Legedia segurtasun informatikoan

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Legedia segurtasun informatikoan

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-ISSKS-31

Legedia segurtasun informatikoan

- Europar Batasuneko ziberdelinkuentziari buruzko hitzarmena (2001)
- Espainiako kode penala
- Datu pertsonalen babesa: DBLO (LOPD)
- Datu pertsonalen babesa: DBEO (RGPD)
- Zer da informatika forentsea?
- Informatika forentsearen prozesua

Informatika-delituak

Europar Batasuneko ziberdelinkuentziari buruzko hitzarmena (2001)

- Edukiarekin lotutako delituak
- Egile-eskubideen arau-hausteekin lotutako delituak
- Informatikarekin lotutako delituak
- Datuen eta sistema informatikoen konfidentzialtasunaren, osotasunaren eta prestasunaren aurkako delituak

Edukiarekin lotutako delituak

- Haur-pornografia
- Mehatxuak
- Kalumniak
- Eduki arrazistak eta xenofoboak zabaltzea (adibidez, Alemanian eduki nazia edo holokaustoa ukatzea)

Kalumniak - Irainak (Injuria)

Kalumnia: norbaitek delitua egin duela esatea

Iraina: norbaiten duintasunaren aurka egitea

Egile-eskubideen arau-hausteekin lotutako delituak

- Jabetza intelektuala eta industriala
- Filmen eta abestien legez kanpoko kopiak banatzea
- Programa informatiko babestuen erreprodukzioa

Informatikarekin lotutako delituak

Informatikoki faltsutzea: kautoak ez diren datuak sortzea (iruzurrak, pasahitzen trafikoa, etab.) eragiten dituzten datu informatikoak aldatzea, edo ezabatzea

Datuen eta sistema informatikoen konfidentzialtasunaren, osotasunaren eta prestasunaren aurkako delituak

- Sistema informatikoetara legez kontra sartzea (intimitatearen aurkako delituak, enpresaren sekretuak ezagutaraztea, ekipo informatikoak baimenik gabe erabiltzea)
- Datuak legez kontra intertzeptatzea
- Kalteak eragiten dituzten datuen interferentzia
- Birusen banaketa

Espainiako kode penala

10/1995 Lege Organikoa

- Intimitatearen eta komunikazioen sekretuaren aurkako delituak (197.1)
- Iruzur elektronikoak (248.2)
- Jabetza intelektualeko eskubideak urratzea (270)
- Kalteen delituak (264.2)
- Ordenagailuak eta telekomunikazio-terminalak erabiltzea titularraren baimenik gabe (256)

Espainiako kode penala

10/1995 Lege Organikoa

- Dokumentu edo euskarri informatikoetan dauden sekretuak aurkitzea eta ezagutaraztea (278)
- Dokumentu elektronikoak faltsutzea (390)
- Delituak egiteko tresnak fabrikatzea edo edukitzea (400)
- Adingabeen artean material pornografikoa banatzea (186)

Espainiako kode penala

10/1995 Lege Organikoa

- Haur-pornografiaren banaketa (189)
- Kalumniak edo irainak argitaratzea

Datu pertsonalen babesa

Intimitaterako eta pribatutasunerako eskubidea: besteak bizitza pertsonalaren ezagutzatik kanpo uzteko eskubidea (sentimenduak, datu biografikoak, irudia...)

Datu pertsonalen babesa

Abenduaren 13ko 15/1999 Lege Organikoa: DBLO

Giza eskubideen adierazpena 1948: inori ez zaio arbitrarioki esku-sartzerik egingo bizitza pribatuan, familian, helbidean edo korrespondentzian, ezta haren ohoreari edo ospeari ere. Pertsona orok du legeak bera babesteko eskubidea esku-sartze edo eraso horietatik

Datu Pertsonalak Babesteko Lege Organikoa (DBLO)

Erakunde publiko, pribatu eta profesional independenteei aplikatzen zaie, ondoren tratatu, erabili edo ustiatzeko datu pertsonalak biltegiratzen badituzte (hauteskunde-errolda edo aldizkari ofizialak bezalako salbuespenekin)

DBLO: Fitxategiaren arduraduna

- Segurtasun-agiria: datu pertsonalen segurtasunaren arloan indarrean dauden legeetara eguneratua
- Beharrezko neurriak hartzea langileek segurtasunaren arloko arauak eta arau horiek ez betetzearen ondorioak ezagut ditzaten
- Erabiltzaileak identifikatzeko mekanismoa ezartzea
- Sistemaren erabiltzaileen eta datu eta aplikazioetara sartzeko eskubideen zerrenda mantentzea

DBLO: Fitxategiaren arduraduna

- Erabiltzaileek baimendutakoak ez diren eskubideak dituzten baliabideak eskuratzea saihesteko mekanismoak ezartzea
- Babes Kopiak eta datuak berreskuratzeko prozedurak egiaztatzea
- Datuak berreskuratzeko prozedurak idatziz gauzatzeko baimena ematea

DBLO: Fitxategiaren arduraduna

- Erakundeen lokaletatik kanpoko tratamendua baimentzea
- Euskarri informatikoak erakundeen lokaletatik ateratzeko baimena ematea
- Segurtasun-auditoretzetan antzemandako akatsak zuzentzeko neurriak hartzea

DBLO: Printzipioak

- **Habeas data** (Habeas corpus): datuak erabiltzailearenak dira, ez biltegiratzen dituen erakundearenak
- Datuen kalitatea: datuak zertarako bildu diren, horretarako izan behar dira egokiak, eta horretarako behar den denboran baino ez dira gorde behar
- Datuen segurtasuna
- Sekretu-betebeharra, baita harremana amaitu ondoren ere
- Datuak biltzeko informazioa

DBLO: Printzipioak

- Datuen jabearen baimena tratamendurako
- Datuak baimenarekin bakarrik lagatzea
- Lagapena beste herrialdeei: babes-maila bera duten herrialdeei bakarrik
- Bereziki babestutako datuak: osasuna, ideologia, bizitza sexuala, arraza-jatorria, erlijioa edo sinesmenak

DBLO: Eskubideak

- Informazio-eskubidea datuak biltzean
- Datuak Babesteko Erregistro Orokorra kontsultatzeko eskubidea
- Datu pertsonalak eskuratzeko eskubidea
- Zuzentzeko eta ezerezteko eskubidea
- Aurka egiteko eskubidea
- Kalte-ordaina jasotzeko eskubidea

Datuak Babesteko Euskal Bulegoa

https://www.avpd.euskadi.eus/

Datuak Babesteko Erregelamendu Orokorra (DBEO)

Herrialde guztietako arauak bateratzeko Europako araudia

2016-ko maiatzak 25

DBEO: Printzipio berriak

Erantzukizun-printzipioa (accountability): beharrezko neurri guztiak hartu direla egiaztatzeko mekanismoak ezartzea (erantzukizun proaktiboa)

Datuen babesa, lehenetsita eta diseinutik

Gardentasuna

DBEO: betebehar berriak erakundeentzat

- Datuak Babesteko Ordezkaria (DBO) izendatzea
- Kasu batzuetan pribatutasunaren gaineko eraginaren ebaluazioak
- Enpresa multinazionalek kontrol-agintaritza bakarra (leihatila bakarra) izango dute interlokutore
- Segurtasun-arrakalak 72 ordu baino gutxiagoan jakinarazi beharko zaizkie kontrol-agintaritzari eta arrail larriak dituzten erabiltzaileei
- Datu berezi gehigarriak: genetikoak, biometrikoak, zigor penalak

DBEO: betebehar berriak erakundeentzat

- Datuen nazioarteko transferentzietarako berme gehigarriak
- Erantzukizun proaktiborako zigiluak eta akreditazioak
- Fitxategiak inskribatzeko betebeharra desagertzen da
- Isun handiagoak, 20 milioi eurora edo enpresa baten fakturazioaren %20ra irits daitezkeenak

DBEO: eskubide berriak herritarrentzat

- Gardentasun eta informazio gehiago
- Ahaztua izateko eskubidea
- Tratamendua denboran mugatzeko eskubidea
- Datuen eramangarritasuna

Zer da informatika forensea?

Diziplina kriminalistikoa

Informazioa lortzeko eta prozesatzeko informatika-sistemak ikertzea (ebidentzia digitalak):

- Balio juridikoa dutenak
- Ikerketa pribatu soilerako (baimenik gabeko sarbideak, informazio-lapurreten susmoak, etab.)

Zer da informatika forensea?

Erantzuten saiatzen da:

- Zer?
- Nor?
- Zelan?
- Noiz?
- Zergatik?

Zer da informatika forensea?

Nork erabiltzen du:

- Legearen agenteak
- Aseguru konpainiak
- Konpainia pribatuak
- Pertsona arruntak
- ...

Zer da informatika forensea?

Zertan datza:

- Sistema baten informazioa erauzi
- Informazio zifratua/ezabatua/kaltetua berreskuratzea
- Sistema baten portaera monitorizatzea
- Enpresaren politiken ez-betetzeak detektatzea
- ...

Zer da informatika forensea?

Locard-en trukaketa printzipioa:

- "Bi objektuk elkar ukitzen dutenean, zati bat transferitzen diote elkarri, beste objektuari eransten zaiona"
- Ekintza guztiek arrastoa uzten dute

Zer da informatika forensea?

Heisenbergen ziurgabetasunaren printzipioa:

- "Sistema baten egoera neurtze hutsak aldatu egiten du"
- Ezin da sistema baten informazioa lortu sistema bera aldatu gabe
- Ahalik eta informazio gehien lortzea, aldaketak eta horien inpaktua minimizatuz

Zer da informatika forensea?

Ebidentzia digital baten balio juridikoa epaileak erabakitzen du

Dokumentu, log, makina etab. manipulatuak izan ahal dira

Sinadura elektroniko aitortua duen dokumentuak balio juridikoa du?

Zer da informatika forensea?

... Eta akusatuak ziurtagiria (txartela) lapurtu ziotela alegatzen badu? Salaketarik bai? Ziurtagiria baliogabetzea (Errebokatzea) eskatu al zen berehala?

Zer da informatika forensea?

Ebidentzia digitalek balio juridikoa izan dezaten, beharrezkoa da:

- Legea errespetatu da horiek lortzeko
- Informazioa zehazki jasotakoa da
- Aztertu bitartean ez da ezer aldatu/sortu/ezabatu
- Egindako analisiak erreproduzitzeko aukera izan behar du

Zer da informatika forensea?

Forensic Examination of Digital Evidence: A Guide for Law Enforcement

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

UNE 71506 - Metodología para el Analisia forense de las evidencias electrónicas

Zer da informatika forensea?

Good Practice Guide for Computer-Based Electronic Evidence

RFC 3227 - Guidelines for Evidence Collection and Archiving

ISO/IEC 27037:2012 Information technology -- Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

Informatika forensea. Prozesua

1. Identifikazioa
2. Kontserbazioa
3. Analisia
4. Azalpena

Informatika forensea. Prozesua

Ezinbestekoa da egiten den guztiaren oharrak, grabazioak, argazkiak, bideoak eta abar hartzea, data eta orduarekin

Beharrezkoa izan daiteke prozesu osoa ahalik eta xehetasun gehienekin gogoratzea epaiketa batean (urte batzuk geroago)

Identifikazioa

Ikerketan beharrezkoak izango diren sistemak (ebidentziak) identifikatzea

Gomendagarria da egiten den guztiaren fede ematen duen notarioa egotea

Komeni da argazkiak ateratzea, haien antolaera/konfigurazioa erakusteko

Identifikazioa

Hasiera-hasieratik, zaintza-katea aktibatu behar da: bildutako ebidentziak nork erabiltzen dituen zehatz-mehatz erregistratu behar da, datak, orduak, non biltegiratzen diren, zaintza-arduraduna nor den eta abar adieraziz

Martxan dauden sistemak badira, ez jarraitu erabiltzen eta informazio lurrunkor guztia jaso (sistema itzaltzean ezabatu egin daiteke): kanpoko programak erabili kopiak, sarbideak eta abar egiteko

Identifikazioa

RAM memoriaren informazioa oso garrantzitsua da (kopiatu egin behar da, ahalik eta gutxien aldatuz):

- Gauzatzen ari diren prozesuak
- Gauzatzen ari diren moduluak
- Artxibo irekiak
- Datuen bertsio desenkriptatuak

Identifikazioa

RAM memoriaren informazioa oso garrantzitsua da (kopiatu egin behar da, ahalik eta gutxien aldatuz):

- Emailen eranskinak, irudiak, chat-en zatiak
- Gako kriptografikoak
- Testu soileko pasahitzak
- ...

Identifikazioa

RAMen edukia iraultzeko tresnak:

- pd Proccess Dumper
- FTK Imager
- Volatility
- EnCase

Identifikazioa

Martxan dauden prozesuei, zerbitzuei, makinari konektatutako erabiltzaileei, portu irekiei eta abarri buruzko informazioa ere jaso beharko da

Kontuz!, notariorik ez badago, zer egin den eta zer informazio lortu den frogatzeko… Nork dio hori zela une hartan sisteman zegoena?

Identifikazioa

Informazio lurrunkor guztia bildu ondoren, sistema itzali eta hegazkorra ez den informazio guztia kopiatzen da (disko gogorrak, USBak, etab.)

Write Blocker-ak erabiltzea komeni da, informazioa eskuratzeko aukera ematen duten sistemak, baina diskoan idaztea saihesten dutenak

Identifikazioa

Kopia bit mailan egiten da: kopia forensea (horrela kopiatzen dira arrastoak eta disko gogorretik dagoen ezkutuko informazioa)

Jatorrizkoaren eta kopiaren laburpen kriptografikoa kalkulatzen (eta biltegiratzen) da, berdinak direla ziurtatzeko

Kopiaren beste kopia forentse bat egiten da, kopiak kalterik izanez gero jatorrizkoarekin lan egin beharrik ez izateko

Identifikazioa

Bit mailako klonazioa:

- dd (Linux)
- Helix3 Pro
- EnCase
- FTK Imager

Kontserbazioa

Saihestu egin behar dira (zaintza-katea):

- Galerak
- Kutsadura
- Kaltea, alterazioa, manipulazioa

Kontserbazioa

Bildutako informazio guztia zehatz-mehatz dokumentatzea

Jasotako gailu guztiak etiketatzea

Marka, modeloa, serie-zenbakia eta abar adierazi

Kontserbazioa

Data, datuak eta lekualdatzen duten eta manipulatzen duten pertsonen sinadura

Jatorrizkoa ondo bilduta geratu behar da (adibidez: notarioaren esku)

Kopia bana eman dakieke alderdi interesdun guztiei

Beti da gomendagarria babes-kopia izatea

Analisia

Lortutako informazio guztia aztertzea lan aspergarria eta "ia ezinezkoa" da

Tresna mota asko erabiltzen dira:

- Ezabatutako elementuak berreskuratzea
- Pasahitza krakeatzea
- Log-en analizatzaileak
- ...

Ordenatua eta zehatza izan behar da; analistaren intuizioa funtsezkoa da

Analisia

Informazioa bilatzeko ohiko guneak:

- Posta elektronikoak
- Mezu-tresnak
- Fitxategi ezabatuak
- Fitxategien metadatuak: sorkuntza, azken atzipena, etab.
- Nabigazioaren historiak
- Aplikazioen eta sistemaren logak
- Beste makina batzuekiko konexioak

Analisia

Garrantzitsua da sistemaren denbora-lerroa kudeatzea:

- Noiz instalatu zen X
- Noiz eskuratu zen Y
- Noiz ezabatu zen Z

Analisia

Ezinbestekoa da DBLO (LOPD) eta komunikazioen sekreturako eskubidea errespetatzea (ezin da mezu elektronikorik irakurri zure medikuarekin edo maitale batekin, ikerketarako garrantzitsuak ez badira)

Analisia

Irtenbidea: bilaketa itsua (Analistaren intuizioa)

- Ez da informazio guztia aztertzen
- Bilaketak gako-hitzen bidez egiten dira
- Gako-hitz horiek agertzen diren informazioa baino ez da aztertzen

Peritu-txosten osoa ezeztatu daiteke hori egiteko legeren bat urratu bada

Aurkezpena

Txostena egiten da prozesu osoa eta lortutako emaitzak azalduz

Nahiz eta prozesua eta lortutako emaitzak oso onak izan, txostenak behar bezala islatzen ez badu, ez dute baliorik izango

Txostena teknikariak ez diren pertsonei zuzenduta dago (epaileak, abokatuak, enpresaburuak, etab.). Ulergarria izan behar da

Txostenak inpartziala izan behar du. Perituak ez du iritzirik eman behar, frogak eta emaitzak baino ez ditu adierazi behar

Aurkezpena

Informe baten zatiak:

- Aurrekariak
- Frogak
- Analisia eta tratamendua
- Emaitzak
- Ondorioak

Aurkezpena

Aurrekariak: Zein egoeratan egin den beharrezkoa peritu baten esku-hartzea

Frogak: Bildu diren ebidentziak eta bilketarekin, bikoizketarekin, kontserbazioarekin eta abarrekin jarraitu diren prozesuak

Analisia eta tratamendua: Informazioa aztertzeko erabilitako teknikak eta tresnak

Aurkezpena

Emaitzak: argi eta ulertzeko moduan azalduko da erabilitako teknikek zer emaitza eman zituzten

Ondorioak: atalik garrantzitsuena. Bertan, adituak lortutako emaitzetatik zer ondoriozta daitekeen azaltzen du. Ondorio guztiak emaitzaren batetik eratorri behar dira, bestela suposizio hutsa da

Aurkezpena

Epaiketarik badago, adituak lekuko gisa jardungo du

Bere garaian egin zuen txostena azaldu beharko du, eta abokatuen galderei erantzun

Justiziaren moteltasuna dela eta, hainbat urte igaro ahal izan dira. Komeni da txostena berrikustea epaiketa baino egun batzuk lehenago

Aurkezpena

Batzuetan, peritu bati deklaratzera deitzen zaio, beste peritu baten txostena desegin dezan:

- Zaintza-katea hautsi zelako eta ebidentziak aldatu zitekeelako
- Txostenaren ondorioak ezin direlako lortutako emaitzetatik zuzenean eratorri
- Teknika desberdinak aplikatuta txostenean lortutakoekin kontraesanean dauden emaitzak lortzen direlako