Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Teze bakalářské práce

Bezpečnostní analýza webové aplikace

Matěj Řezníček

© 2015 ČZU v Praze

Souhrn

Tato práce se zabývá kvalitativní analýzou rizik webové aplikace určené pro bytová družstva a společenství vlastníků jednotek. Teoretická část práce obsahuje východiska pro analýzu, základní rozdělení metodik, které lze pro analýzu využít, a popis vybraných z nich. Dále jsou zde rozebrány postupy, jak identifikovat a kvantifikovat aktiva, hrozby a zranitelnosti a z daných hodnot vypočítat hodnoty rizik. V analytické části jsou výše uvedené postupy aplikovány. Výsledkem práce je seznam rizik působících na tuto aplikaci včetně jejich stanovené hodnoty a návrh opatření, která by mohla, v případě zavedení, zjištěná rizika zmírňovat.

Klíčová slova: analýza rizik, webová aplikace, informační systém, informace, data, informační bezpečnost, aktiva, hrozby, zranitelnosti, protiopatření

Cíle práce

Cílem předložené práce je zpracovat analýzu rizik webové aplikace a poskytnout tak jejímu provozovateli informace o tom, jakým hrozbám jsou aktiva podílející se na provozu této aplikace vystavena a jaká opatření připadají v úvahu, pokud se společnost rozhodne rizika snižovat.

Metodika práce

Pro zpracování práce byly využity zejména odborné knižní publikace zabývající se bezpečností a zabezpečením informací a analýzou rizik informačních systémů. Dalšími podklady pro zpracování bakalářské práce byly odborné články z tištěných i elektronických médií zabývajících se problematikou analýzy rizik a normy pokrývající oblast bezpečnosti informací. Na základě poznatků získaných studiem uvedené literatury byla provedena kvalitativní analýza rizik konkrétní webové aplikace.

Řešená problematika

V současné době si již uživatelé moderních technologií zvykli, že takřka veškeré služby, které chtějí nebo potřebují v běžném životě využívat, mohou obsluhovat pomocí internetu z pohodlí domova. Přináší to s sebou však kromě komfortu také bezpečnostní rizika. Proti těmto rizikům se jednak musí chránit samotný uživatel, větší zodpovědnost

však leží na poskytovateli služby, který musí kromě ochrany vlastních systémů zajistit také bezpečnost dat, která mu uživatel svěřil.

Ke zjištění, jaká rizika na konkrétní systémy působí a jak se proti nim lze chránit, slouží analýza rizik.

Struktura práce

Předložená práce je rozdělena do sedmi hlavních kapitol – Úvod, Cíl práce a metodika, Teoretická východiska, Popis analyzované aplikace, Analytická část, Výsledky analýzy rizik a Závěr.

Teoretická část práce (třetí kapitola) obsahuje východiska pro analýzu. Je zde rozebráno jak vystupují informace v podniku, jakou mají pro obchodní společnosti hodnotu a proč a jak je chránit. Dále jsou v této části práce vysvětleny základní pojmy analýzy rizik (aktivum, hrozba, zranitelnost, protiopatření, riziko), vztahy mezi nimi a způsoby zvládání rizik (monitoring, retence,redukce, pojištění, transfer a sdílení, vyhnutí se riziku). Hlavním prvkem teoretické části je rozbor postupu analýzy, která se skládá z identifikace a kvantifikace aktiv, hrozeb a zranitelností a vyhodnocení samotných rizik.

Ve čtvrté kapitole je uveden stručný uživatelský popis analyzované aplikace.

Analytická část práce, pátá kapitola, obsahuje samotnou analýzu rizik. Jsou zde ilustrovány postupné kroky procesu stanovení hodnoty aktiv, hrozeb, zranitelností a rizik.

V šesté kapitole – Výsledky analýzy rizik – jsou prezentovány zjištěné skutečnosti.

Zhodnocení a závěry práce

V rámci analýzy rizik bylo identifikováno celkem 181 rizik působících na danou aplikaci, respektive společnost. Z toho bylo 0 z kategorie kritických, 10 vysokých, 51 středních a 119 nízkých. Nejvíce ohroženým aktivem je samotná aplikace a největší hrozbou pro společnost je selhání softwaru.

Pro řešení nízkých a středních rizik byl připraven seznam protiopatření, která by mohla být ve společnosti zavedena, aby tato rizika minimalizovala. U každého protiopatření je uveden jeho popis, informace o tom, na jaká rizika nalezená v rámci analýzy působí, a také jaká je jeho odhadovaná efektivita, náročnost zavedení, časová náročnost a náklady na zavedení a provoz.

Vedení bylo na základě zjištěných skutečností doporučeno zavést proces hlášení a evidence bezpečnostních incidentů, zavést pravidelnou kontrolu nastavení přístupových

oprávnění, stanovit pravidla pro přidělování a správu privilegovaných účtů a zavést provozní deník. Tato opatření jsou snadno zaveditelná, relativně nenákladná a poskytnou vedení firmy konkrétnější informace o tom, co a kdy se v systému děje. Vzhledem k tomu, že analýzou nebylo nalezeno žádné kritické riziko, bylo doporučeno zavedení dalších, náročnějších, případně nákladnějších opatření naplánovat v delším časovém horizontu, kdy už bude management společnosti disponovat informacemi získanými prostřednictvím výše uvedených opatření.

Seznam vybrané použité literatury

1. MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, c2007, vi, 154 s. ISBN 978-80-251-1511-4.
2. RODRYČOVÁ, Danuše a Pavel STAŠA. *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha: Grada, 2000, 143 s. Manažer. ISBN 80-716-9144-5.
3. ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Brno: Tribun EU, 2009, 134 s. Knihovnicka.cz. ISBN 978-80-7399-731-1.