Oprava chybných oprávnění ve Windows

Chybná oprávnění

Pokud jste správci systému Windows nebo se ve své organizaci nějakým způsobem podílíte na zabezpečení Windows či správě oprávnění, vsadím se, že jste se už někdy setkali s chybnými oprávněními ve Windows. „Chybné“ může samozřejmě znamenat celou řadu věcí, protože v systému NTFS existuje mnoho způsobů, proč a jak mohou být oprávnění chybná nebo poškozená.

Oprávnění mohou být chybná i v případě, že jsou technicky vzato v pořádku. Z hlediska autentizace sice fungují, jak mají, přesto ale nezajišťují správnou autorizaci. Pokud například máte složku přístupnou pro skupinu Everyone, jsou oprávnění této složky pravděpodobně považována za chybná. Nesprávnou autorizací se na tomto místě ale zabývat nechci. Raději přejděme k situacím, kdy jsou oprávnění složky ve Windows technicky chybná, tedy kdy správně nefunguje „dědičnost“ v NTFS.

Dědičnost

Složka ve Windows se obecně může z hlediska dědičnosti nacházet ve třech stavech: první z nich znamená, že jednoduše dědí všechna oprávnění nadřazené složky, takže má shodný seznam ACL jako nadřazená složka. Ve druhém stavu složka dědí všechny položky od nadřazené složky, má však i další oprávnění. Varonis takové složky označuje jako „jedinečné“. V obou těchto případech se změny oprávnění nadřazené složky* promítnou i na složku podřízenou. Ve třetím stavu se složka nachází, pokud je dědičnost poškozená nebo vypnutá. Společnost Microsoft (a Varonis také) takovým složkám říká „chráněné“. Tyto chráněné složky nedědí oprávnění od svých nadřazených složek a změny provedené v oprávněních nadřazené složky se nepromítají do jejich seznamu ACL. Obvyklé administrační nástroje Windows příliš dobře neukazují, které složky mají vypnutou dědičnost nebo pro ně byla nastavena vlastní oprávnění. To je jeden z hlavních důvodů, proč organizace často ani nevědí, že k některým údajům má přístup příliš mnoho lidí.

Situaci ještě více komplikuje skutečnost, že v některých případech může dojít k poškození dědičnosti. Podřízená složka v takovém případě buď správně nezdědila oprávnění, která zdědit měla (takže nějaká položka řízení přístupu (ACE) v jejím seznamu ACL chybí), nebo zdědila oprávnění, která její nadřazená složka nemá (a tedy má ve svém seznamu ACL nějakou položku ACE navíc). Každopádně tím vzniká zmatek. Buď si lidé z IT oddělení myslí, že přístup ke složkám je jen omezený, a on není, nebo jsou naopak přesvědčeni, že přístupné jsou, ale uživatelé se k nim nemohou dostat. Když takový zmatek nastane, je k nalezení a opravě příčiny nutno analyzovat všechny seznamy ACL v dotčené hierarchické větvi.

K poškození seznamů ACL může dojít z několika důvodů. Je známo, že používání některých automatických kopírovacích programů má neočekávané následky. Problémy tohoto druhu mohou způsobit i skripty vlastní výroby. Nekonzistence mohou vzniknout i tehdy, když někdo jednoduše přesune soubor nebo složku z jedné složky na určitém svazku do jiné, která je sice na stejném svazku, ale má jiná oprávnění. Při přesunu souboru nebo složky v rámci svazku dojde ve skutečnosti jen k přejmenování v alokační tabulce souborů a přiřazená oprávnění se nemění. Při přesunu souboru nebo složky mezi svazky (z jednoho na jiný) zdědí kopírovaná položka oprávnění své nové nadřazené složky.

Nyní naštěstí máme technologii, která umí takové problémy najít a opravit. Varonis DatAdvantage sestavuje úplnou mapu oprávnění Windows doplněnou o uživatele a skupiny z Active Directory. Snadno dokáže sestavit zprávu, v níž jsou uvedeny všechny složky s poškozeným seznamem ACL nebo s jinak nekonzistentní sadou oprávnění. Tímto způsobem lze opravittechnicky chybná oprávnění. Ještě nám však zbývají oprávnění, která sice fungují správně, ale přesto k údajům pouští příliš mnoho lidí.

Souhrn

Pomocí bezpečnostního nástroje Varonis DatAdvantage zajišťují stovky organizací celopodnikovou produktivní správu dat prostřednictvím jejich účinného a efektivního automatizovaného řízení. Varonis DatAdvantage zajišťuje řádné využívání dat, správná oprávnění a pomáhá organizacím plnit právní i finanční požadavky a požadavky týkající se práv k duševnímu vlastnictví a ochrany osobních údajů.

* pokud není nastaveno, aby je podřízené složky nedědily