

ISSKS Sarrera

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



ISSKS Sarrera

DOI 10.5281/zenodo.5506995

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



Zer da segurtasuna informatikoa?

Ondasunak (Zerbitzuak): babestu nahi duguna (Datuak, softwarea, hardwarea, azpiegitura, langileak, informazioa, ...)

Arriskua: Kalteak jasan edo desagertzeko posibilitatea (Lapurketak, ondatzea, aldatzea, ordezkatzeta, ...)

Zer da segurtasuna informatikoa?

Hauek bermatzeko egiten direnak:

- Ondasunak behar bezala erabiltzen dira
- Ondasunek sarbidea behar denari bakarrik ematen diete
- Ondasunek legeak eta araudiak betetzen dituzte

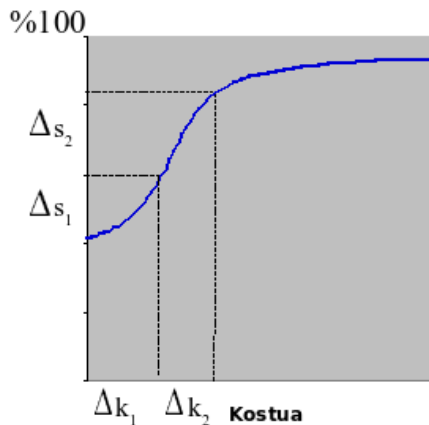
Zer da segurtasuna informatikoa?

Xedeak:

- Arriskuak eta mehatxuak detektatzea, halakorik gerta ez dadin edo haien eragina txikiena izan dadin
- Ondasunen erabilera egokia bermatzea
- Izan daitezkeen galerak mugatzea eta sistema lehenbailehen berreskuratuko dela ziurtatzea
- Dagokion legeria betetzea

Zer da segurtasuna informatikoa?

Ezinezkoa 100% segurtasuna lortzea: segurtasuna prozesu bat da, ez egoera bat



Nori dagokio segurtasun informatikoa?

Segurtasun-administratzailea:

- Segurtasun informatikoaren ardura eta erabakiak hartzen dituen
- Segurtasuna planifikatu eta inplementatu

Nori dagokio segurtasun informatikoa?

Zuzendaritza:

- Segurtasuna enpresaren helburu estrategikoa izan behar da
- Dirua inbertitu behar du
- Segurtasun informatikoko saila antolatu

Nori dagokio segurtasun informatikoa?

Erabiltzaileak:

- Prestakuntza
- Segurtasun-politika ezagutu behar dute
- Legedia ere ezagutu behar dute

Arriskuen analisia

Babestu nahi diren ondasunen identifikazioa

Ondasun horien balioaren (B) estimazioa

Aipatutako ondasunek jasaten dituzten mehatxuen identifikazioa

Mehatxu horiek egi bihurtzeko probabilitatearen (P) estimazioa

Arriskuen analisia

Mehatxu horietako bakoitzaren arriskuak gutxitzeko neurrien azterketa

Neurri horien kostuaren (K) azterketa

$$K < P * B$$

Segurtasunaren printzipioak

- Konfidentzialtasuna
- Osotasuna
- Prestasuna
- Kautotzea
- Zapuztezintasuna

Konfidentzialtasuna

Bildutako edota transmititutako informazioa soilik baimendutako alderdiek atzi dezaketela ziurtatzen du

Osotasuna

Bildutako edota transmititutako informazioa soilik baimendutako alderdiek alda dezaketela ziurtatzen du

Prestasuna

Bildutako edota transmititutako informazioa oztopo edo degradaziorik gabe baimendutako alderdiek erabil dezaketela ziurtatzen du

Kautotzea

Transmititutako informazioaren jatorria modu fidagarrian identifikatzen dela ziurtatzen du

Zapuztezintasuna

Transmititutako informazioaren igorleak edo jasotzaileak transmisioa ukatzerik ez daukatela ziurtatzen du

Adibideak

El ciberataque de Wanna Cry que ha afectado a casi todo el mundo

El viernes, 12 de mayo, nos hacíamos eco de una noticia que afectaba a varias empresas españolas, entre ellas, Telefónica. Esta teleoperadora, entre otras compañías, había sufrido un ciberataque en su red corporativa informática. Se trata del **"ransomware" Wanna Cry**, un virus informático malicioso tipo "malware". Este virus ha afectado a más empresas, entre ellas, a la compañía aérea Iberia.

<https://www.elrincondelombok.com/internet/el-ciberataque-de-wanna-cry-que-ha-afectado-a-casi-todo-el-mundo/>



Adibideak



<https://www.genbeta.com/seguridad/ciberatacante-destruye-miles-bases-datos-mongodb-elasticsearch-deja-solo-firma-miau>



Adibideak

AGOSTO 15, 2020 – JULIO SAN JOSÉ

MAPFRE víctima de un ataque de ransomware.

El ransomware y lo cibercriminales no descansan ni en vacaciones.

Hace escasas horas, la aseguradora admitió en una publicación por Twitter, que el retraso en su atención se debía que estaba siendo víctima de un ataque de ransomware:



<https://derechodelared.com/mapfre-victima-de-un-ataque-de-ransomware/>

Adibideak

LinkedIn, «hackeada», recomienda a los usuarios a cambiar la contraseña

https://www.abc.es/tecnologia/redes/abci-linkedin-hackeada-recomienda-usuarios-cambiar-contrasena-201605191319_noticia.html

Adibideak

CIBERDELINCUENCIA • Malware informático

Un expleado deja un virus informático en su antigua empresa para robar sus clientes

<https://www.elmundo.es/madrid/2019/05/22/5ce5280afdddf7b688b46a2.html>

Adibideak

El ordenador de Merkel en el Bundestag sufrió un ciberataque

EFE / BERLÍN | Día 14/06/2015 - 10.22h

- El equipo de la canciller se utilizó también para enviar correos electrónicos infectados a otros políticos

Publicidad

<https://www.abc.es/internacional/20150614/abci-ordenador-merkel-ciberataque-201506141013.html>

Adibideak

Hazte socio/aInicia sesión

CoronavirusMascarillasVuelta al coleMemoria históricaJosé Luis Martínez-AlmeidaJuan Carlos I+ Temas

Todos los programas de espionaje de la NSA desvelados por Snowden

El último de los programas de espionaje masivo desvelado por Edward Snowden es MYSTIC, que permite la grabación del 100% de las llamadas telefónicas de un país

El ciberespionaje de la NSA incluye desde el análisis de metadatos a la recopilación de mensajes de texto (SMS) o la propagación de virus informáticos ("malware")

Cuáles son y cómo funcionan los programas de espionaje de la NSA

https://www.eldiario.es/turing/vigilancia_y_privacidad/nsa-programas-vigilancia-desvelados-snowden_1_4974573.html

Espioitza eta informazio konfidentzialaren lapurketa

"Bere askatasunari segurtasunagatik uko egiten dionak ez du merezi ez bata ez bestea" B. Franklin

Vigilancia permanente. Edward snowden. Grupo Planeta, 2019.

Adibideak

La web para infieles 'hackeada' disponía de 39.000 perfiles de ciudadanos vascos

Bilbao, con 10.523 inscritos en Ashley Madison, lidera la lista de contactos vascos, seguida por Durango y San Sebastián. Vitoria sólo cuenta con 311 afiliados



<https://www.elcorreo.com/bizkaia/tecnologia/internet/201508/23/para-infieles-hackeada-disponia-20150821190325.html>

Adibideak

NOTICIAS > ECONOMÍA

LOS TRABAJADORES NO TIENEN PROBLEMAS



Un hackeo de la web del Banco de España la deja prácticamente inoperativa

Aunque desde la institución defienden que no existe riesgo de filtración de datos, el funcionamiento normal de la página web todavía no ha vuelto.



https://www.antena3.com/noticias/economia/hackeo-web-banco-espana-deja-practicamente-inoperativa_201808275b8427f90cf26ed5cf1aaf4e.html

Adibideak

NOTICIAS > ESPAÑA

DURANTE EL DEBATE DE INVESTIDURA



Anonymous hackea la página web del Congreso de los Diputados para "rodearlo a nuestra manera"

Un grupo de activistas aprovecha el **debate de investidura** de **Mariano Rajoy** para utilizar la página web del **Congreso de los Diputados** para "rodearlo", mientras **miles de personas asisten a la convocatoria** de 'Rodea el Congreso'.

www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=*****

loda: java lang.NumberFormatException: For input string:

Las que la impericia del programador ((mode pitorreo sano on) amiguetes, las excepciones en JavaScript hay que saber gestionarias cuando se curra para tan elevada entidad (mode pitorreo sano off)) nos permite a unos interesantes (por llamarlos de alguna forma). Este es uno de esos casos, y aunque queda feo escribir sin acentos y obviando algunos caracteres para mejorar la visibilidad del texto, la vamos a utilizar para "ro

https://www.lasexta.com/noticias/nacional/hackean-la-pagina-web-del-congreso-de-los-diputados-para-rodearlo_201610295814e4680cf24962cc0c6aba.html

Adibideak

[Home](#)
[Videos](#)
[Twitter](#)
[Archive](#)
[Mobile](#)
[RSS](#)

[Text](#)
 Agosto 02, 2020
 [6 notas](#)

[ABOUT](#)

Half-track en AVALMADRID

Tras tanta demora y vista la expectación, vamos a desvelaros dónde estaba uno de nuestros half-tracks: en AVALMADRID 🤖

¿Y qué hacíamos allí tanto tiempo? Pues ver documentos y documentos de préstamos, de embargos... A los periodistas les encataría 🤖 El caso es que a nosotras más que encantarnos, nos divierte.

Y es que, por ejemplo, ahora sabemos que Elena González-Moñux Vázquez, ex concejala del Ayuntamiento de Madrid y diputada en la Asamblea de Madrid por el Partido Popular, tenía su sueldo y sus cuentas corrientes bajo amenaza de embargo en 2019. ¿Qué habrá pasado?

Cópula de la primera página del documento principal del mensaje enviado con ELJANET 2019101040710 y Fecha de Presentación: 05/10/2019 08:03

AL JUZGADO 1 INSTANCIA 10 DE MADRID

Ejecución Título No Judicial [REDACTED]
 Parte demandante: AVALMADRID S.G.R.
 Parte demandada: ELENA GONZALEZ MOÑUX, RICARDO JOSE FERNANDEZ GIL, PLANAIR S.A.

Inglourious /b/asterds

Adibideak



The screenshot shows the top of The Register website. The header is red with the logo "The Register" and the tagline "Biting the hand that feeds IT". Below the header is a navigation bar with links: DATA CENTRE, SOFTWARE, SECURITY, DEVOPS, BUSINESS, PERSONAL TECH, SCIENCE, EMERGENT TECH, BOOTNOTES, and VENDOR VOICE. There are also icons for a user profile and a search function.

Below the navigation bar is a banner for Dynatrace. It features the Dynatrace logo, a "Leader badge 2020", and a bar chart comparing Dynatrace (95%) and AppDynamics (84%). The text "Is the product heading in the right direction?" is above the chart, and a "Read the report" button is to the right.

Below the banner is a section titled "SECURITY" with a red asterisk. The headline reads: "Intel NDA blueprints – 20GB of source code, schematics, specs, docs – spill onto web from partners-only vault". Below the headline is a sub-headline: "Leaker only 'a bit concerned' about getting sued".

https://www.theregister.com/2020/08/06/intel_nda_source_code_leak/

Adibideak

JUSTICIA CIERRA TEMPORALMENTE EL PORTAL

Un fallo en el sistema telemático de Justicia permitió acceder a todos los casos abiertos

Un fallo de permisos en el sistema telemático del Ministerio de Justicia ha dado acceso durante horas a abogados y procuradores a los casos judiciales del resto de profesionales en el sistema



https://www.elconfidencial.com/tecnologia/2017-07-27/lexnet-justicia-sistema-telematico_1421771/

Adibideak

Una ciudad de Florida pagará más de 600.000 \$ por un rescate de ransomware

<https://news.sophos.com/es-es/2019/06/24/una-ciudad-de-florida-pagara-mas-de-600-000-por-un-rescate-de-ransomware/>

Adibideak

TELEFONÍA MÓVIL ›

El timo de la SIM duplicada: si su teléfono hace cosas raras, revise la cuenta bancaria

El fraude conocido como 'sim swapping', muchas veces precedido por el robo de otros datos, ha ganado relevancia en los últimos años, según la Guardia Civil y los expertos

https://elpais.com/economia/2019/05/21/actualidad/1558455806_935422.html

Adibideak

SEGURIDAD

Criminales utilizan deepfakes de audio para hacerse pasar por CEOs y robar a empresas

By Jorge Quijje - Jul 22, 2019

<https://www.tekcrispy.com/2019/07/22/deepfakes-audio-empresas/>

Adibideak

NAVARRA

Salud debe pagar 125.000 euros por un acceso "ilegítimo" a un historial clínico

DIJES PAMPLONA

A+ A-

■ Los datos fueron consultados 2.825 veces por 417 usuarios integrados en 55 servicios y procedentes de todos los centros sanitarios, cuando la paciente "sólo estuvo en un hospital y en cuatro servicios"

Actualizada 22/02/2012 a las 18:26

Comentarios 14

Twitter 34

Me gusta 38

Tuenti

+1 2

Anuncios Google

Salud Médico Médico Salud Médica Salud La Salud

La Sala de lo Contencioso-Administrativo del **Tribunal Superior de Justicia de Navarra** (TSJN) ha confirmado una condena de 125.000 euros al **Servicio Navarro de Salud** por el acceso "ilegítimo" y masivo, por parte del personal sanitario, al historial clínico de una paciente fallecida.

La sentencia, que es firme y obliga a retirar las **fotografías de la historia clínica**, establece que se ha producido un funcionamiento "anormal" en el sistema sanitario público navarro "en la medida en que ha

https://www.diariodenavarra.es/noticias/navarra/mas_navarra/salud_debe_pagar_125_000_euros_por_acceso_ilegitimo_historial_una_paciente_70815_2061.html

Adibideak



<https://www.businessinsider.es/consiguen-abrir-arrancar-tesla-model-3-traves-movil-dueno-1062031>

Adibideak



<https://www.xataka.com/seguridad/log4shell-vulnerabilidad-critica-proporciones-catastroficas-que-amenaza-destrozar-internet>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>

Adibideak



<https://unaaldia.hispasec.com/2020/07/doki-el-nuevo-malware-de-linux-fija-como-objetivo-las-apis-de-contenedores-docker-mal-configurados.html>

Adibideak



ransomware cafetera

<https://computerhoy.com/noticias/tecnologia/ransomware-maquinas-cafe-cafetera-726041>