Butlletí del
Consell General

Any 2022 – VIII Legislatura – Núm. 69 /2022

24 de maig del 2022

SUMARI pàgina

4. IMPULS I CONTROL DE L'ACCIÓ POLÍTICA DEL GOVERN

4.4.2 Respostes escrites

Edicte

La síndica general, d'acord amb les previsions de l'article 90 del Reglament del Consell General,

Disposa

Publicar la resposta del Govern a la pregunta formulada pel M. I. Sr. Roger Padreny Carmona, conseller general del Grup Parlamentari Socialdemòcrata, per escrit de data 11 d'abril del 2022, relativa **als atacs a la ciberseguretat d'Andorra Telecom, SAU**, i publicada en el Butlletí del Consell General número 48/2022, del 13 d'abril.

Tot el que es fa públic per a general coneixement i efectes.

Casa de la Vall, 24 de maig del 2022

Roser Suñé Pascuet
Síndica General

Ministeri de Turisme i Telecomunicacions
Resposta escrita (Reg. núm. E-298-2022)

Resposta escrita del Govern (M. I. Sr. Jordi Torres Falcó, ministre de Turisme i Telecomunicacions) a les preguntes presentades pel M. I. Sr. Roger Padreny Carmona, Conseller General del Grup Parlamentari Socialdemòcrata, per escrit de data 11 d'abril del 2022, relatives als atacs a la ciberseguretat d'Andorra Telecom, SAU (Reg. núm.E-298-2022)

Els atacs rebuts els mesos de gener i d'abril als quals fa referència la pregunta corresponen a atacs de denegació de servei distribuït (DDoS). Andorra Telecom ha observat una evolució del tipus d'atac de denegació de servei del tipus 1 al tipus 2:

- Tipus 1: atacs de denegació de servei DDoS l'objectiu dels quals són adreces IP concretes (seria el tipus d'atac més comú que s'havia estat observant, que anomenarem *de tipus 1* d'ara endavant).

- Tipus 2: atacs de denegació de servei DDoS que van dirigits indiscriminadament a moltes adreces IP en molt poc temps (coneguts com a *atacs de bombardeig en estora (*carpet bombing*)* o *de tipus 2* d'ara endavant).

La mitigació d'aquests atacs per part d'Andorra Telecom pot comportar segons els casos una degradació del servei d'internet en què, de manera puntual i aleatòria, els usuaris que estan connectats a internet poden percebre una connexió més lenta.

El procés de mitigació consisteix a identificar i netejar tot el trànsit maliciós per deixar passar només el trànsit net.

Alhora que els ciberatacs cada vegada són més sofisticats, Andorra Telecom, igual que les operadores de telecomunicacions mundials, també va adoptant i perfeccionant les mesures de seguretat i mitigació dels atacs. Andorra Telecom inverteix de forma permanent en solucions i actualitzacions de ciberseguretat i en equips de resposta als incidents per fer front a aquestes amenaces, i ho fa a través de proveïdors de primer nivell.

Preguntes que es formulen relatives als atacs a la ciberseguretat d'Andorra Telecom, SAU:

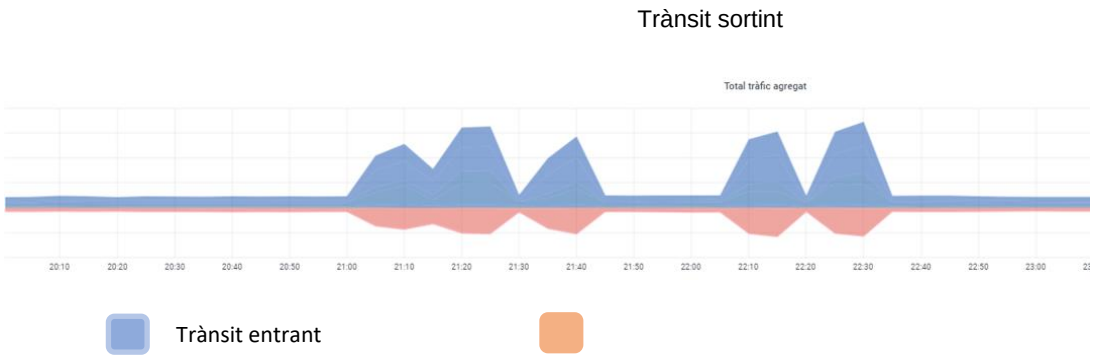
1. A quina hora detecta Andorra Telecom, SAU que s'ha produït el ciberatac citat?

Andorra Telecom detecta l'atac DDoS del 10 d'abril a les 21.07 h.

2. S'ha solucionat l'atac? En cas afirmatiu, a quina hora es va solucionar? Quant de temps va durar l'atac?

L'atac DDoS del 10 d'abril va tenir una durada d'una hora i 30 minuts i va finalitzar a les 22.30 h.

Durant aquest temps, es van observar diverses onades amb moments de calma tal com es mostra en el gràfic inferior.



3. Es tracta d'un atac de denegació de servei (DDoS) del mateix tipus i grandària que el ciberatac a Andorra Telecom, SAU, que es va produir el passat 21 i 22 de gener del 2022? I si ho comparem amb el ciberatac del 24 de gener?

El ciberatac del 10 d'abril, tot i ser molt virulent, no és del mateix tipus que els rebuts el mes de gener.

Durant l'atac DDoS del mes de gener es va rebre una gran quantitat de trànsit de dades maliciós des de múltiples localitzacions internacionals i dirigit cap a diversos destins d'Andorra. Aquest seria l'atac més comú per atacar un objectiu concret (atacs de tipus 1)

Durant l'atac DDoS del mes d'abril es va rebre una gran quantitat de trànsit de dades maliciós, però en aquesta ocasió es va fer des de múltiples localitzacions internacionals i dirigit cap a múltiples destinacions, moltes més que en els atacs del mes de gener. Aquestes destinacions anaven canviant durant l'atac (atacs de tipus 2)

4. Quines conseqüències ha tingut aquest atac pels usuaris?

Mentre dura el procés de defensa i mitigació, els usuaris, de manera puntual i aleatòria, poden notar una degradació del servei d'internet. En cap d'aquests atacs el servei va quedar interromput.

En més del 80% dels atacs rebuts durant el primer trimestre, la neutralització dels atacs ha passat desapercebuda per als usuaris, sense cap afectació del servei.

5. I quines conseqüències ha tingut aquest atac per Andorra Telecom, SAU?

Andorra Telecom ha pogut continuar perfeccionant els seus coneixements sobre l'evolució de les tècniques emprades pels ciberdelinqüents i ha continuat adaptant els sistemes de defensa a partir del coneixement adquirit. El risc zero davant dels atacs no existeix. Andorra Telecom ha incrementat les seves capacitats de mitigació i ha contractat serveis d'assessorament d'entitats de prestigi reconegut per desplegar les millors tècniques, estretint la col·laboració amb la recentment creada Agència de Ciberseguretat Nacional i la Policia per lluitar contra el cibercrim organitzat.

6. Ha tingut alguna afectació pels serveis públics essencials?

Els atacs de denegació de servei distribuït afecten exclusivament serveis suportats per la xarxa d'internet. Mentre dura el procés de defensa i mitigació, els usuaris, de manera puntual i aleatòria, poden notar una degradació del servei d'internet. En cap cas el servei va quedar interromput.

Els serveis públics essencials, com ara la telefonia de veu fixa o mòbil, no s'han vist afectats.

7. Les conseqüències d'aquest ciberatac haurien estat diferents si aquest atac es produeix en un dia laborable?

Andorra Telecom té desplegades solucions per donar resposta a aquests ciberatacs 24 hores al dia, 7 dies a la setmana, 365 dies l'any, gestionades per l'equip de seguretat. En cas d'atac en un dia laborable, la reacció i actuació per part d'Andorra Telecom hauria estat igual de ràpida i eficaç.

L'impacte hauria estat el mateix tant durant la jornada laboral com fora.

8. Quants ciberatacs s'han detectat des d'inici d'aquest any 2022?

Des de principis de l'any 2022 s'han detectat 276 ciberatacs, tots ells referents a atacs de denegació de servei (DDoS). D'aquests ciberatacs, aproximadament més del 80% han estat mitigats satisfactòriament sense que els usuaris els hagin pogut percebre.

Per tal de contextualitzar el nombre de ciberatacs rebuts, podem indicar que durant un sol mes (abril del 2022) al món s'han enregistrat de l'ordre de 773.000 atacs DDoS (informació pública: https://horizon.netscout.com/?atlas=summary).

9. Pel mateix període l'any, pels anys 2021 i 2020, quants atacs s'havien produït? De quin tipus de ciberatacs es tracten? (establir una taula resum per quantitat (en nombres absoluts i percentuals) i tipus de ciberatac).

2020	**Tipus ciberatac (*)**	**Quantitat**	**Quantitat en %**	**Comentari**
Gener-abril	DDoS	148	35% respecte a tot l'any	Respecte a l'any 2019 hi ha un increment del 139%.

2021	**Tipus ciberatac(*)**	**Quantitat**	**Quantitat en %**	**Comentari**
Gener-abril	DDoS	68	33% respecte a tot l'any	Respecte a l'any 2020 hi ha un decrement del 49,28%.

2022	**Tipus ciberatac(*)**	**Quantitat**	**Quantitat en %**	**Comentari**
Gener-abril	DDos	276	100% respecte a tot l'any fins ara	Respecte a l'any 2021 hi ha un increment del 273%.

(*) Als efectes d'aquesta pregunta només s'han computat els ciberatacs que poden tenir afectació als serveis de telecomunicacions.

10. En cas que l'atac del 10 d'abril ja s'hagi solucionat, quants recursos s'han dedicat a reduir aquest últim atac? Són els mateixos que els que es van destinar per reduir el ciberatac del passat 21 i 22 de gener del 2022? I pel ciberatac del passat 24 de gener del 2022? (establir les diferències de recursos destinats a solucionar els diferents atacs).

Andorra Telecom va perfeccionant les seves solucions de forma permanent per tal de protegir la xarxa de l'augment de les ciberamenaces i augmentant la seva capacitat de resposta per mitigar-les.

No es poden establir diferències de recursos destinats a solucionar els diferents atacs, atès que els recursos van evolucionant per protegir de forma general les amenaces de forma proactiva i adaptant-se en funció de les noves tècniques utilitzades. Els recursos no es contracten en el moment de rebre els atacs i protegir-se'n.

11. Quins dispositius d'emergència té previstos Andorra Telecom, SAU per garantir el funcionament dels serveis essencials?

Andorra Telecom disposa de les mesures necessàries per garantir l'alta disponibilitat de les infraestructures que suporten els serveis essencials. Els serveis de telecomunicacions del

país disposen de la redundància física i lògica necessària per garantir la continuïtat dels serveis.

Davant d'incidents de seguretat extraordinaris s'activen de manera immediata els equips de resposta a incidents de la mateixa companyia i els seus proveïdors, igual que es fa davant de qualsevol altre eventualitat que pugui afectar els serveis.

12. En un comunicat oficial d'Andorra Telecom, SAU, del 23 de gener del 2022, posterior als ciberatacs del passat 21 i 22 de gener, s'establia que "Andorra Telecom seguirà invertint en la seguretat del servei d'internet per tal que aquesta mena d'atacs afectin cada vegada menys als seus usuaris, ja que són atacs que, any rere any, van augmentant arreu del món". Fruit de la repetició dels ciberatacs, quina nova inversió té previst fer Andorra Telecom, SAU?

Andorra Telecom inverteix i seguirà invertint en matèria de seguretat, a través d'entitats especialitzades en la matèria per tal de protegir la xarxa de telecomunicacions del país i fer front al creixement de les ciberamenaces.

Les mesures adoptades i els proveïdors o serveis contractats per Andorra Telecom són de caràcter reservat i confidencial i no poden fer-se públics per raons de seguretat. Per això la Direcció General ha preparat la informació relacionada amb aquest punt i la posa a disposició del M. I. Sr. Roger Padreny, perquè els pugui consultar exhaustivament.

13. El passat 27 d'octubre del 2021 es publicava al Butlletí Oficial del Principat d'Andorra número 111, del 27 d'octubre, el Decret 346/2021, del 20 d'octubre del 2021, de creació de l'Agència Nacional de Ciberseguretat i de l'Equip de Resposta de Referència del Principat d'Andorra per al tractament d'incidents de seguretat de les xarxes i els sistemes d'informació. Quin paper han desenvolupat aquests organismes en els ciberatacs d'aquest any 2022?

Des de la seva creació a l'octubre del 2021, i especialment arran dels incidents de ciberseguretat esdevinguts durant aquest 2022, el paper desenvolupat per l'Agència Nacional de Ciberseguretat (en endavant, "l'ANC-AD") i de l'Equip de Resposta del Principat d'Andorra per al tractament d'incidents de seguretat de les xarxes i els sistemes d'informació ha estat principalment el de situar-se al costat de qualsevol organisme o entitat en el context d'un incident, amb la voluntat d'oferir la seva màxima col·laboració i suport. En concret, l'Agència i l'Equip de Resposta han col·laborat durant els incidents aportant, entre d'altres, informació rellevant o d'interès, obtinguda gràcies a la seva relació amb altres organismes internacionals relacionats amb la ciberseguretat.

En aquest sentit, l'Agència i l'Equip de Resposta estan elaborant un marc de col·laboració i d'intercanvi d'informació amb els responsables de seguretat de les empreses o entitats catalogades com a crítiques o essencials. La col·laboració es tradueix en reunions de treball periòdiques (amb més freqüència en cas d'incident), en què s'intercanvien experiències, rutines de treball i anomalies detectades i es posa en comú tot el que pugui afectar la integritat i disponibilitat de les infraestructures crítiques o essencials que donen servei al país.

Addicionalment, l'Agència i l'Equip de Resposta han portat a terme l'acció de difondre i proporcionar informació sobre la naturalesa dels incidents i les seves principals

característiques a la ciutadania, al teixit empresarial i a la societat en general. La dita acció ha estat possible gràcies als canals de comunicació que l'Agència Nacional ha posat a disposició de la societat, sigui a través de la seva pàgina web com a canal principal (notícies més rellevants, subscripcions, etc.), o bé mitjançant els seus comptes a les xarxes socials, on actualment s'està fent difusió de forma diària de tots els continguts i casos de rellevància especial relatius a incidents que puguin afectar el Principat.

14. Quins són els protocols i procediments d'actuació efectius entre Andorra Telecom, SAU i l'Agència Nacional de Ciberseguretat?

D'acord amb el que s'ha exposat a la pregunta anterior, i atenent la creació recent de l'ANC-AD, en l'actualitat s'està treballant en l'elaboració de protocols específics, no únicament per la seva relació amb Andorra Telecom, sinó per a tot el conjunt d'entitats enteses com a importants o essencials per al desenvolupament de l'activitat socioeconòmica del país. Aquests protocols seran recollits i desplegats reglamentàriament mitjançant els decrets de l'Esquema Nacional de Ciberseguretat i el Reglament d'infraestructures crítiques. Ambdós decrets seran desplegats conjuntament amb la Llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació, un cop sigui aprovada i entri en vigor.

Atesa la necessitat d'actuacions a curt termini davant l'existència d'incidents que requereixen l'atenció i col·laboració immediata entre entitats, i particularment amb Andorra Telecom, l'ANC-AD ha establert protocols que inclouen des de la creació de canals de comunicació àgils entre les parts fins a l'elaboració conjunta de procediments de detall que permetin una actuació ràpida i directa enfront de qualsevol contingència.

Més en detall, i en referència als darrers incidents, l'ANC-AD ha intercanviat amb Andorra Telecom la informació necessària per avaluar i diagnosticar conjuntament el que ha succeït, incloent-hi el suport addicional de la xarxa internacional de col·laboració de l'ANC-AD en l'àmbit de la ciberseguretat.

Davant d'un incident, Andorra Telecom facilita (previ tractament) les dades tècniques i mètriques de detall obtingudes a partir de les eines i recursos de supervisió utilitzats per als seus entorns de seguretat perimetral. Si es convé i es creu escaient, aquesta informació es facilita a diferents organismes internacionals amb l'objectiu de rebre informació complementària que permeti introduir mesures addicionals de protecció tant reactives com proactives davant l'incident present i incidents futurs de la mateixa naturalesa.

Andorra la Vella, 24 de maig del 2022

Jordi Torres Falcó
Ministre de Turisme i Telecomunicacions

Carrer de la Vall, 9-13 – AD500 Andorra la Vella – Principat d'Andorra – Tel. (376) 877877 – www.consellgeneral.ad

Dipòsit legal: AND.282-2021