IT bezpečnosť automatizačných a SCADA systémov (2)

Politika hesiel

Heslo je prvou líniou obrany akéhokoľvek počítačového systému. Malo by spĺňať dve protichodné požiadavky – musí byť silné (aby ho nebolo ľahké odhaliť) a súčasne ľahko zapamätateľné. Hoci ochrana heslom vo všeobecnosti nie je najsilnejším typom ochrany, voľba dostatočne silného hesla môže spomaliť útočníka, takže sa získa čas na vykonanie protiopatrení, alebo môže znechutiť útočníka, ktorý potom obráti pozornosť na ľahšie dostupné ciele. Silné heslo definujeme ako slovo zložené minimálne zo šiestich a viac znakov, v ktorom sa nepravidelne striedajú malé a veľké písmená, číslice a špeciálne znaky (?&*, a pod.). Heslo by nikdy nemalo vytvárať zrozumiteľné slovo, dátum a pod., a to ani po nahradení písmen číslicami a špeciálnymi znakmi.

Na odhalenie hesla sa používajú dve techniky – vyhľadávanie v slovníku a prelomenie hesla hrubou silou. Odhalenie hesla, ktoré má zmysel (pomocou slovníka), trvá niekoľko minút, a to aj v prípade, že je napísané v inom jazyku. Ak je zvolené silné heslo, potom vyhľadávanie pomocou slovníka nestačí a útočník použije metódu hrubej sily. Hľadanie hesla sa začína skúšaním všetkých slov v slovníku, potom sa postupne pridávajú číslice, špeciálne znaky atď. Dostupné softvérové nástroje celý proces automatizujú, takže v konečnom dôsledku je úspešnosť uhádnutia hesla 100 %. Dôležitý je však čas, za ktorý sa dosiahne výsledok. Tab. 1 veľmi výstižne ukazuje pomer medzi silou hesla a časom potrebným na jeho prelomenie [3].

Údaje v tabuľke boli vypočítané pre heslá zložené zo 4, 6 a 8 znakov, pretože takéto heslá sa používajú v zariadeniach automatizačných systémov. So zvyšovaním počtu znakov sa, samozrejme, čas potrebný na prelomenie hesla zvyšuje. Bezpečnostné praktiky hesiel obsahujú aj ďalšie aspekty, ktorých dodržiavanie podstatne zvyšuje úroveň ochrany heslom:

1. Používanie rôznych hesiel pre rôzne úrovne systému.
2. Periodická zmena hesiel jedenkrát mesačne, maximálne jedenkrát štvrťročne.
3. Okamžitá zmena hesiel po akýchkoľvek zásahoch (napr. servisných) tretích strán.

Počet znakov hesla	Počet preskúmaných slov	Prenosová rýchlosť			
		9,6kb/s	19,2kb/s	38,4kb/s	10Mb/s
Slovník					
4	11 022	1,9 hod.	1,4 hod.	1,3 hod.	0,9 hod.
6	20 721	3,5 hod.	2,7 hod.	2,5 hod.	1,7 hod.
8	23 955	4,0 hod.	3,1 hod.	2,9 hod.	2,0 hod.
Hrubá sila					
4	66 347 190	11 168 hod.	8 625 hod.	7 961 hod.	5 528 hod.
6	$5,3741 \times 10^{11}$	10 326 rokov	7 975 rokov	7 361 rokov	5 112 rokov
8	$4,3530 \times 10^{15}$	83 647 831 rokov	64 599 315 rokov	59 630 136 rokov	41 409 817 rokov

Tab.1

4. Okamžitá zmena hesiel po zistenom útoku alebo podozrení na útok, po akomkoľvek konflikte so zamestnancami, ktorí obsluhujú automatizačný systém.
5. Používanie generátorov hesiel namiesto vymýšľania hesiel.
6. Používanie programov na prelomenie hesiel s cieľom zistiť slabé heslá.
7. Dôsledná ochrana proti fyzickému ukradnutiu hesla (heslá napísané na papierikoch, uložené v počítači a pod.).

Politika hesiel je jedným z najlacnejších, avšak v špecifickom prostredí automatizačných a SCADA systémov nie vždy najľahšie aplikovateľným obranným mechanizmom, pretože závisí od zodpovedného prístupu ľudí a od ich dôveryhodnosti. Nariadenia v tejto oblasti veľmi nepomôžu, pretože sú ťažko kontrolovateľné a postupy využívané v štandardných počítačových systémoch často nemožno použiť.

Uvažujme napríklad, čo by sa stalo, ak by sme použili štandardný systém periodickej kontroly zmeny hesla, často používaný v podnikových intranetových systémoch, a z akéhokoľvek dôvodu by nedošlo k zmene hesla po vypršaní doby jeho platnosti – daná časť automatizačného systému by sa mohla zablokovať práve v čase, keď treba vykonať nejakú činnosť na zariadení VVN/VN. Alebo s obľubou používaná funkcia odpojenia systému po zadaní troch po sebe nasledujúcich nesprávnych hesiel. Predstavte si riešenie havarijnej situácie a práve vtedy používateľ v strese zadá omylom nesprávne autentifikačné údaje – dôjde k zablokovaniu systému s nepredvídateľnými dôsledkami. Výrobcovia zariadení procesnej úrovne mnohokrát rátajú s týmito rizikami, a tak nie je ojedinelé, že sa stretávame so zariadeniami, pri ktorých sa autentifikácia nepoužíva. Tieto zariadenia sú chránené obvykle mechanicky – zámkom. Prelomenie takejto ochrany však znamená otvorenie brány minimálne do danej dôveryhodnej zóny a eventuálne poškodenie alebo nesprávne vydaný a vykonaný príkaz sa môže rozšíriť v elektrizačnej infraštruktúre ďalej napriek tomu, že útok zostane izolovaný v rámci danej zóny.

Literatúra

[1] When SCADA Systems Are Attacked!, Dick Lord, The Steadfast Group, August 2005

[2] Industrial information system security, Dzung D., Naedele M., ABB Review, 2/2005

[3] Concerns about intrusions into remotely accessibile substation controllers and SCADA systems, Paul Oman, Edmund O. Schweitzer, Deborah Frincke, III Schweitzer Engineering Laboratories Inc., University of Idaho, SEL 2000

Pokračovanie v budúcom čísle.

Ing. Július Tomčík, PhD. 58

Východoslovenska energetika, a. s., Košice
e-mail: tomcik_julius@vse.sk

Ing. Iveta Tomčíková, CSc.

Technická univerzita Košice
e-mail: iveta.tomcikova@tuke.sk