NIL

NIL-OV VARNOSTNO OPERATIVNI CENTER

NIKOLI NE BOSTE 100-ODSTOTNO VARNI PRED KIBERNETSKIMI NAPADI

Lahko pa ste nanje 100-odstotno pripravljeni.

Organizacije ste v odnosu do kibernetskih kriminalcev v nezavidljivem položaju. Varovati se morate pred napadi, ki izkoriščajo tako znane, kot tudi še javno neznane ranljivosti. Vaše IT-okolje in poslovni procesi so vedno bolj kompleksni, kar je posledica vse večje prepletenosti, povezanosti in obsežnosti kibernetskega prostora. Nadzorovati vsako potencialno šibko točko v vse bolj dinamičnih informacijskih sistemih organizacij je iz dneva v dan bolj zahtevno in za varnostno zrele organizacije tudi na robu kadrovsko in tehnološko izvedljivega.

Ste prepričani, da vas (še) niso napadli?

Ni presenetljivo, da zaznava in odziv na kibernetske napade sodita med največje izzive obvladovanja informacijskih tveganj. Raziskave za koledarsko leto 2017 kažejo, da je pri vseh napadenih podjetjih v povprečju preteklo **več kot 100 dni**, preden je bila prisotnost napadalca v IT-sistemu sploh zaznana. **Taka nezmožnost zaznave daje kriminalcem ogromno časa za spoznavanje vašega okolja, prestrezanje občutljivih informacij ter nepooblaščeno dostopanje do podatkov in procesov**. Rezultat je velika poslovna škoda, ki jo v enem incidentu po navadi merimo v sto tisoč ali milijon evrih.

Stalno spremljanje in analiziranje dogajanja v informacijskemu okolju je zahteven, drag proces, saj zahteva obvladovanje ogromne količine podatkov, v kateri morajo visoko šolani, sposobni analitiki najti iglo, ki večinoma ni očitna, in ukrepati prilagojeno vašemu poslovnemu okolju. Dobra novica je, da lahko slovenska podjetja, ki takšnega okolja ne morejo vzpostaviti sama, tovrstno storitev najamejo.

UČINKOVITO OBVLADOVANJE VARNOSTNIH TVEGANJ, KI SI GA LAHKO PRIVOŠČITE

Na NIL-u smo kot prvi v Sloveniji vzpostavili varnostno operativni center (angl. Security Operations Center – SOC) z možnostjo najema, ki omogoča preprečevanje naprednih kibernetskih groženj in hkrati rešuje oviro kroničnega pomanjkanja specializiranega, visoko usposobljenega kadra za analizo in odzivanje na napade.

S storitvijo NIL-ovega SOC-a si zagotovite visoko učinkovito orodje za obrambo pred kibernetskimi napadi po dostopni ceni, bistveno ceneje in hitreje, kot če bi tako storitev vzpostavili sami.

REŠITEV VAM PRINAŠA NASLEDNJE POSLOVNE KORISTI:

- preprečevanje oziroma omejevanje poslovne škode zaradi kibernetskega vdora,
- takojšnjo, učinkovito reakcijo v primeru kritičnega incidenta,
- skladnost z zahtevami zakonodaje, standardov in internih regulativ (ZInfV, GDPR, ISO itd.),
- vpeljavo nadzorne komponente IT-varnosti.

VRHUNSKA EKIPA, PROCESI IN ORODJA ZA PREPOZNAVANJE IN ODZIV NA VARNOSTNE INCIDENTE

NIL-ov SOC sestavljajo vrhunski strokovnjaki, ki pri svojem delu uporabljajo preplet tehnoloških rešitev, uveljavljenih praks in industrijsko priznanih metodologij. V sklopu SOC-a vam tako omogočamo:

- **visoko stopnjo prilagodljivosti** vašemu okolju glede na vaše poslovne prioritete,
- **neprekinjen proces opazovanja, analize, zaznave in triaže** varnostnih dogodkov v vašem IT-okolju,
- **proaktivno iskanje notranjih in zunanjih groženj** (angl. threat hunting) še pred pojavitvijo incidentov,
- **odziv na varnostne incidente** (odvisno od resnosti: od obveščanja do hitrega obiska strokovnjakov), tesno povezan z vašimi poslovnimi procesi,
- **preventivno odkrivanje** vaših varnostnih ranljivosti,
- izdelavo mesečnih **poročil** in prednostnih priporočil o potrebnih izboljšavah v vašem IT-okolju,
- **preizkušanje učinkovitosti zaznave** kibernetskih napadov,
- **merljivost učinkovitosti** vašega obvladovanja kibernetske varnosti.

NIL-OV SOC VAM JE NA VOLJO TAKOJ IN BREZ DODATNIH INVESTICIJ

- Vrhunska ekipa strokovnjakov (analitikov), posvečena izključno storitvi SOC.
- Delovanje 24/7 s striktnimi pogoji SLA – ker sovražnik nikoli ne spi.
- Prilagoditev storitve glede na specifike naročnikovega okolja oziroma poslovne vertikale.
- Tesno sodelovanje SOC-ovih analitikov z drugimi NIL-ovimi specialisti posameznih področij in vašo IT-ekipo.
- Uporabljati ga lahko začnete takoj.

> “V finančnem sektorju so kibernetski napadi (ali odtekanje podatkov) lahko poslovno izredno škodljivi, zato moramo biti stalno na preži. Ker sami nimamo na razpolago dovolj virov, nam pri spremljanju in preprečevanju potencialnih varnostnih incidentov pomagajo NIL-ovi strokovnjaki iz varnostno operativnega centra.”
>
> **Gregor Nastran**, Vodja sektorja za Informatiko, Agencija za trg vrednostnih papirjev

NIL-OV SOC IN ZAKON O INFORMACIJSKI VARNOSTI (ZINFV)

ZInfV izvajalcem bistvenih storitev, ponudnikom digitalnih storitev in organom državne uprave nalaga konkretne obveznosti.

NIL-ov SOC jim lahko še posebej pomaga pri **izvajanju tehničnih in organizacijskih ukrepov za prepoznavanje, obvladovanje, preprečevanje in zmanjšanje vpliva varnostnih incidentov**. Če pa do incidenta vendarle pride, **NIL-ov SOC poskrbi za priglasitev nacionalnemu CSIRT-u** brez nepotrebnega odlašanja, z upoštevanjem zahtev po ustreznem zavarovanju dnevniških zapisov oziroma revizijskih sledi, če te obstajajo.

NIL d.o.o.
Baragova ulica 5
1000 Ljubljana
Slovenija

T: 01 4746 500
prodaja@nil.com
nil.com