Testování bezpečnostní politiky

Bezpečnost ICT je pod neustálým tlakem. Organizace musejí provozovat svoji činnost v souladu s nejrůznějšími předpisy a normativy. Tyto předpisy stanovují i detailní bezpečnostní parametry. Míru souladu s těmito parametry zjišťujeme pomocí testování bezpečnostní politiky.

Základními oblastmi testování, které se obvykle provádějí na zařízeních ICT, jsou penetrační testování a správa zranitelností. Tento způsob testování sleduje, zda se na zařízeních nevyskytují zranitelnosti zneužitelné útočníkem, případně zda jsou nainstalovány všechny bezpečnostní aktualizace.

Z hlediska sledování bezpečnosti existuje další velmi důležitá kategorie – testování a audit konfigurace zařízení ICT. Tento požadavek kontroly konfigurace vychází z nejrůznějších legislativních nebo technických požadavků, jejichž cílem je zaručit maximální bezpečnost zařízení a dat, minimalizovat možné škody a výpadky způsobené činností externích či interních subjektů.

Základními zdroji, které určují nastavení konfigurace zařízení ICT, obvykle jsou:

- podnikové předpisy a směrnice, které určují práva a povinnosti uživatelů, administrátorů a všech osob přicházejících do styku s informačními technologiemi a stanovují požadavky na bezpečnostní parametry zařízení. V organizacích obvykle existují pravidla pro interní i externí subjekty;
- právní předpisy a normy jako je ISO/IEC 27002, SOX, HIPAA, COBIT, PCI DSS a další. Některé normy jsou pro určité segmenty podnikání povinné;
- doporučené konfigurace pro různé typy zařízení. Na internetu jsou k dispozici doporučené konfigurace např. pro servery s cílem eliminovat bezpečnostní slabiny, vypnout všechny nepotřebné služby a zařízení maximálně zabezpečit. Příkladem jsou bezpečnostní doporučení pro konkrétní operační systémy a aplikace, které vydává organizace CIS (Center for Internet Security) nebo návody z oblasti „Securing and Hardening Servers“;
- vlastní postupy pro konfiguraci a zabezpečení serverů – většinou vycházejí z praktických zkušeností.

Tyto zdroje určují všeobecná pravidla pro používání prostředků ICT v rámci organizace nezávisle na použitých informačních technologiích, ale obsahují i detailní doporučení a nastavení, která mají přímou vazbu na technické a bezpečnostní parametry zařízení ICT.

Cílem testování bezpečnostní politiky je určit míru souladu (Policy Compliance) mezi požadovanou konfigurací a skutečným bezpečnostním nastavením zařízení ICT. Na rozdíl od testování zranitelností, kde se odstraňují konkrétní zranitelnosti využitelné útočníkem, bezpečnostní politika a konfigurace bezpečnostních parametrů nejsou přesně určeny. Záleží na výchozích legislativních a technických požadavcích, což je v každé organizaci odlišné.

Parametry bezpečnostní politiky

Po technické stránce se bezpečnostní politiky skládají z jednotlivých kapitol a jednotlivých opatření, která mají vazbu na příslušné bezpečnostní parametry operačního systému nebo aplikačního programu. Sledovaných bezpečnostních parametrů jsou obvykle desítky až stovky v závislosti na operačním systému nebo aplikaci. Základními oblastmi bezpečnostních parametrů, které jsou kontrolovány na zařízeních ICT, jsou např. přihlašovací parametry, přístupová práva, nastavení auditních a logovacích možností a mnoho dalších. Přehled nejdůležitějších oblastí bezpečnostní politiky udává Box 1.

Pro vysvětlení vlastního principu testování bezpečnostní politiky lze použít následující příklad. Jeden z obvyklých požadavků bezpečnostní politiky v organizaci určuje, že musí být evidována všechna přihlášení na zařízení (úspěš-

Přehled oblastí testování bezpečnostní politiky BOX 1

Přístupová práva
- vytváření účtů, seznamy uživatelů a skupin;
- správa hesel;
- autorizace;
- přístupová práva k systému, souborům a databázím.

Bezpečnostní parametry
- nastavení bezpečnostních parametrů služeb;
- nastavení výkonnostních parametrů operačního systému;
- parametry síťových služeb.

Antivirus / zranitelnosti
- stav aktualizace softwaru;
- stav antivirového software.

Integrita a dostupnost
- logování a audit;
- monitorování logů.

Šifrování
- šifrování síťových spojení a přenosu dat;
- šifrování souborů a disků;
- délka klíče a použitý algoritmus.

Nastavení síťových parametrů
- přístupová práva k síťovým službám;
- nastavení lokálních firewallů, IDS, VPN.

Síťové služby
- status síťových služeb;
- kontrola vypnutých služeb.

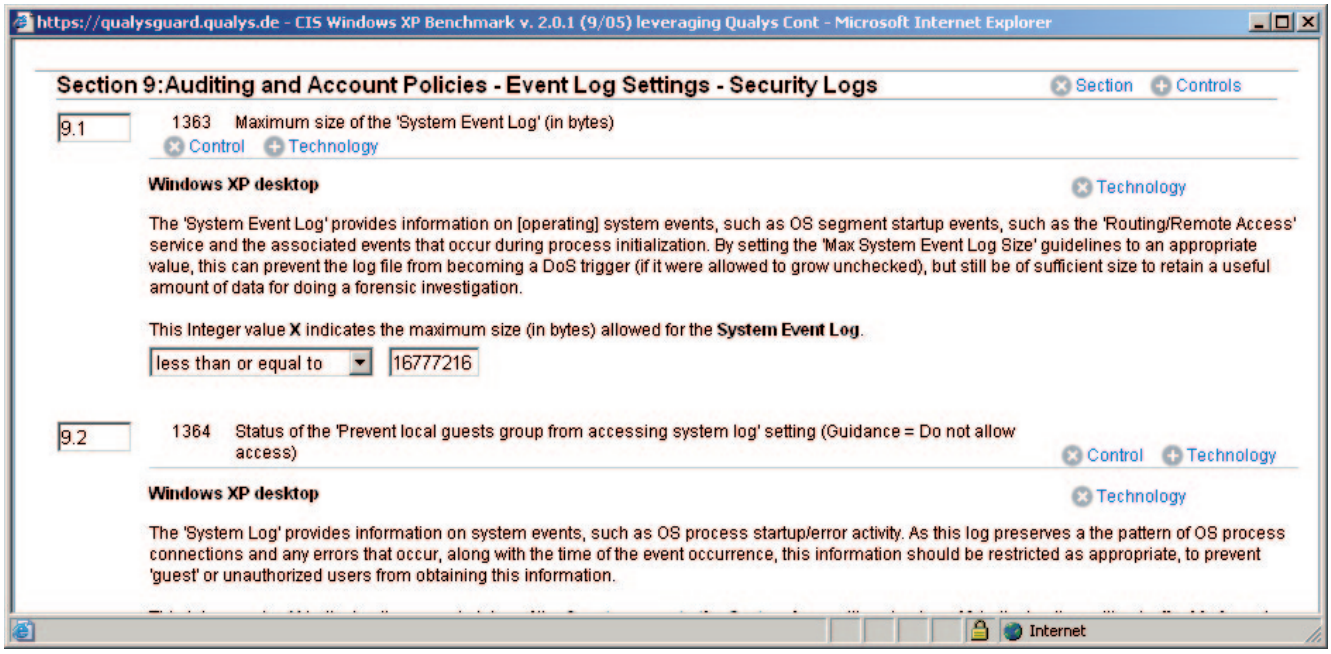
ná i neúspěšná), současně musí být zaručena funkčnost ukládání záznamů a ochrana před zaplněním logů. Odpovídajícím opatřením je v případě operačního systému Windows nastavení následujících auditních parametrů:

- Parametr „Audit Account Logon Events“ ve Windows registrech určuje úroveň logování; možné hodnoty jsou ‚Success,‘ ‚Failure,‘ and ‚No Auditing‘.
- Parametr Maximum size of the ‚Security Event Log‘, požadovaná velikost je určena v bitech.
- Pokud jsou v příslušných Windows registrech nastaveny hodnoty na ‚Success‘ a ‚Failure‘ a velikost Event logu je nastavena na 80 MB (doporučená velikost), je v těchto bodech nastavení zařízení v souladu s požadovanou bezpečnostní politikou.
- V případě, že konfigurace není v souladu s požadovanou konfigurací, je nutné konfiguraci zařízení změnit nastavením příslušného registru.

Z povahy jednotlivých bezpečnostních parametrů vyplývá, že konfigurační parametry jsou závislé na použitém operačním systému nebo aplikaci. Některé bezpečnostní parametry jsou úzce svázány s konkrétním operačním systémem, dále jsou to bezpečnostní parametry, které se týkají aplikačních programů. Příkladem jsou specifická nastavení registrů u operačního systému Windows nebo konfigurační parametry relačních databází Oracle nebo MS SQL. Na druhou stranu existují bezpečnostní parametry, které jsou obdobné u většiny platforem. Typickým příkladem jsou vlastnosti přístupových hesel, tj. požadovaná délka hesla pro přihlášení, složitost hesla nebo přístupová práva k souborům. Pro tyto parametry existují univerzální opatření, která jsou k dispozici pro všechny operační systémy.

Pro testování politiky je na trhu k dispozici celá řada nástrojů od různých výrobců bezpečnostního softwaru. Příkladem nástrojů jsou nástroje od firem Qualys, NetIQ, Tenable, Symantec. Protože existuje velké množství operačních systémů, obvyklou vlastností nástrojů je podpora celé řady hlavních platforem, jako jsou Windows, AIX, HP-UX, Linux (Red Hat, Suse, Debian), Solaris, Mac OS a další. Deklarace podpory pro příslušné verze operačních systémů je klíčová. Nástroje pro testování politiky neumožňují správně testovat operační systémy, které nejsou uvedeny v seznamu podporovaných platforem. Některé nástroje tyto systémy vůbec neumožní testovat a případné testování skončí chybovým hlášením pro nepodporovanou platformu.

Každý nástroj má svůj Policy Editor, který umožňuje vytvořit šablony bezpečnostních politik. Šablona bezpečnostní politiky se obvykle skládá pro větší přehlednost



Obr. 1: Popis jednotlivého opatření pomocí nástroje Policy Editor.

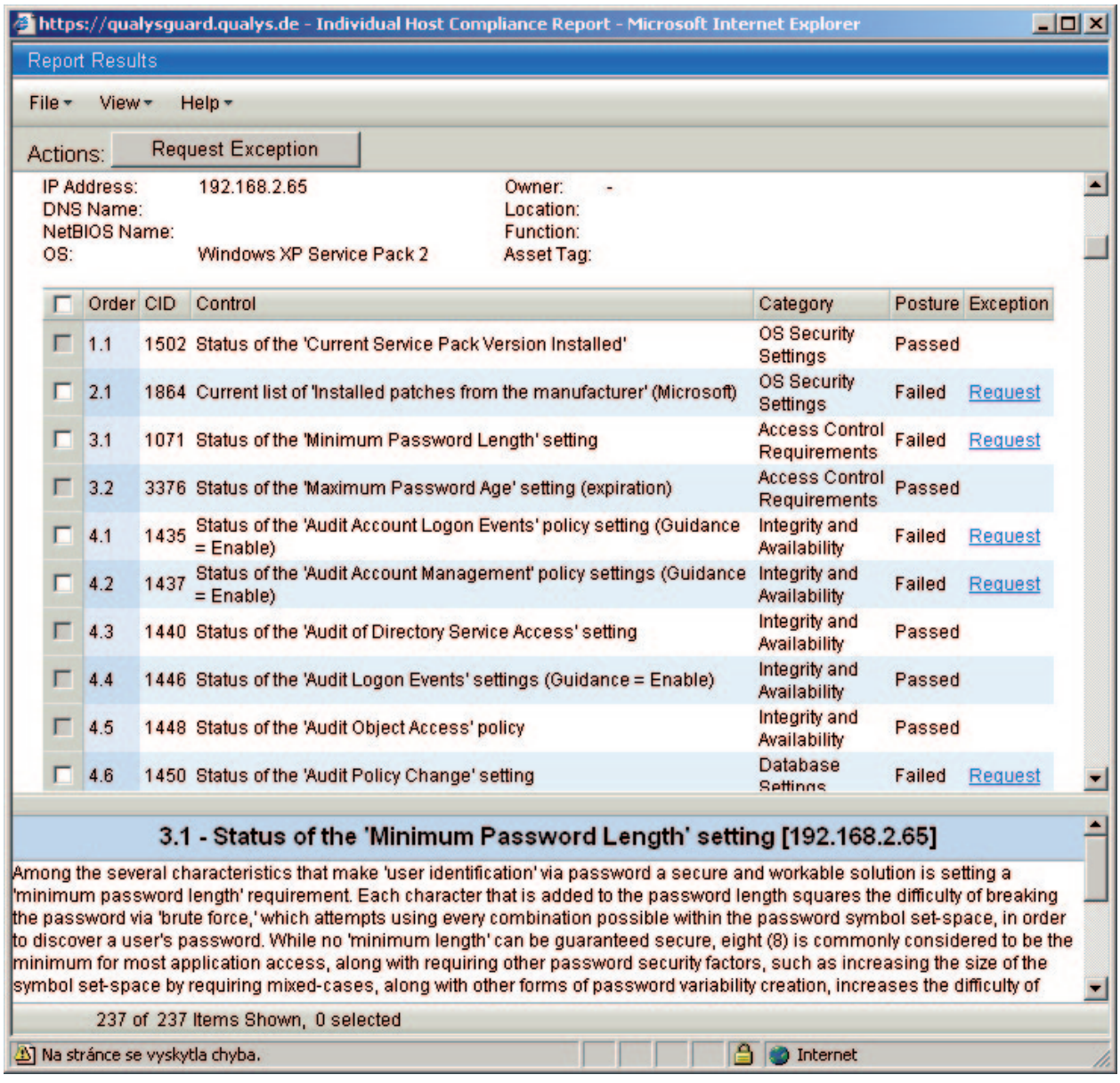
z jednotlivých kapitol, jejichž součástí jsou jednotlivá opatření. U každého opatření lze nastavit požadovaný výsledek. Obvykle je možnost použití logických operátorů (je rovno, je vetší, je menší, není rovno, obsahuje, neobsahuje apod.). U některých parametrů lze vložit klasické regulární výrazy. Každé opatření dále obsahuje podrobný popis, do kterého lze obvykle vložit i vlastní komentář nebo webový odkaz na intranetovou firemní dokumentaci.

Programy na testování politiky obvykle umožňují testovat i všeobecné parametry, jako např.:

- existenci, obsah a přístupová práva k registrům;
- přístupová práva k adresářům a souborům;
- obsah a kontrolní součty souborů.

Tyto parametry nemusí být již použity v bezpečnostní politice, ale umožňují větší univerzálnost nástrojů a provádění testování dle vlastních požadavků. Umožňují rychlé nalezení výskytu modifikovaného souboru (např. virem) na všech zařízení. Nástroje jsou často kombinované s dalšími bezpečnostními funkcemi, obvykle umožňují např. i provádění penetračního testování a správu zranitelností.

Protože testování zjišťuje konfigurační parametry cílového zařízení, v jeho průběhu je nutný přístup s autentizací na cílovém zařízení. Obvykle pomocí služby/agenta, který je nainstalován na cílovém zařízení, nebo lépe u některých produktů pomocí přímého (agentless) přístupu. V tomto případě probíhá testování u zařízení s operačním systémem Unix přes SSH port, u operačního systému Windows přes RPC port, případně je využíván přímý



Obr. 2: Výsledný report testování politiky jednoho zařízení.

přístup do relační databáze s vlastní autentizací. Protože testování obvykle vyžaduje přístup k systémovým souborům a konfiguračním parametrům, je nutné provádět testování převážně v kontextu administrátorských práv na cílovém zařízení. V případě Windows systému to znamená práva na úrovni role administrátora (nejčastěji role Domain Admin), v případě unixových zařízení práva na úrovni superuživatele (root). Pro testování je proto nutný souhlas odpovědných osob v organizaci s vytvořením příslušných účtů. Obvykle to může znamenat komplikaci při zavádění procesu testování, zvláště při auditu, který je prováděným externím subjektem.

Implementace a testování politiky

Jak již bylo uvedeno, hlavním cílem testování a auditu bezpečnostní politiky je zjistit míru souladu mezi požadovanou konfigurací a skutečným nastavením. Zjišťuje se, v jaké míře jsou aplikovány požadované bezpečnostní parametry, určuje se míra souladu (Policy Compliance) nastavení bezpečnostních parametrů s požadavky bezpečnostní politiky. Celý proces testování bezpečnostní politiky má obvykle formu procesního cyklu (workflow).

Nejdříve se provádí sestavení jednotlivých politik na základě sumarizace všech podkladů. Jak již bylo uvedeno, vychází se z podnikových směrnic, právních předpisů a norem. Na základě těchto požadavků se vytvoří v testovacím nástroji šablony bezpečnostní politiky. Nástroje obsahují často předdefinované šablony, které je možné modifikací upravit pro vlastní použití. V praxi má vytváření bezpečnostních politik obvykle na starosti bezpečnostní manager. Sestavení bezpečnostních politik je dost složité, obvykle vyžaduje detailní znalosti operačního systému. Z tohoto důvodu se šablony bezpečnostních politik často tvoří ve spolupráci s externí firmou nebo v úzké kooperaci s administrátory ICT.

Dokončené bezpečnostní politiky se přiřadí k systémům, aplikacím a službám podle relevance. Obvykle se přidruží odlišné politiky ke skupinám s různou hodnotou aktiv a významu, tedy jiné pro internetové a intranetové servery, pracovní stanice, přenosné počítače atp.

Vlastní ověření shody se provádí spuštěním auditu pomocí testovacího nástroje. V jednom kroku se obvykle spouští test celé skupiny aktiv. Testování se většinou provádí v nočních hodinách, kdy je činnost serverů minimální. Obvyklá doba testování politiky 10 zařízení trvá řádově desítky minut. Výjimkou jsou pracovní stanice a notebooky, kde bývá nutné provádět testování v pracovní době, kdy jsou počítače zapnuté.

Nástroje umožňují vytvoření reportů. Obvykle se generují přehledy podle jednotlivých zařízení nebo celých skupin aktiv. V reportech je u každého opatření uveden výsledek shody (úspěšný/neúspěšný) a stanovuje se souhrn úspěšnosti za jednotlivá zařízení i celé skupiny aktiv.

Nalezené neshody se evidují a procesně zpracovávají. Příslušní administrátoři informačních systémů dostanou přidělené úkoly (tickety) s termínem pro odstranění nesouladu. Lhůta je 14 dní až měsíc. Každý administrátor může požádat o výjimky z nastavení bezpečnostní politiky. Nikdy totiž není požadován stoprocentní soulad s politikou, jde hlavně o dosažení rozumné míry souladu. V organizacích obvykle není jediné hledisko dosažení maximální bezpečnosti, ale velmi důležitým parametrem je i dostupnost zařízení ICT. Prakticky jsou operační systémy a aplikace velmi složité a změny některých nastavení mohou způsobit nefunkčnost služby nebo celého zařízení. Z tohoto důvodu bezpečnostní manažer, případně auditor, obvykle akceptuje žádosti o výjimky.

Celý tento cyklus se provádí periodicky v určitém časovém intervalu. Dle zkušeností je pro testování politiky obvyklý interval 1–2 měsíce.

Závěr

Použitím nástrojů pro testování bezpečnostní politiky může organizace významně snížit vnitřní i vnější rizika. Otestování politiky umožňuje provést zpětnou kontrolu nastavení zařízení ICT. Bez použití těchto nástrojů je skoro nemožné zjistit celkový stav. Kontrolovat ručně konfigurační parametry je velmi obtížné, ne-li skoro nemožné. Manažerům ICT a bezpečnostním manažerům umožní testování prostřednictvím nástrojů provést nezávislou kontrolu bez detailní znalosti operačního systému a vytvořit z kontroly rutinní činnost. Dále je možné provádět nezávislou kontrolu konfigurace všech zařízení pod správou třetích stran.

Procesní cyklus testování bezpečnostní politiky obvykle splňuje požadavky interních i externích auditorů, dostatečně umožňuje ověření shody mezi požadovanou politikou a skutečností. Nástroje umožňují vytváření reportů ve formátech, které jsou přímo použitelné jako podklady pro auditory. Z tohoto důvodu testování politiky velmi usnadní proces případné certifikace, jelikož auditorům zpravidla stačí předložení aktuálních reportů a seznámení s procesním cyklem testování a řízení výjimek.

Viktor Tichý
tichy@rac.cz

Ing. Viktor Tichý

Absolvent Vysoké školy chemicko-technologické. V současné době pracuje jako samostatný konzultant ve společnosti Risk Analysis Consultants, s. r. o.

POUŽITÉ ZDROJE

[1] Qualys, *POLICY COMPLIANCE GETTING STARTED GUIDE, 2010.*
[2] *ISO/IEC 27002:2005. Code of practice for information security management.*
[3] *CIS, Windows Server 2003 Security Benchmark, 2007.*