ČESKÁ TECHNICKÁ NORMA

ICS 35. 100. 01

Červen 1999

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura bezpečnostního auditu a alarmů

ČSN

ISO/IEC 10181-7

36 9694

idt lTU-TX. 816: 1995

Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework

Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres pour la sécurité dans les systèmes ouverts: Cadre pour l'audit de sécurité et les alarmes

Informationstechnik - Kommunikation Offener Systeme - Rahmenrichtlinien für IT Sicherheit in Offener Systemen: Rahmenrichtlinien für die Sicherheitsalarme

Tato norma je českou verzí mezinárodní normy ISO/IEC 10181-7: 1996. Mezinárodní norma ISO/IEC 10181-7: 1996 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10181-7: 1996. The International Standard ISO/IEC 10181-7: 1996 has the status of a Czech Standard.

Anotace obsahu

Tato mezinárodní norma se zabývá aplikací bezpečnostních služeb auditu a alarmů v prostředí otevřených systémů. Dále rozvíjí koncepci bezpečnostního auditu popsanou v doporučení ITU-T X. 810 | ISO/IEC 10181-1, včetně detekce událostí a činností, které vyplývají z těchto událostí. Zabývá se proto jak bezpečnostním auditem, tak i bezpečnostními alarmy. Zejména definuje základní pojetí bezpečnostního auditu a alarmů, poskytuje obecný model bezpečnostního auditu a alarmů a identifikuje vzájemný vztah služby bezpečnostního auditu a alarmů a ostatních bezpečnostních služeb.

56054

Národní předmluva

Citované normy

ISO/IEC 7498-1: 1994 zavedena v ČSN EN ISO/IEC 7498-1 Informační technologie - Základní referenční model - Základní model (36 9614)

ISO 7498-2: 1989 zavedena v ČSN ISO 7498-2 Systémy na spracovanie informacií - Propojenie otvořených systémov (OSI) - Základný referenčný model - Časť 2: Bezpečnostná architektúra (36 9615)

ISO 7498-4: 1989 zavedena v ČSN ISO 7498-4 Systémy na spracovanie informacií - Propojenie otvořených systémov (OSI) - Základný referenčný model - Časť 4: Základná štruktúra spracovania (36 9617)

ISO/IEC 10164-5: 1993 zavedena v ČSN ISO/IEC 10164-5+Amd. 1 Informační technologie - Propojení otevřených systémů - Management systémů: Funkce managementu podávání zpráv o událostech (36 9679)

ISO/IEC 10164-6: 1993 zavedena v ČSN ISO/IEC 10164-6+Amd. 1 Informační technologie - Propojení otevřených systémů - Management systémů: Funkce řízení zápisů v deníku (36 9679)

ISO/IEC 10164-7: 1992 zavedena v ČSN ISO/IEC 10164-7+Amd. 1 Informační technologie - Propojení otevřených systémů - Management systémů: Funkce podávání bezpečnostních poplašných zpráv (36 9679)

ISO/IEC 10164-8: 1993 zavedena v ČSN ISO/IEC 10164-8 Informační technologie - Propojení otevřených systémů - Management systémů: Funkce bezpečnostního auditního záznamu (36 9679)

ISO/IEC 10181-1: 1996 zavedena v ČSN ISO/IEC 10181-1 Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Přehled (36 9694)

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky κ textu a slovník použitých termínů.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jitka Procházková

MEZINÁRODNÍ NORMA

Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Struktura bezpečnostního auditu a alarmů

ICS 35. 100

ISO/IEC 10181-7

První vydání 1996-08-01

Deskriptory: data processing, information interchange, network interconnection, open systems interconnection, communication procedure, protection of information, security techniques

Obsah

Strana

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří

specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům ke schvalování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících národních orgánů.

Mezinárodní norma ISO/IEC 10181-7 byla připravena Společnou technickou komisí ISO/IEC JTC 1 Informační technologie, subkomisí SC 21 Propojení otevřených systémů, správa dat a otevřené distribuované zpracování, ve spolupráci s ITU-T. Identický text je publikován jako Doporučení ITU-T X. 816.

ISO/IEC 10181 se skládá z následujících částí se společným názvem Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů:

- Část 1: Přehled
- Část 2: Struktura autentizace
- Část 3: Struktura řízení přístupu
- Část 4: Struktura nepopiratelnosti
- Část 5: Struktura důvěrnosti
- Část 6: Struktura integrity
- Část 7: Struktura bezpečnostního auditu a alarmů Přílohy A až D této části ISO/IEC 10181 jsou pouze pro informaci.

Úvod

Toto doporučení | mezinárodní norma dále rozvíjí koncepci bezpečnostního auditu popsanou v doporučení ITU-T X. 810 | ISO/IEC 10181-1, včetně detekce událostí a činností, které vyplývají z těchto událostí. Struktura se proto zabývá jak bezpečnostním auditem, tak i bezpečnostními alarmy.

Bezpečnostní audit je nezávislá revize a přezkoumání systémových záznamů a činností systému. Účelem bezpečnostního auditu je:

- asistovat při identifikaci a analýze neautorizovaných činností nebo útoků;
- pomáhat zajistit, že činnosti mohou být přisuzovány entitám, odpovědným za tyto činnosti;
- přispívat κ vývoji zdokonalených procedur pro kontrolu poškození;

- potvrdit shodu se stanovenou bezpečnostní politikou;

- hlásit informace, které mohou indikovat nedostatky v systémových kontrolách; a

- identifikovat případné nutné změny v kontrolách, politice a procedurách.

V této struktuře je bezpečnostní audit chápán jako zjišťování, shromažďování a zaznamenávání různých událostí týkajících se bezpečnosti v bezpečnostním auditním záznamu a analýza těchto událostí.

Jak audit tak odpovědnost vyžadují, aby informace byly zaznamenávány. Bezpečnostní audit zajišťuje, že je zaznamenáno dostatečné množství informací o běžných a výjimečných událostech, takže pozdější vyšetřování může určit, zda došlo κ narušení bezpečnosti, a pokud ano, které informace nebo jiné zdroje byly kompromitovány. Odpovědnost zajišťuje, že jsou zaznamenány relevantní informace týkající se činností vykonávaných uživateli nebo procesy jednajících v jejich zastoupení tak, že následky těchto činností mohou být později spojeny s dotyčným uživatelem (uživateli), a tento uživatel (uživatelé) může být učiněn zodpovědným za své činnosti. Zajištění služby bezpečnostního auditu může přispět κ zajištění jednoznačné odpovědnosti.

Bezpečnostní alarm je varování vydané vůči individuálnímu uživateli nebo procesu, naznačující, že došlo κ situaci, která může vyžadovat včasný zásah. Účelem služby bezpečnostního alarmu je:

- hlásit skutečné nebo očividné pokusy o narušení bezpečnosti;

- hlásit různé κ bezpečnosti se vztahující události, včetně "normálních" událostí; a

- hlásit události, aktivované dosažením prahových hodnot.

1 Předmět normy

Toto doporučení | mezinárodní norma se zabývá aplikací bezpečnostních služeb v prostředí otevřených systémů, přičemž termín "otevřený systém" zahrnuje takové oblasti jako databáze, distribuované aplikace, otevřené distribuované zpracování a OSI. Bezpečnostní struktury se zaměřují na definování prostředků pro zajištění ochrany systémů a objektů uvnitř systémů a na interakce mezi systémy. Bezpečnostní struktury se nezabývají metodologií konstrukce systémů nebo mechanismů.

Bezpečnostní struktury se zabývají datovými prvky a posloupnostmi operací (ale nikoliv prvky protokolů), které jsou použity κ získání specifických bezpečnostních služeb. Tyto bezpečnostní služby se mohou aplikovat na komunikující entity systémů stejně jako na data vyměňovaná mezi systémy a na data spravovaná systémy.

Účelem bezpečnostního auditu a alarmů, jak je popsáno v tomto doporučení | mezinárodní normě, je zajistit, aby bylo v otevřených systémech s událostmi, které se vztahují κ bezpečnosti, zacházeno v souladu s bezpečnostní politikou příslušné bezpečnostní autority.

Tato struktura zejména:

a) definuje základní pojetí bezpečnostního auditu a alarmů;

b) poskytuje obecný model bezpečnostního auditu a alarmů; a

c) identifikuje vzájemný vztah služby bezpečnostního auditu a alarmů a ostatních bezpečnostních služeb.

Stejně jako ostatní služby bezpečnosti může být bezpečnostní audit zajištěn pouze v kontextu definované bezpečnostní politiky.

6

Model bezpečnostního auditu a alarmů uvedený v článku 6 podporuje rozmanité cíle, které ale nemusí být vždy nutné nebo žádoucí ve specifickém prostředí. Služba bezpečnostního auditu poskytuje auditní autoritu schopnou specifikovat události, které je potřeba zaznamenat v rámci bezpečnostního auditního záznamu.

Tuto strukturu může využívat mnoho různých typů norem, včetně:

1) norem, které zahrnují pojetí auditu a alarmů;

2) norem, které specifikují abstraktní služby obsahující audit a alarmy;

3) norem, které specifikují používání auditu a alarmů;

4) norem, které specifikují prostředky κ poskytnutí auditu a alarmů v architektuře otevřených systémů; a

5) norem, které specifikují mechanismy auditu a alarmů. Tyto normy mohou používat tuto strukturu takto:

- normy typu 1), 2), 3), 4) a 5) mohou využívat názvosloví této struktury;

- normy typu 2), 3), 4) a 5) mohou využívat dílčí služby, definované v článku 8;

- normy typu 5) mohou být založeny na charakteristikách mechanismů definovaných v článku 9.

7