ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de ciberintel·ligència

Ciberseguretat al núvol

TLP:WHITE

25/04/2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	26/04/2023	26/04/2026

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGÍA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar TLP:RED quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com TLP:RED amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar TLP:AMBER quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com TLP:AMBER únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar TLP:GREEN quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com TLP:GREEN amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar TLP:WHITE quan la informació no suposa cap risc de mal ús, dins de 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

El *cloud computing*, comunament conegut com "el núvol", fa referència a tots aquells recursos i serveis informàtics als quals es poden accedir mitjançant internet. Permet disposar de serveis d'infraestructura (IaaS), plataforma (PaaS) i programari (SaaS) a mida, fent possible accedir a ells de manera remota i deslocalitzada.

2.1 Diferències entre entorns *cloud* i entorns locals convencionals

Ateses les principals diferències entre la tecnologia *cloud* i els entorns locals tradicionals, caldria destacar que:

- En els entorns locals, les empreses són les responsables de la gestió i el manteniment dels seus servidors i la seva infraestructura, mentre que, al núvol, aquesta responsabilitat es comparteix amb el proveïdor de serveis *cloud*.

- En els entorns locals, les empreses han d'invertir en maquinari i programari, mentre que, al núvol, els recursos informàtics es lliuren com a servei, per la qual cosa les organitzacions només paguen pel que utilitzen.

- Els entorns *cloud* tenen una capacitat d'escalabilitat pràcticament il·limitada, podent adaptar-se ràpidament a les necessitats de l'empresa. En el cas dels entorns locals aquesta capacitat queda limitada per la seva dependència dels servidors i la infraestructura de maquinari i programari amb la qual es compti prèviament.

Per tant, els avantatges que ofereixen els serveis sota demanda al núvol han aconseguit que moltes empreses hagin triat aquesta opció per desenvolupar la seva infraestructura IT, relegant a un segon pla als entorns locals convencionals.

2.2 Elements que componen la infraestructura IT al núvol

Depenent de la solució que precisi cada organització, els elements que componguin la seva infraestructura IT poden variar. No obstant això, podria dir-se que n'hi ha alguns que solen ser presents en la gran majoria d'entitats, vegem-los.

- Servidors: són la base de la infraestructura *cloud* i proporcionen capacitat de processament per les aplicacions i serveis allotjats al núvol.

- Xarxa: es podria dir que és la vèrtebra de tota la infraestructura *cloud* ja que s'encarrega d'interconnectar altres elements, des dels servidors fins a qualsevol altre dispositiu que formi part d'ella. Les xarxes, al seu torn, poden ser físiques o virtuals.

- Emmagatzematge: és necessari per guardar les dades i allotjar aplicacions al núvol. La infraestructura *cloud* sol comptar amb sistemes d'emmagatzematge escalables i redundants per garantir la disponibilitat i la integritat de les dades.

- Sistemes operatius: s'utilitzen per gestionar els diferents recursos informàtics dels quals es disposi i, a més, proporcionen una interfície pels usuaris i les aplicacions.

- Hipervisors: són *softwares* que s'utilitzen per a virtualitzar els recursos de la infraestructura *cloud*, permetent que múltiples sistemes operatius i aplicacions s'executin en un sol servidor físic.

- Middleware: proporcionen una capa de programari entre les aplicacions i els sistemes operatius subjacents, permetent usar les aplicacions de manera descentralitzada i flexible.

- Aplicacions: són l'objectiu final de la infraestructura *cloud* i tenen diferents objectius, depenent de les necessitats de cada organització. S'executen en els servidors virtualitzats del núvol.

- Eines de gestió: conjunt de serveis que s'empren per administrar els recursos a la infraestructura *cloud* com, per exemple, les eines de gestió d'identitats i accessos, les de monitoratge, o els serveis d'automatització de recursos.

- Seguretat: és probablement l'element més important de la infraestructura, atès que repercuteix en tots els altres, i serà sobre el qual aprofundim en aquest document. Comprèn diferents solucions i serveis orientats a garantir la seguretat de les dades i les aplicacions allotjades en el núvol. Els tallafocs, els IDS, o el xifratge de dades serien alguns d'ells.

3. SERVIDORS AL NÚVOL I ESTRATÈGIES DE DESENVOLUPAMENT

Segons els últims informes elaborats al 2022, es va constatar que pràcticament més de la meitat de les organitzacions de tots els sectors estan recorrent al núvol per desplegar, almenys, part dels seus serveis.

3.1 Serveis més demandats per les organitzacions el 2022

Atesa la tipologia d'aquests, els serveis relacionats amb la seguretat són implementats per fins al 58% de les entitats, seguits per serveis informàtics (56%), emmagatzematge (55%), virtualització (53%), aplicacions de negoci (52%), bases de dades (49%) i, en últim lloc, les aplicacions orientades a la productivitat (47%).

58%
Seguretat
(Gestió d'identitat, control de accessos, protecció de dades...)

56%
Ser. Informàtics
(Servidors, contenidors...)

55%
Emmagatzematge
(Emmagatzematge d'objectes, arxius, còpies de seguretat...)

3.2 Tendències en estratègies de desenvolupament d'entorns *cloud* al 2022

Les organitzacions opten per dues estratègies de desplegament de serveis al núvol majoritàriament: l'estratègia híbrida i l'estratègia *multi-cloud*. Anem a conèixer què implica cada concepte.

- Estratègia de desenvolupament *cloud* híbrid: és la principal tendència i per la qual aposten el 39% de les organitzacions, superant els registres de l'any anterior.

  Aquesta estratègia implica la combinació de recursos del núvol públic i privat, així com d'infraestructures *on-premise*. En aquest enfocament, les aplicacions i les dades es poden moure de manera fluida entre els diferents entorns del núvol segons les necessitats del negoci.

El principal avantatge que ofereix aquesta estratègia és que permet aprofitar els beneficis del núvol públic, com són la seva escalabilitat i baix cost, mentre es manté el control sobre les dades i els processos crítics al núvol privat o en les instal·lacions de l'empresa.

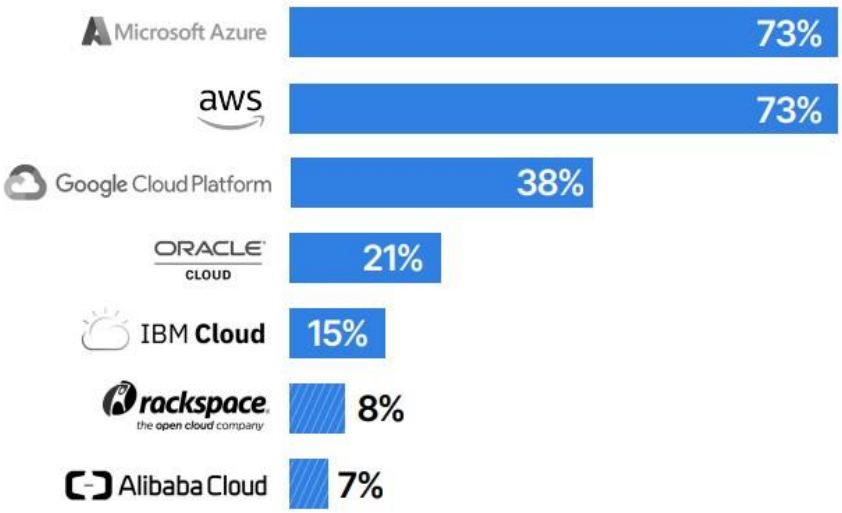
- Estratègia de desenvolupament *multi-cloud*: el 33% de les entitats trien aquesta opció per desplegar els seus serveis. Si bé és cert que és un percentatge molt significatiu, cal tenir en compte que, al contrari que en el cas de l'estratègia *cloud* híbrida, l'ús de les infraestructures *multi-cloud* van disminuir un 2% respecte de l'any anterior.

  Aquesta estratègia consisteix a fer ús de serveis i recursos de múltiples proveïdors del núvol públic, en lloc de limitar-se a un únic proveïdor. Amb aquest enfocament, l'empresa pot seleccionar el proveïdor de serveis que millor s'adapti a les seves necessitats per cada aplicació o càrrega de treball.

  El benefici d'aquesta metodologia de desplegament de serveis, respecte a recórrer a un únic proveïdor, és que ofereix més flexibilitat i majors garanties sobre la continuïtat de negoci.

Del que no hi ha cap dubte, és que el nombre d'organitzacions que no fan ús del núvol és pràcticament residual, suposant només un 4% del total. I que, de les quals només recorren al *cloud* un 20% aproximadament. Aquests opten per concentrar el desplegament de serveis en un únic proveïdor.

Si s'analitzen les dades sobre els proveïdors de serveis al núvol més demandats al 2022, Microsoft Azure i AWS mantenen la seva hegemonia en aquest mercat, facilitant infraestructures *cloud* al 73% de les companyies.



4. PRINCIPALS PUNTS CRÍTICS DE SEGURETAT AL NÚVOL

De la mateixa manera que la tecnologia *cloud* ha vingut acompanyat d'importants beneficis per les organitzacions i els usuaris quant a facilitat d'accés i gestió, noves oportunitats d'escalabilitat i, fins i tot, reducció de costos, també ha provocat que s'hagin hagut de replantejar les metodologies i els mecanismes amb els quals protegir aquest tipus d'entorns.

L'objectiu d'aquest informe és aprofundir en els riscs als quals cal parar atenció a causa de la idiosincràsia d'aquesta mena d'infraestructures, i abordar les solucions que permetin garantir la seva seguretat en mesura del possible.

La mala configuració de les plataformes al núvol és el problema de seguretat que es dona amb més freqüència i pot implicar incidents de major gravetat. A partir de les dades analitzades al llarg del 2022 sobre bretxes de seguretat al núvol, així com la informació proporcionada per responsables de ciberseguretat enquestats durant el darrer any, podem establir que els principals punts crítics de seguretat en entorns *cloud* són:

4.1 Problemes de configuracions incorrectes de les plataformes al núvol:

Malgrat que les conseqüències derivades d'errors de configuració són més que conegudes, fins al 62% dels incidents detectats durant l'any 2022 estaven relacionats amb l'ús de contrasenyes febles o el seu ús compartit, configuracions incorrectes dels permisos d'accés, errors en la configuració dels servidors i altres configuracions incorrectes que, en un grau o un altre, van propiciar que la infraestructura al núvol fos vulnerable a diversos atacs.

És important tenir en compte que fins i tot els proveïdors del núvol més segurs poden ser susceptibles de veure's els seus serveis compromesos si no es configuren adequadament.

4.2 Interfícies i APIs insegures:

Aquest error de seguretat va ser present dins el 52% dels incidents cibernètics registrats durant l'any passat al núvol. Les interfícies o les APIs serveixen perquè els usuaris puguin interactuar, gestionar o administrar els serveis al núvol.

Quan existeix una bretxa de seguretat en aquest punt, les conseqüències principals solen ser accessos a dades sensibles mitjançant accessos no autoritzats que, posteriorment, poden desencadenar altres accions malicioses.

4.3 Exfiltració de dades sensibles:

És un altre dels problemes de ciberseguretat que van tenir més incidents durant el 2022, comptabilitzant-se fins al 51% dels casos. Fa referència a la transferència no autoritzada de

dades des d'un sistema al núvol a un sistema extern i pot produir-se per diverses raons, com l'explotació de vulnerabilitats o errors als controls d'accés.

4.4 Accessos no autoritzats:

Aquest problema de seguretat va ser present dins del 50% dels ciber-incidents que es varen produir l'any passat. Encara que els proveïdors de serveis al núvol solen oferir eines de control d'accés i autenticació per evitar aquest tipus de situacions, cal tenir en compte que sempre existirà la possibilitat que usuaris malintencionats o no autoritzats puguin accedir a sistemes al núvol i prendre dades o executar altres activitats malicioses.

4.5 Intercanvi extern de dades:

Aquesta problemàtica també va ser un altre dels punts crítics que més impacte va tenir sobre els entorns *cloud*, ja que el 39% dels incidents van tenir algun tipus de nexe amb la transferència d'informació des del núvol i a altres sistemes externs de l'organització, incloent-hi la transmissió de dades entre diferents aplicacions i sistemes, la col·laboració amb proveïdors externs, clients o socis comercials, l'accés remot d'usuaris i la connexió amb xarxes públiques d'Internet.

4.6 Ciberatacs d'actors patrocinats per Estats:

Els grups de ciberdelinqüents patrocinats per Estats s'han convertit en una amenaça important pels entorns *cloud*, perquè són conscients que vulnerant-los poden provocar importants estralls en les organitzacions que tenen en el punt de mira. Així ho demostren les dades, i és que el 37% dels incidents al *cloud* del 2022, s'hi van veure involucrats alguns d'aquests grups.

La seva activitat contra els serveis al núvol d'entitats "enemigues" permet que, si l'atac té èxit, aconsegueixi comprometre la seguretat del proveïdor de serveis i, al seu torn, pugui acabar afectant altres clients, provocant un impacte en cadena en tota la xarxa de subministrament. A més, la naturalesa distribuïda dels sistemes *cloud* pot dificultar la detecció i la resposta davant els seus atacs, ja que solen ser dels més sofisticats i complexos a nivell tècnic.

5. ASPECTES A TENIR EN COMPTE SOBRE LA SEGURETAT AL NÚVOL

A priori, podria semblar que únicament es tracta d'una extensió de la seguretat informàtica convencional heretada, però la veritat és que es tracta d'un nou paradigma que abasta tecnologies, protocols i mètodes. A continuació, veurem sobre quins elements han de dirigir-se les mesures de protecció i quina és la finalitat de cadascuna d'elles.

5.1 Protecció de dades i privacitat:

La seguretat de les dades és un tema crític en qualsevol sistema de tecnologia de la informació. No obstant això, en el núvol, on les dades s'emmagatzemen i administren en servidors de proveïdors externs, la seva protecció es converteix en una preocupació encara major. A més, aquests servidors poden estar en diferents ubicacions geogràfiques i sota la propietat de diferents entitats, la qual cosa exigeix que tinguin en compte totes i cadascuna de les normatives que apliquin en cada cas.

La implementació de controls d'accés, el xifratge de dades, les còpies de seguretat de dades crítiques o el compliment normatiu són només alguns dels aspectes clau que han de tenir-se en compte per garantir un grau de protecció i privacitat adequat. Donat que tots dos aspectes convergeixen en molts punts, un correcte maneig i gestió de les dades dificulta que es produeixin falles de protecció o privacitat que puguin ser explotades per un atacant. A continuació, es detallen els procediments i recomanacions que poden facilitar un major nivell de protecció:

- Implementació de controls d'accés: és essencial garantir que només les persones autoritzades podran accedir a les aplicacions o a les dades d'una companyia. Aquests controls han d'incloure autenticació d'usuaris mitjançant el sistema multifactor en el qual s'exigeixi l'ús de contrasenyes segures, i accessos basats en rols i amb permisos restringits, la qual cosa permet als administradors limitar l'accés a les dades segons la funció i el nivell de responsabilitat de cada usuari.

  A més, la gran majoria de proveïdors de serveis *cloud*, ofereixen solucions avançades de gestió centralitzada d'identitats per a facilitar la seva administració i oferir un major control a organitzacions i usuaris.

- Xifratge de dades: aquesta mesura és una altra de les bàsiques i essencials per garantir la protecció de les dades perquè encara que algú tingués accés de manera il·legítima, no podria usar-les sense la corresponent clau de desxifrat. El xifratge de dades *cloud* pot realitzar-se a la capa d'aplicació o en la capa d'emmagatzematge.

  Els proveïdors de serveis al núvol poden oferir l'opció de xifrar les dades tan en repòs com en trànsit, la qual cosa ajuda a garantir que les dades confidencials es mantinguin segures

en tot moment. A més, poden proporcionar eines per la gestió de claus de xifratge, la qual cosa permet als usuaris tenir un major control sobre les seves dades.

- Còpia de seguretat de dades crítiques: és un altre dels punts essencials del manual de bones pràctiques, perquè davant qualsevol classe d'incident que provoqui la pèrdua, furt o encriptació de les dades, ràpidament es podria tornar a comptar amb ells. És imprescindible dur a terme còpies de seguretat amb la periodicitat que millor s'ajusti a les necessitats de cada negoci, però tenint en compte sempre que, a major freqüència, existeix major probabilitat de disposar d'una còpia de seguretat amb les dades més recents i actualitzats.

- Control de versions: és una pràctica comuna en el desenvolupament de programari que també és important per a la protecció de dades en el núvol. Permet als administradors portar a cap un seguiment dels canvis en les dades i revertir a una versió anterior en cas que es produeixi un error o una pèrdua de dades.

- Monitoratge d'activitat de l'usuari: és una pràctica crucial per controlar les activitats dels usuaris i detectar qualsevol activitat que sigui inusual. D'aquesta manera es poden detectar possibles incidents, com un intent d'accés no autoritzat a les dades, i donar una resposta ràpida i eficaç.

- Protecció de la informació personal de l'usuari: l'anonimització de dades és una tècnica que elimina les dades identificatives dels registres per garantir que les dades no puguin ser associades amb un individu en particular.

- Ús de VPN: millora la protecció de les connexions ja que xifren el seu trànsit a internet i camuflen les identitats en línia, la qual cosa dificulta que es pugui fer un seguiment de l'activitat que té una organització o qualsevol dels seus usuaris.

- Compliment de regulacions de privacitat: els proveïdors de serveis al núvol poden oferir solucions i eines que els permetin complir amb les normes i regulacions de seguretat i privacitat aplicables, com el Reglament General de Protecció de Dades (GDPR) o la Llei de Portabilitat i Responsabilitat d'Assegurances de Salut (HIPAA).

5.2 Seguretat de la infraestructura:

En aquest punt s'aprofundirà sobre com protegir una infraestructura desplegada al núvol i els diferents elements que la componen:

- Seguretat de la xarxa: és un element crucial en una infraestructura *cloud*. S'han d'implementar mesures de seguretat com tallafocs, detecció d'intrusions, filtrat de paquets i altres tecnologies per a protegir la xarxa i els sistemes contra amenaces.• Seguretat d'aplicacions: han de ser segures i estar protegides contra atacs de seguretat. És important

implementar mesures de seguretat com el control d'accés, la validació d'entrades, la gestió d'errors i el xifratge de dades.

- Autenticació i autorització: és important implementar mecanismes d'autenticació i autorització robustos per a garantir que només els usuaris autoritzats tinguin accés als sistemes i aplicacions en el núvol.

- Gestió de vulnerabilitats: com ja se sap, les vulnerabilitats són una porta d'entrada per als ciberdelinqüents. És rellevant implementar una estratègia de gestió de vulnerabilitats, que inclogui l'aplicació de pegats i actualitzacions de seguretat de manera regular.

- Monitoratge i anàlisi: són fonamentals per a detectar i respondre ràpidament a les amenaces de seguretat en el núvol. S'han d'implementar eines de monitoratge i anàlisi per a detectar patrons de comportament anòmals i alertar al personal de seguretat en cas d'activitat sospitosa.

5.3 Gestió de riscs:

La gestió de riscos en el núvol se centra en l'enfocament estratègic sobre identificació i plans d'actuació per a mitigar qualsevol amenaça que pugui derivar-se de desplegar serveis en una infraestructura *cloud*. Per això, és important elaborar una anàlisi prèvia, avaluacions contínues i assegurar-se que l'organització en qüestió compleix amb les següents pràctiques:

- Avaluació de riscs: és important identificar i quantificar els riscs associats amb la migració de dades al núvol així com seleccionar adequadament els proveïdors que garanteixin complir amb els requisits de seguretat de l'organització.

- Contractes i acords de nivell de servei (SLA): establir requisits de seguretat clars als contractes i SLA amb proveïdors de serveis al núvol, incloent-hi la responsabilitat compartida per la seguretat.

- Pla de continuïtat del negoci i recuperació davant de desastres: garantir que l'organització pugui recuperar les dades i els sistemes al núvol en cas d'interrupcions al servei o desastres naturals.

- Monitoratge d'amenaces i vulnerabilitats: identificar i abordar de manera proactiva les amenaces i vulnerabilitats de seguretat al núvol.

- Capacitació i conscienciació: garantir que els empleats comprenguin els riscs associats amb l'adopció de sistemes al núvol i sàpiguen com protegir les seves dades i recursos.

5.4 Governança, compliment i auditories de seguretat:

En darrer lloc, és imprescindible exercir un control sobre l'administració i gestió tècnica dels recursos dels quals disposa una organització. De tal manera que és de vital importància implementar:

- Polítiques i procediments clars: necessari per establir expectatives clares sobre els requisits de seguretat i els processos necessaris per garantir la seguretat de les dades i els recursos del núvol.
- Monitoratge i supervisió: rellevant per avaluar contínuament l'eficàcia dels controls de seguretat en el núvol, així com la identificació i resposta a possibles amenaces.
- Compliment regulador: essencial per a garantir que les activitats en el núvol compleixin amb els requisits legals, reglamentaris i contractuals, així com amb les millors pràctiques de seguretat.
- Auditoria i revisió: important per tal d'avaluar l'eficàcia dels controls de seguretat al núvol i assegurar que es mantinguin els requisits de seguretat al llarg del temps.

6. INCIDENTS DE SEGURETAT AL NÚVOL MÉS IMPORTANTS DEL 2022

6.1 Fuga de dades de FlexBooker

Al maig del 2022, FlexBooker, una empresa estatunidenca de software de programació d'esdeveniments, va experimentar una violació de dades que va comprometre la informació personal i de pagament de més d'1 milió de clients.

La violació de dades de FlexBooker va ser el resultat d'una vulnerabilitat a la seva infraestructura al núvol que va permetre a un atacant no autoritzat accedir a les seves bases de dades. Segons els informes, les dades compromeses van incloure noms, adreces de correu electrònic, números de telèfon, adreces físiques i detalls de pagament, inclosos els números de targeta de crèdit i els respectius codis de seguretat.

FlexBooker va notificar als seus clients de la violació de dades i els va proporcionar informació sobre com protegir les seves credencials personals i financeres. També va treballar per enfortir la seguretat de la seva infraestructura al núvol i prevenir futures fugues de dades.

Aquest incident de seguretat és un exemple de com una mala configuració de la infraestructura al núvol i la falta de mesures de seguretat adequades poden comportar una filtració de dades important. Per prevenir aquest tipus d'incidents, és important implementar controls de seguretat robustos a la infraestructura del núvol, realitzar proves regulars de seguretat i dur a terme exercicis de monitoratge de manera activa i constant per detectar qualsevol activitat sospitosa.

6.2 Fuga de 2,4TB de dades relacionada amb BlueBleed

La fuga de dades de BlueBleed es va produir el gener del 2022 i es va considerar un dels incidents de ciberseguretat més destacats de l'any. L'empresa afectada va ser la companyia de *hosting web* estatunidenc DreamHost, que albergava els servidors de la plataforma de *blogging* de codi obert WordPress.

L'incident va ser provocat per una vulnerabilitat al programari de gestió de continguts del servidor, coneguda com a BlueBleed. Aquesta vulnerabilitat va permetre a un atacant remot accedir a les dades de més d'1,5 milions de llocs web de WordPress allotjats als servidors de DreamHost, la qual cosa va suposar un escapament de dades del voltant d'uns 2,4 terabytes.

Entre les dades filtrades es trobaven credencials d'inici de sessió, contrasenyes, informació personal dels usuaris i dades de pagament. La gravetat de l'incident va ser de primer ordre, ja

que la informació compromesa podia ser utilitzada pels ciberdelinqüents per dur a terme atacs de phishing i altres delictes cibernètics relacionats amb el furt d'identitats.

Aquesta fuga de dades va subratllar la importància de mantenir actualitzat el programari de gestió de continguts i altres sistemes al núvol, així com de dur a terme proves de seguretat regulars per detectar i posar remei a possibles vulnerabilitats. També va destacar la necessitat de comptar amb protocols de seguretat sòlids i mesures de protecció de dades per garantir la seguretat de les dades al núvol.

6.3 Fuga de dades de la policia de Shanghai

És una de les filtracions de dades més greus i extenses que s'han registrat fins avui dia. Els atacants van aconseguir accedir a les dades de més de 1.000 milions de ciutadans xinesos. Entre les dades obtingudes i de més rellevància, hi podem trobar noms, números de contacte, números d'identificació del govern i informes policials.

L'accés no autoritzat a la base de dades de la policia de Shanghai es va produir a través d'un panell d'administració al qual es podia accedir públicament des d'Internet. Malgrat que la base de dades en si era segura, la mala configuració del panell d'administració va permetre als atacants accedir a la informació que aquesta contenia. La base de dades compromesa estava allotjada a Alibaba Cloud, la plataforma de serveis al núvol del proveïdor Alibaba Group.

Els atacants van intentar coaccionar al departament de policia de Shanghai per 200.000 dòlars a canvi de no fer pública tota la informació aconseguida. Aquest tipus d'extorsió s'ha tornat cada vegada més comuna als incidents de ciberseguretat, i posa en relleu la importància de tenir una estratègia sòlida de resposta a amenaces en cas que es produeixin filtracions de dades.

6.4 Atac de Lapsus$ a Microsoft

Aquest fet va ocórrer el març de l'any 2022 i es tracta d'un atac de *ransomware* dirigit a la infraestructura del núvol de Microsoft. El grup de hackers, Lapsus$, va ser responsable de l'atac en qüestió i es creu que es va originar a Rússia.

L'atac va afectar els serveis de núvol de Microsoft, incloent-hi Azure i Office 365, i es va informar que les dades d'alguns clients de Microsoft també es van veure compromeses. Els atacants van dur a terme un furt i a continuació van xifrar les dades, exigint un rescat en criptomonedes a canvi del seu alliberament.

Malgrat que Microsoft va afirmar que va poder contenir l'atac i que només es van veure afectats un nombre limitat de clients, l'incident va posar en relleu la importància d'implementar mesures

de seguretat adequades al núvol per prevenir i mitigar de manera específica els atacs de *ransomware* inclús en les entitats més grans on els protocols de seguretat són més estudiats.

6.5 Fuga de dades de Medibank

L'incident de violació de dades de Medibank va ocórrer el febrer del 2022, quan es va informar que les dades personals d'aproximadament un 100,000 clients de Medibank, una companyia d'assegurances de salut australiana, havien estat exposats en línia. Les dades robades incloïen informació personal com ara noms, adreces, dates de naixement i números de contacte, així com números de pòlissa d'assegurança i detalls de reclamacions.

L'incident de Medibank es relaciona amb la seguretat *cloud* perquè la companyia hi havia migrat recentment gran part de la seva infraestructura tecnològica amb l'objectiu d'augmentar l'eficiència i reduir els costos.

No obstant això, després d'aquesta migració un tercer no autoritzat va poder accedir a la informació a través d'una aplicació en el núvol que Medibank havia utilitzat per a compartir dades amb proveïdors externs. La companyia australiana va dir que s'havien pres mesures per tancar la bretxa de seguretat i que havia notificat als clients afectats de l'incident.

Això subratlla la importància d'assegurar adequadament els sistemes al núvol i tenir en compte els riscos de seguretat inherents a la tecnologia *cloud*. Les empreses han d'implementar mesures de seguretat adequades per protegir els seus sistemes i dades, i han de tenir en compte els riscs específics de compartir dades amb tercers.

6.6 Fuga de dades de Pegasus Airlines

L'incident de seguretat de Pegasus Airlines va involucrar l'exposició del voltant 23 milions d'arxius que contenien informació de passatgers i empleats de l'aerolínia. Les dades exposades incloïen noms complets, dates de naixement, números de telèfon, adreces de correu electrònic, números de passaport, informació de vols i dades de targetes de crèdit.

La bretxa es va deure a una vulnerabilitat en un servidor d'Amazon Web Services (AWS) utilitzat per l'aerolínia per a emmagatzemar dades de clients i empleats.

Segons els informes, una mala configuració del servidor va permetre l'accés no autoritzat als arxius. Aquest incident destaca la importància d'assegurar adequadament els servidors i la infraestructura al núvol, així com de seguir les millors pràctiques de seguretat recomanades pels proveïdors de serveis al núvol per evitar fugues de dades i altres problemes de seguretat.

6.7 Fuga de dades de Mangatoon

Mangatoon és una plataforma en línia que permet als usuaris llegir còmics i novel·les gràfiques. El setembre del 2022, es va descobrir que la plataforma havia sofert una violació de dades que va afectar milions d'usuaris. Els atacants van aconseguir accedir a les dades personals dels internautes. Entre les dades aconseguides hi ha noms d'usuari, contrasenyes, adreces de correu electrònic i números de telèfon.

Totes aquestes dades estaven allotjades al núvol i, segons es va informar, la filtració va ser causada per una configuració incorrecta de seguretat al servidor que contenia la informació dels usuaris. El servidor afectat, que pertany a l'empresa xinesa Tencent Cloud, va ser descoberta per un investigador de seguretat que va informar del problema a Mangatoon.

A més de la informació personal, els atacants també van aconseguir accedir a les dades de pagament d'alguns usuaris. Mangatoon va notificar als usuaris afectats i els va recomanar canviar les seves contrasenyes i vigilar els seus comptes bancaris per a detectar qualsevol activitat sospitosa. La companyia també va millorar la seva seguretat i va anunciar plans per a enfortir encara més la seva seguretat en el futur.

6.8 Exposició de dades d'Amazon Prime Video

Aquest incident es va produir el setembre del 2022 i es va produir per la configuració incorrecta de permisos d'accés en un servidor d'Amazon Web Services (AWS) que contenia dades i registres de visualització de programes de televisió i pel·lícules, incloent-hi informació d'identificació personal, com ara noms i adreces de correu electrònic dels usuaris. La conseqüència va ser que les dades eren accessibles de manera pública.

Encara que Amazon va afirmar que no hi havia evidència que les dades exposades haguessin estat utilitzades maliciosament, l'incident va posar en relleu la importància de la configuració adequada dels permisos d'accés al núvol i la necessitat de les empreses de mantenir la seguretat de les seves dades.

6.9 Fuga de dades de Civicom

L'any 2022 es va produir una fuga massiva de dades a l'empresa de serveis de comunicació Civicom, on es van exposar més d'1,4 terabytes de dades delicades dels seus clients, incloent-hi noms, adreces de correu electrònic, contrasenyes i números de telèfon. La informació també

incloïa detalls de les transaccions realitzades pels clients, la qual cosa augmentava el risc de frau i abús de targetes de crèdit.

L'escapament de les dades es va produir per una configuració incorrecta al servidor d'emmagatzematge al núvol d'Amazon Web Services (AWS) utilitzat per Civicom, la qual cosa va permetre l'accés no autoritzat a les dades emmagatzemades.

L'empresa va trigar diverses setmanes a informar els clients sobre l'incident i, segons els informes, no havia implementat mesures adequades de seguretat per a protegir les dades dels seus clients.

7. GLOSSARI

Accés no autoritzat

Fa referència a l'acció d'ingressar o utilitzar un recurs informàtic, sistema o xarxa sense permís o consentiment del propietari o administrador autoritzat. Aquest tipus d'accés sol ser considerat com una violació de la seguretat informàtica i pot portar conseqüències legals i financeres per l'infractor. L'accés no autoritzat pot ser intencional o accidental, i pot ser causat per una varietat de factors, com la feblesa en les contrasenyes, la falta de mesures de seguretat adequades o l'explotació de vulnerabilitats en el sistema.

Actors patrocinadors per Estats

Grup d'individus que realitzen atacs cibernètics en nom d'un govern o d'una organització governamental. Aquests actors poden ser emprats pel govern o treballar en col·laboració amb el mateix i solen tenir accés a recursos i eines avançades, com programari maliciós sofisticat, tècniques d'enginyeria social i vulnerabilitats de *day zero*. Els seus objectius poden incloure l'obtenció d'informació confidencial, el furt de la propietat intel·lectual, el sabotatge o la interrupció d'infraestructures crítiques.

API

Una *Application Programming Interface*, per les seves sigles en anglès: API, és un conjunt de protocols, eines i estàndards de programació que permeten la comunicació entre diferents aplicacions o sistemes informàtics. En altres paraules, una API és un intermediari que permet que diferents programes o serveis es comuniquin entre si, intercanviant informació i recursos de manera estructurada i estandarditzada. Això fa possible que les aplicacions de tercers puguin accedir a les dades o funcionalitats d'un sistema o plataforma, sense necessitat d'haver de desenvolupar tot des de zero.

Ciberatac

Intent deliberat d'un ciberdelinqüent d'obtenir accés a un sistema informàtic sense autorització servint-se de diferents tècniques i vulnerabilitats per la realització d'activitats amb finalitats malicioses, com el robatori d'informació, extorsió del propietari o simplement danys al sistema.

Entorn cloud

Es refereix a la infraestructura i serveis de computació, emmagatzematge i xarxes que es lliuren a través d'Internet per proveïdors de serveis al núvol, com Amazon Web Services, Microsoft Azure i Google Cloud. Aquest entorn permet a les empreses i organitzacions accedir a recursos

informàtics flexibles i escalables segons les seves necessitats, sense haver d'invertir en maquinari i programari propi. A més, l'entorn *cloud* també permet la implementació de solucions de seguretat, còpia de seguretat i recuperació davant desastres de manera eficient i efectiva.

Entorn local

També conegut com a entorn *on-premise*, es refereix a la infraestructura informàtica que una empresa posseeix i administra dins de les seves pròpies instal·lacions físiques, en lloc d'utilitzar serveis al núvol. En aquesta mena d'entorn, l'empresa és responsable de l'adquisició, instal·lació, configuració, manteniment i seguretat dels seus propis servidors, xarxes, sistemes d'emmagatzematge i aplicacions informàtiques.

Fuga de dades

També coneguda com a bretxa de dades, és una situació en la qual es produeix una divulgació no autoritzada d'informació confidencial, que pot incloure dades personals, financers, mèdiques o comercials. Les fugues de dades poden ocórrer a causa d'errors humans, falles tècniques, atacs informàtics o qualsevol altra causa que permeti que la informació confidencial sigui accessible a persones no autoritzades. Els escapaments de dades poden tenir greus conseqüències, com el furt d'identitat, el frau financer, la pèrdua de reputació i la responsabilitat legal.

Hipervisors

Són softwares que s'utilitzen per virtualitzar els recursos de la infraestructura cloud, permetent que múltiples sistemes operatius i aplicacions s'executin en un sol servidor físic.

Malware

És un tipus de programari que té com a objectiu danyar o infiltrar-se sense el consentiment del seu propietari en un sistema d'informació. El mot neix de la unió dels termes en anglès de programari maliciós: *malicious software*. Dins d'aquesta definició té cabuda un ampli ventall de programes maliciosos: virus, cucs, troians, *backdoors*, *spyware*, etc. La part que comparteixen tots aquests programes és el seu caràcter nociu o lesiu.

Middleware

Proporcionen una capa de programari entre les aplicacions i els sistemes operatius subjacents, permetent usar les aplicacions de manera descentralitzada, i flexible.

VPN

VPN són les sigles de "Virtual Private Network" o en català, "Xarxa Privada Virtual". Es tracta d'una tecnologia de xarxa que permet establir una connexió segura i xifrada entre dos dispositius a través d'Internet, com si estiguessin connectats a una xarxa local privada. Les VPN s'utilitzen comunament per protegir la privacitat i la seguretat de les comunicacions en línia, ocultar la ubicació geogràfica i el trànsit d'Internet i per permetre l'accés remot a recursos de xarxa restringits.

CLÀUSULA DE CONFIDENCIALITAT