Datu noplūdes: No pazaudētiem dokumentiem līdz izspiedējvīrusiem

diena.lv, 13/03/2018, Diena.lv

Pēdējos mēnešos teju visiem uz mēles ir Vispārējās datu aizsardzības regulas jeb GDPR iedzīvināšanas izaicinājums. Kaut arī daļa sūkstās par laikietilpīgo un dārgo procesu, tomēr, ilgtermiņā raugoties, ieguvēji ir gan uzņēmēji, gan privātpersonas, portālam Diena.lv pavēstīja zvērinātu advokātu biroja Sorainen advokāts un partneris Agris Repšs.

Pēc eksperta paustā, GDPR (no angļu: General Data Protection Regulation) ieviešana, protams, negarantē, ka nākotnē nesaskarsimies ar datu noplūdēm un kiberuzbrukumiem, taču regula uzņēmējiem liek ar datiem rīkoties atbildīgi, kā arī pārskatīt un pārvaldīt ar to glabāšanu saistītos procesus. Sabiedrības uzmanības lokā ir nonācis ne viens vien skandāls par uzlauztām sistēmām un noplūdušiem datiem, no kuriem varētu izvairīties, ja uzņēmumi būtu pievērsuši pienācīgu uzmanību apstrādāto datu aizsardzībai.

"Regulas prasību ieviešanā vienlīdz liela nozīme ir gan juridiskajiem, gan informācijas tehnoloģiju procesiem, tāpēc Sorainen apvienoja spēkus ar IT uzņēmumu Squalio un radīja vienotu pakalpojumu GDPR Ready," piebilda Repšs.

Uzņēmuma pārstāvji ir sagatavojuši sarakstu ar piemēriem, kas ilustrē datu drošības nepieciešamību.

Uber samaksā hakeriem 80 000 eiro

2016.gadā hakeri uzlauza Uber datu bāzes un piekļuva 57 miljonu klientu vārdiem, uzvārdiem, e-pastiem un mobilo tālruņu numuriem, kā arī 600 tūkstošu taksometru vadītāju personas datiem, tostarp informācijai par licencēm. Notikušais nāca gaismā vien 2017.gadā - izrādās Uber hakeriem samaksājis 80 tūkstošus eiro, lai nozagtie dati tiktu dzēsti un netiktu izmantoti.

"Faktiski visi šie cilvēki var kļūt par upuri dažādiem kiberuzbrukumiem – krāpniecībai e-pastā, pikšķerēšanai un pat identitātes zādzībai. "Uber" taksistiem nodrošina bezmaksas aizsardzību, lai šo cilvēku vārdā netiktu noformēti krāpnieciski aizņēmumi, bet cietušajiem klientiem pagaidām nekas nav piedāvāts," norāda Sorainen sadarbības partnera Squalio pārstāvis Mareks Gruškevics.

Lietuviešu plastiskās ķirurģijas klīnika izspiedējiem nesamaksā un nonāk skandālos

2017.gadā pavasarī atklājās, ka kibernoziedznieki ir nozaguši lietuviešu plastiskās ķirurģijas klīnikas Grožio Chirurgija pacientu datus, fotogrāfijas, tostarp kailfoto, "pirms un pēc" foto un izlikuši tos pārdošanā "tumšajā internetā" (dark web). Cenas svārstījās no 50 līdz 2000 eiro par pacienta kartīti, bet visu kopumu varēja iegādāties par 300 bitkoiniem jeb aptuveni 344 tūkstošiem eiro. Pacientu vidū bija gan vietējās, gan starptautiskās slavenības, kuras šie kibernoziedznieki arī šantažēja.

Hakeri publiskoja informāciju, ka vispirms viņi centušies šantažēt klīniku, nodēvējot izpirkuma maksu par salīdzinoši nelielu sodu par vājajām IT sistēmām, ko šī medicīnas iestāde izmanto. "Klīnika atteicās to darīt (šķiet, viņiem ir ļoti, ļoti, ļoti liels EGO), tādēļ mēs izveidojām šo vietni un piedāvājam datus nopirkt jebkuram," rakstīja pārkāpēji. Saiti uz vietni ar nozagtajiem personu datiem noziedznieki nosūtīja vienam no lielākajiem Lietuvas medijiem 15min.lt. Plašāk par gadījumu šeit.

Arī Deloitte kritusi par upuri kiberuzbrukumam

Diemžēl arī viena no pasaulē lielākajām auditorfirmām Deloitte, konkrētāk, tās Ņujorkas birojs cieta kiberuzbrukumā, kura rezultātā tika uzlauzta uzņēmuma e-pastu sistēma, pērn septembrī rakstīja The Guardian. Tiek uzskatīts, ka hakeri, iespējams, piekļuvuši informācijai par uzņēmuma labākajiem ("blue-chips") klientiem – uzvārdiem, parolēm, personiskai informācijai un konfidenciālai sarakstei. Starp cietušajiem pārsvarā esot ASV klienti, bet potenciāli arī klienti no Lielbritānijas.

"Kompānija uzbrukumu esot atklājusi 2017.gada martā, tomēr tiek uzskatīts, ka hakeri sistēmām piekļuva vēl 2016.gada rudenī. Efektīvi izveidota IT sistēma ļauj šādus uzbrukumus pamanīt daudz agrāk. Turklāt, ja iepriekš uzņēmumi paši varēja izlemt informēt vai neinformēt par notikušo incidentu, tagad no tā vairs nevarēs izvairīties, jo GDPR nosaka, ka par visiem incidentiem ir jāziņo obligāti," skaidro Gruškevics.

Zviedrijā sensitīvu datu noplūdes dēļ krēslu zaudē divi ministri

Zviedrijā sensitīvu datu noplūdes dēļ pērn augustā amatu zaudēja iekšlietu ministrs Anderss Jegmans, infrastruktūras ministre Anna Johansone un Nacionālās transporta aģentūras (NTA) vadītāja Marija Agrēna, vēstīja The Guardian.

Kā raksta medijs, pārkāpums noticis 2015.gadā, kad Zviedrijas NTA kā ārpakalpojumu nolīgusi kādu IT kompāniju, taču nav veikusi uzņēmuma personāla pārbaudi. Starp noplūdušajiem datiem esot nacionālā auto vadītāju licenču datu bāze, iespējams, arī slepeno dienestu, armijas un policijas transporta informācija, kā arī ziņas par personām, pret kurām sāktas kriminālllietas, un liecinieku aizsardzības programmā iekļautiem cilvēkiem. Tiesa, NTA noliedza, ka viņu rīcībā bijusi militāra informācija. Turklāt līdz šim neesot ziņu ka dati "būtu izplatīti kādā neatbilstošā veidā".

"2017.gadu mēdz dēvēt par kibergedonu, jo uzņēmumi un privātpersonas piedzīvoja skandalozus uzbrukumus, piemēram, WannaCry, NotPetya un citus. Tāpēc GDPR ieviešana ir loģisks Eiropas Savienības lēmums, proti, uzņēmējiem ir uzlikts pienākums rūpēties par klientu privātumu un drošību," secina Repšs. Viņš gan piebilst, ka vienlaikus arī pašiem cilvēkiem jākļūst apdomīgākiem un piesardzīgiem, daloties ar saviem un ģimenes locekļu datiem.

ZAB Sorainen un IT uzņēmums Squalio ir apvienojuši zināšanās un izveidojuši produktu GDPR Ready, kas ietver neatkarīgu juridisko

un IT sistēmu auditu, profesionālus ieteikumus nepieciešamajām izmaiņām, lai uzņēmums būtu gatavs GDPR.

https://www.diena.lv/raksts/viedokli/latvija/datu-nopludes-no-pazaudetiem-dokumentiem-lidz-izspiedejvirusiem-14193148