**Prilog 1.** SEClarci – Opis sustava, smjernice i zahtjevi za Idejno rješenje

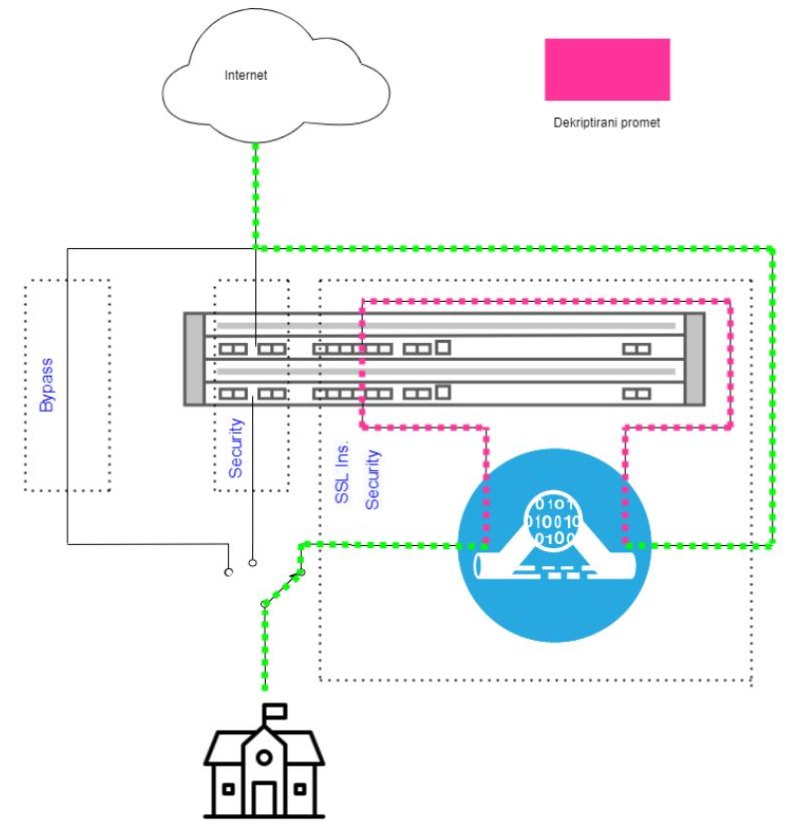
U svrhu kvalitetne realizacije projekta sigurnosna rješenja e-škole SEClarci, sustav smo podijelili u dvije glavne komponente (4 funkcionalne):

* Sigurnosni sustav za zaštitu korisnika školskih mreža
  + detekcija i prevencija malicioznog mrežnog prometa,
  + TLS/SSL dekripcija mrežnog prometa.
* Sigurnosni sustav za zaštitu elektroničke pošte
  + sigurnosna komponenta za zaštitu mail sustava,
  + filtriranje nepoželjnih (*Antispam*) poruka.

Sigurnosni sustav za zaštitu školskih mreža - opis

Sustav za zaštitu školskih mreža treba biti sačinjen od više komponenata:

* sigurnosna komponenta za detekciju i prevenciju malicioznog mrežnog prometa koji se odnosi na sve srednje i osnovne škole u RH,
* sigurnosna komponenta za TLS/SSL dekripciju mrežnog prometa,
* implementacija sustava na način da se omogući premošćivanje navedenih komponenti u slučaju bilo kakvog kvara ili potreba održavanja.



*Slika 1 - idejna shema prijedloga rješenja sustava zaštite korisnika školskih mreža*

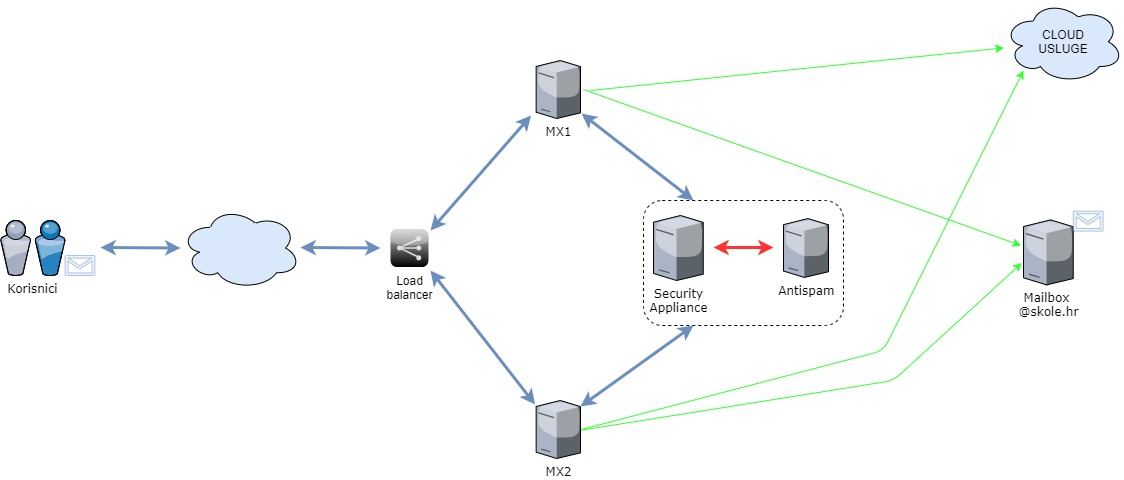
Sigurnosni sustav za zaštitu korisnika školskih mreža – funkcionalna specifikacija

* Minimalna mrežna (fizička) propusnost sustava za zaštitu školskih mreža mora biti 50 Gbps
* očekivana potrebna propusnost pojedinih komponenti sa uključenim svim dolje navedenim sustavima zaštite (eng. IPS Performance/FW Throughput ) mora biti 10 Gbps,
* idejno rješenja mora biti osmišljeno na način da omogućava skalabilnost, tj. mogućnost povećanja propusnosti prema potrebama,
* sustav mora omogućiti analizu mrežnog prometa prema Internetu i otkrivanje izvršavanja aplikacija ili funkcija povratnog poziva (eng. callback functions),
* sigurnosni sustav za zaštitu školskih mreža mora podržavati konfiguraciju visoke dostupnosti (redundancija komponenti na lokaciji) rada svih komponenti sustava u slučaju kvarova, ispada, prekida rada, …
* provjera datoteka prenesenih putem mreže putem nesigurnih, to jest nekriptiranih/nešifriranih, protokola te provjera datoteka prenesenih putem mreže SSL/TLS konekcija,
* mogućnost prepoznavanja zlonamjernih datoteka na osnovi kriptografskog sažetka, potpisa ili drugih definicija,
* mogućnost analize izvršnih datoteka uz pokretanje u izoliranom okruženju (eng. sandboxing),
* retrospektivna klasifikacija prometa i sadržaja prometa na temelju novopridošlih pravila (poglavito sandboxa),
* mogućnost provjere sadržaja unutar arhiviranih i komresiranih/komprimiranih formata,
* filtriranje DNS prometa u "inline", odnosno transparentom, načinu rada uz mogućnost biranja akcije koja će se provoditi - u smislu blokiranja, preusmjeravanja ili sinkholanja DNS upita,
* filtriranje HTTP promenta (web filtering) na osnovi domene/hostnamea, dijela URL-a ili cijelog URL-a iz HTTP zahtjeva u "inline", odnosno transparentnom, načinu rada. Mogućnost preusmjeravanja korisnika na stranicu s upozorenjem ili prikazivanje stranice s upozorenjem,
* filtriranje HTTPS prometa (web filtering) na osnovi domene na osnovi SNI (Server Name Indicatora) unutar TLS/SSL rukovanja (eng. handsake) prilikom uspostavljanja TLS/SSL veze u "inline", odnosno transparentnom, načinu rada. Mogućnost preusmjeravanja korisnika na stranicu s upozorenjem ili prikazivanje stranice s upozorenjem,
* SSL/TLS dekripcija/inspekcija prometa - terminacija SSL/TLS veza na sigurnosnom sustavu u svrhu provođenja analize nad dekriptiranim/dešifriranim prometom uz uspostavljanje nove TLS/SSL veze između sigurnosnog sustava i krajnjeg uređaja korištenjem svojih certifikata,
* mogućnost SSL/TLS dekripcije/dešifriranja bez forsiranog degradiranja SSL/TLS veze između sigurnosnog sustava i web poslužitelja,
* prepoznavanje potencijalno zlonamjernog prometa sa i prema IP adresama i adresnim prostorima s lošom reputacijom (skeniranja, pokušaji neovlaštenog pristupa, komunikacija s C2 poslužiteljima)
* dokumentirana IPS/IDS pravila uz opis prijetnje, zahvaćeni hardware/software, ozbiljnost, posljedica i pripadajuće CVE oznake,
* redovno ažurirana i aktualna baza poznatih servisa potrebu whitelistanja istih. (uz visok stupanj razlučivosti - npr. razlikovati YouTube adresni prostor od Google Cloud (user content)),
* redovno ažurirana i aktualna baza poznatih zlonamjernih domena, URL-ova, IP adresa,
* redovno ažurirana i aktualna baza potpisa zlonamjernih datoteka,
* redovno ažurirana i aktualna baza potpisa za IDS/IPS,
* rješenje treba ponuditi najnižu moguću stopu lažno pozitivnih upozorenja,
* rješenje bi trebalo imati mogućnost pohrane korisnih informacija malicioznih aktivnosti (eng. payload) i artefakte kao što je PCAPS otkrivenih prijetnji za daljnju analizu u zaštićenom okruženju,
* rješenje mora nuditi mogućnost konfiguriranja korisničkih profila i privilegija za različite uloge: (npr. Administrator, operater, revizor / gledatelj, itd.) i mogućnost konfiguriranja izvješća, upozorenja, prikazanih informacija ovisno o definiranom korisničkom profilu.
* mogućnost udaljenog logiranja (npr. syslog) uz zadržavanje lokalnih logova (dnevničkih zapisa),
* podrška za upravljanje i konfiguriranje uređaja putem REST API-a za sve gore navedeno.

Sigurnosni sustav za zaštitu elektroničke pošte – opis

Sustav za zaštitu elektroničke pošte treba biti sačinjen od više komponenata:

* sigurnosna komponenta za zaštitu mail sustava konfigurirana kao MTA (mail transfer agent).
* komponenta za filtriranje nepoželjnih (*Antispam*) poruka elektroničke pošte,



*Slika 2 - idejna shema prijedloga rješenja sustava za zaštitu elektroničke pošte*

Ukupan broj sandučića elektroničke pošte (eng. mailbox) za domenu @skole.hr trenutno je oko 435 000.

Aktivan broj mail korisnika po danu je 1000, trenutni dnevni (radno vrijeme) prosjek mail prometa (mailflow) je 10 mailova po sekundi, uz privremeno pojedinačno povećanje mail prometa do 100 mail-ova u sekundi.

Sigurnosni sustav za zaštitu elektroničke pošte – funkcionalna specifikacija

* Blokiranje poruka s malicioznim privitkom

Svaku poruku koja je usmjerena prema sigurnosnom uređaju mora proći kroz provjeru da li sadrži privitak i ako sadrži da li se radi o malicioznom privitku. Ova značajka mora reagirati brzo kako ne bi dolazilo do većeg kašnjenja poslanih poruka prema korisnicima. Poruke koje se označe kao sigurne isporučuju se prema krajnjem korisniku, a poruke za koje se ne može utvrditi radi li se o zlonamjernoj ili legitimnoj prelaze na sljedeći nivo sigurnosne provjere,

* „Sandbox“ analiza privitaka

Svaku poruku za koju se utvrdi da sadrži privitak koji je na prvoj provjeri detektiran kao "opasan" sustav mora poslati na dubinsku analizu privitka kako bi se sa stopostotnom sigurnošću utvrdili radi li se o malicioznom privitku i koji je stupanj opasnosti za korisnika. Sukladno navedenom uređaj mora imati mogućnost slanja privitka na analizu u lokalnu ili udaljenu zaštićenu okolinu tzv. Sandbox / generiranje izvještaja na temelju detektiranih malicioznih radnji,

* Blokiranje poruka s malicioznom poveznicom

Sustav mora detektirati svaku poveznicu unutar tijela poruke, te imati način provjere što se iza takve poveznice nalazi (mogućnost otvaranja poveznice u zaštićenoj okolini ili provjera na nekim od javnih servisa, npr. Virustotal),

* Karantena

Poruke koje se označe kao nedozvoljene (poruke sa malicioznim privitkom ili malicioznom poveznicom) na određeni rok koji se može izmijeniti po potrebi se pohranjuju u karantenu iz koje se mogu propustiti ili trajno obrisati u bilo kojem trenutku,

* Retroaktivno djelovanje

Ako sustav retroaktivno sazna da je propustio poruku s privitkom ili poveznicom za koju naknadno utvrdi da je maliciozna šalje upozorenje korisniku da je zaprimio malicioznu poruku, te uputu da je ukloni iz svog sandučića,

* Detekcija masovne kampanje

Kada jedna te ista poruka (ili vrlo slična poruka – npr sa 80% istog teksta) bude poslana na veliki broj adresa sustav bi trebao prepoznati da se radi o masovnoj kampanju usmjerenoj prema korisnicima te istu zaustaviti/blokirati,

* Mogućnost dodavanja primatelja/pošiljatelja na white/black liste

U svakom trenutku potrebno je pratiti ima li nekih adresa na white/black listama, te postupiti prema dobivenim informacijama i automatski ažurirati liste,

* Sustav obavještavanja korisnika i administratora

Ako je neka poruka blokirana, sustav treba obavijestiti korisnika o toj poruci, ova značajka se treba moći prilagoditi i po potrebi deaktivirati

* svaki mail Spam dolazi do korisnika s oznakom da korisnik sam može raspolagati i razvrstati poruku (npr. u SPAM folder )
* malicioznu mail poruku se NE smije propuštati do korisnika, nego ga samo obavijestiti.
* Blokiranje neželjeno pošte – antispam

Sustav mora imati razvijen način detekcije spam/neželjenih poruka, te mogućnost povezivanja tj. implementacija vanjskih blacklisti,

* mogućnost udaljenog logiranja (npr. syslog) uz zadržavanje lokalnih logova (dnevničkih zapisa),
* rješenje treba ponuditi najnižu moguću stopu lažno pozitivnih upozorenja,
* rješenje mora nuditi mogućnost konfiguriranja korisničkih profila i privilegija za različite uloge: (npr. Administrator, operater, revizor / gledatelj, itd.) i mogućnost konfiguriranja izvješća, upozorenja, prikazanih informacija ovisno o definiranom korisničkom profilu.
* sigurnosni sustav za zaštitu elektroničke pošte mora podržavati konfiguraciju visoke dostupnosti (redundancija komponenti na lokaciji) rada svih komponenti sustava u slučaju kvarova, ispada, prekida rada, …