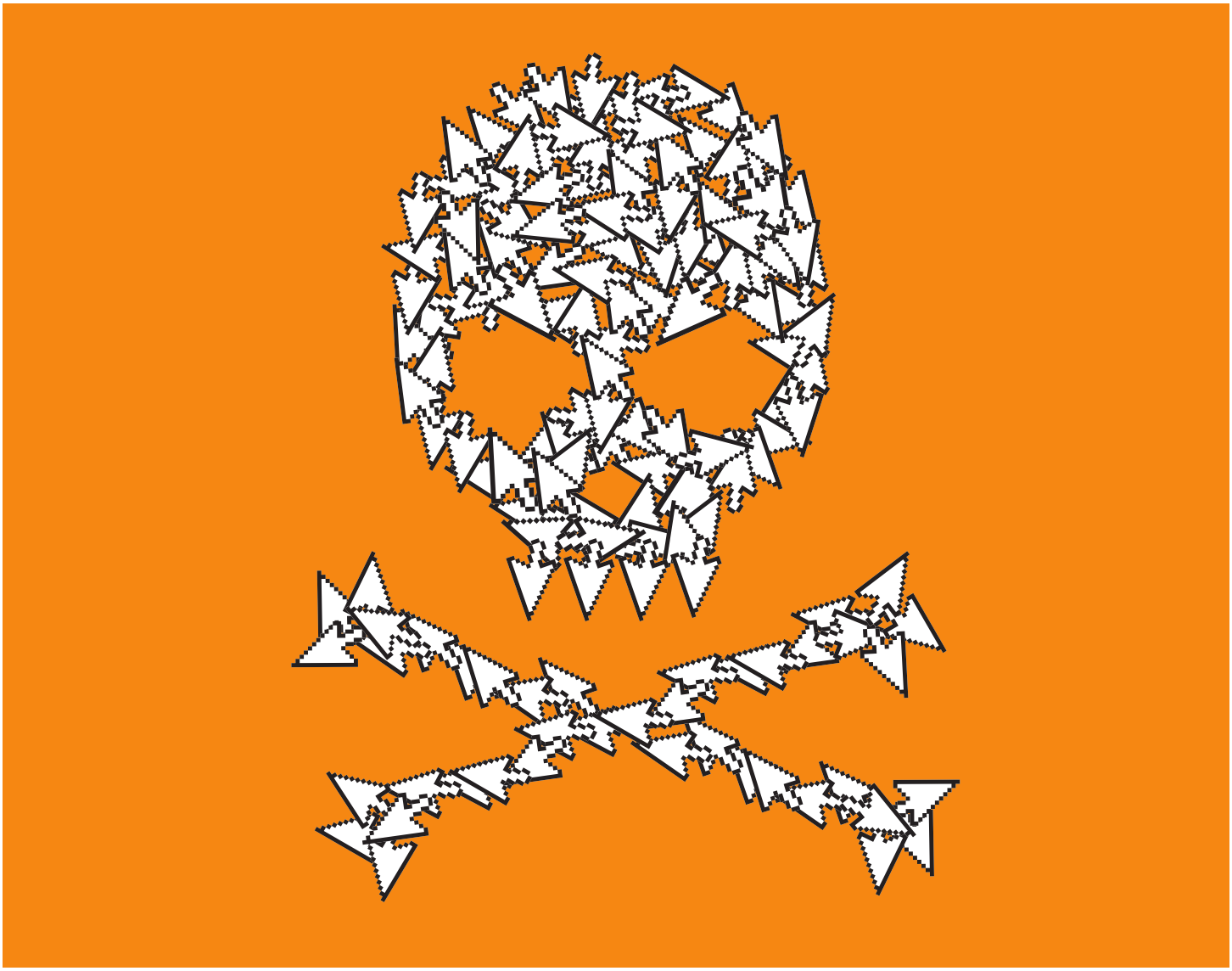
EL PAÍS
El País (Ed. Cataluña) -Quadern
Cataluña
23/10/22
Pr: Semanal (Domingo)
Tirada: 13.417
Dif: 8.106
Cod: 151425522
Pagina: 1
Secc: CULTURA Valor: 16.570,54 € Area (cm2): 743,5 Ocupac: 79,86 % Doc: 1/3 Autor: PER JOSEP PEGUEROLES Num. Lec: 32424



QUINTATINTA

Els perills de l'era digital

Cal acompanyar la transició al medi virtual d'una pedagogia adient, un manual d'ús que ens previngui del que significa aquesta nova manera de ser en el món

PER **JOSEP PEGUEROLES**

Inconsciència digital". El concepte el va proposar la professora Mireille Hildebrandt a *Les tecnologies intel·ligents i els límits de la llei*. Era el 2015. Però la gran majoria fem com si no tinguéssim vida digital. Malgrat que gairebé el 95% de la població es connecta regularment a internet (ho diu l'Institut Nacional d'Estadística), pocs percebem que vivim entre dos mons. Un el coneixem bé. L'altre és l'online i, malgrat que hi desenvolupem gairebé el 50% de la nostra activitat, és molt més desconegut.

Les institucions s'esforcen (i fan bé) a reduir l'escletxa digital. El coneixement de la tecnologia no pot ser un impediment per entrar en aquest metavers, no d'avatars i realitat virtual, sinó més prosaic. Són les noves maneres d'aconseguir cita al CAP, pagar impostos, lligar o matricular-se a la universitat. Però cada cop que afavorim fer per internet allò que fins ara fèiem sense la intervenció de cap aparell informàtic, incrementem la inconsciència. Cal acompanyar la transició al món virtual d'una pedagogia adient, un manual d'ús que ens previngui del que significa aquesta nova manera de fer les coses.

Els ciutadans avui som amfibis, a cavall de dos medis. Ens ens sortim molt bé en superfície, però desconeixem què ens pot passar quan ens capbussem a la web, sigui o no profunda.

Fa poc més d'un any, un atac de *ransomware* va inutilitzar els serveis informàtics de la Universitat Autònoma de Barcelona. El mateix tipus d'atac que aquest octubre ha filtrat 52 gigues d'informació confidencial mèdica de pacients de diferents centres del Consorci Sanitari Integral a Catalunya. Bé sigui com a estudiants de la universitat, bé com a pacients d'un centre de salut, demanem als responsables dels serveis que vetllin per la segu-

Passa a la **pàgina 2**

EL PAÍS
El País (Ed. Cataluña) -Quadern
Cataluña
23/10/22
Pr: Semanal (Domingo)
Tirada: 13.417
Dif: 8.106
Cod: 151425522
Pagina: 2
Secc: CULTURA Valor: 20.702,75 € Area (cm2): 928,9 Ocupac: 99,77 % Doc: 2/3 Autor: PER JOSEP PEGUEROLES Num. Lec: 32424

Ve de la **pàgina 1**

retat de les nostres dades, però no som conscients de la nostra corresponsabilitat en la seguretat dels sistemes informàtics que utilitzem.

A la nostra vida analògica prenem un mínim de precaucions: tanquem la porta amb clau, vigilem la bossa en llocs públics... però el nostre comportament general respecte de la tecnologia es podria considerar irresponsable. La digitalització ens aboca a un entorn perillós. I el més greu: no ho sabem i la nostra actuació pot incrementar molt els perills a què fem front. Com diu Hildebrandt: som uns inconscients.

La inconsciència digital es produeix principalment per desconeixement. També per una falsa sensació d'invulnerabilitat, que ens fa pensar que el que veiem a les notícies no ens pot passar a nosaltres. En paraules de René Serral, responsable acadèmic del pioner Coordinación de Emergencias en Redes Telemáticas (esCERT), "no cal ser ric perquè t'atraquin pel carrer, a internet la majoria som turistes despistats". Tots hi estem exposats, individus, institucions, empreses, estats... Tots els qui tenim una vida digital podem ser víctimes, bàsicament perquè criminals i delinqüents també han fet el salt al món virtual.

● Universos diferents, proteccions diferents

Una de les grans paradoxes que observem en el ciberespai és el tipus de precaucions que prenem els usuaris. Tendim a reproduir les mesures de protecció a què estem acostumats en l'entorn tradicional. Utilitzem antivirus com qui es vacuna (i està molt bé) i usem contrasenyes més o menys com les claus de casa (i amb les directrius correctes, és del tot recomanable), però realitats diferents requereixen funcionaments diferents. No podem protegir una botiga online de la mateixa manera que ho faríem per a un establiment a peu de carrer. O els nostres diners com ho fèiem quan eren de paper.

Amy Zegart, professora a Stanford i assessora de governs en polítiques de ciberdefensa, destaca les cinc grans diferències que hi ha entre el ciberespai pel que fa a riscos i amenaces.

En la manera de pensar tradicional, els qui tenen la tecnologia més sofisticada són també els més poderosos. Entre els exèrcits o la policia, aquells que disposen de les armes més avançades i en un nombre més gran, són també els més forts. En el ciberespai és just al contrari: aquells que tenen més tecnologia són alhora els més vulnerables. Si parlem d'empreses, les més cotitzades a la borsa són les més avançades tecnològicament, i a la vegada són les més vulnerables als ciberatacs. El 2017, el *ransomware* Wannacry, ho va fer evident.

La segona diferència és la superfície d'atac. Al ciberespai és enorme, i indubtablement molt més gran. Quan protegim les nostres cases, empreses o inclús estats, els llocs on concentrem els esforços estan molt ben identificats: assegurem portes i finestres, caixes fortes i cambres cuirassades, protegim fronteres. Identifiquem clarament els llocs vulnerables i actuem proporcionalment per protegir-los.

En el món digital, en canvi, cada nou dispositiu, cada aplicació o programa informàtic, cada connexió a la xarxa, cada funcionalitat avançada que afegim, suposa una nova amenaça. Els punts vulnerables creixen constantment i sense que depengui completament de nosaltres.

Directament i indirectament, estem en mans del correcte funcionament d'una realitat electrònica que no acabem d'entendre i controlar. Perills fortuïts o atacs premeditats que no avisen que ens ho poden trasbalsar tot. Penseu en els cotxes actuals. Ja no és mecànica, el que s'ha de saber per conduir tranquil. L'ordinador del vehicle pot prohibir arrencar-lo o fins i tot impedir que bloquegem les portes, sense que hi tinguem control. Ningú t'explica que no importa que siguis doctor en telecomunicacions: si la bateria deixa d'alimentar l'electrònica, estàs perdut.

Un altre exemple, ara de dependència indirecta: l'errada en l'actualització del programari del sistema de control de trens atura tot el servei ferroviari català, m'impedeix anar a la feina i perjudica l'economia. A més, dona pistes als hackers d'on es troba el punt més feble d'aquesta infraestructura crítica. Imagineu les conseqüències catastròfiques que podrien tenir errades o atacs similars en hospitals, centrals elèctriques o gasoductes.

La nostra ignorància no és només de l'existència del perill, també del fet de ser atacat: la tercera diferència. Les víctimes digitals normalment no sabem que ho som. Són tants els punts vulnerables, i tan gran la nostra inconsciència, que no detectem ni tan sols que ens ataquen. Una invasió de fronteres és evident, un robatori es percep a simple vista. La intrusió d'un ordinador o un mòbil no només és difícil de detectar, sinó que qui ho fa actua de manera sigil·losa per tenir tot el temps del món i poder fer les seves il·legalitats sense ser descobert. Al nostre país tenim exemples famosos com els *spywares* o programes com Pegasus.

L'asimetria de tempos és la quarta diferència. Els exèrcits són conscients que s'estan produint moviments de tropes molt abans que es produeixi un atac. En el moment en què es produeix la invasió, es pot actuar ràpidament i sabem contra qui hem de contraatacar. En el món virtual, els temps d'advertència i decisió s'inverteixen. Estem desinformats i desprevinguts del moment de l'atac, el temps d'advertència es redueix al mínim, són atacs per sorpresa (o indetectables). I, quan es produeixen, no podem reaccionar immediatament, ja que no sabem qui és l'atacant; a més, estarem més enfeinats a mitigar i conèixer l'abast de tot plegat. El temps de resposta és molt més llarg.

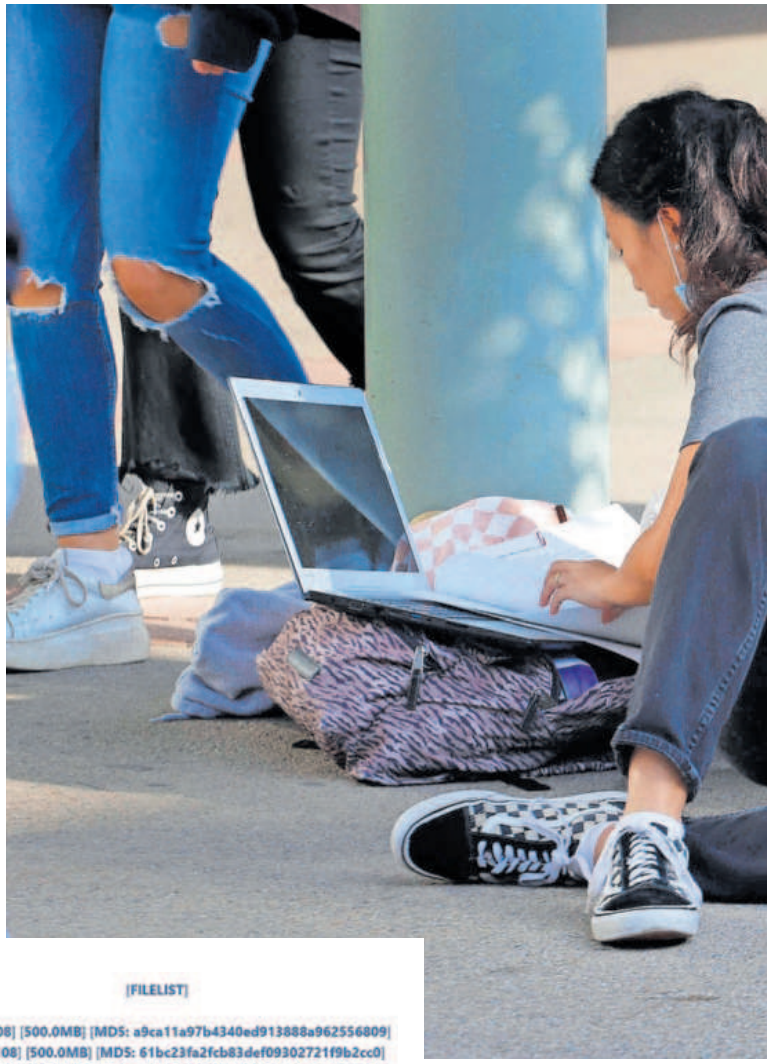
Per últim, en el món analògic deixem la responsabilitat de defensar-nos a un únic agent: aquell que ostenta el monopoli legítim de la força. Policia, exèrcit, empresa de seguretat, depenent del que vulguem protegir. En un o altre dipositem la confiança per protegir-nos. En el món digital, per contra, els límits dels dominis de protecció són difusos. La defensa digital no es pot deixar únicament en mans d'un sol agent. Cal una actuació coordinada de diferents actors, i en tots ells hem de confiar.

● Manual d'instruccions

Què hem de fer si volem ser ciutadans protegits en l'entorn digital? Òscar Esparza, responsable del grup de Seguretat de la Informació de la Universitat Politècnica de Catalunya (ISG-UPC), posa en valor la importància de la divulgació en matèria de ciberseguretat. "No n'hi ha prou que els investigadors estiguem al dia de les amenaces existents i les proteccions necessàries. Als grups de recerca fem la nostra feina, però la societat ha d'estar previnguda, cadascú de manera individual som els primers responsables de la nostra protecció, la primera línia de defensa".

I és que molts dels atacs que es produeixen aprofiten les males praxis dels usuaris per perpetrar-se. És el que s'anomena "enginyeria social", explotar la ingenuïtat humana per fer-li fer clic allà on no l'hauria de fer, endevinar les seves contrasenyes insegures o infectar un USB que es va propagant d'ordinador en ordinador. Fer cas dels consells bàsics d'"higiene informàtica" és fonamental per aquesta primera línia de defensa. Quants de nosaltres usem *passwords* diferents per a comptes diferents i que siguin robustos? Els actualitzem sovint? Usem un gestor de credencials? Tenim activat el doble factor d'autenticació? Tenim l'antivirus i el *firewall* instal·lat i actualitzat? Comprovem la validesa dels certificats digitals dels correus electrònics que rebem i llocs webs que visitem? Evitem compartir dispositius USB? Ens connectem només a xarxes wifi de confiança? Sense una bona primera línia de defensa, posem les coses més fàcils als que volen atacar-nos.

Les empreses i institucions són cada cop més conscients d'aquests riscos, tal com prova l'increment en la demanda de professionals qualificats. Els titulats dels màsters en ciberseguretat, com el de l'Escola de Telecomunicació i la Facultat d'Informàtica de la UPC, en són l'exemple. S'incorporen als equips especialitzats que les empreses creen per fer



[FILELIST]

[Part 1 of 108] [500.0MB] [MD5: a9ca11a97b4340ed913888a962556809]
[Part 2 of 108] [500.0MB] [MD5: 61bc23fa2fcb83def09302721f9b2cc0]
[Part 3 of 108] [500.0MB] [MD5: edc4a555048b133f95732a13a8bfe22e]
[Part 4 of 108] [500.0MB] [MD5: bf426821adcf547e37456e77935c7aa5]
[Part 5 of 108] [500.0MB] [MD5: ebb53c163d788407ba26d02f2c90c999]
[Part 6 of 108] [500.0MB] [MD5: bfb3e66effc357dd74bcc7a2603bbdaa]
[Part 7 of 108] [500.0MB] [MD5: 8c8cebb00ed54bc3fc9d91536135c73a]
[Part 8 of 108] [500.0MB] [MD5: faf27cbdbb2342b48caf1b7a37cf16f3]
[Part 9 of 108] [500.0MB] [MD5: 97efcc2cd044205f8f17a1246b1b370f]
[Part 10 of 108] [500.0MB] [MD5: c60fd78381221e3dc59f1bb9bd8b7c11]
[Part 11 of 108] [500.0MB] [MD5: 41a861f639be2ef09c902f49c35cbc9a]
[Part 12 of 108] [500.0MB] [MD5: 10c32f13de7c9855976a9b743d93cffa]
[Part 13 of 108] [500.0MB] [MD5: 5b77193a43d096ca62449cf01b11e03b]
[Part 14 of 108] [500.0MB] [MD5: 751dbe468d1609ccad2800c7faf01476]
[Part 15 of 108] [500.0MB] [MD5: 7c7bfde221879669e7466dc5bb0f819c]
[Part 16 of 108] [500.0MB] [MD5: 69ff0fa0fffdf797f3678845b7d0439e]
[Part 17 of 108] [500.0MB] [MD5: e36b6bd5f46ed28c032bc1d298653b2e]
[Part 18 of 108] [500.0MB] [MD5: 680d28f7741f2983d4d59b94ba5b3902]
[Part 19 of 108] [500.0MB] [MD5: c902f9d3f3019c5d0d742e064e6112f9]
[Part 20 of 108] [500.0MB] [MD5: cdbbd24d71b896d167ce7c8390ff3ed3]
[Part 21 of 108] [500.0MB] [MD5: a5d1a5036efd07597fe617ec8004985f]
[Part 22 of 108] [500.0MB] [MD5: 120faa677c260ed69141183e904f15aa]
[Part 23 of 108] [500.0MB] [MD5: 59b5228b1a376c35a5dd51623cdcff1d]
[Part 24 of 108] [500.0MB] [MD5: 8c20bae61e75e55e22e87df1af900017]
[Part 25 of 108] [500.0MB] [MD5: 6a25138453bc4ba7de4a06ff45f515b6]
[Part 26 of 108] [500.0MB] [MD5: e0d736c1d45194a1cfbff5128714c553]
[Part 27 of 108] [500.0MB] [MD5: 8d066b64fb370b952dca6284fc851f5b]
[Part 28 of 108] [500.0MB] [MD5: 5a7812f61c7dd06ebd2fff0f6be872d9]
[Part 29 of 108] [500.0MB] [MD5: b282e851d99324d197516d65a8295ae5]
[Part 30 of 108] [500.0MB] [MD5: 48f3bf2d5d9754e3dd439f9bd64e8b4e]

La inconsciència digital es produeix per desconeixement. També per una falsa sensació d'invulnerabilitat, que ens fa pensar que el passa no ens pot passar a nosaltres. CRISTÓBAL CASTRO

EL PAÍS
El País (Ed. Cataluña) -Quadern
Cataluña
23/10/22
Pr: Semanal (Domingo)
Tirada: 13.417
Dif: 8.106
Cod: 151425522
Pagina: 3
Secc: CULTURA Valor: 20.740,19 € Area (cm2): 930,6 Ocupac: 99,95 % Doc: 3/3 Autor: PER JOSEP PEGUEROLES Num. Lec: 32424

front als perills digitals: la segona línia de defensa.

Els SOC (Security Operation Center), nom que reben aquests equips dins les empreses, són cada cop més importants. Actuen segons l'esquema Blue Team: disposen d'eines de protecció digital davant d'eventualitats i actuen de manera preventiva. Qualsevol institució o empresa altament digitalitzada hauria de tenir-ne un. Els Blue Teams, per estar preparats, necessiten els Red Teams: els que simulen un atac de manera controlada, intentant explorar els punts febles que puguin trobar abans que siguin aprofitats per usuaris maliciosos. Els hackers ètics són aquests: els qui exploten, sense fer mal, tots els *bugs* o forats de seguretat que existeixen en l'entorn digital. La tercera línia de defensa.

Diversos estudis indiquen que de mitjana trobem de 20 a 30 errades de seguretat cada mil línies de codi de programa informàtic. Errades que són forats en la nostra tanca de seguretat, susceptibles de ser aprofitades per comprometre la nostra seguretat. Els exploradors d'aquestes errades, que intenten colar-se dins la tanca, són els membres del Red Team. Els guàrdies de seguretat que van patrullant per impedir-ho són el Blue Team.

Usualment, aquests serveis "d'atac controlat" es demanen a experts externs. Empreses com INCIDE Digital Data, pionera i molt coneguda al sector, no només ofereix aquestes auditories Red Team, també ofereix Blue Teams externalitzats, per si l'empresa no els vol o no els pot tenir internament. Abraham Pasamar, el seu CTO, explica que la bona coordinació entre els dos equips és bàsica. Ells van ser dels primers a incorporar la metodologia porpra (Purple Team, combinació de vermell i blau): atacants (simulats) i defensors treballant plegats per bastir les "tanques virtuals" més fortes possibles.

La tercera línia de defensa també pot ser governamental. Tenim experts treballant per la nostra seguretat en grups especialitzats dels Mossos d'Esquadra, de l'Agència de Ciberseguretat de Catalunya (ACC), l'Instituto Nacional de Ciberseguridad (INCIBE) i el Mando Conjunto del Ciberespacio (depenent de l'exèrcit). Com deia Zegart, no podem deixar la seguretat digital a un sol agent. La cooperació i col·laboració de les diferents peces de l'engranatge per protegir els actius digitals és clau, des del ciutadà fins a l'estat. I l'èxit més gran és que no els notem. Quan ens adonem que hi són, és que hem detectat que estem sent atacats. Perquè, tot i els múltiples nivells de protecció, els atacs no es poden evitar.

● I llavors?

Actuar ràpidament: hem d'acudir als especialistes de Resposta a Incidents. Aquests, igual que fa un metge quan li arriba un pacient a urgències, prioritzen aturar l'hemorràgia i estabilitzar-lo per evitar que el mal sigui més gran. Sebastien Kanj, especialista en respostes a incidents de *malware*, explica que molts cops l'entrada a urgències s'hauria pogut evitar si hi hagués hagut les tres línies de defensa. Malauradament, encara queda molta pedagogia per fer, però tot i així, quan s'arriba a aquest estadi, encara es poden salvar moltes coses.

Cada cop hi ha més casos de companyies amb "dades segrestades", a les quals demanen que paguin un rescat

Les empreses més cotitzades a la borsa són les més avançades tecnològicament i les més vulnerables als ciberatacs

La intrusió és difícil de detectar pel qui és atacat, com passa amb els 'spywares' o programes com Pegasus

L'atac més freqüent avui dia és el *ransomware*. Moltes empreses no ho fan públic, però cada cop hi ha més casos de companyies amb "dades segrestades", que no poden seguir amb la seva activitat i se'ls demana que paguin un rescat. Com en les urgències, haver-se enfrontat prèviament a situacions similars ajuda els professionals a encarar bé la reacció per mitigar les conseqüències. Tenir còpies de seguretat actualitzades és bàsic per minimitzar l'impacte de l'atac.

I tot això es pot fer impunement? No. La llei ens protegeix. La mala notícia és que, com dèiem abans, no és evident identificar el responsable. En la invasió de territori ucraïnès, tristament recent, els satèl·lits van detectar moviments de tropes de l'exèrcit rus molt abans de l'atac. Alguna cosa estava passant, sabíem perfectament qui era. En el mateix període es van detectar nombrosos ciberatacs tant a Ucraïna com a països de l'OTAN. Les notícies informaven que es tenia la "sospita" de l'autoria, però la certesa és més difícil d'aconseguir. En l'àmbit de la determinació de les causes i responsabilitats entra en joc la pràctica forense digital.

● És greu, doctor?

Un forense digital, com un metge forense, entra en escena quan el d'urgències ja ha fet la seva feina. En el millor dels casos, el pacient està estable a l'habitació, i llavors un altre professional investiga les causes per evitar recaigudes. En el pitjor dels casos, l'oficina del forense és el dipòsit de cadàvers i la seva feina serà determinar les causes de la defunció i ajudar a trobar l'assassí, si es tracta d'un homicidi.

La inconsciència digital aquí agafa un altre significat. Igual que no sabem tot el que depèn del món virtual, tampoc som conscients de l'enorme quantitat de pistes que anem deixant quan actuem dins del ciberespai. Gairebé tota interacció amb un sistema electrònic o informàtic deixa rastre. Afortunadament per als investigadors digitals, els usuaris van deixant empremtes a l'escena del crim. Si el malfactor no ha pres la precaució de posar-se guants, o no sap que l'estan gravant, és fàcil trobar evidències del que ha passat en un atac informàtic, i en última instància, trobar proves per saber qui és el culpable i portar-lo a la justícia.

Un forense digital és un expert que sap quines són les pistes que ens dona un sistema digital i és capaç de reconstruir l'acció per explicar-la al jutge. Potser els casos més sofisticats no es poden resoldre, però la majoria de delictes informàtics els cometen usuaris sense coneixement profund de la tecnologia. Inconscients de les traces que deixen, descuiden esborrar-les. Un forense digital és capaç de posar-les sobre la taula i inclús recuperar les que s'han esborrat de manera matussera.

És habitual que el forense digital actuï coordinadament amb l'equip de resposta d'incidents (equips DFIR: *digital forensics and incident response*), de manera que no només s'aturi l'hemorràgia sinó que a la vegada s'impedeixi que s'esborrin proves i es vagin recollint totes les evidències possibles per a l'anàlisi posterior. A més, les dades recollides serveixen per enfortir les primeres línies de defensa, tancant el cercle de protecció digital.

De ciberdelictes concrets (espionatge industrial, fuga d'informació, *cyberbulling*, sextorsió...) en podríem parlar molt. De fet, se n'han fet sèries de televisió. De totes maneres, el primer que hem de fer per protegir-nos és ser conscients que tots podem ser víctimes. Cal reduir la inconsciència digital i posar en acció les diferents línies de defensa, des de la individual fins a la col·lectiva, coordinadament. Cal saber que, si som atacats, la llei ens protegeix i es pot treballar per determinar els responsables.