Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

Ciberseguretat: "Careful where you step"



<img src="https://tec.mx/sites/default/files/styles/header_full/public/2021-08/cibersegurida</pre>

Index

- Objectius: -> readME <-
- Proposta final: -> readME <-
- \mathbf{DNS} : \rightarrow readME <-
 - **DNSSEC**: -> readME <-
- **DHCP**: \rightarrow readME \leftarrow
- FIREWALL (IPTABLES): -> readME <-
- HACKING & DOS: -> readME <-
 - DNS SPOOF: -> readME <-
 - **ARP SPOOF**: -> readME <-
 - BRUTE FORCE PASSWORD CRACKING: $-> {\rm readME} < -$
 - **SSLSTRIP**: -> readME <-

- KALI LINUX: -> readME <-
 - ETTERCAP: -> readME <-
 - SETOOLKIT: -> readME <-
 - − PROVA: ¬> readME <−</p>
- **WAZUH**: -> readME <-
- Let's Encrypt ACME Certbot HTTPS: -> readME <-
- Encrypted File Systems: -> readME <-

La ciberseguretat

En la societat d'avui en dia, l'ús de les tecnologies de la informació, ens faciliten intercanviar informació des de qualsevol part del món.

<img src="https://gdempresa.gesdocument.com/sites/default/files/styles/large/public/2021-12,</pre>

Millons de dades, viatgen per la "xarxa" anomenada "Internet", que bàsicament son un conjunt de dispositius interconnectats entre sí.

Internet, abarca una rutina cotidiana d'ús de xarxes socials, entreteniment, educació, formació, medis de comunicació, televisió... etc.

Tota aquesta informació viatja en un xarxa on hi hà "de tot".

Molta de la informació que viatja per Internet, pot ser que sigui confidencial i

Molta de la informació que viatja per Internet, pot ser que sigui confidencial i delicada, n'hi hà que viatja segur i d'altre insegur, si viatja insegur... és un problema greu....

Un dels principals problemes de l'ús de les tecnologies de la informació, es la *incapacitat* de prevenir aquests *atacs* quant ja es produeixen. És a dir, el desconeixement de la seguretat d'avant d'aquestes tecnologies d'ús cotidià.

Com ja diu el refrà: "Millor prevenir que lamentar", la solució davant d'aquests problemes a usuaris inexperts, és la ciberseguretat.

<img src="https://elordenmundial.com/wp-content/uploads/2019/03/800px-Deepweb_graphical_rep</pre>

Qué es la ciberseguretat?

La ciberseguretat és la pràctica d'establir "zones de defensa" a diferents dispositius com ordinadors, servidors, dispositius mòbils, xarxes ...etc, d'atacs maliciosos (Com virus o exploits) o de denegació de servei (DoS).

També es coneix com a seguretat de tecnologia de la informació o seguretat de la informació electrònica.

El terme s'aplica en diferents contextos, des dels negocis fins a la **informàtica mòbil**, i es pot dividir en algunes categories comunes.

El seu funcionament es basa en implantar tècniques i eines de **maquinari** / **programari** perquè elaborin **barreres** que impedeixin l'accés desconegut a la informació delicada. La protegeix i treu a l'enemic si es tracta d'una **vulneració**.

Un ciberatac no nomes consisteix en la **pèrdua i destruccio de dades** confidencials, si no que tambe **afecta** el nivell de **productivitat i rentabilitat**, portant com a conseqüencia la perdua del capital, de la confiança per part dels clients y de la competivitat davant del mercat legal.

<img src="https://static.vecteezy.com/system/resources/previews/001/406/100/non_2x/types-of-</pre>

La **ciberseguretat** s'ha tornat un assumpte de vital importancia per a tot tipus d'empreses, sense importar el tamany.

Gràcies a les diferents eines que disposa aquesta materia, el teu sistema pot esta protegit de atacs, d'hackers o qualsevol tipos de delicte informàtic.

La ciberseguretat es dedica a cumplir tres objectius la prevenció, la detecció i la recuperació.

Entre els principals tipus de ciberseguretat es troben els següents:

- Seguretat informatica en àmbit de xarxa: és la pràctica de protegir una xarxa informàtica dels intrusos, ja siguin atacants dirigits o codi maliciós oportunista.
- Seguretat informatica en àmbit de software: s'enfoca a mantenir el programari i els dispositius d'amenaces lliures. Una aplicació afectada podria oferir accés a les dades que està destinada a protegir.
- Assegurar la informació: La seguretat de la informació protegeix la integritat i la privadesa de les dades, tant en l'emmagatzematge com en el trànsit.
- Seguretat operativa: inclou els processos i decisions per manejar i protegir els recursos de dades.
- La recuperació davant de desastres i la continuïtat del negoci defineixen la manera com una organització respon a un incident de ciberseguretat oa qualsevol altre esdeveniment que causi que s'aturin les seves operacions o es perdin dades.

La capacitació de l'usuari final és fonamental en el factor de més impredictible: les persones.

Si s'incompleixen les bones pràctiques de seguretat, qualsevol persona pot introduir accidentalment un virus en un sistema que altament seria segur.

Ensenyar-los als usuaris a eliminar els fitxers adjunts de correus electrònics sospitosos, a no connectar unitats USB no identificades i altres lliçons

importants és fonamental per a la seguretat de qualsevol **organització**.

Tipus d'amenaçes davant la "Ciberseguretat"

Bibliografia

Ciberseguretat

- $\bullet \ \, \text{https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security} \\$
- https://www.santaluciaimpulsa.es/ciberseguridad-en-la-actualidad/
- $\bullet \ \ https://madridpress.com/art/297262/la-ciberseguridad-en-la-actualidad$