ANDORRA DIGITAL

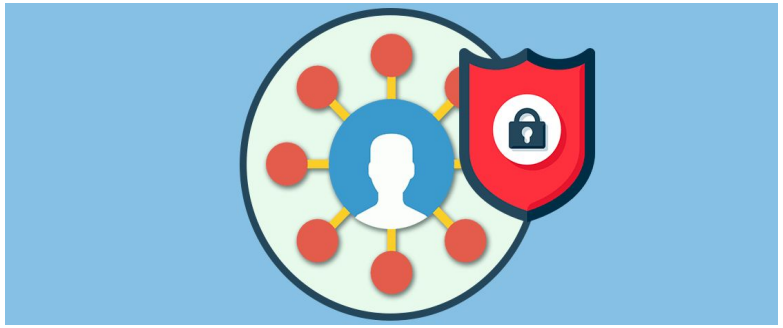
ANC.AD Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

AMENACES DE CIBERSEGURETAT EN LA CADENA DE SUBMINISTRAMENT

Setembre 2025
Document d'ús públic



1. INTRODUCCIÓ

La cadena de subministrament, en el context de la ciberseguretat, es defineix com la cadena formada per proveïdors de serveis digitals que són externs a l'organització que els contracta.

- La cadena de subministrament connecta fabricants, proveïdors, distribuïdors i clients.
- Els ciberatacs a la cadena de subministrament poden tenir conseqüències devastadores: **interrupcions operatives, pèrdues financeres i dany reputacional.**
- La part més dèbil són els **PROVEÏDORS EXTERNS**.

Per què és tan vulnerable la cadena de subministrament?

1. Gran nombre de parts externes amb diferents nivells de ciberseguretat.
2. Interconnexió de sistemes i dades entre les organitzacions.

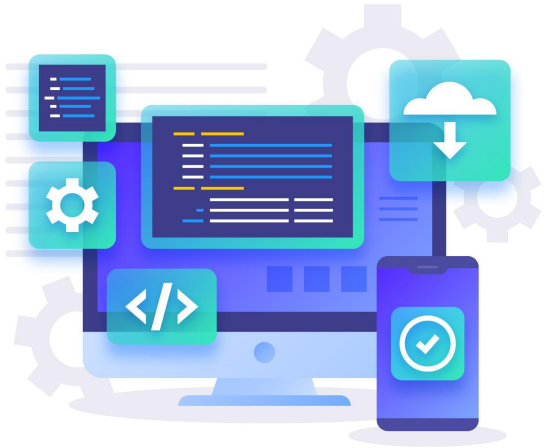
Manca d'avaluació i supervisió de la seguretat del

Els **ciberatacants** busquen **codis insegurs**, **pràctiques insegures en infraestructures o procediments de xarxa insegurs** que els permetin injectar components malintencionats a la cadena.

L'**atac es consuma** quan el ciberdelinqüent, a través de la cadena de subministrament o d'un proveïdor, **és capaç d'infiltrar-se a l'organització i accedir a la seva infraestructura tecnològica**.

- ➔ La cadena de subministrament moderna depèn de múltiples proveïdors i sistemes interconnectats, cosa que fa més gran la superfície d'atac.
- ➔ Els ciberdelinqüents aprofiten la confiança entre empreses i proveïdors per infiltrar-se i comprometre dades, operacions i reputació.

2. ATACS A LA CADENA DE SUBMINISTRAMENT



No existeix un únic tipus d'atac a la cadena de subministrament, sinó més aviat una categoria d'atacs amb un **objectiu comú: aprofitar una vulnerabilitat i treure'n profit**.

Els atacs es poden categoritzar en:

- **Programari compromès**: pot ser el codi d'un component de programari o les eines que s'han utilitzat per desenvolupar-lo.
- **Maquinari compromès**: els atacants disposen de portes del darrere en el microprogramari del dispositiu o han instal·lat components maliciosos en el mateix maquinari.
- **Programari maliciós preinstal·lat**: s'ha instal·lat programari maliciós en dispositius amb l'objectiu final de poder accedir a xarxes internes o a informació delicada.
- **Certificats robats**: els ciberdelinqüents roben certificats d'empreses per signar el seu programari amb modificacions malicioses i fer que sembli legítim.

3. POSSIBLES RISCOS PRODUÏTS PER TERCERS

Vulnerabilitats de tercers

- **Sistemes menys protegits**: els atacants cerquen proveïdors amb mesures de seguretat deficients per accedir a la xarxa principal.
- **Accés privilegiat**: els proveïdors solen tenir accés a sistemes crítics, fet que incrementa el risc.
- **Programari maliciós a través de tercers**: el programari o maquinari subministrat pot contenir un codi maliciós.

Atacs de programari de segrest i programari maliciós

- **Programari de segrest**: els ciberdelinqüents xifren dades i exigeixen rescats, la qual cosa paralitza operacions i genera pèrdues econòmiques.
- **Propagació per actualitzacions**: el programari maliciós es pot distribuir mitjançant actualitzacions de programari legítimes, i això afecta tots els clients d'un proveïdor vulnerable.

Frau electrònic o enginyeria social

- ✔ **Pesca dirigida**: els atacants suplanten proveïdors o treballadors per obtenir credencials o informació financera.
- ✔ **Compromís de correu electrònic professional (BEC)**: s'envien factures falses o instruccions de pagament fraudulentes des de comptes aparentment legítims.
- ✔ **Manipulació de pagaments**: els atacants poden redirigir fons o modificar ordres de compra.

Filtracions i robatori de dades

- ✔ **Accés indegut**: els atacants poden accedir a informació delicada a través de proveïdors amb controls dèbils.
- ✔ **Risc de sancions**: les filtracions poden derivar en sancions legals i pèrdua de confiança de clients i socis.
- ✔ **Fuga massiva**: un sol proveïdor compromès pot exposar dades de múltiples empreses simultàniament.

4. POSSIBLES AMENACES

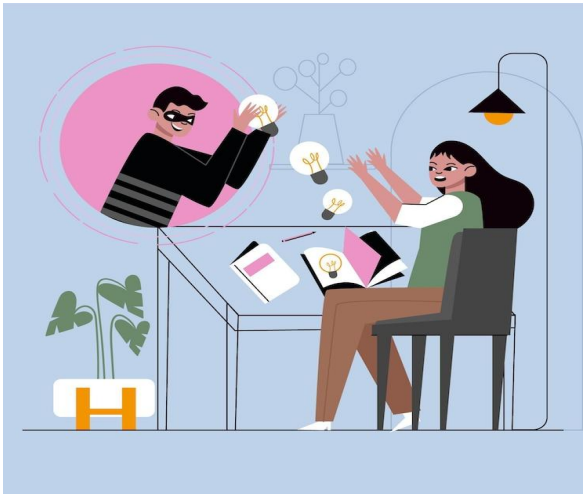
Amenaces internes i sabotatges

- **Treballadors deslleials**

El personal de proveïdors amb accés privilegiat pot robar, manipular o sabotejar informació crítica.

- **Detecció difícil**

Sense controls i auditories adequats, aquests incidents poden passar desapercebuts durant molt de temps.



Amenaces físiques i maquinari compromès

- **Components maliciosos**

Un fabricant pot inserir microxips o maquinari modificat per espiar o obrir portes del darrere a la xarxa de l'empresa.

- **Dispositius infectats**

USB, discs durs o perifèrics es poden introduir a la cadena de subministrament per comprometre sistemes interns.

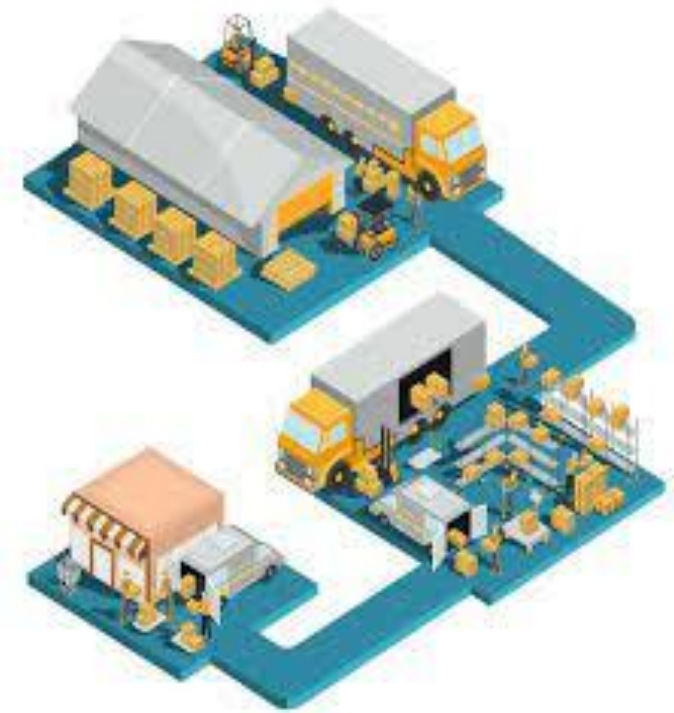
5. IMPACTE DE LES VULNERABILITATS A LA CADENA DE SUBMINISTRAMENT I COM DETECTAR-LES

1. Senyals d'alerta

- ✔ Comportaments inusuals en sistemes o accessos fora d'horari.
- ✔ Canvis inesperats en configuracions o programari de proveïdors.
- ✔ Increment d'incidents de seguretat notificats per tercers.

2. Eines de detecció

- ✔ Anàlisi de comportament de xarxa (*network behavior analysis*).
- ✔ Sistemes d'intel·ligència contra amenaces (*threat intelligence*).
- ✔ Auditories forenses i revisions de compliment.



6. CONSEQÜÈNCIES D'AQUESTS CIBERATACS

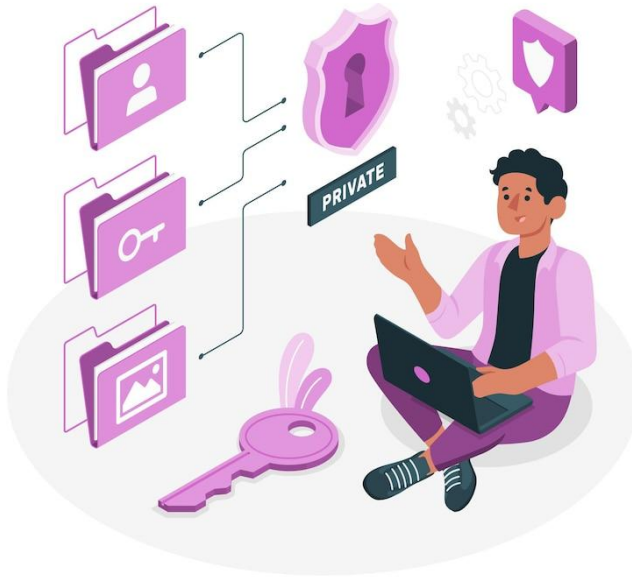
- ✔ **Interrupció d'operacions**: els atacs poden paralitzar la producció i la distribució de productes.
- ✔ **Pèrdues econòmiques**: costos directes per rescats, recuperació i sancions, a més de pèrdues indirectes per interrupció del negoci.
- ✔ **Dany reputacional**: la pèrdua de confiança pot afectar la relació amb clients, socis i amb el mercat en general.

IMPORTANT!

Les formacions contínues han de ser un punt CLAU dins de la ciberseguretat de l'empresa.

7. RECOMANACIONS QUE CAL TENIR EN COMPTE

- ✔ **Avaluació i auditoria de proveïdors**: revisar periòdicament la ciberseguretat de tots els proveïdors crítics amb qui es treballa.
- ✔ **Contractes amb requisits de seguretat**: incloure clàusules de notificació d'incidents de seguretat i estàndards mínims de protecció.
- ✔ **Monitoratge continu**: supervisar accessos i activitats de tercers als sistemes interns de l'organització.
- ✔ **Formació i conscienciació**: formar els treballadors i col·laboradors de l'organització sobre els riscos que es poden produir a la cadena de subministrament.
- ✔ **Gestió de l'inventari**: mantenir un registre de proveïdors actualitzat, així com dels sistemes connectats a la xarxa corporativa.



Avís Legal

Aquest document conté informació pública.

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