# IZJAVA O SIGURNOSTI MREŽE

Kaspersky Endpoint Security 11 za Izjavu o Windows Kaspersky sigurnosti mreže (u daljem tekstu "Izjava o SM") odnosi se na računarski program Kaspersky Endpoint Security (u daljem tekstu "Softver"). Kaspersky-eva Izjava o SM zajedno sa Licencnim ugovorom o softveru sa krajnjim korisnikom, naročito Dio "Uslovi obrade podataka", definiše uslove, odgovornosti i procedure prenosa i obrade podataka, što je naznačeno u Izjavi o SM. Pažljivo pročitajte uslove Izjave o SM, kao i sve dokumente iz iste, prije nego što je prihvatite. Kada krajnji korisnik aktivira upotrebu SM-a, u potpunosti je odgovoran da obezbijedi da obrada ličnih podataka nosilaca podataka bude zakonita, naročito u okviru značenja Člana 6 (1) (a) do (1) (f) Propisa (EU) 2016/679 (Propis o zaštiti opštih podataka, "GDPR"), ako je nosilac podataka u Evropskoj Uniji, ili važećih zakona o povjerljivim informacijama, ličnim podacima, zaštiti podataka ili slično. Zaštita podataka i obrada podataka koje vlasnik prava dobije od krajnjeg korisnika tokom upotrebe SM-a tretiraju se u skladu sa politikom privatnosti vlasnika prava koja je objavljena na stranici www.kaspersky.com/Products-and-Services-Privacy-Policy.

Svrha upotrebe Kaspersky SM-a

Upotreba Kaspersky SM-a može dovesti do veće efikasnosti softverske zaštite od prijetnji po sigurnost informacija i mreže. Ta svrha se postiže putem slijedećih aktivnosti:

- definisanje reputacije skeniranih objekata,
- identifikacija prijetnji po sigurnost informacija koje su nove i teške za otkrivanje i njihovi izvori,
- preduzimanje hitnih mjera radi povećanja zaštite podataka koje krajnji korisnik čuva i obrađuje putem računara,
- smanjenje mogućnosti za lažnu pozitivnost,
- povećanje efikasnosti softverskih komponenti,
- sprječavanje incidenata po pitanju sigurnosti informacija i istraživanje incidenata koji su se dogodili,
- unapređenje izvedbe proizvoda vlasnika prava,
- prijem referentnih informacija o broju objekata koji imaju poznatu reputaciju.

Vlasnik prava će dobijati obrađene podatke tokom upotrebe SM-a i obrađivati slijedeće podatke:

- informacije o fajlovima i URL adresama koje će se skenirati: provjera skeniranih fajlova (MD5, SHA2-256, SHA1) i uzoraka (MD5), veličina uzorka, vrsta otkrivene prijetnje i njen naziv po klasifikaciji vlasnika prava, identifikator za anti-virusne baze podataka, URL adresa za koju je tražena reputacija, kao i URL adresa upučivaća, identifikator protokola priključka i broj korištenog porta,

- informacija o rezultatima kategorizacije traženih web resursa koji sadrže obrađenu URL i IP adresu hosta, verziji softverske komponente koja je izvršila kategorizaciju, načinu kategorizacije i setu kategorija koje su definisane za web resurs,

- identifikator zadatka skeniranja koji je otkrio prijetnju,

- informacija o digitalnim sertifikatima koji su korišteni i potrebni za provjeru njihove autentičnosti: provjere (SHA2-256) sertifikata za potpisivanje skeniranog objekta i javnog ključa sertifikata,

- informacija o softveru koji je instaliran na računaru: ime softverskih aplikacija i prodavača softvera, ključevi registra i njihove vrijednosti, informacija o fajlovima instaliranog softverskih komponenti (provjere (MD5, SHA2-256, SHA1), naziv, put do fajla na računaru, veličina, verzija i digitalni potpis), informacija o jezgrenim objektima, drajverima, uslugama, prišireni Microsoft Internet Explorer-a, proširenje sistema štampanja, proširenje Windows Explorer-a, elementi aktivnog podešavanja, apleti na kontrolnoj tabli, unosi u hostane fajlove i sistemski registar, verzije pretraživača i mail klijenata,

- informacija o stanju anti-virusne zaštite računara: verzije i vremenske oznake verzije korištenih anti-virusnih baza podataka, statistika o ažuriranjima i priključcima sa uslugama vlasnika prava, identifikator posla i identifikator softverske komponente koja vrši skeniranje,

- informacija o fajlovima koje je krajnji korisnik preuzeo: URL i IP adrese preuzimanja i stranice koje su preuzete, identifikator protokola za preuzimanje i broj porta priključka, status URL-ova da li su zlonamjerni ili ne, atributi fajla, veličina i provjere (MD5, SHA2-256, SHA1), informacija o procesu preuzimanja fajla (provjere (MD5, SHA2-256, SHA1), datum i vrijeme kreiranja/ ugradnje, status auto-play, atributi, nazivi pakera, informacija o potpisima, moguća oznaka fajla, identifikator formata i entropija), naziv fajla i njegov put na računaru, digitalni potpis fajla i vremenska oznaka njegove generacije, URL adresa na kojoj je došlo do detekcije, broj skripte na stranici koja izgleda sumnjiva ili štetna, informacija o generisanim HTTP zahtjevima i odgovoru na njih,

- informacija o tekućim aplikacijama i njihovim modulima: podaci o procesu koji teče na sistemu (ID procesa (PID), naziv procesa, informacija o računu sa kojeg je proces pokrenut, aplikacija i komanda koja je inicirala proces, potpis pouzdanog programa ili procesa, kompletan put do fajlova procesa, i početna komandna linija, nivo integriteta procesa, opis proizvoda kojem proces pripada (naziv proizvoda i informacija o izdavaču), kao i korišteni digitalni sertifikati i informacija za provjeru njihove autentičnosti ili informacija o nepostajnju fajlovog digitalnog potpisa), i informacija o modulima na procesima (njihovi nazivi, veličine, vrste, datumi kreiranja, atributi, provjere (MD5, SHA2-256, SHA1), putevi do njih na računaru, PE fajl informacije u zaglavlju, nazivi pakera (ako je fajl zapakovan),

- informacija o svim potencijalno zlonamjernim objektima i aktivnostima: naziv detektovanog objekta i njegov kompletan put do računara, provjere (MD5, SHA2-256, SHA1) obrađenih fajlova, datum i vrijeme detekcije, nazivi i veličina inficiranih fajlova i puteva do njih, šira obrasca puta, oznaka koja pokazuje da li je objekat kontejner, nazivi pakera (ako je fajl zapakovan), šifra vrste fajla, identifikator formata fajla, lista aktivnosti zlonamjernih aplikacija i srodnih odluka od strane softvera i krajnjeg korisnika, identifikatori anti-virusnih baza podataka koje je softver koristio za odlučivanje, naziv detektovane prijetnje po klasifikaciji vlasnika prava, nivo opasnosti, status i metoda detekcije, razlog za stavljanje fajla u analizirani kontekst i serijski broj fajla u tom kontekstu, provjere (MD5, SHA2-256, SHA1), naziv i atributi ostvarivog fajla za aplikaciju koja je prošla inficiranu poruku ili link, anonimizirana IP adresa (IPv4 i IPv6) hosta blokiranog objekta, entropija fajla, status auto-play, vrijeme prve detekcije fajla u sistemu, broj vođenja fajla od zadnje dostave statistike, informacija o nazivu, provjere (MD5, SHA2-256, SHA1) i veličina mail klijenta koji je korišten za prijem zlonamjernog objekta, identifikator zadatka softvera koji je izvršio skeniranje, oznaka za provjeru reputacije ili potpisa fajla, rezultat obrade fajla, provjera (MD5) uzorka koji je prikupljen na objektu i veličina uzorka u bajtima, tehnički parametri važećih tehnologija detekcije,

- informacija o skeniranim objektima: dodijeljena pouzdana grupa kojoj i/ili od koje je fajl postavljen, razlog zbog kojeg je fajl stavljen u tu kategoriju, identifikator kategorije, informacija o izvoru kategorija i verziji baze podataka kategorije, oznaka pouzdanog sertifikata fajla, naziv prodavca fajla, verzija fajla, naziv i verzija softverske aplikacije koja uključuje fajl,

- informacija o otkrivenim ranjivostima: ranjivost ID-a u bazi podataka o ranjivosti, klasa opasnosti po ranjivost i status detekcije,

- informacija o emulaciji ostvarivog fajla: veličina fajla i njegove provjere (MD5, SHA2-256, SHA1), verzija komponente emulacije, dubina emulacije, niz osobina logičkih blokova i funkcija u logičkim blokovima koji su rezultat emulacije, podaci iz PE zaglavlja ostvarivog fajla,

- informacija o mrežnim napadima: IP adrese napadačkog računara (IPv4 i IPv6), broj računarskog porta na koji je usmjeren mrežni napad, identifikator protokola IP paketa koji sadrži napad, cilj napada (naziv organizacije, web stranica), oznaka reakcije na napad, težina napada, nivo pouzdanosti,

- informacija o napadima u vezi sa lažnim mrežnim resursima, DNS i IP adrese (IPv4 i IPv6) posjećenih web stranica,

- DNS i IP adrese (IPv4 i IPv6) traženog web resursa, informacija o fajlu i web klijentu koji traži web resurs, naziv, veličina, provjere (MD5, SHA2-256, SHA1) fajla, njegov kompletan put i šifra obrasca puta, rezultat provjere digitalnog potpisa i njegov status u skladu sa SM-om,

- informacija o vraćanju aktivnosti malvera: podaci o fajlu čije aktivnosti su vraćene (naziv fajla, kompletan put do fajla, njegova veličina i provjere (MD5, SHA2-256, SHA1)), podaci o uspješnim i neuspješnim aktivnostima brisanja, preimenovanja i kopiranja fajlova i ponovnog uspostavljanja vrijednosti u registru (nazivi ključeva registra i njihove vrijednosti), informacija o sistemskim fajlovima koje je malver promijenio, prije i poslije vraćanja,

- informacija o modulima koje je softver učitao: naziv, veličina i provjere (MD5, SHA2-256, SHA1) fajla modula, njegov kompletan put i šifra obrasca puta fajla, parametri digitalnog potpisa modula fajla, vremenska oznaka generisanja potpisa, nazivi subjekta i organizacije koja je potpisala modul fajl, identifikator procesa, u kojem je modul učitan, naziv prodavca modula, indeks broj modula u redu učitavanja,

- servisna informacija o radu softvera: verzija kompajlera, oznaka za potencijalnu zlonamjernost skeniranog objekta, verzija seta statistike koja je dostavljena, informacija o raspoloživosti i važnosti te statistike, identifikator moda za generisanje statistike koja je dostavljena, oznaka koja pokazuje da li softver radi u interaktivnom modu,

- ukoliko se detektuje potencijalno zlonamjeran objekat, daje se informacija o podacima u procesnoj memoriji: elementi u hijerarhiji sistema objekta (ObjectManager), podaci u memoriji UEFI BIOS, nazivi ključeva registra i njihove vrijednosti,

- informacije o događajima u logovima sistema: vremenska oznaka događaja, naziv loga u kojem je događaj pronađen, vrsta i kategorija događaja, naziv izvora događaja i opis događaja,

- informacija o mrežnim priključcima: verzija i provjere (MD5, SHA2-256, SHA1) fajla sa kojeg je započeo proces koji je otvorio port, put do fajla procesa i njegov digitalni potpis, lokalne i udaljene IP adrese, brojevi lokalnih i udaljenih priključnih portova, stanje priključka, vremenska oznaka otvaranja porta,

- informacija o datumu instalacije i aktiviranju računarskog softvera: vrsta instalirane licence i datum njenog isteka, identifikator partnera od kojeg je licenca kupljena, serijski broj licence, vrsta softverske instalacije na računaru (početna instalacija, ažuriranje, itd.) i oznaka uspješne instalacije ili broj pogrešne instalacije, jedinstveni identifikator za instalaciju računarskog softvera, vrsta i identifikator aplikacije koja je ažurirana, identifikator zadatka ažuriranja,

- informacija o setu svih instaliranih ažuriranja i set najnovijih instaliranih/uklonjenih ažuriranja, vrsta događaja koji je prouzrokovao slanje informacije o ažuriranju, trajanje od instalacije zadnjeg ažuriranja, informacija o svim trenutno instaliranim anti-virusnim bazama podataka,

- informacija o radu softvera na računaru: podaci o upotrebi CPU-a, podaci o upotrebi memorije (Private Bytes, Non-Paged Pool), broj softverskih aktivnih sesija i sesija u stanju čekanja, trajanje softverske operacije prije nastanka greške,

- broj softverskih ispisa logova i sistemskih ispisa logova (BSOD) od instalacije softvera i zadnjeg ažuriranja, identifikator i verzija softverskog modula koji je pao, memorija u softverskom procesu, i informacija o anti-virusnoj bazi podataka u vrijeme pada,

- podaci o sistemskom ispisu logova (BSOD): oznaka da je došlo do BSOD-a na računaru, naziv drajvera koji je prouzrokovao BSOD, adresa i memorija u drajveru, oznaka trajanja OS sesije prije BSOD-a, memorija drajvera koji je pao, vrsta pohranjenog memorijskog ispisa logova, oznaka OS sesije prije nego što je BSOD trajao duže od 10 minuta, jedinstveni identifikator ispisa logova, vremenska oznaka BSOD-a,

- informacija o greškama za vrijeme rada softverskih komponenti: status softverskog ID-a, vrsta greške, šifra i vrijeme dešavanja, ID-ovi komponente, modul i proces proizvoda na kojem je došlo do greške, ID zadatka ili kategorija ažuriranja tokom kojeg je došlo do greške, logovi drajvera koje je softver koristio (pogrešna šifra, naziv modula, naziv izvornog fajla i linija na kojoj je došlo do greške), identifikator metode za identifikaciju greške u radu softvera, naziv procesa koji je inicirao presretanje ili razmjenu saobraćaja što je dovelo do greške u radu softvera,

- informacija o ažuriranju anti-virusnih baza podataka i softverskih komponenti: naziv, datum i vrijeme indeksnih fajlova koji su preuzeti tokom zadnjeg ažuriranja i tokom trenutnog ažuriranja, kao i datum i vrijeme završetka zadnjeg ažuriranja, nazivi fajlova ažuriranih kategorija i njihove provjere (MD5, SHA2-256, SHA1),

- informacija o neuobičajenom prekidu rada softvera: kreiranje vremenske oznake ispisa logova, njegova vrsta, naziv procesa u vezi sa ispisom logova, verzija i vrijeme dostave statističkog ispisa logova, vrsta događaja koji je prouzrokovao neuobičajen prekid softverskog rada (neočekivano gašenje, pad aplikacije treće strane, greške u obradi presretanja), datum i vrijeme neočekivanog gašenja,

- informacija o aplikacijama treće strane koje su dovele do greške: njihov naziv, verzija i lokalizacija, pogrešna šifra informacija o grešci sa sistemskog loga aplikacija, adresa greške i memorija aplikacije treće strane, oznaka o pojavi greške u softverskoj komponenti, period u kojem je aplikacija treće strane bila u funkciji prije pojave greške, provjere (MD5, SHA2-256, SHA1) slike aplikativnog procesa u kojem je došlo do greške, put do slike aplikativnog procesa i šifra puta, informacija sa sistemskog loga s opisom greške na aplikaciji, informacija o modulu aplikacije gdje je došlo do greške (identifikator izuzetka, adresa pale memorije kao offset u aplikativnom modulu, naziv i verzija modula, identifikator pada aplikacije memorije pada kod vlasnika prava, trajanje sesije aplikacije prije pada),

- verzija softverske updater komponente, broj padova updater komponente tokom zadataka ažuriranja u životnom ciklusu komponente, ID vrste ažuriranja, broj propalih pokušaja updater komponente da završi zadatke ažuriranja,

- informacija o radu komponenti za nadzor softverskog sistema: kompletne verzije komponenti, šifra događaja koji je prekrio niz događaja i broj tih događaja, ukupni broj događaja prekrivanja niza, informacija o fajlu procesa iniciranja događaja (naziv fajla i njegov put na računaru, obrazac šifre puta fajla, provjere (MD5, SHA2-256, SHA1) procesa u vezi sa fajlom, verzija fajla), identifikator presretanja događaja do kojeg je došlo, potpuna verzija filtera presretanja, identifikator vrste presretnutog događaja, veličina niza događaja i broj događaja između prvog događaja u nizu i trenutnog događaja, broj zakašnjelih događaja u nizu, informacija o fajlu procesa iniciranja trenutnog događaja (naziv fajla i njegov put na računaru, obrazac šifre puta fajla, provjere (MD5, SHA2-256, SHA1) procesa u vezi sa fajlom), trajanje obrade događaja, maksimalno trajanje obrade događaja, mogućnost za slanje statistike,

- informacija o zadnjem neuspješnom ponovnom startovanju OS-a: broj neuspješnih restarta od instalacije OS-a, podaci o sistemskom ispisu logova (šifra i parametri greške, naziv, verzija i provjere (CRC32) modula koji je prouzrokovao grešku u radu OS-a, pogrešna adresa kao offset u modulu, provjere (MD5, SHA2-256, SHA1) sistemskog ispisa logova),

- informacija o provjeri autentičnosti digitalnih sertifikata koji se koriste za potpisivanje fajlova: otisak sertifikata, algoritam provjere, javni ključ i serijski broj sertifikata, naziv izdavača sertifikata, rezultat provjere sertifikata i identifikator baze podataka sertifikata,

- informacija o procesu koji napada softverovu samo-odbranu: naziv i veličina procesnog fajla, njegove provjere (MD5, SHA2-256, SHA1), cijeli put do procesnog fajla i obrazac šifre puta fajla, vremenske oznake za kreiranje/izgradnju, oznaka ostvarivog fajla, atributi procesnog fajla, informacija o sertifikatu za potpisivanje procesnog fajla, šifra računa za puštanje procesa u rad, ID operacija za pristup procesu, vrsta resursa s kojim je operacija izvršena (proces, fajl, objekat registra, funkcija za pretraživanje FindWindow), naziv resursa s kojim je operacija izvršena, oznaka za uspjeh operacije, status fajla procesa i njegov potpis u skladu sa SM-om,

- informacija o softveru vlasnika prava: njegova kompletna verzija, vrsta, jezik i operativno stanje, verzija instaliranih softverskih komponenti i njihovo operativno stanje, informacija o instaliranim ažuriranjima, vrijednost CILJANOG filtera, verzija protokola za povezivanje sa uslugama vlasnika prava,

- informacija o verzijama operativnog sistema i instaliranih ažuriranja, veličina riječi, izdanje i parametri OS run moda, verzija i provjere (MD5, SHA2-256, SHA1) jezgrenog fajla. Isto tako, da bi se postigla svrha povećanja efikasnosti zaštite koju pruža softver, vlasnik prava može dobijati objekte koje mogu koristiti uljezi da oštete računar i kreiraju prijetnje po sigurnost informacija. Ti objekti obuhvataju kako slijedi:

  - izvršne i neizvršne fajlove ili njihove dijelove,
  - dijelove računarskog RAM-a,
  - sektore koji su uključeni u proces pokretanja OS-a,
  - pakete podataka o mrežnom saobraćaju,
  - web stranice i e-mailove sa sumnjivim i zlonamjernim objektima,
  - opis klasa i instanci klasa WMI repozitorija,
  - izvještaji o aktivnostima aplikacije. Ti izvještaji sadrže slijedeće podatke o fajlovima i procesima:
  - naziv, veličina i verzija fajla koji je poslan, njegov opis i provjere (MD5, SHA2-256, SHA1), identifikator formata fajla, naziv prodavca fajla, naziv proizvoda kojem fajl pripada, kompletan put na računaru, obrazac šifre puta fajla, vremenske oznake kreiranja i modifikacije fajla,
  - početni i krajnji datum/vrijeme perioda važnosti sertifikata (ukoliko fajl ima digitalni potpis), datum i vrijeme potpisa, naziv izdavača sertifikata, informacija o vlasniku sertifikata, otisak, javni ključ i odgovarajući algoritmi sertifikata, i serijski broj sertifikata,
  - naziv računa s kojeg se vodi proces,
  - provjere (MD5, SHA2-256, SHA1) naziva računara na kojem teče proces,
  - naslovi prozora procesa,
  - identifikator anti-virusnih baza podataka, naziv otkrivene prijetnje po klasifikaciji vlasnika prava,
  - podaci o instaliranoj licenci, njen identifikator, vrsta i datum isteka,
  - lokalno vrijeme računara u momentu davanja informacije,
  - nazivi i putevi fajlova kojim je proces pristupio,
  - nazivi ključeva registra i njihove vrijednosti kojim je proces pristupio,
  - URL i IP adrese kojim je proces pristupio,
  - URL i IP adrese s kojih je trenutni fajl preuzet.

Isto tako, da bi se ostvarila svrha po pitanju sprječavanja lažne pozitivnosti, vlasnik prava može dobiti pouzdane izvršne i neizvršne fajlove ili njihove dijelove. Davanje gore navedene informacije za SM je dobrovoljno. Nakon instalacije softvera, krajnji korisnik uvijek može omogućiti ili onemogućiti upotrebu SM-a u postavkama softvera koje su opisane u Uputstvu o upotrebi.