Rizika v prostředí Microsoft 365

Je nutné upozornit na reálná nebezpečí pro školské organizace, které využívají prostředí Microsoft 365 a dosud nezavedly požadovanou komplexnost uživatelských hesel, popřípadě nezavedly vícefaktorové ověřování uživatelů. Tuto situaci je možné považovat za vážné bezpečnostní riziko pro školní prostředí Microsoft 365. Implementace vícefaktorového ověřování a vyžadování komplexních hesel jsou klíčovými kroky k zajištění lepší ochrany účtů a dat školy.

Bez vícefaktorového ověřování a s použitím slabých hesel se zvyšuje riziko, že útočníci mohou získat neoprávněný přístup k uživatelským účtům. To může vést k odcizení citlivých informací nebo dokonce k manipulaci s účtem, což může mít za následek ztrátu dat nebo poškození reputace instituce.

- Útočník může například ukrást identitu uživatele (administrátora) a pod jeho jménem skrytě objednat služby a prostředky od Microsoftu. Ani samostatný IT správce v roli globálního administrátora nemusí na to hned přijít. Toto zneužití ukradené identity zjistíte až po první faktuře, z které je patrné, že daný útočník se vám dostal do vašeho prostředí Microsoft 365.
- Útočník ve vašem prostředí může vytvořit nové “Předplatné” (po napadení administrátorského O365 účtu) a provozovat tam svoje vlastní prostředí v podobě virtuálních serverů, sítí a disků atd., s možným nelegálním obsahem.
- Útočník může snáze provádět phishingové útoky pod ukradenou identitou jakéhokoliv uživatele O365 (učitele i studenta). Poté, co se vám tato situace stane, se může vaše doména dostat na “Black list” Microsoftu v rámci ochrany proti phishingu, ze kterého je obtížné se dostat zpět a trvá to určitou dobu. Tím nebudete schopni po tuto dobu posílat například emaily.
- Útočník může získat přístup k osobním informacím, dokumentům a dalším citlivým datům. Útočník se může dostat na všechna datová úložiště dotčené osoby (OneDrive) učitele i studenta.
- Útočník pod cizí identitou se může dostat do školní sítě a může snadněji šířit škodlivý software (ransomware, malware), což může vést k výpadkům systému, ztrátám dat a jiným nepříjemnostem ve vaší školní síti.
- Nedostatečná ochrana dat a účtů může vést k porušení předpisů o ochraně osobních údajů a právním problémům. Škola může být vystavena žalobám a finančním sankcím, pokud nedodržuje příslušné zákony týkající se ochrany dat.
- Útočníci mohou využít kompromitované školní účty k odesílání spamu, šíření dezinformací nebo škodlivých zpráv, což může negativně ovlivnit reputaci školy.

SoftwareOne Czech Republic s.r.o.
Vyskočilova 1410/1
140 00 Praha 4
Czech Republic

telefon: +420 241 405 297
e-mail: info.cz@softwareone.com
web: www.softwareone.cz

IČO: 24207519
DIČ: CZ24207519

Registrováno pod číslem C 188674
u Městského soudu v Praze

Co je nutné udělat?

1. Vyžadovat striktně pro všechny účty nastavení komplexních hesel
   - minimální délku 8 znaků
   - využít kombinaci malých a velkých písmen a čísel
   - nepoužívejte stejné heslo pro jiné účely (online nákupy, online hry, online bankovnictví)
   - Nepoužívejte častá a lehká hesla, např. Heslo123, Karel333, Škola111, HesloVeslo

   Více o těchto doporučeních najdete na Doporučení k zásadám hesel - Microsoft 365 admin | Microsoft Learn

2. Zavést vícefaktorové ověřování uživatelů (u IT správců je toto nutné).

   Popis najdete zde Nastavení vícefaktorového ověřování pro uživatele - Microsoft 365 admin | Microsoft Learn

3. Nastavení politiky podmíněného přístupu, kdy se uživatelé například mohou hlásit pouze z České republiky. Popřípadě je tu možnost vymezit známý rozsah IP adres pro vaše školy, ze kterých se vícefaktorové ověřování nebude vyžadovat a Microsoft tento rozsah IP adres bude považovat za bezpečný.

V případě zájmu o více informací nebo pomoc s nastavením kontaktujte:

Darina Macejková - Mobil +420 775 151 617 - E-mail darina.macejkova@softwareone.com