Nabava sigurnosnih komponenti podatkovnih centara
-
središnji vatrozidni sustav

Obavijest gospodarskim subjektima s ciljem prethodnog istraživanja tržišta

CARNET

Sadržaj

1 Uvod

Hrvatska akademska i istraživačka mreža – CARNET planira započeti postupak javne nabave **sigurnosnih komponenti podatkovnih centara - središnji vatrozidni sustav** u sklopu II. faze programa „e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće“.

Sukladno Zakonu o javnoj nabavi (NN 120/16) sa svrhom pripreme nabave i informiranja gospodarskih subjekata o svojim planovima i zahtjevima u vezi s nabavom, u nastavku obavijesti CARNET objavljuje zahtjeve vezane za nabavu i isporuku sigurnosnih komponenti podatkovnih centara - središnji vatrozidni sustav.

Radi daljnjeg planiranja i provedbe postupka nabave te izrade Dokumentacije o nabavi molimo sve zainteresirane gospodarske subjekte da dostave primjedbe i prijedloge prema traženim informacijama i troškovnikom najkasnije do 15.06.2022. na adresu elektroničke pošte nabava@carnet.hr.

CARNET će analizirati dostavljene informacije i temeljem dobivenih podataka sastaviti dokumentaciju o nabavi.

Prilikom provođenja istraživanja tržišta CARNET će postupati na način da svojim postupcima ne narušava tržišno natjecanje niti krši načela zabrane diskriminacije i transparentnosti.

Rezultati provedenog istraživanja ne obvezuju CARNET niti se stvara bilo kakav pravni posao ili odnos s gospodarskim subjektima koji sudjeluju u istraživanju.

1.1 Kontekst postupka ove javne nabave

Planirana nabava provodi se u sklopu programa modernizacije hrvatskog školskog sustava naziva “e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće”.

Opći cilj programa e-Škole je jačanje kapaciteta osnovnoškolskog i srednjoškolskog obrazovnog sustava, s ciljem osposobljavanja učenika za tržište rada, daljnje školovanje i cjeloživotno učenje.

Program e-Škole se provodi kroz sljedeće:

1. Pilot projekt „e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot -projekt)" u razdoblju od 1. ožujka 2015. godine do 31. kolovoza 2018. godine u koji je bilo uključeno 151 škola diljem Hrvatske,
2. Veliki projekt koji je planiran u trajanju od 1. rujna 2018. godine do listopada 2023. godine.

Nositelj projekta je Hrvatska akademska i istraživačka mreža - CARNET. Mjerodavno tijelo koje je nadležno CARNET-u je Ministarstvo znanosti i obrazovanja kojemu je nadležna Vlada RH. Projekt se financira sredstvima iz Europskog fonda za regionalni razvoj (EFRR) u sklopu Operativnog programa "Konkurentnost i kohezija" (OPKK) i iz Europskog socijalnog fonda (ESF) u sklopu Operativnog programa "Učinkoviti ljudski potencijali" (OPULJP) te je iz tog razloga projekt podijeljen na Projekt A (sufinanciran sredstvima EFRR) i Projekt B (sufinanciran sredstvima ESF).

2 Predmet nabave

Predmet nabave je u planu nabave naveden kao „Nabava sigurnosnih komponenti podatkovnih centara - središnji vatrozidni sustav“.

Predmet se planira realizirati nabavom sljedećih komponenti sustava:

- Izrada dokumentacije upravljanja informacijskom sigurnošću u okruženju softverski upravljanog podatkovnog centra (eng. SDDC – Software Defined Data Center)
- Sustav za upravljanje log zapisima i sigurnosnim događajima (eng SIEM – Security Information and Event Management)
- Vatrozidni sustav koji će omogućiti zaštitu SDDC okruženja i središnjih računalnih usluga od napada s Interneta
- Uspostava i konfiguriranje sustava zaštite putem rekurzivne rezolucije domena koji će omogućiti zaštitu SDDC okruženja, središnjih računalnih usluga i korisnika koristeći DNS (eng. DNS - Domain Name System)

2.1 Izrada dokumentacije upravljanja informacijskom sigurnošću SDDC okruženja

Kako bi se osiguralo kvalitetno i sveobuhvatno upravljanje sigurnosnim zahtjevima SDDC okruženja, planirana je izrada sljedeće dokumentaciju koja definira osnovne aspekte sigurnosnog upravljanja SDDC okruženjem.

Potrebno je izraditi sljedeću dokumentaciju:

- Krovna dokumentacija upravljanja informacijskom sigurnošću SDDC okruženja
  - politika sigurnosti SDDC okruženja
  - politika upravljanja ranjivostima i sigurnosnim zakrpama SDDC okruženja
  - politika upravljanja log zapisima SDDC okruženja
  - politika upravljanja mrežnom sigurnošću SDDC okruženja
  - politika upravljanja pričuvnom pohranom SDDC okruženja
  - politika upravljanja i zaštite repozitorija programskog koda SDDC okruženja
  - politika upravljana korisničkim i privilegiranim pristupom SDDC okruženja
  - politika upravljanja razvojem i isporukom aplikacija SDDC okruženja
- Operativne procedure za održavanje mjera sigurnosti unutar SDDC okruženja
  - procedura za klasifikaciju SDDC imovine prema kritičnosti
  - procedura za zamjenu hardvera unutar SDDC okruženja
  - procedura odgovora na sigurnosne incidente unutar SDDC okruženja
  - procedura nadzora i praćenja sigurnosnih događaja SDDC okruženja
  - procedura za testiranje sigurnosnih ranjivosti i instalaciju sigurnosnih zakrpi unutar SDDC okruženja
  - procedura za sigurnosno ojačavanje komponenti SDDC okruženja
  - procedura za isporuku aplikacija i servisa unutar SDDC okruženja (interni i vanjski razvoj)
  - procedure za oporavak u slučaju katastrofalnih događaja (eng. disaster recovery)
  - procedura za sigurno brisanje medija.

Od Ponuditelja se očekuje provođenje sljedećih aktivnosti:

- pregled postojeće dokumentacije vezane uz dizajn i sigurnosne zahtjeve SDDC okruženja,
- identifikacija sigurnosnih zahtjeva SDDC okruženja korištenjem sljedećih aktivnosti:

  - radionice i intervjui s odgovornim osobama odgovornim za uspostavu i održavanje SDDC okruženja,
  - radionice i intervjui s osobama odgovornim za upravljanje informacijskom sigurnošću CARNET-a
  - radionice i intervjui s vanjskim partnerima koji su sudjelovali u implementaciji SDDC okruženja,
  - analiza postojećih politika i procedura vezanih uz upravljanje informacijskom sigurnošću CARNET informacijskog sustava,
- izrada prethodno navedene dokumentacije.

2.2 Sustav za upravljanje log zapisima i sigurnosnim događajima (SIEM)

S ciljem unaprjeđenja razine sigurnosti SDDC okruženja i podizanja razine sposobnosti pri detekciji i rješavanju sigurnosnih incidenata, CARNET je implementirao Splunk Enterprise SIEM za upravljanje operativnim (eng. log) zapisima i sigurnosnim događajima koji omogućuje:

- prikupljanje i agregaciju podataka o log zapisima unutar DC okruženja,
- Vizualizaciju podataka prikupljenih iz komponenti IT infrastrukture i poslovnih aplikacija.
- korelaciju informacija o sigurnosnim događajima između različitih izvora log zapisa,
- uzbunjivanje odgovornih osoba pri detekciji sigurnosnih događaja,
- naprednu istragu detektiranih sigurnosnih incidenata, odnosno forenzičku analizu,
- potpuno upravljanje životnim ciklusom log zapisa (prikupljanje, obrada, pohrana,

Naručitelj raspolaže postojećim SIEM sustavom kojim obrađuje 28 GB zapisa dnevno, te je planirano proširenje kapaciteta sustava na minimalno 50GB dnevno.

Uz proširenje kapaciteta sustava potrebno je implementirati elemente sigurnosnog upravljanja SDDC okruženjem koji će biti definirani dokumentacijom upravljanja informacijskom sigurnošću SDDC okruženja.

2.3 Vatrozidna zaštita

SDDC dizajn predviđa uspostavu vanjskog vatrozida koji će omogućiti zaštitu SDDC okruženja od napada s Interneta, sljedećih karakteristika:

Kategorija	Opis
Opće karakteristike	• vatrozid nove generacije (eng. NG Firewall)
Form factor	• maksimalno 1RU, 19 inch, rack mountable
Karakteristike	• minimalna propusnost vatrozida pri IPS inspekciji prometa: 40 Gbps pri veličini IP paketa od 1024 okteta • minimalna propusnost sabirnice vatrozida: 40 Gbps • Broj podržanih istovremenih konekcija: minimalno 10.000.000 • mogućnost rada u *active/standby*, *active/active* i *cluster* modu za minimalno 2 uređaja • podržano ograničavanje resursa po virtulanim vatrozidima (*Security Context*) i to minimalno po sljedećem: broju

	istovremenih TCP ili UDP konekcija, broju poslužitelja koji se mogu konektirati kroz vatrozid, broju SSH konekcija, broju sistemskih log zapisa i broju adresnih translacija
	• sve komponente sustava moraju podržavati IPv4 i IPv6 protokole za sve ugrađene funkcionalnosti sigurnosne zaštite
	• podrška za primjenu politika temeljenih na korisnicima definiranim na imeničkom servisu
	• mogućnost provjere DNS prometa te detekciju manipulacija istim
	• napredna zaštita od zlonamjernog sofvera (eng. malware) uključujući *zero-day* napade s detekcijom anomalija, a koja omogućava:
	  ○ kontinuiranu analizu datoteka i prometa s ciljem detekcije i sprječavanje zlonamjernih datoteka
	  ○ funkcionalnost sandboxinga za maliciozne datoteke u cloudu
	  ○ mogućnost provjere sadržaja unutar arhiviranih i komprimiranih datoteka bez dodatne kriptografske zaštite (ZIP, RAR, 7Z, gzip, arj, cab i sl.)
	  ○ praćenje širenja malwarea i komunikacije
	  ○ detekcija i blokiranje pokušaja exploita
	  ○ korelacija diskretnih događaja u koordiniranim napadima
	• vidljivost i kontrola aplikacija (eng. *Application Visibility and Control*)
	• mogućnost otkrivanja i prevencije zlonamjernih mrežnih aktivnosti - IPS (Intrusion Prevention System)
	• mogućnost izuzimanja dijelova prometa iz provođenja naprednih provjera zbog uštede resursa ili nekog drugog razloga
	• *network reputation* globalna korelacija
	• prilagođavanje IPS pravila,
	• mogućnost podrške filtriranja HTTP prometa koji prolazi kroz uređaj na temelju URL-a, domene, hostnamea i dijela URL-a.
	• mogućnost podrške za SSL/TLS dekripciju
	• sve funkcionalne komponente ponuđenog rješenja moraju imati mogućnost slanja dnevničkih zapisa minimalno u syslog formatu na udaljene sustave uz zadržavanje lokalnih dnevničkih zapisa

Komunikacijska sučelja i priključivanje	• minimalno ugrađeno 4 integrirana Ethernet sučelja minimalne brzine 10 Gbps • minimalno jedno integrirano i dedicirano Gigabit Ethernet upravljačko sučelje • minimalno 1 x konzolni port (RJ-45) • minimalno 1 x USB port • Naručitelj na mrežnoj opremi raspolaže s 100G QSFP28 sučeljima. Obaveza Ponuditelja je da isporuči opremu i priključne kabele potrebne za međusobno spajanje isporučene opreme na mrežu Naručitelja. • Ponuđeni sustav mora podržavati funkcionalnost virtualnih vatrozida koji imaju sve funkcionalnosti vatrozida nove generacije centralno upravljanih zajedničkim upravljačkim sustavom • Sustav virtualnih instanci vatrozida mora imati mogućnost instaliranja na KVM hipervizor i podržavati OpenStack network mode • Sustav mora podržavati detektiranje i označavanje zaraženih virtualnih poslužitelja unutar OpenStack platforme te prosljeđivati informacije o zaraženim virtualnim poslužiteljima OpenStack SDN (eng. Software Defined Network) kontroleru
Upravljanje	• ukoliko Ponuditeljevo rješenje sadrži zasebnu upravljačku komponentu ista može biti isporučena u obliku zasebnog uređaja (eng. appliance), u obliku virtualnog poslužitelja • u slučaju da Ponuditelj upravljačku komponentu sustava želi isporučiti u obliku virtualnog poslužitelja isti mora podržavati KVM hipervizor (Proxmox/OpenStack)" • Upravljačka komponenta mora centralno upravljati svim vatroizdnim funkcionalnostima, uključujući fizičke sustave, virtualne kontekste i virtualne instance vatrozida na OpenStack platformi • Sustav za upravljanje mora imati mogućnost povezivanja sa više OpenStack SDN kontrolera • Sustav za upravljanje mora imati mogućnost automatskog dohvaćanja i dinamičkog ažuriranja objekata iz više OpenStack SDN kontrolera za OpenStack • Sustav za upravljanje mora imati mogućnost korištenja objekata dohvaćenih iz OpenStack SDN kontrolera u vatrozidnim sigurnosnim politikama i automatsku primjenu politika nakon ažuriranja objekta iz OpenStack SDN kontrolera
Napajanje	• standardno AC napajanje 220-240V, 50/60 Hz • potrebni kabeli za napajanje
Količina / licence	• Broj uređaja u sustavu: minimalno 6 • sve potrebe licence je potrebno isporučiti na period od minimalno 5 godina
Mjesta isporuke	• tri lokacije u Republici Hrvatskoj, na svakoj lokaciji minimalno 2 uređaja

2.4 Uspostava i konfiguriranje sustava zaštite putem rekurzivne rezolucije domena koristeći DNS (Domain Name System)

Sustav zaštite putem rekurzivne rezolucije domena treba omogućiti dodatnu zaštitu SDDC okruženja, središnjih računalnih usluga i korisnika programa e-Škole upravljanjem upitima i odgovorima od DNS (Domain Name System) sustava.

Ključne planirane mogućnosti sustava:

- Upravljanja DNS sustavom, putem jedinstvene upravljačke konzole, uključivo sa sustavom izvješćivanja
- Sustav mora biti izveden on-premise, isključivo sa sigurnosnim ažuriranjima od dobavljača.
- Sustav mora podržavati IPv4 i IPv6 adrese
- Sustav mora omogućavati rekurzivnu rezoluciju domena koristeći DNS sukladno zahtjevima po RFC 1034, 1035, 1995, 1996, 2671, 2782, 3596
- Uređaj mora podržavati slijedeće algoritme javnih ključeva za DNSSEC: RSA/MD5, DSA, RSA/SHA1, RSA/SHA-256, RSA/SHA-512
- Sustav mora osigurati REST API mehanizam za kontrolu sustava, izvođenje i automatizaciju zadataka, dokumentacija API sustava mora biti dostupna zajedno s primjerima korištenja.
- Sustav mora sigurno zapisati i omogućiti pristup do neizmijenjene informacije o svim promjenama koje su izvršili administratori (tko, kada, što se promijenilo)
- Sustav mora moći slati zapise (logove) u centralni repozitorij pomoću Syslog mehanizma (TCP i UDP)
- Sustav mora omogućiti administratorima da imaju prava na temelju grupa i uloga (eng. RBAC - Role Based Access Control), radi kontrole pristupa resursima
- Sustav mora podržavati autentifikaciju korisnika minimalno putem lokalne korisničke baze, RADIUS protokol, LDAP, Microsoft Active Directory, SAML
- Pristup konzoli za administraciju sustava mora biti moguć putem udaljenog sučelja dostupnog putem SSH protokola, koji podržava SSHv2
- Rekurzivna DNS izvedba, sa svim omogućenim sigurnosnim značajkama od najmanje najmanje 4000 DNS upita u sekundi
- Sustav mora podržavati uslugu DNS Anycast za IPv4 i IPv6 (koristeći BGP i OSPF protokole)
- Sustav mora podržavati DNSSEC validaciju
- Sustav mora imati funkciju otkrivanja i blokiranja DNS tuneliranja koristeći analitičke obrasce koji se temelje na strojnom učenju te koji omogućuju i otkrivanje nepoznatih uzoraka tuneliranja kao i eksfiltraciju podataka putem DNS-a.
- Sustav mora imati funkciju otkrivanja infiltracije preko DNS-a, posebno mora otkriti tehnike koju koriste zlonamjerni softveri
- Sustav mora imati Response Policy Zones (RPZ) funkcionalnost kako bi djelovao kao DNS vatrozid na temelju aktualnog popisa zlonamjernih domena
- Sustav mora imati sposobnost poduzimanja radnji na DNS upitima i odgovorima na temelju definiranih sigurnosnih politika
- Sustav mora moći filtrirati domene na temelju kategorizacije sadržaja

U sklopu elemenata troškovnika potrebno je uključiti potrebne pristupe sustava aktualiziranim podacima o prijetnjama kibernetičkoj sigurnosti na razdoblje od najmanje 5 godina nakon primopredaje.

Izvedeni sustav mora biti pokriven uslugom podrške u trajanju od najmanje 5 godina od primopredaje, u režimu 24x7, s odzivom najkasnije sljedeći radni dan.

3 Troškovnik i istraživanje tržišta

Od zainteresiranog gospodarskog subjekta očekujemo da u Prilogu 2.Troškovnik navede u svim stavkama gdje je primjenjivo:

Za komponentu nabave: „Izrada dokumentacije upravljanja informacijskom sigurnošću SDDC okruženja“ sljedeće odgovore i procjene:

1. Procjena ukupne cijene za Izradu dokumentacije

Za sustav za upravljanje log zapisima i sigurnosnim događajima (SIEM) sljedeće:

1. Procjenu troškova nabave proširenja postojećeg sustava do minimalno 50GB zapisa/dnevno
2. Procjenu godišnjeg operativnog troška korištenja sustava, za minimalno ukupno korištenje sustava od pet godina, po svim troškovnim komponentama sustava,

Za sustav vatrozidne zaštite:

1. Prijedlog jednog ili više modela uređaja, proizvođača i cijene uređaja za opisanu nabavu koji zadovoljavaju navedenu minimalnu specifikaciju
2. Prijedlog jednog ili više modela uređaja, njegovog proizvođača i cijene uređaja koji ne zadovoljavaju u cijelosti navedenu minimalnu specifikaciju, ali su cijenom prvi povoljniji od prijedloga modela pod 1.
3. Prijedlog jednog ili više modela uređaja, njegovog proizvođača i cijene uređaja koji je boljih specifikacija od traženih i cijenom su prvi skuplji model od prijedloga modela pod 1.

Za sustav zaštite putem rekurzivne rezolucije domena koristeći DNS (Domain Name System):

1. Prijedlog jednog ili više sustava i/ili modela uređaja, proizvođača i cijene za opisanu nabavu koji zadovoljavaju navedenu minimalnu specifikaciju i tražene usluge

Ponuditelj može elektroničkom poštom dodatno navesti pisane odgovore, opise i argumentaciju za sljedeća pitanja:

- Za komponentu nabave: „Izrada dokumentacije upravljanja informacijskom sigurnošću SDDC okruženja“ sljedeće informacije:
  - Opis profila stručnjaka (jedan ili više) koji je potrebni za izradu navedene dokumentacije za SDDC okruženje Naručitelja
- Za sustav vatrozidne zaštite:
  - Dizajn rješenja i logičku shemu pozicioniranja i mrežnog povezivanja elementa sustava kako međusobno tako i prema okolnim sustavima Naručitelja
  - Za razlike u predloženim uređajima Ponuditelj može dodatno navesti pisanu argumentaciju koju Naručitelj može uzeti u obzir pri odabiru alternativnog (povoljnijeg ili skupljeg) modela za postupak nabave.
- Ostale primjedbe i sugestije povezane s planiranim postupkom nabave

3.1 Ostali uvjeti i upute

Za jamstvo za kvalitetnu implementaciju sustava odabrani Dobavljač će dostaviti Naručitelju jamstvo za otklanjanje nedostataka u trajanju od 5 godina nakon izvršenja Ugovora.

Temeljem svih dobivenih podataka, CARNET će sastaviti dokumentaciju o nabavi.

Dodatna pitanja zainteresirani gospodarski subjekti mogu dostaviti na elektroničku poštu **nabava@carnet.hr** najkasnije

CARNET će sve informacije koje nastanu temeljem dodatnih pitanja javno objaviti na mrežnim strancima na isti način kao i ovu obavijest.