



2Element

MFA

(Multi-Factor Authentication)

Petr.Chmelik@sonpo.cz

Pavel.Novak@sonpo.cz



Argumenty pro MFA

- Přidává k účtům další důležitou vrstvu zabezpečení nad rámec hesla (které může být snadno zneužito).
- Pomáhá ověřit a zajistit, aby každý, kdo se přihlašuje, byl skutečně tím, za koho se vydává. Tím je výrazně sníženo riziko kompromitace účtů.
- Moderní nástroje vícefaktorového ověřování podporují metody s vysokým uživatelským komfortem a zároveň vysokou bezpečností. Např. posílají Push notifikace na telefon s biometrickým zabezpečením (otisk prstu, obličeje) nebo kontrolují fyzický token uživatele. Není tak nutné ručně přepisovat číselné kódy, jako u starších metod.
- Doporučované bezpečnostními autoritami (NÚKIB, CISA).

MFA – Obecně k faktorům pro autentizaci

- Faktory ověřování jsou kategorizovány do tří skupin:
 - Něco, co znáte (například heslo nebo PIN).
 - Něco, co máte (například mobilní telefon nebo hw token).
 - Něco, čím jste (například otisk prstu, scan obličeje nebo jiná biometrická data).
- MFA vyžaduje, aby se uživatel autentizoval pomocí dvou nebo více autentizačních faktorů z různých kategorií (např. „Něco, co znáte“ v kombinaci s „něčím, co máte“).
- Moderní metoda Push notifikací na chytré telefony s biometrickým ověřením spojuje všechny tři tyto kategorie. Přihlášení jménem a heslem (něco, co znáte) je doplněno push notifikací na mobil (něco, co máte), kterou je třeba potvrdit po biometrickém ověření (něco, čím jste).

2Element – naše řešení MFA

- Univerzální řešení pro organizace a firmy
- Doplnuje problematická hesla dalšími faktory
- MFA se používá především pro:
 - Privilegované účty (různá administrátorská oprávnění) – pro všechny typy přístupů
 - VPN, přihlašování na servery, správce hesel, ...
 - Uživatelské účty – především pro přístupy z Internetu do organizace (nebo do cloudu)
 - VPN, vzdálené plochy, ...
- Podpora českého a anglického jazyka (další jazyky možné doplnit)
- Flexibilní řešení pro autentizaci – zaměstnanců, partnerů, zákazníků
- Možnost instalace on-premise (celé pouze u zákazníka, bez cloudu)

Typické služby a aplikace pro MFA

- VPN přístupy (Fortinet, Cisco, CheckPoint, ...)
- Administrátorské RDP přístupy na MS servery
- Vzdálené plochy (RDP) pro uživatele, včetně Terminal Server přístupů
- Lokální přihlášení uživatelů do počítače
- ADFS (Active Directory Federation Services) integrace
- Cloudové služby (O365, ...)
- Aplikace na správu hesel (LastPass, BitWarden, ...)
- Vlastní aplikace zákazníka (Helpdesk, Intranet, ...) pomocí API, SAML
- Portály a řešení pro partnery a zákazníky
- Další integrace protokoly Radius či LDAP

Podporované druhé faktory

- Push notifikace do aplikace pro iPhone či Android
 - (po ověření otisku/obličeje/PINu stačí zvolit „schválit“ nebo “odmítnout“)
- Hardware tokeny – Yubico
- OTP kódy
 - z mobilní aplikace
 - z SMS zprávy

Napojení na AD nebo ADFS

- Napojení na Active Directory, včetně nastavení, které stromy či skupiny uživatelů synchronizovat a jak.
- Současná podpora jak lokálních skupin a uživatelů, tak těch předávaných z AD.
- Možnost provozu i zcela bez napojení na AD. Lokální uživatele je možno založit přímo v MFA serveru. Vhodné pro instalace, které nemají AD, nebo uživatele, kteří nejsou v AD.
- Možná je i podpora dalších LDAP kompatibilních adresářů.
- Integrace do ADFS přihlášení – takto se o MFA snadno rozšíří celý ekosystém podporující ADFS přihlášení a řetězově také SAML.

Možnosti integrace MFA

- Otevřené API pro integraci do aplikací třetích stran
- Napojení na ADFS a SAML (např. cloudové služby zákazníka)
- Podpora RADIUS (např. pro VPN)
- SMS brány
- Správce hesel – můžeme dodat na klíč

Univerzální „MFA aplikace“ pro zákazníka

- Pro větší implementace nabízíme řešení, které je dnes populární například v bankách pod názvy - KB klíč, RB klíč, ...
- To znamená dodat zákazníkovi upravenou mobilní aplikaci, kterou může využívat pro všechny MFA přístupy.
- Vhodná konsolidace všech aplikací, které mají používat MFA ověření.
- “White label” customizace
 - pro server (vlastní název a design)
 - pro mobilní aplikace (vlastní název, design a pevné propojení se serverem zákazníka)

Instalace MFA serverů u zákazníka

- Jedná se o řešení instalované na dedikované servery (Linux CentOS)
 - Doporučuje se instalace do virtualizace - VMware, Hyper-V, KVM
- Obsahuje webové rozhraní pro administrátory
- Optimálně rozděleno na dvě části:
 - V DMZ - web server - komunikuje do Internetu (push notifikace aj.), poskytuje API
 - V (V)LAN - proxy server - Auth proxy, zprostředkovává komunikaci s AD a RADIUS
- Pro velké instalace dodáme škálovatelné řešení, které bude splňovat požadované SLA.

MFA - bezpečnost našeho řešení

- Podrobné logování (audit log) všech procesů v celém řešení.
- Registrace a autorizace mobilních aplikací je zajištěna asymetrickou kryptografií. Soukromý klíč je v moderních mobilních telefonech uložen v dedikovaném bezpečnostním úložišti, nelze ho z něj dostat ven a je chráněn biometricky.
- Administrátor definuje požadované security politiky pro uživatele.
- Přenosy dat jsou standardně šifrovány pomocí *SSL / TLS*.
- Export logů pomocí Syslogu pro externí zpracování (*podpora SIEMu*).
- Integrace přihlášení (*SSO*) s poskytovateli SAML nebo ADFS.
- Aplikace je testována penetračními testy dle metodiky OWASP.
- Možnost poskytnutí zdrojového kódu k auditu.

MFA - konzultace a demo ukázka

- Pro zákazníky a partnery poskytujeme odborné konzultace v této oblasti
- Vysvětlíme všechny pojmy jako např. FIDO2, WebAuthn, U2F, TOTP, ..
- Provádíme předvedení MFA řešení pomocí Teams nebo jiné konference
- Během konference pomůžeme analyzovat nasazení MFA u zákazníka

MFA - Trial verze a PoC instalace

- Pro interní testy poskytujeme trial licence.
- Instalace serveru MFA může být v našem hostingu.
- Rovněž můžeme instalovat u zákazníka do jeho infrastruktury.
- V rámci PoC nabízíme odborné konzultace pro další integrace.

SONPO - přehled služeb

- vývoj software (Java, JavaScript, React, Python, .NET)
- security řešení SOFiE, 2Element
- instalace a správa bezpečnostních produktů Fortinet
- instalace a správa serverů (Linux, Microsoft)
- implementace cloudových služeb (AWS, Azure, Digital Ocean)
- instalace a správa infrastruktury (VMware, KVM, HyperV)
- servisní služby, monitoring a helpdesk 24x7
- penetrační testy
- bezpečnostní audit

MFA - Schéma s příkladem přihlášení k VPN

