„SIGURNOST WINDOWS VISTA OPERACIJSKOG SUSTAVA“

Windows Vista predstavlja najsigurniji od svih operacijskih sustava iz Windows obitelji. Predavanje obrađuje glavne sigurnosne funkcionalnosti Windows Vista operacijskog sustava pri čemu su funkcionalnosti obrađene kroz pet glavnih grupa. Sigurnost je tako analizirana na razini jezgre, na razini mreže, na razini korisnika, kroz enkripciju te kroz dodatne sigurnosne elemente koje Vista pruža.

Na razini jezgre opisane su osnove sigurnog razvoja koji je Microsoft uveo kako bi osigurao sigurnost razvijanog programskog koda. Microsoft je uz to redizajnirao kompletnu arhitekturu Vista operacijskog sustava u odnosu na prethodne verzije Windows sustava. Jedan dio sigurnosti na razini jezgre sustava su i ASLR (eng. *Address Space Layout Randomization*) te DEP (eng. *Data Execution Prevention*) mehanizmi, a postoji i mehanizam za provjeru integriteta učitanih programskih kodova.

Na razini mreži ugrađeni su novi sigurnosni elementi od kojih je potrebno izdvojiti Windows Defender, Windows Firewall s naprednijim mogućnostima korištenja u odnosu na prethodne verzije te NAP (eng. *Network Access Protection*). Windows Defender dolazi integriran u Vista operacijski sustav, a moguće ga je instalirati i na druge Windows operacijske sustave. Njegova namjena je detektiranje, čišćenje i blokiranje nepoželjnih aplikacija u stvarnom vremenu, a zasnovan je na MSRT-u (*Malicious Software Removal Tool*). Novi Windows Firewall predstavlja unaprjeđenje starog vatrozida prisutnog na XP sustavima kod kojeg je sad moguće kontrolirati dolazni i odlazni promet, primjenjivati različite sigurnosne politike za različite mreže i slično. NAP predstavlja novu tehnologiju za kontrolu pristupa računalnoj mreži kojoj je cilj zaštita mreža i pojedinih računala. Njena osnovna politika je da se nezaštićenim korisnicima ne dozvoljava pristup računalnoj mreži kako bi se i mreža zaštitila od korisnika, ali i sami korisnici od mogućih prijetnji protiv kojih nemaju zaštitu.

Na razini korisnika uvedena je naprednija kontrola korisničkih računa pod nazivom UAC (eng. *User Account Control*) koja razdvaja standardne privilegije i zadatke od onih koje traže administratorske ovlasti. Po tom principu su na sustavu omogućene tri razine pristupa: visoka, srednja i niska. Radi povećanja sigurnosti i fleksibilnosti uveden je i novi sustav za prijavu korisnika (*WinLogon*) koji omogućava višestruke oblike autentikacije. Korisnička sigurnost dodatno je podignuta i kroz novi mehanizam za sigurno kreiranje i obnavljanje kopija (eng. *Backup and Restore*) koji korisnicima znatno olakšava planiranje izrade sigurnosnih kopija. Korisnicima Windows Vista operacijskog sustav omogućeno je i verzioniranje željenih datoteka pri čemu se čuvaju promjene između pojedinih verzija.

Na razini enkripcije uveden je novi sustav zaštite pod nazivom BitLocker Drive Encryption. Njime je omogućena enkripcija sistemskih particija diska pri čemu je glavni cilj zaštiti podatke u slučaju krađe računala (najčešće prijenosnog). Zaštita je time podignuta na veoma visoku razinu jer u slučaju deset neovlaštenih uzastopnih pokušaja pristupa, ključ za dekripciju se uništava. Sigurnost kroz enkripciju ne postoji samo na

razini zaštite cijelog diska već i na razini zaštite pojedinih datoteka i direktorija. To je ostvareno kroz već od prije poznatu EFS (eng. *Encryption File System*) funkcionalnost. Na Vista operacijskom sustavu primjenjuje se novi set kriptografskih algoritama koji koriste sigurne ključeve.

Od ostalih sigurnosnih elemenata Windows Vista operacijskog sustava važno je spomenuti i SRP (eng. *Software Restriction Policies*) mehanizam za zabranu pokretanja pojedinih programa i datoteka. Također, Vista sustav omogućava i kontrolu instalacije i korištenja pojedinih uređaja ovisno o korisnicima (eng. *Device Control*). Vrlo važan sigurnosni mehanizam je i RMS (eng. *Rights Management Services*) koji zaštićuje dokumente od ovlaštenih korisnika, tj. nisu svim korisnicima dodijeljene iste ovlasti za upravljanje dokumentima pa je time onemogućeno da npr. jedan korisnik čita dokument koji nije njemu namijenjen. Za Vista sustave raspoloživa je i opcionalna komercijalna usluga Windows Live OneCare koja je dostupna za testiranje tijekom razdoblja od 90 dana. Ona objedinjuje i organizira više različitih prethodno opisanih sustava zaštite, a značajno je da uključuje i antivirusnu podršku. Tijekom razdoblja od čak 120 dana moguće je testirati i Forefront Client Security, komercijalnu uslugu zaštite od svih neželjenih programa. Poseban dio Windows Vista operacijskog sustava je i Internet Explorer verzija 7 koja sadrži filtar za zaštitu od krađe identiteta (eng. *phishing filter*), a uz to radi u zaštićenom modu rada na Vista sustavima.