POMEMBNOST IZVAJANJA REDNIH VARNOSTNIH PREGLEDOV

Dandanes je vsaka organizacija tarča nepridipravov, ne glede na vrsto njene dejavnosti in velikosti. Hekerji in kibernetski kriminalci imajo pred seboj postavljen cilj – pridobiti vaše podatke, ki jih lahko nato vnovčijo na razne načine. Kot to načeloma velja, proaktivnost in pripravljen preventivni načrt bosta obrodila sadove – redni pregledi varnosti informacijskega sistema so odlična preventiva za preprečevanje zlorabe in povezanih poslovnih tveganj.

Ali bi leteli z letalom, ki nima opravljenih vseh varnostnih pregledov? Ali pa se odpravili na daljše potovanje z avtomobilom, ki daje vtis, kot da je le vožnjo stran od odpada? Odgovor je ne. Kako pa se vse to povezuje s področjem informacijske tehnologije? Vzdrževanje je torej pomembno, varnost pa ima pomembno vlogo pri vzdrževanju neoporečnosti vašega IT-okolja. Vendar za razliko od mehanika, ki samo pregleda vaš avtomobil, pregled vašega IT-okolja zahteva mnogo več – ocenjevalec pri pregledu zavzame zahtevno vlogo inženirja, ki je oblikoval vaše omrežje.

Informacijska tehnologija predstavlja dinamično okolje – nenehno se razvija in posledično postaja vse bolj zahtevna. In medtem ko se IT-infrastruktura v organizacijah spreminja, se lahko v njeno zapleteno strukturo prikradejo razne varnostne vrzeli. Te vrzeli predstavljajo ranljivosti. Vendar ni dinamična samo vaša infrastruktura, na preži so tudi napadalci, ki vedno znova najdejo nove načine napadov, ki ciljajo na ranljivosti informacijskega sistema. Če je torej vaše okolje včeraj še bilo varno, vam to ne zagotavlja varnosti tudi v bodoče.

Trud neodvisnega strokovnjaka, ki bo občasno preverjal prisotnost morebitnih varnostnih pomankljivosti in nevidnih ranljivosti vašega IT okolja, vam lahko kasneje prihrani marsikateri siv las. Seveda lahko to nalogo prepustite vašemu osebju, vendar se je v praksi to že večkrat izkazalo za neučinkovito. Strokovnjaki s področja varnosti razmišljajo kot hekerji, imajo potrebne izkušnje in strokovna znanja ter pri varnostnem pregledu iščejo razpoke v varnosti vašega sistema, na katere vaša ekipa ne bi niti pomislila.

Stroškovno učinkovita pot do optimalne varnosti

Varnostni pregled vašega sistema lahko predstavlja prvi korak na stroškovno učinkoviti poti do optimalne ravni varnosti. A bodimo odkriti – ko govorimo o informacijski tehnologiji, 100 odstotne varnosti preprosto ni. Varnost je vedno nek kompromis. Podjetja, ki se tega kompromisa lotijo le s stroškovne plati in morebiti neustrezno zavarujejo svoje podatke, pogosto pozabijo na dolgoročne posledice takšnega mišljenja.

Vendar je lahko varnost tudi stroškovno učinkovita. Zmotno je prepričanje, da morate vsakih nekaj mesecev kupiti nove naprave. Ključnega pomena je pravilna konfiguracija vaših obstoječih varnostnih rešitev in informacijskih sistemov. Le tako bodo lahko učinkovito varovale vaše IT-okolje in podatke.

NIL-ovi strokovnjaki bodo opravili varnostni pregled in podrobno ovrednotili varnost vašega IT-okolja. Na podlagi naših ugotovitev lahko nato tudi sami poskrbite, da se morebitne luknje, ki bi privedle do odtekanja podatkov, pravočasno zakrpajo. Ne pozabite – vaše IT-okolje je močno le kot njegov najšibkejši člen.

Ključen je pravi pristop

Ko se lotite pregleda varnosti, je pomembna predvsem celovita obravnava. To pomeni, da morate preučiti vse vidike varnosti – od varnostnih politik, lastnih spletišč in aplikacij, SCADA/industrijskih sistemov, omrežnega načrta in požarnih zidov, do vaših zaposlenih. Varnostni pregled mora obravnavati vse stopnje življenjskega cikla informacijskega sistema.

Ko je govora o varnosti vašega IT-sistema, bližnjice preprosto ne obstajajo. Pomembno je torej pregledati vsa področja vašega sistema, enako pomembno je, da se varnostni pregled opravi metodološko in v pravem zaporedju, ob rabi primernih metod in orodij. Samo celovit varnostni pregled lahko poda dragocene rezultate.

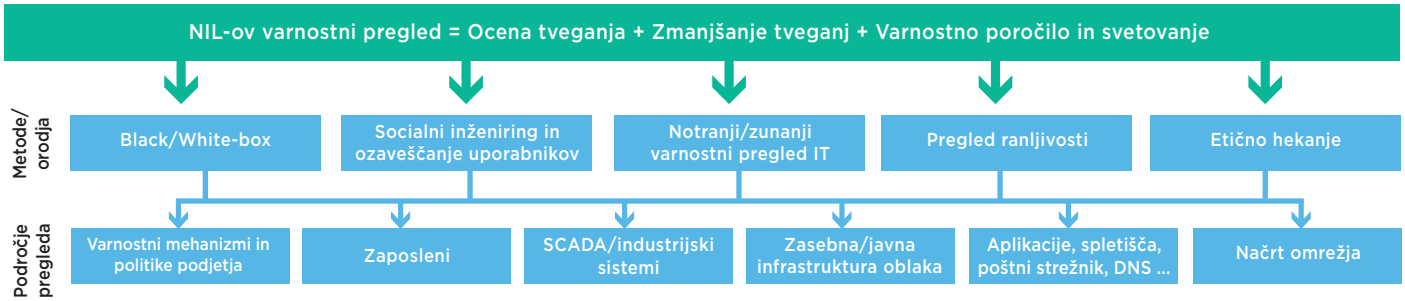
NIL

CILJI IN KORAKI VARNOSTNEGA PREGLEDA

1. Predtestna faza odkrivanja in zbiranja informacij o sistemu in storitvah.
2. Metodološko (avtomatizirano in z uporabo orodij) odkrivanje ranljivosti informacijskih sistemov, katerega namen je omejitev področij, kjer v nadaljnjih korakih opravljamo ročni varnostni pregled.
3. Ročni validacijski testi (na fokusiranih področjih, ki so rezultat prejšnjih korakov), saj le selektivne metode zagotavljajo verodostojno izločanje »lažnih alarmov«, ki so značilni v prejšnjih korakih odkrivanja ranljivosti.
4. Analiza pridobljenih informacij o tveganjih ter povezovanje tveganj s poslovnim okoljem in procesi – beleženje, kje se grožnje in ranljivosti pojavljajo v sistemu.
5. Ocena varnostnih tveganj, posledic izrabe sistema in kompleksnosti tveganj/ranljivosti ter odprave lažnih tveganj.
6. Podrobno poročilo testiranj, opažanj in tveganj s podanimi priporočili, kako naprej ukrepati.
7. Predstavitev ugotovitev in varnostnih priporočil tehničnemu osebju in vodstvu.

NIL pričakovanja tudi izpolni. Po zaključku ocene boste prejeli podroben povzetek in tehnično poročilo o zaznanih tveganjih. Poročilo bo vsebovalo tudi priporočila z usmeritvami, kako stroškovno učinkovito zaščititi svoje IT-okolje.

Ocenjevalne metode in orodja ter potencialna področja tveganja



Kaj morate vedeti preden izberete izvajalca varnostnega pregleda?

Vse ranljivosti ne predstavljajo nujno tudi tveganj, saj imajo različne vloge v procesih vašega poslovanja. Pri izbiri izvajalca varnostnega preglede mora biti primarni kriterij izbire strokovnost. Izjemni strokovnjaki za varnost se ponašajo z obširnimi izkušnjami in znanjem, zato mora ponudnik, ki ga izberete za izvedbo ocene varnosti vašega sistema, sestaviti skupino strokovnjakov za informacijsko varnost.

Tako kot pri izbiri primernega zdravnika želite zdravje in varnost svojega IT-sistema prepustiti zaupanja vrednemu strokovnjaku. Vsekakor pa naj cena pri izbiri ponudnika ne igra ključne vloge – najboljši strokovnjaki za informacijsko varnost nikakor ne morejo biti tudi najcenejši.

Pred izbiro strokovnjaka za izvedbo varnostnega pregleda odgovorite na naslednja vprašanja

- Ali je ponudnik tako dober v praksi kot v teoriji? Ali je njihova glavna prednost samo kup certifikatov s področja informacijske varnosti ali pa ima dokazljive praktične izkušnje z upravljanjem sodobnih in kompleksnih IT infrastruktur, po možnosti na vašem poslovnem področju (bančništvo, e-trgovanje, uprava, itd.)?
- Kdo vse sestavlja skupino strokovnjakov, ki bo opravljala varnostne preglede? Kakšni certifikati in specializacije jih odlikujejo?
- V kolikšni meri bo njihova skupina strokovnjakov lahko sodelovala z vašo skupino IT strokovnjakov?
- Kakšna poročila in rezultate vam lahko ponudijo?
- Ali boste na podlagi poročila lahko sami ponovili del testiranja in izvedli določene protiukrepe?