

Kedy sa dôvera zmení na monitoring: sledovanie partnera ako tichý kyberútok

„Pošli mi polohu, nech viem, že si v poriadku.“ Veta, ktorá môže znieť ako starostlivosť, sa v niektorých vzťahoch nenápadne zmení na zmluvu o kontrole. A technológie tomu prajú. Telefón je dnes zároveň denník, kľúčienka, aj mapa návykov. Keď raz dáme niekomu prístup, často si neuvedomíme, že sme neodovzdali len pohodlie, ale aj moc a s ňou aj riziko, ktoré už nie je iba partnerské, ale aj kybernetické. Na riziká spojené so sledovaním partnera cez telefón upozorňuje spoluzakladateľka konferencie venujúcej sa kybernetickej bezpečnosti Qubit Conference[®] Mária Krahulecová.

Bratislava, 11.2.2026

Poloha neznamena tu som. Zdieľať polohu znamená zdieľať kde bývam, kedy odchádzam, ktorou cestou chodím, kde sa zdržiavam a s kým sa pravdepodobne stretávam. A čo je kľúčové, aj keď sa tvárime, že údaje sú anonymné, často to vôbec neznamena, že sa nedajú priradiť ku konkrétnemu človeku. [Výskum](#) ukázal, že na jednoznačnú identifikáciu osoby v anonymizovaných dátach môžu stačiť už štyri náhodné body polohy. Mária Krahulecová, spoluzakladateľka konferencie venujúcej sa kybernetickej bezpečnosti Qubit Conference[®], to pomenúva priamo: „Vždy, keď dáte niekomu prístup k svojej polohe, nedávate mu len bod na mape, ale časový záznam vášho života.“ V praxi to znamená, že stačí pár nevinných návykov, napríklad rovnaká trasa do práce, pravidelná návšteva fitka, obľúbená kaviareň, k tomu sa pridajú metadáta, kto s kým komunikuje, kedy, ako často a odkiaľ a obraz života sa poskladá aj bez čítania jedinej správy. Sociologička zaoberajúca sa rodovou rovnosťou PhDr. Silvia Porubánová tvrdí: „Všetci bez rozdielu prahneme po bezpodmienečnej láske a prijatí. V túžbe po naplnení nášho ideálu, dokonalého, či "aspoň" optimálneho partnerského vzťahu sme ochotní/é pristúpiť na kompromisy, alebo konkrétne podmienky, ktoré by sme v inom type vzťahov (priateľských, príbuzenských...) považovali prinajmenšom za čudné, podozrivé, ba priam za neakceptovateľné.“

Do hry vstupujú aj aplikácie, ktoré by sme vôbec nepodozrievali. Fitness platformy, mapy behov či výletov, zdieľané kalendáre, rodinné skupiny, cloudové albumy. Rutiny a citlivé miesta človeka sa dajú zrekonštruovať aj bez hackovania. Stačí poskladať údaje, ktoré vznikajú pri bežnom používaní telefónu a aplikácií, napríklad polohu, časy pohybu, prihlásenia či nákupné a komunikačné vzorce. A aj keď človek niektoré služby nepoužíva, môžu o ňom vzniknúť takzvané tieňové profily z dát, ktoré o

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference[®]
Martinčekova 17
821 01 Bratislava

ňom odovzdajú iní. „Technológia sama o sebe vzťahy neničí, ale zosilňuje to, čo už medzi ľuďmi existuje. Nedôveru, žiarlivosť, potrebu kontroly. Ak sa zdieľanie polohy stane podmienkou lásky, už to nie je starostlivosť, ale kontrola,“ hovorí M. Krahulecová.

Stalkerware, phishing a prevzaté účty: keď sa intímny konflikt zmení na incident

Najnebezpečnejšie na partnerskom sledovaní je, že často nevyzerá ako útok. Neprichádza s kapucňou a kódom na monitore. Prichádza cez - *poznám tvoje heslo, tvoj mobil je aj tak vždy odomknutý, veď sme rodina, čo skrývaš?* Práve preto sa v medzinárodných diskusiách stále častejšie používa pojem technology-facilitated abuse (zneužívanie technológií v intímnych vzťahoch, ktoré môže zahŕňať sledovanie, manipuláciu, vydieranie či narušanie súkromia). Do tejto kategórie spadá aj stalkerware: aplikácie, alebo správčovské nástroje určené na monitorovanie bez súhlasu. Podľa dostupných údajov bolo v roku 2023 globálne zasiahnutých 31 031 unikátnych používateľov stalkerware, čo predstavovalo medziročný nárast oproti roku 2022. ([Zdroj](#))

Nejde pritom len o špiónážne aplikácie. Často ide o prevzaté účty, prístup do cloudu, zrkadlené notifikácie, zneužitie zdieľaných rodinných služieb alebo náhodné prihlásenie na cudzom zariadení, ktoré ostalo uložené. Mária Krahulecová, ktorá je doma vo svete kybernetickej bezpečnosti, upozorňuje, že v partnerských konfliktoch sa kyberútok málokedy začne ako sofistikované hackovanie. Upozorňuje, že častejšie ide o zneužitie dôvery, spoločného hesla, odomknutého telefónu či automatického prihlásenia.

Riziko navyše rastie aj mimo čistého partnerského kontextu. Na Slovensku je podľa ESET v poslednom období dominantnou hrozbou phishing a jeho kvalita sa zvyšuje aj vďaka nástrojom umelej inteligencie. ([Zdroj](#)) V toxickom vzťahu sa tak môže bežná kyberkriminalita stať veľmi osobnou. Podvrhnutý e-mail na overenie účtu, falošná stránka, cez ktorú útočník získa prístup, alebo manipulatívna správa, ktorá má človeka dotlačiť k zdieľaniu kódov a hesiel.

Digitálny dohľad nie je láska: ako získať kontrolu späť

Čo teda robiť, keď máte pocit, že nejde len o žiarlivosť, ale o digitálny dohľad? Najprv si pripomeňte, že bezpečnosť je aj o stratégii. Ak máte podozrenie na stalkerware alebo sledovanie, prudké kroky môžu situáciu eskalovať, najmä ak je vo vzťahu prítomná agresia či hrozby. „Pri podozrení na stalkerware je dôležité postupovať opatrne. Náhle odinštalovanie môže eskalovať správanie páchateľa,“ upozorňuje Krahulecová. V takom prípade býva rozumnejšie poradiť sa s odborníkmi,

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava

bezpečnostnou linkou alebo políciou a zároveň si vytvoriť plán. Získať kontrolu nad účtami, vymeniť heslá z bezpečného zariadenia, zapnúť dvojfaktorové overenie, skontrolovať zdieľanie polohy a oprávnenia aplikácií, a prejsť aj nenápadné miesta ako rodinné skupiny, cloudové albumy, zdieľané kalendáre, prihlásené zariadenia. „Nielen v súvislosti s Dňom zaľúbených, ale prakticky kedykoľvek a kdekoľvek je preto potrebné, užitočné a preventívne pripomínať si kybernetické i osobné riziká, ktoré vyplývajú z prílišnej dôvery a následnej moci, ktorú vkladáme do rúk partnera, partnerky ak zdieľame naše osobné údaje, citlivé informácie, prístupy či polohu. Prísľub bezpečia, ochrany, podpory sa môže odhaliť alebo zmeniť na sledovanie, dohľad, nátlak, obťažovanie, šikanovanie, manipuláciu, agresiu, násilie. Uchovajme si, prosím, osobnú integritu, ostražitosť, obozretnosť v mene ozajstnej individuálnej slobody a skutočného bezpečia,“ apeluje na bezpečnosť sociologička Porubánová.

A možno najdôležitejšie je vrátiť technológii jej správnu rolu. „Má slúžiť človeku, nie nahrádzať dôveru. Lebo vzťah, v ktorom je poloha povinnosť, heslo majetok a súkromie podozrenie, sa časom mení na niečo, čo už nie je intímne, ale incident,“ dodáva Krahulcová. Zdieľajte polohu len vtedy, keď je to dobrovoľné, časovo ohraničené a bezpečné. Účty chráňte tak, akoby k nim raz mohol mať prístup niekto, koho dnes milujete, no zajtra sa ho môžete báť. Ak sa dohľad stane nástrojom nátlaku, riešte to ako bezpečnostný problém, nie ako partnerskú výmenu názorov.

Qubit Conference® je najpopulárnejšia cyber konferencia v strednej Európe, ktorá víta odborníkov, bezpečnostných špecialistov a majiteľov podnikov z celého sveta. Jedným z výnimočných aspektov Qubit Conference® je medzinárodná účasť, ktorá prispieva k globálnemu pohľadu na problematiku kybernetickej bezpečnosti a je zárukou vysokokvalitného obsahu. Konferencia tiež slúži ako platforma pre prezentáciu najnovších inovácií a technologických trendov v oblasti kybernetickej bezpečnosti a poskytuje možnosť na prepojenie s priemyslom a obchodnými partnermi.

WEBwww.qubitconference.com**EMAIL**info@qubitconference.com**OFFICE**

Qubit Conference®
Martinčekova 17
821 01 Bratislava