

Multifaktorová autentizace: ujistěte se, že bude nejen bezpečná, ale i flexibilní

Zajistit bezpečnost přístupů k datům, aplikacím a dalším zdrojům je mnohem náročnější, když se uživatelé přihlašují mimo tradiční perimetr firemní sítě. A v dnešním digitálním světě se právě takové přístupy mnohem více požadují. Organizace přesouvají své informační zdroje a operace do cloudu, práce a obchody se realizují prakticky kdekoli, kde je připojení na internet. V takových prostředích se bezpečnost přístupů zajišťuje velice složitě. Je nutné zavádět systémy silné autentizace a multifaktorová autentizace ([multi-factor authentication, MFA](#)) se stala téměř nutností. Vaše organizace potřebuje systém MFA, který nejen poskytne dostatečnou bezpečnost, ale bude ho možné přizpůsobit různým uživatelským potřebám a také růstu nebo změnám ve vaší organizaci. Budete-li se při volbě řešení MFA řídit následujícími principy, dosáhnete správné rovnováhy:

Čím více způsobů autentizace, tím lépe pro všechny

Hledejte řešení MFA, které nabízí více způsobů, jak se uživatelé mohou autentizovat – bez ohledu na to, o koho jde, kde pracují nebo jaký druh zařízení či OS používají. Například pro členy prodejního týmu, kteří se připojují přes chytré telefony, se výborně hodí autentizace na bázi rozpoznání obličeje v mobilu, na druhé straně pro osoby pracující v zabezpečeném prostředí, kde je přístup k mobilním zařízením omezený, bude vhodnější bezpečnostní klíč na bázi standardu FIDO. A pokud uvažujete o rozšíření autentizace i na zákazníky, zřejmě narazíte na ještě širší spektrum požadavků z jejich strany.

Kamkoli vás cloud zavede, mělo by řešení MFA jít s vámi

Dnes již zřejmě každá organizace zahájila cestu do cloudu, ale tyto cesty mohou mít odlišnou podobu. Pokud má podnik své strategie opravdu silně založené na cloudu, měl by zvolit takovou cestu, která do cloudu vede metodicky od jednoho kroku k druhému. Správné řešení MFA je takové, které vám bude poskytovat veškeré funkce ve všech fázích, tedy kamkoli vás cesta do cloudu zavede. Ujistěte se, že řešení, které zvolíte, bude růst spolu s vámi a nepřipraví vám cestou nepříjemné překvapení v podobě narušení chodu systému nebo nutnosti řešení nahradit jiným.

Možnost autentizace kdekoliv, i bez připojení na internet

Každý to zná, jak je frustrující, když se nemůže dostat ke svým zdrojům, protože zrovna není k dispozici připojení na internet – ať jde o uživatele aplikací nebo zákazníky, kteří se nemohou připojit ke zdrojům. A organizace tím také ztrácejí –

Jak organizace
přesouvají své
informační zdroje
a operace do
cloudu a práce
a obchody se
realizují prakticky
kdekoli, kde je
připojení na
internet, zajišťuje
se bezpečnost
přístupů velice
složitě.

přicházejí v důsledku nemožnosti připojení o příjmy i produktivitu. Zvolte takové řešení MFA, které funguje i tehdy, když se osoba, která se autentizuje, nemůže připojit na internet.

SecurID: multifaktorová autentizace pro více lidí na více místech

SecurID je nejčastěji používané řešení MFA na světě. Je to díky tomu, že má komplexní funkce pro zajištění bezpečnosti přístupů a zároveň je velice flexibilní a pohodlné:

Široké možnosti volby autentizátorů dokážou vyhovět celému spektru uživatelských potřeb a požadavků organizace, včetně biometrie, push-to-approve, jednorázových hesel na bázi biometrie (otisk prstu, rozpoznání obličeje), autentizace na bázi FIDO, možnosti využití vlastních autentizátorů nebo hardwarových tokenů.

Možnost snadného **rozšíření podnikového systému autentizace SecurID i do cloudu**, vlastním tempem a v návaznosti na cloudovou strategii organizace.

Stále zapnutá silná autentizace s **dostupností 99,95%** a unikátní „no-fail“ schopností pro Windows a Mac OS, která zajišťuje bezpečný pohodlný přístup i v případě přerušení síťového spojení.

Technologické integrace RSA Ready, které poskytují autentizaci pro specifická přístupová prostředí, jsou pečlivě testované, dokumentované a mají certifikovanou interoperabilitu. Navíc jsou k dispozici otevřené standardy na podporu dalších integrací.

Zjistěte více o zajištění bezpečného pohodlného přístupu ke zdrojům v podnikovém systému nebo v cloudu pomocí multifaktorové autentizace SecurID.

O SecurID

SecurID, technologie vyvinutá RSA, je osvědčenou platformou pro ověřování identit. Využívá ji třináct tisíc organizací po celém světě, které pomocí SecurID spravují padesát milionů identit a poskytují bezpečný pohodlný přístup třiceti milionům uživatelů. SecurID přispívá k úspěšnému působení organizací v digitálním světě, neboť jim umožňuje veškeré možnosti moderní autentizace, správy po celou dobu životního cyklu a řízení identit. SecurID propojuje lidi s digitálními zdroji v podnikové síti či v cloudu, ať žijí, pracují nebo se baví kdekoli.

Více informací získáte na securid.com.