

TEHNIČKI ZAHTJEVI PREDMETA NABAVE

Red. broj	Obvezne tehničke značajke kojima AV sustav mora udovoljavati i mogućnosti koje mora imati	Zadovoljava DA/NE
1.	Zaštita od zločudnog koda (malware)	
	Instalacija AV SW	
2.	Mogućnost automatske instalacije cijelokupnog sustava antivirusne zaštite na nova umrežena računala	
3.	Automatsko pronalaženje nezaštićenih radnih stanica u vlastitoj mreži, te njihovo uključivanje u sustav nadzora i sinkronizaciju ili izoliranje iz mreže	
4.	Postavljanje programskog rješenja na umreženu (WAN, VPN LAN) računalnu opremu korisnika sa središnjeg mjesta	
	Objekti (uređaji, sklopovi, ...) na kojima se štite sadržaji	
5.	Sustav mora provjeravati i štititi od ugroza (prijetnji) sve sastavne dijelove (komponente) radnih stanica kao i sve one uređaje izravno priključene na radnu stanicu Pod sastavnim dijelovima naročito se podrazumijevaju glavna memorija (RAM), BIOS, čvrsti diskovi (HDD), disketni (FDD) i optički uređaji (ODS), USB flash memorije, vanjske diskove, kartične memorije (CF, SD, xD i drugi) te bilo koja druga ulazno-izlazna periferna jedinica	
6.	Zaštita prometa elektroničke pošte poslužitelja odnosno klijenata e-pošte (primjerice MS Exchange, MS Outlook, OE, Win Live Mail, Mozilla, Lotus Domino)	
	Radna okolina AV SW	
7.	Mogućnost rada u okviru poslužiteljskih operativnih sustava, najmanje: Windows (minimalno Microsoft Windows Server 2008) Unix, Linux,	
8.	Mogućnost rada u okviru jednog ili više sljedećih (klijentskih) upravljačkih sustava za radne stanice Windowsa (minimalno Windows 7), Unix, Linux (minimalno RedHat, SUSE, UBUNT)	
9.	Mogućnost rada u okviru jedne od sljedećih okolina predviđenih za tzv. virtualizaciju i to za sva od proizvođača podržana izdanja Hyper-V i VMware ESX	
10.	Mogućnost nadziranja sljedećih podsustava elektroničke pošte (email server): Microsoft Exchanga Server 2010 i Lotus Domino	
	Način rada AV SW	

Red. broj	Obvezne tehničke značajke kojima AV sustav mora udovoljavati i mogućnosti koje mora imati	Zadovoljava DA/NE
11.	Uočavanje, prepoznavanje, uklanjanje ili izoliranje zločudnog koda	
12.	Uočavanje, prepoznavanje, uklanjanje ili izoliranje sumnjivog koda (zero-day)	
13.	Određivanje najvišeg dozvoljenog udjela procesorskog vremena tako da korisnik za vrijeme skeniranja računala (radnih stanica) neometano koristi računalno, odnosno rabi aplikativnu programsku opremu u svom poslovanju	
14.	Sustav mora imati integrirani modul proaktivne zaštite primjenom heurističkih algoritama	
15.	Provjere u stvarnome vremenu (real-time) svake ulazne datoteke ili niza ulaznih podataka u radnu stanicu, poslužitelja ili drugu sličnu opremu. Provjere u stvarnome vremenu (real-time) kod svakog pokušaja pristupa bibliotekama, datotekama, zapisima ili podacima na ili u bilo kojem dijelu radne stanice, poslužitelja ili slične opreme.	
16.	Pomoćni alat za stvaranje neovisnih medija za uklanjanje ili izoliranje ugroza ili prijetnji na neumreženoj računalnoj opremi	
17.	Zaštita prometa nastalog pokretanjem prijenosa podataka posebnim protokolima (primjerice FTP, HTP, HTTPS, ...)	
18.	Zaštita u prijenosu (kriptiranje) vlastitog prometa između upravitelja (administratora) sustava zaštite i štićene računalne opreme	
19.	Mogućnost skeniranja na temelju unaprijed određenih listi (bijela i crna lista)	
	Upravljanje AV SW	
20.	Daljinsko oblikovanje (konfiguriranje) zaštite s udaljenog, odnosno središnjeg mjesta	
21.	Pokretanja skeniranja računalne opreme i medija s udaljenog, odnosno središnjeg mjesta	

Red. broj	Obvezne tehničke značajke kojima AV sustav mora udovoljavati i mogućnosti koje mora imati	Zadovoljava DA/NE
22.	Sustav mora imati mogućnost definiranja standardnih konfiguracija za klijentsku zaštitu ('security policy') i mogućnost primjene zadataka na određene grupe klijenata (Grupe, Active Directory sinkronizacija)	
23.	Središnje upravljanje karantenama na korisničkoj računalnoj opremi (smještaj, naknadna provjera, trajno uklanjanje ili povrat pogrešno izoliranih datoteka)	
24.	Planiranje i raspoređivanje poslova i zadataka (na zahtjev, s odgodom, periodički)	
25.	Zaštita antivirusnog sustava od neovlaštenog pristupa	
26.	Održavanje softvera/otiska virusa	
27.	Automatizirani postupci obnavljanja programskog rješenja (AV softvera), središnja razdioba (odrednica) virusnih definicija i drugog zločudnog koda po radnim stanicama u vlastitoj računalnoj mreži (LAN, WAN) radi optimiranja korištenja resursa i smanjenja troškova	
	Štićeni sadržaj	
28.	Provjera cijelokupnoga sadržaja (zaglavila, poruke, prilozi i drugo) ulaznog i izlaznog prometa elektroničke pošte (e-mail), neovisno o vrsti programske opreme za upravljanje e-poštom na strani poslužitelja, odnosno na strani radne stanice kojima korisnik raspolaže. Provjera svih datoteka u IS korisnika bez obzira na medij, uz mogućnost filtriranja datoteka koje se štite	
29.	Dubinski pregled (skeniranje) sažetih (komprimiranih) priloga (u ZIP, RAR ili kojem drugom obliku)	
	Informiranje o ugrozama, prijetnjama i poduzetim mjerama	
30.	Vođenja dnevnika svih događaja, odaslanih upozorenja i poduzetih mjera, te izvješćivanje o tome	
31.	Vođenja dnevnika događaja, odaslanih upozorenja i poduzetih mjera i koraka o promjenama biblioteka programa, registra i drugih sistemskih datoteka i podataka te izvješćivanje o istom	

Red. broj	Obvezne tehničke značajke kojima AV sustav mora udovoljavati i mogućnosti koje mora imati	Zadovoljava DA/NE
32.	Vođenje dnevnika planiranih izvršenja i neizvršenih zadataka, upozoravanje na neizvršene zadatke i izvješćivanje o tome	
33.	Upozoravanje i/ili izvješćivanje najmanje slanjem poruke elektroničke pošte	
	Ostalo	
34.	Sučelja antivirusne programske opreme - najmanje na engleskom jeziku	
35.	Detaljne upute za rad s isporučenim softverom	

Datum i mjesto: _____

M.P. _____
potpis odgovorne osobe