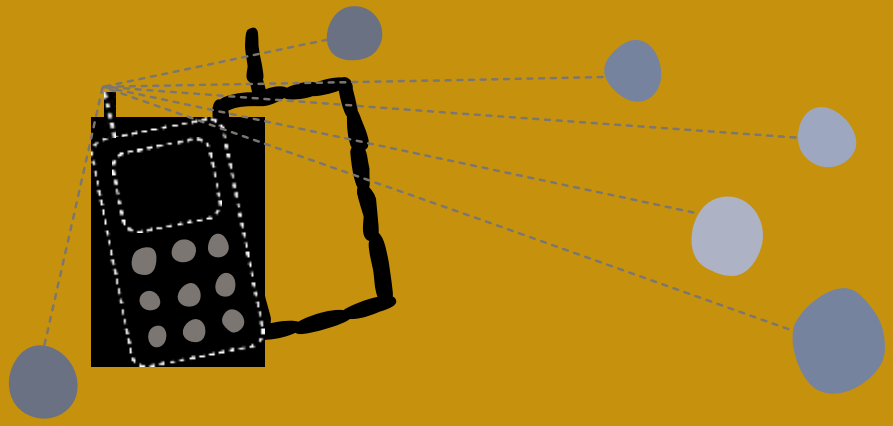
Siguria dhe privatësia e telefonave celularë dhe internetit



TEKNOLOGJITË E REJA, SIÇ JANË TELEFONAT CELULARË DHE INTERNETI, JANË MJETE TË FUQISHME PËR AVOKIM, POR DUKE PËRDORUR ATO PËR KOMUNIKIM TË INFORMACIONEVE TË NDJESHME, MUND TË KRIJONI RREZIK PËR JU, KONTAKTET TUAJA, MIQTË DHE KOLEGËT. KJO KARTË DO TË NDIHMOJË QASJEN NË INFORMACION NË MËNYRË TË SIGURT DHE TË MBRONI TË DHËNAT TUAJA KUR SHFRYTËZONI TELEFONA CELULARË DHE INTERNET.

ÇFARË ËSHTË SIGURIA DIGJITALE DHE PRIVATËSIA?

Shenjat që të drejtat informative dhe siguria digjitale është komprometuar mund të përfshijnë:

- Ndryshim misterioz të fjalëkalimeve
- Porositë private që duket se kanë qenë të lexuara nga dikush tjetër dhe jo nga marrësi i synuar
- Faqet e internetit që janë bërë të pa arritshme nga shtete të caktuara
- Zyrtarët qeveritar kanë zbuluar apo shpalosur njohuri në lidhje me korrespondenca private, duke përfshirë edhe datat, emrat apo temat e diskutuara
- Bisedat me telefona celularë, që individët besojnë se janë monitoruar

A DUHET TË BRENGOSEM PËR KËTË?

Në qoftë se skenare të tilla do të kompretojnë projektet tuaja ose do të vë në dukje ju ose kontaktet tuaja të ndiqeni penalisht, atëherë ju duhet të jeni të shqetësuar. Njohuritë dhe zgjidhjet softuerike të nevojshme për të kryer sulme të tilla në privatësinë tuaj digjitale shpesh janë në dispozicion në internet.
Në qoftë se sulmuesi ka qasje të mjaftueshme në internet ose infrastrukturë

të telefonisë celulare në vendin tuaj, teknologjia e nevojshme është fare e thjeshtë. Agjencitë qeveritare, ofruesit e shërbimeve të internetit (ISP) dhe kompanitë e telefonisë celulare kanë qasje të privilegjuar në atë infrastrukturë, por kolegët nga zyra, fqinjët dhe operatorët e internet kafeneve mund të ketë disa qasje.

CILAT ÇËSHTJET TË SIGURISË JANË MBULUAR NË KËTË KARTELË?

Kjo kartelë është e fokusuar në telefonat celularë dhe mjetet e bazuara në internet. Megjithatë, ka shumë teknologji të tjera që mund të ju lënë të pambrojtur në censurë, mbikëqyrje, dhe në ndjekje penale. Edhe pse ato nuk janë diskutuar këtu, përditësimi i rregullt i sistemit tuaj operativ i kompjuterit tuaj, anti-malware softueri i besueshëm, dhe procedurat konzistente të ruajtjes së të dhënave, janë masat më të rëndësishme themelore. Nëse keni arsye për të besuar se kompjuterët tuaj ose pajisjet për ruajtjen e të dhënave, duke përfshirë edhe kthimin prapa të të dhënave tuaja, janë në rrezik të humbin, vidhen apo të konfiskohen, ose që organizata juaj mund të jetë subjekt i mbikëqyrjes në internet (ose në qoftë se kjo është e zakonshme në rajonet ku ju veproni), atëherë ju duhet t'i referoheni paketës së sigurimit të Tactical Tech.

Mjete për avokim të bazuara në internet

Kur përdorni mjetet publike të bazuara në ueb, të tilla si Blogger, Facebook, dhe Twitter për mobilizim apo koordinim, mos harroni që informacioni që ju ruani në platforma të tilla, në një farë mase bëhet pronë e operatorëve, dhe se shumë nga këto mjete vënë në dukje më shumë informacione, sesa ju mund të mendoni.

Kur i besoni një projekti të ndjeshëm të operatorit të ndonjë mjeti në internet, lexoni mirë politikat e tyre të privatësisë ose marrëveshjet e ofruara për përdoruesit. Mos harroni se edhe politika më e ndriçuar lë informacionin tuaj direkt nën kontrollin e administratorëve të platformës, të cilët do të jenë në gjendje të shpalosin, të shesin ose të vënë atë informacion në vend të gabuar, pa lejen ose njohurinë tuaj. Edhe nëse ju përfundon llogaria juaj, shumë nga këto faqe në fakt nuk fshijnë përmbajtjen që ju keni postuar apo të dhënat personale që ju keni dhënë. Së fundi, nëse nuk është e rëndësishme që ju të përdorni një shërbim të caktuar komercial, ose për shkak të qasjes së tij ose për shkak të lidhjes me përdorues të profilit më të ulët, mendoni në shfrytëzimin e disa nga alternativat që janë shumë më progresive nga aspekti i të drejtës: Blip.tv në vend të YouTube; riseup.net në vend se Gmail. Nëse keni burimet teknike, ju mund të aktivizoni shërbimet tuaja të bazuara në ueb.

Në qoftë se ju përdorni platforma komerciale, merrni masa paraprake për të mbrojtur veten nga individët me qëllim të keq, të cilët e dinë se si të gjejnë informacion privat në shërbime të tilla. Kjo është veçanërisht e vërtetë në platformat sociale të tilla si Facebook dhe MySpace.

Zhvilloni një kuptim të plotë nga tiparet private që janë ndërtuar në këto platforma, dhe mendoni për llojet e informacionit që ju mund pa qëllim të zbuloni për veten ose organizatën tuaj, për shembull, emrin tuaj të vërtetë, vendbanimin tuaj, vendet ku keni udhëtuar ose informacione në lidhje me ngjarje të ardhshme apo takime të planifikuara. Nëse jeni monitoruar një kohë më të gjatë, ky informacion mund të sigurojë gjithashtu një pasqyrë të shprehive dhe praktikave të punës tuaj.

Një teknikë e dobishme është që të krijoni llogari të shumta në ndonjë shërbim të bazuar në internet që ju përdorni, duke ju lejuar që të përdorni llogari të ndryshme ose profile për projekte të ndryshme, dhe për të mbajtur llogaritë testuese që ju mund t'i përdorni si 'spiun' mbi veten tuaj. Privatësia juaj është e mbrojtur më mirë në qoftë se jeni në gjendje ta kontrolloni, në mënyra të ndryshme, çka është zbuluar në lidhje me llogarinë tuaj, për shembull, me anë të kërkimeve të internetit, ose njerëz që mbajnë privilegje të veçanta të qasjes.

FJALËKALIMET

Shumica e burimeve të bazuara në internet varen nga një fjalëkalim i vetëm për të mbrojtur llogarinë tuaj. Nëse një individ me qëllim të keq ose organizatë mëson këtë fjalëkalim, kjo nuk ka rëndësi nëse i besoni administratorëve të faqes, apo se sa me kujdes ju keni testuar privatësinë tuaj: ju menjëherë do të humbni fshehtësinë tuaj dhe anonimitetin.

Mënyra më pak e njohur për të thyer një fjalëkalim: dikush mund të instaloj malware në një kompjuter që ju përdorni për të hyrë në një faqe

interneti të sigurt. Ose, dikush mund të monitorojnë lidhjen tuaj të internetit, përderisa ju hyni në një faqe interneti të pasigurt.

Që të mbroheni kundër llojit të parë të sulmit, përdorni kompjuterin tuaj, ose një kompjuter që mbahet nga dikush që ju besoni, dhe sigurohuni që sistemi i tij operativ dhe anti-malware softueri janë të përditësuar. Për t'u mbrojtur kundër llojit të dytë të sulmit, shërbimet më të popullarizuara të bazuara në ueb, si posta elektronike, rrjete sociale, blogerimi dhe video platforma në internet ofrojnë lidhje të sigurt, të quajtur HTTPS. Ju mund të kontrolloni nëse keni një lidhje të sigurt për një faqe, duke kërkuar për "https://' (në vend se vetëm 'http://') në fillim të shfletuesit tuaj për adresën. Shumë mjete të bazuara në internet, megjithatë nuk e përdorin HTTPS për të mbrojtur çdo informacion që jepni ose me të cilat keni qasje në faqet e tyre, përveç fjalëkalimit tuaj. Si rezultat i kësaj, në qoftë se dikush monitoron lidhjen tuaj për kohë të mjaftueshme, ata do të mësojnë se çfarë keni ruajtur në këtë faqe interneti. Mbrojtja juaj më e mirë kundër kësaj është që të përdorni mjetet e bazuara në internet që përdorin HTTPS për të gjitha faqet.

ANASHKALIMI I CENSURËS

Ju mund të përdorni autorizim (proxies) të sigurt të bazuar në internet, mjete për anashkalim të censurës ose softuer për të siguruar anonimitetin, të tilla si Tor, për të fshehur identitetin tuaj nga faqet e internetit që ju vizitoni ose të anashkaloni filtrat e internetit. Këto mjete janë të dobishme kur ju duhet për të hyrë në faqet e internetit që janë të bllokuara, për shembull për hulumtime, ose në mënyrë që të përditësoni të dhënat në internet platformat të tilla si Facebook.

TË JESH ANONIM NË INTERNET

Softueri për sigurinë e anonimitetit, i tillë si Tor është i dobishëm kur nuk dëshironi të zbuloni se cilat faqe të internetit i keni vizituar. Tor kthen lidhjen tuaj ndërmjet disa kompjuterëve të rastit të zgjedhur në bazë vullnetare në mënyrë që të parandalojë edhe ofruesin e shërbimit të internetit tuaj ose vëzhguesit të nivelit qeveritar që të dinë se çka keni punuar në internet. Megjithatë, mos përdorni Tor për të dërguar ose marrë informacione të ndjeshme nga faqe të pasigurta të internetit. Nëse jeni të lidhur në një faqe interneti që mbështet HTTPS, është e mundur për një nga kompjuterët të zgjedhur në bazë vullnetare të ju mundësojë për të përdorur Tor, për të monitoruar përmbajtjen përderisa ajo postohet. Tor është softuer mjaft i sigurt, por tani për tani ngadalëson lidhjen tuaj të internetit.

Telefonat celularë

Telefonat celularë janë përdorur nga mbrojtësit në të gjithë botën, por ata shpesh kanë ruajtur një pjesë të madhe të informacionit që duhet të mbahen private. Përveç listës së kontakteve, një telefon celularë mund të përmbaj historitë e thirrjeve, kalendarë, porositë tekstuale dhe postën elektronike.

Mendoni për informacionet që ruani në telefonin tuaj, veçanërisht për shkak se telefonat lehtë mund të konfiskohen. Për shembull, ju ndoshta nuk keni nevojë të mbani të gjitha kontaktet tuaja në celularin tuaj, nëse jeni duke bërë punë të ndjeshme si të drejtat, dhe ju duhet t'i fshini informacionet nga telefoni juaj dhe SIM kartela, sa herë që mundeni. Për organizimin e ngjarjeve apo për mobilizimin e rrjetit, është ide e mirë që të përdorni anonim SIM kartelë të para-paguar dhe të ndryshoni aparatin herë pas here. Sepse SMS lehtë kontrollohen dhe filtrohen, prandaj duhet të shmangni përdorimin e fjalëve kyçe të ndjeshme kur dërgoni porosi tekstuale. Për aq kohë sa janë të kyçur, telefonat celular mund të përdoren për të gjetur vendndodhjen tuaj. Njerëzit që marrin pjesë në një mbledhje të ndjeshme, duhet fikin telefonat e tyre dhe heqin bateritë, para se të dalin për në mbledhje, dhe të presin deri sa të kthehen në shtëpi dhe sërish t'i vendosin bateritë dhe të kyçin telefonat e tyre. Ofruesit e shërbimeve të telefonave celularë kanë qasje në të dhënat për të gjitha thirrjet: kur keni thirur, kur dhe ku keni qenë kur keni thirrur. Ofruesit mund të kenë detyrim ligjor që të regjistrojnë ose dorëzojnë këto detaje në qoftë se kjo kërkohet nga zyrtarët, dhe mund t'i mbajnë këto të dhëna për disa vjet.

AKTIVITET: IDENTIFIKIMI I RREZIQEVE TË SIGURISË SUAJ

Përdorni pyetjet e mëposhtme për të vlerësuar rreziqet e sigurisë dhe do të ju ndihmojë të vendosni se cilat mjete ju mund të përdorni për të larguar atë rrezik.

1. **Unë jam duke punuar me informacione të ndjeshme.** Është e rëndësishme të dini se keni të bëni me informacione të ndjeshme që mund të çojë të tjerët të ndjekin atë që ju bëni. A jeni përfshirë në aktivitete që mund të konsiderohen të ndjeshme ose përçarëse nga qeveria, policia, ushtria apo një kompani private? Nëse përgjigjja është po, ju mund të veni veten ose të tjerët në rrezik nëse nuk zbatoni disa masa të sigurisë.
2. **Unë punoj me njerëz, identiteti dhe të dhënat e të cilëve duhet të mbahen private.** Ndoshta ju jeni duke mbledhur informacione private nga njerëzit që ju mbështesin, të tilla si informacione në lidhje me dhunën në familje, punë të detyruar apo përdhunim. Nëse njerëzit iu japin informacione që mund t'i vë ata në rrezik, ju duhet të ndërmerrni hapa për t'i siguruar ata se është ruajtuar privatësia e të dhënave të tyre.
3. **Unë nganjëherë komunikoj me njerëz në internet të cilët merren me informacione të ndjeshme.** Edhe në qoftë se mendoni se nuk keni rreziqe të sigurisë, nëse komunikoni në internet me njerëz të cilët përballen me këto rreziqe, mund të jeni në shënjestër nga njerëz që i kundërshtojnë ata. Kjo është sepse njerëzit mund të ju përdorin për qasje të informacioneve private të të tjerëve.
4. **Kam qasje ose postoj përmbajtje në faqet e internetit që mund të konsiderohen të ndjeshme.** Ndoshta ju kontribuoni me informacion në faqet e internetit për të drejtat e njeriut, ose postoni artikuj në të cilat kundërshtohen grupe për të cilat besoni se nuk kanë respektuar të drejtat e njeriut. Thjesht edhe duke vizituar faqet e ndjeshme në internet ju mund të jeni një objektiv..

Burimet e sigurisë dhe privatësisë në internet

Për të mësuar më shumë dhe për të shkarkuar mjetet e sigurisë:

1. **Kutia e sigurisë** u krijua nga Tactical Tech dhe Front Line për të përmbushur nevojat e sigurisë digjitale dhe privatësisë së avokatëve dhe të mbrojtësve të të drejtave të njeriut. http://security.ngoinabox.org/
2. **Siguria digjitale dhe privatësia për Mbrojtësit e të Drejtave të Njeriut** nga Front Line ofron informata të dobishme për vlerësimin dhe trajtimin e kërcënimeve digjitale. http://bit.ly/1aCkSs (frontlinedefenders.org)
3. **Celularët në një kuti** nga Tactical Tech përmban një seksion të tërë për privatësinë dhe sigurinë në telefoninë celulare. http://mobiles.tacticaltech.org/security
4. **Blogim anonim me Wordpress dhe Tor.** Global Voices ka krijuar këtë udhëzues për të mbështetur të drejtat e mbrojtësve të të drejtave të njeriut, të cilët dëshirojnë të zbulojnë të vërtetën dhe të shprehin veten e tyre në internet, por që mund të vënë veten në rrezik duke bërë këtë. http://advocacy.globalvoicesonline.org/projects/guide/
5. **Të jesh anonim në internet dhe të shmangësh censurën.** Tor është dizajnuar për të rritur anonimitetin e aktiviteteve tuaja në internet dhe gjithashtu mund të përdoret për të anashkaluar filtrimin në internet. Ju mund ta shkarkoni në kompjuterin tuaj apo të aktivizoni atë nga një kartele memorie. http://www.torproiect.org/

ONEWORLDSEE
ONEWORLD PLATFORM FOR SOUTHEAST EUROPE
TACTICAL TECHNOLOGY COLLECTIVE