ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

VECTORS D'ENTRADA

Maig 2026
Document d'ús públic

6 BONES PRÀCTIQUES PER EVITAR ELS VECTORS D'ATAC

1. QUÈ ÉS UN VECTOR D'ATAC EN CIBERSEGURETAT?

En ciberseguretat, un vector d'atac és el camí o mètode que utilitza un atacant per accedir a un sistema, una xarxa o un dispositiu amb l'objectiu d'explotar-lo.

DE QUINA MANERA ENTRA L'ATAC

2. IMPORTÀNCIA DELS VECTORS D'ATAC

Per què són tan importants els vectors d'atac?

- L'**usuari sol ser el primer punt d'entrada.**
- Més del 80 % dels incidents comencen per errors humans.
- Conèixer els vectors permet **prevenir abans de reaccionar.**
- La tecnologia no protegeix si el vector és una persona enganyada.

VECTORS D'ENTRADA

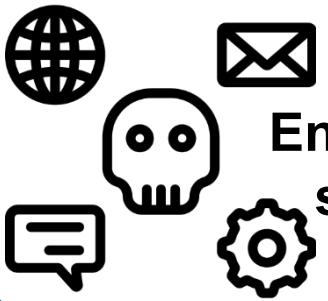
Correus de pesca

Programari sense actualitzar

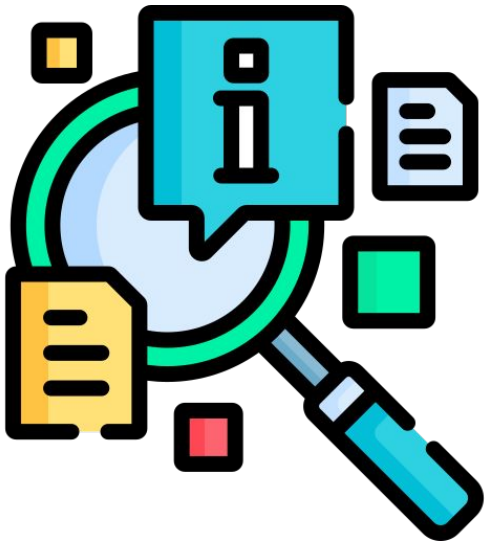
Dispositius USB infectats

Contrasenyes dèbils o reutilitzades

Xarxes wifi insegures



Enginyeria social



Identificar els vectors d'atac ajuda a:

- **Prevenir incidents de seguretat.**
- **Prioritzar mesures de protecció.**
- **Formar millor els equips.**
- **Reduir el risc d'atacs reeixits.**

UN VECTOR D'ATAC NO ÉS L'ATAC EN SI MATEIX, SINÓ EL MITJÀ A TRAVÉS DEL QUAL ES DUU A TERME.

3. CLASSIFICACIÓ ESSENCIAL DELS VECTORS D'ATAC

Vectors basats en el factor humà

- **Pesca / Pesca dirigida** □ correus o missatges que enganyen l'usuari.
- **Enginyeria social** □ manipulació psicològica (trucades, suplantació, etc.).
- **Robatori de credencials** □ enregistradors de teclat (*keyloggers*), pàgines falses, espionatge de reüll (*shoulder surfing*).

Vectors tècnics sobre sistemes i xarxes

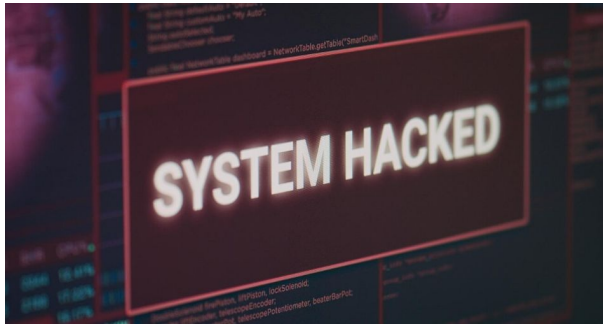
- **Vulnerabilitats de programari**
- **Ports i serveis exposats**
- **Atacs a protocols**
- **Programari maliciós**

Vectors al núvol

- **Configuracions incorrectes (contenidors d'objectes S3 públics, *S3 buckets*)**
- **Robatori de claus API**
- **Escalada de privilegis en serveis al núvol**
- **Atacs a contenidors i Kubernetes**

Vectors de cadena de subministrament

- **Programari compromès en origen**
- **Dependències malicioses**
- **Atacs a proveïdors o tercers**

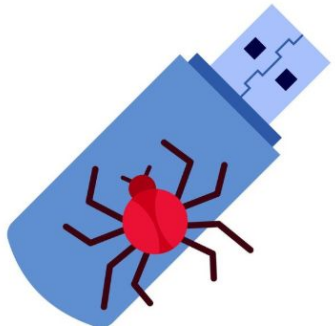


Vectors basats en aplicacions web

- **Injecció (SQLi, NoSQLi)**
- **XSS (injecció indirecta de scripts)**
- **CSRF (falsificació sol·licituds entre llocs web)**
- **Pujada d'arxius maliciosos**

Vectors en dispositiu i maquinari

- **USB maliciós**
- **Atacs a IoT**
- **Microprogramari compromès**
- **Atacs físics (accés no autoritzat a equips)**



4. COM PODEM DETECTAR ELS VECTORS D'ATAC?

SENYALS D'ALERTA

**Atacs d'enginyeria social*

- Urgència («actua ara»)
- Enllaços sospitosos
- Remitent estrany
- Arxius adjunts inesperats

Prevenció → No feu clic, verifiqueu el remitent, reporteu el missatge.

5. QUÈ PODEM FER PER CONTROLAR AQUESTES VIES D'ATAC?

El que tenen en comú totes les vies d'atac és que exploten vulnerabilitats tant humanes i organitzatives com tècniques i de configuració.

Davant la facilitat de cometre **errors** o **fallades** i les mancances organitzatives podem:

- Formar-nos i sensibilitzar-nos.
- Aplicar polítiques d'ús, amb restriccions i usos permesos i, si cal, amb sancions.
- Establir acords i compromisos.
- Identificar els responsables de la seguretat de cada servei que utilitzi les TIC. Assegurar-ne la formació i competència.

6. BONES PRÀCTIQUES PER EVITAR ELS VECTORS D'ATAC

RECORDA

- **Desconfia de la urgència** i verifica remitents.
- **No obris enllaços/adjunts sospitosos**.
- **Contrasenyes fortes** + **AMF** sempre.
- **Actualitza** els sistemes i les aplicacions **i posa-hi pegats**.
- **Desactiva els serveis innecessaris** i aplica **mínim privilegi**.
- **Validació d'entrades** a apps.
- **Configura bé el núvol**.
- **Antivirus/EDR actiu** i bloqueig de macros.
- **No facis servir USB desconeguts**.
- **Verifica programari i dependències** (cadena de subministrament).
- ***Backups* segurs** i pla de resposta a incidents.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.