

2016 GPEN Sweep – Interneti i Gjërave*

(me një fokus mbi përgjegjësinë)

Panoramë

Sweep GPEN i vitit 2016 synoi kontrollin e praktikave të organizatave/kompanive ndërkombëtare në lidhje me mënyrën se si ato i adresojnë çështjet e privatësisë me klientët e tyre, subjekte të të dhënave, duke u fokusuar specifikisht në pajisjet e Internetit të Gjërave (IoT). Me rritjen në numër të pajisjeve që janë të lidhura me internetin, qasja me IeGJ (IoT) është e një rëndësie të madhe për Agjencitë Ligjzbatuese të Privatësisë (ALP). Pajisjet/aplikacionet u mundësojnë njerëzve të kontrollojnë dhe mbikëqyrin shumë aspekte të jetës së tyre, që nga gjurmimi i aktivitetit fizik e deri në aktivizimin e ngrohjes qendrore nga telefoni i tyre. Pajisje/aplikacione të tilla kanë potencialin për të mbledhur një sasi të madhe të dhënash personale nga përdorues të ndryshëm dhe është e rëndësishme për t'u theksuar se konsumatorët duhet të informohen plotësisht se çfarë ndodh me të dhënat personale që ata u transmetojnë këtyre pajisjeve/aplikacioneve.

Në këtë aksion u përdorën një larmi metodologjish, përfshirë por jo e limituar në:

Shënim: Numri i ALP që përdorin metodën e tyre tregohet më poshtë.

- Kontrolli i komunikimeve në kohë reale të privatësisë dhe materialeve të disponueshme për përdorues potencialë të një produkti (p.sh. përpara blerjes) – 21 ALP;
- Komunikimi direkt me kompanitë – gojarisht dhe me shkrim – 14 ALP;
- Kontrolli i pajisjeve/aplikacioneve – kontrolli se çfarë informacioni është dhënë për produktin dhe si funksionon në praktikë mbrojtja e privatësisë – 9 ALP.

ALP zgjedhën ta fokusojnë aksionin e tyre monitories mbi lloje pajisjesh të një rëndësie dhe interesi të veçantë për ta. Llojet e pajisjeve/aplikacioneve të kontrolluar nga ALP përfshijnë:

Shënim: Numri i ALP që kontrollojnë lloje të ndryshme pajisjesh është si më poshtë.

- Matësa inteligjente (për konsumin e energjisë/ujit/gazit)– 2 ALP;
- Pajisjet e përdorimit të sigurimit bazë – 1 ALP;

- Pajisja e gjendjes fizike –10 ALP;
- Pajisjet shtëpiake – 6 ALP;
- Pajisje të lidhura me kontrollin e shëndetit (p.sh. matës i tensionit, monitorët e gjumit) –11 ALP;
- Makinat e lidhura me internet –1 ALP;
- Lojrat e lidhura me internet –1 ALP;
- Televizorët inteligjentë – 2 ALP;
- Transponderët – 1 ALP;
- Video survejimi CCTV –1 ALP.

Konstatime përmbledhëse

Komunikimet e privatësisë që lidhen me pajisjet IoT janë në përgjithësi të varfra dhe nuk informojnë përdoruesit se çfarë kategorie të dhënash mbledhet saktësisht nga ato dhe se çfarë ndodh më pas me këtë sasi të dhënash personale. Në veçanti, pajisjet/aplikacionet në politikat e privatësisë neglizhojnë shpjegimet rreth mënyrës së arkivimit dhe se si një përdorues mund të fshijë të dhënat e tij personale. Të marra në tërësi, pajisjet/aplikacionet grumbullojnë një sasi të madhe të dhënash personale (sasia ndryshon nga lloji i pajisjes/aplikacionit, por ka edhe disa të tilla që mbledhin shumë pak të dhëna). Sidoqoftë, komunikimet e privatësisë janë, në përgjithësi, jo të specifikuara në pajisje/aplikacione. Kompanitë që shpallin praktika të mira janë të pakta dhe ALP mendojnë, në përgjithësi, se ka vend për përmirësim të komunikimeve të privatësisë.

Të dhënat kryesore

Autoritetet e Mbrojtjes së të Dhënave (AMD) që komunikuan rezultate: 25
Pajisjet/aplikacionet e kompanive të kontrolluara:314

Llojet e kompanive të ekzaminuara

Prodhuese: 179

Shitëse me pakicë: 20

Shpërndarëse: 7

Ofruese:18

Institucione shtetërore: 79

Reklamuese: 4

Kontrollues të tjerë të dhënash:7

Shënim metodologjie: jo të gjithë AMD raportuan për çdo fushë. Si rezultat, statistikat për këtë aksion u përpiluan bazuar mbi grumbullimin e të dhënave për një fushë të caktuar raportuese, si një përqindje e atyre pajisjeve/aplikacioneve të kontrolluara nga ato AMD që raportuan për atë fushë të caktuar.

Mbledhja, përdorimi dhe përhapja e të dhënave (Indikatori 1)

ALP pjesëmarrëse në këtë aksion raportuan se 60% e pajisjeve/aplikacioneve nuk u shpjeguan mjaftueshëm përdoruesve se si u mblodhën, përdorën apo u përhapën të dhënat e tyre personale.

Informacioni i mëposhtëm (si dhe informacioni i sektorit tjetër specifik) u mblodh mbi baza detyruese apo fakultative nga pajisja e kontrolluar:

- Emri/mbiemri – 84% e pajisjeve;
- E-mail – 83% e pajisjeve;
- Ditëlindja/mosha – 64% e pajisjeve;
- Vendndodhja – 68% e pajisjeve;
- Adresa – 53% e pajisjeve;
- Numri i telefonit – 55% e pajisjeve;
- Fotografi/video/regjistrim audio – 41% e pajisjeve;
- Identifikues unik – 61% e pajisjeve.

Lloje të caktuara pajisjesh/aplikacionesh grumbullonin, gjithashtu, më shumë të dhëna personale sensitive (p. sh. pajisjet mjekësore të lidhura me internetin dhe disa matës të gjendjes fizike mblidhnin detaje nga përdoruesit e tyre). Shumë nga këto pajisje/aplikacione grumbullonin të dhëna rreth peshës dhe gjatësisë së përdoruesve të tyre.

Prirjet e identifikuar në lidhje me Indikatorin 1:

- Politikat e privatësisë shpesh nuk ishin specifike nëpër pajisje. Shumë nga ato ishin projektuar për mbulimin e një numri shërbimesh të ofruara nga organizata dhe disa të tjera, të fokusuara mbi ndërveprimin e përdoruesve me faqen zyrtare në internet, në raport me projektimin dhe veprimin e vetë pajisjes.
- Në shumë raste, politikat e privatësisë japin shembuj të të dhënave që mund të mblidhen, në vend që të listojnë të dhënat që grumbullojnë.

- Disa organizata priren të interpretojnë termin “të dhëna personale” në mënyrë të ngushtë, për të përfshirë vetëm ato më të zakonshmet (p.sh.emri/mbiemri, numri i telefonit, adresa, etj) dhe nuk arrijnë të jenë të qarta se informacioni tjetër, si p.sh. numri i hapave të hedhura dhe kaloritë e djegura, mund të jenë, gjithashtu, të dhëna personale, nëse ato i bashkëlidhen të dhënave të tjera të një individi të identifikueshëm.
- Shpesh, eksperiencia e përdoruesit nuk u përshtat me komunikimet e privatisë.
- Disa pajisje/aplikacione mbledhnin të dhëna sensitive (veçanërisht, pajisjet/aplikacionet mjekësore) dhe ky qëllim nuk është përmendur në politikat e privatësisë.
- Disa herë u konstatua se grumbullimi i të dhënave personale ishte i papritur, sepse kompanitë nuk qartësonin qëllimin (p.sh. një pajisje/aplikacion për jetesën e shëndetshme grumbullonte të dhëna të caktuara mjekësore – matjet e tensionit të gjakut për një periudhë të caktuar; ALP konstatuan se njëkohësisht pajisja/aplikacioni grumbullonte llojeve të tjera të dhënash personale, si vendndodhja dhe data e lindjes së përdoruesit).
- ALP nxitën disa kompani, që ofrojnë një grup të madh produktesh, të plotësonin politikat e privatësisë me më shumë detaje (p.sh. politika specifike për matësat e gjendjes fizike).
- ALP e konsideruan si arritje faktin se disa kompani patën një qasje specifike për privatësinë.
- Pavarësisht mungesës së detajeve, në disa raste politikat e privatësisë ishin të qarta, koncize dhe të shkruara në gjuhë të thjeshtë.
- ALP e konsideruan si arritje faktin se disa kompani përfshijnë në komunikimet e privatësisë konceptin “në kohë” për përdoruesit e në momentin kur ata i ngarkojnë të dhënat e tyre personale, duke i informuar kështu ata për çfarë kërkohen të dhënat personale.

Arkivimi i të dhënave (Indikator 2)

ALP konstatuan se 68% e pajisjeve nuk u shpjegojnë siç duhet klientëve se si i arkivojnë informacionet e mbledhura nga pajisjet/aplikacionet e tyre.

Gjithashtu, 68% e kompanive nuk informojnë nëse të dhënat personale të mbledhura nga pajisjet/aplikacionet e tyre u arkivuan në mënyrë të koduar.

Në shumë raste, ALP vunë re se në politikat e privatësisë arkivimi nuk ishte përfshirë fare si shërbim, apo edhe nëse përmendej, detajet për këtë proces ishin të paqarta. Politikat e privatësisë rrallë herë informonin përdoruesit për periudhën e ruajtjes, shtetin në të cilin ruheshin dhe në cilën mënyrë (p.sh. informacioni arkivohej në vetë pajisjen, apo ruhej në mënyra të tjera).

49% e pajisjeve/aplikacioneve të kontrolluara nuk i informonin përdoruesit se cili ishte niveli i sigurisë për të dhënat e tyre personale dhe cilat masa merreshin në rastet e përhapjes së këtyre të dhënave nga përdorues të paautorizuar (p.sh. përdorimi i fjalëkalimeve, ose pyetjeve specifike autentike).

Detajet për kontaktet (Indikator 3)

ALP konstatuan se 38% e pajisjeve/aplikacioneve nuk jepnin të dhëna për të kontaktuar lehtësisht, në rastet kur konsumatorët kishin shqetësime për privatësinë e tyre.

Duke marrë në konsideratë sasinë e informacionit që disa pajisje grumbullojnë, përdoruesit duhet të jenë të sigurt që nëse ata kanë shqetësime, ato duhet sa më shpejt të adresohen tek personi/ekipi përgjegjës në strukturën e kompanisë.

Fshirja e të dhënave (Indikator 4)

ALP zbuluan se rreth 72% e kompanive nuk dhanë shpjegime të sakta se si përdoruesit mund t'i fshijnë/shkatërrojnë të dhënat e tyre personale nga pajisjet/aplikacionet. Vetëm 16% e këtyre kompanive paraqitën informacion për instrumentat në dispozicion të përdoruesve për fshirjen/shkatërrimin e të dhënave personale në rastet e shitjes së pajisjes/aplikacionit, apo mospërdorimit më të saj/tij. Në mënyrë të ngjashme, 13% e kompanive dhanë informacione të qarta për instrumentat/mënyrat se si konsumatorët mund të fshinin/shkatërronin në mënyrë manuale të dhënat e tyre personale, në rastet e humbjes apo vjedhjes së pajisjes/aplikacionit.

ALP raportuan se në shumë raste procesi i fshirjes ishte shumë i ndërlikuar. Në disa raste, përdoruesit nuk kishin mundësi të fshinin të dhënat direkt në aplikacion, por këtë mund ta realizonin në faqen zyrtare

të kompanisë në internet. Po ashtu, në shumë raste edhe kur përdoruesit ishin të informuar për mënyrën e ç'aktivizimit të llogarisë së tyre në aplikacion, kompania nuk dha informacion të saktë se çfarë ndodhte me të dhënat personale dhe nëse kjo nënkuptonte se ato do të fshiheshin.

Përgjigje në kohë, e përshtatshme dhe e saktë nga kompania (Indikatori 5)

ALP konstatuan se shumë organizata jepnin përgjithësisht me vonesë një përgjigje për shqetësimet/pyetjet, ndërsa disa të tjera nuk jepnin fare asnjë përgjigje. Kështu, 43% e kompanive të kontaktuara dështuan të jepnin një përgjigje në kohë, të përshtatshme dhe të qartë. Tre ALP raportuan se konstatuan një tregues mesatar për një përgjigje prej 50% ose më pak, ndërsa një ALP raportoi se nuk mori asnjë përgjigje.

Përfundime

Në mënyrë të përmbledhur, komunikimet e privatësisë që kanë lidhje me pajisjet IeGj (IoT) janë përgjithësisht të varfëra dhe nuk dhanë informacione se çfarë ndodh me të dhënat personale që këto pajisje grumbullojnë. Gjetjet e këtij aksioni janë në përputhje edhe me studime të tjera. Për shembull, Forumi për të Ardhmen e Privatësisë ka konstatuar se një numër i konsiderueshëm i aplikacione për shëndetin, nuk u jep përdoruesve madje as informacione bazike, se si të dhënat e tyre personale grumbullohen, përdoren apo përhapen. ALP vijojnë të inkurajojnë organizatat për të përmirësuar praktikën e tyre në këtë fushë, për të siguruar se përdoruesit janë në gjendje të kuptojnë se si trajtohen të dhënat e tyre në çdo fazë të procesit: grumbullimi, përdorimi; përhapja dhe arkivimi. Përdoruesit duhet, gjithashtu, të informohen se si të kenë kontroll mbi të dhënat e tyre, p.sh. nëse ata dëshirojnë t'i fshijnë këto të dhëna.

Të tjera përfundime

- Ka prezencë të konsiderueshme në treg një lloj pajisjeje që lidh në kohë reale shumë përdorues (p.sh. për të konkuruar për diçka, ose për të rakorduar kalendarin/agjenden e anëtarëve të një familje).

- Disa pajisje/aplikacione kanë funksionin për të dërguar rezultate tek mjekët, ose tek çdokush që ka lidhje me rastin, duke përdorur adresa të zakonshme e-mail-i të pakoduara.
- Disa pajisje/aplikacione kanë vendosjen e parazgjedhur (default setting) si masë të fundit mbrojtëse për privatësinë, p.sh. qasjen nga “të gjithë”, në vend të qasjes për grupe specifike përdoruesish, lidhje unike ose një përdoruesi të vetëm (përveç se të domosdoshme për të mbështetur funksionimin e pajisjes).

*Ky është një përkthim jo zyrtar i Zyrës së Komisionerit.