

INTERVJU

Matjaž Kocjančič, Reisswolf, d.o.o.*

KO IZBRIS NI DOVOLJ: VARNO UNIČENJE PODATKOV KOT DEL KORPORATIVNE ODGOVORNOSTI

Podjetja pogosto vlagajo ogromno v varnostne sisteme, šifriranje in digitalno zaščito, pozabljajo pa na zadnjo, pogosto najšibkejšo fazo življenjskega cikla podatkov tj. uničenje. Od pozabljenih diskov in odprodane računalniške opreme do odsluženih uniform ter promocijskih materialov. Vsak od teh nosilcev podatkov lahko postane varnostno tveganje z vidika zlorabe podatkov, ki jih vsebuje. O tem, zakaj varno uničenje podatkov ni zgolj tehnična naloga, temveč del širše korporativne odgovornosti in varnosti, smo se pogovarjali z Matjažem Kocjančičem iz podjetja REISSWOLF, ki se že vrsto let strokovno ukvarja s celovitim ter varnim upravljanjem dokumentacije in varnostjo podatkovnih nosilcev v njihovem celotnem življenjskem ciklu ter v vseh njihovih pojavnih oblikah.

Podjetja pogosto veliko pozornosti namenjajo zaščiti in obdelavi podatkov, manj pa njihovi končni fazi tj. uničenju. Zakaj je prav ta faza tako ključna?

Vsak podatek ima svoj življenjski cikel, ki je od nastanka, njegove uporabe, hrambe in vse do njegovega končnega uničenja. Prav zadnja faza, ko podatek postane nepotreben, pa je pogosto tista, kjer se zgodi največ napak. Podjetja pogosto domnevajo, da z izbrisom ali prenosom dokumentacije na odpad zaključijo svojo odgovornost, kar pa ne drži. Podatek obstaja, dokler ni dokazljivo in nepopravljivo uničen. V praksi to pomeni, da mora biti

proces uničenja dokumentiran, sledljiv in izveden skladno z zakonodajo in standardi. Samo tako lahko podjetje zagotovi skladno uničenje podatkov in prepreči njihovo ponovno uporabo in zlorabo.

Ko govorimo o uničenju podatkov, mnogi pomislijo le na papirne dokumente. Katere druge nosilce v praksi pogosto spregledamo?

Danes podatki niso več vezani le na papir. Podatkovni nosilci so lahko različni kot npr.: trdi diski, magnetni trakovi, CD-ji, DVD-ji, USB-ključki, SD kartice, pаметne kartice, GSM telefoni, pomnilniki tiskalnikov ipd. Vsi ti podatkovni nosilci

so potencialni viri informacij. Zanimivo pa je, da se tveganja pojavljajo tudi tam, kjer jih najmanj pričakujemo, na primer pri uniformah, akreditacijah, ID-karticah ali promocijskih materialih, ki nosijo logotip podjetja ali osebne podatke posameznikov. Ko taki podatkovni nosilci končajo v nepravih rokah, ne gre le za zlorabo opreme kot take, temveč zlorabo podatkov, ki se nahajajo na podatkovnih nosilcih. Gre torej za širši problem, gre za resno varnostno vprašanje, vprašanje korporativne integritete in vprašanje ugleda blagovne znamke in podjetja kot celote. V preteklosti smo že videli primere, ko so rabljene uniforme ali reklamni materiali povzročili varnostne incidente, saj

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

so omogočili nepooblaščen predstavljanje podjetja ali prodajo na črnem trgu.

Veliko uporabnikov še vedno misli, da zadostuje formatiranje diska ali brisanje datotek. Zakaj to ne drži?

Formatiranje podatkovnega nosilca ne pomeni fizičnega uničenja podatkov pomeni le odstranitev povezav do njih. V praksi je takšne podatke mogoče obnoviti z relativno enostavnimi in dostopnimi orodji. Zato se v profesionalnih okoljih uporabljajo postopki, ki temeljijo na popolnem mehanskem ali digitalnem uničenju podatkovnega nosilca, ne zgolj brisanju vsebine. Le na ta način se zagotovi, da podatki postanejo neobnovljivi.

Pri tem se pogosto omenjajo različni standardi – GDPR, ISO 27001 in tudi DIN 66399. Kako ti standardi vplivajo na prakso uničevanja podatkov? Ali se tukaj standardi kako spreminjajo ali dopolnjujejo?

Standardi določajo, kako varnostno zahtevno mora biti uničenje glede na vrsto podatkov in medija, na katerem se ti nahajajo. DIN 66399 je bil dolgo osnova za razvrščanje varnostnih stopenj pri mehanskem razrezu dokumentov in elektronskih nosilcev. Danes ta pristop nadgrajuje ISO/IEC 21964, ki je nastal iz DIN-a, a ga postavlja v širši, mednarodni okvir. Nekatere evropske države ta standard že uporabljajo kot osnovo za certificiranje izvajalcev uničenja, saj določa strožje zahteve glede sledljivosti, postopkov in revizijske sledi procesov uničevanja. Gre za evolucijo v smeri večje odgovornosti izvajalcev in večje transparentnosti procesa uničevanja.

Kako se varno uničenje podatkov povezuje z okoljskimi in trajnostnimi vidiki poslovanja?

Varno uničenje podatkov ne pomeni, da mora vse končati na odlagališču. Prav nasprotno. Sodobni postopki omogočajo, da se materiali po uničenju reciklirajo in ponovno uporabijo. Tako podjetje hkrati zaščiti podatke in prispeva k zmanjšanju okoljskega odtisa. V tem smislu ima odgovorno uničenje dvojno vrednost: varnostno in okoljsko. V zadnjih letih postaja to pomemben del ESG-poročanja, saj vlagatelji, partnerji, dobavitelji ali pa kupci vse bolj pričakujejo transparentnost tudi pri ravnanju s podatkovnimi nosilci in občutljivimi materiali. Podjetja, ki se tega zavedajo, s tem gradijo zaupanje in dokazujejo, da varnost ni samo tehnična, temveč tudi etična kategorija.



Katere so po vaših izkušnjah najpogostejše napake, ki povzročajo resne varnostne incidente?

Največ težav povzročajo neorganizirani, nesledljivi ali improvizirani postopki. Odprti zabojniki na hodnikih, neustrezni prevozi podatkovnih nosilcev od lokacije prevzema do lokacije uničenja, vreče brez varnostnih oznak ali pa odsotnost revizijske sledi postopkov in procesa uničevanja. Vse to so situacije, kjer lahko pride do tveganj nepooblaščenih dostopov do podatkovnih nosilcev in podatkov, ki se na njih nahajajo. Ko se to združi s pomanjkanjem ozaveščenosti in varnostne kulture zaposlenih, lahko hitro pride do uhajanja informacij, kraje podatkov, kraje identitete in posredno negativnih objav v medijih. Rešitev je v standardiziranih postopkih in sodelovanju s certificiranimi izvajalci, ki zagotavljajo popolno sledljivost od trenutka prevzema podatkovnega nosilca do njegovega trajnega uničenja ter izdaje potrdila o varnem in sledljivem uničenju. To podjetju omogoča dokazljivo skladnost in varnost, obenem pa zmanjšuje tveganja, povezana z zlorabo podatkov.

Kako vidite prihodnji razvoj tega področja? Bo uničenje podatkov postalo še bolj avtomatizirano in regulirano?

Vsekakor. Digitalizacija bo prinesla še večjo sledljivost, saj bo vsak korak procesa elektronsko zabeležen, od prevzema do reciklaže (revizijska sled). Standardi se bodo še naprej razvijali v smeri povežovanja varnosti, okoljske odgovornosti in skladnosti. Podjetja bodo morala tudi procese uničevanja obravnavati kot integralni del upravljanja s podatki, ne kot obrobno tehnično nalogo. Največjo prednost pa bodo imela tista, ki bodo združila naslednje elemente: varnost, transparentnost, skladnost in trajnost. To je prihodnost korporativne varnosti in odgovornega ravnanja s podatki v vseh njihovih pojavnih oblikah in v vseh fazah njihovega življenjskega cikla.

Če bi morali podjetjem dati en sam nasvet glede ravnanja s podatki, ne glede na njihovo obliko – kaj bi postavili kot najpomembnejše?

Podatek ima vrednost le, dokler je pod nadzorom. Ko izgubimo sled nad njim zaradi slabe hrambe, neustreznega uničenja ali nepozornosti zaposlenih le-ta postane tveganje. Zato naj podjetja vsak korak življenjskega cikla podatka obravnavajo z enako resnostjo. Varnost ni projekt, temveč odgovornost, ki povezuje tehnologijo, procese in ljudi. ■

Foto: arhiv Reisswolf, d.o.o.