ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ciberseguretat al sector financer

TLP:WHITE

ABRIL 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	19/04/2024	22/04/2024

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

Malgrat que la tecnologia aplicada a les finances ha generat oportunitats sense precedents, també ha comportat riscos sense precedents. La ciberseguretat en el sector financer és una preocupació crítica atès l'augment d'amenaces cibernètiques a nivell mundial en àmbits diferents. Els ciberdelinqüents han posat el punt de mira en aquest sector, sobretot arran de la digitalització dels serveis financers que estan experimentant tant les entitats com els usuaris. Com veurem més endavant, el sector financer abasta els subsectors següents: banca, asseguradores i borsa de valors.

El Fons Monetari Internacional (FMI) va emetre una advertència el 9 d'abril passat sobre l'alta exposició del sector financer a riscos de ciberseguretat. Segons l'informe, un de cada cinc incidents d'aquesta mena afecta entitats financeres, cosa que ressalta la importància d'abordar aquesta problemàtica.

Els ciberatacs poden tenir conseqüències devastadores com ara pèrdues financeres, robatori de dades delicades, dany a la reputació de la institució financera, degradació de serveis i violacions regulatòries. Igualment, un ciberatac a una institució financera podria desencadenar un incident capaç de desequilibrar el sistema financer i l'economia global.

Els actius digitals són al punt de mira dels ciberdelinqüents, que busquen explotar vulnerabilitats en sistemes i xarxes per obtenir-ne accés no autoritzat, robar-hi dades delicades o interrompre'n operacions comercials. Aquests ciberdelinqüents poden ser des de grups organitzats que busquen guanyar diners fins a grups amb motivacions polítiques.

En aquest informe explorarem els desafiaments de ciberseguretat als quals s'enfronta el sector financer, com també les estratègies i les pràctiques més bones que les institucions financeres poden implementar per mitigar aquests riscos. Analitzarem els tipus d'amenaces cibernètiques més comunes, com la pesca, el programari maliciós i el programari de segrest, com també les vulnerabilitats en aplicacions i sistemes. A més a més, examinarem la importància del compliment normatiu i la necessitat d'una cultura de seguretat cibernètica sòlida a tota l'organització.

En comprendre els desafiaments únics als quals s'enfronta el sector financer en matèria de ciberseguretat i en adoptar un enfocament proactiu per abordar aquests desafiaments, les institucions financeres poden protegir els seus actius digitals, mantenir la confiança del client i complir amb les regulacions de seguretat cibernètica en un entorn cada vegada més amenaçant i complex.

3. CIBERSEGURETAT I EL SECTOR FINANCER

Les institucions financeres emmagatzemen i gestionen una gran quantitat de dades confidencials, des d'informació personal i financera dels clients fins a dades relacionades amb transaccions comercials i actius.

3.1. Digitalització / revolució tecnològica del sector financer

La integració de la tecnologia en el sector financer ha revolucionat la manera com es duen a terme els processos de transacció i la prestació de serveis financers. Des de plataformes de comerç en línia fins a aplicacions bancàries mòbils, la innovació digital ha proporcionat un nivell de comoditat i accessibilitat mai vist. No obstant això, a causa d'aquests avenços sorgeixen amenaces noves que requereixen una vigilància constant. Els ciberatacs adreçats a institucions financeres estan en augment i els ciberdelinqüents fan servir tècniques cada vegada més sofisticades, inclòs l'ús de la intel·ligència artificial (IA) per superar les defenses de seguretat, tant tecnològiques com humanes.

Un dels desafiaments de la digitalització del sector financer és la seguretat i la privacitat. La digitalització augmenta l'exposició a amenaces cibernètiques i planteja desafiaments en termes de protecció de dades delicades i privacitat del client.

Per entendre a què fem referència quan parlem de la importància de la ciberseguretat en el sector financer, hem fet una subdivisió entre banca, asseguradores i bosses de valors.

3.1.1. Banca

L'ús de les tecnologies per dur a terme operacions i interactuar amb entitats bancàries està en augment constant. La digitalització de la banca s'ha accelerat arran de la pandèmia, principalment. I ha estat clau per resoldre els reptes del sector i millorar l'experiència d'usuari dels clients.

El sector bancari va ser uns dels objectius principals dels ciberdelinqüents el 2023. Els ciberatacs a bancs es basen en campanyes de programari maliciós impulsades per col·lectius de cibercriminals prorussos i estan adreçats a objectius de la Unió Europea (UE), com ara el Banc d'Inversions d'Europa o a entitats russes. El motiu d'aquests ciberatacs es basa en l'ajuda econòmica, logística i militar a Ucraïna per part de la UE. En concret, la situació d'aquests ciberatacs ha empitjorat a causa del conflicte entre Ucraïna i Rússia, segons l'informe *Threat Landscape Report* de S21sec.

A Espanya, malgrat l'increment dels ciberatacs, la majoria de la població manté la seva confiança en la seguretat de les institucions bancàries. Segons l'enquesta 'Ciberseguretat i hàbits d'ús de canals digitals', feta per Sigma Dos en col·laboració amb la CECA (Associació de caixes d'estalvis i bancs espanyols), sis de cada deu espanyols admeten tenir coneixements limitats o nuls sobre ciberseguretat. Malgrat aquesta manca de coneixement, quatre de cada deu ciutadans afirmen que fan servir la banca digital diàriament (41 %), mentre que el 88 % la fa servir almenys una vegada per setmana. Les operacions més freqüents són les consultes de saldo i moviments (35 %), les compres en línia (26 %) i els pagaments amb Bizum (21 %). Específicament, els joves de 18 a 20 anys són els que utilitzen més Bizum com a mètode de

pagament, cosa que suggereix un canvi en l'ús de les transferències. Per altra banda, fins als 45 anys, la compra en línia és l'operació més comuna, cosa que pot estar relacionada amb el nivell d'ingressos d'aquest grup demogràfic.

El repte principal al qual s'enfronten les entitats bancàries en termes de ciberseguretat no només radica en qüestions tecnològiques, sinó que els ciberdelinqüents exploten vulnerabilitats psicològiques, i s'aprofiten de l'engany i l'error humà. Per tant, és fonamental sensibilitzar i capacitar els ciutadans en matèria de ciberseguretat. Molts atacs tenen el seu origen en vectors difícils de contrarestar sense una comunicació sòlida i una educació efectiva en aquest camp, segons destaquen des de la CECA, cosa que planteja una preocupació seriosa per als bancs. Tot i que és encoratjador que els clients siguin conscients del risc, això per si sol no és suficient. A més a més, destaca l'augment continuat en la sofisticació de les amenaces, amb l'ús cada vegada més freqüent de l'enginyeria social, cosa que subratlla la necessitat d'una vigilància constant.

3.1.2. Asseguradores

A l'igual de la banca, les empreses asseguradores depenen en gran manera de les tecnologies de la informació per dur a terme les seves operacions diàries. La digitalització ha permès agilitar-ne els processos, millorar-ne l'eficiència i ampliar la capacitat d'arribar a un nombre més gran de clients. No obstant això, la integritat i la seguretat de la informació confidencial dels clients, com també la continuïtat de les operacions i la protecció dels sistemes, són elements fonamentals per a la reputació i l'èxit de les asseguradores.

Cal afegir també que, en els darrers anys, s'ha observat un increment marcat en el volum de primes en les assegurances ciber. Les empreses asseguradores han experimentat un creixement significatiu, i han arribat a augmentar en més del 50 % les seves primes l'últim any. Això reflecteix una preocupació més gran per la protecció contra les amenaces al sector.

3.1.3. Borsa de valors i fons d'inversió

La ciberseguretat al mercat de valors és molt important per la naturalesa crítica de la informació financera i comercial gestionada en aquest entorn. És molt important protegir les dades delicades, preservar la integritat del mercat, prevenir activitats fraudulentes, complir les regulacions i mantenir la confiança de l'inversor. Les institucions financeres, empreses cotitzades i els organismes reguladors han de col·laborar per mitigar els riscos cibernètics i protegir la seguretat i l'estabilitat del mercat de valors.

Per a la Comissió Nacional del Mercat de Valors (CNMV) és important analitzar l'impacte de la intel·ligència artificial i la ciberseguretat en els mercats de valors. Aquest organisme regulador ha assumit noves competències derivades de la normativa sobre criptoactius i sobre ciberseguretat, i ambdós temes estan com a prioritaris en el marc de l'actualització del seu pla d'activitats de 2024.

3.2. Amenaces cibernètiques: evolució, tendència i impacte

Tal com hem esmentat prèviament, les amenaces cibernètiques al sector financer han evolucionat significativament en els últims anys, impulsades per avenços tecnològics i canvis en el panorama de seguretat digital. La combinació de dades delicades, importància econòmica,

complexitat tecnològica, risc d'interrupció del servei i exigències regulatòries fan que el sector financer sigui especialment vulnerable als ciberatacs.

Les amenaces cibernètiques han experimentat una evolució constant en termes de la seva complexitat i sofisticació, cosa que presenta desafiaments significatius per al sector financer. Algunes tendències i aspectes importants a considerar inclouen:

- **Creixement exponencial dels atacs**: en els últims anys, hi ha hagut un augment exponencial de la quantitat i varietat d'atacs cibernètics adreçats al sector financer. Això, en part, és causa de l'augment de la digitalització al sector financer, cosa que amplia la superfície d'atac per als ciberdelinqüents.

- **Sofisticació de les amenaces:** els ciberdelinqüents han desenvolupat tècniques cada vegada més avançades per eludir les defenses de seguretat i comprometre els sistemes financers. Això inclou l'ús de programari maliciós altament sofisticat, atacs d'enginyeria social dirigits i tàctiques d'evasió de detecció.

- **Robatori de dades financeres:** un dels objectius principals dels atacs cibernètics en el sector financer és el robatori de dades financeres delicades, com ara números de targetes de crèdit, informació bancària personal i dades de comptes. Aquestes dades poden ser utilitzades per cometre fraus financers, robatori d'identitat i altres delictes financers.

- **Augment dels atacs de programari de segrest:** els atacs de programari de segrest, en els quals els ciberdelinqüents bloquegen l'accés als sistemes informàtics i exigeixen un rescat per restaurar-ne l'accés, han augmentat en freqüència i gravetat en el sector financer. Aquests atacs poden causar interrupcions significatives a les operacions i provocar pèrdues financeres substancials.

- **Atacs adreçats a la cadena de subministrament:** els ciberdelinqüents s'adrecen cada vegada més als proveïdors de serveis externs del sector financer, com ara empreses de tecnologia i proveïdors de programari, com un mitjà per comprometre les institucions financeres a través de la cadena de subministrament.

L'impacte d'aquestes amenaces cibernètiques en el sector financer pot ser devastador. A més de les pèrdues financeres directes, els atacs cibernètics poden causar danys a la reputació de la institució, pèrdua de confiança dels clients, sancions regulatòries i conseqüències legals. Per tant, és crucial que les institucions financeres estiguin a l'avantguarda de la ciberseguretat, i implementin mesures sòlides de protecció i resposta per mitigar aquests riscos.

Per fer front a aquestes amenaces, les institucions financeres estan invertint en tecnologies de seguretat avançades, com ara solucions de detecció d'amenaces en temps real, anàlisis de comportament d'usuaris, autenticació multifactor i capacitació en conscienciació sobre seguretat per a empleats i clients. A més, la col·laboració entre institucions financeres i organismes reguladors i agències d'aplicació de la llei és vital per abordar de manera efectiva les amenaces cibernètiques en el sector financer.

Últims esdeveniments i panorama actual

La guerra entre Rússia i Ucraïna, com també el conflicte Israel-Hamàs han tingut (i tenen) un impacte a països de l'OTAN, entre els quals hi ha diversos països d'Europa i els Estats Units. Els

ciberatacs estan molt vinculats a aquests conflictes i el sector financer no n'és aliè. En concret, el conflicte entre Rússia i Ucraïna està demostrant que les guerres també tenen lloc al ciberespai.

Més endavant veurem que els actors d'Amenaces persistents avançades (ATP) com KillNet, Anonymous Sudan, Bloodnet, NoName057(16), CyberArmy of Russia o Kvazar, han dut a terme ciberatacs importants.

3.3. Reptes i desafiaments de la ciberseguretat al sector financer

La digitalització creixent dels serveis financers ha expandit la superfície d'exposició, i ha proporcionat oportunitats més grans als ciberdelinqüents per explotar vulnerabilitats. A més a més, la sofisticació creixent d'aquests actors ha donat lloc a l'ús de tàctiques cada vegada més avançades per assolir les seves metes.

La manca de consciència en matèria de ciberseguretat i la inversió insuficient en aquest àmbit plantegen desafiaments considerables per a les institucions financeres.

Els atacs cibernètics adreçats a entitats financeres tenen repercussions significatives a diversos nivells:

- **Per als clients:** poden desencadenar pèrdues monetàries, robatori d'identitat i la interrupció dels serveis financers, tot generant inquietud i desconfiança.

- **Per a les institucions financeres:** aquests atacs poden ocasionar pèrdues econòmiques, danys a la reputació i la interrupció de les operacions, cosa que es tradueix en costos substancials.

- **A nivell econòmic:** els ciberatacs poden fomentar la incertesa i desconfiança en el sistema financer, cosa que podria impactar negativament en l'estabilitat econòmica.

Segons va indicar l'FMI recentment, la resistència cibernètica del sector financer s'ha de reforçar mitjançant una estratègia nacional de ciberseguretat adequada, marcs reguladors i de supervisió apropiats, recursos humans capacitats i acords nacionals i internacionals d'intercanvi d'informació. Igualment, esmenta que és molt important que les entitats financeres notifiquin els incidents a les agències supervisores.

Regulació i legislació a nivell nacional i internacional.

El compliment normatiu és un pilar del sector financer i opera dins d'una xarxa complexa de regulacions i requisits de compliment dissenyats per garantir l'estabilitat, protegir els consumidors i mantenir la confiança.

El **TIBER-EU**, acrònim de *Threat Intelligence-Based Ethical Red Teaming for the European Union Financial System* (proves ètiques basades en intel·ligència de ciberamenaces per al sistema financer de la Unió Europea), és un marc desenvolupat específicament per al sector financer a la Unió Europea. El seu objectiu principal és enfortir la ciberesiliència mitjançant la realització d'exercicis estructurats de Red Teaming.

El TIBER-EU es va presentar el 2018 i va esdevenir el primer marc europeu per a gestió i realització de proves avançades de ciberseguretat. En el seu cas, el Banc d'Espanya va aprovar i va adoptar localment la regulació TIBER-EU basada en l'estàndard europeu, i va aprovar la seva guia d'implementació el desembre de 2021.

Addicionalment, s'ha desenvolupat el **Reglament DORA** (Digital Operational Resilience Act) - Regulation (EU) 2022/2554 que prova de mesurar la resiliència operativa del sector financer. Està dissenyat per establir un marc únic que homogeneïtzi com han de gestionar les entitats financers el risc digital a les finances de la Unió Europea.

Tot i que DORA va entrar en vigor el gener del 2023, no s'espera que s'apliqui totalment fins al gener del 2025. Aquest marc exigeix dur a terme proves avançades sobre funcions crítiques, inclosos tercers, cada tres anys, i, tot i que el marc de referència encara no ha estat totalment desenvolupat, es farà en col·laboració amb el Banc Central Europeu, d'acord amb el marc TIBER-EU.

Per altra banda, l'*European Insurance and Occupational Pensions Authority* - EIOPA (Autoritat Europea d'Assegurances i Pensions de Jubilació) va definir la seva **estratègia per al període 2023-2026** centrada a reforçar la resistència i la sostenibilitat dels sectors de les assegurances i les pensions, i garantir una protecció sòlida dels interessos dels consumidors de la UE. Tot això sorgeix d'una situació de tensions geopolítiques per la invasió de Rússia a Ucraïna, unida als efectes persistents de la pandèmia, la volatilitat dels mercats i la inflació, cosa que subratlla la necessitat d'una supervisió eficaç.

Malgrat els avenços, d'acord amb una enquesta duta a terme per l'FMI entre bancs centrals i autoritats de supervisió, els marcs de polítiques de seguretat cibernètica, específicament en mercats emergents i economies en desenvolupament, solen estar mancats de solidesa. Per exemple, aproximadament només la meitat dels països enquestats disposaven d'una estratègia nacional de seguretat cibernètica focalitzada en el sector financer, o una regulació específica en matèria de seguretat cibernètica.

Com els atacs se solen originar més enllà de les fronteres del país on està ubicada la institució financera afectada i els beneficis es poden desviar fora del país, la cooperació internacional és imprescindible per abordar aquest tipus de riscos.

Comunitat, eficiència operativa i experiència de l'usuari

Quan es produeixin incidents cibernètics, el sector financer ha de ser capaç d'oferir serveis empresarials bàsics durant aquests períodes. A aquest efecte, les empreses financeres haurien de desenvolupar i posar a prova procediments de resposta i recuperació, i les autoritats nacionals haurien, per la seva banda, de disposar de protocols de resposta eficaços, com també marcs de gestió de crisis.

4. CIBERATACS AL SECTOR FINANCER

L'objectiu d'aquest apartat és conèixer en profunditat la tipologia d'atacs cibernètics que s'han executat contra aquest sector.

Per això descriurem quins són els mètodes que fan servir els atacants per aconseguir comprometre les xarxes i els sistemes de les entitats del sector financer, com també els tipus de programari maliciós més utilitzats.

Per últim, comentarem alguns dels ciberatacs més representatius ateses les conseqüències o importància que van tenir.

4.1. Vectors d'atac utilitzats

4.1.1. Correu electrònic

El correu electrònic és un dels mètodes més utilitzats pels atacants per aconseguir accedir i comprometre les xarxes de tota mena d'organitzacions, incloses les del sector financer.

Avui dia, el factor humà continua essent un dels punts febles de moltes empreses. Això fa que els atacs estiguin adreçats contra el seu personal, per fer-los servir com a porta d'entrada a la xarxa i els seus sistemes. Així, mitjançant el robatori de credencials poden, posteriorment, comprometre estacions de treball.

4.1.2. Xarxes de tecnologia de la informació (TI)

Les entitats del sector financer disposen d'una infraestructura TI. Aquesta està conformada per maquinari, programari, xarxes, servidors i instal·lacions. A més a més, també es podria diferenciar entre infraestructures de TI tradicionals i *cloud*.

Aquests xarxes TI juguen un paper clau en l'execució correcta de les funcions d'una organització, tant en els seus processos productius i de gestió interna, com en les seves tasques orientades a la relació amb proveïdors o clients finals.

Si un atacant aconsegueix accedir a la xarxa TI, pot obtenir una gran quantitat d'informació delicada i confidencial. Igualment, té la capacitat d'alterar o interrompre el seu funcionament i pot arribar a segrestar aquesta informació.

4.1.3. Proveïdors

Una altra de les portes d'entrada a la xarxa interna de les empreses que pertanyen al sector financer poden ser els proveïdors. En aquest punt és important tenir en compte el nivell de dependència de les empreses financeres en els proveïdors externs de serveis informàtics. Aquesta dependència està en augment, especialment si considerem el paper cada vegada més rellevant de la intel·ligència artificial. Si bé la contractació d'aquests proveïdors externs pot millorar la resiliència operativa, també exposa el sector financer a riscos que poden afectar tot el sistema.

Per exemple, el 2023, un incident de segrest de dades o programari de segrest contra un proveïdor de serveis informàtics al núvol va provocar la interrupció simultània dels serveis a 60 cooperatives de crèdit estatunidenques. Aquest incident ressalta com un sol esdeveniment pot tenir un impacte significatiu en múltiples entitats financeres, i subratlla la importància de gestionar adequadament els riscos associats amb la dependència de tercers proveïdors de serveis informàtics.

4.2. Tipologia de ciberatacs

Tot seguit, veurem quines són les tècniques i tipus d'atacs més comuns. Entre ells hi ha els atacs de programari maliciós, pesca, programari de segrest, etc.

4.2.1. Pesca (*phising*)

La suplantació d'identitat és una altra de les tècniques d'atac amb una prevalença més gran. Concretament, l'*spear-phising* o pesca dirigida, que és la modalitat de pesca que es caracteritza per adreçar-se a persones, organitzacions o empreses específiques, i el BEC (*Business Email Compromise),* són dues de les amenaces basades en pesca i enginyeria social a les quals les entitats cal que hi prestin una atenció més gran.

Els atacants fan servir correus electrònics falsos o enganyosos per ensarronar les persones i obtenir informació confidencial, com ara contrasenyes i números de targeta de crèdit. Aquesta tècnica permet obtenir credencials que possibiliten que els atacants accedeixin a les xarxes de les organitzacions, i permetin que posteriorment s'executin diferents tipus d'accions malicioses.

La conscienciació dels empleats sobre bones pràctiques i les mesures que es prenguin per tal que sàpiguen com actuar enfront d'aquesta manera d'amenaces, són la primera barrera per evitar problemes derivats d'aquesta tipus d'atacs.

4.2.2. Programari maliciós (*malware*)

Els programaris maliciosos poden infectar sistemes i dispositius per robar informació o permetre l'accés no autoritzat a sistemes financers.

4.2.3. Programari de segrest (*ransomware*)

Aquest tipus d'atacs tenen per objectiu xifrar els fitxers dels sistemes que compromet i això, alhora, pot tenir un impacte enorme a diferents nivells per a una organització perquè traspassen l'àmbit merament econòmic.

Els ciberdelinqüents xifren les dades i exigeixen un rescat per desbloquejar-les, cosa que pot paralitzar les operacions d'una institució financera. Els atacants busquen obtenir un rèdit en forma de rescat a canvi de desxifrar les dades.

A més a més, si l'empresa no ha xifrat i fet còpies de seguretat de tota aquesta informació, mitjançant els procediments adequats, un atac d'aquesta mena pot afectar la seva reputació i tenir conseqüències relacionades amb les regulacions competents i les lleis de protecció de dades.

4.2.4. Atacs DDoS

Els atacs de denegació de servei, coneguts comunament per les seves sigles en anglès DDoS, tenen per objectiu interrompre els serveis oferts per llocs web o qualsevol altra recurs de xarxa, i sobrecarreguen el seu tràfic.

4.2.5. Atacs a la infraestructura financera

Els atacs dirigits a la infraestructura financera, com ara els sistemes de pagament, poden tenir implicacions greus per al funcionament del sistema financer.

4.2.6. Notícies enganyoses (*fake news*)

Els ciberdelinqüents poden intentar manipular els mercats financers mitjançant la difusió d'informació falsa o l'execució d'operacions fraudulentes.

4.3. Casos rellevants

Tot seguit, esmentem tres casos de ciberatacs al sector financer que considerem rellevants.

Fons Monetari Internacional (2024)

Qualsevol organisme internacional està constantment en el punt de mira dels ciberdelinqüents. El Fons Monetari Internacional (FMI) va detectar un ciberatac el 16 de febrer passat, que va ser dirigit a 11 dels seus comptes de correu electrònic, segons va informar l'entitat en un comunitat.

Aquest incident ha posat en perill la fortalesa del programa de ciberseguretat de l'FMI, una entitat que ha alertat en moltes ocasions sobre els riscos que suposen els atacs cibernètics per al sistema financer global. El descobriment d'aquest atac suscita preguntes crucials sobre la seguretat de la informació a les institucions financeres internacionals i sobre les mesures que calen per salvaguardar els secrets econòmics de les nacions.

Cal destacar que, el 2011, l'FMI també va ser víctima d'un ciberatac que va comprometre el seu sistema de seguretat informàtica. Tot i que els detalls específics sobre l'extensió del dany o la quantitat d'informació compromesa es van mantenir en gran manera sota confidencialitat, l'atac va ser significatiu per l'alt perfil de la institució i les seves implicacions pe a la seguretat financera global. Es va especular que el ciberatac podria haver estat una operació d'espionatge destinada a accedir a dades econòmiques delicades o influir en les decisions financeres a nivell mundial.

Banc Europeu d'Inversions (2023)

El 19 de juny el Banc Europeu d'Inversions (EIB), banc de desenvolupament de la Unió Europea i propietat dels estats membres, va ser víctima d'un ciberatac quan els pirates informàtics es van infiltrar amb èxit en els sistemes de l'entitat.

L'EIB va recórrer a Twitter per confirmar el ciberatac en curs i va revelar que els llocs web de l'empresa, eig.org i eif.org, havien experimentat problemes greus de disponibilitat. L'atac va deixar completament inaccessible el lloc web del banc, mentre que el Fons Europeu d'Inversions, que és responsable d'ajudar les petites i mitjanes empreses amb l'accessibilitat financera, per romandre funcional, però va mostrar alteracions notables.

Aquest ciberatac va ser propiciat per KillNet i Anonymous Sudan, i va coincidir amb amenaces de pirates informàtics russos els dies previs, com Anonymous Sudan i REvil, que indicaven les seves intencions de desestabilitzar els mercats financers occidentals.

Bancs i altres entitats d'Espanya (2023)

El juliol de 2023 entitats financeres i d'altres sectors a Espanya (Caixabank, Bankinter, Caja Rural, Abanca, Transports de Barcelona, Metro de Madrid i Puertos del Estado) van rebre atacs informàtics, tot coincidint amb les eleccions generals del 23J (23 de juliol). Aquests atacs de DDoS es van atribuir als actors d'amenaça russos Killnet, Anonymous Sudan, Anonymous Russia i NoName057.

Banc d'Espanya (2018)

El Banc d'Espanya va patir un atac DDoS, que va impedir l'accés a la seva pàgina web des de servidors externs, tot i que no va tenir més conseqüències com ara robatori d'informació. El compte de Twitter Anonymous Catalonia va publicar un missatge a través del qual informaven que la pàgina web del Banc d'Espanya havia caigut, amb els hashtag #OpCatalonia, que s'havia fet servir en ocasions anteriors en què s'havien perpetrat ciberatacs en aquesta línia.

5. ACTORS D'AMENAÇA

Els APT, que són les sigles d'Amenaça persistent avançada, en català, són grups organitzats de cibercriminals que generalment actuen contra corporacions per considerar que són objectius molt més interessants i lucratius. Les APT consten de certa complexitat a les seves operacions i accions, per això es troben entre els tipus de ciberatacs més perillosos en el sector financer.

Blind Eagle o APT-C-36

Des de l'abril de 2018, el grup delictiu conegut com a Blind Eagle o APT-C-36, i d'origen presumptament sud-americà, és sospitós de dur a terme atacs continuats dirigits contra institucions del sector financer, com també d'altres sectors de països com ara Equador, Xile, Espanya, Panamà, Mèxic, entre d'altres. Se sospita que Blind Eagle és un grup de parla hispana atès l'ús de l'idioma en els seus correus electrònics de pesca. Tanmateix, actualment no està clar on està ubicat el grup delictiu i si els seus atacs estan motivats per espionatge o per guanys financers.

NoName057(16)

El 10 de gener de 2023, el Banc Central de Dinamarca i set bancs del país es van veure afectats per un atac de denegació de servei distribuït (DDoS), que va ser reivindicat pel grup hacktivista prorús NoName057(16). L'impacte es va limitar als llocs web i no va afectar altres sistemes ni a les operacions diàries. L'atac DDoS va afectar primer el lloc web de Bankdata, una empresa TI que ofereix solucions per al sector financer, i posteriorment va provocar restriccions breus a l'accés als llocs web de set bancs privats (Danske Bank, Jyske Bank, Sydbank, Sparekassen Sjælland-Fyn, BankInvest, Arbejdernes Landsbank i Svenska Handelsbanken AB).

A més de les institucions financeres daneses, l'11 de gener del mateix any NoName057 es va atribuir el ciberatac al Ministeri de Finances de Dinamarca, que es va estendre fins a almenys el 13 de gener, segons va publicar aquest actor d'amenaça.

El juliol de 2023, NoName057(16) va dur a terme una onada d'atacs de denegació de servei distribuït (DDoS) contra entitats financeres espanyoles com ara Bankinter, Abanca, Grupo Caja Rural, Banco Cooperativo Español, Triodos Bank i Banco Mediolanum. Igualment, van atacar entitats governamentals i empreses de telecomunicacions d'Espanya. En grau més baix, s'han dirigit a organitzacions espanyoles d'altres sectors.

Els atacs van començar just abans de les eleccions nacionals espanyoles del juliol de 2023. La motivació per atacar les institucions i empreses espanyoles és el subministrament d'armes a Ucraïna per lluitar a la guerra contra Rússia.

Com hem esmentat prèviament, altres actors d'amenaça que han dut a terme ciberatacs a entitats financeres són **Killnet**, **Anonymus Sudan**, **Bloodnet**, **CyberArmy of Russia** i **Kazar**.

6. RECOMANACIONS

És innegable que el sector financer està a l'avantguarda d'una batalla silenciosa i continua contra les amenaces cibernètiques. Per augmentar la seva resiliència, les autoritats haurien de desenvolupar una estratègia nacional de seguretat cibernètica adequada. Algunes de les accions que s'haurien de dur a terme són:

- Fer de manera periòdica valoracions del panorama de la ciberseguretat i identificar riscos potencials, inclosa l'**anàlisi a proveïdors de serveis**.
- Fomentar la maduresa cibernètica entre les empreses del sector financer, inclòs l'accés al coneixement expert en matèria de seguretat cibernètica a nivell de consell d'administració i una **governança** més bona en temes de ciberseguretat.
- A les empreses, millorar la seva **seguretat en línia i la salut dels seus sistemes** (per exemple, amb solucions anti programari maliciós i autenticació multifactorial), com també la capacitació i la sensibilització.
- Prioritzar la compilació i publicació de dades sobre incidents cibernètics i que la informació es comparteixi entre els participants en el sector financer per millorar la seva preparació col·lectiva davant de possibles eventualitats.

Com ja hem esmentat, cal la cooperació internacional per abordar amb èxit la qüestió del risc cibernètic perquè és usual que aquests ciberatacs traspassin les fronteres.

Igualment, les entitats financeres haurien d'implantar una sèrie de mesures internes, com ara:

- Implementar mesures de seguretat avançades, com ara **tallafocs** (*firewalls)*, **xifratge i doble factor d'autenticació**, per protegir les dades i les transaccions.
- Dur a terme una vigilància continuada de l'activitat sospitosa per tal de detectar i respondre ràpidament als ciberatacs.
- Conscienciar i capacitar els treballadors i clients per prevenir ciberatacs d'enginyeria social com la pesca.
- Col·laborar amb organismes reguladors i de seguretat cibernètica per desenvolupar i aplicar normatives que enforteixi la protecció contra ciberatacs.

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.