Cvičný text

Manipulace s hesly
Pravidla pro manipulace s hesly představují tu nezákladnější, avšak pravděpodobně jednu z nejdůležitějších částí komplexní bezpečnostní strategie, neboť podle dlouhodobých odhadů CERT Internetu bylo až 80% průniků umožněno použitím „slabých“ (snadno odhalitelných) hesel. Jako základní opatření se doporučuje periodická kontrola „kvality“ používaných hesel prováděná odpovědnými správci systémů pokud možno stejnými (nebo velmi podobnými) prostředky, které by mohl použít potenciální průnikář (např. programovým balíkem crack) s následným podmíněným zákazem kont s odhalenými hesly (dokud si je dotčení uživatelé nezmění). Pravidla pro manipulaci s hesly musí být také v souladu s komplexní bezpečnostní strategií v oblasti IT, musí tedy obsahovat např. zákaz zapisování hesel, specifikaci kdo a jakou formou smí distribuovat hesla, zda (a za jakých okolností) mohou uživatelé sdílet svá hesla s jinými uživateli apod. Důrazně se doporučuje striktně dodržovat pravidla umožňující provedení jednoznačného auditu: „jeden uživatel-jedno konto-jedno heslo“ (neexistují anonymní nebo „skupinová“ konta).

Princip individuální znalosti hesla by měl být uplatněn i pro tzv. superuživatele (a/nebo administrátory) systému, ovšem s možností autorizovaného získání znalosti hesla v případě náhlé potřeby při jejich nepřítomnosti. Pro tento účel lze využít vhodné varianty některé z kryptogrfaických metod sdílení tajemství (secret sharing) založené na tzv. (m,n)-prahovém schématu (threshold scheme), kdy je heslo superuživatele (jím samotným) rozděleno na n částí, z nichž alespoň m libovolných částí pak stačí k rekonstrukci původního hesla. Tím je jednak superuživatel chráněn proti možnému zneužití jinou osobou, neboť pro rekonstrukci původního hesla je zapotřebí znát současně alespoň m jeho částí (a ze znalosti menšího počtu nelze odvodit zbývající části chybějící k celkové rekonstrukci hesla) a jednak toto schéma umožňuje uplatnit i princip hierarchické kolektivní odpovědnosti, kdy některým služebně nadřízeným osobám lze přidělit větší počet částí tak, že např. rekonstrukci hesla může provést buď vedoucí projektu společně s jedním svým zástupcem, nebo společně 3 zástupci, nebo 2 zástupci společně s 2 vedoucími oddělení apod.

Kritickou činností je správná volba inicializačních hesel při zavádění nových uživatelů tak, aby nebyla snadno odhadnutelná, a přesto dobře zapamatovatelná. Nikdy by se neměla používat tzv. „implicitní“ hesla (stejná pro každé konto), nýbrž každý nově zaváděný uživatel musí mít své unikátní inicializační heslo. Toto pravidlo je zvlášť kritické v těch organizacích, v nichž je paušální přidělení konta pravidlem i u těch uživatelů, kteří jej možná v blízké budoucnosti nebudou vůbec používat. Dobrou zvyklostí je i povinné přihlášení každého nového uživatele z bezpečné pracovní stanice okamžitě po zřízení jeho konta s vynucenou změnou hesla.

Volba hesla
Pravděpodobně nejzranitelnější částí každého počítačového systému (bez ohledu na jeho další zabezpečení proti útoku ze sítě) je právě uživatelské heslo chránící jeho konto, neboť nejsnazší způsob, jak může průnikář získat přístup do systému je „uhodnutí“ špatně zvoleného uživatelského hesla. Proto je nutné definovat závazná pravidla pro volbu „silných“ hesel a informovat o nich všechny uživatele. Doporučuje se (pokud možno) používat speciální software pro automatické generování „silných“ hesel (npasswd, passwd+), který je naprogramován tak, že zabezpečí splnění předepsaných pravidel.

Základní pravidla pro volbu „silných“ hesel jsou:
nikdy nepoužívejte:

1. své uživatelské jméno v žádné formě (pozpátku, malá/velká písmena, zdvojené, …),
2. jakékoliv informace odvoditelné z osobních údajů uživatele (jména, číslo auta, bydliště, …),
3. heslo tvořené buď pouze čísly, nebo pouze písmeny,
4. slovo obsažené v nějakém slovníku (i cizojazyčném) nebo libovolném seznamu či jako vzor „silného“ hesla z knihy o bezpečnosti počítačových systémů,
5. sekvence sousedních znaků klávesnice (qwerty, fredfred, …),
6. heslo kratší než 6 znaků,

používejte:

1) heslo tvořené kombinací malých a velkých písmen,
2) heslo obsahující nealfanumerické znaky (interpunkční znaménka, …),
3) snadno zapamatovatelná hesla (abyste si je nikdy nemuseli zapisovat),
4) heslo, které umíte rychle zapsat (i bez pohledu na klávesnici).

Empirické metody volby hesel odpovídajících těmto pravidlům zahrnují (v kombinaci s vhodným střídáním malých/velkých písmen či doplněním číslic a interpunkčních znamének):

a) použijte počáteční písmena slov sloky oblíbené písně,
b) zvolte nesmyslnou, avšak snadno vyslovitelnou či zapamatovatelnou sekvenci slabik,
c) vyberte 2-3 krátká slova spojená navzájem interpunkčními znaménky (no^TE*pic),
d) krátká věta (10letvAsii).

Uživatelé by měli být nuceni periodicky měnit svá hesla (obvykle každých 3 až 6 měsíců), což zajistí, že i úspěšný a dosud neodhalený průnikář nakonec ztratí přístup do systému.

Procedura změny hesla

Přesná specifikace procedury změny hesel je důležitým prvkem pro udržení jejich utajení před nepovolanými osobami. Uživatelé by měli být schopni měnit svá hesla on-line po síti, avšak pokud možno pouze z bezpečných segmentů sítě tak, aby riziko odposlechu nežádoucí osobou bylo co nejvíce minimalizováno. Při požadavku uživatele na provedení změny hesla systémovým administrátorem (např. při jeho zapomenutí) je nezbytné přesně definovat tuto proceduru z hlediska zachování důsledného ověření identity žadatele (např. nelze akceptovat prostou telefonní žádost či žádost elektronickou poštou neobsahující digitální podpis apod.).

V případě podezření na úspěšný průnik do systému se doporučuje, aby systémový administrátor provedl okamžitou změnu všech hesel. Pak ovšem nastává organizační problém, jak co možná nejrychlejším ale také nejbezpečnějším způsobem informovat uživatele o jejich nových heslech. Procedura organizace změny hesel však musí být současně odolná i vůči možnému imitování pravého systémového administrátora potenciálním průnikářem (aby důvěřiví uživatelé např. nezměnili svá hesla na hesla, která obdrželi příkazem jako součást neautorizované zprávy elektronickou poštou od svého údajného systémového administrátora). Všichni uživatelé by měli být podrobně seznámeni se všemi organizačními procedurami týkající se změny hesel a pro tyto standardní procedury by neměli platit žádné výjimky. Uživatelé by měli být také nabádáni k tomu, aby veškeré podezřelé aktivity v této oblasti hlásili svému systémovému administrátorovi (lepší planý poplach než dlouhodobě nedetekovaný průnik do systému).