Študija primera

Kibernetski operativni center južnomoravske regije

Zaradi vse večjega števila kibernetskih incidentov, med katerimi je bilo več javno objavljenih, se je Južnomoravska regija odločila za uvedbo dodatnih varnostnih ukrepov.
Na podlagi interne analize je njen center za kibernetske operacije ugotovil, da je ESET-ova rešitev za končne točke in EDR pravo orodje za povečanje kibernetske varnosti in zgodnje odkrivanje kibernetskih napadov.

KYBERNETICKÉ OPERAČNÍ CENTRUM

INDUSTRIJA
Varnost IT, javni sektor

SPLETNA STRAN
www.kr-jihomoravsky.cz

DRŽAVA
Češka republika

IZDELEK
ESET Inspect, 3000 sedežev

eset Digital Security
Progress. Protected.

www.eset.com

NAROČNIK

Kibernetski operativni center (KOC) je oddelek, ki je vključen v urad direktorja regije Južna Moravska. Njegova naloga je centralno spremljanje in ocenjevanje morebitnih groženj kibernetski varnosti v omrežjih regionalnega urada in povezanih prispevnih organizacij. To prinaša več prednosti za regijo Južna Moravska in organizacije, zahvaljujoč dodelanim strokovnjakom, ki se ukvarjajo z varnostnimi grožnjami v celotnem omrežju, izmenjavo informacij med temi subjekti in izvajanjem učinkovitih ukrepov v najkrajšem možnem času. Kibernetski operativni center je prvi, ki je uspešno izvedel tovrstni projekt na regionalni ravni.

IZZIV

Glavni izziv bi lahko povzeli z besedami*: "Ne moreš nadzorovati in se boriti proti temu, česar ne vidiš,*" pravi Aleš Staněk, vodja oddelka KOC.

Družba KOC je potrebovala vire podatkov, ki zagotavljajo podrobne informacije o obnašanju računalnikov in strežnikov v posameznih organizacijah. Končne postaje in strežniki so bili še en pomemben element te varnostne sestavljanke. Hkrati je moralo upravljanje protivirusne rešitve ostati v rokah organizacij, rešitev EDR pa ni smela na noben način posegati v obstoječe delovanje.

"Ni šlo samo za zbiranje informacij. Morali smo imeti možnost aktivnega odzivanja na varnostne incidente. To je bila še ena ključna zahteva za potrebno rešitev EDR," dodaja Staněk.

REŠITEV

ESET Inspect družbi KOC zagotavlja dodatne podatke, k i jih varnostni analitiki potrebujejo pri svojem delu. KOC jih nato oceni v orodju SIEM v kontekstu informacij iz drugih virov (operacijski sistem, požarni zid, omrežna sonda itd.). *"Zahvaljujoč podatkom iz orodja ESET Inspect skoraj takoj izvemo za varnostni incident in se lahko nanj takoj odzovemo,"* pojasnjuje Staněk. Zahvaljujoč rešitvi lahko družba KOC aktivno ukrepa v sodelovanju z organizacijami za zaustavitev morebitnega ogrožanja infrastrukture, na primer z izolacijo osumljenega računalnika iz omrežja, dokler se incident ne razišče.

IZVAJANJE

Družba ESET je v sodelovanju z družbo AXENTA, a.s., projekt razdelila na dve fazi - izvajanje in optimizacijo.

Postopek izvajanja

Glavna prednost sistema ESET Inspect je enostavnost njegove namestitve v okolju, v katerem so prisotni varnostni izdelki ESET, vključno z osrednjim upravljanjem. Izvedba je bila sestavljena iz dveh korakov - delov za namestitev strežnika in zagotavljanja distribucije agentov EI. *"ESET-ova rešitev EDR je bila nameščena v približno 3.000 končnih napravah v 11 različnih organizacijah. Kljub tako velikemu številu postaj in različnih infrastruktur, smo implementacijo upravljali v okviru 4 tednih,* "opisuje Lukáš Přibyl, generalni direktor podjetja AXENTA. Uvedba je bila dolgotrajna zaradi usklajevanja urnika z vsemi posameznimi organizacijami. Ko smo jim zagotovili, da ni nobenih konfliktov z njihovim okoljem, smo prešli na drugo, optimizacijsko fazo.

Optimizacija ali iskanje igle v kopici sena

Faza optimizacije projekta je bila še bolj zahtevna, predvsem zato, ker je bilo 11 različnih omrežij. Ta faza je vključevala tri glavne korake:

- oblikovanje univerzalnega nabora pravil za bolnišnično okolje,
- distribucija v vse organizacije,
- prilagoditev občutljivosti pravil glede na specifično okolje.

Za poenostavitev faze optimizacije je bil za množično distribucijo pravil uporabljen strežnik API, natančno prilagajanje pa je potekalo prek spletnega vmesnika Enterprise Inspector. *"Začetno optimizacijo v vseh organizacijah smo lahko opravili v treh mesecih,"* dodaja Pribil. Vendar je treba dodati, da je bila optimizacija zaradi visoke občutljivosti rešitve ESET Inspect del neprekinjen proces, saj lahko vsaka na novo uvedena aplikacija v okolje organizacije pokaže nepričakovano obnašanje, ki ga je treba popraviti.

VIDLJIVOST OMREŽJA KOT KLJUČ DO PREPREČEVANJA

ESET Inspect pomaga pri odkrivanju nepravilnosti in napak različne resnosti. *"Običajno je šlo za slabo konfiguracijo omrežij ali neustrezne nastavitve aplikacij, ki lahko v skrajnih primerih privedejo do varnostnih incidentov,"* pojasnjuje Aleš Staněk. Na podlagi ugotovljenih pomanjkljivosti KOC nenehno pripravlja priporočila za prilagoditev varnostnih politik in nastavitev aplikacij v organizaciji. "*Dragocene informacije iz programa ESET Inspect so postale sestavni del reševanja večine morebitnih incidentov z varnostnimi težavami. Tako nam zagotavlja dodatne informacije za ponazoritev konteksta dogodka, kij ih prej nismo imeli,"* sklene.

KLJUČNE PREDNOSTI

- Enostavna uvedba
- Aktivno odzivanje in zgodnje odkrivanje
- Izjemna vidljivost omrežja