

Ochrana pred nebezpečným kódom

V súčasnosti narastá tlak na ochranu sofistikovaných sieťových prostredí a množiacich sa vzdialených používateľských počítačov a sieťových klientov, proti stále zložitejším hrozbám. Vzhľadom na skutočnosť, že sa cenné kritické aktíva nachádzajú na klientskych systémoch (vrátane vzdialených počítačov), rozptýlených po celej organizácii, je potrebné v súlade s bezpečnostnými štandardmi zabezpečiť kontrolu všetkých vstupných bodov do infraštruktúry na prítomnosť nebezpečného kódu, vírusov a neautorizovaných aktivít. Každý takýto bod je potrebné vybaviť vhodným bezpečnostným mechanizmom, ktorý bude vykonávať pravidelné prehliadky systému.

Základnou funkciou antivírových systémov je zamedzenie infikovania súborových systémov a operačnej pamäte sieťových serverov a klientskych staníc škodlivým kódom. Antivírový systém kontroluje všetky súborové aktivity a v prípade známej podozrivej činnosti vykoná jej zablokovanie, alebo inú naplánovanú reakciu. Pri neznámých hrozbách vyhodnocuje podozrivé aktivity na základe heuristických analýz.

Systém musí mať vlastnosti centrálne riadeného riešenia, ktoré má zároveň centrálne vyhodnocovať všetky bezpečnostné udalosti prebiehajúce na klientskych staniciach a sieťových serveroch.

Medzi hlavné riziká dnes patria útoky nebezpečného kódu za pomoci e-mailovej komunikácie. Preto je potrebné zamedziť doručeniu e-mailu s nebezpečným obsahom ešte pred vstupom do firemnej infraštruktúry. Na to sú vhodné systémy, pomocou ktorých sa v organizácii zabezpečuje ochrana elektronickej pošty pred nevyžiadanou poštou a bezpečnostnými rizikami.

V tejto oblasti Vám ponúkame:

- Implementáciu komplexných riešení na ochranu pracovných staníc a serverov pred zavedením nebezpečného kódu
- Komplexné riešenie na ochranu vstupných a výstupných brán do a z internetu
- Zavedenie firemnej antivírovej ochrany
- Implementáciu prevenčných systémov (IPS)
- Systémy na kontrolu obsahu a redukciu nevyžiadanej pošty (antispam)
- Implementáciu riešenia na identifikáciu adware a spyware

Používané technológie:

- Symantec BrightMail Gateway
- Symantec Endpoint Protection

Využitie:

- Ochrana organizácie pred infiltráciou neželaným kódom
- Zníženie rizika nefunkčnosti systémov z dôvodu infiltrácie neželaným kódom
- Výrazná redukcia nevyžiadanej pošty