ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

La importància de protegir la cadena de subministrament

TLP:WHITE

FEBRER 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	22/02/2024	26/02/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

La cadena de subministrament ha sigut històricament vulnerable a tota mena d'atacs (fraus, robatoris, pesca, etc.), però en els darrers anys ha sigut el blanc de ciberatacs significatius. De fet, segons l'Agència de la Unió Europea per a la Ciberseguretat (ENISA), es preveu que la cadena de subministrament sigui la principal amenaça de ciberseguretat l'any 2030. Així mateix, Gartner augura un augment considerable dels atacs a les cadenes de subministrament el 2025, i estima que afectaran el 45 % de les empreses arreu del món, que significa el triple de la incidència actual.

La seguretat de la cadena de subministrament ha esdevingut un aspecte crític i una gran preocupació per a les organitzacions a l'era digital, en què la interconnexió i la dependència de tercers són cada vegada més freqüents. En aquest escenari, les empreses i les organitzacions en general han d'estar preparades i adoptar mesures preventives per protegir-se contra les amenaces cibernètiques que puguin comprometre la integritat de la seva cadena de subministrament i posar en perill la confidencialitat de la informació i les dades delicades.

Aquest informe se centra en la importància de la protecció de la cadena de subministrament en l'àmbit de la ciberseguretat i aborda els desafiaments, els riscos i les estratègies clau per mitigar les amenaces que poden comprometre la integritat, la confidencialitat i la disponibilitat dels recursos i els processos relacionats amb la cadena de subministrament. També proposa implementar mesures proactives per protegir la cadena de subministrament contra possibles atacs i escletxes de seguretat.

En resum, l'objectiu d'aquest informe és proporcionar una visió integral d'aquest tema crucial i oferir recomanacions pràctiques per enfortir la seguretat a la cadena de subministrament en un entorn digital cada vegada més complex i amenaçant.

3. FONAMENTS DE LA PROTECCIÓ DE LA CADENA DE SUBMINISTRAMENT

Històricament, la cadena de subministrament ha sigut víctima de ciberatacs, tanmateix, aquestes amenaces s'han intensificat a l'era de la Indústria 4.0. En aquests moments, en l'àmbit operatiu d'una organització, i segons el sector en què operi, és habitual disposar d'una àmplia xarxa de proveïdors i serveis proporcionats per tercers. Per aquest motiu, és fonamental planificar i organitzar els processos i els controls de manera efectiva per assegurar que les empreses amb les quals es treballa estan compromeses amb la seguretat.

És essencial tenir en compte que les organitzacions tenen recursos limitats, per la qual cosa han d'avaluar molt bé els costos i els beneficis potencials a l'hora de prendre decisions i adoptar compromisos relacionats amb la seguretat dels actius.

3.1. Conceptes clau

A continuació, presentem algunes definicions clau que ajuden a entendre què és la cadena de subministrament, la seva importància i què està fent la Unió Europea per fer front als riscos.

3.1.1. Cadena de subministrament

La cadena de subministrament comprèn el conjunt de processos, individus, entitats i distribuïdors que participen en la concepció i el lliurament d'un producte o una solució final. En l'àmbit de la ciberseguretat, aquesta cadena inclou diversitat de recursos, com equips i programari, emmagatzematge (tant en el núvol com local), mitjans de distribució (com aplicacions web i botigues virtuals) i programes informàtics de gestió.

Els elements clau d'una cadena de subministrament són els següents:

- **Proveïdor:** és una entitat que subministra un producte o servei a una altra entitat.
- **Actius del proveïdor:** són elements valuosos emprats pel proveïdor per produir el producte o el servei.
- **Client:** és l'entitat que consumeix el producte o el servei produït pel proveïdor.
- **Actius del client:** són elements valuosos propietat de l'objectiu.

Una entitat pot ser una persona física, un grup de persones o també organitzacions. Es consideren actius persones, programes informàtics, documentació, finances, equips informàtics o altres.

3.1.2. Atacs a la cadena de subministrament

Un atac a la cadena de subministrament suposa una amenaça per a tots els elements que en formen part, cosa que es pot traduir en més atacs, ja que estan tots interconnectats. Primer, s'ataca un proveïdor específic, que s'utilitza de punt d'entrada per dirigir l'atac cap a l'objectiu final, per accedir als seus actius. Aquest objectiu pot ser el client final o fins i tot algun altre proveïdor de la cadena. Per tant, perquè un incident es consideri com un atac a la cadena de subministrament, tant el proveïdor com el client han de ser blancs de l'atac.

Les cadenes de subministrament poden ser molt complexes i tenir un gran abast, per la qual cosa alguns atacs poden causar danys catastròfics, i són molt difícils de detectar i de preveure. Això passa, sobretot, quan els proveïdors i en altres membres de la cadena no tenen establertes unes polítiques de seguretat estrictes ni utilitzen les eines adequades.

Les cadenes de subministrament complexes ofereixen finestres d'oportunitat per a ciberatacs. Si l'objectiu final d'un atacant és una organització de gran envergadura amb defenses cibernètiques robustes, és possible que l'atacant explori vies alternatives per accedir al seu objectiu.

3.2. Importància de la seguretat en la cadena de subministrament

Com s'ha comentat, la seguretat de la cadena de subministrament està enfocada a administrar els riscos relacionats amb proveïdors. El seu objectiu és identificar, analitzar i mitigar els riscos associats a la cadena de subministrament. Això inclou aspectes tant de seguretat física com de ciberseguretat de programari i dispositius.

L'evolució i l'expansió de les xarxes de comunicació, el núvol, l'internet de les coses (IoT) i altres tecnologies han creat un entorn propici per a la proliferació d'amenaces i desafiaments nous. En aquest context, la cadena de subministrament és una de les vies preferides per atacar empreses objectiu.

Cada vegada més, els actors d'amenaces s'adrecen a petits i mitjans proveïdors amb pràctiques de ciberseguretat menys sòlides, amb l'objectiu d'accedir posteriorment a un objectiu identificat entre els seus clients. Si un atacant entra als sistemes del proveïdor, podria posar en perill qualsevol organització que utilitzi el producte o el servei, fins i tot grans empreses i organismes públics. Els blancs dels atacs poden ser infraestructures crítiques o serveis essencials.

Els incidents en la cadena de subministrament demostren la interdependència de les organitzacions i la creixent necessitat d'abordar la ciberseguretat de la cadena en el seu conjunt, i per a això cal identificar i reforçar les baules més dèbils. També cal enfortir la regulació de la seguretat de la cadena de subministrament, cosa que es tradueix en propostes que van des de la comunicació o la divulgació de vulnerabilitats fins a restriccions o obligacions per als proveïdors segons determinats estàndards i marcs normatius. A tall d'exemple, més endavant comentarem la Directiva NIS2.

Segons un estudi del Fòrum Econòmic Mundial, el 39 % de les organitzacions enquestades el 2022 es van veure afectades per un ciberincident de tercers. D'altra banda, un estudi fet per Tehtris demostra que vuit de cada deu companyies se senten vulnerables als ciberatacs contra la cadena de subministrament.

3.3. Directiva NIS2 i la cadena de subministrament

La cadena de subministrament pren especial rellevància amb la publicació de la nova Directiva europea NIS2, que, amb l'objectiu de fer front als riscos de ciberseguretat d'una entitat, la incorpora com a element essencial que cal avaluar.

La directiva se centra en:

- Definir les obligacions de gestió de riscos de les cadenes de subministrament d'entitats essencials i importants dins del seu abast.
- Donar suport a petites i mitjanes empreses, amb la finalitat d'enfortir la ciberseguretat tant de la Unió Europea com de les pròpies cadenes de valor d'aquestes entitats.
- Establir una avaluació coordinada dels riscos de seguretat de les cadenes de subministrament crítiques per ajudar les entitats a gestionar-los de manera efectiva.

4. TIPUS D'ATACS A LA CADENA DE SUBMINISTRAMENT

A continuació, comentarem alguns tipus d'atacs a la cadena de subministrament que considerem rellevants pel fet que els atacants coneixen prèviament que hi ha certa relació de confiança entre els components de la cadena.

4.1. Atacs a la cadena de subministrament de programari

Els atacs a la cadena de subministrament és una de les tàctiques preferides del ciberdelinqüents. I aquesta amenaça continua creixent. Aquests atacs impliquen infiltrar-se a un desenvolupador de programari o fabricant de maquinari per després fer servir aquest accés per atacar els seus clients. Això succeeix perquè moltes empreses descuiden la seguretat dels seus proveïdors mentre se centren a protegir els seus propis sistemes.

Un atac a la cadena de subministrament mitjançant programari requereix només que una aplicació compromesa o una part d'un programari enviï el programari maliciós per tota la cadena. Els atacs solen anar dirigits al codi font d'una aplicació: envien un codi maliciós a una aplicació de confiança o al sistema del programari.

L'objectiu dels ciberdelinqüents solen ser les actualitzacions del programari o d'aplicacions, que serveixen de punt d'entrada. Els atacs a la cadena de subministrament a través de programari són difícils de rastrejar, atès que els ciberdelinqüents soler fer servir certificats robats per «signar» el codi i fer-lo semblar legítim.

4.2. Atacs a la cadena de subministrament mitjançant maquinari

Els atacs de maquinari utilitzen dispositius físics, com un enregistrador de teclat allotjat en una unitat USB o connexió d'equips no autoritzats a punts de xarxa, sense vigilància o sense gaire protecció (per exemple, una xarxa wifi oberta o de baixa seguretat). Els ciberdelinqüents adrecen l'atac a dispositius que puguin obrir camí a través de tota la cadena de subministrament amb l'objectiu d'ampliar l'abast de l'atac i causar el màxim de dany possible.

4.3. Atacs a la cadena de subministrament mitjançant programari

Injectar programari maliciós en el codi d'inici d'un ordinador és un tipus d'atac que es pot fer amb només un segon. Un cop s'inicia l'ordinador, el programari maliciós s'activa i compromet tot el sistema. Els atacs de microprogramari són ràpids (i poden passar desapercebuts si no es busquen) i tenen un potencial de dany extremament alt.

5. INCIDENTS RELLEVANTS

A continuació, exposem tres incidents rellevants:

- **Orion - SolarWinds (2021)**

  El 2020, uns ciberdelinqüents van aconseguir infiltrar-se a SolarWinds, un proveïdor de solucions de programari per a la cadena de subministrament, introduint un virus de tipus porta del darrere (*backdoor)* en el programari Orion de l'empresa. Aquest atac va comprometre les dades, les xarxes i els sistemes de més de 18.000 organitzacions que usaven el programari Orion. S'estima que aquest ciberatac va afectar nou agències federals i aproximadament cent empreses del sector privat. El més preocupant és que els ciberdelinqüents no van ser detectats fins al cap d'uns mesos, durant els quals probablement van robar i van exposar enormes quantitats de dades.

- **Kaseya (2021)**

  El juliol de 2021, Kaseya, una empresa dels Estats Units de gestió de programari de TI, amb més 40.000 clients arreu del món, va ser objecte d'un atac de gran envergadura a la cadena de subministrament. A través de l'explotació d'una vulnerabilitat en el servei de gestió remota VSA de Kaseya, es va distribuir, mitjançant el programari de segrest REvil un paquet d'actualització maliciosa dirigit als clients de proveïdors de serveis gestionats (MSP) i altres usuaris empresarials que utilitzaven la versió local del programari.

  El ciberatac va afectar aproximadament 1.500 companyies a diferents llocs del món, com els Estats Units, Canadà, Suècia, Nova Zelanda, Mèxic, Argentina i Espanya, entre altres països. Cal destacar que una cadena de supermercats sueca va haver de tancar 800 de les seves botigues a causa del ciberatac. A més a més, l'abast de l'incident va arribar fins i tot a la Casa Blanca i es va identificar Rússia com el principal sospitós.

- **Kojima - Toyota (2022)**

  Un ciberatac a Kojima Industries, un dels proveïdors de Toyota, va provocar que l'empresa tanqués les seves operacions en tot el Japó. El ciberatac va tenir lloc el 28 de febrer de 2022, cosa que va provocar la suspensió d'operacions en vint-i-vuit línies de producció distribuïdes en catorze plantes del Japó durant tot un dia. Aquesta aturada va impactar en la fabricació de 17.000 vehicles, quantitat que equival a un terç de la producció global de Toyota, aproximadament. Es van estimar unes pèrdues de 356 milions de dòlars.

6. GESTIÓ DE RISCOS

S'han identificat cinc mesures concretes per minimitzar els riscos a la cadena de subministrament:

- **Accessos a dispositius:** no conèixer qui accedeix als sistemes d'una empresa representa un risc significatiu. Per contrarestar aquesta amenaça, existeixen eines que recopilen informació des de fora. Per assegurar la màxima protecció, és recomanable fer una anàlisi d'acompliment de seguretat (SPA, en anglès) del proveïdor, amb l'objectiu de conèixer de quines mesures de seguretat disposa i avaluar si compleixen els requisits necessaris. És important per garantir que els sistemes i les eines emprades estiguin protegides contra possibles amenaces de seguretat.
- **Seguretat a les API:** la seguretat a les API és fonamental per garantir la integritat dels processos de digitalització, especialment ara que el seu ús està molt estès. Per tant, és crucial implementar mesures de seguretat adequades per evitar qualsevol possible mal ús d'aquestes plataformes.
- **Confiança zero:** amb això se cerca protegir els actius de l'empresa a través d'una estratègia de seguretat proactiva que comprengui una autenticació ininterrompuda i una validació permanent d'identitats i accessos.
- **Suplantació d'identitat:** amb l'objectiu de prevenir la suplantació d'identitat, és important utilitzar processos de pagament segurs i una sòlida autenticació d'usuaris, com ara l'autenticació de doble factor (2FA) o sistemes d'alerta per detectar activitats sospitoses.
- **Anàlisi de seguretat dels dispositius:** és fonamental escollir bé els proveïdors de maquinari i assegurar-se que no existeixen vulnerabilitats conegudes en els dispositius que s'adquireixen.

7. ESTRATÈGIA PER PROTEGIR LA CADENA DE SUBMINISTRAMENT

Per protegir la cadena de subministrament, les empreses han de tenir una estratègia que inclogui els punts següents:

7.1. Avaluació de riscos

Fer una avaluació exhaustiva dels riscos de seguretat en tota la cadena de subministrament és el primer pas fonamental. També fer una avaluació acurada dels riscos potencials per identificar possibles vulnerabilitats i punts dèbils. Identificar les vulnerabilitats i les possibles escletxes de seguretat ajuda a comprendre els punts dèbils i a dissenyar estratègies de protecció efectives.

7.2. Avaluació preventiva de proveïdors

Fer una avaluació preventiva exhaustiva a l'hora de seleccionar els proveïdors i els socis comercials és fonamental. Cal definir criteris específics per seleccionar proveïdors confiables i segurs, que estiguin alineats amb estàndards de seguretats i de compliment. Això implica avaluar el seu historial de seguretat, les polítiques de protecció de dades i les pràctiques de seguretat. Treballar només amb proveïdors confiables i establir contractes clars que incloguin clàusules de seguretat pot ajudar a minimitzar els riscos vinculats amb el ciberespionatge.

Tal com hem esmentat anteriorment, és crucial aplicar el principi de confiança zero a tots els proveïdors. Per fer-ho, és essencial tenir la capacitat d'examinar minuciosament els proveïdors per garantir que siguin segurs i que no representin cap mena d'amenaça.

A més, una altra mesura necessària és fer proves de penetració (*pentesting*) tant des de fora com des dels mateixos proveïdors. Avaluar la capacitat dels proveïdors per generar possibles amenaces internes o externes és crucial.

7.3. Protecció de dades

La protecció de les dades és essencial a la cadena de subministrament. És fonamental implementar mesures de seguretat sòlides, com ara el xifratge de dades, l'autenticació de doble factor i la segmentació de xarxes. També és important establir polítiques clares sobre l'accés i l'intercanvi de dades amb proveïdors i socis comercials.

7.4. Auditories i monitoratge constant

És important fer auditories de manera periòdica als proveïdors i monitorar constantment les activitats de la cadena de subministrament per detectar possibles anomalies o activitats sospitoses.

El monitoratge constant de la cadena de subministrament és crucial per detectar activitats sospitoses o inusuals. Implementar eines de monitoratge de seguretat i sistemes de detecció d'intrusions pot ajudar a identificar amenaces potencials i a respondre-hi de manera ràpida i efectiva.

7.5. Formació i conscienciació

La formació i la conscienciació dels treballadors i dels proveïdors són elements clau en la defensa contra la ciberdelinqüència. El personal de l'empresa i els proveïdors han de conèixer les bones pràctiques de seguretat, estar conscienciats sobre la pesca (*phishing*) i conèixer la importància d'informar de qualsevol activitat sospitosa que pugui vulnerar la seguretat de la cadena de subministrament.

7.6. Gestió d'incidents i resposta davant de crisis

Les organitzacions han de tenir un pla de gestió de resposta a incidents que estableixi els processos i les tecnologies per respondre als incidents que es puguin produir. Aquest pla cal que determini com es poden identificar, contenir i resoldre els diferents tipus de ciberatacs. Això inclou la identificació de rols i responsabilitats, la comunicació clara i efectiva durant l'incident i la col·laboració amb experts en seguretat per contenir i mitigar qualsevol escletxa de seguretat.

L'objectiu és ajudar els equips de ciberseguretat a detectar i contenir ciberamenaces, a accelerar la restauració dels sistemes afectats i a reduir la pèrdua d'ingressos, les multes normatives i altres costos associats als ciberatacs.

7.7. Implementació d'estàndards i certificacions

Existeixen estàndards i certificacions que avalen l'esforç de les organitzacions per millorar la protecció contra ciberamenaces, com la norma internacional ISO/IEC 27001 i la NIST 800-55 de l'Institut Nacional d'Estàndards i Tecnologia (NIST), una entitat del Departament de Comerç dels Estats Units.

La norma ISO/IEC 27001 conté diversos procediments de control per ajudar les empreses a garantir la seguretat de les seves infraestructures de tecnologies de la informació. Aquests

procediments inclouen aspectes com el control d'accés, la seguretat física, l'adquisició de sistemes, els procediments de manteniment i les relacions amb proveïdors, entre d'altres.

L'estàndard NIST 800-55, per la seva banda, proposa una metodologia sòlida per identificar i mesurar els efectes dels controls de seguretat en tres àrees clau: implementació, eficiència i eficàcia, i mesures d'impacte organitzacional.

El NIST ha elaborat una guia especialitzada anomenada Pràctiques de gestió de riscos de ciberseguretat a la cadena de subministrament (C-SCRM). Se centra a abordar la ciberseguretat a les cadenes de subministrament, principalment en els àmbits de l'adquisició, la contractació de proveïdors i l'intercanvi d'informació. En conseqüència, activitats com la selecció de proveïdors, les ofertes, les sol·licituds de cotització, l'avaluació de propostes i els termes contractuals cal dur-les a terme d'acord amb els requisits de ciberseguretat establerts.

Els estàndards de seguretat han de comunicar-se i exigir-se a tots els proveïdors i socis comercials que formen part de la cadena de subministrament. Això garantirà un nivell mínim de seguretat i ajudarà a evitar l'accés no autoritzat als sistemes de dades.

8. CONCLUSIONS

Cal prendre consciència de la interconnexió i la interdependència entre els diversos actors de la cadena de subministrament per tal d'implementar una protecció especialitzada que protegeixi l'empresa de possibles ciberatacs. Això implica que una empresa o organització només pot protegir les seves operacions i equips de manera efectiva amb la participació dels seus proveïdors i professionals de ciberseguretat. En aquest sentit, és molt important elaborar un inventari de les interconnexions amb els proveïdors per garantir-ne la supervisió.

El repte radica a vigilar constantment la seguretat dels proveïdors seleccionats i a assegurar una sòlida higiene de seguretat. És fonamental aplicar i monitorar rigorosament els requisits contractuals establerts per als proveïdors i les cadenes de subministrament respectives.

Es recomana també implementar una vigilància en relació amb les vulnerabilitats que puguin tenir algun impacte en els sistemes i disposar d'una funció de gestió de riscos de la cadena de subministrament.

Davant de qualsevol sospita, és fonamental utilitzar indicadors de compromís (IoC) coneguts i registres d'activitat dels usuaris per rastrejar el moviment lateral i determinar si l'organització està realment afectada o no.

Finalment, com a part de la gestió de riscos, és important disposar d'una llista documentada de proveïdors i venedors crítics en cas que es produeixi una escletxa.

9. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.