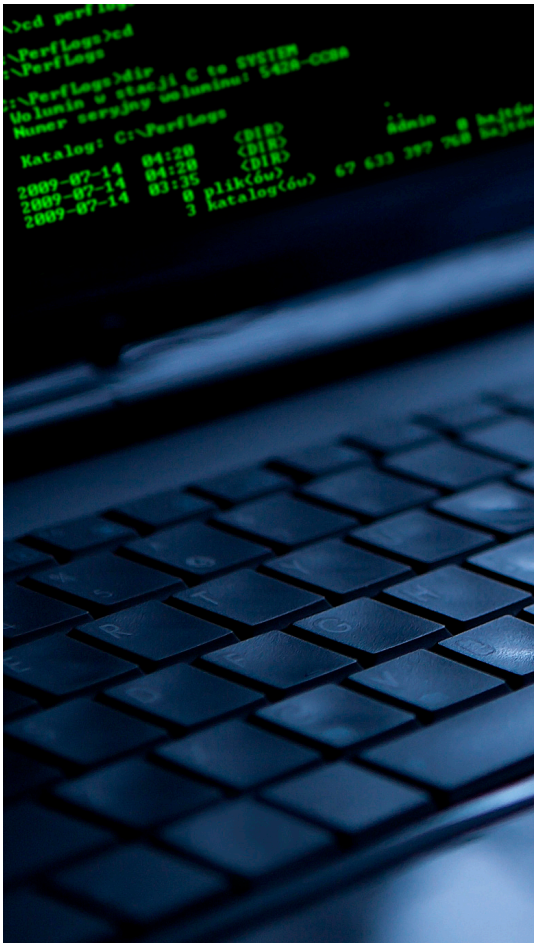
El mite de la ciberseguretat



En la informàtica, la seguretat completa és inexistent. I, en alguns casos, genera situacions força contradictòries. Una encriptació menor dels missatges, per exemple, podria haver evitat els atemptats recents a Londres i Sant Petersburg. El debat és a taula.

El concepte seguretat informàtica és una contradicció. Només durant l'any passat es van donar tres esdeveniments que ho demostren. D'un costat, 81 milions de dòlars del banc central de Bangla Desh van ser robats per lladres cibernètics. Alhora, la companyia Verizon, de telecomunicacions, va adquirir Yahoo per 4.800 milions de dòlars després que el portal d'internet patís episodis de pirateig de les seves dades. També és coneguda la ingerència de furoners russos en les eleccions estatunidenques.

El mercat negre d'extorsió informatitzada, contractació de pirates cibernètics i béns digitals està en auge. Per tant, el problema empitjorarà. Els ordinadors ja no treballen *només* amb dades abstractes de targetes de crèdit. També tenen incidència directa sobre el món real dels objectes físics i del cos humà. Avui, un cotxe és un ordinador amb rodes i un avió és un altre ordinador, però amb ales. L'arribada de "l'internet de les coses" implica la necessitat de disposar d'ordinadors a tot arreu per fer funcionar els senyals de carretera o els escànners de ressonància magnètica. Cap indici pronostica que aquests dispositius seran més fiables que els ordinadors d'avui. Els pirates han demostrat que poden controlar remotament cotxes i marcapassos.

És temptador creure que els problemes de seguretat es poden resoldre amb la màgia tecnològica i apel·lant a una vigilància més intensa. I és cert que moltes companyies encara no es prenen seriosament el tema de la seguretat. Tot plegat requereix una mena de paranoia cultivada inexistent en les empreses no relacionades amb tecnologia. Les companyies de tot tipus haurien de sumar-se a iniciatives com els *bug bounty programmes*, que recompensen els pirates ètics per trobar vulnerabilitats i resoldre-les abans que ningú se n'aprofiti.

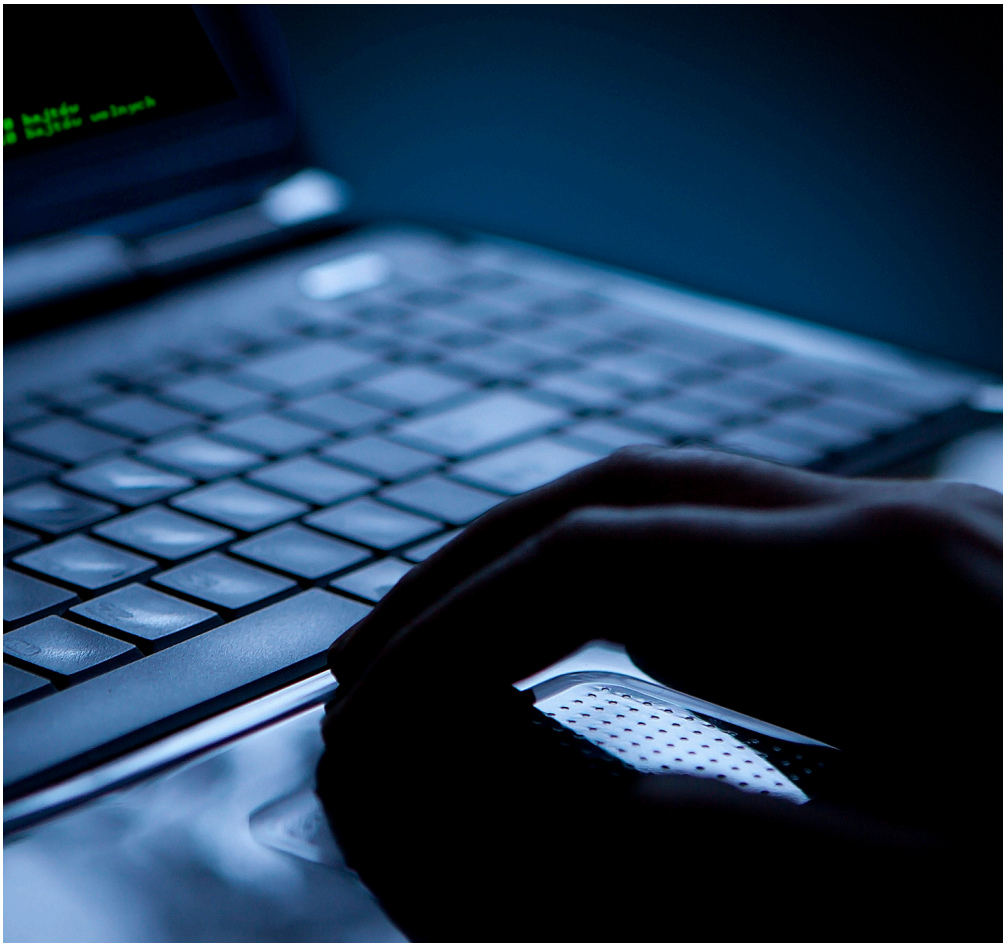
La complexitat dels *softwares*, però, entrebanca la possibilitat de fer ordinadors completament segurs. Google, per exemple, ha de gestionar vora dos mil milions de línies de codi font, cosa que fa que els errors siguin inevitables. Cada programa té una mitjana de catorze vulnerabilitats separades, i cadascuna és una possible entrada il·lícita. Aquestes deficiències són el reflex de la història d'internet, on la seguretat sempre ha tingut un paper secundari.

Deixar les finestres obertes

La batalla, però, encara no s'ha perdut. El risc de frau i els accidents de carretera no es podran eliminar per complet, però les societats han desenvolupat maneres de gestionar aquests riscs: des de regulacions governamentals relacionades amb la responsabilitat jurídica a assegurances per incentivar les bones pràctiques.

Convé començar per la regulació. La gran prioritat dels Governs és evitar que la situació empitjori i, en aquest sentit, cal incidir sobre l'encriptació. Disminuint-la s'hauria tingut més control sobre atacs terroristes com els patits de fa poc a Sant Petesburg i Londres. Reduir l'encriptació implica un control més alt dels serveis de seguretat sobre els individus, i per això és impossible realitzar aquesta pràctica només sobre els terroristes: aquest exercici protegeix també programes de missatgeria com WhatsApp, transaccions bancàries o identitats en línia. És, per tant, el millor tipus de seguretat que se'ns pot oferir.

La següent preferència és establir una regulació bàsica per a productes. La manca d'experiència obstaculitzarà la capacitat dels usuaris de protegir-se, i per això els Governs haurien de promoure la



salut pública de la informàtica. Podrien insistir perquè els dispositius que estiguin connectats a internet s'actualitzin quan es detecti qualsevol tipus d'amenaça. També hi ha l'opció d'obligar els usuaris a canviar els seus *usernames* i contrasenyes. La normativa vigent en alguns estats nord-americans pot obligar les companyies a informar quan les empreses o els seus productes són atacats, una solució que fomenta la solució del problema.

Qui va de pressa plega tard

Establir una regulació mínima, però, no és suficient: només és un incentiu per prendre's la seguretat més seriosament, tot i que no resol la incapacitat d'un usuari per protegir-se. Normalment, a més, els danys causats per un pirata no afecten només el propietari del dispositiu afectat. Els *botnets*, xarxes d'ordinadors que, una vegada són infectats, poden ser controlats remotament sense el permís del propietari, en són un exemple. En aquest cas poden sortir perjudicats equips de sobretaula, *routers* o bombetes intel·ligents. El subjecte damnificat seria col·lectiu: una empresa, una institució o qualsevol entitat que funcioni amb una xarxa conjunta.

La intenció és que la indústria del *software*, després de dècades d'omissió de responsabilitats pels danys causats sobre els productes venuts, es faci càrrec d'aquests greuges. Estratègies dissenyades com la innovadora de Silicon Valley, "vés ràpid i trenca les coses", només tenen cabuda si les companyies gaudeixen de relativa llibertat per posar nous productes a la venda quan encara necessiten perfeccionament. Aquesta possibilitat serà irrellevant en poc de temps, ja que els ordinadors s'estenen a productes amb responsabilitats legals com cotxes o productes domèstics i la indústria s'haurà d'enfrontar a les legislacions vigents.

Les companyies han de ser conscients que, si els tribunals no implementen les qüestions de responsabilitat, l'opinió pública s'encarregarà de fer-ho. Molts experts en seguretat informàtica han establert similituds amb la indústria estatunidenca automobilística dels anys 60, que també va ignorar els sistemes de seguretat durant dècades. El 1965, Ralph Nader va publicar *Unsafe at any speed* ('Insegur a qualsevol velocitat'), un èxit editorial que exposava i criticava l'actitud tan relaxada d'aquest sector. L'any següent, el Govern dels EUA va fer un canvi dràstic i implementà noves normes sobre els cinturons de seguretat, reposacaps, etc. Ara, imaginin el clam per una legislació correcta després de la primera mort infantil en un accident de cotxe sense conductor.

Afortunadament, el petit però creixent mercat de les assegurances cibernètiques ofereix la manera de protegir els usuaris, tot preservant la capacitat de la indústria per innovar. Per això, una empresa que disposi de productes en mal funcionament o susceptibles d'atacs serà incitada perquè prengui mesures. D'altra banda, una companyia amb un comportament adequat però afectada pels atacs informàtics podrà demanar ajuda per evitar la fallida.

I és aquí on es podrien negociar algunes excepcions de responsabilitat. Hi ha precedents: quan la quantitat de demandes contra les companyies d'avionetes estatunidenques era excessiva i amenaçava amb la fallida d'aquesta indústria als anys 80, el Govern va canviar les lleis, i va alliberar les companyies de responsabilitats sobre productes fabricats anteriorment.

La seguretat informàtica mai no s'ha pres tan seriosament com requereix la situació. Aquesta és una de les raons per les quals avui ens trobem amenaçats. Quan internet encara era una novetat, s'admetien els riscs dels virus i de la pirateria com a conseqüències normals de l'ús de la xarxa. Ara, la seva importància fa imprescindible un canvi d'actitud de la gent i de les empreses que no només exigirà solucions tècniques: també demandarà grans inversions econòmiques.•

Traducció de Vicent Sanchis Puerto