Devět z deseti firem je špatně zabezpečeno proti kyberútokům

23.6.2023 - | BDO

Dvě pětiny firem v Česku nepoužívají dvojí ověření při přihlašování do sítě

Dvě z pěti firem v Česku nepoužívají vícefaktorové ověřování pro připojení do firemní sítě. *Polovina firem pak při přihlašování do systému nepožaduje silná hesla, která jsou pro útočníky hůře prolomitelná. „Práce s hesly představuje pro firmy jedno z největších bezpečnostních rizik. Téměř každá třetí firma (30 %) umožňuje uživatelům používat beze změny stejné heslo do více aplikací a programů. Firemní sítě jsou tak nedostatečně chráněny a riziko prolomení do systému se zvyšuje. Pro úspěšný ransomware útok přitom stačí jeden úspěšný pokus a firma může i přijít o většinu dat, která dostane možná zpět až po případném zaplacení vysokého výkupného,*“ varuje expert na kyberbezpečnost ze společnosti BDO Martin Hořický. Důležité je také používat vícefaktorové ověření při připojení z internetu do interní počítačové sítě. To aktuálně používá pouze o něco více než polovina firem.

Špatně zabezpečený vzdálený přístup má čtvrtina firem v ČR

Firmy se potýkají také s nedostatečným zabezpečením vzdáleného přístupu do firemních systémů. Odlišná pravidla a postupy pro jeho zřizování chybí podle BDO u skoro čtvrtiny z nich. *„Ani po roce práce z domova nemá 26 % firem stanovena jasná pravidla pro vzdálený přístup do interních systémů. Zaměstnanci, kteří pracují z domova, často ze svých soukromých počítačů, ale představují značné bezpečnostní riziko. Internetové sítě, přes které se pracovníci přihlašují do firemních systémů, mají totiž nižší stupeň zabezpečení, které útočníci snáze prolomí. Firmy by měly školit své zaměstnance, aby nepoužívali stejná hesla například do soukromého či firemního e-mailu. Důležité je také používat bezpečné aplikace pro jejich správu,*“ upřesňuje Martin Hořický z BDO.

Kontrolu oprávnění uživatelů k připojení do firemní sítě neprovádí každá třetí firma

Studie BDO zjistila také nedostatky v oprávněních uživatelů pro přihlašování do firemních sítí. Jejich pravidelné kontroly neprovádí třetina firem v Česku. Další třetina přístupy zaměstnanců do sítě sice kontroluje, ale nedostatečně a s velkými prodlevami. Změny uživatelských účtů neprobíhají u každé osmé firmy. *„Pokud firma pravidelně nekontroluje, kdo má do její interní sítě přístup, vystavuje se riziku úniku dat, například ze strany bývalých zaměstnanců. Nemusí se pak jednat o kybernetický útok, pouze stačí, aby se neoprávněná osoba připojila původním heslem do systému, a může z firmy vynést cenná data. Kontroly oprávnění k přístupu do systému firmy by měly probíhat automaticky, minimálně jednou za půl roku,*“ uzavírá Martin Hořický z BDO

https://www.bdo.cz/cs-cz/novinky/2021/devet-z-deseti-firem-je-spatne-zabezpeceno-proti-kyberutoku m