CEA MAI MARE PANĂ INFORMATICĂ DIN ISTORIE. CÂTEVA CONCLUZII

Autor: Petru Dimitriu | 31 iulie 2024

Dacă trecem cu vederea ultimele valuri ale pandemiei de COVID-19, Crăciunul anului 2021 a fost, pentru majoritatea, unul obișnuit. Mulți, posibil majoritatea programatorilor profesioniști, își vor aminti, însă, că în acele zile, cu două săptămâni înaintea Crăciunului, în cercurile IT din toată lumea s-a dezlănțuit haosul. În aproape cel mai prost moment posibil din anul calendaristic fusese descoperită cea mai gravă vulnerabilitate de securitate informatică de până atunci. Denumită *Log4Shell*, ea a fost, de fapt, o scăpare de proiectare într-un modul informatic folosit pe scară foarte largă care permitea unui atacator să execute cu ușurință de la distanță practic orice operațiune pe dispozitivul țintă.

Odată făcut anunțul descoperirii acestei vulnerabilități uriașe, companiile IT din întreaga lume s-au dat peste cap să-și actualizeze cât mai repede infrastructurile IT pentru a nu fi ținte imediate ale atacurilor. Site-uri de tot felul, servicii web, jocuri, dispozitive *smart* – nimic nu a scăpat. Pentru a înțelege magnitudinea acestui eveniment, merită să menționez că producătorii de dispozitive au emis actualizări urgente de securitate pentru *toate* telefoanele Android aflate în perioada de suport, în ceea ce, pentru utilizatorii obișnuiți a apărut, probabil, un *update* ca oricare altul, însă pentru multe echipe de programatori din toată lumea a fost doar un efect superficial al unui adevărat infern în plină desfășurare. La doar câteva zile după anunț, milioane de dispozitive care nu primiseră încă actualizarea de securitate, din indolența sau naivitatea deținătorilor, au fost atacate cu succes de hackeri; poate vă amintiți mesaje primite de la prieteni de pe Facebook cu un *link* dubios și un mesaj îngrijorat: „Tu ești cel care apare în video?”, care s-au precipitat cu varii frecvențe până spre sfârșitul anului 2023.

Dacă nu sunteți programator, probabil că relatarea anterioară vă apare drept o noutate, pentru că, în România, deși Directoratul Național de Securitate Cibernetică și-a făcut datoria conștiincios și la timp[1], mass-media a ignorat subiectul aproape complet până când atacurile s-au întețit suficient de mult ca să atragă atenția.[2] Această ignoranță este

întrucâtva firească, având în vedere că universul IT de astăzi este în bună măsură suficient de ermetic și capabil de autoreglare încât să nu solicite atenția publicului în cea mai mare parte a timpului. Cu alte cuvinte, fără să înțelegem ce se întâmplă „sub capotă”, ne-am obișnuit că, în general, calculatoarele, telefoanele, programele cu care lucrăm zi de zi „pur și simplu merg” – o conexiune la internet fiind suficientă pentru ținerea la zi a tuturor produselor digitale.

Reversul medaliei acestei fericite separări aproape totale a responsabilităților între utilizatori și companiile producătoare s-a văzut cu vârf și îndesat acum două săptămâni. Cea mai mare pană IT din istorie a refulat în toată lumea, prăbușind angrenaje informatice întregi unul câte unul, ca piesele de domino. Au fost afectate aeroporturi și instituții financiare și medicale din toată lumea, iar la Sky News știrile s-au citit timp de o oră direct de pe foi printate, fără burtiere, fără grafică și fără reportaje video. Milioane de calculatoare cu sistemul de operare Windows n-au mai pornit, afișând infamul „ecran albastru al morții” ce anunță o eroare irecuperabilă. Confuzia a trenat timp de câteva ore, timp în care pana a fost descrisă ca fiind „a produselor Microsoft”, ca mai apoi să fie reperată ca venind, în mod ironic, de la o actualizare a unui foarte popular program de securitate întreținut de compania CrowdStrike.

Fără a intra în multe detalii tehnice, acest efect devastator a fost posibil deoarece aplicația de securitate, pe nume *Falcon Sensor*, își inserează propriul cod informatic atât de intim printre procesele sistemului de operare Windows pentru a-și îndeplini sarcinile, încât o eroare precum cea de acum două săptămâni pur și simplu incapacitează întregul sistem. Deoarece calculatoarele afectate nu se mai puteau conecta la internet pentru a primi o eventuală actualizare de corectare a erorii, depășirea acestui impas a necesitat efectuarea în manieră fizică a unor operațiuni pe calculatoarele afectate.

Eroarea introdusă[3] în codul firmei CrowdStrike în acea dimineață fatidică – pe care nu o voi explica aici pentru a nu transforma articolul într-unul tehnic – nu reprezintă un atac informatic (cel puțin, nu în sensul clasic), ci este o greșeală de programare pe cât de gravă, pe atât de ridicolă. Studenții în științele calculatoarelor se lovesc de această eroare negreșit în anul I de studiu (cel puțin în România), așadar este o eroare banală, arhicunoscută. De fapt, mă pot „lăuda” că eu însumi am picat mai mulți studenți pentru introducerea inadvertentă a acestei erori la testele și examenele pe care le-am supervizat la disciplina Programarea Calculatoarelor (și sper, cu această ocazie, că orice sentimente negative ale foștilor mei studenți față de exigența mea s-au risipit).

Până la intervenția fizică a IT-iștilor care să readucă situația la normal, multe dintre instituțiile afectate au reușit să funcționeze în continuare, pe modul de avarie, punând în mișcare proceduri manuale, de redundanță, precum validarea manuală a cărților de îmbarcare în aeroporturi. Treptat, efectele au fost atenuate, funcționarea calculatoarelor afectate a fost restabilită, însă urmările încă trenează, iar prețul acțiunilor CrowdStrike

s-a înjumătățit.

Rămâne, pentru moment, un mister cum a fost posibil ca o greșeală de programare atât de devastatoare să fie propagată nestingherit de o companie de un renume semnificativ precum CrowdStrike în condițiile în care lansările în producție ar trebuie să parcurgă, de regulă, procese bine puse la punct de testare, tocmai pentru evitarea incidentelor. O necunoscută la fel de mare este de ce a fost emis acest *update* într-o zi de vineri, în care uzanțele din interiorul companiilor IT spun că nu se fac lansări de noi versiuni, pentru a nu pune în pericol liniștea angajaților și a clienților în timpul weekend-ului. În așteptarea unor explicații oficiale ample, se cuvine să extragem, între timp, primele învățăminte în urma acestui moment de cumpănă a infrastructurii IT globale.

Un prim aspect la care acest incident ne-a atras atenția vrând-nevrând se referă la riscul ascuns de a sprijini funcționarea angrenajelor informatice pe produse software care, în ultimii ani, s-au transformat, în fapt, în servicii – atât de puternic încât utilizatorilor obișnuiți li se retrage însăși posibilitatea de a refuza actualizările software de pe propriile lor dispozitive. Este, practic, o concretizare punctuală, dar exacerbată a avertismentului repetat în manieră obsedantă de excentricul programator american Richard Stallman, care a atras atenția că folosirea software-ului cu sursă închisă echivalează cu o restrângere benevolă a libertății.

Cei mai mulți dintre noi trăim iluzia că deținem cópii ale programelor cu care suntem obișnuiți să lucrăm zi de zi, când, de fapt, noi suntem deținătorii unor simple *licențe*, care ne permit să utilizăm „produsele” software la discreția companiilor care le dezvoltă, doar în termenii și condițiile kilometrice pe care, bineînțeles, le acceptăm bifând mecanic. În același timp, este adevărat și că alternativa este, la acest moment, nefezabilă pentru cei mai mulți dintre noi – multe programe alternative gratuite și cu sursă liberă nu oferă toate capacitățile omologilor cu licență proprietară, iar mulți dintre utilizatori se complac, sau de nevoie, sau din lene, în propria rigiditate psihologică, fiind reticenți la înlocuirea programelor familiare, învățate, poate, cu multă bătaie de cap.

În aceeași cheie, ca și breșa descoperită în decembrie 2021, acest eveniment ne-a demonstrat empiric riscurile asociate oligopolului tehnologic, care nu este nici măcar generat în mod obligatoriu de capitalismul deșănțat, așa cum ar fi unii tentați să declame – incidentul de acum doi ani referindu-se la o componentă de software liber. Asigurarea unor mecanisme de redundanță, atât la nivelul arhitecturilor *software* care îi preocupă pe programatori și pe arhitecții IT, cât și la nivelul propriilor rutine de lucru cu dispozitivele digitale, este soluția cea mai bună în acest caz. Mobilizarea aeroporturilor și spitalelor din toată lumea care au revenit cu succes pentru scurt timp la lucrul cu documente de hârtie scrise de mână, este lăudabilă și demonstrează că este imperios necesar ca abilitățile ce implică decizii umane și manualitate să nu intre în desuetudine.

Mai concret, cred că este timpul să învățăm cu toții să ne depanăm (sau măcar să diagnosticăm) problemele propriilor dispozitive, așa cum suntem învățați să facem cu automobilele la instructajul din timpul școlii de șoferi; să ne procurăm și un sistem de operare alternativ: dacă folosim Windows, să ne familiarizăm și cu MacOS sau Linux; dacă folosim Office, să încercăm și LibreOffice; dacă folosim Photoshop, să avem habar și de GIMP; să nu mai considerăm drept apanajul pasionaților depanarea de bază a calculatoarelor (în frunte cu celebra „reinstalare a Windows-ului” – devenit, iată, substantiv comun); să stocăm informațiile digitale importante în mai multe cópii de rezervă (pe principiul „dacă nu are *backup* înseamnă că nu e important”); să ținem cópii „tari” (printate) ale documentelor extrem de importante și, nu în ultimul rând, să nu uităm să scriem de mână. Cu alte cuvinte, trebuie să trăim pregătiți, împăcați în permanență cu gândul că o pană informatică sau un incident electronic sunt întotdeauna posibilități reale și care trebuie să fie gestionabile de aproape oricine, cel puțin în spațiul său personal. Necesitatea acestei „vigilențe tehnologice” nu ține de o formă de paranoia, după cum tocmai ne-a fost demonstrat.

Este reconfortant că astăzi putem delega tot mai multe activități tehnologiei, dar proliferarea chatboților și arhitecturilor recente de inteligență artificială ne pune înainte o nouă tentație, fără precedent: delegarea gândirii creative. Într-un scenariu tragicomic, exagerat, dar totuși coșmaresc, să ne imaginăm cum ar arăta o lume într-un viitor îndepărtat în care oamenii și-au delegat cu toții gândurile lui ChatGPT, dar acesta a intrat, la un moment dat, în pană… de idei. Să nu fie!

NOTE

1. „Vulnerabilitate critică de tip zero-day afectează Log4j, o bibliotecă Java utilizată la scară largă” în dnsc.ro, publicat la 12 decembrie 2021, disponibil la adresa https://dnsc.ro/citeste/alerta-vulnerabilitate-zero-day-log4j-java , accesat în 30 iulie 2024; ↑
2. „ «Tu ești în acest video?» România, ținta principală a unui atac informatic de peste 100.000 de sms-uri cu linkuri infectate” în observatornews.ro, publicat la 27 ianuarie 2022, disponibil la adresa https://observatornews.ro/tehnologie/tu-esti-in-acest-video-romania-tinta-principala-a-unui-atac-informatic-de-peste-100000-de-smsuri-cu-linkuri-infectate-456260.html , accesat în 30 iulie 2024. ↑
3. Pentru cititorii tehnici, fac precizarea că eroarea de programare este dereferențierea unui pointer invalid, așa cum a arătat programatorul Zach Vorhies pe rețeaua X, la adresa web: https://x.com/Perpetualmaniac/status/1814376668095754753/photo/1 . ↑

Imagine: Unsplash