Informazio Segurtasuna Kudeatzeko Sistemak

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Informazio Segurtasuna Kudeatzeko Sistemak

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

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Google Data Center security

Zer da segurtasun fisikoa?

Detektatzeko eta prebenitzeko mekanismoak

Sistemaren baliabideak fisikoki babesteko

Mehatxuen aurkako oztopo fisikoak eta kontrol-prozedurak aplikatzea baliabideei

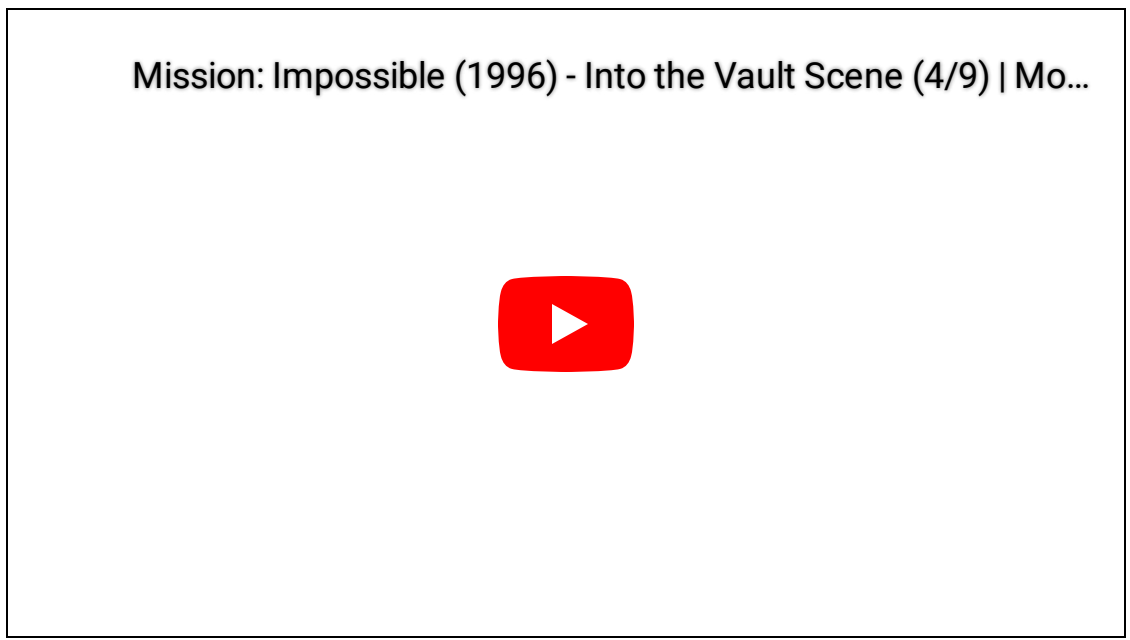
Zertarako balio du softwarea hackerren aurka babestuta edukitzeak, edozeinek ordenagailua eraman badezake?

Zer da segurtasun fisikoa?

CIAko kamera korazatua: erretinako eskaner bidezko sarbidea, hatz-markadun sarbidea, ahots-sentsoredun sarbidea, mugimendu-sentsorea, soinu-sentsorea, tenperatura-sentsorea, presio-sentsorea lurrean

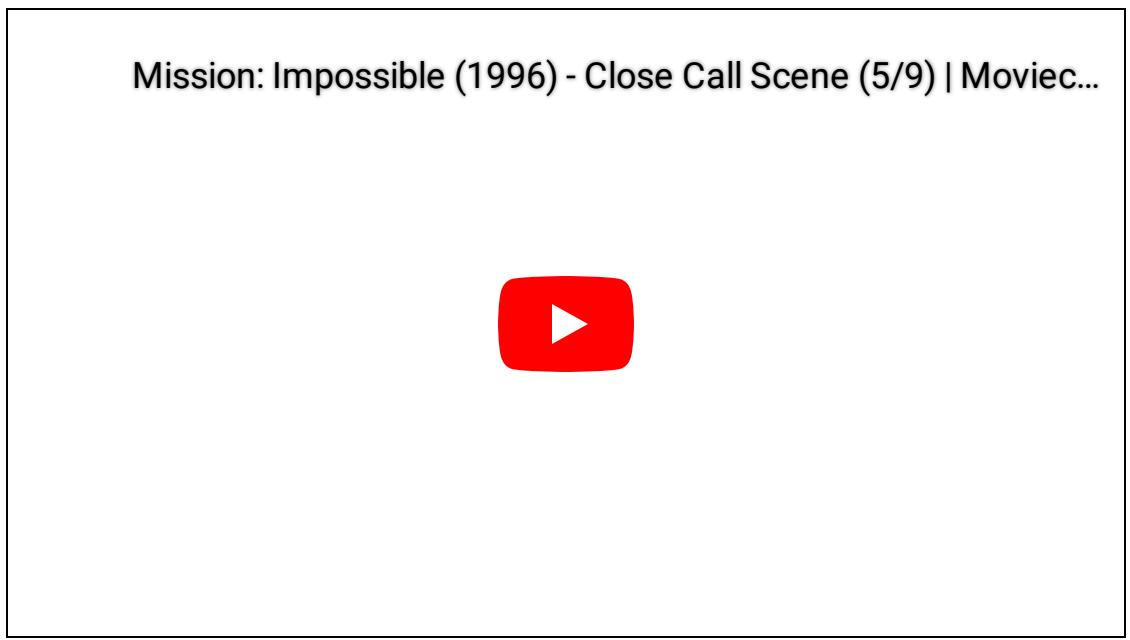
Zer da segurtasun fisikoa?

Tenperatura-sentsorea



Zer da segurtasun fisikoa?

Soinu-sentsorea



Zer da segurtasun fisikoa?

PCak pasahitz sinple bat du!

Zer da segurtasun fisikoa?

Segurtasun fisikoa logikoa bezain garrantzitsua da:

- Babestu beharreko informazioaren balioarekiko koherentea izan behar du
- Segurtasun-neurriak orekatuak
- Segurtasun-neurriak enpresak eskaintzen dituen zerbitzuei ere aplikatu behar zaizkie

Estandarrak eta segurtasun arauak

ISO (International Organization for Standardization, 1947): Nazioarteko estandarrak sortzeko erakundea, estandarizazioko hainbat erakunde nazionalez osatua

AENOR (Asociación Española de Normalización y Certificación, 1986): Normalizazio- eta zertifikazio-jarduerak garatzen ditu (N+C), produktuak eta zerbitzuak hobetzeko

Estandarrak eta segurtasun arauak

ISO 27002: Informazio-sistemen segurtasuna kudeatzeko neurriak zehazten ditu

9. kapitulua - sarbide kontrola: Erabiltzaileek enpresaren baliabideetara / zerbitzuetara duten sarbidea kontrolatzea

11. kapitulua - Segurtasun fisikoa eta ingurumenekoa: Enpresaren baliabideen segurtasun fisikoari eta ingurumen-segurtasunari buruzko alderdiak definitzen ditu

Estandarrak eta segurtasun arauak

ISO 27003 ISKS bat diseinatzeko jarraitu beharreko urratsak deskribatzen ditu.

Aplikazioaren ondorioz, ISKS ezartzeko plan bat lortzen da.

Estandarrak eta segurtasun arauak

ISO 27004: iada ezarrita dagoen ISKS baten eraginkortasuna nola neurtu definitzen du

ISO 27005: arrisku-plan bat nola sortu definitzen du

ISKS

PDCA prozesua (Plan-Do-Check-Act):

1. Planifikatu
2. Egin
3. Konprobatu
4. Jokatu

Planifikatu (1)

Gure erakundea osatzen duten arloen azterketa xehatua, hondamendi baten aurrean berreskuratze-politika bat ezartzeko balioko diguna

Arriskuen analisia: kontingentzia-plana

- Mehatxuak identifikatzen dira
- Mehatxuak beteko balira galeren balorazioa
- Informazioa babestearen kostua kalkulatzen da

Planifikatu (1)

Kontingentzia-planak honako neurri hauek biltzen ditu:

- Teknikoak
- Antolaketakoak
- Gizakientzakoak

Neurri Teknikoak

Suteen aurkako su-itzalgailuak

Ke-detektagailuak

Larrialdi-irteerak

Babes-ekipo informatikoak

Sarbideen kontrola

...

Antolaketako neurriak

Suteen asegurua

Ekipo informatikoak alokatzeko aurrekontratua eta ordezko kokapena

Backups prozedura

Sutea gertatuz gero jarduteko prozedura

Lan-arriskuen auditoria-zerbitzu bat kontratatzea

...

Gizakientzako neurriak

Sutea gertatuz gero, jokatzeko prestakuntza

Aretoko arduradun bat izendatzea

Rolak eta erantzukizunak esleitzea segurtasun-kopiarako

...

Planifikatu (1)

Kontingentzia-planak azpiplanak ditu:

- Babesa
- Larrialdia
- Berreskuratzea

Planifikatu (1)

Babes plana:

- Zer egin mehatxua gertatu aurretik
- Helburua: mehatxua ez gauzatzea
- Su-itzalgailuak berrikustea, sute-simulazioak, babeskopiak egitea (+ berreskuratzeko testak) , ...

Planifikatu (1)

Larrialdi plana:

- Zer egin mehatxua gertatzen den bitartean edo justu ondoren
- Helburua: mehatxua gauzatzearen ondorio kaltegarriak arintzea
- Ekipo informatikoak alokatzeko aurrekontratua aktibatzea, babeskopiak berreskuratzea , ...

Planifikatu (1)

Berreskuratze plana:

- Zer egin mehatxua kontrolatu ondoren
- Helburua: mehatxua gauzatu aurretik zeuden egoerara ekartzea gauzak
- Kalteen ebaluazioa, larrialdiko kokalekutik ohikora datuak eramatea, alokairu-aurrekontratua desaktibatzea, aseguru-etxeari erreklamazioak egitea, ...

Planifikatu (1)

Kontingentzia plana ez da mugatu behar neurri batzuk zerrendatzera. Honako hauek ere jaso behar ditu:

- Zer baliabide material behar dira
- Zein pertsona daude inplikatuta plana betetzeko
- Zein dira pertsona horien erantzunkizun zehatzak eta planaren barruan duten rola
- Zein jarduera-protokolori jarraitu behar dioten

Egin (2)

Ondasunak babesteko egokitzat jotako kontraneurriak inplementatzen dira

Hainbat motatako kontraneurriak: arriskuak arintzea, galerak gutxitzea, susperraldi azkarra ziurtatzea

Funtsezkoa: eragindako langileei prestakuntza eta informazioa ematea

Konprobatu (3)

Aldizkako berrikuspenak (auditoriak)

Bereziki mehatxu bat gauzatu ondoren

Bermatzen du:

- Mehatxu berrien aurrean eguneratzea
- ISKSaren funtzionamendu zuzena

Jokatu (4)

Egiaztapenaren emaitza

Aurreikusitako mehatxua, neurriak eraginkorrak: alderdi txikiak berrikustea eraginkortasuna hobetzeko

Aurreikusitako mehatxua, eraginkortasunik gabeko neurriak: akatsaren arrazoia aztertzea eta neurriak proposatzea

Mehatxuak

Gizakiek eragindakoak

Hondamendi naturalek eragindakoak

Ingurunearen alterazioak

Informaziorako sarbidea euskarri fisikoan

Mehatxuak (Gizakiak)

Zibererasotzaile bat sar al daiteke informatika-sistema itxietan eta ekipoak zuzenean ukitu gabe?

Mehatxuak (Gizakiak)

Mehatxuak (Gizakiak)

Sistema batera fisikoki sartzeko aukerak erabilitako segurtasun-neurriak alferrikakoak izatea eragin dezake

Eremu seguruak ezarri behar dira

Batzuetan ez dago sistemara fisikoki sartu beharrik ere (TEMPEST erasoa)

Mehatxuak (Gizakiak)

Jario elektromagnetikoak eraso-bektore bat izan litezke

Nola hartu jariatze elektromagnetikoak? Aparatu elektroniko guztiek igortzen dituzte erradiazioak eta jarioak seinale elektromagnetiko eta akustiko moduan

Mehatxuak (Gizakiak)

Distantzia eta mugikortasuna bezalako hainbat faktoreren arabera, antenen edo sentsibilitate handiko mikrofonoen bidez har daitezke osagaien seinaleak (seinale akustikoen kasuan) eta informazioa lortzeko prozesatu

Aparatu horien artean **monitoreak** eta **teklatuak** daude: beraz, zibererasotzaileek ere erabil ditzakete

Mehatxuak (Gizakiak)

Informazio kritikoa edo sentikorra prozesatzeko instalazioek segurtasun-perimetro bat duten eremu babestuetan egon behar dute, honako hauek definituta:

- Hesiak
- Sarbide-kontrol egokiak

Babesak identifikatutako arriskuekiko proportzionala izan behar du

Mehatxuak (Gizakiak)

Babestutako eremu batera sartzeko kontrola: segurtasuneko langileak, giltzak, sartzeko txartelak, PIN, sistema biometrikoa...

Mehatxuak (Gizakiak)

Sistema biometrikoak: pertsonak ezaugarri fisiko baten arabera identifikatzen dituzten sistemak:

- Aztarna digitala
- Esku-ahurra
- Begi-patroiak
- Aurpegia ezagutzea
- Ahots egiaztapena
- Ibilera egiaztatzea

Mehatxuak (Gizakiak)

Eremu babestuetako bisitariak ikuskatu egin behar dira

Sarrera-irteeren data eta ordua erregistratu behar dira

Helburu espezifiko eta baimenduekin sartu ahal izango da

Bisitariari inguruko segurtasun-neurriak irakatsi behar zaizkio

Mehatxuak (Gizakiak)

Sarbideak aldizka ikuskatu behar dira

Sarbideei buruzko informazioa ere babestu egin behar da

Gomendagarria da identifikazio ikusgarri bat etengabe eramatea

Langileak identifikatu gabeko pertsonen berri ematera animatzea

Mehatxuak (Gizakiak)

Enplegatu guztiek ez dute jakin behar zer egiten den eremu babestuan

Okupatu gabeko eremu babestuak blokeatuta geratu behar dira

Ezin da argazki-kamerak, mugikorrak eta abar sartzen utzi

Mehatxuak (Gizakiak)

Inicio / **Política**

Fotos del príncipe Guillermo como piloto revelan información clasificada

EFE - Londres

20/11/2012 - 20:13h

Me gusta 0 Twittear 1

La web de los duques de Cambridge de Inglaterra tuvo que retirar hoy unas fotos del príncipe Guillermo como piloto militar después de que el Ministerio de Defensa británico advirtiera de que mostraban información clasificada.

Las imágenes se publicaron esta mañana en la web del príncipe Guillermo y la princesa Catalina, en un intento de mostrar el trabajo del nieto de Isabel II como capitán de la Real Fuerza Aérea Británica en la base de rescate de Anglesey (Gales).

Mehatxuak (Hondamendi naturalak)

Lurrikarak, Sua, Ekaitz elektrikoak, Uholdeak

Enpresaren segurtasun-politikan kontuan hartu behar dira

Mehatxuak (Hondamendi naturalak)

Informazioa galtzea

Ekipamendua galtzea

Berreskuratzeko denbora = dirua

Erresilientzia: kontrako egoera bat gainditzeko gaitasuna

Mehatxuak (Hondamendi naturalak)

Zer gertatu zen egoitza Windsor Dorrean (2005) zuten enpresekin?

Bulego-eraikin horretan Deloitte aholkularitza-etxea (32 solairutatik 20 hartzen zituen) eta Garrigues abokatu-bulegoa zeuden

Mehatxuak (Hondamendi naturalak)

Deloitte:

- Ondo prestatuta
- Hurrengo astelehenean baldintza "normaletan" lan egitea

Garrigues abokatu-bulegoa:

- Segurtasun-kopiak eraikin bereko beste solairu batean
- Informazio-kopuru handiak galdu zituzten

Mehatxuak (Hondamendi naturalak)

Deloitte:

Datu guztien kanpoko segurtasun-kopiak, eta dokumentu fisikoko informazio guztia euskarri informatikoan zegoen

Backup horiek enpresarenak ez diren beste leku batzuetan kudeatzen dira, eta, horrela, segurtasun-araudiak, Datuak Babesteko Legea (DBLO) eta

Mehatxuak (Hondamendi naturalak)

Disaster Recovery Institute Internationalen arabera, datuen galera esanguratsuak dituzten enpresen % 90ek porrot egiten dute 3 urteko epean

Hondamendien aurreko kontingentzia-neurriak, datuen babesa, ezinbesteko zeregina da enpresa batek bere negozioaren garapenean jarraipena izan dezan

Mehatxuak (Hondamendi naturalak)

Texasko Unibertsitatearen ikerketa baten arabera, datuen galera katastrofikoa duten enpresen % 6k baino ez du biziraungo; % 43k, berriz, ez du bere negozioa berriro irekiko, eta % 51k, berriz, 2 urteko epean itxi beharko du

Mehatxuak (Hondamendi naturalak)

Zein da enpresa batek bere biziraupena arriskuan jarri gabe jasan dezakeen jarduerarik ezaren gehieneko aldia?

- Aseguruen sektorea: 5,6 egun
- Fabrikazio-sektorea: 4,9 eguneko
- Industria-sektorea: 4,8 eguneko
- Banaketa-sektorea: 3,3 egun
- Finantza-sektorea: 2,0 eguneko

Mehatxuak (Hondamendi naturalak)

Lurrikarak:

- Kokapenaren araberako probabilitatea
- Bibrazio txikiek makinaria delikatua hondatu dezakete
- Inguruko obrek bibrazioak sor ditzakete
- Prebentziozko konponbideak
- Irtenbide arkitektonikoak
- Kokaleku egokiak
- Eraikinaren babesak

Mehatxuak (Hondamendi naturalak)

Sua:

- Instalazio elektriko txarra
- Hutsegite pertsonalak, hala nola ordenagailu-gelan erretzea
- Itzaldu gabeko zigarro bat botatzen den gaizki kokatutako paperontziak
- Sistemak kearen aurrean dituen ahultasunak

Mehatxuak (Hondamendi naturalak)

Sua (Prebentzio neurriak):

- Kea eta beroa detektatzea
- Suaren aurkako materialak
- Makinetatik bereizitako paperaren biltegia
- Zoru faltsuaren egoera berrikustea
- Berrikusitako su-itzalgailuak

Mehatxuak (Hondamendi naturalak)

Ekaitz elektrikoak:

- Tentsio-igoerak
- Prebentziozko konponbideak
- Tentsio-mugatzaileak
- Korronteen egonkortzaileak
- SAI (Etengabeko elikadura-sistema)

Mehatxuak (Hondamendi naturalak)

Uholdeak eta antzekoak:

- Enpresaren berezko arrazoiengatiko uholdeak
- Besteren arrazoiengatiko uholdeak
- Gertakari pertsonal txikiak (ur botila , kafedun katilua)

Mehatxuak (Hondamendi naturalak)

Uholdeak eta antzekoak (irtenbide prebentiboak):

- Larrialdietako drainatze-sistemak instalatzea
- Enplegatuen adostasuna
- Uraren hodiak berrikustea
- Ekipamenduaren kokapena

Mehatxuak (Hondamendi naturalak)

Mehatxuak (Alteraciones del entorno)

- Tenperatura
- Hautsa
- Intsektuak
- Prebentzio-irtenbideak
    - Hozte-sistemak
    - Garbiketa
    - Ganbera korazatuak
    - Iragazkiak

Mehatxuak - Acceso a información en soporte físico

Isilpeko informazioa ateratzeko edozein gailu segurtasun-eremu batean egon behar da

- Gailu berriak
- Datuak inprimatzeko edo ateratzeko baimenak , benetan behar duten erabiltzaileentzat
- Inprimatu soilik erabiltzaileak eskatuta (txartel adimendunak)
- Segurtasun-arloa uztean enplegatuen berrikuspena