EAPC blog

La Ciberseguretat a debat

16 d'abril de 2019

Relatoria duta a terme per Mònica Sabata, Parc de les Humanitats i les Ciències Socials de la Universitat de Barcelona

D'ençà que l'any 2013, el Sr. Edward Snowden va fer públics -a través de la premsa- els milers de documents classificats com a d'alt secret de diferents programes de l'Agència de Seguretat Nacional dels Estats Units on es descrivien alguns dels programes de ciberseguretat més rellevants i amb un gran impacte mundial, **la ciberseguretat ha esdevingut una qüestió que omple portades de diaris i a més, ha arribat a ser una de les prioritats dels països avançats**, els quals han desenvolupat estratègies de ciberseguretat que han de permetre als governs tenir una visió a llarg termini sobre l'estat de protecció del ciberespai.

Catalunya no ha quedat exclosa d'aquesta tendència. Ans al contrari. Per això, l'Escola d'Administració Pública, conjuntament amb la Universitat de Barcelona, van proposar dur a terme un diàleg sobre aquesta temàtica, el qual va dibuixar el context actual i al mateix temps, va abordar la importància que totes aquestes qüestions tenen en el dia a dia dels servidors públics. La jornada va aplegar dos experts en

la matèria que van assenyalar els riscos i els reptes i les oportunitats que la ciberseguretat planteja. Es tracta del Sr. Tomàs Roy, director d'estratègia de seguretat al Centre de Seguretat de la Informació de Catalunya (CESICAT); i el Sr. Jaume Abella, professor associat de La Salle Barcelona (Universitat Ramon Llull), responsable de xarxa i ciberseguretat i coordinador del Màster en Ciberseguretat.

El diàleg va iniciar-se amb la visualització, a proposta del Sr. Jaume Abella, d'un vídeo de la companyia HP en que es podia veure una història sobre ciberseguretat que acaba amb un advertiment del protagonista: **"a todos los que ocupáis puestos de responsabilidad, vosotros podéis ser los siguientes"**. Una història real en gran part que és, segons l'expert, "una situació que reflexa molt fidelment la realitat que pot passar a moltes companyies". Aquesta visualització fou rellevant perquè **de la mateixa manera que pot succeir en una empresa privada també pot passar en una administració**. I és que segons Abella, **"en una administració pública on hi ha molta gent i moltes dades, hi ha molt perill"**, i va continuar "hi ha moltes dades, de les dades se'n treu profit i, per tant, les venen i fan negoci". La qüestió és que quan t'ataquen, normalment no te n'assabentes i, per tant, "es produeix un *gap* entre el moment en que es produeix una vulneració i la detecció i l'avaluació".

I tots aquests processos de qui són culpa? Dels hackers? Segons Abella, per als experts parlar de hackers té una dimensió positiva. No en va, un hacker és una persona que té unes habilitats molt bones per fer una cosa. Per exemple, **"Mozart era un hacker de la música i Picasso un hacker de la pintura".** Per això, creu que per parlar amb propietat cal tractar a les persones que ens ataquen o que ataquen les empreses o les institucions com a **ciberdelinquents** o **cibercriminals**. I és que, "ells formen part del lado oscuro". I en aquest món obscur no ens poden oblidar les estructures dels estats que s'ataquen i que intenten fer manipulacions polítiques.

Ara bé, un dels temes que més preocupen a les administracions -perquè és molt inquietant- és el de les **infraestructures crítiques** de les administracions perquè a través d'elles es pot fer molt mal. Això és així perquè "**quan parlem de ciberdelinqüència cal homologar-la a un negoci que és molt lucratiu".** Per exemple, "si vols crear una denegació de servei, vas a internet i el compres".

Un altre problema que cal abordar és el del crim perquè el punt més dèbil és la pròpia persona. I és que sovint prenem molt poques precaucions. Per exemple: qui no ha rebut un mail estrany que t'envien per incloure't a l'ordinador un software maliciós? Aquesta és una forma com qualsevol altra d'enganyar-te, per bé que formes per enganyar-nos n'hi ha moltes de diverses. I és que com a usuari cal tenir moltes precaucions amb els enllaços dels correus electrònics, amb els USB a través dels quals ens poden controlar remotament l'ordinador, amb els gestors de continguts i els virus, entre d'altres.

Com a resum d'aquesta primera intervenció, el Sr. Abella ens va deixar dos titulars: el primer, **"avui en dia, Google sap més coses de nosaltres que nosaltres mateixos"** i en segon lloc, el fet que **"a l'actualitat només hi ha dos tipus d'empreses: les que han estat hackejades i les que no ho saben"**. I per fer front a això, la realitat tossuda: **"no hi ha prou especialistes que puguin treballar en aquest món"**.

La segona intervenció fou a càrrec del **Sr. Tomàs Roy, director d'estratègia de seguretat al CESICAT** i va començar amb l'anunci d'una bona notícia: "estem en un moment amb un creixement molt espectacular. La realitat és que tothom està creixent: les empreses, les administracions públiques....! Això és així perquè "hi ha una nova combinació en el món de la seguretat que és la confiança. **I és que les coses no només**

han de ser segures sinó que has de poder-hi dipositar confiança". Des d'aquest punt de vista "no es podria créixer si el nostre nivell de seguretat fos tan dolent que la gent no usés les eines que ofereixen les noves tecnologies".

Això és un indicador: **el creixement és exponencial i la gent opta per les noves tecnologies**. No en va, cada tres anys es dobla el número de pàgines web que existeixen i hi ha 4000 milions d'usuaris connectats a internet. **"Si la seguretat fos un desastre el sistema ja hauria col·lapsat pel seu propi pes"**, va afirmar Roy, i va continuar: **"I malgrat que queda molta feina per fer, la realitat és que a l'actualitat no hi ha cap activitat humana que no s'exporti a internet"**. En conseqüència, sembla evident que alguna cosa s'està fent bé entre la gent que munta els negocis, la gent que legisla, la gent que fa productes, la gent que certifica.. Ara bé, també afirmava l'expert que: "òbviament, tot es pot millorar".

Si parlem de l'administració catalana, cal subratllar l'existència d'una Conselleria de Polítiques Digitals i d'Administració Pública, encarregada de vincular les polítiques digitals amb la modernització de l'administració pública i la provisió de serveis de l'administració pública amb una aposta clara a favor del govern obert. I en aquest sentit, cal subratllar que és un repte molt interessant que el pla de govern plantegi temes com e-ciutadania, la identitat i la residència digital, l'entorn digital, els entorns de col·laboració, el país cibersegur, el desplegament d'una agència de ciberseguretat, la innovació en entorns de ciberseguretat, l'e-vot, l'e-participació, el blockchain... En definitiva, **"es vol apostar per ser referents en aquestes matèries"**, afirmava Roy. I és que **"és esperançador pensar que el país que farem es fonamentarà en aquestes matèries. Hi ha la consciència i els reptes".**

Més en general, hem d'afirmar que el terreny de la ciberseguretat és un espai abonat on s'ha especialitzat el crim. No en va, "el cibercrim mou més diners que la droga utilitzant, per exemple, sistemes com la criptomoneda, que permet especular i invertir. Són negocis sòlids que eviten que els qui lluiten contra el cibercrim els puguin enxampar" . I també afirmava Roy: "S'ha generat una tecnologia molt segura -la criptomoneda- que està molt associada al sector del crim. Tanmateix, aquesta moneda també pot empoderar molts d'altres serveis gràcies, precisament, a la seva robustesa". En definitiva, s'ha desplaçat el crim cap a l'entorn ciber, on robar dades personals ha esdevingut senzill, encara més si es fa des d'algun correu de persones conegudes que tenen una reputació.

Ara bé, si parlem de bones notícies, podem afirmar que **la ciberseguretat ha generat un motor econòmic al voltant de la indústria 4.0 i de l'e-commerce**. I això és així perquè es considera segur. I malgrat no ho són del tot, estem parlant de noves tecnologies que són prou fiables i segures com perquè sigui una tecnologia adaptada a construir eines útils, cotxes autònoms que són segurs, un 5G que facilitarà que el cotxe funcioni, els nous entorns bancaris.. En canvi, "cal recordar que el mòbil no és segur. Serveix per trucar però no ofereix seguretat".

Al mateix temps, com afirmàvem, existeix un sector de la ciberseguretat que busca protegir altres entorns i que ha esdevingut un motor econòmic. De fet, s'espera un creixement exponencial durant els propers anys. L'IoT (*internet of things*, internet de les coses) està creixent moltíssim i per això, també és un factor d'atac. Convé recordar que des del 2004 i fins al 2017 el creixement sostingut ha estat d'entre el 12 i el 15%, amb una inversió de milers de milions d'euros, i arribant al 2018 amb xifres esperades de 93 mil milions d'euros. En definitiva, és un sector, i en conseqüència, és molt positiu que "tinguem un pla de govern que aposta per una indústria que té aquesta rellevància".

Convé, però, assenyalar altres temes. Per exemple, el legislatiu. Aquest és un assumpte important del qual la nostra societat en depèn, doncs **"cal que apareguin lleis i regulació diversa, a vegades amb retard i a vegades amb efectes no desitjables com que per cobrir drets es perden drets".** Ara mateix, ja hi ha una reforma del codi penal que cobreix què és un delicte informàtic, hi ha un reglament per cobrir les dades personals que empodera al ciutadà i que al mateix temps fa responsable a les empreses. Finalment, Roy acabava aquest argument sentenciant que "**ara ja no tenim un papa estat que ens protegeix, sinó que són els ciutadans i les empreses els que n'han d'aprendre i s'han de protegir. Anem cap aquí".**

Però el diàleg també va aportar altres temes rellevants en els quals s'ha avançat durant els darrers anys:

– **Directiva del copyright**: es tracta de protegir els drets d'autor. Però per fer-ho s'exagera una mica en el sentit de fer una censura prèvia, fet que xoca amb els drets de privacitat i informació que volem que no es pugui inspeccionar. En conseqüència es produeixen col·lisions de drets.

– **Regulació sobre IoT**: a Califòrnia han estat capdavanters. Durant el mes de setembre passat van llençar una reglamentació de l'IoT per la qual els dispositius de IoT han de tenir controls adequats en relació als sistemes d'infraestructura industrial on estiguin. No es poden acceptar coses que en el passat havien estat normals com per exemple els *passwords* posats per la mateixa empresa.

– **Cossos de seguretat per a la xarxa**: ara mateix tenim moltes més estructures que no teníem en el passat. Per exemple: la policia i l'exèrcit d'internet, la defensa en contra de l'assetjament dels infants, el CESICAT, la lluita contra el ciberassetjament,l' agència de ciberseguretat, les unitats de delictes informàtics.. i al mateix temps tenim policies com la Interpol o l'Europol, amb unitats que treballen contra el cibercrim a nivell europeu, fins i tot assumint que a vegades hi ha problemes de comunicació i relació entre elles.

La realitat és que cada vegada més el ciutadà és menys dèbil. "Si bé és cert que ara encara és l'eslavó dèbil de la cadena, també és veritat que cada vegada ho serà menys", afirmava Roy. Per això, l'administració ha d'utilitzar al ciutadà. I és que el ciutadà és l'instrument més barat per detectar que alguna cosa va malament. Per exemple, si canviem el mòbil ara ja hi ha mesures perquè les mateixes companyies ens ho preguntin. Això els estalvia molts diners. I malgrat tot, tal i com ja s'havia afirmat durant el diàleg, l'expert va tornar a reiterar que és evident que encara hi ha molts reptes per assolir i molta feina per fer.

Al mateix temps, convé assenyalar aliances globals que s'han produït per millorar la situació:

– **Els fabricants d'antivirus comparteixen informació**. Ells ja saben que la ciberseguretat és cosa de tots i que la font de negoci ja no està aquí. Per això comparteixen informació i s'ajuden.

– **Global Ciber Security Alliance** feta entre els operadors de telefonia que tenen presència a seixanta països, 1200 milions d'usuaris i sis mil experts en ciberseguretat. Això implica tenir un volum d'informació que els dona avantatge competitiu però també tenen molt coneixement nou que fa avançar.

– I finalment, també **hi ha seixanta firmes** (amb Facebook, Microsoft i HP entre moltes d'altres) **que han fet un *teach accord*** per empoderar i protegir els ciutadans.

Tots aquests factors donen un escenari positiu que, per bé que és molt millorable, també implica que s'ha evolucionat molt. **"Venim d'un entorn que ha anat evolucionant. És cert que hi ha molta feina per endavant però hi ha una indústria i s'ha millorat molt**. Ara només cal tenir la consciència que aquesta feina només es podrà fer comptant amb tothom: els ciutadans, les empreses, les administracions i els fabricants".

Arribats a aquest punt, la sessió va avançar cap a un debat molt interessant, del qual recollim -en aquesta relatoria- els principals elements:

– Com s'acosengueix l'empoderament dels ciutadans?

Abella va respondre a la pregunta afirmant que "de la mateixa manera que per conduir t'has de treure el carnet, per navegar per internet -encara que sigui gratuït- cal tenir una mínima formació sobre coses que cal fer i coses que no es poden fer". Per això, **"els governs han de fer campanyes i sensibilitzar l'usuari.** Aquesta tasca és senzilla de fer a les escoles però no està tan clar amb el públic en general". En relació a les empreses, cal tenir en compte que a vegades les mesures de seguretat es veuen com un cost massa car.

Roy, va afegir que "cal tenir en compte que els ciutadans cada vegada tenen més eines i més propostes de com resoldre els seus anhels i les seves necessitats". Per això **"cal empoderar el ciutadà però cal fer-ho de veritat, se li ha de donar eines".** Una de les claus importants és que cal adequar-se al ciutadà. Per fer-ho, **"l'administració ha de diferenciar entre protecció i proteccionisme"**. Si les administracions no ho fan bé **"crearem ciutadans hackers que se'ns escaparan"** i això cal fer-ho al mateix temps del fet que "els estats volen ser sobirans i volen construir espais de sobiranies". Per tant, **un dels reptes és fer conviure la sobirania dels ciutadans amb la sobirania que volen tenir els estats**. En definitiva, l'empoderament implica cessió de sobirania i cal veure com es fa.

– I la seguretat?

La cosa menys segura que tenim a les mans és el mòbil. És, segons Abella, una eina perillosa, perquè cal aprendre a utilitzar amb seguretat. A l'actualitat, ja hi ha moltes eines que permeten que sigui més segur. Tanmateix, cal fer campanyes i sensibilitzar. Potser, segons l'expert, **"cal començar campanyes de sensibilització sobre l'ús del mòbil"**.

Un altre dels temes a tenir en compte és el software. La solució sempre són les actualitzacions, que han de ser ràpides i automàtiques.

Per tant, cal conscienciar a l'usuari però també cal fer-lo participar. Segons Roy, el que acabarà passant és que els fabricants de mòbil entendran que els ciutadans volen comprar mòbils segurs i, en conseqüència, faran mòbils compatibles amb tot el que els usuaris utilitzen. En definitiva, **"el mòbil no va ser creat segur i ara haurà d'esdevenir-ho".**

– Formació: en quin punt cal situar la formació perquè estiguem formant ciutadans conscients i empoderats?

Segons Abella, cal parlar de la formació del ciutadà i de la formació dels experts que podran treballar en entorns que poden tenir un creixement exponencial molt gran. Ara mateix, ja s'estan fent campanyes a les escoles però no és suficient. Massa sovint les escoles acaben pensant que formen als alumnes però que caldria formar als pares. "L'administració hi té molt a dir".

Si parlem dels experts, és la part més complicada. Ara mateix, els experts en ciberseguretat els formem a nivell de màster. Per tant, primer has d'haver passat per una enginyeria i per un batxillerat tecnològic. Aquest recorregut és minoritari i per això, caldrien plans d'accions que portessin a l'alumnat cap a aquests camps.

Roy explica, arribats a aquest punt, que el CESICAT té el programa "Internet segura". És un programa paraigua en que actuen diferents professionals, com per exemple els mossos d'esquadra i també professors que imparteixen unitats didàctiques per a l'alumnat i també formació per a les AMPES. I continua: **"Amb el nou pla de govern aquesta és una estratègia de país i la bona notícia és que el govern s'ho ha fet seu".**

Tanmateix, Roy també afirmava que cal veure quins són els hàbits i les conductes que no són segures. Ens hi pot portar la professió, per exemple, però com que "mai no tindrem prou diners per protegir, cal parlar dels hàbits de risc que té la gent".

A l'àmbit escolar, també cal parlar de la motivació, segons Abella. Tot ha evolucionat molt ràpidament i, en canvi, les escoles tenen estructures del segle passat. Totes aquestes temàtiques vinculades a la robòtica, la ciberseguretat, les noves tecnologies.. motiven molt als alumnes. En conseqüència, vol dir que l'escola s'haurà d'adaptar i s'haurà de facilitar un canvi del sistema educatiu. I és que les noves tecnologies han canviat molts sectors: l'escola, però també el món del taxi, per exemple.

– I aquesta formació, ha de ser obligatòria per al treballador públic?

Segons Roy, hauria de ser obligatòria, però també cal ser conscients que mai no tindrem prou diners per poder-ho fer. Per tant, hi hauria d'haver formacions en altres entorns. En aquest sentit, afirma que "el model a seguir no ha de ser el de les formacions en riscos laborals".

– I el ciutadà, es refia de l'administració?

Segons Roy, l'administració haurà d'adoptar fórmules -a l'estil de com han fet es bancs- perquè els ciutadans confiïn en ella, tal com per exemple ja s'ha fet des del cos de Mossos d'Esquadra. Però també està clar que "l'administració no ha de substituir al ciutadà. És ell que s'ha de protegir". Segons el director del CESICAT, **"cal recuperar la confiança del ciutadà perquè sinó costarà molts diners protegir-lo".**

Segons Abella, les administracions tenen molt bons professionals per contribuir a la seguretat de l'usuari i per això, el problema és que **"cal millorar l'experiència de l'usuari".**

– L'administració catalana és segura? I quins són els grans reptes per als propers anys?

Roy explica que s'està treballant per a la creació d'un nou CV per als treballadors públics, fet que contribuirà a la millora. Ara mateix, contribueix el fet que el CESICAT i l'EAPC estiguin al mateix

Departament. Segons ell **“l’administració no és segura perquè si digués que sí que ho és, automàticament ja no ho seria. Això és així perquè la seguretat és una cosa que es degrada”**. En aquest sentit “hi ha moltes coses de l’administració que es fan molt bé, sobretot en relació al perímetre. La prova és que quan s’ha atacat a la Generalitat, s’ha aguantat”.

També cal recordar que l’administració catalana està en plena transformació digital. No en va, el CTTI ha migrat els serveis cap a entorns molt més segurs. Ara bé, també cal tenir en compte que hi ha vulnerabilitats internes perquè és més difícil connectar a la gent de manera segura.

“L’administració catalana té robustesa interna malgrat quan hi ha un virus que afecta mundialment, doncs inevitablement pot afectar, com també ho pot fer el risc que assumeixin usuaris concrets que han decidir utilitzar eines diferents”, afirmava Roy. Tanmateix, l’administració catalana inspira confiança en els serveis que dona. No en va, els seus serveis finalistes inspiren fiabilitat. **“I és que l’administració és altament resilient i per això, cada vegada és més segura”**.

Abella recordava que la seguretat 100% no existeix i per això, cal tenir la capacitat de reaccionar ràpid. En aquest sentit, “els treballadors de l’administració pública han de saber què han de fer davant d’un atac informàtic de la mateixa manera que saben què cal fer quan hi ha un incendi”. Però si parlem de seguretat **el gran repte és la detecció de l’incident**. Cal treballar en el temps previ a l’incident, segons Roy. Per això cal tenir clar que d’aquí a deu anys, hi ha molts sistemes que ara tenim a l’administració que hauran canviat.

Les empreses ara i en el futur s’han de gastar els diners en no ser insegures. **Però també en explicar que són segures**. Segons Roy, la realitat és que abans dèiem que Microsoft era insegura i ara diem que tenen les nostres dades. Això vol dir que no som segurs al 100% però tampoc som insegurs. Aquestes grans empreses han invertit molt en seguretat i en informació. En aquest sentit, **“les administracions hauran de fer el mateix. I a més, hauran de fer gestió del risc, la qual serà clau en el futur”.**

I finalment, és evident que la manera en que ens defensem és diferent de com ho fèiem fa deu anys. Les tècniques de defensa fan que puguis ser igualment vulnerable però que l’administració no ho sigui. “Aquesta és la feina que s’està fent per buscar i estudiar als potencials atacants, la qual permet que, per exemple, que WannaCry bloquegés a Telefònica durant dos dies i, en canvi, no afectés a la Generalitat”, explicava Roy. En aquest sentit, segons Abella **“és vital la innovació, la qual aporta llocs de treball i millora l’economia”.**

El diàleg es va cloure amb la constatació que en matèria de ciberseguretat hi ha molts reptes de futur i amb la seguretat que **“d’aquí a deu anys en continuarem parlant”.**

DIRECCIÓ PÚBLICA, FORMACIÓ, INNOVACIÓ