VISA Europe

Výchozí a sdílené přihlašovací údaje

Mnozí výrobci dodávají své produkty s již přednastaveným výchozím uživatelským jménem a heslem, s úmyslem usnadnit instalaci zařízení a software. Bohužel, v běžné praxi mnoho organizací neprovede základní kontrolu zásad informační bezpečnosti před nasazením nového zařízení nebo instalací nové aplikace. Pokud je takové zařízení nasazeno nebo aplikace nainstalována, aniž by nejprve došlo k zablokování nepotřebných uživatelských účtů a změně výchozích hesel, organizace se vystavuje vážnému riziku úniku dat. Výchozí nastavení uživatelských účtů a hesel jsou často publikována na Internetu a to napomáhá hackerům aktivně využít tyto informace k nelegálnímu přístupu do informačních systémů.

Použití výchozího nastavení přihlašovacích údajů je totéž jako zakoupení drahého zámku k vlastním vchodovým dveřím a následné poskytnutí kopií klíčů pachatelům trestné činnosti. V momentě, kdy hackeři proniknou vaším zabezpečením, jejich jednání postupně vyústí ve ztrátu reputace vaší společnosti a masivní finanční újmu.

„Použití výchozího nastavení přihlašovacích údajů je totéž jako zakoupení drahého zámku k vlastním vchodovým dveřím a následné poskytnutí kopií klíčů pachatelům trestné činnosti.“

Zásady zmírňující závažnost rizika

Správné řízení uživatelských účtů a hesel tvoří významnou bariéru v obraně proti neoprávněnému úniku dat. Důkladné dodržování jednoduchých pokynů uvedených níže napomůže ke znatelnému zvýšení míry zabezpečení vaší organizace. Vezměte prosím na vědomí, že tyto zásady by měly být přijaty a implementovány společně (spíše než odděleně) tak, aby bylo docíleno vícenásobné ochrany informačních systémů.

Změňte výchozí hesla	První krok, který musí organizace před uvedením zařízení nebo aplikace do produkčního prostředí učinit, je změna / zakázání všech výchozích uživatelských účtů a hesel. V případě, že si nebudete vědět rady, jak toto provést, řiďte se pokyny uživatelské příručky dodané k zařízení nebo kontaktujte přímo dodavatele. U již využívaných zařízení nebo aplikací byste měli ihned prověřit, které z těchto systémů využívají standardně nastavené přístupové údaje, a změnit je co nejdříve, jakmile to bude možné.
Používejte komplexní hesla	Pouhá změna hesla není dostatečná, pokud je heslo samotné považováno za „slabé“. Pro hackera není problém „slabé“ heslo uhodnout. Za slabé heslo může být považováno například běžně používané slovo nebo slovníkový výraz. Vámi používané heslo by mělo mít nejméně 7 znaků a používat kombinaci velkých a malých písmen, čísel či speciálních znaků (jako jsou např.:!“Ł$%^).
Odstraňte neaktivní uživatelské účty	Uživatelské účty, které jsou neaktivní, by měly být zakázány. V případě odchodu zaměstnance ze společnosti by mělo být jeho uživatelské konto ihned deaktivováno.
Nesdílejte přístupové údaje	Sdílené přístupové údaje jsou velmi podobné systémům univerzálního (centrálního) klíče, a pokud to není opravdu nezbytně nutné, neměli byste používat stejné uživatelské účty napříč několika systémy nebo tyto údaje sdílet mezi více uživateli. V případě, že je správa systémů zajišťována třetí stranou, ujistěte se, že uživatelské účty používané pro správu vašich systému jsou specifické pro vaši organizaci a nejsou stejné pro další klienty této třetí strany.
Měňte pravidelně heslo	Uživatelská hesla by měla být měněna nejméně jednou za tři měsíce.
Sledujte podezřelé aktivity	Sledování nepovolených přístupů do systému by mělo být průběžné. Například pokusy o vstup do systému mimo pracovní dobu uživatele nebo vícenásobné neúspěšné pokusy o přihlášení by měly být prověřeny jako možný útok na váš systém.

Další kontrolní mechanizmy

Omezte počet neúspěšných pokusů o přihlášení	Pokud zařízení nebo aplikace umožňuje uzamknutí účtu po vícenásobných neúspěšných pokusech o přihlášení, tuto funkci zapněte. Pokud si nejste jisti, zda je vaše zařízení nebo aplikace tuto funkci podporuje nebo jak ji povolit, řiďte se pokyny přiloženého manuálu nebo kontaktujte přímo dodavatele
Používejte pouze nezbytně nutná oprávnění	Pokud není pro uživatele vyžadován přístup k systému nebo aplikaci, měl by být standardně omezen přístup k systému. Pro uživatele by mělo být povoleno pouze takové oprávnění, které je potřebné k výkonu jeho práce.

Příloha A - Další zdroje informací

Microsoft

- Nástroj pro kontrolu komplexnosti hesel (EN)- https://www.microsoft.com/security/pc-security/password-checker.aspx
- Příručka pro tvorbu silných hesel (EN) - http://www.microsoft.com/en-gb/security/online-privacy/passwords-create.aspx