Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

Cât de sigure sunt dispozitivele electronice în era interconectivității globale?

În fiecare zi, trăim conectați. De la smartphone-ul care ne alarmează dimineața, la laptopul de pe care lucrăm, până la termostatul inteligent care reglează temperatura casei în funcție de preferințele noastre, tehnologia e omniprezentă. Dar, să fim realiști, câți dintre noi ne întrebăm cum funcționează cu adevărat aceste dispozitive? Și mai important, cât de mult avem încredere că ele lucrează în interesul nostru?

Adevărul e că povestea încrederii în tehnologie a devenit mai complicată decât ne-am fi imaginat acum câțiva ani. În trecut, unelte precum topoarele sau cuțitele erau ușor de verificat. Nu te gândeai că un topor ar putea „lucra împotriva ta." Dar astăzi, lucrurile stau altfel. Electronicele din viața noastră nu doar că sunt incredibil de complexe, dar sunt și conectate, deseori la distanță, cu producătorii lor. Practic, relația dintre noi, ca utilizatori, și cei care construiesc aceste dispozitive e mai mult decât o simplă tranzacție, devine un parteneriat pe termen lung.

Și acum vine partea interesantă, ce se întâmplă dacă producătorul decide să-și folosească această poziție pentru a acționa împotriva noastră? Poate pare o idee desprinsă dintr-un film SF, dar exemplele din viața reală ne arată că astfel de scenarii nu sunt deloc de neimaginat. De la routere manipulate pentru a transmite date către agenții de spionaj, până la telefoane care trimit mesaje secrete către servere din alte țări, istoria recentă ne arată că încrederea în tehnologie nu ar trebui să fie niciodată oarbă.

Cu toate acestea, majoritatea dintre noi preferăm să închidem ochii și să sperăm că lucrurile vor funcționa. Când descoperim o funcție nouă pe telefon, exclamăm cu entuziasm: ***„Wow, habar n-aveam că poate face asta!"*** **Dar rareori ne întrebăm:** ***„Oare ce altceva mai poate face, fără ca eu să știu?"***

Acesta este punctul de pornire al articolului meu: nu doar cum putem înțelege mai bine dispozitivele pe care le folosim, ci și cum putem naviga într-o lume în care încrederea în producători devine la fel de importantă ca funcționalitatea unui produs. Indiferent dacă ești un utilizator obișnuit sau o organizație care face investiții în infrastructuri critice, întrebarea rămâne aceeași: putem avea încredere? Și dacă da, cum putem verifica asta?

Problema încrederii, sau când tehnologia devine un joc de noroc ...

Încrederea este liantul care ne unește ca oameni, atât în interacțiunile noastre sociale, cât și în cele cu lumea digitală, dar cât de mult ne gândim la acest lucru când ne cumpărăm un telefon nou sau când guvernele investesc miliarde în infrastructuri critice? Problema încrederii în tehnologie este mai mare decât pare la prima vedere, iar uneori, deciziile pe care le luăm seamănă mai mult cu un joc de noroc decât cu o alegere bine calculată.

Când cumperi un telefon, un laptop sau o cameră de supraveghere, în esență îți pui încrederea într-un producător. Ai încredere că dispozitivul va funcționa așa cum trebuie, că va fi sigur de utilizat și că nu îți va trăda așteptările. Dar, dacă te gândești puțin mai profund, ce garanție ai că acel dispozitiv nu va face ceva împotriva intereselor tale?

Să luăm exemplul discuțiilor globale despre Huawei și ZTE. Aceste companii chinezești au devenit subiectul unor controverse aprinse în țări precum Statele Unite, Australia sau Canada. Motivul? Temeiuri de securitate națională. Chiar dacă nu există dovezi clare că aceste companii ar fi folosit tehnologia pentru a spiona sau sabota, suspiciunile persistă. De ce? Pentru că, în lumea electronicelor complexe, verificarea intențiilor reale ale unui producător este aproape imposibilă.

În zilele noastre, **majoritatea dispozitivelor sunt mai mult decât niște simple unelte**. Ele sunt conectate la internet, primesc actualizări software și, prin urmare, sunt în permanență legate de producătorul lor. Asta înseamnă că, odată ce ai cumpărat un produs, relația cu producătorul nu se termină, continuă pe toată durata de viață a dispozitivului.

Problema este că această conexiune s-ar putea transforma într-o adevărată poveste cu final neașteptat. De exemplu, **actualizările software, prezentate ca soluții, ar putea ascunde capcane digitale care să te dezavantajeze.** De la manipularea traficului de internet, cum s-a întâmplat în cazul routerelor Cisco, până

la spionaj direct, cum a demonstrat cazul telefoanelor Android produse de Shanghai Adups Technology, exemplele abundă.

Unii spun că încrederea într-un producător vine din reputația acestuia sau din experiențele trecute. Dar, adevărul este că încrederea reală nu ar trebui să fie doar despre trecut, ea trebuie să ia în considerare și viitorul. **Un producător poate fi de încredere astăzi, dar ce se întâmplă dacă interesele sale se schimbă mâine?** Sau dacă presiuni externe, să zicem, de la un guvern, îi determină să acționeze contrar intereselor tale?

Este o problemă reală, mai ales în cazul investițiilor în infrastructuri critice. Imaginează-ți un stat care depinde de echipamentele unui furnizor străin pentru comunicații, apă sau energie. Dacă acel furnizor decide, dintr-un motiv sau altul, să oprească echipamentele sau să le manipuleze, consecințele pot fi devastatoare.

Problema încrederii în tehnologie este, așadar, una extrem de complexă. Este un subiect care influențează deciziile economice și politice la nivel global. Într-o lume unde depindem atât de mult de tehnologie, răspunsul la întrebarea „Putem avea încredere?" devine tot mai greu de găsit. Și, poate cel mai frustrant, soluțiile nu sunt simple. Nu putem verifica fiecare cip sau linie de cod, iar deciziile trebuie luate în condiții de incertitudine.

Dar, chiar și așa, **eu consider că este important să începem această conversație**. Să recunoaștem că încrederea în tehnologie nu mai poate fi tratată cu superficialitate și că, în final, e nevoie de transparență, colaborare și inovație pentru a construi relații de încredere solide, indiferent că vorbim despre un telefon personal sau o infrastructură națională.

Vulnerabilități și riscuri, sau când tehnologia poate deveni o armă ...

Te-ai gândit vreodată că telefonul, routerul sau mașina ta ar putea lucra împotriva ta? Realitatea ne arată că, odată cu creșterea complexității dispozitivelor electronice, crește și posibilitatea ca ele să fie folosite pentru spionaj, sabotaj sau fraude. Vulnerabilitățile există, iar riscurile sunt mai reale decât ne place să credem.

În lumea electronicelor, o vulnerabilitate este ca o mică crăpătură într-un baraj. Poate părea nesemnificativă la început, dar, dacă este exploatată, poate cauza un dezastru. Vulnerabilitățile pot fi greșeli de programare, componente hardware defectuoase sau chiar funcționalități intenționat adăugate pentru a permite accesul neautorizat. Ce este cu adevărat înfricoșător? De cele mai multe ori, nici măcar nu știm că ele există.

Hai să luăm un exemplu real: routerele Cisco manipulate de NSA pentru a redirecționa traficul de internet.

"Un caz bine documentat de spionaj este acela în care routerele și serverele fabricate de Cisco au fost manipulate de Agenția Națională de Securitate (NSA) pentru a trimite traficul de internet înapoi la ei. Acest caz este bine documentat prin documentele puse la dispoziția presei de Edward Snowden și este, prin urmare, un exemplu solid de spionaj realizat prin intermediul unui furnizor de echipamente. Nu există nicio dovadă că Cisco era la curent cu manipularea efectuată de NSA, dar exemplul este totuși relevant." (Olav Lysne)

Documentele dezvăluite de **Edward Snowden** au arătat cum echipamentele erau interceptate înainte de livrare și modificate pentru a trimite date către agenția de securitate. Cumperi un router de top, îl instalezi crezând că îți protejează rețeaua, dar de fapt el transmite informații către alții. Problema? Nu aveai nicio șansă să descoperi asta fără o investigație amănunțită.

Adesea, este foarte dificil să separăm vulnerabilitățile de erorile adevărate. **În 2016, o companie americană de securitate cibernetică, Kryptowire, a descoperit că telefoanele produse de Shanghai Adups Technology trimiteau date personale, mesaje, contacte, istoricul apelurilor, către un server din China.** *"Informațiile scurse includeau corpul integral al mesajelor text, listele de contacte și istoricul apelurilor, cu numerele de telefon complete."* Cei de la Adups au spus că totul a fost o „greșeală" și că software-ul fusese creat pentru un producător chinez, nu pentru telefoane vândute în SUA. Greșeală sau nu, încrederea utilizatorilor a fost deja zdruncinată.

Un alt exemplu notoriu este scandalul Volkswagen. Cine s-ar fi gândit că un producător auto de renume mondial ar include intenționat un software care să înșele testele de emisii? A fost o fraudă deliberată, iar problema nici măcar nu a fost descoperită prin analiza software-ului, ci prin testarea comportamentului mașinilor în condiții reale. Asta ridică o întrebare importantă: dacă nici autoritățile nu pot detecta astfel de manipulări la timp, ce șanse avem noi, utilizatorii obișnuiți?

Când vorbim despre riscuri, temerile pot varia de la scenarii de spionaj personal până la sabotaj la scară națională. De exemplu, în 2007, radarele siriene au eșuat în timpul unui atac aerian israelian. Speculațiile au sugerat că un „buton de oprire" ascuns în echipamente ar fi fost activat pentru a dezactiva radarele. Deși aceste afirmații nu au fost confirmate, ele arată cât de reală este posibilitatea sabotajului prin intermediul tehnologiei.

Recent, Libanul a fost zguduit de o serie de explozii simultane ale pagerele folosite de membrii Hezbollah, incident soldat cu nouă morți și aproape 3.000 de răniți. Exploziile au avut loc pe 17 septembrie 2024, în special în zonele cu prezență semnificativă a Hezbollah.

Pagerele au explodat după ce au primit mesaje, provocând confuzie și panică. Multe dintre victime au fost surprinse în momentul în care au încercat să verifice mesajele. Se suspectează că agenția israeliană de spionaj Mossad a plantat explozibili în aproximativ 5.000 de pagere importate de Hezbollah, ceea ce reprezintă o breșă majoră de securitate pentru grupare. Dispozitivele erau dotate cu baterii litiu, care, conform unor experți, ar fi putut fi modificate pentru a include o încărcătură explozivă.

Riscurile sunt amplificate în special în infrastructurile critice, rețele de energie, telecomunicații sau apă. Dacă un furnizor de echipamente decide să manipuleze dispozitivele vândute, consecințele pot fi catastrofale așa cum sa și întâmplat deja.

Identificarea vulnerabilităților și reducerea riscurilor nu sunt sarcini ușoare. Într-o lume în care complexitatea dispozitivelor depășește adesea înțelegerea utilizatorilor, verificarea integrității acestora devine o provocare uriașă. Totuși, există câteva lucruri pe care le putem face:

- **Alegerea furnizorilor cu grijă:** Transparența și reputația contează, dar ele nu sunt suficiente.
- **Audituri independente:** Infrastructurile critice ar trebui să fie supuse unor verificări riguroase, realizate de terți.
- **Actualizări constante:** Deși actualizările software pot fi o poartă pentru vulnerabilități, ele rămân și cea mai bună apărare împotriva atacurilor cunoscute.

Problema vulnerabilităților și a riscurilor în tehnologie nu poate fi ignorată. De fiecare dată când apăsăm „update," ne bazăm pe o relație de încredere cu producătorul, o relație care, după cum am văzut, poate fi fragilă. De aceea, trebuie să fim mai conștienți de riscurile pe care le implică dependența noastră de tehnologie. Poate că nu putem elimina complet aceste riscuri, dar primul pas este să le înțelegem, și să cerem mai multă transparență de la cei care ne construiesc viitorul digital.

Cum putem verifica și construi încrederea?

Tocmai ți-ai cumpărat un nou telefon, plin de funcții impresionante și cu un design impecabil. Dar, în timp ce îl configurezi, o întrebare îți trece prin minte: ***Cum pot ști cu siguranță că acest dispozitiv funcționează doar pentru mine, nu și împotriva mea?*** Într-o lume în care tehnologia devine tot mai complexă, iar dependența noastră de ea crește, verificarea și construirea încrederii sunt mai importante ca niciodată. Dar cum facem asta, mai ales când nici măcar experții nu pot să descopere toate capcanele ascunse?

De ce e atât de greu să verificăm ce face tehnologia? Să începem cu o realitate simplă, dar frustrantă: **verificarea completă a unui dispozitiv modern este aproape imposibilă.** De ce? Pentru că tehnologia pe care o folosim zilnic, telefoane, routere, servere, este incredibil de complexă și producătorii nu sunt întotdeauna transparenți cu privire la modul în care funcționează produsele lor. Lipsa documentației tehnice detaliate și a accesului la codul sursă îngreunează înțelegerea completă a unui dispozitiv și identificarea potențialelor probleme de securitate.

De exemplu, dacă producătorul ar include o funcție ascunsă, cum ar fi transmiterea datelor tale personale către un server extern, probabil n-ai avea cum să descoperi asta. Și chiar dacă ai fi un expert care analizează codul sursă (presupunând că acesta ar fi disponibil), cine îți garantează că următoarea actualizare software nu adaugă o altă funcție ascunsă?

Există, totuși, câteva metode care pot ajuta la verificarea și construirea încrederii:

1. **Testare independentă și audituri:** Unele companii permit testarea dispozitivelor lor de către terți independenți. Acest lucru poate oferi un strat suplimentar de încredere. Dar problema e că aceste teste nu sunt întotdeauna exhaustive.
2. **Metode formale și analiza software:** Tehnici precum verificarea formală, folosirea matematicii pentru a demonstra că un sistem funcționează corect, sunt folosite în cazuri critice. Problema? Sunt foarte costisitoare și dificil de aplicat la sisteme complexe.
3. **Trusted Computing Base (TCB):** Ideea e simplă: reducem totul la un nucleu de componente esențiale, care să poată fi verificate în întregime. Dar chiar și acest „nucleu" poate fi compromis dacă producătorul nu este complet transparent.
4. **Criptografia și securitatea hardware:** Modulele de securitate, cum ar fi Trusted Platform Module (TPM), sunt integrate în dispozitive pentru a asigura că software-ul și hardware-ul sunt autentice. Totuși, dacă nu ai încredere în cine a construit acest modul, soluția devine inutilă.

Încrederea nu este doar o problemă tehnologică iar verificarea unui dispozitiv nu rezolvă complet problema. Încrederea este un concept mai larg, care implică și reputația producătorului, transparența acestuia și relațiile pe termen lung.

De exemplu, companiile care își deschid codul sursă sau care permit audituri independente regulate transmit un semnal puternic că nu au nimic de ascuns. La fel, producătorii care investesc în educarea consumatorilor despre riscuri și măsuri de securitate construiesc relații mai solide.

Dar să fim realiști, **încrederea nu este veșnică**. O companie poate fi de încredere azi, dar circumstanțele pot schimba prioritățile mâine. Poate apare presiune din partea unui guvern sau o criză financiară care forțează compromiterea valorilor.

Ce putem face noi, utilizatorii care nu avem puterea de a analiza fiecare linie de cod, dar asta nu înseamnă că suntem lipsiți de opțiuni.

1. **Alege producători transparenți:** Înainte de a cumpăra un dispozitiv, informează-te despre reputația companiei. Este deschisă cu privire la practicile sale? Are un istoric de comportament etic?
2. **Actualizări inteligente:** Actualizările sunt esențiale pentru securitate, dar asigură-te că vin de la surse de încredere și că înțelegi ce schimbări aduc.
3. **Presiune colectivă:** Ca utilizatori, avem o voce puternică. Cerând mai multă transparență și standarde de securitate, putem influența practicile industriei.
4. **Educație continuă:** Învață despre riscurile tehnologice și cum să te protejezi. Într-o lume conectată, educația este cea mai bună armă împotriva vulnerabilităților.

Construim încrederea împreună, deoarece verificarea și construirea încrederii nu sunt doar responsabilitatea companiilor, sunt un efort comun. Prin transparență, colaborare și vigilență, putem face ca tehnologia să devină nu doar mai sigură, ci și un partener pe care să ne putem baza cu adevărat.

Așadar, data viitoare când apeși „update," gândește-te: ***„Cum pot contribui la o lume în care încrederea devine o normă, nu o excepție?"*** Poate că nu avem toate răspunsurile acum, dar primul pas e să începem să punem întrebările potrivite.

Învățături pentru organizații și decidenți, sau cum să navighezi în apele tulburi ale tehnologiei ...

Când vine vorba de tehnologie, multe organizații și decidenți se confruntă cu o dilemă destul de complicată: cum alegem furnizorii și echipamentele potrivite fără să ne asumăm riscuri uriașe? Într-o lume în care infrastructurile critice, comunicații, energie, apă, sunt interconectate și depind de tehnologii complexe, această întrebare nu este doar despre performanță sau preț. Este despre securitate, încredere și, în unele cazuri, despre supraviețuire.

Hai să vedem ce putem învăța din experiențele recente și cum putem lua decizii mai bune, fie că ești într-o corporație care își alege partenerii tehnologici, fie că faci parte dintr-o instituție guvernamentală cu responsabilități strategice.

Lecția 1: Încrederea e fragilă, dar vitală. Să ne amintim de cazul Huawei și ZTE. Deși nu există dovezi concrete că aceste companii ar fi sabotat infrastructuri, suspiciunile legate de posibilele lor legături cu guvernul chinez au fost suficiente pentru a declanșa interdicții și dezbateri aprinse în țări precum SUA, Australia sau Canada. Lecția? Încrederea nu se construiește doar prin performanță tehnică, ci prin transparență și reputație.

Pentru organizații, asta înseamnă că selecția unui furnizor nu ar trebui să fie bazată doar pe costuri sau pe caracteristici tehnice, ci și pe un audit riguros al istoricului și al practicilor acestuia. Alegeți furnizori care sunt deschiși în privința proceselor lor și care demonstrează un angajament real față de securitate.

Lecția 2: Verificarea trebuie să devină un obicei, nu o excepție. Un alt punct important este dificultatea verificării echipamentelor complexe. După cum am discutat, nu e realist să verifici fiecare componentă a unui dispozitiv modern. Dar asta nu înseamnă că trebuie să accepți totul fără întrebări.

Organizațiile ar trebui să investească în audituri independente și în teste regulate ale echipamentelor, mai ales pentru infrastructurile critice. Un exemplu ar fi colaborarea cu firme specializate în securitate cibernetică pentru a evalua riscurile. De asemenea, menținerea unei politici clare privind actualizările software și verificarea impactului acestora sunt esențiale pentru a evita surprize neplăcute.

Lecția 3: Diversificarea furnizorilor reduce riscurile. Un principiu important în orice strategie de reducere a riscurilor este diversificarea. Să depinzi de un singur furnizor pentru echipamente critice e ca și cum ai merge pe o frânghie întinsă fără plasă de siguranță.

Decidenții ar trebui să opteze pentru o strategie care să includă mai mulți furnizori, preferabil din diferite regiuni geografice. În acest fel, chiar dacă unul dintre aceștia devine nesigur sau inaccesibil dintr-un motiv sau altul, infrastructura poate continua să funcționeze fără întreruperi majore.

Lecția 4: Gândiți pe termen lung, nu doar pe termen scurt. Un alt aspect esențial este să privim dincolo de câștigurile imediate. Uneori, un furnizor mai ieftin poate părea o alegere atractivă, dar costurile pe termen lung pot fi mult mai mari dacă apar vulnerabilități. Aici intervine importanța analizării ciclului de viață al echipamentelor: cum va fi întreținut, ce garanții oferă furnizorul și cât de repede poate răspunde în cazul unei crize?

Deciziile trebuie luate având în vedere nu doar costurile inițiale, ci și riscurile asociate și costurile de remediere în cazul unui atac sau al unei defecțiuni.

Lecția 5: Educația este cheia. În final, dar nu în ultimul rând, educația joacă un rol critic. Decidenții trebuie să fie informați nu doar despre beneficiile tehnologiei, ci și despre riscurile acesteia. Organizarea de traininguri periodice pentru personal, crearea unor politici clare de securitate și promovarea unei culturi a responsabilității în utilizarea tehnologiei pot face o diferență enormă.

Concluzie: Deciziile informate sunt singurele decizii bune. Pentru organizații și decidenți, provocarea nu este doar să aleagă tehnologia potrivită, ci și să construiască un ecosistem de încredere. Prin verificări regulate, diversificare și investiții în educație, putem face față riscurilor dintr-o lume tot mai interconectată.

Așadar, data viitoare când luați în considerare o investiție majoră în tehnologie, puneți-vă o întrebare simplă: ***„Această alegere mă ajută să dorm liniștit noaptea?”*** Dacă răspunsul nu este un „da” categoric, poate e momentul să regândiți strategia. Pentru că, până la urmă, securitatea nu e doar o linie de buget – este fundația încrederii.

Concluzie: Încrederea, cheia unui viitor sigur ...

Când vine vorba de tehnologie, concluzia e simplă: **încrederea este indispensabilă, dar niciodată de la sine înțeleasă.** Trăim într-o lume în care fiecare telefon, fiecare router, fiecare actualizare software aduce cu sine nu doar beneficii, ci și riscuri. Iar aceste riscuri, odată ignorate, pot avea consecințe greu de reparat.

Pentru utilizatori, organizații și decidenți deopotrivă, provocarea este aceeași: **cum navigăm prin complexitatea tehnologiei moderne, fără să renunțăm la siguranță sau la progres?** Răspunsul nu este un simplu „da” sau „nu.” Este un proces, unul care începe cu educație, continuă cu transparență și se construiește prin colaborare.

Încrederea nu înseamnă să ne bazăm orbește pe producători, ci să cerem mai mult. Să cerem audituri, diversitate în furnizori, verificări constante și politici de securitate bine gândite. Pentru că doar prin eforturi comune, consumatori, companii, guverne, putem crea un ecosistem tehnologic sigur.

Așadar, data viitoare când îți actualizezi telefonul sau când organizația ta cumpără echipamente noi, întreabă-te: ***„Cum ne asigurăm că tehnologia funcționează pentru noi, nu împotriva noastră?”*** E o întrebare simplă, dar cu impact enorm. Și de aici începe adevărata schimbare.

Impresiile voastre pozitive, sau negative, și recomandările pentru acest subiect, contează. Împreună putem învăța, crește și excela în profesiile noastre. Lectură plăcută!

Surse:

- The Huawei and Snowden Questions Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment? by Olav Lysne;
- Cybersecurity for the IoT: How trust can unlock value (mckinsey.com);
- A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review, by Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat;
- Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (Raport NIST);
- Digital trust: Why it matters for businesses (mckinsey.com).