Atacants
- Desconeguts: Robots, xarxes organitzades
- Entorn familiar
- Entorn laboral
- Entorn escolar

Delictes/Conflictes a empreses

Tipus de delictes/conflictes
- Robatori i/o manipulació de dades
- Filtració de dades, continguts i propietat intel·lectual
- Incompliment de contractes amb proveïdors (amb engany)
- Conflictes laborals (quan hi ha un delicte de danys)

Assetjadors/Atacants
- Desconeguts: Robots, xarxes organitzades
- Competidors
- Clients/Proveïdors
- Entorn laboral

Com actuar?

En el cas que vingui un ciutadà amb un possible delicte i/o conflicte informàtic:

Recopilar les dades i preservar la prova

Recopilar les dades

- Els sistemes informàtics generen molta informació

- És necessari acotar al màxim el dia i la hora que s'ha comès el delicte

- Conèixer l'antecedent i tots els detalls pot ajudar a trobar noves proves
    - Des de quan s'estava gestant el conflicte?
    - Qui és el responsable del delicte?
    - El denunciant pot estar cometent un delicte?

- Anotar els models, números de sèrie i característiques dels dispositius afectats

- Seguir el procediment de **preservació de la prova** i de **la cadena de custòdia**

En cas de fuga de dades subjectes a RGPD avisar al DPO responsable de les dades

Preservar la prova

Preservar la prova i la cadena de custòdia és clau perquè la prova sigui admesa en un **procediment judicial**

- Tenim la capacitat de clonar la prova (a diferència dels metges forenses)
- Varis experts poden analitzar la prova de forma simultània
- Un bon peritatge és aquell que és objectiu, clar i entenedor
- La veritat s'amaga a les bones proves

És important seguir uns procediments per a preservar la prova (**cadena de custòdia**)

Com actuar?

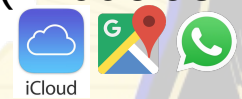
Tractament de diferents tipus de delictes i implicació de dispositius electrònics

1. Quines dades extraodinàries recollir a la declaració?

2. Quin procediment seguir per a preservar cadena de custòria i la prova?

Què fer quan?

Telèfons mòbils

1. Recopilació de dades del dispositiu i del seu propietari
   - Anotar l'IMEI (*#06#)
   - Factura de compra del dispositiu
   - Darrera factura del proveïdor
   - Claus de desbloqueig (del telèfon i de la SIM)
   - Taxació del dispositiu (+400€ delicte penal)
   - Programa/es afectats 

2. Preservació de la prova
   - Extreure la bateria / Apagar-lo
   - Introduïr-lo dintre un sobre "especial", sellar-lo i indicar el numero de cas 
   - Enviar-lo a un expert informàtic per a la extracció de la prova

Aspertic ofereix el servei de taxació telemàtica aspertic@aspertic.org i 93 160 01 60

Què fer quan?

Portàtils / Ordinadors de sobretaula

1. Recopilació de dades del dispositiu
    - Anotar el model, característiques i número de sèrie
    - Factura de compra del dispositiu (recomanable)
    - Claus de desbloqueig
    - Dades i programa/es afectat/s
    - Què estava fent quan …? i els dies previs?

2. Preservació de la prova
    - Apagar el dispositiu i desendollar-lo de la xarxa i la corrent
    - Avisar a un expert informàtic
        - Extreu-re'n els discs i sellar-los amb el número de cas
        - Si s'escau, restaurar el sistema (en el cas de no tenir backup clonar els discs)
    - Enviar el disc original al laboratori d'anàlisi forense per a l'extracció de les proves

Què fer quan?

No cal endur-se la impresora, el router, la torre sencera i…

EL MICROONES!

Què fer quan?

Discs durs / Unitats de memòria externa

1. Recopilació de dades del dispositiu
   - Anotar el model, capacitat i número de sèrie
   - Factura de compra del dispositiu (recomanable)
   - En cas d'estar xifats, la clau i mètode de descifratge
   - Directoris i detalls del seu contingut

2. Preservació de la prova
   - Si no pot ser reemplaçat avisar a un expert per a fer-ne una clonació
   - Preservar l'original i entregar la còpia
   - Sellar la prova amb el numero de cas

Què fer quan?

ASPERTIC

```
Disk /dev/sda - 26 GB / 25 GiB - CHS 3263 255 63
Current partition structure:
     Partition                  Start        End    Size in sectors

 1 * Linux                        0   1  1     5 254 63       96327 [/boot]
 2 P Linux                        6   0  1   514 254 63     8177085 [/]
 3 P Linux                      515   0  1  3132 254 63    42058170 [/home]
 4 E extended                  3133   0  1  3262 254 63     2088450
 5 L Linux Swap                3133   1  1  3262 254 63     2088387









*=Primary bootable  P=Primary  L=Logical  E=Extended  D=Deleted
>[Quick Search]  [ Backup ]
```

Què fer quan?

Servidors (empreses)

1. Recopilació de dades del dispositiu
    - Anotar el model i número de sèrie
    - Factura de compra del dispositiu
    - Claus de desbloqueig

2. Preservació de la prova
    - Apagar el servidor i desendollar-lo de la xarxa i la corrent
    - Avisar a un expert informàtic
        - Extreu-re'n els discs i sellar-los amb el número de cas
        - Restaurar el sistema (en el cas de no tenir backup clonar els discs)
    - Enviar el disc al laboratori d'anàlisi forense per a l'extracció de les proves

Al laboratori d'aspertic disposem també del servei de recuperació de discs malmesos

Què fer quan?

Mitjans audiovisuals i/o videovigilància

1. Recopilació de dades del dispositiu
    - Mitjà utilitzat per a crear el mitjà audiovisual
    - Anotar marca/model i numero de sèrie
    - Factura de compra del/s dispositiu/s
    - La càmera estava gravant a un espai públic o privat?

2. Preservació de la prova
    - En el cas d'un mitjà mòbil, tractar-lo com un telèfon mòbil
    - Avisar a un expert informàtic
        - Extreu-re'n la informació, hash md5/sha2 i sellar-los amb el número de cas
        - Restaurar el sistema (en el cas de no tenir backup clonar els discs)
    - Enviar els mitjans extrets al laboratori d'anàlisi forense per a l'extracció de la prova

Què fer quan?

Xarxes socials (extorsió/bullying)

1. Recopilació de dades dels comptes
   - Anotar la xarxa social
   - Anotar els noms d'usuari
   - Realització de captures de pantalla
   - Descripció dels fets i mitjans compromesos

2. Preservació de la prova
   - No contactar amb l'atacant ni pagar cap quantía econòmica
   - Que la víctima actuï de forma natural (l'agressor no ha de saber que ha denunciat)
   - Avisar als experts
     - Els psicòlegs sabran com conduïr la víctima per al trauma
     - Els pèrits informàtics sabran extreure les proves necessàries fent-se passar si s'escau per la víctima
   - Minimització de danys
     - Avisar a la resta de contactes de confiança que s'ha comès un delicte

Tipus de contravencions

Robatori

- Substrauen a la víctima el seu dispositiu
- Substrauen a la víctima les seves dades

Assetjament

- Un tercer l'hi fa la vida impossible a la víctima

Extorsió

- Un atacant obté un mitjà de la víctima i en demana una quantía econòmica (sextorsió, ransomware, etc.)

Irresponsabilitat

- Incompliment de contractes de servei

Tipus de contravencions

- Quan és un delicte penal, contravenció civil o laboral?

- Com tipificar un delicte informàtic?

- Res pot ser el què sembla, tot és falsificable a primera vista
    - Correus electrònics
    - Trucades telefòniques
    - Missatges de whatsapp/telegram
    - Vídeos
    - Etc.

Una falsificació sempre sol deixar rastres

La tecnologia,
forma part de la nostra vida... o viceversa?

La tecnologia és un món de possibilitats que es fa realitat segons cada individu, però no ens dóna més intel·ligència per saber que el nostre lliure albir pot ser una arma de doble fil.