# NIL-OVE REŠITVE ZA ZAŠČITO PRED ŠKODLJIVO PROGRAMSKO OPREMO

Strankam prilagojene rešitve za preprečevanje (posledic) na poslovna okolja uperjene škodljive programske opreme

*Škodljiva programska oprema (ang. malware) vsebuje vrsto podrazličic, kot so kriptovirusi, virusi, trojanci, črvi, logične bombe itd., ter predstavlja stalno grožnjo posameznikom in podjetjem, saj z brisanjem ali zaklepanjem podatkov povzroči nepravilno delovanje sistemov, ki pogosto vodi v odpoved delovanja storitev in resnih motenj v poslovanju. Starejše tehnologije, kot so klasični protivirusni programi, proti novim grožnjam niso več učinkovite, kar se pozna tako pri zaščiti delovnih postaj, prenosnikov in mobilnih naprav, kot tudi strežnikov. Te tehnologije so preprosto preživete in zato niso kos zaščiti pred sodobnimi grožnjami, ki se znajo skriti in izogibati odkritju.*

*Škodljivo programje danes ogroža prav vsa podjetja, kot ključno orodje ga uporabljajo predvsem kiberkriminalci, ki s pomočjo kriptovirusov zašifrirajo vaše podatke in vas za povrnitev podatkov izsiljujejo z odkupnino. Večje okužbe računalnikov in sistemov v velikih podjetjih lahko le tem povzročijo izjemno visoke stroške – ti se merijo v sto tisočih ali celo milijonih evrov na posamezni varnostni incident.*

## Še vedno menite, da niste tarča?

Najbolj nevarne so tiste škodljive kode, ki ciljajo posamezno podjetje, proti takšnim se je tudi najtežje (a seveda možno) braniti. Kiberkriminalci sicer sprva ciljajo NA VSAKOGAR, saj se v ogromno digitalno mrežo škodljivih kod ujame veliko uporabnikov in podjetij – škodljivo programje pač ne dela razlik, čigav računalnik ali drugo napravo okuži.

Brez ustreznega sistema zaščite pred škodljivo programsko opremo sta okužba ali napad računalnikov in zaposlenih v podjetju le vprašanje časa. Za podjetja so najbolj nevarni kriptovirusi in izsiljevalska programska oprema, saj lahko povzročijo astronomske stroške odprave posledic v kompleksnih IT-okoljih. Teh digitalnih groženj preprosto ne more preprečiti le en »magični« varnostni program, temveč mora biti IT-okolje zaščiteno sistemsko.

### KAJ POČNEMO DRUGAČE? IN ZAKAJ.

- *Imamo več kot 25 let izkušenj z zaščito pred najbolj trdovratno ter napredno škodljivo programsko opremo, vključno z napadi »ničtega dne« (day-zero).*
- *Zagovarjamo visoko varnostno zanesljivost z rabo več komplementarnih varnostnih tehnologij, s katerimi ustvarimo robustne varnostne rešitve.*
- *Nudimo natančno svetovanje glede ureditve področja informacijske varnosti in pomoč ob morebitnih varnostnih incidentih.*

## Koga varovati – zaposlene, računalnike, omrežje ali naprave? Ne smete se osredotočiti le na eno področje.

Proti sodobnim škodljivim kodam se lahko podjetja zoperstavijo le z napredno načrtovanim sistemom ukrepov, ki združujejo sodelovanje različnih varnostnih tehnologij in strokovnjakov. Naša filozofija informacijske varnosti narekuje, da so varnostne rešitve bistveno bolj učinkovite takrat, ko so prilagojene posameznemu podjetju in njegovemu IT-okolju. Nasprotnih dokazov o neučinkovitosti generičnih varnostnih rešitev kar mrgoli, posebej kadar se poslovna okolja zanašajo na potrošniške varnostne rešitve, ki jih sicer uporabljamo v domačem okolju.

NIL-ove varnostne rešitve za obrambo pred škodljivo programsko opremo vsebujejo celovit pregled delovanja vaše organizacije in načrtovanje ustreznih varnostnih ukrepov. Vsebujejo naslednje elemente in rešitve:

- Jasen načrt varnostnih ukrepov in delovanja rešitev glede na poslovne procese vašega podjetja ob upoštevanju znanja, izkušenj, vlog in potreb zaposlenih pa tudi tehnološkega okolja in njegovih omejitev.
- Varnostne rešitve za omrežje podjetja, kot so filtriranje in analiza vsebin, izvajanje prenosne programeske opreme v t. i. peskovniku, podpis prometa, varnostne politike, analiza anomalij, filtriranje URL-naslovov, pregled »ugleda« spletnih strani, omrežna segmentacija, požarni zidovi, preverjanje sumljivih kod in vzorcev v zmogljivem računalniškem oblaku itd.
- Zaščito računalnikov in naprav zaposlenih, vključno z analizo vsebin, preverjanjem sumljivih vzorcev lokalno in v zmogljivem računalniškem oblaku, seznami varnih/odobrenih aplikacij, temeljitim preverjanjem delovanja aplikacij v peskovniku ali virtualnem okolju itd.
- Zaščito poslovnih procesov z ustreznim izobraževanjem zaposlenih glede na njihovo vlogo v podjetju ter implementacijo proaktivnih in reaktivnih varnostnih procesov, definiranje varnostnih politik itd.

NIL

- Povezovanje številnih virov informacij o digitalnih nevarnostih, ki izboljša kakovost podatkov in pomaga pri odkrivanju škodljivih kod ter zmanjšuje obremenitev sistemskih skrbnikov..
- Našo pomoč v primeru varnostnih incidentov in vprašanj.

## Pomagamo vam do mirnega spanca: učinkovite zaščite pred škodljivo programsko opremo, nevarnostmi ničtega dne in ciljanimi napadi

Nevarnosti t. i. ničtega dne so nevarnosti v obliki povsem novih napadov, ki se na določen dan prvič pojavijo v javnosti. V preteklosti so bile uporabljene razmeroma redko, tipično pa so bile napisane za napad na ciljano organizacijo. Danes lahko kiberkriminalci takšno škodljivo programsko opremo preprosto kupijo v temnih predelih spleta za vsega nekaj sto evrov.

Zaščita pred nevarnostmi ničtega dne je zato še kako nujna za vse organizacije in podjetja, ki morajo skrbno varovati svoje podatke. Ker je prag nakupa zmogljivih orodij za spletne napade tako nizek, morajo podjetja svojo obrambo pred digitalnimi nevarnostmi postaviti zelo temeljito.

## ZAUPAJO NAM

Seznam naših referenc na področju zagotavljanja informacijske varnosti in varovanja IT-okolij pred škodljivo programsko opremo je resnično dolg. Zaupajo nam velika podjetja s področja financ, zdravstva, industrije in številne vladne organizacije. Mnogi projekti s področja informacijske varnosti so zaupne narave, zato o njih javno ne govorimo. Kratki povzetki nekaterih varnostnih projektov so potencialnim strankam na voljo na zahtevo.

Naše varnostne rešitve za obrambo pred škodljivimi kodami vseh vrst uporabljajo kombinacijo komplementarnih varnostnih ukrepov in rešitev, ki so bili zasnovani prav za odkrivanje in preprečevanje nevarnosti ničtega dne.

Vaše IT-okolje temeljito pregledamo in opravimo analizo potencialnih groženj vaši organizaciji. Ne gremo se vsakdanjih projektov, niti ne uporabljamo splošnih varnostnih rešitev, saj nobeno IT-okolje danes ni več običajno, nasprotno, številna so (zelo) kompleksna, saj v njih deluje več povezanih sistemov in aplikacij, ki so se razvijali skozi čas. Našo ekipo varnostnih strokovnjakov sestavljajo IT-arhitekti, preizkuševalci varnostnih lukenj, sistemski inženirji ter namenski IT varnostni strokovnjaki. Ti skupaj načrtujejo in postavijo varnostno rešitev, ki je učinkovita, prijazna do zaposlenih ter enostavno upravljiva – predvsem pa povsem prilagojena VAM.

### POSKRBIMO ZA:

- *Temeljit pregled in analizo IT-okolja stranke ter svetujemo glede ureditve področja informacijske varnosti.*
- *Načrtujemo sisteme zaščite pred škodljivimi kodami.*
- *Implementiramo sisteme zaščite pred škodljivimi kodami.*
- *Podpiramo sisteme zaščite pred škodljivimi kodami ter (po potrebi) pomagamo pri odpravi posledic varnostnih incidentov.*

### SPECIALISTI ZA INFORMACIJSKO VARNOST

*Pri informacijski varnosti je ubiranje bližnjic lahko zelo nevarno in drago. V NIL-u si jih ne privoščimo. Smo specialisti za ureditev področja informacijske varnosti, naše tipične stranke so:*

- *Organizacije z visokim tveganjem ciljanih napadov in ranljivosti na škodljivo programsko opremo*
- *Organizacije s kompleksnimi sistemi in poslovnimi procesi, ki uporabljajo varnostne rešitve starejšega datuma*

Za dodatne informacije o NIL-ovih rešitvah in storitvah s področja informacijske varnosti nam pišite na elektronski naslov **consulting@nil.com**.