Obvezni dnevniški zapisi za večjo kibernetsko varnost

V podjetju Telprom kot cenovno ugodno alternativo priporočajo odprtokodno rešitev Wazuh.

Eden izmed glavnih ukrepov za obvladovanje tveganj, ki jih uvaja novi zakon o informacijski varnosti (ZinfV-1), je vodenje dnevniških zapisov o delovanju sistemov. Zakon pravi, da morajo zavezanci – to so ponudniki bistvenih in pomembnih storitev, kot so energetika, zdravstvo, banke, digitalne storitve, javna uprava in drugi subjekti – obvezno beležiti vse, kar se dogaja v njihovih računalniških sistemih in aplikacijah. Beležiti morajo dnevniške zapise vseh sistemov v organizaciji kot tudi dejavnosti uporabnikov in administratorjev. Te zapise morajo hraniti vsaj šest mesecev, lahko pa tudi dlje, če analiza tveganj in ocena sprejemljive ravni tveganj pokažeta, da je to potrebno in smiselno.

Zakon še določa, da morajo biti zapisi shranjeni tako, da so v primeru incidentov zagotovljene njihova avtentičnost, celovitost in razpoložljivost. To pomeni, da se jih ne da ponarediti ali izgubiti. Poskrbljeno mora biti tudi, da so zapisi dostopni samo tistim z odobrenim dostopom do njih.

Glavni razlog je varnost

Vid Grosek, strokovnjak za kibernetsko varnost v podjetju Telprom in certificiran etični heker, pojasnjuje, da dnevniški zapisi pokažejo, kaj se dogaja v sistemu, kdo je dostopal do sistema ter kdaj in kaj se je spremenilo. »Na podlagi teh podatkov se lahko ob morebitnem incidentu hitreje odzovemo in morda napad celo ustavimo ter s tem zmanjšamo škodo,« pojasnjuje sogovornik. »Prav tako ti podatki omogočijo, da lažje raziščemo, kaj se je zgodilo ob varnostnem incidentu – je šlo za napako zaposlenega, poskus vdora ali pa za zlorabo. Dnevniški zapisi služijo tudi kot dokaz pri notranjih preiskavah, poročanju vodstvu ali celo v pravnih postopkih.«

Zahteven zalogaj, a obstajajo dostopne rešitve

Tako finančno kot organizacijsko je lahko vzpostavitev sistema za beleženje in analizo dnevniških zapisov precej zahteven zalogaj. Pri komercialnih rešitvah so stroški za vzdrževanje licenc in infrastrukture ter izobraževanje strokovnjakov za manjša podjetja pogosto preveliki, zato je smiselno razmišljati o bolj dostopnih alternativah. V podjetju Telprom na primer uporabljajo odprtokodno rešitev Wazuh, pri čemer so se specializirali tudi za njeno uvajanje v drugih podjetjih.

TAJA HARRIS

»

Dnevniški zapisi omogočajo pregled in rekonstrukcijo dogajanja v primeru varnostnih incidentov ali dogodkov.

Vid Grosek, strokovnjak za kibernetsko varnost v podjetju Telprom in certificiran etični heker

Več o uporabi platforme Wazuh v praksi boste lahko 9. oktobra 2025 izvedeli na 6. Telprom IT akademiji. Udeležba je brezplačna. Za več informacij skenirajte QR-kodo.

Zbiranje, analiza in hramba na enem mestu

Wazuh podjetjem omogoča, da na enem mestu zbirajo, analizirajo in varno hranijo vse dnevniške zapise. S tem centralizirajo pregled nad dogajanjem v svojih sistemih, pospešijo odkrivanje nepravilnosti in zmanjšajo možnosti, da bi spregledali resne grožnje. Wazuh zna tudi zaznavati poskuse vdorov, iskati ranljivosti v sistemih, spremljati skladnost s predpisi in standardi ter sproti opozarjati na težave.

Prav tako se lahko kosa z vsemi komercialnimi rešitvami.

Odlična rešitev za manjša podjetja, primeren tudi za večja

Največja prednost Wazuha je stroškovna učinkovitost. Čeprav zanj ni treba plačevati dragih licenc, ponuja funkcionalnosti, ki jih imajo tudi komercialne rešitve. »Zato je super alternativa za manjša podjetja, ki iščejo cenejšo rešitev, hkrati pa dobro deluje tudi v večjih podjetjih, kjer je potrebna zmogljiva in zanesljiva platforma,« pojasnjuje Grosek in dodaja, da program omogoča razširitev po meri, kar pomeni, da je prilagodljiv potrebam posamezne organizacije.

Izberite partnerja z izkušnjami

Pri uvajanju vsake rešitve za vodenje in hranjenje dnevniških zapisov je glavno, da se najprej jasno določi, katere dnevniške zapise podjetje res potrebuje in kako dolgo jih mora hraniti. »V nasprotnem primeru se hitro nabere ogromno nepotrebnih podatkov, ki ob morebitnem incidentu le ovirajo učinkovit odziv,« pravi sogovornik. Pravilna nastavitev rešitve je po njegovih besedah pomembna tudi zato, da sistem sproži opozorila le ob dejanskih grožnjah. IT-strokovnjaki jih tako lažje in hitreje zaznajo, s tem pa se zmanjša verjetnost, da bi grožnje ostale spregledane.

V podjetju Telprom imajo z zagotavljanjem in preverjanjem varnosti v informacijskih sistemih dolgoletne praktične izkušnje. »Sistem znamo pravilno postaviti, nastaviti znamo pravila in urediti pregledne nadzorne plošče ter poskrbeti za dovolj prostora in prave politike hrambe,« pravi Grosek.

Telprom tako omogoči, da podjetje iz produkta in storitve pridobi največ: večjo varnost, skladnost z zakonodajo in jasen pregled nad dogajanjem v sistemu, brez nepotrebnih alarmov in morebitnih zapletov.