Spune-mi cine ești ca să-ți spun cum să-ți protejezi datele

A.Cine ne atacă?

Siguranța noastră online este azi parte atât din discuțiile politice, cât și cele despre tehnologie. Dacă ar fi să răspundem la întrebarea “care e cea mai mare amenințare la adresa siguranței noastre în mediul online”, răspunsul s-ar putea să pară evident doar pe moment.

De-a lungul anilor, fiecare din următoarele răspunsuri a părut de la sine înțeles:

- autoritățile statului sunt principala amenințare, pentru că se pot folosi de puterea lor politică pentru a permite supravegherea în masă a comunicațiilor, pot pune presiune pe companiile din sectorul privat să ofere datele clienților sau pot chiar să naționalizeze servicii precum accesul la Internet și telefonie, împreună cu întreaga infrastructură;
- marile companii sunt principala amenințare, pentru că ele prelucrează și stochează toate datele noastre din mediul online și, desigur, pot să mintă în legătură cu faptul că nu se folosesc de datele noastre pentru a ne influența comportamentul și a-și mări profitul;
- hackerii sunt cei mai periculoși pentru că se pot folosi de neajunsuri ale tehnologiei pentru a exploata sistemele de operare, alte programe software sau protocoalele pe care le folosim și ne pot sustrage date și pot distruge inclusiv infrastructură fizică folosindu-se de viruși sau alt tip de malware.

Fiecare dintre aceste răspunsuri este valid și, pentru a demonstra asta, merită să facem o scurtă incursiune în istoria recentă a Internetului.

1. Când statul vrea să afle informații cu orice preț

Acum mai bine de zece ani, **scandalurile legate de supravegherea în masă**, disproporționată, facilitate de tehnologie au pus subiectul siguranței pe Internet pe buzele tuturor. Începând cu 2013, mulțumită avertizorului de integritate american Edward Snowden, întreaga lume a aflat despre eforturile pe care Agenția Națională de Securitate (NSA) din America le face pentru a intercepta, stoca și analiza date personale ale propriilor cetățeni. NSA colecționa date de la operatori de telefonie (Verizon), iar de la echivalentul său britanic (GCHQ) primea datele pe care această agenție le obținea accesând direct cablurile de fibră optică de pe fundul oceanului. Poate cel mai dureros punct al revelațiilor din documentele obținute de Snowden este programul Prism, care indica faptul că NSA-ul primea informații și de la mari companii de tehnologie precum Google, Apple sau Meta. Conform documentelor, acest parteneriat cu companiile permitea NSA-ului să colecteze materiale, inclusiv istoricul căutărilor, conținutul e-mailurilor, transferurile de fișiere și conținutul chat-urilor.

Desigur, merită repetat că aceste informații sunt din anul 2013. Companiile au negat vehement că oferă datele utilizatorilor și conținutul conversațiilor acestora unei agenții guvernamentale în lipsa unui mandat judecătoresc. Între timp, tehnologia în sine a avansat, iar criptarea end-to-end este cel mai puternic garant, în momentul de față, al siguranței datelor digitale.

În prezent, însă, vedem că guvernele unor țări și chiar și Comisia Europeană nu au renunțat la dorința lor de a avea acces la datele noastre. Mai multe proiecte legislative care subminează criptarea end-to-end ori au trecut și sunt în vigoare, ori se încearcă ca ele să treacă. În Regatul Unit, Online Safety Bill este deja o legislație în vigoare. În Statele Unite ale Americii, KOSA Act și alte propuneri legislative similare, încearcă să oblige companiile să renunțe la criptarea datelor și comunicațiilor. În Uniunea Europeană, un proiect de regulament supranumit #ChatControl caută să facă obligatorie scanarea tuturor comunicațiilor cetățenilor direct pe dispozitivele lor.

Când o putere nu poate obține date cu frumosul, poate da naștere unui alt tip de scandal, cum este cel legat de programele software de tip **spyware**. Cel mai răsunător nume în acest domeniu este Pegasus. Creat de compania israeliană NSO Group, acest software poate să infecteze de la distanță dispozitivul mobil al unei persoane și să îi extragă toate datele stocate în acesta. Mai mult, poate folosi camera și microfonul dispozitivului pentru a supraveghea în timp real persoana respectivă.

Din 2020 până în prezent, jurnaliștii de investigație și organizații de drepturi digitale precum Amnesty International și Citizen Lab publică rapoarte care **demonstrează că acest spyware a fost folosit de guverne** pentru a supraveghea atât activiști, apărători ai drepturilor omului, cât și jurnaliști și oponenți politici.

2. Companiile vor bani și nu le interesează daunele colaterale

Companiile cele mai profitabile de pe Internet fac bani din “reclame personalizate”. Pentru a putea afla care ar fi produsele și serviciile care ar putea fi de interes pentru o persoană, companii precum Google și Meta adună date atât despre ce fac utilizatorii platformelor pe care le dețin (YouTube, Facebook, Instagram), pe site-urile unde sunt implementate scripturi ale acestora, dar și despre rețelele de prieteni și urmăritori ai acestora (și gusturile lor).

Dincolo de practica extrem de invazivă a acestei monitorizări constante, datele pe care companiile ajung să le dețină și să le folosească pentru a livra reclame pot fi folosite și în alte scopuri. De exemplu chiar în Statele Unite ale Americii, o mamă și fiica sa sunt în închisoare datorită faptului că au discutat pe Facebook, pe un chat care nu era criptat, despre cum plănuiesc să cumpere și să folosească medicamente pentru avort (într-un stat în care avortul medicamentos după limita de 20 de săptămâni nu este legal).

Informațiile personale ale cetățenilor, adunate de pe platforme de social media, au fost - și încă sunt - folosite pentru a influența procesul alegerilor democratice. O investigație jurnalistică a demascat, în 2023, un grup de contractori - denumit Team Jorge - care oferea ca servicii acest tip de campanii de influență, folosind boți (conturi de social media automatizare). Jurnaliștii sub acoperire au filmat interacțiunea cu liderul grupului, care a susținut că încercat, folosind social media, să influențeze 33 de alegeri prezidențiale în numele clienților săi.

Faptul că profitul acestor mari companii depinde de acest sistem de reclame este cumva și călcâiul lui Ahile, pentru ele. Numeroase reclame complet false împânzesc platformele de social media, iar algoritmii care ar trebui să le verifice veridicitatea par să fie neputincioși în comparație cu inventivitatea celor care le creează.

3. Hackerii - la fel de prezenți ca oricând

Hackerii sunt figura emblematică a Internetului, iar poveștile despre cine sunt și ce vor au evoluat cu timpul. La începuturi, termenul se refereau la persoane care nu căutau să facă rău, cât, mai degrabă, să testeze limitele tehnologiei. Tot despre “hackeri” se vorbește însă și atunci când ne referim la ceea ce cel mai probabil opera unei instituții a statului (cum e cazul Sandworm și entitatea neidentificată din spatele Stuxnet).

În unele cazuri, nu hackerii, ci atacul folosit de aceștia rămâne în memoria colectivă din cauza daunelor făcute. Acesta este cazul Wannacry, un virus care cripta datele dispozitivelor pe care le infecta și care a afectat nu doar calculatoarele personale ale oamenilor, ci inclusiv echipamentul medical al sistemului medical din Regatul Unit. Un alt caz similar este Mirai, un nume care nu aparține unui hacker, ci botnet-ului creat de un virus, adică grupul de dispozitive infectate care sunt, apoi, controlate de hackeri, de la distanță. Aceste dispozitive au fost folosite inclusiv pentru a ataca Dyn DNS, o companie care oferea servicii esențiale pentru buna funcționare a protocolului care permite utilizatorilor să acceseze website-uri pe Internet.

Termenul de “hacker” este, de obicei, folosit pentru a descrie o persoană cu cunoștințe tehnice, care face rău folosindu-se de vulnerabilități ale tehnologiei. În prezent, însă, multe atacuri nu provin de la persoane care își construiesc proprii viruși sau automatizări, ci cumpără sau închiriază acest software ofensiv. În plus, există persoane care rulează automatizări care caută echipamente și dispozitive

vulnerabile la anumite atacuri, oriunde în lume și le exploatează oportunist, fără să fie interesați de identitatea celor care dețin sau operează aceste ținte.

O persoană obișnuită are mici șanse să fie ținta unui atac, pregătit de un hacker, care să o vizeze personal. În schimb, cele mai îngrijorătoare fenomene de violență intimă care folosesc tehnologia sunt pornografia non-consensuală (inclusiv cea creată folosind inteligența artificială - raportată ca fiind 98% din cumulul materialelor de tip deepfake) și stalkerware-ul. Acest termen din urmă se referă la programele software de supraveghere pe care, de obicei, o persoană le instalează manual pe dispozitivul victimei, pentru a-i controla și monitoriza acțiunile.

B. Cum ne apărăm?

1. Nu-i vorba “dacă”, ci “când”

De-a lungul timpului, siguranța și securitatea au revenit în atenția oamenilor cu fiecare nou scandal, cu fiecare hack. Deși impactul acestor revelații e mare, explicațiile din spatele modului în care a fost posibil ca viața privată a unor persoane să fie supravegheată pot fi deseori complicate. **Tehnologia în sine joacă un rol cel puțin la fel de mare ca situația politică, dar și modul în care supravegherea a fost motivată și justificată.**

Când vine vorba de cum ne protejăm viața privată în mediu online sau de stocarea datelor digital, sfaturile pe care le citim în mass-media sunt și ele strâns influențate de cele mai recente evenimente. Articolele din presă culeg bune practici de la specialiști și le explică, apoi, pentru public, însă tind să se concentreze pe amenințarea cea mai recentă sau care e percepută ca fiind cea mai gravă.

În realitate, însă, siguranța noastră nu este niciodată garantată. Nu există un program software care să ne protejeze de orice atac cibernetic din viitor. Și nici nu există un anumit dispozitiv de comunicare care să nu poată, sub nici o formă, să fie urmărit sau supravegheat. Experții în securitate cibernetică rezumă, de obicei, acest adevăr, spunând că **nu-i vorba dacă o să fim vreodată ținta unui atac și e vorba doar de când vom fi țintiți**.

2. Cum să ne gândim la siguranță fără să ne pierdem în detalii

Nu există o soluție unică pentru orice amenințare la adresa vieții noastre private online, însă există un anumit mod de a decide care ar trebui să fie prioritățile noastre când vine vorba de a ne proteja.

În primul rând, trebuie să ne gândim la noi înșine din perspectiva acestor entități din afara noastră, care contribuie activ la amenințarea drepturilor noastre digitale. Cine suntem noi, pentru un guvern, o platformă de social media sau un hacker? Acest răspuns poate varia - putem fi un simplu “cetățean”, sau putem fii o persoană care este de interes pentru o entitate prin prisma muncii noastre (de exemplu, ca jurnaliști, activiști etc.). Chiar și la cel mai jos “rang” al ierarhiei acesteia, datele noastre sunt prețioase pentru toate trei entitățile, pentru că informația este cheia controlului și, deci, a puterii acestor entități.

Cum spunea Edward Snowden, avertizor de integritate, "**Să spui că nu îți pasă de dreptul la confidențialitate pentru că nu ai nimic de ascuns nu e cu nimic diferit de a spune că nu îți pasă de dreptul la liberă exprimare pentru că nu ai nimic de spus**".

Funcție de cine suntem noi pentru entitățile care amenință drepturile noastre digitale și viața noastră privată, putem să ne imaginăm care sunt pericolele (și există resurse care să ne ajută cu acest exercițiu).

Gândurile legate de amenințări și de ce ni s-ar putea întâmpla sunt foarte inconfortabile și ne pot împinge să ne dorim soluții rapide, pe care să implementăm și să scăpăm de grijă. Anumite firme de securitate cibernetica exploatează această nevoie și vând servicii care, deși susțin că ne protejează, ajung să se folosească de datele noastre în scop comercial. Să înțelegem unde ne ajută și unde ne pot încurca:

3. Antivirușii și serviciile de VPN - cum le alegem?

Două produse sunt deseori citate ca fiind esențiale pentru siguranța datelor noastre - **un antivirus** (mai nou găsită sub denumirea de soluție de securitate cibernetică) **și un serviciu de VPN**. Ambele produse software pot rezolvă, teoretic, probleme cât se poate de reale. Însă, funcție de cum sunt implementate și funcție de practicile firmelor care le comercializează, pot face mai mult rău decât bine.

a) Antivirușii protejează un dispozitiv (un calculator, smartphone sau tabletă) de viruși și alte atacuri încercând - simplist explicat - să deducă dacă software-ul care rulează face ceva ce seamănă cu ce ar face un virus sau un program malware, sau dacă fișierele stocate sunt infectate cu viruși. Aceasta este o explicație care simplifică mult funcționarea antivirușilor, însă ce este esențial de înțeles este că aceste programe - pentru a face ceea ce spun ca fac - pot fi extrem de invazive: ele supraveghează întreg dispozitivul și au nevoie de privilegii mult mai mari decât alte programe instalate.

Antivirușii în sine au avut, de-a lungul timpului, vulnerabilități de securitate. În trecut, programele antivirus interferau cu buna funcționare a altor programe (de exemplu, a browserului). Antivirușii ajungeau să folosească atât de multe resurse de calcul încât utilizatorul nu-și mai putea folosi dispozitivul, care executa acțiuni extrem de încet. Alții, care aveau un "serviciu gratuit" au vândut date personale ale clienților lor.

Poate cel mai amenințător pentru utilizatori a fost momentul în care o companie de antivirus care avea reputație foarte bună a fost victima unei breșe de securitate care a expus informațiile personale a unora dintre clienți, în 2015.

Antivirușii pot fi însă utili celor care lucrează cu multe fișiere pe care le primesc de la persoane pe care nu le cunosc sau care ar deschide fișiere care par a veni chiar de la persoane cunoscute - un caz în care riscul ca aceste fișiere să fie virusate crește. Ceea ce vrem să subliniem aici este că niciun program antivirus nu este panaceu și ele nu înlocuiesc faptul că trebuie sa fiți atenți. Mai mult, găsirea

unuia potrivit, depinde de nivelul vostru de experiență, dar și felul în care sunteți confortabil cu un anumite nivel de intruzivitate în dispozitivul folosit.

b) **Serviciile de VPN** au scopul de a proteja traficul pe Internet al unui utilizator de anumite metode de supraveghere. În esență, în loc ca un utilizator să acceseze direct site-urile pe care le dorește, va accesa mai întâi serverul de VPN și de acolo va porni o nouă conexiune către site-ul destinație. Astfel, dacă o entitate ar urmări site-urile accesate de acest utilizator, nu ar putea vedea decât faptul că accesează un server de VPN, nu și destinația finală.

Cel mai important lucru pe care îl face un VPN este să șteargă conexiunea directă dintre un utilizator și conținutul online pe care l-a accesat. Multe astfel de servicii susțin că nu păstrează log-uri în care să coreleze identitatea clientului cu conținutul pe care l-a accesat, prin VPN. Însă, s-a dovedit că unele dintre serviciile de VPN au mințit.

La fel ca în cazul serviciilor de antivirus, o breșă de securitatea care cuprinde datele clienților unui serviciu de VPN va putea expune informații extrem de sensibile - ceea ce s-a și întâmplat, recent, în 2021.

În cazul serviciilor de VPN, diversitatea de soluții software oferite de companii e mult mai mare, însă și tehnologia în sine e mult mai recentă (în forma actuală). Din acest motiv, un studiu arată faptul că, dacă un utilizator ar căuta informații despre care este cel mai potrivit serviciu de VPN, aproape orice articol online care compară și ierarhizează serviciile este reclamă plătită. De multe ori, companiile susțin că serviciile de VPN pot oferi o protecție mai mare - spre exemplu, că pot proteja un dispozitiv de atacuri cibernetice - ceea ce se dovedește a fi, extrem de des, complet fals.

În consecința ApTI nu face recomandări legate de un antivirus sau serviciu de VPN ideal sau unul anume, însă oferă o serie de repere pe care orice persoană le poate folosi atunci când evaluează dacă să folosească sau nu un astfel de program software:

- **Protecția oferită datelor personale este extrem de importantă**. Un utilizator poate căuta dacă o companie a fost implicată recent în breșe de securitate, sau dacă există raportări cum că ar fi oferit log-uri cu activitatea clienților unor terțe părți, atunci când susține că nu stochează astfel de informații.
- **Reputația companiei și a expertizei dezvoltatorilor poate fi verificată** căutând ce se spune despre ei în publicații de jurnalism de tehnologie reputabile. Sau chiar în articole științifice. Faptul că produsul în sine are sursele deschise este un atuu, mai ales dacă există articole de specialitate legate de încercări de a găsi vulnerabilități în cod.
- Pentru sfaturi, un utilizator se poate îndepărta de influența companiilor căutând mai degrabă părerile unor organizații mari, non-guvernamentale, care lucrează în domeniul drepturilor digitale: Access Now, Citizen Lab, Amnesty International, Electronic Frontier Foundation etc.

Pentru persoanele care își doresc acest lucru, un serviciu de VPN poate să fie creat și de către persoana care dorește să-l folosească, acest lucru este posibil folosind de exemplu software-ul Wireguard. În acest caz, persoana care își construiește propriul VPN trebuie să își achiziționeze pe cont propriu o soluție de găzduire.

4. Parolele, software-ul de management de parole și 2FA

Parolele folosite pentru toate conturile și dispozitivele, online și offline, sunt primul nivel de protecție ale datelor noastre personale. Dat fiind că protejarea conturilor prin combinația de nume de utilizator și parolă este o practică extrem de veche, există deja foarte multe opinii și sfaturi legat de modul ideal de a alege o parolă.

În fiecare an, un studiu al companiei HiveSystems detaliază cât de ușor de "spart" sunt parolele care au o anumită formă, adică cât de repede pot fi ghicite de un algoritm care le generează și le încearcă, pe rând. În anul 2024, concluzia acestui studiu este că o parolă sigură ar trebui să folosească minim **18 caractere**, ideal combinații între litere mici, mari, numere și simboluri (însă combinația între litere mici și mari este suficientă).

Unul dintre cele mai des întâlnite sfaturi legate de parole este acela de a folosi o parolă diferită pentru fiecare cont online. Dat fiind că avem mult mai multe conturi decât putem ține minte combinații aleatoare de numere și cifre, soluția poate fi un manager de parole, în care fiecare combinație de site, nume de utilizator și parolă e stocată.

Din fericire, programele software care stochează parole nu se pot folosi de datele pe care le stochează pentru a face profit. Însă, aceste companii rămân vulnerabile la breșe de securitate, caz în care datele clienților - parolele - ar putea ajunge să fie expuse. Din fericire, de cele mai multe ori și mai ales în cazul companiilor mari, cu bună reputație, datele clienților sunt stocate criptat, deci, chiar și în cazul unei breșe, parolele nu ar putea să fie citite de către atacatori. Însă, după cum am menționat în acest articol, nici o tehnologie nu este 100% sigură - chiar și algoritmii de criptare pot avea vulnerabilități de implementare.

Două dintre companiile care oferă soluții de management de parole au fost recent ținte ale unor breșe: LastPass și 1Password (însă informațiile sustrase erau criptate). Acestea permit utilizatorilor să stocheze parolele pe serverele deținute de companii - deci, în cloud. Avantajul este că un utilizator poate accesa ceea ce a stocat de pe orice dispozitiv. Dezavantajul, însă, este că datele sunt stocate pe serverele companiilor.

În cazul programelor software care stochează criptat parole, există și soluții care stochează aceste date local, pe dispozitivul utilizatorului. Una dintre cele mai folosite astfel de programe este KeePass (pentru Windows) / KeePassX (pentru Linux și MacOS).

Un nivel în plus de siguranță, absolut esențial în contextul amenințărilor din prezent, pentru protejarea conturilor online, îl oferă tehnologia de two-factor authentication (sau autentificare în doi pași, de obicei prescurtată 2FA). Dat fiind că parolele pot să fie sparte, ghicite sau chiar dezvăluite în anumite condiții, 2FA adaugă încă un lucru pe care utilizatorul trebuie să îl facă pentru putea să îți acceseze contul: anume, să dovedească că deține un anumit lucru. 2FA-ul, de obicei, poate să trimită un SMS utilizatorului (iar acesta dovedește, astfel, că deține propriul telefon), sau un cod unic, sau poate să ceară utilizatorului să introducă în calculator o "cheie" (denumită hardware token).

C. Și de aici - pe unde o apucăm?

Siguranța noastră, a datelor noastre și a tuturor activităților pe care le facem mijlocit de tehnologie depinde nu doar de programele software pe care le folosim ci și de atenția și perspicacitatea noastră. **Intuiția noastră joacă un rol extrem de important.** Dacă ceva pare nelalocul lui când folosim unul din dispozitivele noastre, e bine să ne ascultăm subconștientul și să încercăm să punem în cuvinte ce ni se pare bizar.

Nici dacă se întâmplă ca un dispozitiv să fie infectat cu un virus, nu e capăt de lume. Chiar și în cazul ăsta, sunt pași simpli care pot minimiza răul făcut. Dacă ai făcut un backup e și mai simplu. **ApTI a participat la un webinar (vezi un material video) despre cum putem reacționa în cazul în care am fost victimele unui hack**.

Este foarte probabil că fiecare dintre noi a fost deja victima unor atacuri cibernetice - poate că nici unul dintre atacuri nu a avut succes, poate că unele dintre ele au avut succes, dar ne-au salvat, la vremea respectivă, antivirușii, sau o instalare de sistem de operare. Tehnologia nu trebuie să fie un mister, sau o amenințare - noi putem să o înțelegem și să decidem cum o folosim.