ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen 2014**

Informační technologie – Bezpečnostní techniky – Bezpečnost aplikací – Část 1: Přehled a pojmy

ČSN ISO/IEC 27034-1
36 9703

Information Technology – Security techniques – Application security –
Part 1: Overview and concepts

Technologies de l,information – Techniques de sécurité – Sécurité des applications –
Partie 1: Aperçu général et concepts

Tato norma je českou verzí mezinárodní normy ISO/IEC 27034-1:2011. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27034-1:2011. It was translated
by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 27000:2009 nezavedena

ISO/IEC 27001:2005 nezavedena

ISO/IEC 27002:2005 nezavedena

ISO/IEC 27005:2011 zavedena v ČSN ISO/IEC 27005:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Souvisící ČSN

ČSN ISO/IEC 2382-7:2002 (36 9001) Informační technologie – Slovník – Část 7: Programování počítačů

ČSN EN ISO 9000:2006 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN ISO/IEC 9126-1 (36 9020) Softwarové inženýrství – Jakost produktu – Část 1: Model jakosti

ČSN P ISO/IEC 15000-1 (97 9739) Rozšiřitelný vyznačovací jazyk pro elektronický byznys (ebXML) – Část 1: Profil protokolu o spolupráci a specifikace dohody (ebCPP)

ČSN ISO/IEC 15408-3 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit:

- překlad anglického termínu „control“ preferovaně jako „opatření“ z důvodu návaznosti na vydané normy řady 27000;
- anglické termíny „bug bars“ (A.9.6), „high water mark“ (B.1.8) v původním tvaru vzhledem k neexistenci českého ekvivalentu;
- anglický termín „outsourcing“ a od něho odvozené termíny v původním tvaru vzhledem k rozšíření tohoto termínu v odborné komunitě.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27034-1
Bezpečnost aplikací – Část 1: Přehled a pojmy První vydání
2011-11-15

ICS 35.040

Obsah

Strana

Tabulky

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO nebo 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 další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních
norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv.
ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 27034-1 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

ISO/IEC 27034 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – Bezpečnost aplikací:*

- *Část 1: Přehled a pojmy*

Následující části se připravují:

- *Část 2: Normativní rámec organizace*
- *Část 3: Proces řízení bezpečnosti aplikací*
- *Část 4: Validace bezpečnosti aplikací*
- *Část 5: Protokoly a struktura řídících dat bezpečnosti aplikací*

Úvod

0.1 Obecně

Organizace by měly chránit své informační a technologické infrastruktury, aby se udržely v podnikání. Tradičně toto bylo řešeno na úrovni IT ochranou perimetru a takových komponent technologické

infrastruktury jako jsou počítače a sítě, což je obecně nedostatečné.

Kromě toho se organizace stále více chrání samy na úrovni vlastního řízení provozováním formalizovaných, testovaných a ověřených systémů řízení bezpečnosti informací (ISMS). Systematický přístup přispívá k efektivnímu systému řízení bezpečnosti informací, jak je popsáno v ISO/IEC 27001.

Nicméně organizace čelí stále rostoucí potřebě chránit své informace na aplikační úrovni.

Aplikace by měly být chráněny před zranitelnostmi, které by mohly být inherentní vzhledem k samotné aplikaci (například vady softwaru), objeví se v průběhu životního cyklu aplikace (například prostřednictvím změn aplikace), nebo vznikají v důsledku použití aplikace v kontextu, pro který nebyla určena.

Systematický přístup ke zvýšení bezpečnosti aplikací poskytuje důkaz, že informace používaná nebo uchovávaná aplikacemi organizace je přiměřeně chráněna.

Aplikace mohou být získány prostřednictvím interního vývoje, outsourcingu nebo zakoupením komerčního
produktu. Aplikace mohou být rovněž získány prostřednictvím kombinace těchto přístupů, které by mohly zavést nové bezpečnostní dopady, jež by měly být vzaty v úvahu a měly by být řízeny.

Příklady aplikací jsou systémy lidských zdrojů, finanční systémy, systémy pro zpracování textu, systémy řízení vztahů se zákazníky, firewally, antivirové systémy a systémy detekce průniku.

Po celou dobu svého životního cyklu vykazuje bezpečná aplikace předpokládané charakteristiky kvality softwaru, jako je předvídatelné provedení a soulad, stejně jako splnění bezpečnostních požadavků z hlediska vývoje, řízení, technické infrastruktury a auditu. Procesy a postupy se zvýšenou bezpečností – a kvalifikovaní lidé pro jejich vykonávání – jsou nutné k vytvoření důvěryhodných aplikací, které nezvyšují vystavení riziku nad přijatelnou nebo přípustnou úroveň zbytkového rizika a podporují efektivní ISMS.

Bezpečná aplikace navíc bere v úvahu bezpečnostní požadavky, které vyplývají z typu dat, cílového prostředí (kontext činnosti organizace, regulatorní a technologické kontexty), aktivních účastníků a specifikací aplikace. Mělo by být možné získat důkaz prokazující dosažení přijatelné (nebo tolerovatelné) úrovně zbytkového rizika a udržování této úrovně.

0.2 Účel

Účelem ISO/IEC 27034 je pomoci organizacím v bezproblémové integraci bezpečnosti v průběhu celého životního cyklu jejich aplikací pomocí:

a. poskytování konceptů, zásad, rámců, komponent a procesů;
b. poskytování procesně orientovaných mechanismů pro ustanovení bezpečnostních požadavků, odhadnutí bezpečnostních rizik, přiřazení cílené úrovně důvěry a výběru odpovídajících bezpečnostních opatření a ověřovacích opatření;
c. poskytování směrnic pro stanovení akceptačních kritérií pro organizace, zajišťující vnějšími zdroji vývoj nebo provoz aplikací, a pro organizace nakupující aplikace od třetích stran;
d. poskytování procesně orientovaných mechanismů pro určování, vytváření a shromažďování důkazů potřebných k prokázání, že jejich aplikace může být v definovaném prostředí bezpečně používána;
e. podpory obecných pojmů specifikovaných v ISO/IEC 27001 a asistence s vyhovující implementací bezpečnosti informací založené na přístupu řízení rizik; a
f. poskytování rámce, který pomáhá k implementaci opatření bezpečnosti uvedených v ISO/IEC 27002 a dalších normách.

ISO/IEC 27034:

a. se vztahuje na základní software aplikace a na přispívající faktory, které ovlivňují její bezpečnost, jako jsou data, technologie, procesy životního cyklu vývoje aplikací, podpůrné procesy a aktivní účastníky; a
b. se vztahuje na organizace všech velikostí a typů (například komerční společnosti, vládní úřady, neziskové organizace), které jsou vystaveny rizikům souvisejícím s aplikacemi.

ISO/IEC 27034 neposkytuje:

a. směrnice pro fyzickou bezpečnost a bezpečnost sítí;
b. opatření nebo měření;
c. specifikace bezpečného programování pro žádný programovací jazyk.

ISO/IEC 27034 není:

a. normou pro vývoj softwarových aplikací;
b. normou pro řízení projektů aplikací;
c. normou pro životní cyklus vývoje softwaru.

Požadavky a postupy uvedené v ISO/IEC 27034 nejsou určeny pro izolovanou implementaci, ale spíše pro
integraci do stávajících procesů organizace. Za tímto účelem by organizace měly namapovat své stávající
procesy a rámce na procesy a rámce navrhované normou ISO/IEC 27034 a tím snížit dopad implementace ISO/IEC 27034.

Příloha A (informativní) uvádí příklad, ilustrující jak může být stávající proces vývoje softwaru namapován
do některé z komponent a procesů ISO/IEC 27034. Obecně řečeno, organizace používající libovolný vývojový
životní cyklus by měla provést namapování stejně, jako je popsáno v příloze A, a přidat jakékoliv chybějící
komponenty či procesy potřebné pro dosažení souladu s ISO/IEC 27034.

0.3 Cílové skupiny

0.3.1 Obecně

Následující cílové skupiny budou při vykonávání svých rolí stanovených v organizaci profitovat z ISO/IEC 27034:

a. manažeři;
b. zajišťovací a provozní týmy;
c. akviziční pracovníci;
d. dodavatelé; a
e. auditoři.

0.3.2 Manažeři

Manažeři jsou osoby účastnící se řízení a správy aplikace během jejího celého životního cyklu. Příslušné fáze životního cyklu aplikace zahrnují etapy pořizování a etapy výroby. Příklady manažerů jsou:

a. manažer bezpečnosti informací;
b. projektový manažer;

c. administrátor;
d. nabyvatelé softwaru;
e. manažer vývoje softwaru;
f. vlastníci aplikací;
g. linioví manažeři, kteří dohlížejí na zaměstnance.

Manažeři typicky potřebují:

a. zajistit rovnováhu mezi náklady na implementaci a udržování bezpečnosti aplikace a riziky a hodnotou, kterou představuje pro organizaci;
b. přezkoumat zprávy auditora doporučující přijetí nebo odmítnutí založené na tom, zda aplikace dosáhla a udržela cílenou úroveň důvěry;
c. zajistit shodu s normami, zákony a předpisy v souladu s regulatorním kontextem dané aplikace (viz 8.1.2.2);
d. dohlížet na implementaci bezpečné aplikace;
e. schválit cílenou úroveň důvěry podle specifického kontextu organizace;
f. určit, která bezpečnostní opatření a odpovídající ověřovací měření by měla být implementována a testována;
g. minimalizovat náklady na ověření bezpečnosti aplikace;
h. dokumentovat bezpečnostní politiky a postupy pro aplikaci;
i. poskytovat povědomí o bezpečnosti, školení a dohled pro všechny aktivní účastníky;
j. zavést náležité prověrky v oblasti bezpečnosti informací požadované příslušnými politikami a postupy bezpečnosti informací; a
k. udržovat krok se všemi bezpečnostními plány týkajícími se systému v rámci sítě organizace.

0.3.3 Zajišťovací a provozní týmy

Členové zajišťovacích a provozních týmů (nazývané projektový tým) jsou osoby podílející se na návrhu, vývoji a údržbě aplikace v průběhu celého jejího životního cyklu. Mezi členy patří:

a. architekti,
b. analytici,
c. programátoři,
d. testeři,
e. systémoví administrátoři,
f. databázoví administrátoři,
g. síťoví administrátoři, a
h. technický personál.

Členové typicky potřebují:

a. pochopit, jaká opatření by měla být použita v každé fázi životního cyklu aplikace a proč;
b. pochopit, jaká opatření by měla být implementována v samotné aplikaci;
c. minimalizovat dopad zavedení opatření na vývojové, testovací a dokumentační činnosti v rámci životního cyklu aplikace;
d. získat ujištění, že zavedená opatření splňují požadavky souvisejících měření;
e. získat přístup k nástrojům a osvědčeným postupům s cílem zjednodušit vývoj, testování a dokumentaci;
f. usnadnit vzájemné přezkoumání;
g. podílet se na plánování a strategii akvizic;
h. navázat obchodní vztahy pro získání potřebného zboží a služeb (například pro akvizice, hodnocení a zadávání kontraktů); a
i. zajistit právo disponovat se zbytkovými položkami po dokončení práce (například správa/likvidace majetku).

0.3.4 Nabyvatelé

Zahrnuje všechny osoby zapojené do získávání produktu nebo služby.

Nabyvatelé typicky potřebují:

a. připravit žádosti o nabídky, které zahrnují požadavky na bezpečnostní opatření;
b. vybrat dodavatele, kteří splňují tyto požadavky;
c. ověřit důkazy o bezpečnostních opatřeních uplatňovaných u externě poskytovaných služeb, a
d. hodnotit produkty na základě ověření důkazů o správně implementovaných bezpečnostních opatření aplikace.

0.3.5 Dodavatelé

Zahrnuje všechny osoby zapojené do dodávání produktu nebo služby.

Dodavatelé typicky potřebují:

a. splňovat bezpečnostní požadavky aplikace uvedené v žádosti o nabídku;
b. zvolit vhodná bezpečnostní opatření aplikace pro nabídku, s ohledem na jejich dopad na náklady; a
c. prokázat, že požadovaná opatření jsou u nabídnutých výrobků nebo služeb správně implementována.

0.3.6 Auditoři

Auditoři jsou osoby, které potřebují:

a. pochopit rozsah a postupy používané při ověřovacích měřeních odpovídajících opatření;
b. zajistit, aby výsledky auditu byly opakovatelné;
c. vytvořit seznam ověřovacích měření vytvářejících důkazy, že aplikace dosáhla cílené úrovně důvěry vyžadované vedením; a
d. uplatňovat standardizované auditní procesy založené na použití ověřitelných důkazů.

0.3.7 Uživatelé

Uživatelé jsou osoby, které potřebují:

a. důvěru, že použití a nasazení aplikace je považováno za bezpečné;
b. důvěru, že aplikace vytváří spolehlivé výsledky konzistentně a včas; a
c. důvěru, že opatření a jejich odpovídající ověřovací měření jsou dle očekávání správně umístěny a správně fungují.

0.4 Principy

0.4.1 Bezpečnost jako požadavek

Bezpečnostní požadavky by měly být definovány a analyzovány pro každou fázi životního cyklu aplikace,
adekvátně řešeny a průběžně řízeny.

S bezpečnostními požadavky aplikace (viz 6.4) by mělo být zacházeno stejným způsobem jako s požadavky na funkčnost, kvalitu a použitelnost (viz ISO/IEC 9126 pro příklad modelu kvality). Kromě toho by měly být ustanoveny s bezpečností související požadavky na shodu se zavedenými omezeními zbytkového rizika.

Podle ISO/IEC/IEEE 29148 (připravováno) by požadavky měly být nezbytné, abstraktní, jednoznačné, konzistentní, úplné, stručné, proveditelné, sledovatelné a ověřitelné. Stejné vlastnosti platí pro bezpečnostní požadavky. Příliš často se v dokumentaci k projektům aplikací setkáváme s nejasnými

bezpečnostními požadavky, jako například „Vývojový pracovník by měl odhalit všechna významná bezpečnostní rizika pro aplikaci“.

0.4.2 Bezpečnost aplikace je kontextově závislá

Bezpečnost aplikace je ovlivněna definovaným cílovým prostředím. Typ a rozsah bezpečnostních požadavků aplikace jsou určeny riziky, kterým je aplikace vystavena, což závisí na třech kontextech:

a. kontext činnosti organizace: specifická rizika vyplývající z oblasti činnosti organizace (telefonní společnost, dopravní společnost, vláda, apod.);
b. regulatorní kontext: specifická rizika vyplývající z geografické polohy místa podnikání organizace (práva duševního vlastnictví a licencování, omezení týkající se ochrany kryptografie, autorské právo, zákony a předpisy, zákony na ochranu soukromí, atd.);
c. technologický kontext: specifická rizika technologií používaných organizací během podnikání [reverzní inženýrství, bezpečnost sestavovacích nástrojů, ochrana zdrojového kódu, použití předkompilovaného kódu třetí strany, testování bezpečnosti, penetrační testy, kontrola omezení, kontrola kódu, prostředí informačních a komunikačních technologií (ICT), ve kterém běží aplikace, konfigurační soubory a nezkompilovaná data, privilegia operačního systému pro instalaci a/nebo provoz, údržbu, bezpečnou distribuci, atd.].

    Technologický kontext zahrnuje technické specifikace aplikace (bezpečnostní funkce, bezpečné komponenty, on-line platby, bezpečný záznam formou logu, kryptografie, správa oprávnění, atd.).

Organizace může tvrdit, že aplikace je bezpečná, ale toto tvrzení je platné pouze pro tuto konkrétní organizaci v jejích specifických kontextech činnosti a regulatorních a technologických kontextech. Pokud se například změní technologická infrastruktura aplikace nebo je aplikace používána ke stejným účelům v jiné zemi, mohou mít tyto nové kontexty dopad na bezpečnostní požadavky a cílenou úroveň důvěry. Aktuální bezpečnostní opatření aplikace již nemusí adekvátně reagovat na nové bezpečnostní požadavky a aplikace by již nemusely být bezpečné.

0.4.3 Přiměřené investice pro bezpečnost aplikace

Náklady na použití bezpečnostních opatření a provádění auditních měření by měly být úměrné k cílené úrovni důvěry (viz 8.1.2.6.4) požadované vlastníkem aplikace nebo vedením.

Tyto náklady lze považovat za investici, protože snižují náklady, odpovědnosti vlastníka aplikace a právní
důsledky narušení bezpečnosti.

0.4.4 Bezpečnost aplikace by měla být prokázána

Proces auditu aplikace v ISO/IEC 27034 (viz 8.5) využívá ověřitelných důkazů poskytnutých bezpečnostními opatřeními aplikace (viz 8.1.2.6.5).

Aplikace nemůže být prohlášena za bezpečnou, pokud auditor nesouhlasí s tím, že podpůrné důkazy generované odpovídajícími ověřovacími měřeními příslušných bezpečnostních opatření aplikace prokazují dosažení cílené úrovně důvěry stanovené vedením.

0.5 Vztah k jiným mezinárodním normám

0.5.1 Obecně

Obrázek 1 ukazuje vztahy mezi ISO/IEC 27034 a dalšími mezinárodními normami.

Obrázek 1 – Vztah k jiným mezinárodním normám

0.5.2 ISO/IEC 27001, Systémy řízení bezpečnosti informací – Požadavky

ISO/IEC 27034 pomáhá realizovat, s rozsahem omezeným na bezpečnost aplikací, doporučení z normy ISO/IEC 27001. Používají se zejména následující postupy:

a. systematický přístup k řízení bezpečnosti;
b. procesní přístup „Plánovat, Dělat, Kontrolovat, Jednat“; a
c. implementace bezpečnosti informací založená na řízení rizik.

0.5.3 ISO/IEC 27002, Soubor postupů pro opatření bezpečnosti informací

ISO/IEC 27002 stanovuje postupy, které organizace mohou implementovat jako bezpečnostní opatření aplikace, jak je navrženo v ISO/IEC 27034. Nanejvýš zajímavá jsou opatření z následujících kapitol v ISO/IEC 27002:2005:

a. kapitola 10: Řízení komunikací a provozu;
b. kapitola 11: Řízení přístupu; a co je nejdůležitější
c. kapitola 12: Akvizice, vývoj a údržba informačních systémů.

0.5.4 ISO/IEC 27005, Řízení rizik bezpečnosti informací

ISO/IEC 27034 pomáhá realizovat, s rozsahem omezeným na bezpečnost aplikací, proces řízení rizik předložený v ISO/IEC 27005. Viz příloha C (informativní) pro podrobnější diskusi.

0.5.5 ISO/IEC 21827, Inženýrství zabezpečení systémů – Model vyzrálosti způsobilosti (SSE-CMMR)

ISO/IEC 21827 poskytuje základní postupy inženýrství zabezpečení, které mohou organizace implementovat jako bezpečnostní opatření aplikace, jak je navrženo v ISO/IEC 27034. Kromě toho procesy z ISO/IEC 27034 přispívají k dosažení několika způsobilostí, které definují úrovně způsobilostí v ISO/IEC 21827.

0.5.6 ISO/IEC 15408-3, Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ISO/IEC 15408-3 uvádí požadavky a akční prvky, které mohou organizace implementovat jako bezpečnostní opatření aplikace, jak je navrženo v ISO/IEC 27034.

0.5.7 ISO/IEC TR 15443-1, Struktura záruky IT bezpečnosti – Část 1: Přehled a struktura, a ISO/IEC TR 15443-3, Struktura záruky IT bezpečnosti – Část 3: Analýza metod záruky

ISO/IEC 27034 pomáhá prosazovat a reflektovat zásady záruky bezpečnosti z ISO/IEC TR 15443-1 a přispět k případům záruky v ISO/IEC TR 15443-3.

0.5.8 ISO/IEC 15026-2, Systémy a softwarové inženýrství – Systémy a záruky softwaru – Část 2: Případ záruky

Použití procesů a bezpečnostních opatření aplikace z ISO/IEC 27034 v projektech aplikací přímo poskytuje případy záruky bezpečnosti aplikace. Zejména,

a. tvrzení a jejich ospravedlnění jsou poskytovány procesem analýzy rizik bezpečnosti aplikace,
b. důkazy jsou poskytnuty vestavěnými ověřovacími měřeními bezpečnostních opatření aplikace, a
c. soulad s ISO/IEC 27034 může být použit jako argument v mnoha takových případech záruky.

Viz také 8.1.2.6.5.1.

0.5.9 ISO/IEC 15288, Systémy a softwarové inženýrství – Procesy v životním cyklu systému, a ISO/IEC 12207, Informační technologie – Procesy v životním cyklu softwaru

ISO/IEC 27034 poskytuje dodatečné postupy pro organizaci, stejně jako bezpečnostní opatření aplikace, které organizace může vložit jako dodatečné aktivity do svých stávajících systémů a procesů životního cyklu softwarového inženýrství, jak je uvedeno v ISO/IEC 15288 a ISO/IEC 12207.

0.5.10 ISO/IEC TR 29193 (připravuje se), Inženýrské principy a techniky bezpečného systému

ISO/IEC TR 29193 poskytuje návod pro inženýrství bezpečných systémů pro ICT systémy nebo produkty, které organizace mohou implementovat jako bezpečnostní opatření aplikace, jak je navrženo v ISO/IEC 27034.

1 Předmět normy

ISO/IEC 27034 poskytuje návod s cílem pomoci organizacím integrovat bezpečnost do procesů používaných pro správu a řízení jejich aplikací.

Tato část ISO/IEC 27034 podává přehled o bezpečnosti aplikací. Zavádí definice, pojmy, principy a procesy související s bezpečností aplikací.

ISO/IEC 27034 je použitelná pro aplikace vyvíjené v organizaci, aplikace získané od třetích stran, a pro aplikace, u kterých je vývoj nebo provoz aplikace zajištěn externě.