ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Enfortir les barreres digitals: l'estratègia de la Unió Europea en ciberseguretat

TLP:WHITE

DESEMBRE 2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	27/12/2023	27/12/2023

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

Els ciberatacs representen una gran preocupació creixent a l'era digital. Sectors crucials com ara el transport, l'energia, la sanitat i les finances estan experimentant una dependència creixent de les tecnologies digitals a les seves operacions. Malgrat els beneficis i les oportunitats que representa tot això, els ciutadans i les organitzacions estan més exposats i són més vulnerables a les ciberamenaces i els ciberatacs.

A mesura que avança la tecnologia, els ciberdelinqüents busquen formes noves d'explotar vulnerabilitats i comprometre la seguretat d'individus, empreses i, fins i tot, governs, cosa per la qual estan creant constantment amenaces noves i cada vegada més sofisticades i perilloses.

Segons dades de la Comissió Europea, la incidència econòmica de la ciberdelinqüència es va quintuplicar entre els anys 2013 i el 2017. S'estima que el cost anual de la ciberdelinqüència per a l'economia mundial va augmentar a 5,5 bilions d'euros a finals del 2020, i va duplicar la xifra registrada el 2015. Aquesta tendència s'ha continuat agreujant i la projecció és que per al 2025, aproximadament 41.000 milions de dispositius arreu del món estaran connectats a l'internet de les coses.

La ciberseguretat a la Unió Europa (UE) és un tema d'importància estratègica i està en evolució constant per fer front a les amenaces cibernètiques que estan augmentant considerablement. La UE ha implementat diverses mesures i estratègies per abordar els desafiaments en l'àmbit de la ciberseguretat i protegir la infraestructura digital dels seus estats membres. La cooperació entre els estats membres, la legislació específica i el foment de les millors pràctiques són elements clau en els esforços de la UE per garantir la seguretat digital als països de la UE.

Al llarg d'aquest informe, presentarem quins són els avenços de la UE en matèria de ciberseguretat a nivell d'actors i iniciatives, quines són les tendències de ciberamenaces i ciberatacs a les quals haurà de fer front, i exemples concrets de ciberatacs que han succeït a la UE.

Considerem que el fet de conèixer les polítiques i les accions de la UE en ciberseguretat permet a les empreses i a qualsevol mena d'organització d'aquests països alinear-se amb les millors pràctiques, complir amb els requisits normatius, accedir a recursos i col·laborar amb eficàcia en la lluita contra les amenaces cibernètiques. A més a més, contribueix a la resiliència cibernètica a nivell nacional i europeu.

3. INICIATIVES DE LA UNIÓ EUROPEA

La seguretat a les xarxes i de la informació és essencial per assegurar la prosperitat i mantenir el desenvolupament econòmic de la Unió Europea (UE). En aquest context, la UE ha estat treballant en diferents àrees per assegurar la ciberseguretat a Europa amb l'objectiu de preservar la confiança dels usuaris, estimular una economia digital i, per tant, mantenir el desenvolupament correcte del mercat interior i promoure el creixement i l'ocupació.

Les mesures que està prenent la UE per enfortir la ciberseguretat es duen a terme en els àmbits següents:

- Millorar la ciberresiliència.
- Lluitar contra els ciberdelinqüència.
- Impulsar la ciberdiplomàcia.
- Reforçar la ciberdefensa.
- Fomentar la recerca i la innovació.
- Protegir les infraestructures crítiques.

La implementació de mesures sòlides en ciberseguretat és fonamental per establir un ciberespai obert i segur. Aquestes mesures no només protegiran les infraestructures, sinó que també cultivaran la confiança dels ciutadans en les eines i els serveis digitals. La ciberseguretat exercirà un paper fonamental en cultivar una adopció generalitzada i confiada de les tecnologies digitals a la societat.

Tot seguit explicarem quins són els actors rellevants en matèria de ciberseguretat per a la UE i quins són els avenços més significatius per fer front als ciberatacs i a la ciberdelinqüència.

3.1. Actors rellevants

El mapa dels actors que col·laboren en el marc de la política de ciberseguretat de la UE s'ha anat expandint al llarg dels darrers anys. Igualment, la UE coopera estretament amb socis internacionals en temes de ciberseguretat. Això inclou col·laboració amb organitzacions com ara la INTERPOL, l'OTAN i altres estats per abordar les amenaces cibernètiques de manera conjunta.

Tot seguit, esmentem algunes de les institucions més importants relacionades amb la ciberseguretat a la UE, les quals s'han categoritzat en tres grups:

3.1.1. Actors creats per garantir la ciberseguretat europea

Dintre dels actors creats per garantir la ciberseguretat europea podem esmentar tres entitats.

Agència de la Unió Europea per a la Ciberseguretat (ENISA)

- Data de fundació: 13 de març de 2004.
- Seu: Atenes, Grècia.

ENISA exerceix un paper crucial en la salvaguarda de la ciberseguretat en l'àmbit europeu, i treballa en consonància amb la política de seguretat cibernètica de la Unió Europea. La seva tasca se centra a impulsar millores en l'àmbit de les tecnologies de la informació i la comunicació (TIC). L'objectiu primordial d'ENISA és consolidar la confiança de la població en l'economia digital i el comerç en línia, i alhora dedicar-se a protegir els ciutadans europeus contra l'amenaça de la ciberdelinqüència.

Aquest organisme, a més a més, és una font clau per a informes i avaluacions sobre la ciberseguretat a la UE, atès que publica regularment informes que tracten amenaces emergents, tendències i millores pràctiques en ciberseguretat.

- Equip de Resposta a Incidents de Seguretat Informàtica de la Unió Europea (CSIRT-UE, per les seves sigles en anglès)

Aquest equip forma part d'ENISA i actua com a punt focal per a la cooperació entre els equips de resposta a incidents cibernètics dels estats membres de la UE. El seu objectiu és millorar la capacitat de resposta a incidents cibernètics a nivell europeu.

La Xarxa nacional d'Equips de Resposta a Incidents de Seguretat Informàtica (CSIRT-UE) es configura mitjançant la col·laboració de CSIRT designats pels estats membres de la Unió Europea i el CERT-UE (membres de la Xarxa de CSIRT). La participació de la Comissió Europea en aquesta xarxa es fa en qualitat d'observador.

ENISA està impulsant la xarxa de CSIRT tot proporcionant infraestructures i eines a l'equip de la Secretaria. Això facilita una cooperació efectiva, assegura un funcionament diari sense interrupcions i promou l'intercanvi d'informació.

Xarxa Judicial Europea contra la ciberdelinqüència (EJCN)

- Any de fundació: 2016.

Es va crear amb el propòsit de promoure la interacció entre professionals especialitzats a abordar els desafiaments plantejats per la ciberdelinqüència, la delinqüència cibernètica i les investigacions al ciberespai, per tal d'optimitzar l'eficiència de les investigacions i els processos judicials. L'EJCN facilita i millora la cooperació entre les autoritats judicials competents en possibilitar l'intercanvi de coneixements especialitzats, millors pràctiques i altres sabers rellevants relacionats amb la investigació i l'enjudiciament de la ciberdelinqüència.

Centre Europeu de Competència Industrial, Tecnologia i de Recerca en Ciberseguretat

- Any de fundació: 2021.
- Seu: Bucarest, Romania.

La UE va establir aquest centre de ciberseguretat amb el propòsit d'enfortir la ciberresiliència, donar suport a la recerca i potenciar les iniciatives en desenvolupament tecnològic. Les seves funcions principals inclouen facilitar la tasca de la Xarxa de Centres Nacionals de Coordinació designats pels estats membres, com també proporcionar suport financer en l'àmbit de la ciberseguretat a través dels programes Horitzó Europa i Europa Digital. Inaugurat el maig de 2023, el centre té la seva seu a la Universitat Politècnica de Bucarest.

3.1.2. Noves seccions en departaments o institucions ja existents

En els darrers anys han aparegut organismes (anomenats cèl·lula, comitè, oficina, grup de treball o centre) dedicats a la ciberseguretat, l'objectiu principal dels quals és agilitar la cooperació entre els actors que pertanyen a la xarxa de ciberseguretat.

Direcció General de la Comissió Europea per a les Xarxes els Continguts o les Tecnologies de la Comunicació de l'any 2012.

- Any de fundació: 2012

Aquesta Direcció elabora i implanta les polítiques de la Comissió sobre recerca i innovació, i economia i societats digitals.

Centre Europeu de la Ciberdelinqüència (EC3)

- Data de fundació: 11 de gener de 2013
- Seu: La Haia, Països Baixos.

L'Agència de la Unió Europea per a la Cooperació Policial (Europol) va crear l'EC3 amb el propòsit d'enfortir la resposta policial enfront de la ciberdelinqüència a la Unió Europea, per contribuir d'aquesta manera a la protecció dels ciutadans, les empreses i els governs europeus. En termes operatius, l'EC3 es focalitza en diversos tipus de delictes cibernètics, com ara delictes ciberdependents, explotació sexual infantil i frau de pagament. A més a més, exerceix un paper actiu en la lluita contra la criminalitat al web fosc i a les plataformes alternatives.

Cèl·lula de Fusió Híbrida de la UE del Servei Europeu d'Acció Exterior

- Any de fundació: 2016.
- Seu: Hèlsinki, Finlàndia (des del 2017).

Aquesta va ser creada dins del Servei Europeu d'Acció Exterior. Es basa en el treball d'analistes procedents dels serveis d'intel·ligència i seguretat dels estats membres, tant militars com civils, per examinar informació confidencial i de font oberta relacionada amb amenaces híbrides.

Grup Horitzontal 'Qüestions cibernètiques' ('Ciber')

- Any de fundació: 2016

El grup té la responsabilitat de coordinar els treballs del Consell relatius a qüestions cibernètiques, i es focalitza especialment en polítiques i activitats legislatives en l'àmbit del ciberespai. Manté una col·laboració estreta amb altres grups afins, com també amb la Comissió Europea, el Servei Europeu d'Acció Exterior (SEAE), l'Agència de la Unió Europea per a la Cooperació Policial (EUROPOL), l'Agència de la Unió Europea per a la Cooperació Judicial Penal (EUROJUST), l'Agència dels Drets Fonamentals de la Unió Europea (FRA), l'Agència Europea de Defensa (AED) i ENISA.

3.1.3. Actors rellevants per a la ciberseguretat, amb funcions pròpies

En aquesta classificació s'hi inclouen actors que, atesa la seva importància per a la ciberseguretat, desenvolupen gradualment funcions i competències addicionals, i aprofiten els seus rols i responsabilitats preexistents.

Agència de Defensa Europea (EDA, per les seves sigles en anglès)

- Any de fundació: 2004.
- Seu: Brussel·les, Bèlgica.

Es tracta d'una agència de la Unió Europea que té la responsabilitat de fomentar la cooperació i la recerca en les capacitats militars presents i futures dels estats membres de la UE, amb l'objectiu d'enfortir la indústria europea de defensa.

Equip de resposta a emergències informàtiques de les institucions òrgans i organismes de la Unió Europea (CERT-EU)

- Any de fundació: 2011.
- Seu: Brussel·les, Bèlgica.

El CERT-EU ofereix serveis de resposta a incidents, coordinació i assessorament en ciberseguretat a les institucions i agències de la Unió Europea. Està compost per un grup d'experts en seguretat informàtica que pertanyen a les institucions i òrgans de la UE.

Aquest organisme s'encarrega de recopilar, gestionar, analitzar i compartir informació amb les institucions, els òrgans i les agències de la UE sobre amenaces, vulnerabilitats i incidents relacionats amb infraestructures de TIC no classificades. També coordina les respostes a incidents a escala interinstitucional i institucional, per exemple, tot proporcionant suport i coordinant a l'Equip de Resposta a Emergències Informàtiques de la UE i treballa específicament amb les institucions i agències de la UE.

Cal assenyalar que tant els CSIRT com els CERT se centren en la resposta a incidents. Tot i que comunament es fan servir com a sinònims, hi ha una distinció tècnica entre ambdós termes. CERT és una marca registrada i se sol associar més amb la intel·ligència d'amenaces, mentre que un CSIRT té una connotació més àmplia i s'associa amb un equip multifuncional.

Altres actors

En aquesta categoria també entrarien el Centre de Recerca Conjunta de la Comissió Europea, l'Agència de la Unió Europea per a la Cooperació Policial (EUROPOL) i l'Agència de la Unió Europea per a la Cooperació Judicial Penal (EUROJUST).

3.1.4. Conveni de Budapest

El Conveni sobre Delictes Cibernètics, conegut també com el Conveni de Budapest sobre Delictes Cibernètics o Conveni de Budapest, representa el primer tractat internacional dissenyat per abordar els delictes informàtics i els comesos a Internet. El seu enfocament radica en l'harmonització de lleis entre nacions, la millora de tècniques d'investigació i l'enfortiment de la cooperació entre els països signataris. El Consell d'Europa a Estrasburg va

ser l'organisme que es va encarregar de la seva elaboració, amb la participació del Canadà, el Japó i la Xina com a observadors. Signat l'any 2001, el conveni va entrar en vigor l'1 de juny del 2004.

Aquest conveni ha estat l'eina clau per marcar a nivell internacional les passes que ha de seguir cada estat a l'hora de perseguir els ciberdelictes, proporcionar un marc legal per a la cooperació internacional i una guia comuna de mesures per detectar i perseguir els ciberdelinqüents. No obstant això, també hi ha altres instruments i protocols de vital importància com ara la Convenció de Ciberdelinqüència de les Nacions Unides (UN), actualment en la fase del Comitè d'Experts, i diverses Directives europees i organismes creats per intentar prevenir i, si s'escau, pal·liar els ciberatacs.

3.1.5. Estratègia Global per a la Política Exterior i de Seguretat de la UE (2016)

En aquesta estratègia, la ciberseguretat es configura com una política transversal que s'ha d'enfortir en tots els àmbits d'actuació de la UE i garantir una major eficiència, eficàcia i interoperabilitat en totes les polítiques implementades, on hi ha múltiples actors involucrats. És a dir, la UE ha d'enfortir la cibergovernança multinivell i transversal a totes les seves polítiques.

3.1.6. Estratègia de Ciberseguretat de la UE

La UE ha desenvolupat una estratègia de ciberseguretat que busca garantir un nivell elevat i comú de seguretat en tots els països membres. Aquesta estratègia tracta la prevenció, la preparació, la resposta i la recuperació davant dels ciberatacs.

Primera Estratègia de Ciberseguretat: un ciberespai obert i segur (2013)

La primera Estratègia de Ciberseguretat va representar un pas significatiu en l'enfocament coordinat de la UE per abordar els desafiaments cibernètics en evolució constant. Aquesta estratègia posava èmfasi en la feina de la que seria coneguda com a Directiva NIS (sigla en anglès de «xarxes i sistemes d'informació»), que establiria uns requisits mínims al voltant de la ciberseguretat a tots els estats membres, i en garantiria la coordinació en constituir òrgans de contacte per participar en xarxes pertinents i servir d'enllaç amb l'ENISA i la Comissió Europea.

Nova Estratègia de Ciberseguretat (2020)

La nova estratègia de la UE (2020-2025) se centra en àmbits prioritaris en què la UE pot aportar valor per ajudar els estats membres a promoure la seguretat de tots els habitants d'Europa. L'objectiu és reforçar la resiliència d'Europa enfront de les ciberamenaces i garantir que tots els ciutadans i empreses es puguin beneficiar plenament de serveis i eines digitals segurs i fiables. La nova estratègia conté propostes concretes per a la implantació d'instruments normatius, d'actuació i d'inversió.

3.1.7. Directiva de seguretat de les xarxes i la informació (NIS)

La Directiva sobre la seguretat de les xarxes i sistemes d'informació (NIS, per les seves sigles en anglès), adoptada l'any 2016, va ser la primera mesura legislativa a escala de la UE destinada a estrènyer la cooperació entre els estats membres pel que fa a la qüestió crucial de la ciberseguretat. Hi van establir obligacions de seguretat per als operadors de serveis essencials (a sectors vitals com ara l'energia, el transport, la sanitat i les finances) i els proveïdors de serveis digitals (mercats en línia, motors de cerca i serveis al núvol).

L'any 2022, la UE va adoptar una revisió de la Directiva NIS per substituir la Directiva del 2016. Les noves normes garanteixen un nivell elevat i comú de ciberseguretat a tota la Unió, i responen a l'evolució del panorama de les amenaces tot tenint en compte la transformació digital, que s'ha vist accelerada per la pandèmia de la COVID-19.

La nova legislació de la UE defineix noves normes mínimes relatives a un marc regulador, estableix mecanismes per a una cooperació eficaç entre les autoritats competents de cada estat membre i actualitza la llista de sectors i activitats subjectes a les obligacions de ciberseguretat. La Directiva NIS 2 va entrar en vigor el 16 de gener de 2023.

3.1.8. Llei de Ciberseguretat de la UE

La Llei de Ciberseguretat reforça l'Agència de la UE per a la ciberseguretat (ENISA) i estableix un marc de certificació de la ciberseguretat per a productes i serveis. El 18 d'abril de 2023, la Comissió va proposar una modificació específica de la Llei de Ciberseguretat de la UE. L'esmena proposada permetrà l'adopció futura de sistemes de certificació europeus per a "serveis de seguretat gestionats" que cobreixin àrees com la resposta a incidents, proves de penetració, auditories de seguretat i consultoria. La certificació és clau per garantir un alt nivell de qualitat i confiança d'aquests serveis de ciberseguretat altament crítics i sensibles que ajuden les empreses i les organitzacions a prevenir, detectar, respondre o recuperar-se dels incidents.

3.1.9. Reglament de Ciberseguretat de la UE

El Reglament de Ciberseguretat de la UE, que va entrar en vigor el juny de 2019, va introduir un sistema de certificació per a tota la UE i un mandat nou i reforçat per a l'Agència de la UE per a la Ciberseguretat.

En el Reglament de Ciberseguretat de la UE es recull un sistema de certificació de la ciberseguretat a escala de la UE per combatre la ciberdelinqüència i, especialment, la protecció de les xarxes i sistemes d'informació. Aquesta certificació és fonamental a l'hora de garantir unes normes rigoroses en matèria de ciberseguretat per als productes, serveis i processos de TIC. És així perquè el fet que diferents països de la Unió recorrin actualment a diferents sistemes de certificació de la seguretat provoca una fragmentació del mercat i genera barreres reglamentàries.

3.1.10. Llei de Cibersolidaritat de la UE

El 18 d'abril de 2023, la Comissió Europea va proposar la Llei de Cibersolidaritat de la UE per millorar la preparació, detecció i resposta a incidents de ciberseguretat a tota la UE. Aquesta llei té com a objectiu enfortir les capacitats a la UE per detectar, preparar-se i respondre a les amenaces i atacs de ciberseguretat importants i a gran escala.

La proposta inclou un escut europeu de ciberseguretat, compost per centres d'operacions de seguretat interconnectats arreu de la UE, i un mecanisme d'emergència de ciberseguretat integral per millorar la postura cibernètica de la UE.

3.1.11. Certificació de ciberseguretat

La UE està treballant en un marc comú de certificació de ciberseguretat per a productes, serveis i processos digitals. Això ajudarà els consumidors i les empreses a identificar productes i serveis que compleixen certs estàndards de seguretat.

ENISA exercirà un paper clau en la creació i el manteniment del marc europeu de certificació de la ciberseguretat, i preparará el terreny tècnic per a sistemes de certificació específics. S'encarregarà d'informar el públic sobre els sistemes de certificació i els certificats emesos a través d'un lloc web específic.

3.1.12. Marc Europeu d'Habilitats en Ciberseguretat (ECSF)

La demanda creixent de professionals de la ciberseguretat a la UE, impulsada per requisits legals nous i una panorama d'amenaces en expansió constant, ha destacat la necessitat urgent de millorar i enfortir les habilitats en ciberseguretat. Tanmateix, l'oferta de professionals no ha aconseguit seguir el ritme d'aquesta demanda creixent, cosa que ha provocat una bretxa significativa a la força laboral en ciberseguretat. Per tant, és una eina essencial que recolza la identificació i articulació de tasques, competències, habilitats i coneixements associats amb les funcions dels professionals europeus de ciberseguretat. Serveix com a punt de referència de la UE per definir i avaluar habilitats rellevants, tal com es defineix a l'Acadèmia d'Habilitats de Ciberseguretat.

4. TENDÈNCIES DE LES CIBERAMENACES I ELS CIBERATACS A LA UE

Tal com hem esmentat, la quantitat i el tipus de ciberatacs estan augmentant a nivell mundial i a la UE. Segons l'informe d'ENISA 'Panorama de la ciberseguretat 2023 (juliol 2022-juny 2023)', en aquest període hi va haver un augment en la quantitat i varietat de ciberatacs com també les seves conseqüències. La guerra contra Ucraïna continua influint en aquest panorama i el hacktivisme s'ha estès amb l'aparició de grups nous. Igualment, els incidents de programaris de segrest van augmentar a la primera meitat del 2023 i no van mostrar signes de desacceleració.

En el cas específic de la UE, els estats membres van continuar estant afectats per la crisi geopolítica actual, amb un nombre creixent d'actors d'amenaces que adrecen els seus esforços contra organitzacions públiques i privades. Majoritàriament, són amenaces DDOS amb poc o cap impacte a la major part dels casos informats. Els atacs de programari de segrest també han augmentat a la UE. Igualment, es destaca la importància de mantenir la vigilància de cara a les següents eleccions europees el 2024.

Els sectors més afectats inclouen les administracions públiques, amb un 19 %, i l'àmbit de la salut, amb un 8 %. Tanmateix, a causa de les interdependències, és comú que s'observi un efecte cascada, on un sol esdeveniment impacta alhora diversos sectors. Un 6 % de tots els esdeveniments s'adrecen als sectors de fabricació, transport i finances.

El programari de segrest i els atacs DDoS continuen essent les dues amenaces principals per a la UE.

Dintre dels pronòstics plantejats i les amenaces emergents de ciberseguretat entre els períodes de 2023 a 2030, els que destaquen més són:

- Impactes geopolítics: Ciberconflicte entre Rússia i Ucraïna, ciberatacs destructius, nova onada de hacktivisme i desinformació com a estratègia militar.
- Actors d'amenaces a organismes estatals i no estatals: Explotació de la vulnerabilitat dia zero, model de pirateig com a servei, atacs de cadena de subministrament de TIC, adaptabilitat dels grups de programari de segrest.
- Programari maliciós com a servei: Atacs DDoS, pesca, evolució de l'extorsió amb dades, atacs massius sobre dispositius IoT.
- Amenaces híbrides i emergents: Compromís de dades delicades de persones i estats, ús de la IA amb hipertrucatges i desinformació, atacs a models de màquines d'aprenentatge i pesca per acceptació, accés i permisos a apps.
- Ciberoperacions: Objectius d'alt valor, infraestructures crítiques, grups estatals de ciberoperacions, participació de BigTech en ciberconflicte i explotació de vulnerabilitats al núvol.

5. CASOS RELLEVANTS DE CIBERATACS A LA UE

Tot seguit, presentem tres casos que considerem rellevants per a aquest document:

Estònia (2007)

- **Tècnica emprada:** DDoS**.**
- **Atacant:** desconegut (IP russes).
- **Descripció:** l'abril de 2007, Estònia va patir un atac de DDoS a gran escala contra serveis governamentals, institucions financeres i mitjans de comunicació. Xarxes de robots informàtics (*botnets*) van enviar quantitats massives de correu brossa i comandes automàtiques en línia per saturar els servidors.
- **Impacte i conseqüències:** negació generalitzada de serveis de les institucions estatals d'Estònia durant 22 dies. Les pàgines web de bancs, mitjans de premsa i organismes governamentals van col·lapsar a causa dels alts nivells de trànsit a Internet.
- **Altres dades d'interès:** el ciberatac va ser qualificat de la primera guerra de la xarxa. Va ser una represàlia russa per la decisió del Govern estonià de traslladar un monument en honor dels caiguts soviètics a la Segona Guerra Mundial cap a una plaça secundària de la capital, Tallin.

Diversos països (2008-2009)

- **Tècnica emprada:** programari maliciós.
- **Atacant:** desconegut.
- **Descripció:** Conficker és un programari maliciós de tipus cuc que afecta els ordinadors amb sistema operatiu Windows, i aprofita una vulnerabilitat detectada al servei de Windows Server. Una vegada infectat, un ordinador passa a formar part d'una xarxa de bots, que són controlats de manera remota per un node central.
- **Impacte i conseqüències:** a finals de l'any 2008 i durant tot el 2009, el virus aconsegueix infectar milions d'ordinadors de 190 països amb el sistema operatiu Microsoft Windows. Dos dels països afectats de la UE van ser el Regne Unit (hi va haver incidències en el funcionament d'alguns vaixells de la Marina britànica i al Parlament britànic) i França (es van haver de desactivar els avions de combat francesos). S'estima que Conficker va arribar a infectar fins a 15 milions d'ordinadors arreu de món i va produir danys valorats en 9.100 milions de dòlars.
- **Altres dades d'interès:** el Conficker s'ha fet servir principalment per robar la informació confidencial i fer campanyes de correu brossa des dels equips infectats. La primera versió del virus va ser detectada l'octubre de 2008 però ha patit diverses mutacions.

Diversos països (2009)

- **Tècnica emprada:** pesca (phishing).

- **Atacant:** desconegut (suposadament, d'origen xinès).

- **Descripció:** executats des de la Xina, els atacs es van iniciar a través de correus electrònics de suplantació de la identitat que contenien arxius adjunts maliciosos. Amb aquest atac APT (Amenaça persistent avançada) es van activar els micròfons i les càmeres d'ordinadors de la xarxa amb l'objectiu d'aconseguir informació classificada de caràcter polític, militar, diplomàtic i econòmic.

- **Impacte i conseqüències:** es van comprometre ordinadors a les ambaixades i organismes governamentals de 103 països. Es van descobrir sistemes compromesos a les ambaixades d'alguns països asiàtics (Índia, Corea del Sud, Taiwan, Tailàndia, Indonèsia i Pakistan) i europeus (Romania, Xipre, Malta, Portugal i Alemanya). No hi ha evidència que els sistemes informàtics de les oficines del govern dels Estats Units o del Regne Unit haguessin estat compromesos.

- **Altres dades d'interès:** és el primer cas internacional de ciberespionatge.

Ucraïna i altres països d'Europa (2022)

- **Tècnica emprada**: DDoS**.**

- **Atacant:** desconegut (atribuït a l'agència d'espionatge russa).

- **Descripció:** el 24 de febrer, el mateix dia que Rússia va envair Ucraïna, hi va haver un ciberatac l'objectiu del qual era el satèl·lit de comunicacions KA-SAT.

- **Impacte i conseqüències:** es va interrompre les comunicacions entre agències governamentals d'Ucraïna, a més d'afectar desenes de milers de clients d'Ucraïna i de tota Europa. Aquest ciberatac va deixar sense accés a Internet desenes de milers de persones arreu d'Europa, des de França fins a Ucraïna. Un mes després de l'atac, unes 2.000 turbines eòliques a Alemany encara no funcionaven.

- **Altres dades d'interès:** l'endemà del ciberatac, un post fronterer entre Ucraïna i Romania va ser atacat per un programa maliciós d'eliminació de dades que va alentir els tràmits de les persones refugiades que intentaven fugir del país.

6. CONCLUSIONS

Com hem vist al llarg de l'informe, la ciberseguretat a la UE és un tema crític que ha dut a la implementació de mesures significatives. Tanmateix, l'evolució constant de les amenaces cibernètiques requereix una vigilància contínua i l'adaptació de les estratègies per protegir de manera efectiva els ciutadans, empreses i institucions dels països membres.

La interdependència dels membres de la UE ha comportat un enfortiment del marc jurídic, normatiu i polític europeu. La UE ha implementat diverses iniciatives i regulacions destinades a millorar la ciberseguretat, cosa que es tradueix en canvis visibles pel que fa a actors, disseny i implementació de la política europea en aquest àmbit. Amb això, la UE pot donar resposta conjunta més eficient a les ciberamenaces que poden copejar indistintament i simultàniament tots els països europeus.

La ciberseguretat a nivell de la UE està vivint i viurà en els pròxims anys una expansió considerable en tots els àmbits; normatiu, polític, en termes d'actors i recursos. Aquesta tendència també s'està donant a nivell estatal i és molt important el rol de la UE de coordinar i de fomentar l'eficiència i l'eficàcia entre els seus membres.

La ciberseguretat, per tant, és un tema estratègic per a diferents actors de la societat, cosa per la qual es requereix una cooperació multinivell i entre actors públics i privats. Dintre dels actors destaca ENISA que, des del 2017, té un mandat permanent com a Agència per a la Ciberseguretat Europea. L'augment del pressupost i de la plantilla d'ENISA en els darrers anys confirma la tendència generalitzada en el si de la UE de destinar sempre més recursos financers i personals a la ciberseguretat europea.

Malgrat els avanços que ha donat la UE en temes de ciberseguretat, cal continuar enfortir-se'n, com ja s'ha esmentat, i cal mantenir la vigilància de cara a les pròximes eleccions europees del 2024.

7. 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.