Univerzitetna založba
Univerze v Mariboru

Varstvo osebnih podatkov na področju distribucije električne energije

BOŠTJAN KEŽMAH

Povzetek Varstvo osebnih podatkov trenutno ostaja osrednji normativni mehanizem za splošno zagotavljanje varnosti informacijskih sistemov. Predpisi usmerjajo upravljavce informacijskih sistemov k dobrim praksam upravljanja, vodenja in zagotavljanja varnosti informacijskih sistemov. Pomemben del varnostnih kontrol so revizijske sledi in dosledna identifikacija osebnih podatkov. V prispevku analiziramo definicijo revizijske sledi, njen pomen ter na praktičnih primerih predstavimo identifikacijo osebnih podatkov na področju distribucije električne energije.

Ključne besede: • varstvo osebnih podatkov • distribucija električne energije • informacijski sistem • revizijska sled • identifikacija •

NASLOV AVTORJA: dr. Boštjan Kežmah, višji predavatelj, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Smetanova ulica 17, 2000 Maribor, Slovenija.

https://doi.org/10.18690/978-961-286-071-4.11 ISBN 978-961-286-071-4

Dostopno na: http://press.um.si.

University of Maribor Press

Personal Data Protection in Electric Energy Distribution

BOŠTJAN KEŽMAH

Abstract Personal data protection remains a central regulatory mechanism for ensuring the overall security of information systems. The regulations guide information systems owners towards best governance, management and information security practices. An important part of security controls are audit trails and systematic identification of personal data. In this paper, we analyse the definition of the audit trail, its importance and practical examples to present identification of personal data in the area of electricity distribution.

Keywords: • personal data protection • electric energy distribution • information system • audit trail • identification •

CORRESPONDENCE ADDRESS: Boštjan Kežmah, Ph.D., Senior Lecturer, University of Maribor, Faculty of Electrical Engineering and Computer Science, Smetanova ulica 17, 2000 Maribor, Slovenia.

https://doi.org/10.18690/978-961-286-071-4.11 ISBN 978-961-286-071-4

Available at: http://press.um.si.

1 Uvod

Varstvo osebnih podatkov postaja vse pomembnejši vidik zagotavljanja varnosti informacijskih sistemov. Pri tem se velikokrat postavlja vprašanje kaj je osebni podatek, čeprav je v zakonu jasno opredeljen kot katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen [1]. Kadar je podatek osebni podatek, morata upravljavec in morebitni pogodbeni obdelovalec osebnih podatkov zagotoviti, da se ti podatki obdelujejo skladno s predpisi.

Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1) v 5. odst. 24. čl. določa, da zavarovanje osebnih podatkov obsega tudi ukrepe, ki omogočajo poznejše ugotavljanje kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil. Veliko upravljavcev in pogodbenih obdelovalcev osebnih podatkov po naših izkušnjah dojema to določbo kot izrazito pretirano, nesorazmerno in nepotrebno. Pa je res tako?

2 Dnevniki informacijskega sistema

Velika večina sodobne programske opreme pri svojem delovanju ustvarja t.i. dnevniške zapise. Cilji beleženja dnevniških zapisov so različni, od beleženja dogodkov z namenom odkrivanja napak v delovanju operacijskega sistema, programske in druge opreme, do beleženja aktivnosti uporabnikov z namenom vrednotenja uporabniške izkušnje in beleženja aktivnosti uporabnikov z namenom kasnejšega ugotavljanja kdo, kdaj in katere funkcije v informacijskem sistemu je uporabljal.

Izrazit primer predstavlja operacijski sistem Windows, ki privzeto beleži pomembnejše dogodke, kot je npr. namestitev nove programske opreme, prijava uporabnika v operacijski sistem, izklop operacijskega sistema ipd. Le redki lastniki informacijskih sistemov pa se tega zavedajo in se odločijo, da bodo privzete nastavitve spremenili. Med pomembnejšimi nastavitvami so število dogodkov, ki naj jih operacijski sistem ohrani.

V sklopu revizij informacijskega sistema pogosto ugotavljamo, da upravljavci informacijskega sistema ne poznajo odgovora na vprašanje za koliko časa lahko zagotovijo dnevniške zapise operacijskega sistema. Ko namreč število zabeleženih dogodkov prekorači vnaprej nastavljeno vrednost, najstarejše dogodke operacijski sistem samodejno izbriše.

Nekoliko višja stopnja zrelosti je značilna za procese, kjer so dnevniki pomembni pri operativnem delu. Primer takih procesov so podpora uporabnikom, odprava napak v delovanju programske in mrežne opreme. V teh okoliščinah so dnevniki nepogrešljiv pripomoček za natančnejšo identifikacijo in odpravo napake in imajo praviloma uporabniki teh dnevnikov interes, da skrbijo za njihovo obstojnost in ustrezno vsebino.

Pri izvajanju nadzornih funkcij, kot je npr. revizija informacijskega sistema, so v dnevnikih ključni podatki za izvedbo analize stanja delovanja notranjih kontrol. Predstavljajo pomembne vhodne podatke, na podlagi katerih lahko revizor informacijskih sistemov s pomočjo statističnih in drugih metod odkriva vzorce, nepravilnosti in sumljive dogodke v množici dnevnikov in na ta način bolj uspešno pripravi oceno tveganja, ki je osnova za pripravo revizijskega načrta. Dnevniki so pomemben vir podatkov tudi kasneje, pri testiranju delovanja notranjih kontrol.

Ker naj bi nadzor temeljil na objektivnih, preverljivih in avtentičnih podatkih, se predvsem v zvezi z avtentičnostjo pri podrobni obravnavi posameznih zapisov odpirajo dodatna vprašanja. V primeru, ko v sklopu nadzora ugotovimo pomembne nepravilnosti ali celo goljufije, je namreč bistveno, da je mogoče te ugotovitve povezati s točno določenim uporabnikom. Za potrebe dokazovanja na sodišču je lahko tudi to premalo, saj je treba tudi računalniško identiteto uporabnika povezati s točno določeno osebo.

3 Revizijske sledi

Dnevnik, ki ga želimo uporabiti kot zanesljiv dokaz, mora torej imeti dodatne značilnosti. Te značilnosti praviloma bistveno presegajo obseg tehnične rešitve (kot je shranjevanje podatkov v datoteko), ampak predstavljajo skupek organizacijskih, tehničnih in logično-tehničnih postopkov in ukrepov, ki zagotavljajo avtentičnost in celovitost dnevniškega zapisa.

Pri tem avtentičnost pomeni, da je zapis nastal kot posledica dejansko izvedene aktivnosti uporabnika in da je zapis izdelala prav programska oprema, ki je navedena v dnevniku oz. upravlja predmetni dnevnik, celovitost pa nakazuje, da lahko zaupamo podatkom dnevnika v smislu, da se podatki niso spremenili ter da dnevnik ne vsebuje umetno dodanih ali drugače zavajajočih podatkov ter da posamezni podatki niso bili izbrisani.

Kadar so izpolnjeni ti pogoji, ne govorimo več o dnevniškem zapisu, temveč o revizijski sledi. Po definiciji stroke revizije informacijskih sistemov je revizijska sled od izvirnega dogodka ločen zapis ali več zapisov, ki se nanašajo na izvirni dogodek v informacijskem sistemu, z navedbo vseh ključnih podatkov za enolično prepoznavo okoliščin nastanka dogodka, kot tudi njegovih posledic. Revizijska sled mora biti nedvoumna, neizpodbitna, celovita, nespremenljiva in trajna [2]. Uspešnost beleženja revizijske sledi je neločljivo povezana s splošnimi notranjimi kontrolami informacijskega sistema .

Tudi kontrolni okvir upravljanja in vodenja informacijskih sistemov COBIT 5 v vodstveni praksi DSS05.04 določa, da mora upravljavec informacijskega sistema vzdrževati revizijsko sled dostopa do informacij, ki so bile klasificirane kot visoko občutljive (DSS05-04.8) [3].
Razen tega mora biti upravljavec informacijskega sistema sposoben določiti vse aktivnosti obdelave podatkov posameznega uporabnika (DSS05.04-7) [3].

Podobne zahteve izhajajo tudi iz skupine standardov na področju varovanja informacij, ISO 27000.

Vodenje revizijskih sledi obdelave osebnih podatkov torej sploh ni izum ZVOP-1, temveč so revizijske sledi eno temeljnih načel upravljanja in vodenja informacijskih sistemov, vgrajene v temeljne aktivnosti in strokovne dobre prakse.

Dobro urejeni informacijski sistemi torej sploh ne bi smeli imeti posebnih težav z zagotavljanjem skladnosti z ZVOP-1.

Ne glede na to je treba izpostaviti, da vpeljava ustrezne rešitve za vodenje revizijske sledi ni enostavna. Če se osredotočimo samo na možnost, da bi administrator informacijskega sistema lahko sam, neopaženo spreminjal podatke revizijske sledi, kmalu ugotovimo, da vodenje revizijskih sledi zahteva dobro zasnovan načrt celovite verige notranjih kontrol, kadar je le mogoče samodejnih, ki so zasnovane tako, da ne puščajo prav nobenega dvoma v nedvoumnost, neizpodbitnost, celovitost ter nespremenljivost revizijske sledi.

Ločimo horizontalno in vertikalno vodenje revizijske sledi. Pri horizontalnem se v revizijski sledi zapisujejo vsi podatki zapisa pred spremembo. Ta način je primeren za beleženje izbrisanih zapisov, vendar je prostorsko najbolj zahteven. Pri vertikalnem vodenju revizijske sledi se zapišejo samo podatki, ki so se spremenili . V nekaterih primerih podatkov, ki se navezujejo na obdelavo, ki jo beleži revizijska sled, ne zapisujemo. Zavedati se je treba, da v primeru, ko v revizijsko sled zapisujemo osebne podatke, tudi sama revizijska sled vsebuje kopijo podatkov, kar bo imelo posledice tako pri zagotavljanju varnosti revizijske sledi, beleženju dostopov do revizijske sledi kot tudi morebitnem izbrisu podatkov iz revizijske sledi, ki se nanašajo na posameznika.

S padanjem cene kapacitet za hrambo podatkov obseg beleženja podatkov tako ni več problem ekonomike, temveč iskanje ravnotežja med zadostnim in prekomernim beleženjem podatkov v revizijski sledi.

3.1 Posledice neustreznega zagotavljanja revizijskih sledi

Kljub metodološko doslednemu testiranju in vgrajeni varnosti informacijskih sistemov zaradi velikega števila vejitev, ki so sestavni del sodobne programske kode, v vsaki rešitvi pomemben del vejitev ni testiran pred predajo v uporabo. To pomeni, da je upravičeno pričakovati, da tekom delovanja informacijskega sistema odkrivamo dodatne pomanjkljivosti in ranljivosti informacijskega sistema.

Eden novejših primerov je nepooblaščeno razkritje podatkov Univerzitetnega kliničnega centra Ljubljana (v nadaljevanju UKC Ljubljana).

Neznanec je vdrl v spletno stran UKC Ljubljana, prek katere pacienti rezervirajo termin obiska pri zdravniku z napotnico. Dostopni so bili občutljivi in osebni podatki pacientov, vključno z njihovimi napotnicami, ter osebni podatki zaposlenih [4]. Informacijski sistem je sicer izrekel globo tako zdravstveni ustanovi (4.170 EUR) in odgovorni osebi (830 EUR) [5], vendar globa ne odpravi posledice, to je, da so bili občutljivi osebni podatki, med katere spadajo podatki o zdravstvenem stanju posameznika, že razkriti.

Bistven problem incidenta ni v tem, da je ranljivost obstajala, temveč v tem, da varnostne kontrole, ki bi morale zaznati, omejiti ali vsaj zabeležiti neupravičen dostop do osebnih podatkov, niso delovale. Čeprav postopek nadzora Informacijskega pooblaščenca še ni končan, prve informacije nakazujejo, da UKC Ljubljana nima podatkov o tem kateri podatki in kdaj so bili neupravičeno razkriti. To pa pomeni, da niti če bi želel o incidentu obvestiti posameznike, tega ne more, ker nima dovolj podatkov.

Če bi bila programska oprema ustrezno izdelana, potem bi morala ne glede na to, da je napadalec zlorabil predvideno delovanje programske opreme, v revizijsko sled zabeležiti dostop do podatkov. Na podlagi tega bi moralo biti mogoče ločiti upravičene dostope od neupravičenih in na ta način določiti podatke, ki so bili nepooblaščeno razkriti tretji osebi.
Podoben primer izhaja iz preiskave opr. št. I Kpd 21345/2010, ki je temeljila na sumu storitve kaznivega dejanja, v sklopu katerega je uslužbenec policije nepooblaščeno proti plačilu spreminjal vrsto prometnega prekrška na že vpisanih plačilnih nalogih, z namenom, da voznik ne bi prekoračil predpisanega števila kazenskih točk.

V sklopu preiskave se je izkazalo, da je imela policija leto in pol izključeno revizijsko sled zaradi nadgradnje informacijskega sistema, kar je bistveno otežilo preiskavo. Nazadnje je bilo

mogoče identificirati storilca na podlagi spremljajočih aplikativnih podatkov. Za vsak zapis plačilnega naloga je programska oprema zapisovala tudi uporabnika in čas zadnje spremembe. Pri ročnem pregledu plačilnih nalogov in primerjavo s stanjem v podatkovni bazi smo ugotovili, da je vse plačilne naloge, ki se v elektronski obliki niso ujemali z nalogom v papirni obliki, nazadnje spremenil isti uporabnik.

3.2 Prednosti zagotavljanja revizijskih sledi

Z doslednim vodenjem revizijske sledi se izognemo vprašanju avtentičnosti in zanesljivosti aplikativnih podatkov in hkrati zagotovimo tudi skladnost s predpisi.

Revizijske sledi ne predstavljajo nujno samo pasivne zbirke zgodovinskih podatkov. Predvsem največji upravljavci osebnih podatkov, kot so Google, Facebook ipd., se jasno zavedajo vrednosti zbranih podatkov. V Sloveniji je prepoznavanje vrednosti velike količine podatkov (t.i. velepodatkov – angl. »Big Data«) še v povojih. V veliko podjetjih v sklopu revizije informacijskih sistemov npr. opažamo, da brez tehtnega preudarka in načrta upravljavci informacijskih sistemov preprosto brišejo dnevnike spletnih strežnikov in da so te aktivnosti in presoja koristnosti podatkov prepuščena operativi, kot so npr. administratorji informacijskega sistema.

Vse to vodi v nenadomestljivo izgubo podatkov. Ti podatki pa imajo razen uporabne vrednosti pri analizi vedenja uporabnikov in iskanju zakonitosti, povezanih z razumevanjem navad uporabnikov, visoko uporabno vrednost tudi v nadzornih procesih.

Pravzaprav kmalu ugotovimo, da je v revizijskih sledeh shranjena bistveno večja količina podatkov, kot je poslovnih transakcij samih, zato so prav revizijske sledi odličen vir velepodatkov.

Analitika si je šele začela utirati pot v nadzorne procese, kot je npr. revizija informacijskih sistemov. S povečevanjem števila virov zanesljivih podatkov postajajo vse bolj izvedljivi revizijski postopki, ki prvenstveno temeljijo na velepodatkih, zbranih v informacijskem sistemu. To zahteva miselni preskok, predvsem pa spremembo v načinu dela in prenovo procesov revidiranja, saj analitike nad velepodatki zaradi velike količine podatkov ni smiselno izvajati na samostojnih delovnih postajah, s katerimi delajo člani revizijske skupine. Zahteva celovit pristop in celovito rešitev za analitiko podatkov [6].

3.3 Kriptografsko varne verige zapisov

Tisti, ki jih tudi uporaba velepodatkov ne prepriča v nujnost beleženja revizijskih sledi v naprednih informacijskih sistemih zaradi vložkov, ki so potrebni pri zagotavljanju spremljajočih organizacijskih in drugih ukrepov, da revizijska sled sploh nastane, lahko posežejo po tehnično naprednih metodah, ki se šele uveljavljajo.

Kriptovalute kot so Bitcoin niso koristne samo zato, ker iz transakcije verige izločajo banko in s tem znižujejo stroške prenosa sredstev, temveč predstavljajo tehnično osnovo za inovacije na področju zagotavljanja verodostojnosti revizijskih sledi.

Pojavljajo se že prvi inovativni poskusi uporabe kriptografsko varnih verig za zanesljivo ugotavljanje izvora in nespremenljivosti dejstev, shranjenih v takšni verigi [7, 8].

Izdelava rešitev za vodenje revizijskih sledi, ki temelji na kriptografski varnostni verigi je nova priložnost za ponudnike rešitev, hkrati pa pomembna priložnost za zniževanje stroškov in zapletenosti zagotavljanja revizijskih sledi v informacijskih sistemih, ki jih vodijo.

4 Osebni podatki v distribuciji električne energije

Površen pregled podatkov, ki se uporabljajo pri distribuciji električne energije, bi lahko dal napačen vtis, da informacijski sistem uporablja zelo malo osebnih podatkov, kot npr. ime in naslov uporabnika električnega priključka.

Ob izhodišču, da je tudi IP naslov računalnika osebni podatek, kot izhaja iz mnenj Informacijskega pooblaščenca, pa izhaja, da je treba osebni podatek razumeti veliko širše. IP naslov se v skladu z ZVOP-1 šteje za osebni podatek (dinamični IP naslovi skupaj s podatkom o času dodelitve oziroma vključenosti v omrežje ali statični IP naslovi – ker je na njihovi podlagi posameznik določljiv oziroma določen) [9]. To ne velja samo za statične IP naslove, temveč tudi za dinamične, torej takšne, ki se s časom spreminjajo [10].

Osebni podatek je torej vsak podatek, ki je povezan s posameznikom oziroma določa posameznika, ne glede na to, ali ta informacija izhaja že iz podatka samega. V primeru IP naslovov lahko praviloma posameznika identificira šele ponudnik dostopa do interneta, pa je kljub temu osebni podatek.

Primeri osebnih podatkov v distribuciji električne energije, ne glede na to, da podatki sami po sebi še ne razkrivajo identitete posameznika, so tako npr. številka merilnega mesta in številka električnega števca. Oba podatka lahko distributer ali celo dobavitelj električne energije poveže s posameznikom, zato sta to osebna podatka.

Ob splošno znanem vzdušju uporabnikov interneta, da jih zasebnost ne skrbi, »ker nimajo česa skrivati«, je vendar treba izpostaviti varnostne implikacije razkritja identificiranih osebnih podatkov oziroma dodatnih podatkov, ki so s temi podatki povezani.

Če bi napadalec iz informacijskega sistema distributerja električne energije lahko ugotovil kakšna je poraba električne energije posameznika, bi lahko iz teh podatkov ugotovil kdaj je njegovo stanovanje prazno in temu prilagodil fizični vdor.

Če podatki o električnem števcu ne bi bili osebni podatek, potem tudi z njim povezana poraba električne energije ne bi predstavljala osebnega podatka, kar pomeni, da bi lahko policija te podatke pridobila in tudi analizirala. To pomeni, da bi lahko na podlagi primerjave s povprečno porabo električne energije in značilne porabe za nedovoljene dejavnosti identificirala potencialne porabnike električne energije, pri katerih obstaja utemeljeni sum, da gojijo nedovoljene rastline (npr. marihuano). To pa že vodi v samodejni nadzor države nad državljani.

5 Sklep

Kljub temu, da državljani »ničesar ne skrivamo«, ima varstvo osebnih podatkov pomembno nalogo pri zagotavljanju zasebnosti državljanov. Pomembno vlogo pri tem imajo tudi revizijske sledi, ki pa niso samo posledica varstva osebnih podatkov, temveč predstavljajo enega od temeljnih načel zagotavljanja varnosti informacijskih sistemov.

Na področju distribucije električne energije je ključno, da ne spregledamo podatkov, ki predstavljajo osebne podatke, kot so npr. identifikacijske oznake števcev električne energije za namene samodejnega pošiljanja stanja števcev, saj morebitna povezava teh enoličnih identifikatorjev s posameznikom bistveno povečuje njegova varnostna tveganja.

Literatura

[1] Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 94/07 – uradno prečiščeno besedilo
[2] Revizijske sledi v aplikativni programski opremi, SIR*IUS, 1/2013, Slovenski inštitut za revizijo
[3] COBIT 5: Enabling Processes, ISACA, 2012, ZDA
[4] Nejc Gole, Vdor v sistem UKC Ljubljana: Dostopne tudi napotnice pacientov, Delo, 16. 3. 2017
[5] Barbara Eržen, Po javnem razkritju vdora UKC Ljubljana spremenili protokol, zurnal24.si, dostopno: http://www.zurnal24.si/po-javnem-razkritju-vdora-ukc-ljubljana-spremenil-protokol-clanek-288020
[6] Kress Robert E., Hildebrand Dave M., How Analytics Will Tranform Internal Audit, ISACA Journal, 2/2017, ZDA
[7] Factom, Business Processes Secured by Immutable Audit Trails on the Blockchain, dostopno: http://www.bcventures.net/uploads/3/9/8/6/39865783/_factom_whitepaper.pdf
[8] Lemieux V. L., Trusting records: is Blockchain technology the answer?, Records Management Journal, Vol. 26 Issue: 2, pp.110-139
[9] Mnenje Informacijskega pooblaščenca številka 0712-2/2010/2277, 24. 12. 2010.
[10] Mojca Prelesnik, Generalni pravobranilec EU: "Podatek o dinamičnem IP naslovu je osebni podatek", 16. 5. 2016, dostopno: https://www.ip-rs.si/novice/generalni-pravobranilec-eu-podatek-o-dinamicnem-ip-naslovu-je-osebni-podatek-1367/.