Ricoh

Varnost podjetij mora biti vedno na prvem mestu

.. Kibernetska varnost je največja grožnja sodobnih podjetij in je lahko ključna za preživetje na trgu. Več kot polovica podjetij v Evropi in ZDA je poročalo o tem, da so jim podatki ušli skozi nezavarovan sistem tiskanja (Quocira Enterprise MPS Study) ..

Ko govorimo o kibernetski varnosti, so v nevarnosti prav vsa podjetja. Trditve, kot so "nam pa se to ne more zgoditi" ali "komu pa smo mi kot podjetje zanimivi", žal ne pijejo vode. Žrtve napadov, kot so phishing, DDoS or ransomware, so podjetja vseh velikosti, stroške napadov pa lahko kaj hitro štejemo v milijonih evrov. Medtem širitev in digitalizacija modernih delovnih mest postavljata nove izzive, ko govorimo o varnosti podatkov.

Prezrta grožnja

V zadnjih letih je število pisarniških tiskalnikov in večnamenskih naprav skokovito naraslo, kar pomeni, da takšne naprave predelajo ogromno podatkov, ki so lahko zaupne narave in so ključni za obstoj podjetij. Zato so prav te naprave potencialno ena največjih in prepogosto prezrtih groženj za odtekanje informacij z delovnega mesta. Soočena s temi izzivi morajo danes podjetja imeti varne sisteme za upravljanje dokumentov in podatkov, a mnoga se tega ne zavedajo dovolj.

V podjetju Ricoh so strokovnjaki v razumevanju omenjenih tveganj, saj so desetletja razvijali načine za njihovo blažitev z najsodobnejšimi varnostnimi ukrepi, ki so vključeni v prav vsak njihov izdelek ali rešitev. Njihovi tiskalniki med drugim zagotavljajo prepisovanje diska za kar 20 let.

Celovit pogled na ranljivosti

Filozofija podjetja Ricoh pravi – varnost je v naši DNK, kar tudi udejanjajo v praksi. Ricoh k varnosti svojih naprav zato pristopa večplastno. Varnost se začne z vsako napravo posebej, tako da prestane varnostne preizkuse in je preverjena po standardu IEEE ali ISO 27001. Ricoh je tudi vodilni član in ključni avtor združenja IEEE. Naprave nadzorujejo z lastnim operacijskim sistemom, šifriranim trdim diskom in digitalno podpisanimi posodobitvami programske opreme. S tem se izognejo namestitvam zlonamerne programske opreme na svojih napravah. Zavezali so se, da bodo tudi v prihodnje nadaljevali z uvajanjem najvišjih standardov varnosti.

Potem je tu naslednji vidik varnosti – njihov uporabniški vmesnik, ki je brez nepotrebnih modulov. Korenski dostop (angl. root) ni na voljo, kar zmanjšuje možnost množične okužbe programske opreme in napak, ki bi povzročale težave.

Vgrajene aplikacije sicer ne razvija Ricoh, ampak podjetja, ki uporabljajo Ricohova razvijalska orodja. Te aplikacije so testirane, certificirane in digitalno podpisane s strani Ricoha. Aplikacij, ki niso podpisane na tak način, naprave sploh ne sprejmejo, kar preprečuje, da bi kdo namestil oziroma uporabljal škodljivo programsko opremo. V omrežnem okolju uporabljajo end-to-end enkripcijo za optično branje in tiskanje dokumentov, s katerim zagotovijo, da podatke vidita le pošiljatelj in naslovnik, brez vmesnih členov, kjer bi lahko prav te informacije odtekle neznano kam. Na ravni strežnika pa ponujajo šifriranje datotek in ločevanje vlog skrbnika.

V Ricohu verjamejo, da je celovit pogled na ranljivosti ključnega pomena za preživetje sodobnega posla. Prav vsak vidik njihovega varnostnega pristopa je podprt z načeli: zaupnost, celovitost ter razpoložljivost kjerkoli in kadarkoli.

Ukrepi v štirih fazah

Najprej je tu nadzor, torej zaščita pred kopiranjem, avtentikacija in avtorizacija uporabnika naprave ter omejen dostop in zaščita pred škodljivo programsko opremo.

Potem so tu šifriranje podatkov, infrastruktura za odobritev ter hiter in varen dostop, ne glede na lokacijo naprave. Pri tem je treba zagotoviti, da varnostni protokoli ne ovirajo poslovanja, funkcionalnosti in produktivnosti.

Podatke morate tudi učinkovito uničiti. Temu so namenjeni sistem za prepis podatkov (DOSS), čiščenje naprav ob koncu življenjske dobe, odstranjevanje trdega diska in izpiranje pomnilnika. Tako zagotovijo, da podatki, ki jih je naprava v svoji življenjski dobi "videla", ne bi prišli v napačne roke.

Podpora zagotavlja oceno varnosti infrastrukture, optimizacijo varnosti tiskanja, vključuje pa tudi skupino za odzivanje na varnostne incidente.

Moderno delovno mesto je dinamično in fleksibilno, ob tem pa mora spletna varnost delovati brezhibno. Čeprav tega mnogi ne pomislijo, tudi večnamenske naprave in tiskalniki niso imuni na odtekanje občutljivih informacij, zato še enkrat premislite, preden vas bo ob izgubi podatkov, ki ne bi smeli uiti iz podjetja, bolela glava.

Če želite izvedeti več o novih inteligentnih napravah Ricoh, obiščite spletno mesto www.ricoh-europe.com. Več boste našli tudi na spletni strani uradnega zastopnika znamke Ricoh v Sloveniji, podjetja Vibor d.o.o. (P.R.)