AGOST DE 2018

INFORME D'APROFUNDIMENT DE L'ECONOMIA METROPOLITANA

TROP

APROFUNDIMENT

CIBERSEGURETAT: TENDÈNCIES EN SEGURETAT

TENDÈNCIES, REPTES, OPORTUNITATS I POSICIONAMENT

Institut Cerdà

AMB Desenvolupament Social i Econòmic

ÍNDEX

PRESENTACIÓ DE LA MONOGRAFIA

L'arribada d'internet en el dia a dia de les llars, les empreses i l'administració ha revolucionat la manera de comunicar-nos i de fer negocis. La societat del segle XXI funciona digitalment en l'accés a la informació, la gestió empresarial, les relacions econòmiques, personals i fins i tot la infraestructura de les ciutats (*smart*). I en els darrers anys hi hem afegit la ubiqüitat, la mobilitat, la Internet de les coses, les comunicacions de màquina a màquina o el *big data*, amb el processament de dades desestructurades en temps real.

Al mateix temps, en els últims anys han crescut els riscos relacionats amb les noves tecnologies. La filtració d'informació diplomàtica (amb casos com Wikileaks, Anonymous o Edward Snowden), així com els freqüents ciberatacs per part d'associacions cada cop més organitzades, han posat de manifest fins on poden arribar les amenaces en seguretat, despertant la consciència d'una part significativa de la societat.

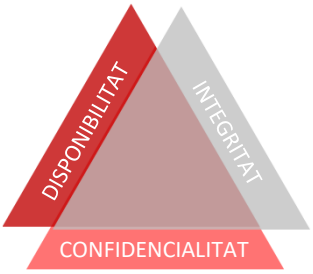
La ciberseguretat ja és a l'agenda dels líders públics i empresarials mundials, cridant l'atenció del World Economic Forum o de la Unió Europea. Es tracta d'una situació complexa, en la que el nombre i la varietat de ciberamenaces és cada cop més elevat.

Aquest informe té com a objectiu definir el concepte i l'abast de la ciberseguretat i identificar els reptes fonamentals als que ha de donar resposta, especialment en relació amb l'activitat econòmica.

DEFINICIÓ

La ciberseguretat és un concepte d'actualitat que fa referència a la seguretat en el món digital. El Consell de la Unió Europea, la defineix com "totes aquelles activitats necessàries per protegir la xarxa i els sistemes d'informació, els seus usuaris, i les persones afectades per les amenaces cibernètiques" [1]. Es tracta d'un concepte complex, que va més enllà de la tecnologia i que, per tant, ha de ser abordat des d'una òptica multidisciplinària que tingui en compte l'afectació a institucions, empreses i ciutadans.

Protegir la informació vol dir protegir les seves tres propietats principals:

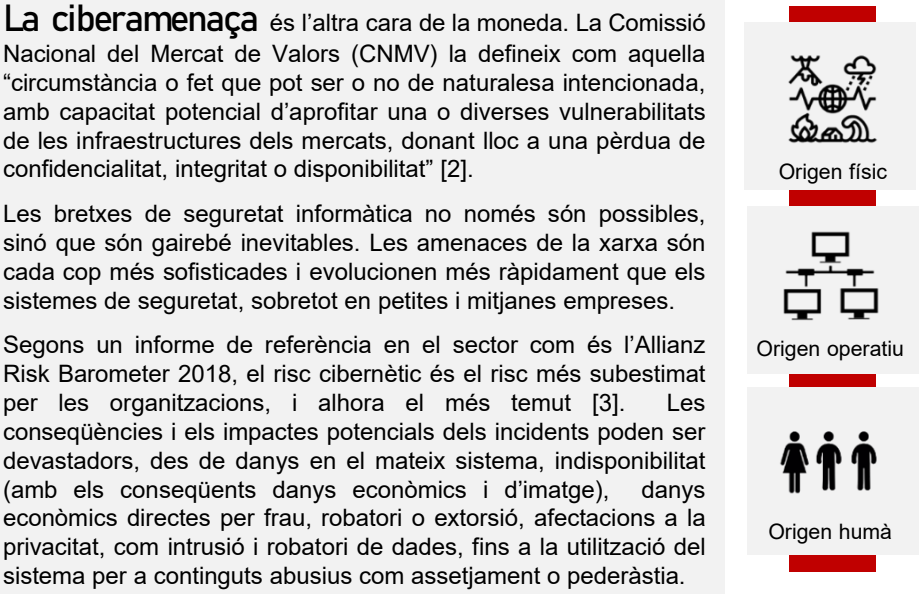


- **DISPONIBILITAT:** La informació ha d'estar sempre accessible pels usuaris que estiguin autoritzats durant un límit de temps raonable
- **INTEGRITAT:** La informació ha de romandre correcta (integritat de dades) i tal com l'emissor la va originar (integritat de font), sense manipulacions per part de tercers
- **CONFIDENCIALITAT:** La informació només ha de ser accessible o divulgada a aquells usuaris que hi estan autoritzats.

La ciberamenaça és l'altra cara de la moneda. La Comissió Nacional del Mercat de Valors (CNMV) la defineix com aquella "circumstància o fet que pot ser o no de naturalesa intencionada, amb capacitat potencial d'aprofitar una o diverses vulnerabilitats de les infraestructures dels mercats, donant lloc a una pèrdua de confidencialitat, integritat o disponibilitat" [2].

Les bretxes de seguretat informàtica no només són possibles, sinó que són gairebé inevitables. Les amenaces de la xarxa són cada cop més sofisticades i evolucionen més ràpidament que els sistemes de seguretat, sobretot en petites i mitjanes empreses.

Segons un informe de referència en el sector com és l'Allianz Risk Barometer 2018, el risc cibernètic és el risc més subestimat per les organitzacions, i alhora el més temut [3]. Les conseqüències i els impactes potencials dels incidents poden ser devastadors, des de danys en el mateix sistema, indisponibilitat (amb els conseqüents danys econòmics i d'imatge), danys econòmics directes per frau, robatori o extorsió, afectacions a la privacitat, com intrusió i robatori de dades, fins a la utilització del sistema per a continguts abusius com assetjament o pederàstia.



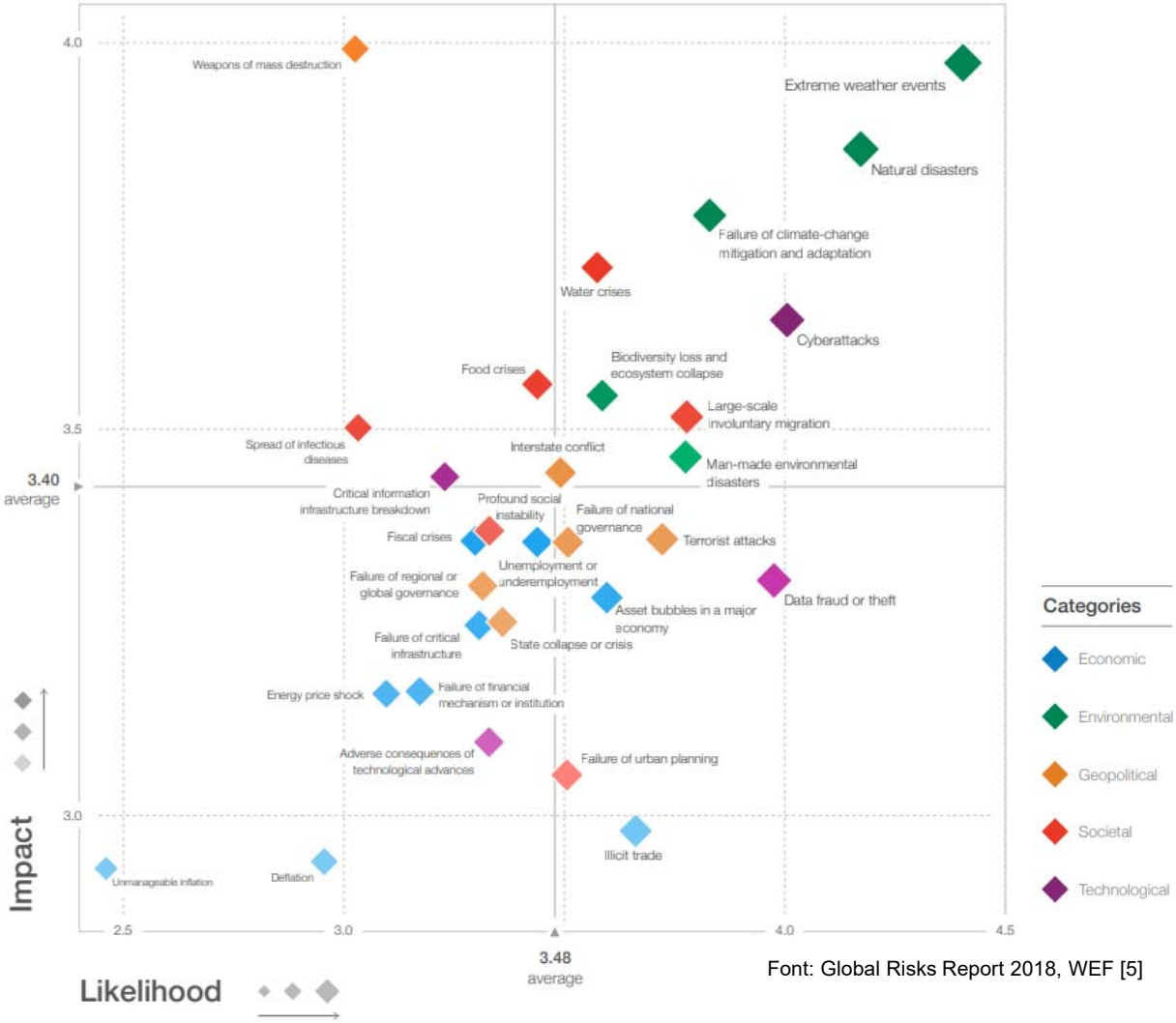
La ciberseguretat, el risc més temut al món per les organitzacions a llarg termini [3].

de les grans organitzacions

afirmen havent patit una bretxa de seguretat en l'últim any [4].

de les PiMEs

Segons l'últim informe anual del World Economic Forum (WEF), publicat el passat mes de gener 2018, els ciberatacs i el frau/robatori de dades són situacions d'alta preocupació per als agents del territori, pel seu impacte i per la seva probabilitat de que passin.



Font: Global Risks Report 2018, WEF [5]

El cost global mitjà mundial dels ciberatacs s'ha incrementat un 27,4% entre 2013 i 2017. El seu import s'estima en 11,7M$ en companyies en els sectors amb més amenaces segons Accenture, després d'haver entrevistat 254 organitzacions.

El cost del cibercrim a les organitzacions en els pròxims anys s'estima en 8 bilions de $.

Font: Accenture [12]

La ciberseguretat al territori

Amb l'objectiu de garantir la ciberseguretat a la xarxa, la Unió Europea va publicar el febrer de 2013 "l'Estratègia de Ciberseguretat de la UE", senyalant cinc eixos prioritaris.

1. Aconseguir la ciberresiliència
2. Reduir la ciberdelinqüència
3. Desenvolupar capacitats de ciberdefensa
4. Desenvolupar recursos industrials i tecnològics de ciberseguretat
5. Establir una política internacional coherent de ciberespai a la UE, promovent els valors essencials de la Unió.

L'estratègia es complementa amb diferents mesures, entre les quals destaquen el RGPD i la Directiva 2016/1148, sobre ciberseguretat. Aquesta última, defineix els mecanismes de cooperació i requisits comuns de seguretat per als operadors de serveis essencials i els digitals. El text estableix l'obligació als Estats Membres d'elaborar una estratègia nacional de seguretat a les xarxes, crear una xarxa d'equips de resposta a incidents de seguretat informàtica i establir requisits en matèria de seguretat i notificació per als operadors de serveis essencials i els proveïdors de serveis digitals [6].

El Reglament General de Protecció de Dades de la Unió Europea (RGPD)

Estableix les normes relatives a la protecció de les persones físiques pel que fa al tractament de les dades personals i les normes relatives a la lliure circulació d'aquestes, garantint una homogeneïtat legislativa absoluta per a totes les empreses que operen a la UE, amb independència de la seva seu.

El Reglament, que va entrar en vigor el 25 de maig de 2018, preveu multes econòmiques importants per atac si no es pot demostrar l'aplicació de mesures adients de protecció i la notificació quasi immediata a afectats.

Atès el caràcter dinàmic del risc a la xarxa, la Comissió ha demanat aquest últim any, enfortir l'actual agència de seguretat de la UE (ENISA) i la introducció d'un règim de certificació de la ciberseguretat de caràcter comunitari [7].

En l'àmbit estatal, l'Estratègia de Ciberseguretat Nacional, aprovada pel Consell de Seguretat Nacional el desembre de 2013 és el marc regulador de la seguretat a la xarxa. Els objectius es desenvolupen anualment a l'Estratègia de Seguretat Nacional [8]. Destaca com a organisme el paper de l'Institut de Ciberseguretat (INCIBE), depenent del Ministeri d'Economia i Empresa, que neix amb l'objectiu de reforçar la ciberseguretat, la confiança i la protecció de la informació i privacitat de la societat de la informació; i el CERT, depenent d'INCIBE, el centre de resposta a incidents.

A Catalunya, el CESICAT és l'organisme encarregat des de 2010 de garantir la protecció, prevenció i governança en matèria de ciberseguretat de la Generalitat de Catalunya i el seu govern. L'entitat és responsable de l'establiment i el seguiment dels programes d'actuació en matèria de ciberseguretat, les activitats de protecció i prevenció de l'administració, el centre de resposta a incidents i el programa de sensibilització i conscienciació al territori.

La creació de l'Agència de Ciberseguretat de Catalunya a l'Hospitalet de Llobregat, aprovada pel Parlament el 2017 en substitució del CESICAT amb l'objectiu d'alinear-se amb la nova Directiva de la UE, va ser suspesa cautelarment pel TC el passat desembre en admetre a tràmit el recurs del govern espanyol d'invasió de competències.

Amenaces similars a l'Estat amb particularitats pròpies... [9]

- Creixement de l'espionatge empresarial
- Més atacs per motius ideològics

La ciberseguretat a Catalunya [10]

- REPRESENTA 0,36% DEL PIB CATALÀ
- EMPLEA 5.898 TREBALLADORS
- INCLOU 352 EMPRESES,
- EL 95% DE LES QUALS SÓN PIMEs
- I EL 38% TÉ MENYS DE 10 ANYS

Sistemes d'informació

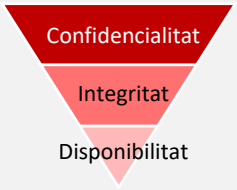
Empreses, organitzacions i administració fan ús actualment de diferents sistemes i dispositius en el seu dia a dia: ERPs, CRMs, *cloud*, *smartphones*, *tablets* o fins i tot aplicatius desenvolupats internament. A continuació es presenten els dos principals sistemes d'informació i els atributs per garantir-ne la seguretat [11].

Information Technology (IT)

La IT abasta el *hardware*, el *software* i les xarxes usades per emmagatzemar, recuperar, transmetre i manipular dades.

L'objectiu de l'amenaça és el contingut.

Pel tipus d'informació que utilitzen els sistemes d'IT, la confidencialitat és de màxima importància, seguida de la seva integritat i que sigui accessible en un període raonable de temps.



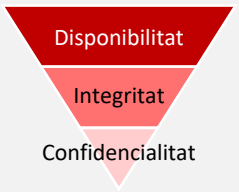
Exemple: breu interrupció del correu electrònic

Operational Technology (OT)

Fa referència a la part més "industrial", tot aquell *hardware* o *software* dedicat a monitoritzar, controlar i alterar l'estat físic d'un sistema.

L'objectiu de l'amenaça són les operacions.

En aquest cas, la capacitat de disposar de forma immediata de la informació prima per sobre de la resta de característiques, donat que els sistemes de control requereixen d'aquesta immediatesa.



Exemple: interrupció dels sensors en una línia de producció

Els atacs, cada cop més severs...

Com hem vist, les característiques d'accés a la informació pel que fa a la seguretat s'inverteixen segons parlem d'IT o OT, imposant un tractament diferenciat en cada cas. Esdevé necessari aplicar diferents mesures i establir diferents responsables segons el tipus d'informació, redundant en una major complexitat de la gestió dels sistemes i eventualment, incrementant-ne la vulnerabilitat.

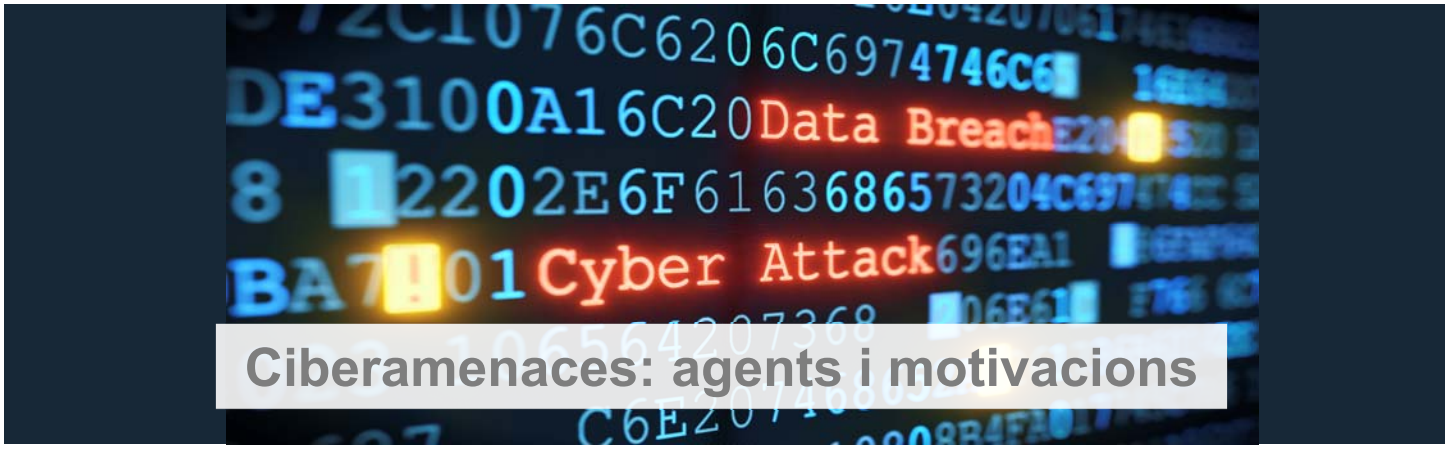
La sofisticació de les amenaces ha augmentat amb el temps, però també ho ha fet el nombre de ciberatacs, principalment per tres motius:

1. Els individus tenen cada cop més capacitat per perpetrar ciberatacs.
2. Amb l'IoT, els potencials objectius són cada cop més ubicus.
3. La creixent interconnectivitat de dispositius mitjançant la xarxa fa que atacs simples siguin més fàcils d'articular i puguin causar més danys.

La ciberdelinqüència costa a l'economia mundial entorn de 445.000 milions de dòlars a l'any, dels quals la meitat recau en les deu principals economies mundials [10]

La detecció i la recuperació suposen el 55% del cost intern de ciberseguretat l'any 2017 [12]

La interrupció de negoci (33%) i la pèrdua d'informació (43%) són les amenaces més costoses [12]



Ciberamenaces: agents i motivacions

CIBERCRIM

Es tracta de la principal amenaça a la xarxa. Els ciberciminals tenen com a objectiu robar informació personal o realitzar activitats fraudulentes. Les seves motivacions són principalment econòmiques.

CIBERESPIONATGE

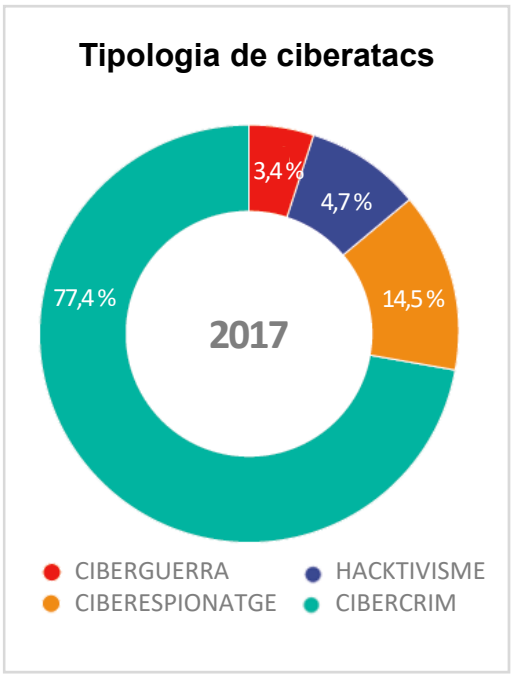
El ciberespionatge és la segona amenaça més comuna a la xarxa. Està dirigida a obtenir dades sensibles dels sistemes d'informació principalment de corporacions o a administracions.

HACKTIVISME

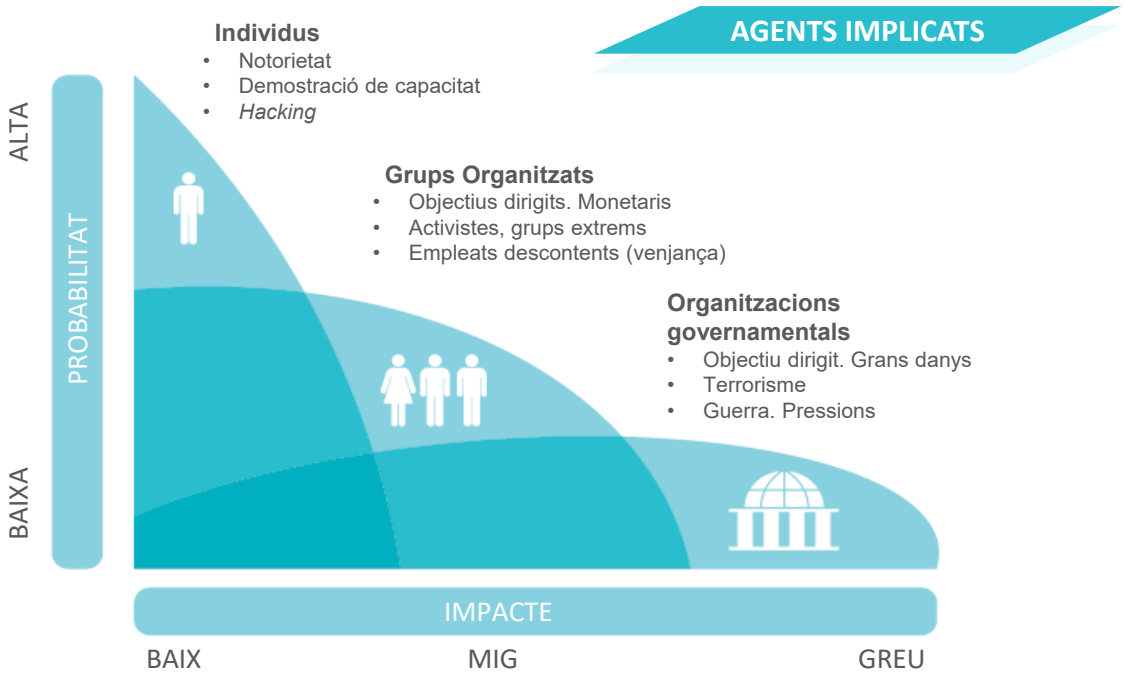
Procedeix de la contracció de "hacker" i "activisme". Inclou la defensa d'ideals polítics o socials mitjançant accions a la xarxa generalment no violentes, però il·legals.

CIBERGUERRA

Els efectes d'aquests atacs tenen com a particularitat abastar tots els agents d'un mateix territori, tot i no estar connectats a la xarxa.



Font: realització pròpia a partir de [13]



Font: Adaptació de [14]

Ciberamenaces més utilitzades

Els tipus d'atac utilitzats pels cibercriminals han evolucionat amb els anys, esdevenint cada cop més sofisticats i majors en nombre. A continuació, es mostren les ciberamenaces més representatives dels últims anys [11]...

1998
Apareix el primer virus informàtic de la història: Morris Worm (malware)

2004
Codi maliciós, troians, cucs avançats

2007
Robatori d'identitat, Phishing

2010
Atac DoS, auge de Botnets, atacs SQL, webs anti-spam

2013
Enginyeria social, Botnets, DDos, emails maliciosos, ransomware, PoS

Present
Malware bancari, Keylogger, lladres de Bitcoins, robatori d'identitat, segrest de mòbils, ransomware, PoS, cibreguerra ...

PHISHING consisteix a suplantar la identitat d'un servei o organització per obtenir dades d'usuaris. Mitjançant algun mètode de comunicació, com pot ser un correu electrònic, el cibercriminal es posa en contacte amb la víctima fent-se passar per una persona o empresa de confiança, requerint-li algun tipus d'informació com contrasenyes, número de compte, etc.

MALWARE, també conegut com a *software* maliciós o virus informàtic. Té com a objectiu danyar un sistema informàtic o infiltrar-s'hi sense el consentiment del seu propietari. És l'atac més freqüent i més costós mundialment [12].

Atac DoS (o de denegació de servei), consisteix a atacar un servidor des d'un sol ordinador. La conseqüència és el bloqueig del servidor.

Quan l'atac s'efectua des d'una xarxa de dispositius o *botnets* al mateix temps, es fa referència a un atac **DDoS**.

Atac SQL consisteix a introduir un codi intrús en una base de dades per accedir a la informació que conté. Es val d'una vulnerabilitat informàtica de la programació (SQL en aquest cas) que estigui incrustat dins d'un altre.

PoS malware (Punt de venda) expressament dissenyat per robar dades bancàries de clients de botigues al detall. El més habitual és sostreure informació de targetes bancàries, llegint la memòria del dispositiu des del qual es realitza el pagament en el punt de venda.

RANSOMWARE és un tipus d'atac informàtic que consisteix a restringir l'accés a contingut crític d'una empresa o un particular i demanar un rescat a canvi de llevar aquesta restricció.

L'any passat (2017), el **ransomware *WannaCry*** va provocar un dels ciberatacs més grans i coneguts fins al moment. Segons l'Europol, va afectar més de 560.000 usuaris, la majoria empreses, a més de 150 països. A Espanya, es calcula que van ser infectats més de 1.200 ordinadors [15]. Davant la notorietat de l'atac, moltes empreses van tallar les seves comunicacions, aturar la seva activitat i enviar els seus treballadors a casa per por d'infectar-se.

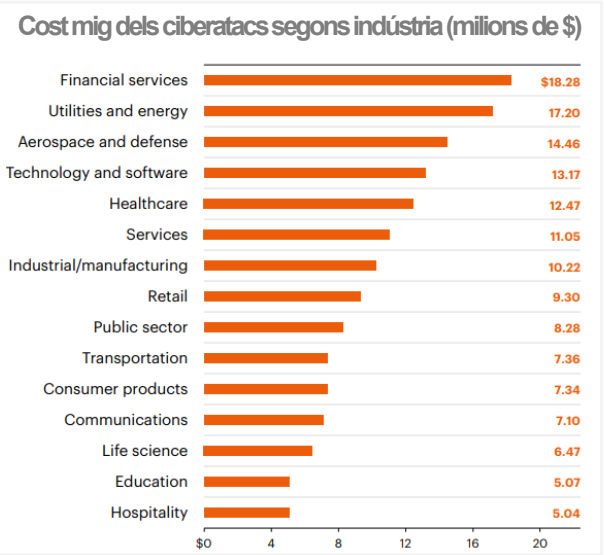
L'atac es va produir de manera aleatòria i no dirigida als sistemes operatius de Microsoft, aprofitant-se d'una vulnerabilitat en el mateix. El *software* maliciós restringia l'accés als ordinadors infectats, segrestant-ne les dades, xifrant-les i exigint un rescat (300$ en *bitcoins*) per lliurar la contrasenya. Un analista britànic de 22 anys va trobar finalment la forma de detenir l'atac.

Reptes en ciberseguretat

1 Menys del 10% de les empreses subscriuen pòlisses contra riscos cibernètics

Després de comparar el cost mitjà de la delinqüència cibernètica en 15 sectors diferents, les empreses que ofereixen serveis financers i serveis públics i energia són les que han tingut un cost més elevat, amb 18 i 17 milions de $ respectivament l'any 2016 [12].

Els riscos cibernètics representen una amenaça cada vegada més gran per a les empreses, i les asseguradores han detectat una creixent demanda dels seus serveis. ACGS preveu que les primes d'assegurances cibernètiques augmentin en l'àmbit mundial un 20% anualment, passant dels 2.000M$ anuals a més de 20.000M$ en la pròxima dècada [10].



Font: Accenture (base 254 companyies) [16]

2 Manca de perfils digitals

La falta de professionals especialitzats en ciberseguretat és un dels principals reptes a què s'enfronta el món en l'actualitat. El 71% de les empreses ja assegura haver patit danys directes i mesurables per la manca de competències en ciberseguretat [17].

L'increment de les amenaces a la xarxa, la creixent exposició tecnològica i l'establiment d'un règim de sancions a curt termini que ha començat a sonar amb força aquest últim any, compel·len a empreses i organitzacions no només a formar als seus treballadors en prevenció de riscos digitals, sinó a comptar amb personal especialitzat i qualificat en ciberseguretat. En són clars exemples:

- L'entrada del RGPD, que preveu sancions econòmiques importants si no es demostren mesures adients de protecció i introdueix com a requeriment la figura del responsable de protecció de dades (DPO) per a empreses de més de 250 treballadors.
- La recent directiva europea de ciberseguretat, que haurà de ser transposada a Espanya pròximament, que preveu multes per a operadors de serveis essencials que no compleixin certs requisits de seguretat o no comuniquin els incidents.

No obstant, en l'actualitat, el sector públic i privat admeten la dificultat en identificar aquest tipus de talent a Europa, on els plans nacionals encara no inclouen la ciberseguretat en la formació secundària, professional o universitària. Es tracta d'un sector poc madur que trigarà a aconseguir equilibrar l'oferta i la demanda de llocs de treball, si les administracions no desenvolupen accions específiques

Segons ISC, l'any 2022 es necessitaran 2 milions de professionals en ciberseguretat al món. En l'actualitat, la majoria de països no compten amb treballadors amb formació suficient [10]

Perfils més demandats [10]

- **Enginyeria tècnica de seguretat** garanteixen la seguretat de la informació (SI)
- **Chief Information Security Officer,** com a responsable de SI
- **Auditoria de ciberseguretat o hacker ètic**, posen a prova i detecten vulnerabilitats als sistemes informàtics
- **Gerència de Seguretat Lògica**, responsables d'accessos a programes o bases de dades.
- Data Protection Officer (DPO)

Reptes en ciberseguretat

3 La llibertat a la xarxa

El disseny d'internet ha fet que sigui possible que organitzacions i comunitats d'usuaris amb prou coneixements construeixin eines que utilitzin Internet de maneres noves i innovadores, i fins i tot infraestructures addicionals que garanteixin la privadesa i l'anonimat.

Es creen així diferents nivells a la xarxa... [18]

Es tracta de la ***internet en superfície***, tal com la coneixem. Pàgines accessibles mitjançant buscadors. Representaria tan sols un 4% del món web

Deep web

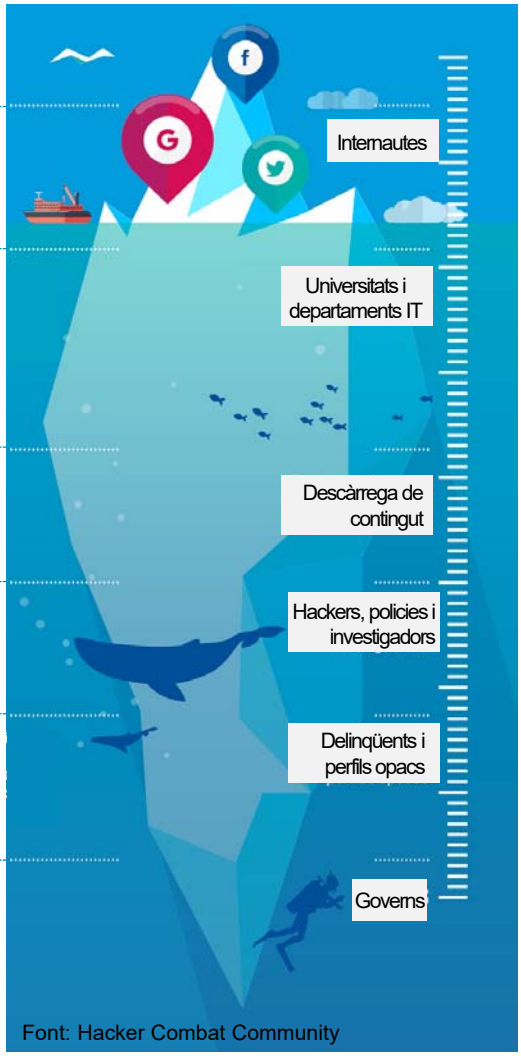
Michael Bergman és el primer a referir-se a aquest concepte l'any 2001, referint-se a la internet invisible, no accessible mitjançant buscadors. Representaria entre el 90 i el 95% del contingut de la xarxa, l'encarnació de la llibertat en el seu màxim exponent.

El nivell 2 inclouria pàgines no indexades (és a dir visibles) o eliminades de motors de cerca; el nivell 3 es caracteritzaria per xarxes P2P de diferent contingut i el 4 pàgines de contingut il·legal, en general monitoritzades per l'administració.

Dark web

Es tracta d'una porció de la *deep web* i es calcula que inclou un 0,1% del contingut de la xarxa. És intencionalment ocult als buscadors, amb adreces IP emmascarades i accessibles des d'un navegador especial (el més popular és TOR). La moneda de canvi és el *bitcoin*.

El nivell 5 inclouria continguts il·lícits en què es trafica amb armes, estupefaents, pornografia infantil, arxius robats, etc. El nivell 6 és suposadament d'accés restringit als governs.



Font: Hacker Combat Community

L'accés lliure i obert a la xarxa no només serveix per compartir coneixement i informació, sinó que possibilita la llibertat d'expressió dels individus que la utilitzen. El naixement de xarxes constituïdes a internet, amb serveis ocults, on l'anonimat i la privadesa no són opcionals, és tremendament polèmic en molts països com l'Iran o la Xina; fins i tot algunes democràcies occidentals castigades pel terrorisme, com França, s'ha plantejat prohibir-ne l'ús.

CASOS I APLICACIONS PRÀCTIQUES

CAS 1

El primer port ciberresilient, a Rotterdam

En ple boom de digitalització i centralització de dades, cada cop esdevé més necessari garantir la seguretat i confidencialitat de la informació. Rotterdam és la primera ciutat europea amb una estratègia oficial de seguretat i ciberresiliència.

CAS 2

Gestió de dades personals; l'escàndol de Facebook

El possible ús de les dades personals amb què compta la companyia per a les eleccions presidencials al Estats Units o la votació del Brexit va portar les administracions a qüestionar-se sobre la normativa de protecció de dades a Europa.

CAS 3

El Model de Maduresa de Capacitat de Seguretat Cibernètica (CMM)

El Centre de Capacitat Mundial de la Seguretat Cibernètica de la Universitat d'Oxford al Regne Unit ha publicat 49 indicadors que avaluen el nivell de maduresa cibernètica d'un territori segons cinc nivells.

CAS 4

L'eficàcia dels algoritmes, posada en dubte en ciberseguretat

Microsoft utilitza diversos algoritmes basats en *machine leaning* o intel·ligència artificial per fer front a ciberamenaces. No obstant, els experts i en concret el MIT ha plantejat els diferents reptes de fer ús d'aquestes noves tecnologies.

CAS 5

La primera ambaixada "digital" d'Estònia, a Luxemburg

Estònia és el primer país a obrir una ambaixada digital per protegir les seves dades. Amb una administració pública totalment digitalitzada, el país bàltic va desenvolupar un sistema propi amb Microsoft per tenir una còpia de seguretat fora de les seves fronteres.

CAS 6

La policia de la ciutat de Londres contra els cibercrims

La Policia de la ciutat de Londres va crear el 2016 l'Oficina Nacional d'Intel·ligència de Fraus (NFIB) per lluitar contra el frau i la ciberdelinqüència. L'oficina utilitza un sistema d'intel·ligència policial per fixar els patrons dels atacs i els seus vincles.

- **Any implantació:** 2016
- **Iniciativa pública i privada**

- **Abast d'actuació**: Rotterdam (Països Baixos)

DESCRIPCIÓ DEL CAS

Rotterdam com a ciutat ciberresilient

L'any 2014 l'Ajuntament de Rotterdam va reconèixer per primer cop la necessitat d'establir un port ciberresilient. El motiu? Les inversions en digitalització a la ciutat augmentaven a un ritme del 27% anual en els últims anys; les inversions en seguretat cibernètica, en canvi, només havien augmentat un 4%, el que indicava un potencial factor de risc a curt termini [19].

L'Autoritat Portuària de Rotterdam ha estat notícia aquest últim any per ser el primer organisme en aplicar Indústria 4.0 a Europa. El lobby Deltalinqs (representant dels interessos logístics i industrials de 700 empreses al port de Rotterdam) i l'Autoritat Portuària van fundar la plataforma de ciberseguretat i resiliència FERM, juntament amb la posada en marxa d'una estratègia municipal de ciberresiliència a la ciutat. Mitjançant aquestes eines, la ciutat ha intentat augmentar la conscienciació de les empreses establertes sobre la importància de la privacitat de la informació i la ciberseguretat en l'entorn de treball. L'equip de treball ha anat més enllà per tal de construir una estructura organitzativa per assegurar que el port sigui accessible durant el possible fracàs d'un sistema TIC.

Resultats

El port de Rotterdam és el port més potent d'Europa, amb una circulació de més de 140.000 vaixells al llarg de l'any. Per mantenir aquesta posició en un mercat global i europeu tan competitiu, l'Autoritat Portuària s'ha esforçat els darrers anys a millorar la circulació de nombrosos vaixells i transformar-lo en un port intel·ligent amb implementació d'un panell de control centralitzat en col·laboració amb empreses privades com IBM i Microsoft.

El juny del 2017, el port va patir un ciberatac. Tot i que només va afectar una empresa, els organismes van aprendre que és important que no només les empreses comptin amb un pla de prevenció a títol individual, sinó que esdevé clau l'existència d'una xarxa de ciberseguretat i resiliència a escala global que reconegui l'amenaça que suposen els ciberatacs i hi faci front amb una estratègia coordinada global. La ciutat i el port de Rotterdam han admès que la ciberseguretat és un element decisor per a les empreses que busquen establir-se al port en l'actualitat, sobretot quan els ciberatacs adopten cada cop formes més diverses i discretes (en forma de correus electrònics, *spam*, enllaços a pàgines web, etc.), causant danys importants i en molts casos irreversibles en els sistemes operatius [20].

LESSONS LEARNT

La creixent digitalització dels processos i el caràcter dinàmic dels ciberatacs IT i OT fan que les infraestructures requereixin cada cop més d'un procés de resposta articulat i adequat per gestionar un ciberatac. La centralització de les dades i el compromís que les ciberamenaces afectin les operacions de les organitzacions o companyies fa que esdevingui necessari articular un pla de prevenció per minimitzar els efectes de possibles ciberatacs en col·laboració amb les empreses de l'entorn.

- **Any del cas:** 2018
- **Iniciativa privada**

- **Abast d'actuació**: Internacional

DESCRIPCIÓ DEL CAS

Crisi de Facebook - gestió de dades personals

Recentment va sortir a la llum la filtració d'informació personal de 87 milions d'usuaris de Facebook. Durant els últims anys, algunes aplicacions es van dedicar a recol·lectar dades de milers de perfils de la xarxa social i una d'aquestes li va vendre aquesta informació a Cambridge Analytica (CA), una consultoria política que presumptament va fer servir aquestes dades per influenciar l'opinió de les persones en processos electorals, com la votació del Brexit o la victòria de Donald Trump.

La crisi va esclatar el dissabte 17 de març del 2018, quan el New York Times i The Guardian van publicar que Cambridge Analytica havia accedit i retingut informació sobre 50 milions d'usuaris de Facebook sense el seu permís. La informació provenia directament d'un dels seus fundadors, Christoper Wylie, que hauria entregat documents sobre el funcionament secret de l'empresa. Segons aquests documents, els protocols de Facebook es van activar el 2014, després de detectar l'enorme quantitat de dades que extreia l'aplicació ThisIsYourDigitalLife, un test que proposava als usuaris descobrir la seva personalitat amb finalitats acadèmiques, i a partir del que CA utilitzava dades per canviar el comportament de les persones. Un dia abans de la filtració en premsa, Facebook va anunciar que suspenia a l'empresa Cambridge Analytica de la seva plataforma, després d'evitar sense èxit que la notícia es filtrés als mitjans. La companyia no va poder contenir les conseqüències de les revelacions: la cotització de les seves accions havien disminuït un 10%. Després d'uns dies de silenci, el seu fundador Mark Zuckerberg va realitzar una entrevista per a la CNN, on va admetre haver detectat que el professor de la universitat de Cambridge Aleksandr Kogan havia compartit amb CA dades d'usuaris de Facebook. L'aplicatiu va ser vetat d'immediat i se'ls va exigir que certifiquessin que havien esborrat les dades obtingudes. Però ja era massa tard, s'havien efectuat múltiples còpies dels fitxers que s'haurien enviat per correu electrònic sense xifrar.

Reformes en la política de privacitat

El 28 de març Facebook va anunciar a través del seu bloc una reforma en les seves polítiques de privacitat per facilitar als seus usuaris poder trobar i editar la informació personal que tenien a la xarxa social. La companyia va assegurar que aquests canvis ja estaven planificats abans de l'escàndol, per complir amb la nova regulació de protecció de dades de la Unió Europea (RGPD), que entrava en vigor el 25 de maig.

Una setmana després de comparèixer davant del Senat d'Estats Units, el 10 d'abril, al qual va demanar repetidament disculpes per la fallada de Facebook, la xarxa social anunciava que modificava el seu domicili fiscal (en aquell moment a Irlanda) a Estats Units, de manera que la majoria d'usuaris (el 70%, 2.000 milions) deixaven de quedar protegits pel nou marc de privacitat que entrava en vigor a la Unió Europea, i la companyia quedava menys exposada a les multes que la nova legislació imposava a aquelles companyies que recol·lectaven dades personals sense consentiment.

La companyia ha sigut penalitzada amb una multa històrica per aquest escàndol: 500.000£ (menys de 600.000€), una quantitat que equival al que Facebook recapta en cinc minuts i mig, i que podria haver suposat entre 20 i 1.600 milions d'euros (4% dels seus ingressos), si s'hagués aplicat el RGPD [22].

LESSONS LEARNT

La informació és un actiu cada cop més valuós per a empreses i administracions. La digitalització de la societat de la informació ha fet que els usuaris cedeixin part de les seves dades a tercers, la majoria de vegades de manera inconscient i sense pensar que aquestes poden ser utilitzades posteriorment per part d'empreses o fins i tot per part de ciberdelinqüents per efectuar atacs dirigits. La falta de transparència de les empreses en aquest sentit és un element de preocupació i quelcom que no ha de deixar de treballar-se.

Global Cyber Security Capacity Centre

- **Any d'implantació:** 2013
- **Iniciativa pública i privada:**

Global Cyber Security Capacity Centre · Oxford Martin School · University of Oxford · Department of Computer Science

- **Abast d'actuació**: Regne Unit i Internacional

DESCRIPCIÓ DEL CAS

El Model de Maduresa de Capacitat de Seguretat Cibernètica (CMM), primer indicador de ciberrisc

El Centre Global de Capacitat sobre Seguretat Cibernètica de la universitat d'Oxford va facilitar l'any 2013 la recol·lecció de dades per part del Banc Interamericà de Desenvolupament (BID) i l'Organització dels Estats Americans (OEA) de diferents organitzacions en seguretat cibernètica de diferents sectors. Aquestes incloïen agències governamentals, operadors d'infraestructures crítiques, forces militars, policia, el sector privat, la societat civil i diferents institucions de coneixement. L'objectiu era l'elaboració d'un informe que fes més comprensible i accessible els riscos a la xarxa [23].

El Centre va desenvolupar arran de l'estudi l'anomenat *Model de Maduresa de Capacitat de Seguretat Cibernètica (CMM)* amb el propòsit d'ajudar les administracions o organitzacions a avaluar la seguretat de la informació i prendre decisions al respecte a partir de 49 indicadors (anomenats subfactors). Aquests avaluen el grau de maduresa de cadascuna de les següents dimensions:

1. Polítiques de seguretat i estratègia
2. Cultura cibernètica i societat
3. Educació, formació i competències
4. Marc normatiu
5. Tecnologia

Cinc graus de maduresa

INICIAL
No existeix res, o es té una idea molt embrionària sobre el problema, però s'han efectuat accions concretes en ciberseguretat.

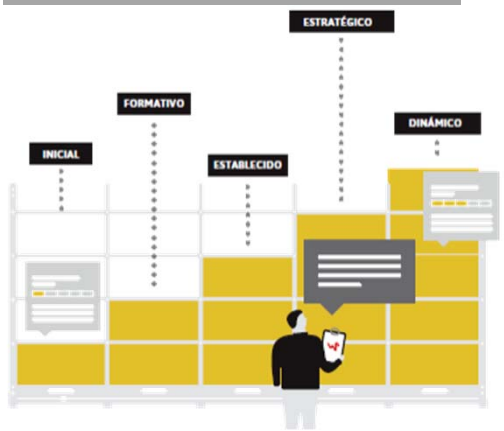
FORMATIU
Algunes característiques del subfactor han començat a ser formulades, però són casuals, estan desorganitzades o mal definides.

ESTABLERT
Els elements del subfactor han estat establerts i funcionen, però l'assignació de recursos no s'ha realitzat adequadament.

ESTRATÈGIC
Es compleixen els aspectes clau del subfactor i s'han establert objectius particulars

DINÀMIC
En aquest nivell ja es tenen mecanismes clars per modificar l'estratègia en funció de les circumstàncies. Són claus la presa de decisions àgil, la reassignació de recursos i l'atenció constant als canvis d'entorn.

Resultats



Des de l'any 2014, l'Observatori de Ciberseguretat d'Amèrica Llatina i el Carib utilitza el model de maduresa com a indicador per comprovar en quina etapa de l'estratègia nacional de seguretat cibernètica es troba cada país o comunitat. El resultat? Només 6 dels 32 països avaluats tenen una estratègia de ciberseguretat prou madura (dinàmica).

En l'actualitat cada cop són més els països i les organitzacions i administracions que han considerat avaluar la seguretat dels seus processos i equips. El present model és tot un exemple d'avaluació col·lectiva d'un territori amb un objectiu comú: assolir l'excel·lència en seguretat cibernètica.

LESSONS LEARNT

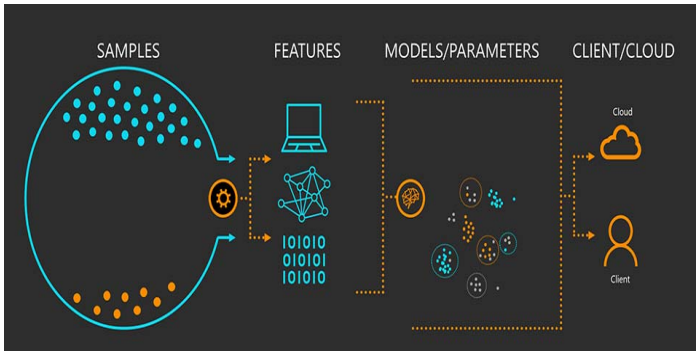
L'elaboració del Model de Maduresa de Capacitat de Seguretat Cibernètica és tot un exemple de col·laboració entre administració, organitzacions i empreses del territori per tal d'assolir indicadors significatius que avaluïn i donin solució a un dels majors reptes del s.XXI: la seguretat a la xarxa.

- **Any d'implantació:** 2018
- **Iniciativa privada**
- **Tecnologia utilitzada:** Intel·ligència artificial i *Machine learning*
- **Abast d'actuació**: Internacional

DESCRIPCIÓ DEL CAS

Protecció del protector a través dels usos d'un conjunt divers d'algoritmes

Microsoft va presentar a Black Hat USA 2018 -jornada internacional d'investigació en tendències en seguretat de la informació- una sèrie de lliçons apreses arran de la seva experiència investigant atacants que havien intentat eludir els seus sistemes de seguretat, basats en m*achine learning* i intel·ligència artificial.



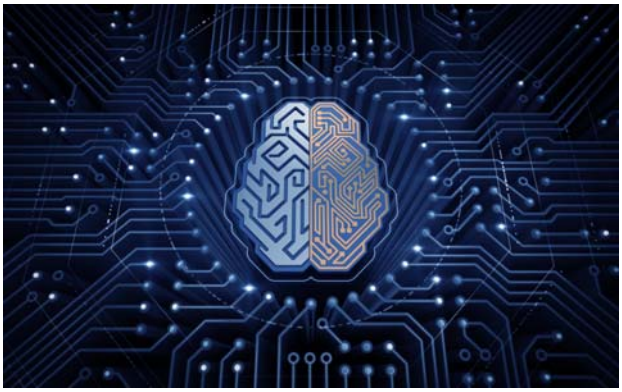
Segons els seus sistemes de protecció, en un dia qualsevol 2,6 milions de dispositius van ser compromesos amb un *malware* recentment descobert en 232 països diferents. D'aquests atacs, hi havia 1,7 milions de *malware* diferents. I el 60% dels atacs es van acabar en una hora.

El servei de protecció *Windows Defender* de Microsoft es basa en un conjunt d'algoritmes amb diferents configuracions. Si un algoritme és hackejat, el resultat de la resta mostren -assumint que no han estat hackejats- l'anomalia del primer model. La distribució de les dades del sistema mitjançant diversos algorismes complica així als atacants arribar a hackejar el sistema [24].

Resultats

Tot i el desenvolupament de noves tecnologies com són el *machine learning* o l'IA en ciberseguetat, l'Institut Tecnològic de Massachussets (MIT) ha assenyalat recentment un cert risc de dependre'n [25].

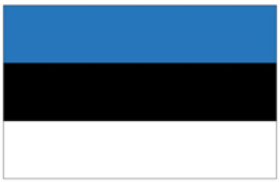
L'Institut considera que en moltes ocasions els proveïdors no presten prou atenció als riscos associats de l'ús intensiu d'aquestes tecnologies, que també són vulnerables. Si bé és cert que el seu ús pot ajudar a automatitzar la detecció i la resposta de ciberamenaces i suplir la manca de professionals en alguns sectors, aquestes noves tecnologies poden crear una falsa sensació de seguretat a les empreses.



Els clients busquen solucions que incloguin aquestes noves tecnologies però no se n'adonen que impliquen un seguiment continu que requereix, entre d'altres, actualitzar el codi i etiquetar el conjunt de dades diferenciant entre codi net i maliciós. I això, en molts casos, compromet la informació i facilita als ciberdelinqüents els atacs a la xarxa.

LESSONS LEARNT

Fer front a les ciberamenaces no és una tasca senzilla, sobretot si volem fer-ho amb més tecnologia. La manca de treballadors en aquest sector és un repte al qual les empreses comencen a fer front amb tecnologies 4.0. L'Institut Tecnològic de Massachussetts, però, busca conscienciar les organitzacions sobre com de contraproduent pot arribar a ser un ús massiu d'aquesta tecnologia, facilitant el robatori de dades i fins i tot l'accés al sistema de seguretat.



- **Any d'implantació:** 2017
- **Iniciativa pública:**

REPUBLIC OF ESTONIA GOVERNMENT

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

- **Abast d'actuació**: Estònia i Betzdorf (Luxemburg)

DESCRIPCIÓ DEL CAS

La primera ambaixada "digital" d'Estònia a Luxemburg

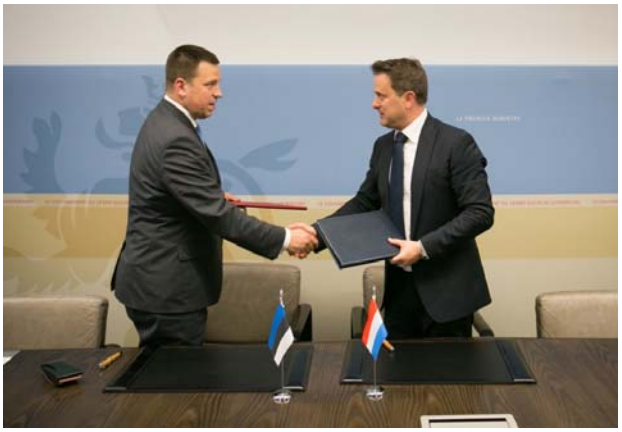
Definida pel Banc Mundial com "el més semblant a una societat digital", la república bàltica és un país model en aprofitament de les TIC. Tota l'administració pública estoniana està digitalitzada, ja no hi ha registres en paper.

El 98% de les transaccions bancàries es fan digitalment i gairebé totes es firmen mitjançant DNI electrònic. Això la converteix en la nació més digitalitzada i, alhora, més depenent de la ciberseguretat del planeta.

L'agressió militar de la veïna Rússia a Ucraïna el 2014 va portar el país a buscar respostes sobre la manera en què podrien fer front a un atac cibernètic o fins i tot un atac militar. Estònia ja va patir massius ciberatacs de Rússia que van afectar les webs del govern, bancs i mitjans de comunicació l'any 2007. No obstant, no es va perdre informació en aquell moment.

En considerar que amb les còpies de seguretat que hi havia dins del país i a les seves més de 30 ambaixades al món no n'hi hauria prou per garantir la continuïtat del sistema en cas d'una gran crisi, es va arribar a la conclusió que calia tenir una còpia de seguretat fora de les seves fronteres. El projecte es va fer efectiu el 20 de juny de 2017, amb la firma d'un acord amb el Govern de Luxemburg per obrir en el seu territori una ambaixada digital: un centre de dades d'alta seguretat reservat dins de les instal·lacions del Govern de Luxemburg, en el que ja es guarden dades crítiques com el cens, el cadastre o el sistema de pagaments i pensions de l'administració estoniana [26].

Més que una innovació tecnològica



Va ser l'any 2014, després de descartar col·locar els continguts en mans d'una empresa privada especialitzada en serveis del núvol digital, quan Estònia i Microsoft van iniciar un acord de col·laboració per desenvolupar el seu propi model de computació en el núvol.

El resultat fou una ambaixada digital de la qual se'n desconeix la localització i que funciona com qualsevol ambaixada tradicional: l'interior dels murs es respecta com si fos el seu propi territori i el país d'acollida no té dret a traspassar els seus murs. Només poden accedir-hi representants autoritzats del govern estonià. "La idea és que si passa qualsevol cosa, Estònia pot continuar funcionant com a Estat encara que no disposi de les seves facilitats físiques aquí. El govern o el Parlament podrien continuar prenent decisions des de qualsevol lloc". Gairebé un any després de la implementació de l'ambaixada digital, Estònia ja es planteja construir espai virtual per a ambaixades de dades d'altres països.

LESSONS LEARNT

La descentralització o diversificació és una de les principals eines per disminuir el risc. En aquest sentit, l'obertura d'una ambaixada digital conseqüència de l'alt nivell de digitalització de l'administració estoniana és tot un exemple d'aquesta estratègia. L'ús de la protecció jurídica atorgada a les ambaixades per resguardar les dades crítiques d'un govern és tot un exemple d'innovació tecnològica que, de ben segur, serà tendència en els pròxims anys.

National Fraud Intelligence Bureau

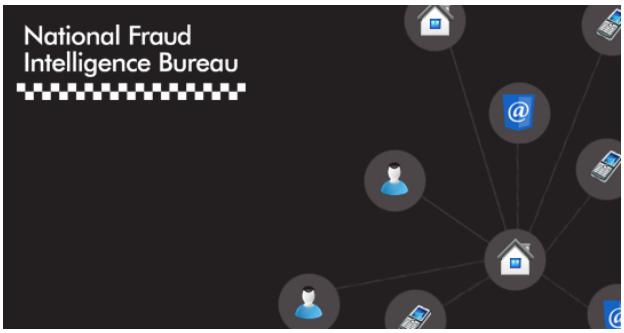
- **Any d'implantació:** 2006
- **Iniciativa pública:**

CITY OF LONDON POLICE

- **Abast d'actuació**: Londres i Regne Unit

DESCRIPCIÓ DEL CAS

La policia de la ciutat de Londres, líder en la lluita contra els cibercrims



L'*Oficina Nacional d'Intel·ligència de Fraus* (NFIB en anglès) és el departament de la Policia de la ciutat de Londres encarregat de lluitar contra el frau i la delinqüència cibernètica. El dispositiu treballa conjuntament amb *Action Fraud*, el centre d'informació i denúncia de fraus d'Anglaterra i Gal·les.

El govern britànic va calcular que el cibercrim costava a Gran Bretanya 27.000M £ l'any i segons dades de la policia, set de cada deu estafes al país estaven relacionades amb TIC o tenien algun component cibernètic (respecte al 40% de fa cinc anys). Alhora, el nombre de cibercrims «purs» denunciats es van gairebé duplicar en un any, amb un notable augment dels «fraus per volum», com són les estafes en subhastes i compres en línia, les estafes amb xecs, targetes de pagament i comptes bancaris en línia o les estafes d'inversions. [27]

Resultats

El Servei d'Inspecció del Cos de Policia de sa Majestat (HMIC) va sol·licitar una resposta coordinada a escala nacional per part de la policia per lluitar contra els ciberdelinqüents. El cos policial va així iniciar un acord de col·laboració amb *Kaspersky Lab,* especialitzats en *malware,* per dissenyar i distribuir el primer programa integral de ciberseguretat del Regne Unit.

L'acord de col·laboració tenia com a objectiu formar agents de policia i grans empreses, equipant-los amb les habilitats i els coneixements necessaris per inspeccionar el tràfic a la xarxa, identificar possibles amenaces cibernètiques i prendre les mesures defensives necessàries requerides segons el tipus d'atac. La formació incloïa aprendre a analitzar imatges d'un disc dur i descompilar software maliciós amb eines i metodologia especialitzada.

Addicionalment, el NFIB va desenvolupar el sistema "Know Fraud", un sistema d'intel·ligència policial avançat amb capacitat de processar grans quantitats de dades i fixar patrons de les ofensives així com els seus possibles vincles. Aquest sistema permet a la policia analitzar el patró de comportament dels ciberdelinqüents a la xarxa i detectar possibles millores legislatives, de les quals s'informa els legisladors [28].

LESSONS LEARNT

Aquest cas demostra la importància de la col·laboració entre els diferents agents del territori per lluitar contra el cibercrim. La professionalització de la seguretat en l'àmbit institucional és un element clau per fer front a la tendència creixent de les ciberamenaces. Paral·lelament, la comunicació entre cossos de seguretat, administració, ciutadania i organitzacions per conscienciar-los sobre els atacs vigents a la xarxa són fonamentals per prevenir aquestes amenaces.

Repercussió i aplicabilitat a l'AMB

Un cop analitzats els sis casos pràctics d'estudi d'abast municipal, nacional i internacional, podem extreure'n algunes conclusions aplicables a l'àrea metropolitana.

La creixent dependència del territori de les tecnologies i el caràcter dinàmic i sistèmic de les amenaces a la xarxa fan que cada cop sigui més difícil garantir la ciberseguretat. Disposar d'un pla de continuïtat en cas d'atac, que permeti a administracions i organitzacions restablir les operacions tan aviat com sigui possible, és fonamental per reduir l'impacte econòmic de l'incident. En aquest sentit, l'estratègia de **ciberresiliència** de la ciutat de Rotterdam, i en especial, del seu port, li atorguen un avantatge competitiu clau i decisor per les empreses que busquen establir-s'hi.

De la mateixa manera, **l'avaluació dels sistemes de ciberseguretat** és cada cop més freqüent, tant en el sector públic, com en el privat. El Model de Maduresa de Capacitat de Seguretat Cibernètica (CMM) és tota una innovació, permetent avaluar les vulnerabilitats d'una organització o territori a diferents nivells. En aquest sentit i per tal de fer front als cibercrims, cada cop més freqüents, la policia britànica ha invertit en millorar la ciberseguretat al país mitjançant la **formació del cos policial** i la incorporació d'un *software* antifrau, que permet identificar tendències de la ciberdelinqüència.

Les noves tecnologies han facilitat la lluita contra el cibercrim i han donat solució a alguns sectors davant la manca de professionals en ciberseguretat. No obstant, tal com ha assenyalat el MIT, l'ús de ***machine learning*** **o intel·ligència artificial** poden comprometre la seguretat de les empreses si no s'utilitza adequadament.

A banda de la ciberseguretat, l'economia de les dades no es pot entendre sense tenir en compte la **protecció de dades**. Si bé és cert que les empreses tenen dret a disposar i explotar les dades personals dels seus clients per realitzar les seves activitats i contribuir al desenvolupament econòmic, han de fer-ho de manera lleial, transparent i amb el màxim respecte. La mala gestió de les mateixes per part d'organitzacions requereix accions sancionadores fermes per part de l'administració. El RGPD és el primer pas; les administracions, però han d'apostar per una solució internacional per evitar que grans corporacions (com *Facebook*) puguin evitar sancions modificant el seu domicili fiscal.

Finalment, la **descentralització de les dades** es presenta com una solució per garantir la protecció de la informació dels territoris més digitalitzats. La creació de la primera **ambaixada digital** per part del govern estonià fora del país és tot un exemple d'innovació, en concret de com desenvolupar noves figures jurídiques combinant el marc normatiu actual i les noves tecnologies.

L'Àrea Metropolitana de Barcelona pot fer ús d'aquestes bones pràctiques, implementant qualsevol de les següents iniciatives:

- Impulsar un debat complet i compromès sobre ciberseguretat a l'àrea metropolitana
- Impulsar la ciberseguretat com a factor de competitivitat territorial per atreure empreses i inversions
- Impulsar la formació específica a tots els nivells de serveis públics i la formació d'especialitats, per protegir i subsanar situacions de ciberseguretat
- Oferir serveis de ciberseguretat als seus municipis
- Implementar mesures d'avaluació dels sistemes de ciberseguretat en els municipis metropolitans, i impulsar des dels mateixos l'avaluació de les organitzacions i empreses del territori
- Impulsar un pla de ciberresiliència a l'àrea metropolitana amb l'objectiu de garantir la continuïtat de les activitats

L'Àrea Metropolitana de Barcelona ha de treballar per ser referent en ciberseguretat, impulsant una estratègia de ciberresiliència per garantir la continuïtat de les seves operacions en cas d'un ciberatac.

La col·laboració entre l'administració pública, les empreses i la ciutadania esdevé clau per crear un model robust i compromès de ciberseguretat.

Recomanacions

La seguretat a la xarxa requereix no només d'eines tecnològiques reactives o defensives per fer front a les ciberamenaces, sinó que cal integrar la seguretat proactivament en l'administració, la societat civil i les empreses, conscienciant-los sobre les implicacions ètiques i socials de la digitalització en la societat actual.

Des d'un punt de vista individual, cal conscienciar i sensibilitzar a la ciutadania del que significa la informació i dels riscos que es deriven del ciberespai. Actualment els usuaris paguen amb dades i pèrdua de privacitat molts serveis; i els servidors poden fer ús, vendre o perdre aquestes dades. Per això és important que els individus coneguin els avantatges i inconvenients d'internet, desenvolupin una cultura de la seguretat cibernètica actualitzant les eines de gestió de seguretat digital i tinguin una actitud permanent d'aprenentatge. Que els individus comparteixin voluntàriament les dades dels ciberatacs serà un factor clau que permetrà una anàlisi més profunda i el disseny de models per millorar la comprensió dels riscos informàtics.

Des d'un punt de vista corporatiu, cal que les empreses coneguin les obligacions legals en gestió de la seguretat i protecció de dades, i que desenvolupin una cultura de seguretat corporativa que impregni tota l'organització. Per això, es recomana que disposin de professionals competents en seguretat de la informació, estableixin plans interns de previsió de riscos i de planificació de la recuperació en cas d'incidència i que implantin normatives internes de seguretat als diferents integrants de la cadena (des de proveïdors de serveis i desenvolupadors de productes i serveis a clients) que complementin la precaució dels usuaris, ella sola insuficient.

Els empleats també són una part clau de la seguretat a l'empresa: està comprovat que una bona cultura de la seguretat digital bàsica pot ajudar a prevenir la major part d'amenaces a les organitzacions.

En l'àmbit públic, cal anar més enllà de la protecció local i establir polítiques públiques més ambicioses, amb un enfocament global i coherents amb la normativa comunitària. L'administració juga un paper primordial en l'escenari ciber, havent d'assumir reptes com a impulsor, coordinador, regulador i protector. En concret:

1. Divulgant i sensibilitzant als agents del territori sobre la importància de la informació, la protecció de dades i les amenaces a la xarxa.
2. Liderant la transició a l'economia digital, proporcionant recursos públics de ciberseguretat.
3. Garantint que els sistemes d'informació i comunicació que utilitzen les administracions gaudeixen d'un nivell adequat de ciberseguretat i resiliència, potenciant les capacitats de prevenció, detecció, reacció, anàlisi i coordinació amb altres sectors, i essent àgil a l'hora d'adaptar-se i respondre a unes amenaces cada cop més dinàmiques
3. Impulsant la seguretat i resiliència del sector empresarial en general i operadors d'infraestructures crítiques, en particular.
4. Escoltant les demandes de tots els actors de l'escenari digital i establint canals de comunicació i cooperació entre l'àmbit públic i el privat.
5. Definint el marc d'actuació d'administracions, empreses, institucions i ciutadans, garantint la seguretat jurídica del món digital.
6. Aconseguint i mantenint els coneixements i les capacitats tecnològiques del territori mitjançant formació a tots els nivells, des de l'educació primària, fins a la universitat. Esdevé essencial en aquest sentit definir un programa digital docent específic per tal de fer front a la manca de perfils especialitzats en aquest sector.

Aquest lideratge s'ha d'exercir en col·laboració amb la societat civil i els sectors privats.

Bibliografia

[1] Consilium of the European Union, Proposal for regulation on ENISA, the EU Cybersecurity Agency [en línia]. Disponible a: http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf

[2] CNMV, Ciberseguridad en las infraestructuras de los mercado, [en línia]. Disponible a: https://www.cnmv.es/DocPortal/Publicaciones/Ciberseguridad/Ciberseguridad_Infraestructuras_Mercados.pdf

[3] Allianz, Allianz Risk Barometer 2018, [en línia]. Disponible a: https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

[4] PWC, Temas candentes de la Ciberseguridad, Un nuevo espacio lleno de incógnitas [en línia]. Disponible a: https://www.pwc.es/es/publicaciones/gestion-empresarial/assets/temas-candentes-ciberseguridad.pdf

[5] World Economic Forum, Global risks landscape 2018, [en línia]. Disponible a: http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#risks///

[6] Instituto Español de Estudios Estratégicos, La ciberseguridad en la UE, [en línia]. Disponible a: http://www.ieee.es/en/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

[7] Consejo de la Unión Europea, Reforma de la ciberseguridad en Europa, [en línia]. Disponible a: http://www.consilium.europa.eu/es/policies/cyber-security/

[8] Departamento de Seguridad Nacional, Ciberseguridad [en línia]. Disponible a: http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad

[9] IDES, Informe 2016 de l'Observatori del Risc: la ciberseguretat a Catalunya, [en línia]. Disponible a: http://www.fundacio-ides.org/ides/wp-content/uploads/Informe2016_web.pdf

[10] ACCIÓ, La ciberseguretat a Catalunya, Informe tecnològic, [en línia]. Disponible a: http://www.accio.gencat.cat/web/.content/bancconeixement/documents/informes_sectorials/ciberseguretat-informe-tecnologic.pdf

[11] Institut Cerdà, La Ciberamenaza: un riesgo del s.XXI [en línia]. Disponible a: https://www.icerda.org/media/files/Publicacions/2017%20IC%20Monografia%203%20Ciberamenaza.pdf

[12] Accenture, Cost of cybercrime study 2017: insights on the security investments that make a difference [en línia]. Disponible a: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[13] Hackmaggedon, Cyber-attacks statistics 2017, [en línia]. Disponible a: https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

[14] Indra, Ciberseguridad industrial, [en línia]. Disponible a: https://www.indracompany.com/sites/default/files/indra-ciberseguridad_industrial.pdf

[15] CESICAT, Informe Anual sobre ciberseguretat [en línia]. Disponible a: http://smartcatalonia.gencat.cat/ca/detalls/noticia/cesicat_publica_informe_anual_ciberseguretat

[16] Talentier, Los perfiles de seguridad más buscados, [en línia]. Disponible a: https://blog.talentier.com/perfil-ciberseguridad-hacking-etico

[17] McAfee, Hacking the skills shortage, [en línia]. Disponible a: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

[18] Panda Security, Tor y Deep web: todos los secretos del lado oscuro de la web, [en línia]. Disponible a: https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/

[19] Port of Rotterdam, Port Vision 2030 [en línia]. Disponible a: https://www.portofrotterdam.com/en/port-authority/about-the-port-authority/the-port-authority-in-society/port-vision-2030

[20] Resilient Rotterdam [en línia]. Disponible a: https://www.resilientrotterdam.nl/

[21] Institut Cerdà, Newsletter: Factsheet 21: Crisis de Facebook, robo de datos

[22] El Mundo, La històrica multa de Facebook, [en línia]. Disponible a: http://www.elmundo.es/television/2018/07/11/5b463e5e268e3e93528b45ca.html

[23] Observatorio de la Ciberseguridad en América Latina y el Caribe, [en línia]. Disponible a: https://publications.iadb.org/handle/11319/7449

[24] Microsoft, Protecting the protector: Hardening machine learning defenses against adversarial attacks. [en línia]. Disponible a: https://cloudblogs.microsoft.com/microsoftsecure/2018/08/09/protecting-the-protector-hardening-machine-learning-defenses-against-adversarial-attacks/

[25] MIT Technology Review [en línia]. Disponible a: https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/

[26] La Vanguardia, Estònia obre la primera ambaixada digital per protegir les seves dades, [en línia]. Disponible a: https://www.lavanguardia.com/encatala/20170704/423881478287/estonia-obre-la-primera-ambaixada-digital-per-protegir-les-seves-dades.html

[27] Kaspersky Lab, Case study: City of London Police [en línia]. Disponible a: https://media.kaspersky.com/es/business-security/enterprise/Kaspersky_case_study_City_of_London_police.pdf

[28] Police UK, Action Fraud [en línia]. Disponible a: https://www.actionfraud.police.uk/about-us/who-is-national-fraud-intelligence-bureau