Zaščitite podatke v poslovnem omrežju in oblaku

Sophos Encryption varuje podatke

..Delovno okolje že kar nekaj časa ni več statično, tako da pri svojem delu za shranjevanje podatkov uporabljamo vire tako v lokalnem poslovnem omrežju kot tudi na gostujočih strežnikih v oblaku..

Dinamično delovno okolje zahteva drugačen pristop k varovanju poslovnih podatkov, ne glede na to, kje se podatki shranjujejo. Sama lokacija hranjenja niti ni pomembna, pomemben pa je način, kako so ti podatki shranjeni. Sophosove rešitve omogočajo ustrezno zaščito podatkov. Na ta način so podatki na voljo le tistim uporabnikom, katerim so namenjeni pri njihovem delu.

Ponudniki shranjevanja podatkov v oblaku (Dropbox, Google Drive, Microsoft OneDrive) omogočajo različna orodja za dostop do podatkov iz različnih naprav. Na ta način je zagotovljena visoka stopnja produktivnosti in medsebojne izmenjave podatkov, vendar pa obstaja kar nekaj varnostnih pomislekov. Prvi primer je nenamerna izguba podatkov. Uporabnik lahko povezavo do dokumenta, ki je shranjen v oblaku, posreduje napačni osebi. Drugi primer je kraja podatkov, kjer uporabnik ni zaščitil dostopa do dokumentov v oblaku z ustreznim geslom. Potem so tu še ranljivosti sistema ponudnika oblačnih storitev ali tehnične težave v določenem trenutku. Poznamo primere, ko je bil dostop do podatkov v oblaku na voljo z naključnim geslom. Na koncu so seveda problematične še navade uporabnikov, da odlagajo dokumente v oblaku, namesto prek varne povezave VPN na strežnike podjetja. Vse omenjene probleme lahko odpravimo z uporabo rešitve Sophos SafeGuard Encryption for Cloud Storage, ki omogoča enostavno kriptiranje dokumentov, preden se shranijo v oblaku. Na voljo je tako za računalnike kot tudi mobilne naprave. Kriptiranje je samodejno, tako da uporabniku ni treba izvajati dodatnih akcij pri shranjevanju dokumentov. Upravljanje s certifikati ali gesli za kriptiranje in dostop do dokumentov sta mogoča s centralno konzolo SafeGuard Management Center.

Podatki, ki se shranjujejo v podjetju, so načeloma varni pred nepooblaščenim dostopom. Problem je, da do podatkov lahko dostopajo tudi skrbniki poslovnega sistema. To so lahko interni zaposleni ali zunanji izvajalci. Tukaj na pomoč priskoči SafeGuard Encryption for File Shares. Uporabniku omogoča nezaznavno kriptiranje podatkov, ki se shranjujejo lokalno ali na podatkovnih strežnikih. Dostop do dokumentov lahko določajo uporabniki sami z lokalnimi ključi za kriptiranje ali pa so ključi nastavljeni s strani skrbnika SafeGuard Management Centra. Možna je tudi uporaba tako imenovane »four-eye« avtentikacije, kjer je za vsako dodelitev ključev potrebna potrditev vsaj dveh skrbnikov.

Na koncu imamo na voljo še klasično zaščito prenosnih naprav, kjer nam Sophos SafeGuard Device Encryption omogoča kriptiranje diskov na prenosnikih. V primeru odtujitve prenosnika ali diska so podatki zaščiteni in nedostopni za pregledovanje. Na voljo pa je tudi modul SafeGuard DataExchange, kjer ustrezno zaščitimo tudi podatke na prenosnih medijih za hranjenje podatkov, kot so ključki USB, mediji CD/DVD, spominske kartice. Tudi za obe omenjeni rešitvi je mogoče centralno upravljanje s SafeGuard Management Centrom.

Pri varovanju podatkov se moramo zavedati, da določene vrste podatkov (na primer osebni podatki) zahtevajo ustrezno zaščito že na podlagi zakonodaje, ki je trenutno veljavna v Sloveniji, in tudi prihajajočih zakonov na nivoju Evropske unije. (P. R.)

SOPHOS

SOPHOS d.o.o.
Germova ulica 9, 8000 Novo mesto
Tel.: (07) 393 5 600, Faks: (07) 393 5 610
e-pošta: slovenija@sophos.si
spletni naslov: www.sophos.si

SafeGuard Encryption for Cloud Storage in action