Mesa redonda: Retos de una sociedad digital

La ciberseguridad creará 3,5 millones de empleos en todo el mundo para 2021.

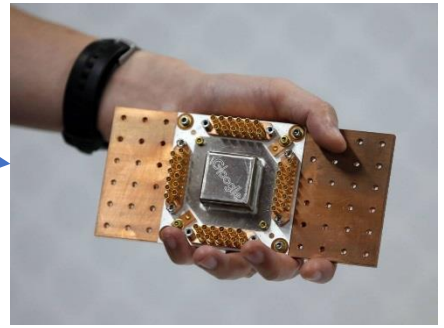
Ref: Informe de riesgo de datos de Varonis

Dr. Llorenç Huguet i Rotger
Universitat de les Illes Balears

Avances tecnológicos y en algorítmica

- Computación en la nube.
- Big Data (Análisis masivo de datos).
- Inteligencia Artificial.
- Internet de les cosas (IoT).
- Computación cuántica

- Temas éticos
- Ciberseguridad



Procesador cuántico de Google 2020

Grupo de Balears

Ciberseguridad

La pandemia COVID-19 ha propiciado el teletrabajo y con ello se han aumentando los ataques a la seguridad computacional en los dispositivos interconectados y en la cada vez más extendida red de puntos de IoT (Internet de las cosas).

Cada puesto de teletrabajo es un objetivo del ciberdelicuente.

La evolución del 5G implica un aumento del ancho de banda lo que conlleva un aumento de vulnerabilidad de los dispositivos conectados.

Es necesario, imprescindible, profundizar en el conocimiento en ciberseguridad, empezando por la concienciación y la prevención de sus efectos así como en las buenas prácticas para “evitar” los ataques de virus cibernéticos.

Llorenç Huguet

Ataques a la seguridad

Malware: *Software provocando intencionadamente un mal funcionamiento del sistema informático (*Virus cibernético*):*

- El 94% del malware se envía por correo electrónico.
- El 48% de los archivos adjuntos de correo electrónico maliciosos son archivos de Office.
- El 53% de las empresas encontraron más de 1000 archivos confidenciales abiertos para cada empleado.

Grupo de Balears

Ataques a la seguridad

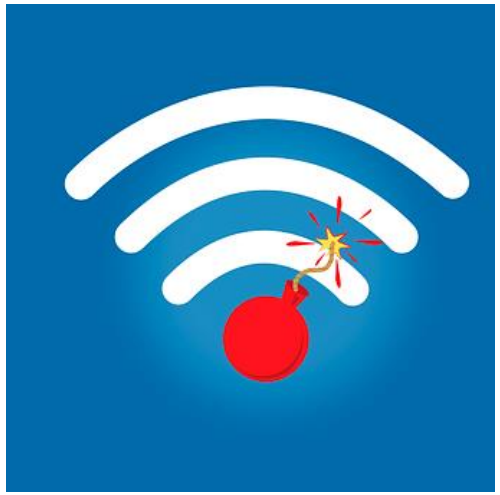
DDos: *Denegación de servicio Distribuido*

- Para 2023, el número total de ataques DDoS en todo el mundo se estima en más de 15 millones.

IoT: *Internet de las cosas*

- El gusano DDoS distribuido por Mirai fue la tercera amenaza de IoT más común en 2018.
- Los ataques a dispositivos IoT se triplicaron en la primera mitad de 2019.
- Los dispositivos de IoT experimentan un promedio de 5.200 ataques por mes.

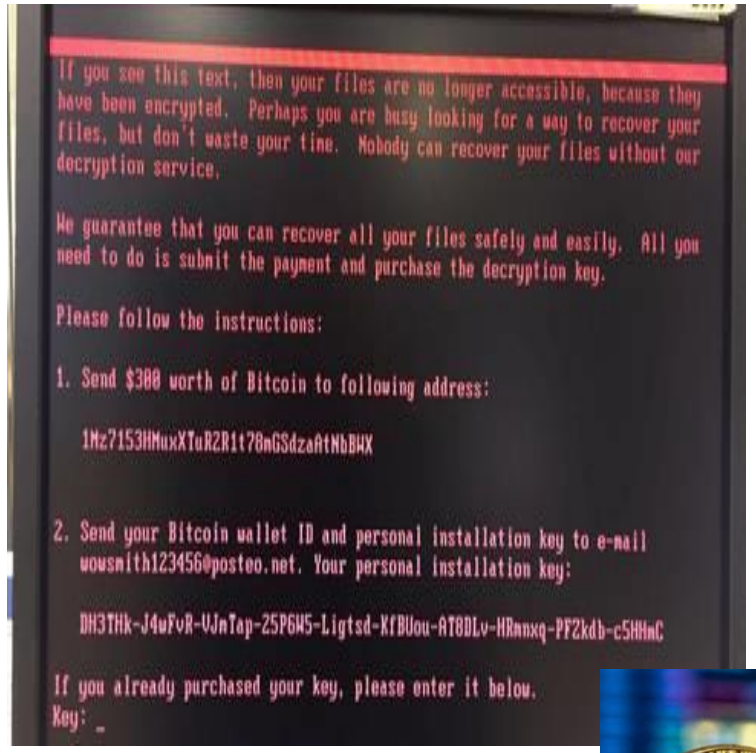
Ataques a la seguridad



Phishing: *Suplantación de identidad*

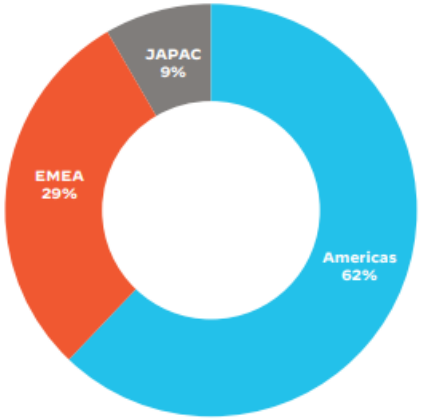
- El phishing aumentó en 2020 afectando a 1 de cada 4200 correos electrónicos.
- Los ataques de phishing representan más del 80% de los incidentes de seguridad notificados.
- El 47% de los empleados citó la distracción como la razón para caer en una estafa de phishing mientras trabajaba desde casa.

Ataques a la seguridad



Ransomware: *Secuestra archivos, los cifra, y el hacker solicita un rescate a cambio de descifrarlos.*

- El pago promedio de rescate medio fue de $312,493 en 2020. En 2019 que fue de $115,123.
  - La mayor demanda fue de $30 millones en 2020 (desde $15 millones en 2019).
  - En 2016, las transacciones estaban entre $200 y $ 500.
- Es una de las mayores amenazas cibernéticas que enfrentan las organizaciones.
  - Americas (62%); EMEA (Europa, Oriente Medio y África (29%) y JAPAC (Japón y Asia-Pacífico (9%).



Grupo de Balears

Estadísticas de ciberseguridad

Râmnicu Vâlcea, «Hackerville», ciudad de Rumanía capital del cibercrimen.

El cibercrimen ya mueve más dinero que el trafico de drogas.

- El 95% de los fallos de ciberseguridad son causadas por “errores humanos”.
- Se estima que se utilizan 300.000 millones de contraseñas.
- El 90% de las organizaciones sufrieron intentos de spear phishing en 2019.
- Los ataques a datos expusieron 36.000 millones de registros en el primer semestre de 2020.
- Los datos personales estuvieron involucrados en casi el 60% de las infracciones en 2020.
- El teletrabajo ha causado una brecha de seguridad en el 20% de las organizaciones.
- El mayor motivo para las infracciones fueron de tipo económico.

Grupo de Balears

Estadísticas de ciberseguridad COVID-19

COVID-19 ha impactado al ciberespacio, especialmente al ámbito de la salud.

- Desde que comenzó la pandemia, el FBI informó un aumento del 300% en los delitos cibernéticos denunciados.
- El 27% de los ataques cibernéticos de COVID-19 se dirigen a organizaciones de atención médica.
- Las filtraciones de datos en el ámbito de la salud aumentaron en un 58% en 2020.
- En abril de 2020, Google bloqueó 18 millones de correos electrónicos de phishing y malware diarios relacionados con el coronavirus.
- Medio millón de cuentas de usuario de Zoom se vieron comprometidas y vendidas en un foro de la web oscura en abril de 2020.
- Los ciberataques basados en la nube aumentaron un 630% entre enero y abril de 2020.

Mutacions de ransomware 2020

"Hackeado" por el virus que Ryuk.

A lo largo de 2020, Ryuk atacó industrias de la energía y la alta tecnología, así como a organizaciones educativas, sanitarias y gubernamentales.

Virus (*)	Año de aparición	Rescate/grupo hackers
WastedLocker	2020	>$10M /Evil Corp
Maze (ChaCha)	2019	$4,8M
Revil (SodinoKibi)	2019	$4,8M
Zeppelin	2019	$13K, $35K
Phobos	2019	$8K, $50K
NetWalker (Mailto)	2019	$100K, $2M / Circus Spider
DoppelPaymer	2019	$50K, 1,5M / Indrik Spider
Ryuk	2018	$600K, $10M / Wizard Spider
GandCrab	2018	$18K, $1.3M
WannaCry	2017	$300, $600
Dharma	2016	$1K, $150K

(*) Palo Alto Report

Llorenç Huguet

Organismos de ciberseguridad

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Entidad pública española de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas y sectores estratégicos.

Gestionó en 2020 133.000 incidentes, un 24% más que en 2019.

Contribuye a la ciberseguridad a nivel nacional e internacional, la prestación de servicios y la coordinación con los agentes con competencias en la materia.

www.incibe.es

Agencia de la Unión Europea para la Ciberseguridad

ENISA es un centro de conocimientos especializados para la seguridad cibernética en Europa y ayudar a los países que la integran a prevenir, detectar y dar respuesta a los problemas de ciberseguridad.

ENISA ofrece soluciones y asesoramiento prácticos a los sectores público y privado de los países de la UE y a las instituciones europeas.

www.enisa.eu

Ciberseguridad en la Unión Europea

Agencia Europea de Seguridad de las redes y de la información(ENISA)

Estrategia para una Sociedad de la información segura

Estrategia Europea de Seguridad

Plan de Ciberseguridad de la UE

Directiva de seguridad en las redes (SRI)

Lucha contra la ciberdelincuencia:

Centro Europeo de Ciberdelincuencia (Europol)

- Plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT).
- Lucha contra los ciberataques, en particular los que siguen un modelo de negocio del delito como servicio.

Directiva de la UE relativa a los ataques contra los sistemas de información (Diario Oficial de la UE)

Llorenç Huguet

Grupo de Balears

Informes sobre ciberseguridad

- Informe sobre el estado de la resiliencia cibernética 2020 de Accenture
- Informes de ciberseguridad de Cisco
- Estudio de trabajo de Cybersecurity Venture
- Informe anual de gobierno de IAPP-EY
- Informe de IBM sobre el costo de la filtración de datos de 2020
- Informe de amenazas de McAfee Labs
- Informe de amenazas a la seguridad en Internet de Symantec
- Informe de violación de datos basado en riesgo
- Informe de riesgo de datos de Varonis
- Informe de investigaciones de filtración de datos 2020 de Verizon

Llorenç Huguet

Hemos migrado, forzadamente, del mundo analógico al mundo digital a causa de un virus biológico.

Instalados en este nuevo paradigma de la sociedad digitalizada, pensemos por un momento:

¿Qué pasaría si este mundo sufriera una pandemia provocada por un virus digital?

Paralización y caos!...

paralización económica y caos social.

Muchas Gracias

l.huguet@uib.es
llhuguetr@gmail.com