



Podjetje

Si.mobil, d. d.



Sektor

Telekomunikacije

Vodja IT oddelka

Andraž Zmajšek

IS topografija

500 računalnikov; Windows in Linux platforme

Varnostne potrebe

Nevarne točke: e-mail; splet; prenosni računalniki, ki se priključujejo na nepreverjene vire neavtoriziran software, ki ga vnašajo uporabniki

Ključne zahteve: Robustna AV zaščita; optimizirana koda, ki ne degradira sistemskih zmogljivosti; avtomatsko posodabljanje; preprosta centralizirana administracija; proaktivna zaščita brez popravkov proti sprotnim grožnjam (manjša odvisnost od hitrosti nadgradenj); enostavna možnost sistemske de-inštalacije.

Rešitev

ESET NOD32 uporabnik od 2005

Lokacija

Si.mobil, d. d., Ljubljana, Slovenija

Spletni naslov

www.simobil.si

Zmagovita omrežna rešitev


Težava večine tako imenovanih »uveljavljenih« znamk protivirusne zaščite je, da so enostavno preobilni in njihovo delovanje degradira delovanje IT sistemov do te mere, da ovirajo normalno delovanje podjetja. A bolj razgledani IT-jevci čedalje pogosteje segajo po vzhajajoči zvezdi, ki velike znamke prehitveva z minimalno porabo sistemskih resursov a z učinkovitostjo težkokategornega borca. Za pričevanje o odločitvi za NOD32 smo povprašali Andraža Zmajška, vodjo IT oddelka podjetja Si.mobil, d.d.

Z velikostjo pride tveganje

Družba Si.mobil je drugi največji mobilni operater v Sloveniji. IT ekipa podjetja obvladuje heterogeno IT okolje, ki vključuje podporo računalnikom in uporabnikom, izobraževanje, internet, elektronsko pošto, hranjenje podatkov, tiskanje in nameščanje ter vzdrževanje aplikacij. S 500 računalniki je možnosti za IT nevarnosti veliko. Izziv za Si.mobil je bil robusten sistem zaščite, ki ne bi imel vrtoglave cene, predvsem pa ne bi upočasnil delovanja sistema.

Negativna plat super-velikosti

Si.mobil-ov prejšnji AV sistem je deloval, a družba je bila soočena z neprijetnim skokom cen ob možnosti podaljšanja pogodbe. Zato si je vzela čas za evaluacijo ostalih možnosti. Čeprav je težko iti mimo uveljavljenih blagovnih znamk, se je vodja IT oddelka iz izkušenj naučil, da avtomatska selekcija ni vedno najboljša. *“Nortoni in McAfeeji tega sveta imajo različne probleme, bodisi s ceno na kos, namestitvijo, ali degradacijo sistema, ki ga tako veliki programi neizbežno povzročijo. Vedno smo se skušali osredotočiti na AV izdelek, ki dobro opravi svoje delo, namesto da je del nekega večjega paketa, ki sicer počne celo vrsto stvari, ki nas ne zanimajo. Želeli smo osredotočeno rešitev”.*



”Ko se je bližal čas obnove AV sistema, je prišlo do mene več sodelavcev, ki so razložili, da doma uporabljajo NOD32 in da je bil videti kot dober izdelek. Imel je dobre lastnosti, dobre povratne informacije od uporabnikov, kakor tudi dobra poročila o učinkovitosti.”

-Andraž Zmajšek,
vodja IT oddelka
Si.mobil, d.d.

Moč izkušene družbe

Odločujoči dejavnik je bil, ko so pretehtali vsa priporočila IT ekipe, mnogi izmed njih so namreč že uporabljali NOD32 na svojih domačih računalnikih. **”Ko se je bližal čas obnove AV sistema, je prišlo do mene več sodelavcev, ki so razložili, da doma uporabljajo NOD32 in da je bil videti kot dober izdelek. Imel je dobre lastnosti, dobre povratne informacije od uporabnikov, kakor tudi dobra poročila o učinkovitosti. Zdelo se je, da se bo dobro prilagajal veliki organizaciji”.**

Majhen a popolno formiran

NOD32 kombinira izjemno majhno porabo sistemskih sredstev z veliko hitrostjo pregledovanja in dokazano sposobnostjo detekcije. Jedro tega delovanja je realno-časovna hevristična tehnologija imenovana ThreatSense, ki drži dobro dokumentiran in preizkušen rekord pri odkrivanju novih groženj v kritičnem časovnem obdobju med pojavitvijo nove grožnje in izidom nadgradnje novih virusnih definicij.

Ključni faktor uspeha za Si.mobil je bila tudi primernost NOD32 za okolja z majhno možnostjo prenosa podatkov (low bandwidth), zaradi majhne instalcijske velikosti (okrog 8MB) in posodobitvami okoli 50K. Z velikim številom oddaljenih uporabnikov je bilo zelo pomembno, da se je dalo operirati s posodobitvami v okoljih z majhnim prenosom podatkov. Super-velike datoteke s posodobitvami bi predstavljale veliko oviro in ena od prednosti NOD32 so brez dvoma bile majhne posodobitve.

Upoštevati je bilo potrebno tudi namestitev ter porabo sistemskih sredstev. Splošno mnenje je, da je visoka poraba resursov zanesljiv indikator problematične namestitve, ki jo produktni paketi še dodatno zapletejo. **”Vseh AV programov ni enostavno namestiti. Požrešni programi včasih povzročijo, da druge aplikacije na računalniku delujejo občutno počasneje. Dodaten problem pa so tudi sestavni deli programskih paketov, ki včasih nočejo delovati individualno.”**



NOD32 doseže vrhunske ocene

Trenutno je z NOD32 zaščiteno 500 računalnikov, a brez centraliziranega pristopa k namestitvi in sprotne vzdrževanju lahko cene za velike sisteme kot je Si.mobil postanejo astronomske. IT si ne more privoščiti individualnega izobraževanja vseh uporabnikov, da bi le ti znali sami pravilno namestiti vse elemente zaščite. Torej je morala biti namestitev končnim uporabnikom takorekoč nevidna, oz. povsem nemoteča. Prav tako pa morajo velike organizacije upoštevati možnost de-instalacije. ***“Če se tega ne da opraviti centralno za celotno mrežo in moraš program odstranjevati s posameznih računalnikov, potem imaš pred seboj lahko velik problem.”***

Z ESETovim NOD32 je IT oddelek dobil cel nabor orodij za upravljanje in poročanje o aktivnostih sistema. Centralni zrcalni strežnik avtomatizira področja administracije, kot je na primer namestitev, ki avtomatsko replicira vnaprej konfiguriran sistem na vse kliente in skrbi za njihovo posodabljanje. Konzola omogoča centralen pregled nad posodobitvami vseh uporabnikov in odkrivanjem virusov pri njih.

Narava antivirusne zaščite ne omogoča precizne ocene prihranka z vlaganjem vanjo, saj je nemogoče oceniti morebitno škodo sistemu, če se le ta še ni zgodila. Brez dvoma pa se da oceniti, da bi resna grožnja tako velikemu sistemu, ki bi ogrozila nemoteno delo, povzročila velik strošek organizaciji. Vendar pa vodja IT oddelka vidi velike prednosti in neposredne prihranke za celoten IT z izkoriščanjem prednosti programa NOD32. ***“Karkoli, kar spodbuja uporabnike, da ohranjajo svoje računalnike redno posodobljene je velika prednost za IT. Administrativnega dela je nedvomno manj. Včasih smo imeli težave s programiranjem prenosa nadgrajenja. Nekateri so celo zahtevali de-instalacijo prejšnje verzije. Posodobitve programa NOD32 pa so enostavnejše in zahtevajo dosti manj truda.”***

”Karkoli, kar spodbuja uporabnike, da ohranjajo svoje računalnike redno posodobljene je velika prednost za IT.

Administrativnega dela je nedvomno manj. Posodobitve programa NOD32 so enostavnejše in zahtevajo dosti manj truda”

-Andraž Zmajšek,
vodja IT oddelka
Si.mobil, d.d.