Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Informační bezpečnost agendového systému webového typu v orgánu státní správy

Bc. Smetana Roman

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Roman Smetana

Hospodářská politika a správa
Veřejná správa a regionální rozvoj

Název práce

Informační bezpečnost agendového systému webového typu v orgánu státní správy

Název anglicky

Information security of the web-type agenda system in the state administration

---

Cíle práce

Hlavním cílem diplomové práce je analýza a návrh ochrany agendových informačních systémů používaných pro administraci úkolů v oblasti věcné působnosti orgánů státní správy.
Dílčí cíle:
Analýza jednotlivých funkčních komponent a vrstev vybraného informačního systému státní správy včetně návrhu všech opatření, která by umožnila stanovit vyšší úroveň zabezpečení systému jako celku.

Metodika

1. Teoretická východiska, studium a analýza odborných informačních zdrojů
2. Analýza vybraného informačního systému, jeho jednotlivých komponent a vrstev
3. Stanovení kritérií pro hodnocení zabezpečení vybraného systém dle OWASP. (vícekriteriální analýza)
4. Identifikace slabých a zranitelných míst vybraného systému
5. Návrh na zlepšení ochrany systémů využívaných pro podporu činnosti státní správy

Doporučený rozsah práce

70

Klíčová slova

Agendový informačních systém

Doporučené zdroje informací

DOUCEK, P. *Řízení bezpečnosti informací : 2. rozšířené vydání o BCM*. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

RAIN, T. – ŠVARCOVÁ, I. *Informační management*. Praha: Alfa, 2011. ISBN 978-80-87197-40-0.

RAIS, K. – SMEJKAL, V. *Řízení rizik*. Praha: Grada, 2003. ISBN 80-247-0198-7.

RAO, Umesh Hodeghatta a Umesha NAYAK. The InfoSec handbook: an introduction to information security [online]. New York, New York: Apress, [2014] [cit. 2019-06-02]. Expert's voice in information security. ISBN 14-302-6382-2. Dostupné z: DOI: 10.1007/978-1-4302-6383-8

TOMAN, P. – POUR, J. – GÁLA, L. – ČESKÁ SPOLEČNOST PRO SYSTÉMOVOU INTEGRACI. *Podniková informatika : počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky*. Praha: Grada, 2006. ISBN 80-247-1278-4.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Karel Kubata, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 26. 8. 2019

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 02. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci, Informační bezpečnost agendového systému webového typu v orgánu státní správy, jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. března 2020

Poděkování

Rád bych touto cestou poděkoval Ing. Karlu Kubatovi Ph.D. za přínosné a podnětné připomínky v rámci řízení mé práce.

Informační bezpečnost agendového systému webového typu v orgánu státní správy

Abstrakt

Diplomová práce „Informační bezpečnost agendového systému webového typu v orgánu státní správy“ hodnotí aktuální stav zabezpečení informačního prostředí v orgánu státní správy a srovnává jeho aspekty v rovině normativní, legislativní, vládních koncepcí a dále i s faktickou úrovní ve vybrané sféře soukromého sektoru. Primárním základem, od kterého se odvíjí, jsou obecné principy zabezpečení informací, které úzce souvisí s historickým vývojem kybernetiky jako celku a vychází z teoretických předpokladů souvisejících s hodnotou informace jako takové. Zaměřuje se však detailně na konkrétní typ informačního systému. Jejím hlavním cílem zůstává ověření a návrh ochrany agendových informačních systémů používaných pro administraci úkolů v oblasti věcné působnosti orgánů státní správy. Provede analýzu jednotlivých funkčních komponent a vrstev vybraného informačního systému státní správy, včetně návrhu všech opatření, která by umožnila stanovit vyšší úroveň zabezpečení systému jako celku. Měla by též upozornit na možná rizika a specifika provozování systémů ve státních institucích a dopady legislativních změn v rámci životního cyklu aplikací s důrazem na informační bezpečnost. Praktický přínos by měl spočívat v uchopení a osvojení postupů ověřování a zajišťování informační bezpečnosti, použitelné pro nejběžnější typ využívaných aplikací ve státní správě. Stejné postupy pak poskytnout pro zadávání veřejných zakázek, i realizaci bezpečnostních testů vlastními prostředky, a to jak ve státní sféře, tak na úrovni regionálních a místních samospráv.

Klíčová slova: Informační bezpečnost, kybernetická bezpečnost, správa zranitelností, eGovernment, Zákon o kybernetické bezpečnosti, analýza rizik, agendový informační systém, webová aplikace, penetrační testování, OWASP.

Information security of the web-type agenda system in the state administration

Abstract

The diploma thesis “Information security of web-type agenda system in state administration body” evaluates the current state of security of the information environment in the state administration body and compares its aspects on the level of normative, legislative, governmental concepts and also with the actual level in the selected sphere of the private sector. The primary basis on which to develop is the general principles of securing information that is closely related to the historical evolution of cybernetics as a whole and is based on theoretical assumptions related to the value of information as such. However, it focuses in detail on an information system. Its main aim is to analyse and propose protection of agendas information systems used for administration of tasks in the area of substantive competence of state administration bodies. Analysis of individual functional components and layers of a selected state administration information system, including the design of all measures that would allow for a higher level of security of the system. It should also draw attention to the possible risks and specifics of operating systems in state institutions and the impact of legislative changes in the life cycle of applications with an emphasis on information security. Practical benefits should be in grasping and mastering authentication and information security practices, applicable to the most common type of government administration applications used. Provide the same procedures for public procurement as well as conducting security tests by their own means, both in the state sphere and at the level of regional and local authorities.

Keywords: Information security, cyber security, vulnerability management, eGovernment, Cyber security law, risk analysis, agenda information system, web application, penetration testing, OWASP.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AIS – Agendový informační systém
ANSI – American National Standard Institute
APKB – Akční plán kybernetické bezpečnosti
ARPANET – Advanced Research Projects Agency Network
ASVS – Application Security Verification Standard
BI – Bussiness Intelligence
BMIS – Bussiness Model for Information Security
BSI – British Standards Institute
CAPEC – Common Attack Pattern Enumeration and Enumeration and Classification
CERT – Computer Emergency Response Team
CMS – Content Management System – redakční systém
CMS2 – Centrální místo služeb druhé generace
COBIT – Control Objectives for Information and Related Technology
CSIRT – Computer Security Incident Response Team
CVE – Common Vulnerabilities and Exposures
CVSS – Common Vulnerability Scoring Systém
CWE – Common Weakness Enumeration
FLOSS – Free/Libre and Open-Source Software
GDPR – General Data Protection Regulation
GovCERT – Vládní CERT
IEEE – Institute Electrical and Electronic Engineers
ICT – Information and Communication Technologies
IKT – Informační a komunikační technologie (z ang. ICT)
ISACA – Information Systems Audit and Control Association

ISG – Information Security Governance
ISMS – Information Management Systém
ISO – Institut Standard Organization
IS o ISVS – Informační systém o ISVS
ISSAF – Information Systems Security Assessment Framework
ISVS – Informační systémy veřejné správy
IT – Informační technologie
ITIL – IT infrastructure Library
NBÚ – Národní bezpečnostní úřad
NCKB – Národní centrum kybernetické bezpečnosti
NSA – National Security Agency
NSKB – Národní strategie kybernetické bezpečnosti
NIST – National Institute of Standards and Technology
OISSG – Open Information Systems Security Group
OSSTMM – Open Source Security Testing Metodical Guide
OVM – Orgán veřejné moci
OWASP – Open Web Application Security Project
PDCA – Princip Demingova modelu (Plan, Do, Check, Act)
ROB – Registr fyzických osob (občanů)
RPP – Registr práv a povinností
SBOM – Software Bill-Of-Materials
SDLC – Systems Development Life Cycle
SIG – Special Interest Group
SRRVS – Strategický rámec rozvoje veřejné správy
ÚNMZ – Ústav pro normalizaci, meteorologii a zkušebnictví
WASC – Web Aplication Security Consortium
WWW – World Wide Web
ZAP – Zed Attack Proxy
ZoKB – Zákon o kybernetické bezpečnosti

Úvod

Chceme-li zkoumat informační bezpečnost, je vhodné si nejdříve uvědomit, jaký význam mají oba výrazy. Co je to vlastně informace a co bezpečnost? Tato práce se snaží tyto pojmy nejen zasadit do kontextu v procesu zkoumajícího okrajově aktuální stav informační společnosti, ale brát je v potaz i při detailní analýze konkrétního informačního systému. Je nutné mít neustále na paměti jejich základní funkci, a to především s ohledem na praktický přínos pro reálné, existující služby, ke kterým se zákonitě vztahuje. Otázky, které si klade, totiž souvisí předně s fungováním státu v aktuálním informačním prostředí, včetně na něj působících hrozeb. Jak toto prostředí vypadá dnes a jak by mělo vypadat? Čím se řídí úroveň zabezpečení ve státní správě a kam směřuje Česká republika v poskytování elektronických služeb? Jsou služby poskytované státem dostatečně chráněny a je možné se na ně spolehnout? Tyto a další otázky souvisejí s hlavním tématem této práce a tvoří osu analýz, směřující k podrobnému poznání jednotlivých vrstev vybraných typů informačních systémů veřejné správy a snaží se upozornit na bezpečnostní aspekty a možná rizika. Odpovědi mohou přinést poznatky využitelné v praxi, především specialistům, kteří se zaměřují na oblast kybernetické bezpečnosti, ale i širší odborné veřejnosti. Také osvětlují některé bezpečnostní aspekty v legislativní oblasti, kde není vždy zcela jasné, jaká technická a technologická opatření se skrývají za jednotlivými paragrafy zákonů, kterými se státní instituce primárně řídí, a to i přes existenci upřesňujících prováděcích vyhlášek a jejich příloh. V některých částech práva nechává zákon jistou míru benevolence, a to z důvodu výrazného technologického rozvoje v oblasti informačních technologií, který není dostatečně rychle akcentován ve schvalovaných předpisech zákonného typu, a oplývá trvale jistou časovou prodlevou. Zde leží tíha odpovědnosti na správném rozhodování odborníků v oblasti informačního managementu, opírajícího se o širší bezpečnostní povědomí, vycházející i z jiných norem a aktuálních poznatků osvědčené praxe (přeneseně z ang. best practice). Ti jsou odpovědní za ověření informační bezpečnosti prostřednictvím externích dodavatelů, tedy pomocí zadávání veřejných zakázek, nebo vlastními prostředky, a to jak v oblasti státní správy, tak na úrovni regionálních a místních samospráv. Je tedy podstatné poskytnout, pro ne vždy jednoduché rozhodování, podklady v podobě ověřených závěrů. Ty by měly být výsledkem zkoumání konkrétního agendového systému webového typu provozovaného v prostředí státní správy a měla by je poskytnout právě tato práce.

1 Cíl práce a metodika

Diplomová práce se bude zabývat problematikou zabezpečení informací v prostředí státní správy, a to především se zaměřením na aplikace využívané v rámci svěřených agend.

1.1 Cíl práce

Hlavním cílem této diplomové práce bude analýza a návrh ochrany agendových informačních systémů používaných pro administraci úkolů v oblasti věcné působnosti orgánů státní správy. Dílčím cílem bude analýza jednotlivých funkčních komponent a vrstev vybraného informačního systému státní správy včetně návrhu všech opatření, která by umožnila stanovit vyšší úroveň zabezpečení systému jako celku.

Pro naplnění těchto cílů byly stanoveny následující kroky:

- Rešerše odborné literatury související se zkoumanou problematikou
- Analýza informačního prostředí vybraného subjektu
- Výběr podoblasti zvolené metodologie a upřesnění postupu
- Otestování a ověření existence krizových míst vybraného systému
- Návrh řešení problémových oblastí – technická opatření na úrovni systému a návrh změn v systému řízení bezpečnosti

1.2 Metodika

Rešeršní část se bude zaměřovat na problematiku informační bezpečnosti z několika úhlů pohledu, například řízením informační bezpečnosti v obecné rovině, v prostředí státní správy a zároveň samostatnými informačními systémy, jejich užitím i konstrukcí a okrajově i aktuálním vývojem této oblasti. Zde bude zkoumat legislativní podmínky pro zabezpečení informačních systémů ve státní správě. Zároveň se zaměří na způsoby a možnosti auditování a kontroly informační bezpečnosti především z pohledu vybrané metodologie OWASP a jejího standardu, a to se zaměřením na výběr a vymezení aplikovatelných částí, které je možné pro tyto účely použít ve státní organizaci. Tato dílčí oblast bude vyžadovat studium pramenů, jejich vzájemné porovnání a hledání souvislostí nebo odlišností.

V analytické části bude hlavním cílem popsat legislativní a funkční vymezení vybraného agendového informačního systému a jeho propojení na architekturu a infrastrukturu organizace a způsob jeho zabezpečení. Porovnat a vybrat vhodnou oblast metodologie OWASP a použít ji pro kontrolu aktuálního stavu informačního zabezpečení, vyhodnotit jeho silné a slabé stránky a na základě tohoto šetření specifikovat nejproblematičtější oblasti bezpečnosti systému a navrhnout jeho vylepšení.

Mezi metody použité ke zpracování diplomové práce patří základní myšlenkové operace a také statistické a průzkumné metody:

- Abstrakce – odtržení určitých částí nebo vlastností procesu za účelem lepšího poznání určité části
- Analýza – rozčlenění na části a jejich zkoumání izolovaně
- Komparace – srovnávání jevů, nalézání společných a odlišných znaků sledovaného jevu
- Syntéza – vytváření celkového obrazu jevu, hledání souvislostí a vzájemných vazeb mezi jednotlivými částmi.

Z průzkumných metod bude pro potřeby práce využito studia a zkoumaní informačních zdrojů. Jedná se o shromažďování informací z existujících dokumentů. Podklady pro obsahovou stránku práce budou získány z navržených zdrojů, a to zejména z odborných publikací, vnitropodnikových materiálů, zkušeností pracovníků a online informačních zdrojů. Pro hodnocení úrovně zabezpečení vybraného systému vzhledem k jeho typu bude použita metodologie OWASP. Na jejím základě bude provedeno šetření pomocí

softwarových nástrojů pro řízení zranitelností i faktické ověření konfigurací. Výsledkem bude popis stávajícího stavu s návrhem na možná opatření v souladu se stanovenými cíli.

2 Teoretická východiska

Tato kapitola se okrajově dotýká historických faktů, od kterých se odvíjí informační bezpečnost, i to, jak je koncipováno její řízení v současnosti. Dále se zde uvádí skutečnosti týkající se jejího legislativního a institucionálního zajištění. Jak státní úřady využívají informační systémy, jak jsou zabezpečeny a co představuje agendový informační systém, a jak provádět jeho bezpečnostní testování.

2.1 Historie počítačové bezpečnosti

Historie zná již prvotní potřebu, kdy bylo nutné omezit komunikaci na vymezený okruh osob, jako zprávy posílané hlavními představiteli zemí, vojenskými veliteli nebo diplomaty. Tajné kódy založené na abecedních substitucích se používaly již v rané Indii během válek. Staří Číňané naopak používali ideografickou povahu svého jazyka ke skrytí významů slov. V minulosti byly citlivé zprávy přenášeny důvěryhodnými osobami, které byly hlídány a střeženy v bezpečí, aby se zajistila bezpečnost informací. Julius Caesar je považován za vynálezce stejnojmenné šifry, která chránila důvěrnost informací. Ten ji používal k ochraně vojenských zpráv, a to nahrazením každého písmene v prostém textu posunem písmene o tři pozice v abecedě. Tuto metodu používal pro všechny své tehdejší vojenské komunikace. Není však známo, jak byla tato šifra efektivní v jeho době. V devatenáctém století se vyskytla technika založená na jednoduchých šifrovacích schématech, kdy se část osobní reklamy v novinách použila k výměně zpráv. Složitější Caesarova šifra byla používána ruskou armádou během válečných dob a je známo, že pro protistranu bylo obtížné ji dešifrovat. Potřeba komunikace na dálku vyústila později ve vynález telegrafů a telefonů jako předchůdců dnešních sítí. Telegraf je komunikační systém vynalezený Samuelem Morsem (1791–1872), kde jsou informace prvně přenášeny po drátu prostřednictvím řady elektrických impulsů zvaných Morseův kód. Elektrické telegrafy změnily radikálně způsob vedení válek, tím že umožnily vojenským velitelům posílat zprávy vzdáleným jednotkám v krátkém čase. Na rozdíl od doručování zpráv pomocí kočárů a koňů se informace mezi dvěma telegrafy uskutečňovaly téměř okamžitě. Existují záznamy o používání telegrafních systémů během krymské války v letech 1853–1856. S příchodem nových komunikačních metod využívající rádiové signály se použití kryptografie stalo velmi důležité, zejména pro koordinaci vojenských operací. Historicky víme, že francouzské, americké a německé armády aktivně používaly různé druhy šifrovacích metod již během první světové války.

První známý případ narušení bezpečnosti komunikačních systémů pochází ze sedmdesátých let dvacátého století, kdy skupina osob v USA, kteří se označovali jako „Pheakeři“ (ang. Pheakers), dokázala pomocí akustických signálů zmást digitální telefonní ústředny a uskutečnit volání zdarma nebo přesměrovat uskutečňované hovory. Ikonou této skupiny se stal John Draper, známý též pod přezdívkou Captain Crunch (Kapitán Křupka), který pro tuto činnost použil plastovou hračku dodávanou jako reklamní doplněk k cereáliím. Tato píšťalka vydávala tón o frekvenci 2 600 Hz, která odpovídala frekvenci pro odblokování americké telefonní sítě AT&T. Tímto tónem operátor označoval volné telefonní linky a pomocí něj si šlo jednu takovou obsadit, aniž by dotyčný musel něco zaplatit. Později sestrojil elektronické zařízení tzv. bluebox, umožňující generovat více použitelných frekvencí, které bylo možné ovládat pomocí tlačítek a volat více funkcí. John Draper je tímto považován za jednoho z prvních hackerů v historii. V té době (v roce 1969) též vznikl předchůdce internetu ARPANET, akademická síť, která spojovala university a výzkumné ústavy v USA. Později se síť rozšířila a spolu s rozvojem TCP/IP protokolu a dostupností osobních počítačů se v osmdesátých letech výrazně zvýšil počet připojených osob a tím i vzniku internetu. Objevily se též první kybernetické útoky, obdobně též na AT&T, ale třeba i na vesmírnou agenturu NASA. Reakcí bylo vytvoření první organizace zajišťující síťovou bezpečnost, v roce 1988, s názvem Computer Emergency Response Team (CERT). S tím, jak se internet stával populárnější, rostl počet uživatelů, kteří byli přitažlivým cílem pro „hackery“ po celém světě. V devadesátých letech dvacátého století se objevily další hackerské aktivity, jako byl například virus „Michelangelo“ a došlo také k zatčení známého hackera Kevina Mitnicka za krádež údajů kreditních karet a za útok Solar Sunrise v roce 1998, který zacílil na počítače Pentagonu.

Dnes žijeme v éře internetu a WWW, kde jsou téměř všichni připojeni. Internet změnil způsob, jakým spolu komunikujeme. Web umožnil okamžitý přístup k informacím odkudkoli na světě. Web první generace byl jen statický web. Web 2.0, nazývaný interaktivní web, dovolil uživatelům komunikovat s důrazem na online spolupráci. Technologie Web 3.0 s názvem „inteligentní web“ akcentuje strojové učení s podporou automatické srozumitelnosti informací, které poskytuje rychlejší a intuitivnější uživatelský komfort. Síť se stala sociálním médiem, kde můžeme vzájemně komunikovat, což bohužel

vede také k mnoha dalším hrozbám a zranitelnostem a rostoucímu počtu narušení bezpečnosti.[1]

Web 3.0 obvykle autoři označují jako sémantický web. Kromě toho se dnes již mluví i o verzi Web 4.0. Zde zatím neexistuje jednotná definice tohoto pojmu. Někteří autoři ho uvádějí jako symbiotický web s interakcemi mezi lidmi a stroji. Při jeho rozvoji by měla být důležitá role technologií IoT a také Big Data pro vytváření, ukládání a prezentaci informačního obsahu – sémanticky sdílených prezentací a jejich archivaci. Do úvahy je nutné brát vývoj, který směřuje k umělé inteligenci, která plně porozumí lidskému jazyku a pro kterou je sémantika webu zásadní, stejně jako je dnes nezbytná například pro všechny současné AI pomocníky, například Google Home, Amazon Echo nebo Siri[2].

2.2 Bezpečnost v informatice

V souvislosti s řízením informační bezpečnosti v libovolné organizaci, se setkáváme s termíny ISG, ISMS nebo BMIS. Tyto pojmy označují různé koncepce a přístupy týkající se řízení informační bezpečnosti v organizacích a dalších institucích, které ke své činnosti využívají digitálních prostředků. Je to ta část řízení, která se zaměřuje na vše, co se týká znalostí a informací v podobě dat a souvisí s jejich zpracováním. V současné době jsou ve vyspělých tržních ekonomikách data pro organizace ten nejcennější i nejdražší klíč, který rozhoduje o prosperitě organizace, celkové kvalitě, úspěšnosti a postavení na trhu nebo umožňuje jejich začlenění do navazujících oblastí společnosti.

Pokud si instituce uvědomí, že základní hodnotou jsou informace a jejich potenciál, měly by mít zájem o nastavení takového systému řízení informační bezpečnosti, který tento kritický faktor náležitě ochrání. Každá organizace je však zároveň ekonomickým subjektem, který se řídí příslušnými legislativními normami. Většina ekonomických subjektů je založena za účelem získání zisku, avšak neméně důležitý je ve fungujícím státě i veřejný a neziskový sektor. Ty se v oblasti kybernetické bezpečnosti řídí obdobnými principy. Stát v oblasti

[1] RAO, Umesh Hodeghatta a Umesha NAYAK. The InfoSec handbook: an introduction to information security [online]. New York, New York: Apress, [2014] [cit. 2019-06-02]. Expert's voice in information security. ISBN 14-302-6382-2. Dostupné z: DOI: 10.1007/978-1-4302-6383-8

[2] MASNER, Jan, Pavel ŠIMEK, Eva KÁNSKÁ a Jiří VANĚK. Creation, Storage and Presentation of Information Content – Semantics, Sharing, Presentation, and Archiving. Agris on-line Papers in Economics and Informatics [online]. 2019, 11(01), 75-82 [cit. 2020-03-30]. DOI: 10.7160/aol.2019.110108. ISSN 18041930. Dostupné z: http://online.agris.cz/archive/2019/1/8

kybernetiky koriguje činnosti státních institucí základními normami, avšak ponechává jim velké pravomoci k vlastním strategiím a politikám.

Jednou ze základních potřeb organizací je zajištění ochrany dat v souvislosti s poskytováním odpovídajících služeb. Nestačí mít dobré technologie, interní procesy a kvalifikované pracovníky, ale je nutné zahrnout k těmto faktorům i hledisko ochrany dat. Nastavit její odpovídající úroveň a dále ji udržet a cíleně rozvíjet. V této dynamicky se rozvíjející se oblasti není zcela jednoduché zajistit odpovídající skladbu vědomostí, znalostí, dovedností, přístupů a postojů, jaké podnik právě potřebuje k podpoře zabezpečení informací.

Účelem řízení bezpečnosti je systematicky utvářet, prohlubovat a rozšiřovat schopnosti a povědomí (znalosti, dovednosti a chování) o informační bezpečnosti v daném subjektu. Z těchto důvodů je nutná existence takového systému řízení informační bezpečnosti, jako základní předpoklad k dílčím organizačním nebo technologickým opatřením, které by sami od sebe nebyly efektivní.

2.3 Řízení provozu informatiky

Řízení informatiky se stává stále významnější součástí celopodnikového řízení, a to z důvodu nárůstu integrace původně podpůrných informačně-technologických procesů do ostatních oblastí produkce. Firmware nebo doplňkové softwarové služby se stávají pevnou součástí produktů a služeb. Jsou dostupné pro široký okruh uživatelů a spolu s tímto vývojem se zvyšují i nároky na jejich bezpečnost. Navíc se zvyšuje ekonomický tlak na vývoj produktů a jeho zrychlování mnohdy způsobuje zanedbávání základních bezpečnostních opatření. Při zajištění provozu a rozvoje je obzvlášť nutné soustředit se i na tuto oblast.

2.3.1 Zajištění provozu a rozvoje

Řízení informatiky představuje souhrn činností a procesů, které jsou spojeny se stanovením základních koncepcí a strategií organizace na úrovni poskytování informačně-technologických služeb, včetně plánování jednotlivých projektů, rozvojových a provozních úloh včetně zajišťování finančních, technických i personálních zdrojů. V rámci ISMS jsou pro řízení informatiky organizací využívány metodiky, založené na řešení těchto úloh v praxi. Mezi hlavní modely patří ITIL a COBIT.

ITIL popisuje praxi prostřednictvím jednotlivých publikací, kdy ITIL verze 4 (známý též jako ITIL 2011) pracuje s pěti knihami definovanými na základě životního cyklu služeb[3]. Tento model také dále pracuje s obecnými manažerskými technikami, mezi které se počítají i některé z oblasti informační bezpečnosti, a to Risk Management a Information Security Management.

COBIT naopak samostatně modeluje procesy a stanovuje metriky efektivnosti, které by měly sloužit vedení organizace k hodnocení stavu řízení informatiky. Slouží tedy ke kontrole a redefinici stávajících nebo jako podpora nově vznikajících procesů. Soustředí se na vazbu mezi primární činností organizace a jejími strategickými cíli s plány v oblasti informatiky. Sleduje přidanou hodnotu IT a optimalizuje její investice a dále pak sleduje rizika a měří výkonnost se zaměřením na hospodárnost procesů.

Také je možné zde zmínit nekomerční přístupy jako je metodika Management of Business Informatics (MBI). Jde o model vyvinutý na Katedře informačních technologií VŠE v Praze. Cílem modelu MBI je nabídnout IT odborníkům pověřeným řízením informačních technologií v organizacích, komplexní metodickou podporu založenou na nejlepších průmyslových postupech. Hlavní výhoda modelu MBI spočívá ve vyhledávání informací. ITIL nemá portál, který by umožnil jeho efektivní využití. Metodika COBIT je dostupná prostřednictvím sady elektronických nebo tištěných průvodců případně verze COBIT 5 je online, ale efektivní vyhledávání informací zde není podporováno. Aplikace MBI se primárně zaměřuje na efektivní vyhledávání informací[4].

Je nutné zde též zmínit důležitost informační strategie, která pracuje s uvedenými modely a má zásadní vliv na způsob provozování a rozvoj služeb. Například na skutečnost, zda správu jednotlivých oblastí bude organizace realizovat prostřednictvím vlastních prostředků nebo využije služeb outsorcingu. Jaké jsou její základní cíle a co vyplývá z analýz současného stavu? Jak bude vypadat architektonické řešení nových aplikací v budoucnosti a jakým způsobem se budou realizovat rozvojové projekty a jejich dopady do kapacitního plánování? To vše má v konečném důsledku dopad do úrovně zajištění jednotlivých služeb a jejich dostupnosti.

[3] Pozn.autora: odvozeno původně od Demingova životního cyklu PDCA.

[4] BUCHALCEVOVA, Alena a Jan POUR. Business Informatics Management Model. Advances in Computer Science and Ubiquitous Computing [online]. Singapore: Springer Singapore, 2015, 2015-12-18, , 65-71 [cit. 2020-03-29]. Lecture Notes in Electrical Engineering. DOI: 10.1007/978-981-10-0281-6_10. ISBN 978-981-10-0280-9. Dostupné z: http://link.springer.com/10.1007/978-981-10-0281-6_10

2.3.2 **Řízení informační bezpečnosti a její zavádění**

Obecné předpoklady pro řízení bezpečnosti vycházejí z historických kořenů a prošly vlastním vývojem, který odrážel především změny využívání elektronických medií a způsoby využívání dat. Zprvu byla data využívána pouze lokálně a nebyla přenášena pomocí sítí. V této době byly požadavky na jejich zabezpečení minimální. Potřeba řízení informační bezpečnosti se zvýšila v souvislosti s rozšiřováním přenosových sítí, nejdříve v akademické a vojenské oblasti, později i v komerční i veřejnoprávní sféře. Právě v tomto období se poprvé objevila potřeba společných jednotných měřítek, tedy standardizace v oblasti kybernetiky.

Doucek a kol. k tomuto historickému vývoji uvádí, že první kritéria stanovilo americké Národní středisko počítačové bezpečnosti (NCSC – National Computer Security Center). Šlo o TCSEC, tedy Trusted Computer Security Evaluation Criteria, známé též jako oranžová kniha.[5]

Z jejich existence se pak odvíjí celá řada dalších amerických, kanadských a později i celosvětových a evropských norem a standardů. Mezi nejvýznamnější, které mají přímý dopad i do prostředí České republiky, patří normy ISO/IEC a jejich evropská obdoba CEN/CENELEC. Ty jsou právě základem ISMS a to konkrétně ISO/IEC 27001 a 27002 které pracují s modelem PDCA a představují množiny požadavků a doporučení při řízení bezpečnosti. Z těchto norem vychází i zákon 181/2014 Sb. o kybernetické bezpečnosti, který dílčím způsobem akceptuje certifikaci ISO jako naplnění požadavků tohoto zákona. Není to však jediná legislativní norma v České republice, vyskytující se v oblasti informační bezpečnosti.

2.3.3 **Realizace kybernetické bezpečnosti a její jednotlivé oblasti**

Identifikace potřeb organizace v oblasti zabezpečení informatiky představuje poměrně obtížný problém, zejména z důvodu, že jednotlivé atributy jsou navázány na typ instituce, způsob poskytování služeb, informační prostředí a hodnotu dat. Lze postupovat tak, že se analyzuje škála údajů, získaných jednak z běžného informačního systému organizace, jednak ze zvláštních šetření. Obvykle jde o tři skupiny údajů:

[5] DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Pub., 2011. ISBN 9788074310508 s. 60

1. Údaje týkající se celé organizace – struktura organizace, její program činnosti, údaje o počtu, struktuře a typu dat
2. Údaje o jednotlivých činnostech – specifikace služeb, množství systémů a jejich zaměření.
3. Údaje o jednotlivých systémech – vyžaduje detailní znalost vedení jednotlivých agend, včetně citlivosti dat.

Při zjišťování potřeb je nutné znát nejen současný stav struktury informačních zdrojů, ale i vývojové tendence. Ty zkoumáme nejen v samotné instituci, ale i jejím okolí, přičemž na veřejný sektor má největší vliv legislativa.

2.3.4 **Řízení rizik**

Riziko je historický pojem, který se objevil v souvislosti s plavební přepravou a jde o původní výraz *risico*, který pochází z italštiny a znamená úskalí, kterému se musely lodě vyhnout. Přesná klasifikace pro její užití v současnosti však neexistuje a lze ji pojmout různými způsoby. Pojem je definován různě:

- Pravděpodobnost či možnost vzniku ztráty
- Variabilita možných výsledků nebo nejistota jejich dosažení
- Odchýlení skutečných a očekávaných výsledků
- Pravděpodobnost jakéhokoli výsledku, odlišného od výsledku očekávaného
- Situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti
- Nebezpečí negativní odchylky od cíle (tzv. čisté riziko)
- Nebezpečí chybného rozhodnutí
- Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko)
- Neurčitost spojená s vývojem aktiva (tzv. investiční riziko)
- Střední hodnota ztrátové funkce
- Možnost, že specifická hrozba využije specifickou zranitelnost systému

V ekonomii je spojován v souvislosti s nejednoznačností průběhu ekonomických procesů a jejich výsledků. Obecně lze ale uvažovat, že je možné tuto vlastnost vztáhnout i na jiné oblasti a druhy rizik. Sem by patřily například rizika právní, spojená s odpovědností za škodu, politická a teritoriální, ale i specifická, jako pojišťovací, manažerská a bezpečnostní, která lze vyjádřit penězi. Jsou tedy často chápána ve svých důsledcích jako změna

ekonomické veličiny v čase, která nabude oproti očekávaným hodnotám pozitivní nebo negativní odchylky. Jde tedy vlastně o kolísavost neboli volatilitu finanční veličiny.[6]

Instituce, přistupující odpovědně k řízení bezpečnosti, odvíjejí své aktivity v této oblasti od prvotní znalosti svého prostředí, a to na základě analýzy rizik, kterou za tímto účelem pravidelně provádějí. Pro státní instituce platí, že se řídí definicí danou ZoKB. Základní princip je ale shodný s organizacemi v privátním sektoru. Vždy jde o identifikaci aktiv, tedy rozpad subjektu na jeho jednotlivé složky v potřebném detailu a stanovení jejich hodnoty. Jde především o stanovení důležitosti pro organizaci, jaké dopady a význam by měla jejich ztráta, narušení, změna a poškození na její primární činnosti. Následně se u těchto aktiv vyhodnotí, jaké slabiny obsahují, nebo se jimi vyznačují, tedy slabá místa, na které mohou působit hrozby a tím negativně ovlivnit jejich hodnotu. Tím, že se stanoví závažnost hrozeb a míra zranitelnosti se určí i pravděpodobnost jejich výskytu a následně dojde ke klasifikaci rizik. Na část z nich se pak aplikují protiopatření.

Při bezpečnostních auditech se pak mimo jiné vychází z poslední provedené analýzy rizik a prohlášení aplikovatelnosti, kdy tento přístup představuje nutný základní postup, umožňující srovnávat relevantní rizika, působící v dané instituci a bez jejichž znalosti by nebylo testování proveditelné. Řízení rizik má vlastní standardy a jde o samostatnou, velmi rozsáhlou oblast, která je součástí informační bezpečnosti a jejíž problematika je zde zmíněna jen okrajově, s ohledem na rámec testování webových aplikací.

2.4 Úřady a instituce zabývající se bezpečností

Česká republika v rámci budování informační společnosti disponuje množstvím zákonných a podzákonných norem a institucí, které upravují tuto oblast nebo dohlížejí na jejich dodržování. Některé z nich se pak přímo nebo nepřímo dotýkají fungování systémů ve svěřené péči jednotlivých státních úřadů. Většinou vymezují nebo ukládají povinnosti na poli ochrany dat nebo i zakládají právní subjektivitu institucí, zabývajících se kontrolou dodržování zákonných opatření v oblasti bezpečnosti informací. Někdy jsou též výsledkem snahy o harmonizaci právního řádu České republiky s právem Evropské unie. Také je vhodné na tomto místě zmínit některé související strategie ČR, předně NSKB a Strategický rámec rozvoje veřejné správy, jehož součástí je i rozvoj eGovernmentu.

[6] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada). ISBN 978-802-4730-516, s. 90-91.

2.4.1 **Legislativní rámec**

Jak bylo výše uvedeno primární normou pro informační bezpečnost je v oblasti veřejné správy ZoKB, stát však samozřejmě disponuje celou řadou zákonných a podzákonných předpisů, které se k této oblasti více či méně rovněž vztahují. Tabulka č. 1 níže uvádí přehled těch nejdůležitějších.

Tabulka 1 - Seznam zákonů v oblasti informatiky

č.z.	název z.
181/2014 Sb.	Zákon o kybernetické bezpečnosti
205/2017 Sb.	Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony
110/2019 Sb.	Zákon o zpracování osobních údajů
106/1999 Sb.	Zákon o svobodném přístupu k informacím
127/2005 Sb.	Zákon o elektronických komunikacích
499/2004 Sb.	Zákon o archivnictví a spisové službě
300/2008 Sb.	Zákon o elektronických úkonech a autorizované konverzi dokumentů
412/2005 Sb.	Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti
297/2016 Sb.	Zákon o službách vytvářejících důvěru pro elektronické transakce
111/2009 Sb.	Zákon o základních registrech
365/2000 Sb.	Zákon o informačních systémech veřejné správy
480/2004 Sb.	Zákon o některých službách informační společnosti
250/2017 Sb.	Zákon o elektronické identifikaci
153/1994 Sb.	Zákon o zpravodajských službách České republiky
154/1994 Sb.	Zákon o bezpečnostní informační službě
148/1998 Sb.	Zákon o ochraně utajovaných skutečností
298/2016 Sb.	Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

2.4.2 **Úřady a instituce**

Stěžejní organizací zabývající se bezpečností informatiky je Národní úřad pro kybernetickou a informační bezpečnost, který vznikl 1. srpna 2017 na základě novelizace ZoKB a to faktickým rozdělením NBÚ. Jeho gescí je kybernetická bezpečnost, včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.

Je správním úřadem pro kybernetickou bezpečnost, ochranu utajovaných informací pro oblast informačních a komunikačních systémů, kryptografickou ochranu a problematiku veřejně regulované služby navigačního systému Galileo (PRS). Disponuje odbornými specialisty v oblasti kybernetické bezpečnosti a kryptografické ochrany, řídí tzv. Vládní CERT České republiky (GovCERT.CZ), spolupracuje s ostatními CERT a CSIRT bezpečnostními týmy doma i po celém světě. Připravuje národní bezpečností standardy

v oblasti kyberbezpečnosti včetně zákonů a strategie (NSKB). Také připravuje a koordinuje kybernetická cvičení[7].

Další institucí je Úřad pro ochranu osobních údajů, který působí v oblasti zpracování osobních údajů. Jeho činnost je vymezena předně zákonem č. 110/2019 Sb., o zpracování osobních údajů, ale i např. správním řádem, kontrolním řádem a v neposlední řadě i zákonem č. 111/2009 Sb., o základních registrech. Kde např. dle § 11 vytváří a vede seznamy identifikátorů fyzických osob a jejich převod mezi jednotlivými agendami[8].

Jako organizaci s širokým záběrem lze uvést Ministerstvo vnitra, které převzalo v roce 2007 kompetence Ministerstva informatiky a rozšířilo tím svoji obsáhlou působnost i o oblast ISVS. V tomto rámci zajišťuje vydávání správních rozhodnutí, tvorbu metodických dokumentů, přípravu právních předpisů a také kontrolu nad atestacemi a akreditujícími osobami. Provozuje též informační systém o datových prvcích nebo informační systém o informačních systémech státní správy, dále také Datové schránky, Czech POINT a část základních registrů ROB a RPP. Kromě ostatních oblastí se věnuje eGovermentu a také je v jeho gesci Informační koncepce České republiky. V souvislosti s ní je vhodné zde zmínit usnesení vlády č. 629 k programu Digitální Česko a návrhu změn Statutu Rady vlády pro informační společnost. Její působnost byla dána do souladu s programem „Digitální Česko“. *Program "Digitální Česko" je souborem koncepcí zajišťujících předpoklady dlouhodobé prosperity České republiky v prostředí probíhající digitální revoluce. Jeho náplň je možné definovat pojmem: "Strategie koordinované a komplexní digitalizace České republiky 2018+". "Digitální Česko" zastřešuje tři hlavní pilíře (dílčí koncepce / strategie), které tvoří jeden logický celek s velkým počtem vnitřních vazeb, ale zároveň ve struktuře reflektují zacílení na různé příjemce a rovněž odlišnosti dané současným legislativním vymezením:*

- *Česko v digitální Evropě (v gesci Úřadu vlády)*
- *Informační koncepce České republiky (v gesci Ministerstva vnitra)*
- *Koncepce Digitální ekonomika a společnost (v gesci Ministerstva průmyslu a obchodu)*[9]

[7] O úřadu. Národní úřad pro kybernetickou a informační bezpečnost [online]. Brno: NÚKIB Brno – Mučednická, 2017 [cit. 2020-01-24]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

[8] Působnost Úřadu. Úřad pro ochranu osobních údajů [online]. Praha: Úřad pro ochranu osobních údajů, 2013, 2019 [cit. 2020-01-24]. Dostupné z: https://www.uoou.cz/pusobnost%2Duradu/ds-1269/archiv=0&p1=1059

[9] Rada vlády pro informační společnost. Ministerstvo vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky, 2019, 2020 [cit. 2020-01-24]. Dostupné z: https://www.mvcr.cz/clanek/rada-vlady-pro-informacni-spolecnost.aspx

Existuje i celá řada menších specializovaných agentur, které se více či méně též zaměřují na oblast informační bezpečnosti. Například úřad zabývající se normalizací nejen na poli informatiky, Česká agentura pro standardizaci. Ta byla zřízena jako státní příspěvková organizace, a to ÚNMZ a od 1. 1. 2018 od něj převzala všechny činnosti týkající se technických norem, jako jsou jejich tvorba, vydávání a distribuce.

Samostatnou kapitolou by pak byly světové a evropské instituce, které také značnou měrou ovlivňují informační prostředí České republiky a mají vliv na tvorbu legislativních a technických norem. Zde lze uvést především normalizační a certifikační instituce jako jsou ISO a dále NIST, NSA, ANSI, IEEE, ISACA nebo BSI a další.

V současné době vznikají na evropské úrovni federace založené na komunitních datových souborech, které umožňují organizacím sdílet data, znalosti a zkušenosti v oblasti informační bezpečnosti. Dobrým příkladem takových federací je Evropská organizace pro kybernetickou bezpečnost (ECSO) a Evropská agentura pro bezpečnost sítí a informací (ENISA). Pro stejné účely jsou po celém světě zřizovány další centra kybernetické bezpečnosti na vnitrostátních úrovních[10].

2.4.3 **Národní Strategie Kybernetické Bezpečnosti**

V současné době je platná NSKB definovaná pro období 2015–2020. Strategie samotná se skládá z několika částí, přičemž v jejím úvodu jsou nejdříve uvedeny vize, které mají dlouhodobější časový rámec, a většina z nich bude mít přesah do návazných období. Jedná se o budování informační společnosti s důrazem na detekci hrozeb, s rozvojem bezpečnostních složek a posílením expertní základny. ČR chce aspirovat na přední pozice v této oblasti a zároveň posilovat mezinárodní a evropskou spolupráci. Nastiňuje zde i spolupráci GovCERTu s národním CERT a tím také dále spolupráci jednotlivých sektorů, veřejného, soukromého i akademické obce. Rovněž je kladen důraz na prioritní atributy, jako je ochrana investic v informatice a důvěra ve stát.

Na tyto vize navazují základní principy, které stát sleduje při zajišťování kybernetické bezpečnosti. Ochrana lidských práv a svobod, komplexní přístup založený na spolupráci, budování důvěry mezi veřejným, soukromým sektorem a občanskou společností s akcentem

[10] MOHASSEB, Alaa, Benjamin AZIZ, Jeyong JUNG a Julak LEE. Cyber security incidents analysis and classification in a case study of Korean enterprises. Knowledge and Information Systems [online]. [cit. 2020-03-30]. DOI: 10.1007/s10115-020-01452-5. ISSN 0219-1377. Dostupné z: http://link.springer.com/10.1007/s10115-020-01452-5

na rozvoj kapacit a investic do výzkumu a vzdělávání. ČR se zde hlásí také k posílení kooperace jednotlivých složek kybernetické obrany s orgány činnými v trestním řízení.
Více konkrétním obsahem se pak zabývají aktuální výzvy, stanovené pro dané období a způsob jejich zvládání. Výzev je celkem devatenáct a představují samostatné oblasti kybernetické bezpečnosti, které vyžadují zvýšenou pozornost a jsou východiskem pro jednotlivé hlavní cíle. Ty tvoří kostru implementace Akčního plánu, který představuje jejich detailní rozpracování. NUKIB zpracovává každoroční zprávy o stavu bezpečnosti v České republice, a podává hlášení o plnění tohoto plánu. NSKB představuje základní dokument vlády pro tuto oblast a je v souladu s Bezpečnostní strategií ČR.[11]

2.4.4 **Strategický rámec rozvoje veřejné správy**

Usnesením vlády č. 680 ze dne 27. srpna 2014 byl schválen Strategický rámec rozvoje veřejné správy České republiky pro období 2014–2020. Jde o širší koncepci, která má vazbu na další strategické dokumenty ČR. Za všechny je možné zde zmínit především Akční plán pro rozvoj digitálního trhu, a to především s ohledem na Strategický cíl 3. Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu. Předběžná podmínka pro jeho naplnění obsahuje: *... Strategický rámec politiky pro digitální růst, který má podněcovat cenově dostupné, kvalitní a interoperabilní soukromé a veřejné služby v oblasti IKT a zvýšit míru jejich využívání občany (včetně zranitelných skupin), podniky a orgány veřejné správy včetně přeshraničních iniciativ.*[12] SRRVS zde navrhuje Společný řídící výbor pro eGovernment a služby informační společnosti ve veřejné správě, kterému má předsedat Ministerstvo vnitra a je průnikovým orgánem mezi Radou vlády pro informační bezpečnost a Radou vlády pro veřejnou správu. Prakticky to znamená, že ČR se bude ve strategickém období věnovat oblasti modernizace veřejné správy, a to i za pomoci zvýšení dostupnosti služeb veřejné správy prostřednictvím nástrojů eGovernmentu. To celé klade samozřejmě zvýšené nároky na oblast informatiky a její důvěryhodnost a spolehlivost při zajišťování těchto veřejných služeb. Zde je tedy možné spatřovat důvod vazby na jinou strategii, a to právě výše zmiňovaný Akční plán pro rozvoj digitálního trhu, který má ve

[11] Národní strategie kybernetické bezpečnosti ČR 2015-2020. In: . Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2014, ročník 2015. Dostupné také z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf
[12] Veřejná správa: Strategický rámec rozvoje. Ministerstvo vnitra České republiky: o nás [online]. Praha: Ministerstvo vnitra České republiky, 2014 [cit. 2020-03-24]. Dostupné z: https://www.mvcr.cz/soubor/strategicky-ramec-rozvoje-verejne-spravy-v-cr-pro-obdobi-2014-2020.aspx, tabulka str. 84

svých klíčových prioritních oblastech položku Rozvoj infrastruktury a její podsložku Zajištění kybernetické bezpečnosti. Ta právě odkazuje na NSKB a NUKIB jako jejího gestora. Tento akční plán zde stručně shrnuje hlavní principy a cíle uvedené v NSKB a AP KB, zároveň však obsahuje funkční řešení pro rozvoj infrastruktury a budování internetových sítí, opatření v oblasti digitální gramotnosti a vzdělávání. Samostatně se zde věnuje právě jednotlivým oblastem rozvoje elektronické veřejné správy, jako je elektronická komunikace s úřady, elektronické zdravotnictví a elektronizace sociálních služeb a justice. Také jsou zde plánována opatření týkající se standardizace k publikaci a katalogizaci otevřených dat veřejné správy (známé též jako OPENDATA).

Výhody otevřených dat jsou rozmanité a sahají od zlepšení účinnosti veřejné správy až k ekonomickému růstu v soukromém sektoru. Jeho nedílnou součástí je i zemědělství. Tato data mohou stimulovat ekonomický růst tím, že ekonomika může mít prospěch ze snadnějšího přístupu k informacím, obsahu a znalostem, což zase přispívá k rozvoji inovativních služeb a tvorbě nových obchodních modelů[13].

Co se týče správy digitální agendy, koncepce se snaží podpořit koordinaci na národní úrovni. Jednotlivá agenda, a tedy i agendové systémy jednotlivých úřadů, by měly mít v rámci svých koncepcí i svůj meziresortní rozměr. Jde především o snahu reflektovat na úrovni celé státní správy nejnovější technologický i obchodní vývoj a sledovat vysokou dynamiku digitálního trhu a souvisejících debat na úrovni EU. Tento přístup pak koordinovaně promítnout do svěřených úkolů v rámci agend.

2.4.5 **Agendové informační systémy**

Úřady, tedy i OVM pracují s dokumenty, ať již v papírové nebo digitalizované formě a dále s informacemi, které jsou obsaženy v informačních systémech. Pokud pomineme informační systémy, zajišťující činnosti související s vnitřním provozem příslušných úřadů, tedy provozní nebo také jinak – podpůrné IS, jsou primárními nositeli informací ISVS, tedy takové, které slouží pro výkon veřejné správy. V těch se uchovává naprostá většina dat, které veřejná správa využívá a zpracovává. Dalším typem informačních systémů jsou systémy zajišťující činnosti podle zvláštních zákonů, tzv. agendy veřejné správy. Příkladem by mohl

[13] VOSTROVSKY, V. a J. TYRYCHTR. Consistency of Open Data as Prerequisite for Usability in Agriculture. Scientia Agriculturae Bohemica [online]. 2018, 49(4), 333-339 [cit. 2020-03-30]. DOI: 10.2478/sab-2018-0040. ISSN 1805-9430. Dostupné z: https://content.sciendo.com/view/journals/sab/49/4/article-p333.xml

být Informační systém evidence obyvatel, upravený zákonem č. 133/2000 Sb., který patří mezi základní IS a slouží k podpoře shromažďování a uchovávání údajů o občanech České republiky. Informace jsou zde zpracovávány a poskytovány dále oprávněným úřadům a jiným orgánům. Jsou zde údaje o státních občanech ČR, jako je jméno, příjmení, datum a místo narození, pohlaví, rodné číslo a dalších, celkem 20 atributů. Dále i údaje o osobách, které pozbyly státní občanství a také o cizincích, kteří jsou v definovaném vztahu k dítěti občana s českou státní příslušností. V §3 odst. (1) je uveden status IS, jako agendový systém veřejné správy podle zvláštního zákona. Jedná se tedy všeobecně o informační systémy jednotlivých OVM, o kterých tak říká zákon, jako v uvedeném případě. Jednotlivé speciální zákony řídí a upravují jaký typ dat ze svěřených agend je zde uchováván, po jakou dobu, jak je možné s daty nakládat, komu a za jakých podmínek mohou být zpřístupněny. Kdo je zdroj dat a jak se data pořizují, a jak probíhá změna a také kontrola, ověření a další definované podmínky. Obecné, ale třeba i bezpečnostní aspekty provozu agendových systémů souvisí s širším pojetím celého provozu informačních systémů státní správy a jsou upraveny zákonem 365/2000 Sb.

Orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.[14]

Bezpečnostní aspekty bývají pevnou součástí informačních koncepcí jednotlivých orgánů veřejné správy a zahrnují delší časový rámec. Řízením na nejvyšší úrovni se přitom zabývá Ministerstvo vnitra, které k němu v rámci svěřených kompetencí využívá různé nástroje. Připravuje právní předpisy v této oblasti a samostatné metodické pokyny a další koncepční, strategické nebo koordinační dokumenty. Je součástí procesů pro schvalování změn a investic do ISVS a provádí kontroly, atestace a akreditace. Zároveň je samo provozovatelem a správcem vlastních IS, především základních registrů nebo i Informačního systému o informačních systémech veřejné správy (IS o ISVS).

2.4.6 **Základní registry**

Systém základních registrů tvoří soubor základních agend. Jde o registr obyvatel (ROB), registr osob (ROS), registr územní identifikace (RÚIAN) a registr práv a povinností (RPP).

[14] ČESKO. § 5b odst. 1 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 8. 2. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365#p5b-1

Jaké údaje jsou v ROB uloženy, bylo již zmíněno v předchozí kapitole. U ROS se jedná o evidenci a registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci. Uvádějí se zde obchodní názvy, IČO, sídla, právní forma, datum vzniku a zániku a další související údaje.

RPP pak slouží jako zdroj při řízení přístupu uživatelů k údajům v jednotlivých agendových informačních systémech i v registrech a v informačních systémech základních registrů a vedou především informace o zákoně, na jehož základě je přístup realizován, jaké činnosti a údaje lze ze základních registrů čerpat a které orgány ji mohou vykonávat. Jsou zde drženy i historické údaje, díky kterým lze zřizovat výpis kdo, kdy a za jakým účelem data v základních registrech četl, měnil či upravoval.

RÚIAN slouží k evidenci o územních prvcích, územních jednotkách, adresách a zobrazuje je na mapách státního mapového díla nebo v digitálních mapách veřejné správy. Jsou zde jednotky jako území státu, regionu, vyššího samosprávného celku, kraje, obce, katastrální území, ale i třeba účelový volební okrsek. Nevedou se zde žádné osobní údaje.

Správci agendových informačních systémů-editorů jsou přitom povinni být připojeni do systému základních registrů, tak jak to definuje Nařízení vlády č. 161/2011 Sb. Nařízení vlády o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až § 68 zákona o základních registrech. Editorem je přitom myšlen editační agendový systém, jehož prostřednictvím jsou v jednotlivých registrech editovány příslušné údaje.

2.5 Informační systém

Organizace v současnosti kladou velký důraz na schopnost ovlivňovat transformační procesy, na kterých se podílejí, pomocí informačních toků. Proto se také mnohdy informace řadí k základním výrobním zdrojům jako je půda, práce a kapitál. Základním nástrojem pro efektivní realizaci využití informací jsou systémy pro jejich sběr, zpracování a poskytování, známé obecně jako informační systémy.

2.5.1 Definice informačního systému

Definic pojmu informační systém je mnoho a záleží na pojetí, kterému přiřadíme priority s ohledem na úhel pohledu a účel pro který má být tato definice použita. Například Steven Alter z University of San Francisco uvádí ve své práci z ledna 2008 - Defining Information

Systems as Work Systems: Implications for the IS Field[15], tabulku s alternativními definicemi informačního systému, která se snaží souhrnně zachytit právě její možné interpretace. Celkem obsahuje dvaadvacet položek a je zde možné sledovat různé přístupy v jejím uchopení. Jsou zde definice oborově neutrální na pomezí informačně manažerského přístupu, ale také přístupy sledující konkrétnější parametry v podobě procesní, analytické nebo rozhodovací složky a některé také berou v potaz i jejich sociální rozměr. Ten by se dal najít i v případě definice autorů Turban, McLean, Wetherbe: *An information system is a collection of components that collect, processes, stores, analyzes, and disseminates information for a specific purpose. The major components of a computer-based information system (CBIS) can include (1) hardware, (2) software, (3) a database, (4) a network, (5) procedures, and (6) people. The system operates in social context, ant the software usually includes application programs which perform specific task for users.*[16] *Informační systém je souborem složek, které sbírají, zpracovávají, ukládají, analyzují a předávají informace pro konkrétní účely. Hlavní součásti systému založeného na počítačovém základě (CBIS – computer-based information system) obsahují (1) hardware, (2) software, (3) databáze, (4) sítě, (5) procesy, a (6) osoby. Tento systém pracuje v sociálním kontextu a software obvykle obsahuje aplikační programy, které provádějí specifické úkoly pro uživatele* (překlad autor). Samozřejmě je možné dále rozlišovat jednotlivé typy informačních systémů, a to zejména z hlediska jejich architektury, ale je nutné si i nadále uvědomovat, které komponenty jsou zde sdruženy, a to i v případě, že se zaměříme již na jeho konkrétní typ. Tento strukturní rozpad tedy bude platný i pro systémy webového typu.

2.5.2 **Životní cyklus aplikace**

Aplikace od svého vzniku prochází různými stádii vývoje a jednotlivé fáze musí navazovat na celkovou strategii, plánování a řízení informatiky jako celku. Jsou zásadně závislé na obchodních procesech celé organizace a některé jsou ekonomicky navázané na nákladovou složku, jiné naopak slouží k podpoře ziskovosti nebo realizaci výstupů. Obrázek 1 níže schematicky shrnuje jednotlivé fáze. Zajímavostí tohoto pojetí je zahrnutí bezpečnostní optimalizace a monitoringu (jehož součástí by měla být kromě provozního monitoringu

[15] ALTER, Steven. Defining information systems as work systems: implications for the IS field. European Journal of Information Systems [online]. 2017, 17(5), 448-469 [cit. 2020-03-24]. DOI: 10.1057/ejis.2008.37. ISSN 0960-085X. Dostupné z: https://www.tandfonline.com/doi/full/10.1057/ejis.2008.37

[16] ŠVARCOVÁ, Ivana a Tomáš RAIN. Informační management. Praha: Alfa Nakladatelství, 2011. Informatika (Alfa Nakladatelství). ISBN 978-80-87197-40-0, s 60

a jeho bezpečnostní složka) do životního cyklu. Výhoda spočívá v nutnosti počítat s bezpečnostními hledisky již při počátečních fázích tedy při přípravě a plánování a také v návrhu. To prakticky znamená, že bezpečnost bude v tomto případě zapracována již do konceptu a bude s ní počítáno po celou dobu životnosti.

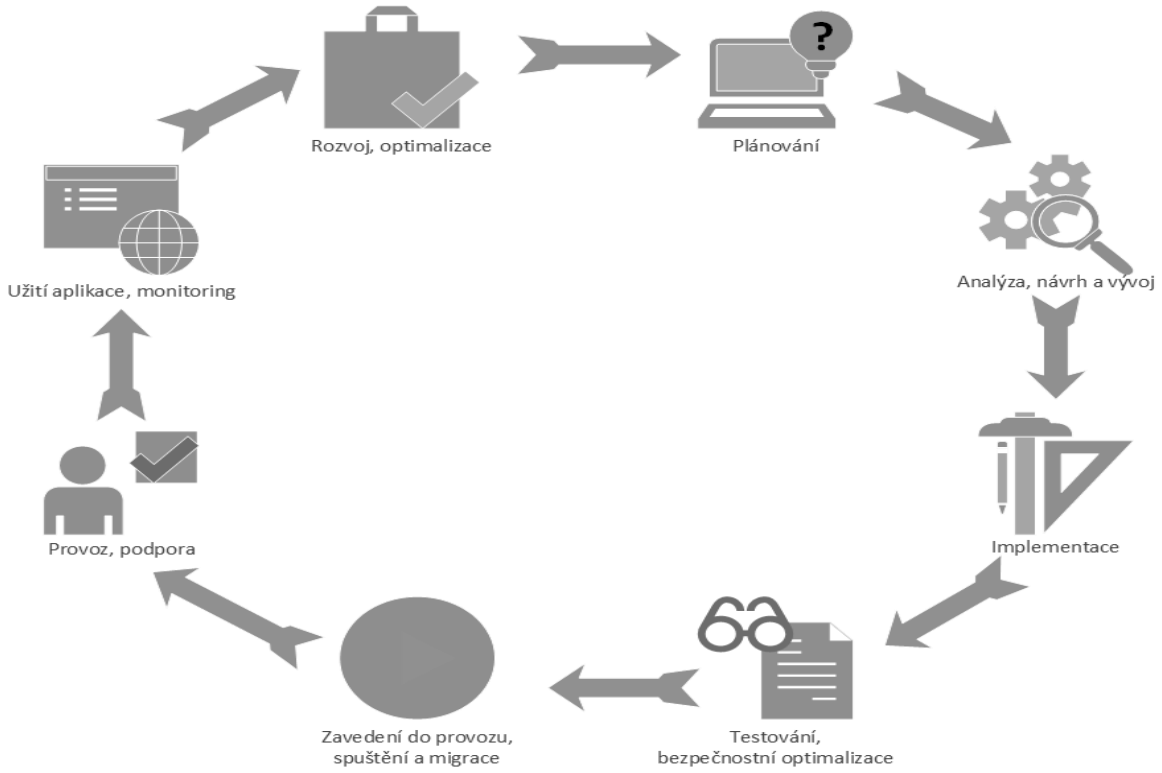
Příkladem by mohla být implementace architektury, která podporuje bezpečnostní politiky prostřednictvím samostatných komponent. Taková architektura umožňuje vývojářům bezpečnostních modelů soustředit se na algoritmy řízení přístupu, bez ohledu na to, jakým způsobem budou vynucovány. Takovým přístupem je například prototyp Configurable Security Architecture (ConSA)[17].

Z praxe jsou naopak známy případy, kdy se analýza a návrh soustředí pouze na funkční požadavky a později již nelze specifické bezpečnostní funkce do produktu zapracovat, nebo to je obtížné a nese to sebou další náklady, jak časové, tak finanční. Tento přístup spíše podporuje ve svém důsledku kompromisní řešení, které v informační bezpečnosti není žádoucí. Je proto výhodné zabývat se jejími aspekty například již ve studii proveditelnosti, která by měla ověřit nejen kompatibilitu se stávající infrastrukturou, ale stanovit vhodná koncepční řešení i na této úrovni. Tato studie pak stanoví architekturu řešení, celkové finanční, technologické a personální náklady. Také se k ní váže příprava smlouvy nebo celého výběrového řízení, pokud se projekt realizuje prostřednictvím externího dodavatele.

Analýza, návrh a vývoj pak musí sledovat několik zásadních oblastí. Především jde o analýzu procesů a návrh změn, včetně dopadů do organizační struktury a stanovení požadavků na jejich změnu nebo zavedení. Tato oblast je mnohdy mnohem náročnější než samostatné technologické zpracování a implementace zvolené aplikace. Ta je samozřejmě též důležitá a měla by obsahovat návrhy na data a jejich migraci a samozřejmě koncepci funkčních požadavků. Bez návaznosti na vnitropodnikové procesy, a tedy i uživatele by sama o sobě nedávala smysl. Nedílnou součástí zde musí být i řešení zabezpečení, jak bylo uvedeno v předchozích kapitolách. Vazby, které se sledují, jsou dány nejen procesní rovinou, ale i její komunikační obdobou pro potřeby začlenění a spojení na jiné systémy a aplikace v organizaci. Řešení funkčních a datových vazeb je tedy velmi podstatnou součástí systému a mělo by obsahovat i jejich odpovídající bezpečnostní zajištění. To bývá

[17] HARDY, Alexandre a Martin S OLIVIER. A Configurable Security Architecture Prototype. Data and Application Security [online]. Boston, MA: Springer US, 2001, 2002, , 51-62 [cit. 2020-03-30]. IFIP International Federation for Information Processing. DOI: 10.1007/0-306-47008-X_5. ISBN 978-0-7923-7514-2. Dostupné z: http://link.springer.com/10.1007/0-306-47008-X_5

pro uživatele v této rovině transparentní a je třeba jej testovat zcela samostatně, odborníky v této oblasti. Opakem jsou funkční testy, které probíhají vždy v součinnosti s konzumenty služeb. Tato jejich úzká kooperace je zde nutná, aby bylo možné celkově posoudit nejen funkcionality a workflow užití, ale případně i uživatelský komfort (UX – user experience) a další aspekty.



Obrázek 1 - Životní cyklus aplikace (autor)

Implementační fáze představuje soubor činností, které umožní provozovat vybranou nebo navrženou technologii ve vnitřním prostředí organizace. Jde o specifické konfigurace nebo uživatelské úpravy, které umožní napojení na ostatní systémy a otestují základní funkčnost modulů nebo zkušebních vzorů. Predispozicí bývá připravenost na úrovni infrastruktury a po nasazení a konfiguracích je možné realizovat dodatečný vývoj specializovaných funkcí nebo nestandardních programových modulů. V této fázi je též vhodné připravovat akceptační procedury. Ty by měly zahrnovat přípravu testovacích dat pro simulaci reálného provozu nebo instalaci podpůrných testovacích modulů nebo testovacího software. Také sem patří příprava testovacích scénářů, v gesci odpovědných osob. Tyto pracovníci by měly být vybaveni nejen odpovídajícími technologickými znalostmi nutnými pro posouzení, ale i kompetencemi pro schválení testovaných řešení.

Samostatné testování bývá součástí akceptace a provádí se bezprostředně před zavedením do provozu. Je nutné se zaměřit především na tyto typy testů:

- Funkční testy – ověřují funkcionality systému
- Integrační testy – ověřují vazby na okolní prostředí
- Zátěžové testy – ověřují robustnost a stabilitu aplikace
- Bezpečnostní testy – ověřují bezpečnostní funkce a auditovatelnost
- Analýza zdrojového kódu – ověřují deklarovanou standardizaci vývoje

Výstupem jednotlivých testů bývají protokoly, které jsou podkladem pro akceptační řízení a obsahují jednotlivé záznamy a celkový výsledek testů, na jejichž základě je nebo není akceptováno řešení a schválen další postup.

Zavedení do provozu nastává zpravidla po akceptaci řešení a v závislosti na tom, zda se jedná o novou aplikaci či náhradu stávající, se realizuje případná migrace dat a konfigurací. Pokud se jedná o náhradu stávající aplikace, je třeba stanovit, zda půjde o postupný přechod, tedy zda obě aplikace budou provozovány v souběhu a po jakou dobu, nebo půjde o jejich okamžitou výměnu. Obě varianty mají své výhody i nevýhody a je třeba zvážit dopad na zvýšené zatížení pracovníků provozem a rizika vyplývajících z chyb nebo výpadků na začátku provozu. Také je nutné se v přechodovém období případně zaobírat možnou duplicitou dat a jejím řešením. V době zavádění řešení se zároveň provádějí uživatelská školení pro optimalizaci využití programových prostředků v rámci stanovených procesů.

Předání do provozu představuje ve standardní organizaci většinou přesun organizačního řízení z projektového týmu na oddělení zajišťující operativu. Tento proces by měl být formalizován a měl by být vyjasněn přechod odpovědnosti z jednoho týmu na druhý. Také je nutné stanovit hranici mezi provozem aplikace a infrastruktury, pokud se jedná o rozdílné osoby nebo provozovatele. Úloha oddělení provozu spočívá v zajištění funkčnosti nejen aplikace, ale i celé infrastruktury, včetně zálohování, monitoringu, řešení výpadků a poruch. Samostatnou kapitolou je pak bezpečnostní monitoring, vyhodnocování a řešení rizik a zajištění oprávněného přístupu k datům a funkcím aplikace. Výstupy provozu a bezpečnosti se pak promítají do rozvojových a optimalizačních aktivit a úprav systému. Postupem času, v závislosti na celkovém technologickém vývoji, mohou vyústit i ve výměnu aplikace. Tím je celý životní cyklus aplikace ukončen a znovu je aktivována fáze plánování.

2.5.3 **Agilní vývoj a DevSecOps**

V současné éře tvorby aplikací se velmi rozšířil přístup agilního vývoje. Ten akcentuje především zlepšování procesů dodávky aplikací, a to v tom smyslu, že se soustředí na možnosti změn ve funkcích a postupech týmů, podporujících obchod a rozvíjí je s cílem lépe dodat projekt nebo produkt předpokládaný konečným uživatelem nebo zákazníkem. To se projeví ve schopnosti flexibilně reagovat na změny během vývoje a dodávky. Agilní vývoj používá vlastní metody a přístupy. Známé jsou metodiky Extrémního programování (XP), Lean development pro zrychlení vývoje, případně Test Driven Devolopment založený na předem definovaných testovacích scénářích a další. Patrně nejběžnější je pak metodologie Scrum. V ČR je spolu s hybridními metodami založenými na tomto přístupu nejčastěji používanou agilní metodou vývoje softwaru[18].

V souvislosti s výše uvedeným je vhodné zmínit existenci systému hodnocení a výběru metodik budování IS/ICT METES (Methodology Evaluation System). Ten se využívá pro výběr správné agilní metodiky vývoje softwaru, vhodnou pro konkrétní projekt. Systém Metes rozděluje kritéria do čtyř základních skupin, a to Proces, Podpora, Produkt a Lidé. Skupiny Proces a Podpora se zaměřují na zhodnocení procesů dané metodiky. Naopak skupiny Produkt a Lidé se zabývají základními charakteristikami produktu a lidským faktorem, který je rovněž účasten na projektu. Každé kritérium má stupnici slovně definovanou a každý bod je detailně popsán. U kritérií skupin Produkt a Lidé jsou definovány i minimální, maximální a optimální hodnoty, podle kterých lze usoudit, zda je metodika pro daný projekt použitelná[19].

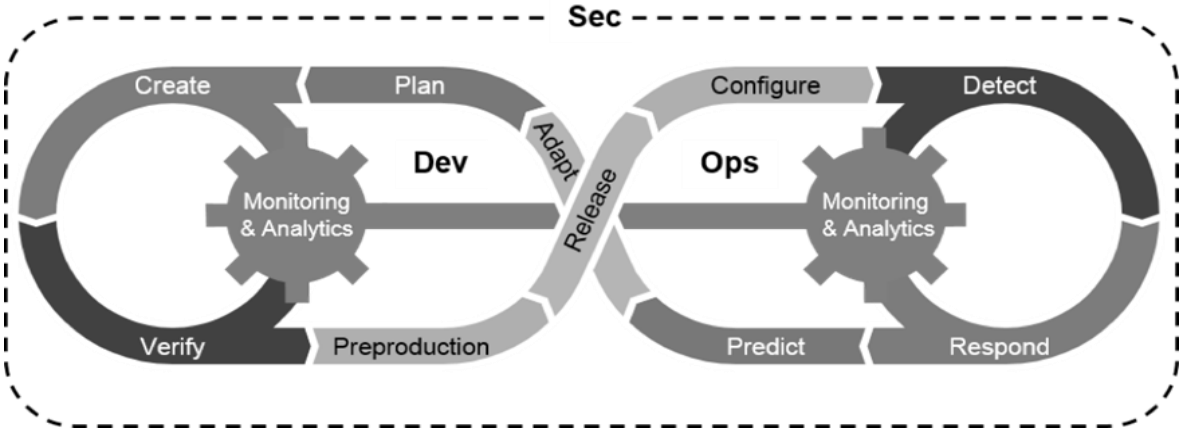
Naopak DevSecOps přístup zkracuje dodací lhůty při dodání výstupů pomocí vylepšených inženýrských postupů, a to podporou soudržnosti a spoluprací mezi vývojovými, bezpečnostními a provozními týmy. Agilní vývoj i přístup DevSecOps mohou být implementovány společně za účelem podpory spolupráce v rámci svých příslušných domén.

---

[18] DOLEZEL, Michal, Alena BUCHALCEVOVA a Michal MENCIK. The State of Agile Software Development in the Czech Republic: Preliminary Findings Indicate the Dominance of "Abridged" Scrum. Research and Practical Issues of Enterprise Information Systems [online]. Cham: Springer International Publishing, 2019, 2019-12-13, , 43-54 [cit. 2020-03-29]. Lecture Notes in Business Information Processing. DOI: 10.1007/978-3-030-37632-1_4. ISBN 978-3-030-37631-4. Dostupné z: http://link.springer.com/10.1007/978-3-030-37632-1_4

[19] BUCHALCEVOVA, Alena. Application of Methodology Evaluation System on Current IS Development Methodologies. International Journal of Information Technologies and Systems Approach [online]. 2018, 11(2), 71-87 [cit. 2020-03-29]. DOI: 10.4018/IJITSA.2018070105. ISSN 1935-570X. Dostupné z: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJITSA.2018070105

To může mít pozitivní následek v kulturním posunu v postupech jednotlivců, kteří je implementují. V ideálním prostředí by organizace mohla používat oba postupy, je však důležité si uvědomit, že přístup DevSecOps lze implementovat v jakémkoli prostředí, agilním nebo jiném.



Obrázek 2 - Proces DevSecOps (zdroj: https://www.bankinfosecurity.com)

DevSecOps znamená především schopnost rozdělit dodávku software na více samostatných částí a zvýšit jejich frekvenci a do spolupráce mezi vývojovým a provozním týmem zapojit i oddělení informační bezpečnosti. Mezery a slabiny jsou pak v procesu vývoje a dodávky zjištěny mnohem dříve a mohou být realizovány nápravná opatření. Životní cyklus je v tomto přístupu ještě více fragmentován.

2.5.4 **Vývoj bussiness inteligence**

Současným trendem v oblasti bussiness inteligence je velmi rychlé tempo vývoje. Dochází k podstatnému rozvoji poskytování služeb na bázi cloud computingu a zvyšování využití specifických analýz nad velkým objemem dat pomocí vizualizace, a to prostřednictvím mobilních technologií na bázi samoobslužného využití. Pro analýzy již není nutné využívat velké komplexní a složité systémy, zvyšuje se tak dostupnost těchto úloh a flexibilita pro uživatele. BI v rámci Cloud Computingu představuje rozvoj aplikací s využitím disponibilní infrastruktury. Tu je možné členit na jednotlivé vrstvy, například na infrastrukturní, zajišťující úložiště dat a výpočetní výkon, a platformní, která poskytuje komponenty datových skladů, integrací, databází nebo hostovaných BI. Dále pak vrstva aplikační poskytující analytické a vizualizační nástroje pro koncové uživatele. Hojně jsou též využívány mobilní BI, zaměřené na způsob využívání pomocí přenosných bezdrátových počítačových a komunikačních zařízení, jako jsou PDA, tablety a chytré telefony

(smartphones) pro práci s analytickými aplikacemi. Tento způsob představuje okamžitý přístup k datům organizace nezávisle na lokaci. Zásadními efekty BI je hlubší pochopení podstaty vlastní činnosti organizace prostřednictvím multidimenzionálního pohledu na informace a také zohledňuje časové dimenze pro predikci budoucího vývoje. Umožňuje tak včasné odhalení kritických a mimořádných stavů a reakci na ně. Usnadňuje rozhodovací aktivity a přispívá ke komplexnějšímu, flexibilnějšímu řízení a zvyšuje rychlost orientace v datech.[20] BI je dnes používáno v mnoha oblastech ekonomiky, specifickou oblastí, kterou je vhodné zde zmínit, je využití metod Business Intelligence v agrární oblasti, kde ji zemědělské podniky využívají k posílení své produkce a potenciálu, zvyšováním technické účinnosti a využitím efektivní podpory manažerských, analytických, plánovacích a rozhodovacích činností manažerů a specialistů[21].

2.5.5 **Vrstvy aplikace**

Co se týče jednotlivých vrstev, jsou záznamy dat prováděny uživatelsky pomocí aplikací nebo jsou získávány alternativními způsoby. Mohou být získávány přenosem z jiného systému nebo zařízení, čidla, snímače, automatu nebo čteček karet a podobně. Aplikace kromě jejich zachycení provádí také uložení, zpracování a prezentaci. Tyto jednotlivé operace jsou zpravidla zpracovávány na samostatných vrstvách. Dříve však nebylo výjimkou, především u menších systémů, jejich provozování bez rozvrstvení. Uživatelská vrstva zpravidla představuje zařízení konzumenta služby, které je umístěno v jeho síti nebo je zpřístupněno pomocí veřejné sítě. Mohou to být různá zařízení od desktopu, laptopu přes PDA nebo v dnešní době více tablety a chytré mobilní telefony. Ty využívají zpravidla desktopové nebo mobilní aplikace a také přímo internetové prohlížeče. Zde je třeba si uvědomit, že jsem lze zařadit i skripty běžící právě na straně uživatelského zařízení. V závislosti na typu aplikace jsou pak data zobrazována uživateli tak, aby je mohl uchopit svými smysly. Mohou to být obrazová data, zvukové záznamy, ale i vibrace nebo hmatová interpretace dat. Některé formy lze vhodně kombinovat. Zvláštním typem obrazových dat jsou data textová, která bývají uspořádána strukturovaně ve formulářích, tabulkách nebo

[20] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-2475457-4, s. 131-135

[21] TYRYCHTR, J., M. ULMAN a V. VOSTROVSKÝ. Evaluation of the state of the Business Intelligence among small Czech farms. Agricultural Economics (Zemědělská ekonomika) [online]. 2016, 61(2), 63-71 [cit. 2020-03-30]. DOI: 10.17221/108/2014-AGRICECON. ISSN 0139570X.

větách a odstavcích. Grafická data pak většinou slouží ke zdůraznění významu dat textových nebo slouží pro jejich lepší uchopení, kdy na jejich místo používáme jinou alternativu. Formuláře naopak představují základní přístup v případě, že jsou data získávána od uživatelů. Používají metody jako výběr hodnot, volná pole, vkládání předefinovaných hodnot, zvolení nebo vynechání, automatické doplnění, číselníky a další. Aplikační logika provádí celou řadu funkcí a algoritmů, které odpovídají požadovaným výstupům a na základě schémat, pracuje se strukturovanými daty a využívá metadat v procesu konceptualizace. Datová logika je tvořena za primárním účelem uchovávání dat a jejich dalšího poskytování v rámci jejich využitelnosti jinými aplikacemi. Lze rozpoznat dva základní přístupy pro jejich ukládání, a to systémy souborové a databázové. U souborového systému je pak možné provádět následující operace:

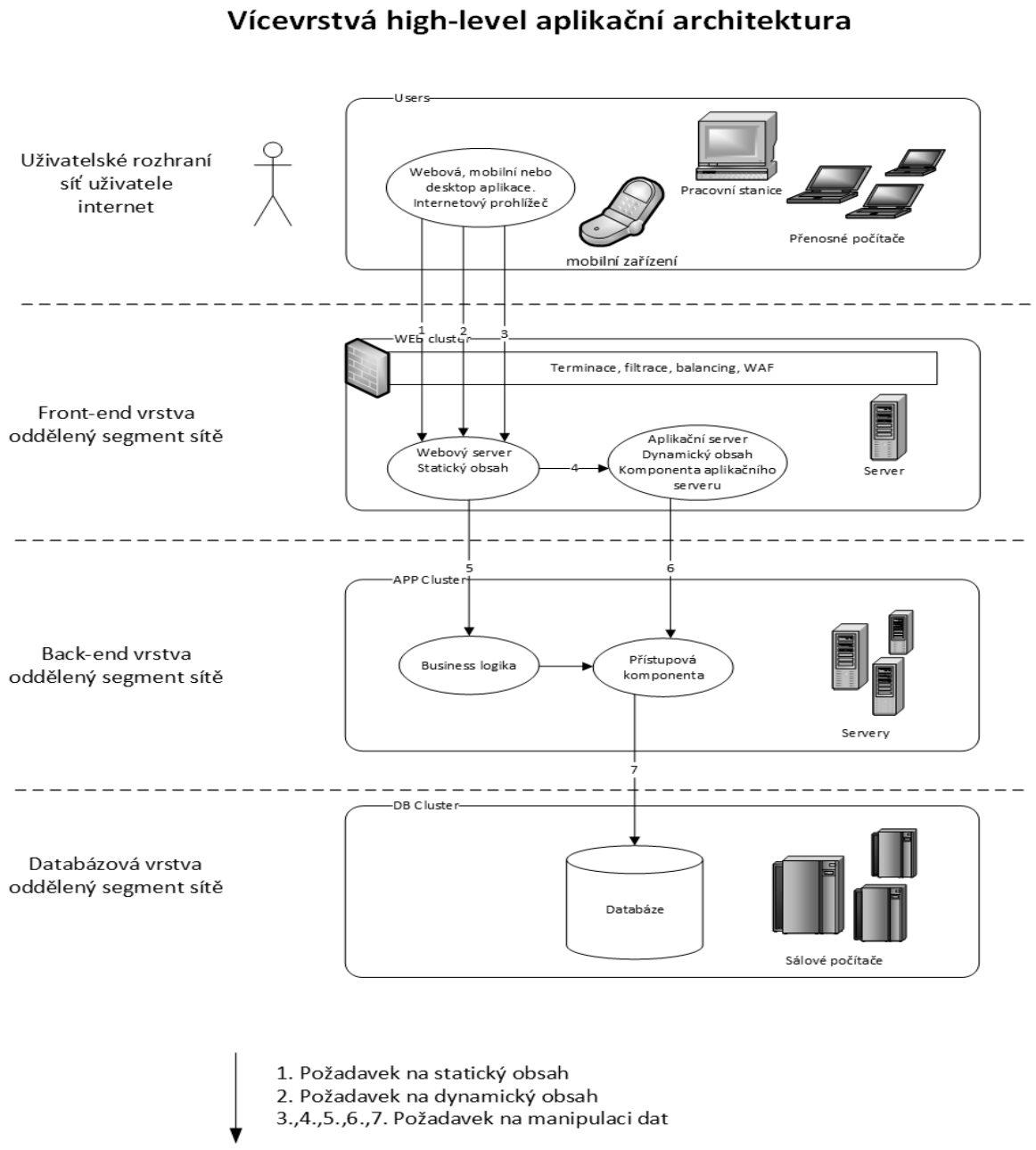
- Otevření a zavření souboru
- Vytvoření nového souboru nebo jeho vymazání
- Čtení souboru
- Zápis do souboru

Souborový systém je vhodný na ukládání vytvořených souborů uživateli, např. textovými procesory nebo grafickými nástroji, do adresářů a představují ucelený soubor dat, který lze v případě potřeby přenášet do jiné lokace. Je však problematické v tomto způsobu ukládání zachytit vzájemné vztahy mezi různými objekty a je též problematické kombinovat strukturovaná a nestrukturovaná data. Databázový přístup naopak vytváří metadatový model, tedy informace o datech, tak aby zde byly podchyceny vztahy mezi entitami, jejich popis a struktura. Nad těmito objekty pak pracuje databázový systém, který umožňuje manipulovat s daty samotnými, ale i se strukturou.[22]

Obrázek 3 zobrazuje variantně vrstvy dle zažitých anglických výrazů, kde je prezentační logika členěna dále na dvě samostatné vrstvy – uživatelské rozhraní a Front-end vrstvu, aplikační logika odpovídá Back-end vrstvě a datová logika vrstvě databázové. Existují však přístupy, kdy mohou být některé komponenty sdružovány v jednotlivých vrstvách s ohledem na vyšší výkon a jejich rychlejší spolupráci. Z pohledu zabezpečení aplikací je ale výhodné, aby prezentační vrstva umožňovala co nejméně prostředků pro přímou manipulaci s daty

[22] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-2475457-4, s.55-56.

a poskytovala pouze vizualizaci, a algoritmy pro zpracování zde nebyly umístěny.



Obrázek 3 - Vrstvy aplikační architektury (autor)

2.5.6 Aplikační a webová bezpečnost

Tato kapitola se zabývá otázkami, které souvisí především se zabezpečením webů a webových aplikací, které vedou k diskuzi, o tom, jak se vyhnout infekci a napadení škodlivým kódem na těchto platformách. Je třeba mít na paměti, že doba, kdy stačilo využívat pouze služeb antivirového programu je dnes již jen historickým faktem. Pokud zajišťujeme bezpečnost software, je třeba se soustředit na všechny propojené oblasti a vrstvy,

počínaje operačním systémem, včetně aplikací, nástrojů, pomůcek a konče sítí. Je zde spoustu možných chyb na různých úrovních, jako je nesprávná konfigurace, neošetřené vstupy, defekty a chyby v kódování, únosy relací, slabá hesla nebo šifrovací klíče, manipulace s pamětí nebo útoky typu „man in the midlle“. V prostředí internetu působí velké množství robotů a automatických kódů, které kontinuálně skenují stávající i nové adresy v síti, a hledají možné slabiny a jejich zneužití. Vystavení nechráněné aplikace do veřejné sítě, byť jen na malý okamžik, znamená zcela jistě výraznou hrozbu infikace.

Zjevná rizika pro narušení bezpečnosti spočívají v tom, že neautorizované osoby mohou získat přístup k omezeným informacím a mohou být schopny eskalovat svá oprávnění za účelem ohrožení aplikace a celého aplikačního prostředí. Mezi oblasti, které mohou být nejvíce ohroženy, patří účty pro správu uživatelů a celého systému[23].

Jak tedy ochránit naše data a nevystavovat se zbytečně útokům SQL nebo command injection, buffer owerflows, session hijacking, cookies poisoning nebo password cracking? Jak bylo výše poukázáno, high level pohled na informační bezpečnost se vztahuje na všechny součásti systémů, tedy včetně fyzické infrastruktury. Mohou to být budovy, zdroje elektrické energie, kabely a rozvody, hardware, síť, software, nástroje, utility a lidé, včetně interních zdrojů i dodavatelů. Žádná část tohoto řetězce nemůže být z pohledu ochrany organizace ignorována.

Fyzická bezpečnost je přitom mnohem snadněji dosažitelná pomocí zábran, plotů, zámků, kamerových systémů, osvětlení, nebo i biometrických čteček a dalších prostředků. Stále jsou zde ale některé výzvy, jako třeba ochrana mobilních zařízení. Zajištění bezpečnosti softwaru je však úkol mnohem náročnější vzhledem k vysokému počtu kombinací možných slabin a útoků. Souhrn těchto kombinací vzhledem k určitému aktivu, je nazýván jako attak surface (souhrn vektorů útoku), který je nutný neustále snižovat a udržovat v minimalizovaném rozsahu.

Autoři Rao a Nayak rozeznávají osm základních charakteristik aplikační bezpečnosti (překlad autor):

1. Úplnost vstupů
2. Správnost vstupů

[23] LEPOFSKY, Ron. Web Application Vulnerabilities and the Damage They Can Cause. The Manager’s Guide to Web Application Security [online]. Berkeley, CA: Apress, 2014, 2014-12-20, , 21-46 [cit. 2020-03-30]. DOI: 10.1007/978-1-4842-0148-0_3. ISBN 978-1-4842-0149-7. Dostupné z: http://link.springer.com/10.1007/978-1-4842-0148-0_3

3. Úplnost zpracování
4. Správnost zpracování
5. Úplnost aktualizací
6. Správnost aktualizací
7. Ochrana integrity uložených dat
8. Ochrana integrity přenášených dat[24]

V případě úplnosti vstupů je nutné, aby aplikace zajišťovala, že budou přijímaná data kompletní a že již v samotném návrhu není nic opomenuto. Tedy, že pro potřebnou transakci, má systém k dispozici všechna data. Druhý parametr naopak sleduje, zda byl dodržen formát dat, jejich typ a struktura a že i všechny ostatní charakteristiky splňují očekávané hodnoty. Také že byla dodržena jejich integrita a nebyly žádným způsobem změněny. Další z charakteristik sleduje, zda bylo zpracování řádně ukončeno, tedy že byl celý proces zpracování řádně ukončen. Metrika správnosti zpracování však sleduje, co se stane, pokud byl sice výpočet zahájen se správnými daty a byl i řádně ukončen, ale došlo k chybě při výpočtu. Je tedy velice důležité, aby výrobce software při vývoji nezapomněl kontrolovat výstupy z procesů, tak aby byly validní a přesné. Úplnost a správnost aktualizací pak souvisí s kontrolou záznamu změn. Pokud byla transakce dokončena, musí o tom být záznam a aplikace sleduje i to, zda byla ukončena s pozitivním výsledkem a že kritické operace neselhaly. Poslední dva parametry poukazují na skutečnost, že data, kromě toho, že mohou být ve stavu procesování, mohou být přenášena nebo naopak uložena, přitom je nanejvýš žádoucí, aby nemohlo dojít k jejich nežádoucí změně ani v jednom z uvedených stavů.

Uvedení autoři dále doporučují dodržovat následující doporučení pro bezpečný návrh a vývoj softwaru:

- Porozumět bezpečnostním požadavkům aplikace (na funkčnost a data) a uvést je do specifikace
- Zajistit, aby byly během návrhu architektury a designu zohledněny
- Dodržet standardy bezpečného kódování
- Provádět ověření všech vstupů, včetně vstupních kontrol, kontrolu povolených hodnot a formátování
- Zajistit důvěryhodné mechanismy přihlášení (včetně potřeby silných hesel)

[24] RAO, Umesh Hodeghatta a Umesha NAYAK. The InfoSec handbook: an introduction to information security [online]. New York, New York: Apress, [2014] [cit. 2019-06-02]. Expert's voice in information security. ISBN 14-302-6382-2. Dostupné z: DOI: 10.1007/978-1-4302-6383-8, s 116.

- Zajistit šifrovaný přenos dat (tam, kde je nutná důvěrnost a integrita dat)
- Zajistit pravidelnou povinnou změnu hesel
- Zavést odpovídající oprávnění a přístupová práva k procesům aplikací na základě rolí a principu nejnižších oprávnění (Least Privilege Principle)
- Používat správné ošetření chyb (včetně upravených chybových hlášení, bez nepotřebných informací v kontextu jejich využití)
- Vhodné mechanismy pro manipulaci s výjimkami, zabudované přímo v aplikaci
- Řádně dokončená konfigurace, všechna nastavení musí dokončena a prověřena
- Využívat pouze prověřené algoritmy
- Zavést kontroly součtu pro zajištění úplného a přesného zpracování kritických procesů
- Odstranit všechny nežádoucí a nevyužívané funkce a rutiny
- Zajistit správné mechanismy pro odhlášení
- Používat zabezpečené protokoly
- Zajistit odpovídající mechanismy logování, protokolování a auditu
- Využívat správu konfigurace během celého vývoje
- Mít zavedený pevný systém pro testování
- Důrazně kontrolovat proces vydávání softwarových verzí[25]

Výše uvedené parametry jsou zajisté podmínkou pro zajištění vysoké úrovně bezpečnosti, nicméně zde narážíme na problém v běžném prostředí státní správy. Většina úřadů státu, a i samospráv není výrobcem těchto řešení, nemá své vývojové týmy a řeší své softwarové potřeby dodavatelsky. Je ale často jejich provozovatelem a samozřejmě též uživatelem. To klade vysoké nároky a smluvní zabezpečení, které musí brát ohled na zajištění uvedených podmínek na straně dodavatele. Objednatel by kromě toho, měl provádět kontroly i u výrobce a soustředit se na to, zda vývoj probíhá v souladu se zavedenými postupy i podmínkami smlouvy.

[25] RAO, Umesh Hodeghatta a Umesha NAYAK. The InfoSec handbook: an introduction to information security [online]. New York, New York: Apress, [2014] [cit. 2019-06-02]. Expert's voice in information security. ISBN 14-302-6382-2. Dostupné z: DOI: 10.1007/978-1-4302-6383-8, s 121.

2.6 Audity a bezpečnostní testování

Za účelem prověření bezpečnostního stavu informačního prostředí je nutné provádět pravidelné kontroly. Tato kapitola se věnuje typům a rozsahu prováděných testů a popisuje také vhodné standardy a metodologie a další použitelné postupy nebo systémy. Odpovědnost provádět penetrační testy je zakotvena pro povinné osoby v ZoKB, respektive v jeho prováděcí vyhlášce o kybernetické bezpečnosti 82/2018 Sb. Zde je výslovně uvedeno, že se testy týkají důležitých aktiv, a to ve fázi uvedení do provozu nebo v souvislosti s významnou změnou takového systému[26]. Méně konkrétní povinnost je vyjádřena v zákoně 365/2000 Sb. o ISVS, který ukládá tvorbu informační koncepce v orgánu veřejné správy[27]. V prováděcích předpisech, jmenovitě ve Vzorové informační koncepci, jsou v kapitole 6.1.2 uvedeny mimo jiné požadavky na kvalitu a požadavky na bezpečnost, vyplývající z dlouhodobých cílů řízení kvality a dlouhodobých cílů řízení bezpečnosti, a požadavky na testování[28]. Bližší specifikaci však ISVS neuvádí.

2.6.1 Audit informační bezpečnosti

Nejširší variantou jsou informační bezpečnostní audity, které se zaměřují na komplexní posouzení bezpečnosti ve všech oblastech, ať již jde o nastavení bezpečnostních charakteristik systémů v souladu s best practice (nejlepší praxí) nebo s platnou legislativou. Například v souvislosti s nedávnými změnami v oblasti ochrany osobních údajů se tyto testy v současnosti často zaměřují na shodu s GDPR. Dále se, v případě orgánů veřejné správy, může jednat o soulad se ZoKB. V takovém případě jde o posouzení bezpečnostních politik, směrnic, systému řízení a technických opatření, zda odpovídají uvedenému zákonu. Také může být zaměřen na bezpečnostní procesy a jejich nastavení, včetně náplně a obsazení bezpečnostních rolí. V hledáčku často bývají incident response procesy (procesy odezvy na bezpečnostní incidenty), disaster recovery procesy (procesy obnovy po havárii) a business

[26] ČESKO. § 25 odst. 1 písm. a) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 13. 3. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#p25-1-a

[27] ČESKO. § 5a odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 2. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365#p5a-2

[28] KUBĚNKA, Pavel. Vzorové informační koncepce: Vzorová informační koncepce ústředního orgánu veřejné správy [online]. 2.8.2006, , 46 [cit. 2020-04-02]. Dostupné z: https://www.mvcr.cz/soubor/informacni-koncepce-ustredniho-organu-verejne-spravy.aspx

continuity plan (plány kontinuity provozu). V technické oblasti jde většinou o zjištění stavu hardware nebo software, zabezpečení dat, konfigurace bezpečnostních prvků, bezpečnostního monitoringu a jeho nastavení, prověření vzdáleného přístupu nebo přístupu privilegovaných uživatelů. Mnohdy je audit též doplněn i o kontrolu fyzické bezpečnosti nebo se naopak soustředí na prostředí třetích stran, například dodavatelů, a to i na bezpečnost jejich vývoje a kódování, případně interní nebo externí personální spolehlivost nebo hodnotí úroveň bezpečnostního povědomí a úroveň interního systému školení v oblasti informační bezpečnosti. Speciálními typy auditů jsou pak penetrační testy, skeny zranitelností nebo dokonce i test odolnosti proti sociálnímu inženýrství, které se věnují praktickému ověření reálného stavu v prostředí organizace.

2.6.2 **Penetrační testy**

Penetrační testování je způsob nebo snaha napodobit útočníka a jde primárně o praktické ověření možnosti kompromitovat interní prostředí organizace nebo jeho vybranou část. Tuto činnost je možné realizovat ve vlastní gesci nebo pomocí zajištění smluvních partnerů. Na základě zadání se tester vždy snaží proniknout do vybraných systémů nebo prostředí a za účelem zhodnocení úrovně jejich zabezpečení vyhotovuje závěrečnou zprávu se shrnutím učiněných nálezů. V souvislosti s tím je možné tuto činnost doplnit i o vlastní pozorování, například je možné testy monitorovat prostřednictvím vlastních bezpečnostních technologií a ověřit schopnost bezpečnostní infrastruktury zachytit potencionální útoky. Smyslem celých testů je pak náprava a přijetí dalších vhodných opatření, které mají napravit zjištěné slabiny. Zde bývají častým problémem neaktualizované systémy nebo i celý chybějící proces aktualizací v informačním prostředí. Zásadním problémem při realizaci a zadávání bezpečnostních testů a i penetračních, bývá rozsah očekávání, tedy to, co má být jejich výsledkem. Bylo by chybné se domnívat, že po jejich provedení a odstranění chyb je již systém zcela bezpečný. Je nutné mít na paměti, že penetrační test ověřuje zranitelnost slabých míst vždy jen v konkrétních případech, vztahujících se k danému systému a jeho aktuálnímu nastavení a tedy ověří, zda je možné kompromitovat systém pouze ve zvoleném vektoru a čase. Neříká již ale nic o tom, zda nemohou existovat slabiny nebo zranitelnosti na jiných místech, které nebyly testovány, případně zda se zde vyskytnou v budoucnosti. Je to především z důvodu časové omezenosti prováděných testů, kdy v rámci zvoleného intervalu lze provést jen vymezenou část testů a vzhledem k času v odpovídajícím detailu.

Je tedy nutné využít heuristický přístup a z velké množiny všech možností vybrat jen omezený počet vhodných způsobů prověření. Ve většině případů tento výběr provádí tester na základě vlastních zkušeností a s ohledem právě na tuto skutečnost, je obecně více problematická standardizace v této oblasti. Důvodem je fakt, že tester se vždy snaží do systému proniknout jakýmkoli možným způsobem a bez ohledu na standardy zkouší všechny dostupné metody a postupy, jelikož jde předně o praktické zneužití slabin, průnik a ovládnutí systému. Standardizace však může pomoci definovat rozsah zadání testů. Při jejich plánování a realizaci nebude takto žádná oblast opomenuta. Také při zachování shodné metodologie, je provádění a srovnávání opakovaných testů výrazně snadnější. Z důvodu těchto přínosů je doporučováno prioritně její použití. Při pravidelném testování, pokud dochází i k odstranění vad, by se měla četnost průniků snižovat. Celý cyklus přitom napomáhá k udržování kontaktu s realitou, kdy při větším množství používaných technologií není možné vždy zajistit, aby byly všechny proklamované vlastnosti v souladu s potřebami a požadovanou bezpečnostní úrovní v organizaci. Testy též mohou poukázat na provozní slepotu v určitých případech, předně při správě systémů s dlouhodobým životním cyklem nebo na chybějící přehled napříč celým prostředím, a tedy i v komunikaci mezi jednotlivými systémy.

Pokud jde o realizaci testů pomocí externích subjektů, je nutné se na samém začátku zabývat jejich přesným zadáním. Ještě problematičtější je specifikace penetračních testů v rámci výběrových řízení ve státní správě. Pro základní definici se určuje typ a rozsah testů, viz zjednodušený přehled:

- Externí penetrační testy
- Interní penetrační testy
- Penetrační testy webových aplikací
- Penetrační testy mobilních aplikací
- Penetrační testy mobilních sítí

typ testování:

- Black box
- White box
- Grey box

Rozsahem je možné se zaměřit na konkrétní systém či zařízení nebo provádět testy v celé šíři perimetru. Důležité hledisko pak bývá samotná invazivnost testů, a tedy jejich možné dopady do provozu. Za tímto účelem je možné požadovat deklaraci úpravy jejich intenzity nebo možnost stanovit vhodná provozní okna, například v nočních časech nebo o víkendech. Je ale nutné mít na paměti, že cena práce v těchto termínech bývá odlišná od běžné sazby a může mít dopad do smluvních podmínek. Proto je v zadáních uváděn požadovaný časový režim realizace. Při hledání vhodného partnera v soukromé sféře je možné sledovat reputační hledisko u jednotlivých firem a zohlednit jej při výběru. Ve státním sektoru je jeho kvantifikace problematická a nelze jej zcela zohlednit v rámci zadávacího řízení. Také výsledky a nálezy již realizovaných testů v jiných organizacích nebývají veřejné a zkušenosti s jednotlivými subjekty poskytující tyto služby nejsou mnohdy dostupné, případně jsou nesrovnatelné. Je ale možné zadat kvalifikační kritéria a požadovat zkušenosti v relevantních oblastech nebo vyžadovat odpovídající reference, jako je například délka praxe nebo velikost testovaných organizací. Zvláštní pozornost je třeba věnovat vlastnickým vztahům mezi dodavatelem systému nebo jeho provozovatelem a firmou, která provádí jejich realizaci. Základní podmínkou testů je totiž jejich nezávislost a není tedy možné akceptovat situaci, kdy jeden a týž subjekt provádí dodávku a testování. V případě rozsáhlejších nebo dlouhotrvajících projektů je možné realizovat vzorový penetrační test se zprávou a dle výsledků pak ohodnotit předpokládanou kvalitu a až následně provést výběr jejich dodavatele. Dalším vhodným parametrem výběru je certifikace, kdy pro tento typ testů bývá zpravidla doporučováno požadovat spíše její technické zaměření.

Odpovídající technické certifikace:

- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Licensed Penetration Tester (LPT) Master
- IACRB Certified Penetration Tester (CPT)
- Certified Expert Penetration Tester (CEPT)
- Certified Mobile and Web Application Penetration Tester (CMWAPT)
- Certified Red Team Operations Professional (CRTOP)
- CompTIA PenTest+
- Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

- Offensive Security Certified Professional (OSCP)[29]

V České republice jsou nejběžnějšími vyskytujícími se certifikáty OSCP a CEH nebo CPT. Certifikát a zkouška OSCP je ale například technicky náročnější než u CEH, v jejím průběhu se provádí reálné testování na pěti přidělených serverech a související infrastruktuře, včetně sepsání zprávy a nutnosti zvládnout předepsaná cvičení. Je tedy často preferován, i když počet osob, které jím disponují, je výrazně nižší než u konkurence. Také je možné vyžadovat postup dle dotčeného standardu, například pro testování webových aplikací využít standardu OWASP a podobně.

Pokud možno, je pro zachování odpovídající úrovně nutné vyžadovat konkrétní osoby nebo realizační tým. To ve svém důsledku znamená, že testy pak bude provádět osoba uvedená ve smlouvě, včetně prokázané kvalifikace a nikoli junior bez odpovídajících zkušeností. Samozřejmě se v rámci výběrového řízení hodnotí i cena, která se běžně uvádí v člověkodnech nebo člověkohodinách, ale je důležité vyžadovat i cenu celkovou, aby nemohlo docházet k nežádoucímu navýšení nebo manipulacím.

Dalším zásadním krokem, který následuje a bývá často podceňován, je příprava prostředí pro testování. Jedná se například o nastavení účtů pro testery nebo specifického prostředí, včetně zapůjčení výpočetní techniky nebo poskytnutí odpovídajících prostor. U větších organizací je proto nutné počítat s jistou časovou rezervou, která může být i v řádu týdnů. Tyto činnosti by měl provádět určený koordinátor na straně testované organizace. Ten také dohlíží na průběh testů a iniciuje jejich zastavení, pokud dojde k narušení běhu aplikací nebo systémů, případně reaguje na vygenerované odezvy a zprávy. Následující fáze se sestává ze samotného testování a je ukončena závěrečnou zprávou. Obě fáze mohou být přibližně stejně časově náročné a je tedy opět nutné počítat s jistou časovou dotací pro stanovení termínu ukončení. Závěrečná zpráva by měla obsahovat několik částí. První z nich je manažerské shrnutí, které zpravidla neobsahuje příliš technických detailů, ale obsahuje veškeré nálezy a opatření, a prezentuje je pomocí přehledných tabulek nebo grafů. Rozsah maximálně jedna strana. Další část by měla obsahovat harmonogram, tedy časový průběh testů, nejlépe s uvedením jednotlivých dnů a časů, ve kterých byly prováděny a také například IP adresy obou komunikačních stran. Nutné je vždy uvést původní zadání a možná omezení, která

[29] Top 10 Penetration Testing Certifications for Security Professionals. INFOSEC [online]. Herndon: Infosec Resources 2020, 2019 [cit. 2020-03-07]. Dostupné z: https://resources.infosecinstitute.com/top-5-penetration-testing-certifications-security-professionals/

vznikla během testování, například když systém začal vykazovat závažné chyby a nebylo možné jej dále testovat či velmi dlouhé odezvy, které znemožnily další pokračování a podobně. Zásadní je pak ta část zprávy, která uvádí všechny nalezené problémy, včetně detailního popisu. Ten by měl být co nejpřesnější a doplňuje jej doporučení s návodem na odstranění jednotlivých problémů. K závěrečné zprávě je vhodné uskutečnit informativní schůzku, na které se vypořádají možné nejasnosti, detaily a upřesní se význam jednotlivých nálezů nebo doporučení. Teprve pak je možná formální akceptace testu. Manažer nebo koordinátor test konzultuje s jednotlivými administrátory systému za účelem odstranění false-positive nálezů nebo úpravy stanovených závažností a priorit. Ze závěrečné zprávy a z jednání by měly vyplynout konkrétní úkoly jednotlivým odpovědným osobám v organizaci, a to i s termíny pro jejich realizaci. V následném kroku se pak provádí opakovaný test (takzvaný retest), který se zaměřuje pouze na ověření odstranění zjištěných chyb.

Vhodným instrumentem pro celou organizaci je zahrnout do bezpečnostní strategie plán pravidelných penetračních testů v krátkodobém a střednědobém horizontu.

2.6.3 **Standardy testování bezpečnosti**

Tato kapitola popisuje běžné známé nebo využívané standardy v oblasti penetračního nebo i obecněji bezpečnostního testování. Ty je možné použít nejen ve fázi zadávání a přípravy smluvní dokumentace, ale i pro požadavky a realizaci testů samotných, včetně vypracování zprávy z testování.

2.6.3.1 PTES

Tato norma k provádění penetračního testování se skládá ze sedmi hlavních částí. Ty pokrývají vše, co může souviset s penetračním testováním, od plánování a počáteční komunikaci v přípravě testů, až po fázi sběru informací a modelování hrozeb, kde se testeři seznamují s pozadím a informačním prostředím s cílem lépe porozumět testované organizaci, a to pomocí testování zranitelností a jejich exploitací[30]. Technické zkušenosti testerů se zde kombinují s obchodním zaměřením organizace. Tato cílená synergie se

[30] Jedná se o reálnou možnost zneužití zranitelnosti např. pomocí existujících postupů nebo nástrojů tzv. exploitů (pozn. autora).

následně promítne do závěrečné zprávy, která zachycuje celý proces a způsob tak, aby zákazníkovi poskytla informace v co nejvíce srozumitelné míře.

V současné době je za její základ považovaná verze 1.0, která byla ověřena a průmyslově testována více než jeden rok v příslušném odvětví. Připravuje se verze 2.0, která by měla poskytovat podrobnější pohled na jednotlivé úrovně a jejich prvky, na kterých se penetrační testy provádějí. Vzhledem k tomu, že testy nejsou nikdy totožné (ani ve svém rozsahu), bude zahrnovat celou jejich škálu od nejběžnějších webových aplikací nebo sítí až po plné nasazení včetně speciálního testovacího týmu (red team). Uvedené úrovně umožní organizaci definovat, jakou sofistikovanost útoků očekávají, a umožní testerům zaměřit se na oblasti, kde je organizace nejvíce očekává.

Hlavní kapitoly definované standardem jako základ pro provedení penetračního testování:

- Iniciační interakce
- Sběr informací
- Modelování hrozeb
- Analýza zranitelností
- Exploitace
- Post exploitace
- Reporting[31]

2.6.3.2 OSSTMM

Jedná se o projekt Institutu pro bezpečnost a otevřenou metodiku (ISECOM), který je komunitně rozvíjen a následně podrobován vzájemnému a mezioborovému přezkumu. ISECOM je nezisková organizace se sídlem v New Yorku, USA a ve Španělsku. Příručka metodiky Open Source Security Testing Metodical Guide (OSSTMM) poskytuje metodologii pro auditní bezpečnostní test, označovaný jako audit OSSTMM. Ten se zaměřuje na přesné měření bezpečnosti na provozní úrovni, a to bez zavádějících předpokladů a neověřitelných faktů. Metodika je navržena tak, aby byla konzistentní a opakovatelná. Jako projekt s otevřeným zdrojovým kódem umožňuje testerům bezpečnosti

[31] IFTACH, Ian Amit. PTES: The Penetration Testing Execution Standard [online]. 2014 [cit. 2020-03-07]. Dostupné z: http://www.pentest-standard.org/index.php/Main_Page

všech projektů přispívat nápady k provádění přesnějších a účinnějších bezpečnostních testů[32].

2.6.3.3 ISSAF

Information Systems Security Assessment Framework je rámec, který se zaměřuje na testování bezpečnosti a člení ji do několika oblastí. Ty obsahují detailní specifikace testovacích kritérií. Standard udržovala nezisková organizace OISSG – Open Information Systems Security Group, ale v současnosti není dále rozvíjen. Je však ponechán jako základ pro vytváření individuálních metodik. Kritéria obsahují jejich popis pro testování, cíle a záměry, vstupní předpoklady pro provedení testu, proces testování, zobrazení očekávaných výsledků, doporučené protiopatření, reference a externí dokumenty.

Celkově je rámec poměrně detailní a má velký záběr, autoři se v něm snaží poskytnout maximum informací k provádění testů. Uživatelé a testeři se pak mohou více soustředit na jejich realizaci a nemusí se příliš věnovat jejich konstrukci. Jednou ze silných stránek je to, že spojuje jednotlivé testy a testovací nástroje.

Metodologie pro penetrační testování ISSAF byla navržena tak, že umožňuje obsáhnout většinu typů testování a pokrývá jejich proces od začátku až po jejich ukončení. V testování se postupuje ve třech fázích:

A. Plánování a příprava
B. Testování
    1) Sběr informací
    2) Mapování sítě
    3) Identifikace zranitelností
    4) Průnik
    5) Získání přístupu a eskalace oprávnění
    6) Enumerace
    7) Kompromitace vzdálených účtů
    8) Zachování přístupu
    9) Zametání stop
C. Reporting a úklid stop[33]

[32] BARCELÓ, Marta a kol. OSSTMM 3 – The Open Source Security Testing Methodology Manual [online]. ISECOM, 2010 [cit. 2020-03-07]. Dostupné z: https://www.isecom.org/OSSTMM.3.pdf
[33] ISSAF: Files [online]. 2005 [cit. 2020-03-08]. Dostupné z: https://sourceforge.net/projects/isstf/

První fáze popisuje kroky při výměně počátečních informací se zákazníkem, plánování a přípravu na testování. Tato fáze je krátká a popisuje pouze kroky k výměně počátečních informací, plánování a přípravu testu. Zdůrazňuje, že před zahájením jakéhokoli testování musí být podepsána formální dohoda o posouzení. Smlouva poskytuje základ pro toto testování a vymezuje vzájemnou právní ochranu. Doporučení obsahu stanoví:

- Zákaznické týmy
- Přesná data a časy
- Eskalační cestu
- Jakákoli jiná ujednání

Aktivity:

- Nastavuje se komunikační kanál mezi společností a týmem zabraňujícím úniku
- Určuje se rozsah, přístup a metodika
- Ustanoví se dohoda o konkrétních testech a jejich eskalaci

Druhá fáze obsahuje devět jednotlivých kroků samotného testování.

Nejdříve se provádí získávání informací, pomocí technických i netechnických metod dojde k vyhledání informací o cílech. Dále dojde k mapování sítě, kde se identifikují všechny systémy a zdroje v cílové síti. Identifikují se chyby v zabezpečení a odhalují se zranitelnosti v cílových assetech[34]. Pokračuje se jejich zneužitím a získáním neoprávněného přístupu obejitím bezpečnostních opatření. Po získání přístupu se eskaluje oprávnění, což je snaha o získání co možná nejvyšších práv, nejlépe na úrovni administrátora (root box). Enumerací se pak získává další výčet informací o procesech v systémech s cílem jejich dalšího možného využití. Pokud dojde ke kompromitaci vzdálených účtů, je možné využít vztah důvěry a komunikace mezi vzdálenými uživateli a podnikovými sítěmi. Pomocí skrytých kanálů, zadních vrátek a rootkitů je možné skrýt přítomnost hackera a poskytovat mu nepřetržitý přístup do systému. Zametání stop pak eliminuje všechny známky kompromitace skrýváním souborů, vymazáváním protokolů, narušením kontrol integrity nebo obejitím antivirového softwaru.

Třetí fáze popisuje vytváření reportu a úklid po ukončení testování. Pokud úklid není možné provést vzdáleně, je nutné o veškerých provedených změnách a přidaných souborech napsat do reportu, aby tyto změny mohly být opraveny příslušnými pracovníky. Soustředí se též na

[34] Asset je terminologický pojem v oblasti správy zranitelností, vyjadřující libovolný typ zařízení (pozn. autora)

komunikační kanály a typ zpráv v projektu. Jsou podporovány hlavní dva způsoby předávání zpráv: ústní a písemný. Ústní hlášení je vyhrazeno pouze pro kritické nebo naléhavé problémy. Ústní komunikace by měla být použita v případech, kdy je identifikován problém, který vyžaduje okamžitou pozornost. Například závažné zjištění zranitelnosti a kompromitace. Písemná forma se pak vyžaduje u závěrečné zprávy.

2.6.3.4 WASC Threat Classification

Web Aplication Security Consortium (Konsorcium Webové Aplikační Bezpečnosti) je nezisková organizace sdružující mezinárodní skupiny odborníků, zástupců průmyslu a organizací spolupracujících na otevřeném standardu v oblasti webových aplikací. Dokument WASC Threat Classification 2.00 (Klasifikace Hrozeb 2.00) byl vytvořen za účelem sjednocení terminologie při vývoji a podpoře a pro jednoznačný popis bezpečnostních problémů v oblasti webů. Vývojáři aplikací, odborníci na bezpečnost, prodejci softwaru a auditoři tak mohou využívat pojmů a jednotného jazyka souvisejícího s webovou bezpečností.

Dokument detailně popisuje útoky a slabiny, které mohou vést ke kompromitaci webových stránek, jejich dat nebo uživatelů a slouží především jako referenční příručka pro jednotlivý daný útok nebo slabinu a poskytuje návod k dotčenému okruhu problémů a je využitelný také jako referenční materiál. Je tedy využíván následujícími způsoby:

- REFERENČNÍ MATERIÁL – primární použití je jako referenční příručka, na kterou lze odkazovat v bezpečnostních zprávách, bezpečnostních auditech, prezentacích a dalších. Obsah i odkazy se vyskytují v řadě knih s bezpečnostní tématikou, u bezpečnostních produktů a v systémech klasifikace zabezpečení třetích stran.
- KONTROLNÍ LIST V HODNOCENÍ BEZPEČNOSTI – při testování aplikací slouží jako výčet hrozeb, které mohou být použity k sestavení plánu penetračních testů.
- BUG TRACKING (SYSTÉM SLEDOVÁNÍ CHYB) - dalším způsobem využití je shromažďování metrik o bezpečnostních chybách v systémech, které mohou ovlivnit chod organizace. Při zadávání bezpečnostních chyb do systému sledování chyb se

přiřadí k nálezu slabina nebo vektor útoku a identifikuje se četnost a výskyt konkrétních hrozeb v dané organizaci.[35]

Svojí formou se již WASC Threat Classification částečně blíží bezpečnostním číselníkům a jde o jakousi přechodovou fázi mezi standardem a skóringovým systémem.

2.6.3.5 OWASP

Open Web Application Security Project (OWASP) je nezisková nadace, která podporuje zlepšování bezpečnosti softwaru, a to primárně se zaměřením na webové aplikace. Mezi její hlavní programy lze zařadit jednotlivé informačně-bezpečnostní komunitní projekty realizované ve více než 275 lokálních skupinách a celkově s desetitisícem členů po celém světě. Věnuje se také osvětě a pořádáním vzdělávacích konferencí se shodnou tématikou. Jde o otevřenou platformu a komunitu zaměřenou na podporu důvěryhodné koncepce, vývoje, provozu a údržby aplikací. Všechny její projekty, nástroje, dokumenty a fóra jsou zdarma (v rámci licence FLOSS[36]) a umožňují širokou spolupráci na zvyšování bezpečnosti aplikací. Nadace OWASP byla založena 1. prosince 2001. V Evropě má sídlo v Belgii.
Hlavními projekty OWASP jsou:

- **OWASP Top Ten**

  Standard je dokument pro vývojáře a bezpečnostní specialisty webových aplikací, který reprezentuje široký konsenzus a shodu na nejvíce kritických zranitelnostech v této oblasti. Je podkladem pro zjednodušenou verzi testování a firmy mohou použít tento dokument pro nastartování procesu ověřování webových aplikací tak, aby na začátku co možná nejrychleji minimalizovaly nejzávažnější rizika. Je vhodný jako první krok v procesu zabezpečení a jako doplněk k jiným standardním postupům, a to velice efektivním. Pro dané období je vždy vyhlášeno 10 nejvíce kritických webových zranitelností a testy, které se dle této metodiky provádějí, prověřují aplikace právě na tyto chyby. Poslední platná verze je z roku 2017, ale nyní se již pracuje na další verzi. Její vydání je plánováno na březen až květen 2020.
- **OWASP Cheat Sheet Series**

[35] SYED, Mohamed A a spol. WASC Threat Classification: version 2.00 [online]. Verze 2. WEB APPLICATION SECURITY CONSORTIUM, 2010 [cit. 2020-03-08]. Dostupné z: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf
[36] Viz seznam zkratek.

(OWASP Cheaty) byly vytvořeny, aby poskytovaly jednoduché a srozumitelné návody pro aplikační vývojáře a bezpečnostní specialisty. Nejsou tolik zaměřené na detaily best-practice (dobré praxe), ale více na její snadnou použitelnost, právě při vývoji a také implementaci. Jsou dále provázány s projekty OWASP Proactive Controls a OWASP ASVS, se kterými tvoří de facto jeden celek. Zde je nutné zvlášť upozornit na ASVS, který představuje komplexní standard pro užití tvorby aplikace, a to v rámci jejího celého životního cyklu.

- **OWASP Dependency-Track**

  je inteligentní platforma pro průběžnou analýzu kontinuálních dodávek komponent a umožňuje identifikovat a snižovat riziko používání Open Source komponent a komponent třetích stran. Jedná se o jedinečný a vysoce užitný přístup s využitím schopností tzv. Software Bill-of-Materials (SBOM). Umožňuje tím trvale sledovat použití komponent, a to ve všech verzích aplikace a aktivně identifikovat rizika v celé šíři organizace. Platforma má API design, který je ideální pro použití v prostředích s procesem kontinuálních dodávek a integrací.

- **OWASP Juice Shop**

  Moderní a sofistikovaná nezabezpečená webová aplikace a je možné ji použít jako vhodný studijní materiál a na demonstraci bezpečnostních ochran a postupů. Kromě zranitelností OWASP Top Ten obsahuje i mnoho dalších chyb a nedostatků existujících v běžných reálných aplikacích. Je možné na ní zkoušet penetrační testy nebo provádět školení hackerů. Juice Shop je napsán v Node.js, Expressu a Angularu a jedná se tedy o aplikaci pojatou v Javascriptu. Zcela tak poskytuje možnost si v této aplikaci ověřit, jak se bezpečnostní nástroje dokáží vypořádat s aplikačními rozhraními s vysokým obsahem Javascriptu a REST API.

- **OWASP Mobile Security Testing Guide**

  Tento projekt se věnuje tvorbě bezpečnostního standardu pro testování mobilních aplikací a poskytuje průvodce, který pokrývá potřebné procesy techniky a nástroje které se zde používají.

- **OWASP ModSecurity Core Rule Set**

  Jedná se o souhrn pravidel pro webový aplikační firewall ModSecurity, který obsahuje obecné definice na ochranu před známými útoky proti široké škále

zranitelností ve webovém provozu, včetně hlavních definic z OWASP Top Ten. Snaží se též o maximální možnou eliminaci falešně-pozitivních upozornění.

- **OWASP SAMM**

  Je sebehodnotící rámec poskytující měřitelné postupy při analýze vlastní organizace a její snaze zlepšit bezpečnost software při návrhu, vývoji a dodávkách. Jde o postupy řízené vlastním zlepšováním a na základě rizik. Bere v potaz specifika, která jsou pro každou organizaci rozdílná.

- **OWASP security Knowledge Framework**

  Online znalostní báze s informacemi o bezpečnostních aspektech a sadou nástrojů pro tvorbu kódu, pro použití vývojovými týmy. Umožňuje integraci zabezpečení již v konceptu webových aplikací. Jedná se o otevřenou databázi znalostí o zabezpečeních a obsahuje kontrolní seznamy a příklady kódů, včetně osvědčených postupů v různých programovacích jazycích s ukázkami např. autentizační ochrany a znemožnění zneužití pomocí exploitů apod. Podporuje architekturu bezpečnosti a její zohlednění již při plánování a návrhu a vychází z OWASP (M)ASVS.

  Hlavní členění databáze:

  - Kontrolní listy
  - Znalosti
  - Kód (tvorba)
  - Laby (laboratorní cvičení)

- **OWASP Web Security Testing Guide**

  Tento projekt se zaměřuje na tvorbu postupů na bezpečnostní testování webových aplikací. Existuje i jeho varianta pro mobilní aplikace. Jde o komplexního průvodce obsahujícího detailní popis osvědčených postupů používaných penetračními testery a organizacemi. Obsahuje i odkazy na vhodné testovací nástroje a utility. Vyznačuje se rámcem pro testování v celém SDLC cyklu, tedy už před samotným zahájením vývoje, během definování a návrhu, vývoje i později při provozu a údržbě aplikace. Testování samotné je zde rozděleno do tří fází:

  - Pasivní mód – provádí se sběr informací o systému
  - Aktivní mód – v této fázi dochází k provádění samotných testů rozčleněných do jedenácti podkategorií a celkem jednadevadesáti kontrol

- Reporting – konečná fáze, člení se do tří částí – manažerský pohled, testovací parametry a nálezy

Testy jsou rozděleny do jednotlivých kategorií. Každá z nich má pevné označení „TEST ID“, které se skládá z polí „OTG-PREFIX-ČÍSLO“. Je tedy možné záznamy strukturovat a dále je analyticky zpracovávat.

V současné době je platná OTG ve verzi 4.0 a v přípravě je její nástupce v podobě verze 5.0.

- **OWASP ZAP**

  Zed Attack Proxy (ZAP) je bezplatný nástroj pro penetrační testování s otevřeným zdrojovým kódem, který je udržován komunitou projektu Open Web Application Security Project (OWASP). ZAP byl navržen speciálně pro testování webových aplikací. Podstatou ZAP je model známý jako „man in the middle“. Její pozice je tedy mezi prohlížečem testera a webovou aplikací, kde může zachytávat a kontrolovat zprávy odesílané mezi prohlížečem a webovou aplikací a v případě potřeby upravovat obsah této komunikace. Může být použita jako samostatně běžící aplikace nebo i na pozadí, jako systémová služba. Lze jí nakonfigurovat na zachytávání samostatných komunikačních kanálů nebo ji připojit na již existující proxy server organizace.

  ZAP poskytuje celou řadu funkcí pro různé úrovně činností vývojářů a specialistů na testování zabezpečení. Jsou dostupné verze pro všechny druhy hlavních operačních systémů a též pro Docker (systémově nezávislá kontejnerizační platforma). Přímo z klienta ZAP jsou pak dostupné i další funkce, pomocí různých doplňků ze ZAP Marketplace.

  Protože je vyvíjena v rámci Open-Source licence, je možné zkoumat a měnit její zdrojový kód. Je také přesně zřejmé, jaké funkce a jak jsou zde implementovány. Ty je pak možno dále komunitně řídit, opravovat chyby, přidávat funkce na základě změnových požadavků a také vytvářet doplňky k podpoře specializovaných funkcí.

2.6.4 Skóringové systémy a katalogy

V této kapitole je popis databází, rejstříků a seznamů používaných v oblasti zranitelností a slabin, které obsahují hodnotící škály, popisy a další detailní informace, případně

i využitelné nástroje. Ty slouží obvykle pro analytickou činnost se zaměřením na detekci, ocenění a odstraňování zjištěných nálezů.

2.6.4.1 CVSS-SIG

The Common Vulnerability Scoring System – CVSS (Běžný systém hodnocení zranitelnosti) je otevřený systém nebo také rámec pro sdělování charakteristik a závažnosti zranitelností softwaru. CVSS zde sleduje tři hlavní metriky: Base, Temporal a Environmental. Skupina Base se zaměřuje na vnitřní vlastnosti zranitelnosti, které jsou v průběhu času a v uživatelských prostředích konstantní, skupina Temporal odráží vlastnosti zranitelností, které se v průběhu času mění, a skupina Environment představuje vlastnosti zranitelností, které jsou jedinečné pro uživatele a jeho prostředí. Base metrika produkuje skóre v rozsahu od 0 do 10, kterou lze pak upravit bodováním v rámci metrik Temporal a Environment. CVSS skóre je také reprezentováno významově jako vektorový řetězec, představující komprimované textové znázornění hodnot použitých k odvození skóre. Aktuální platná verze vyšla v červnu 2019 a je ve specifikaci verze 3.1. Její další vývoj a zlepšování zajišťuje v rámci CVSS průběžně skupina SIG (Special Interest Group), která je složena ze zástupců průmyslového, finančního, technologického a akademického sektoru. CVSS tedy především poskytuje způsob, jak vytvořit číselné skóre zranitelnosti, které skutečně odráží její závažnost.
Pro zjednodušené použití je k dispozici kalkulátor, prezentovaný online.[37]
Skóre lze následně převést do kvalitativní reprezentace a použít v procesech správy zranitelností.

2.6.4.2 CWE

Common Weakness Enumeration (CWE) je komunitně vyvinutý seznam běžných typů slabin softwaru a hardwaru, které mají své bezpečnostní dopady. „Slabiny“ jsou zde nedostatky, chyby v kódu, nebo jiné chyby v implementaci softwaru nebo hardwaru, designu nebo architektuře, které, pokud by byly zneužity, by mohly mít za následek jejich celkovou zranitelnost. Seznam CWE a související klasifikační taxonomie slouží jako prostředek, který lze použít k identifikaci a popisu těchto slabin. CWE spolupracuje s komunitou odborníků

[37] First - improving security together: Common Vulnerability Scoring System Version 3.1 Calculator [online]. 2019 [cit. 2020-03-08]. Dostupné z: https://www.first.org/cvss/calculator/3.1

v oblasti vývoje a zabezpečení a hlavním cílem je eliminovat zranitelnosti u zdroje jejich vzniku. Toho lze dosáhnout vzděláváním architektů, návrhářů, programátorů a poskytováním informací o tom, jak odstraňovat nejčastější chyby při vývoji a dodání softwaru a hardwaru. V konečném důsledku pomáhá předcházet těm druhům bezpečnostních chyb, které trápí softwarový a hardwarový průmysl. Seznam CWE obsahuje konkrétní typy softwarových a hardwarových slabin. Vydán byl poprvé v roce 2006 a původně se zaměřoval jen na slabiny softwaru. V posledních letech se však objevily problémy i s hardwarovou bezpečností (např. zranitelnosti LoJax, Rowhammer, Meltdown / Specter) s velkými dopady do provozu podnikových systémů. Souběžně se rozvíjí též oblast IoT obecně, od průmyslových řídicích systémů a lékařských zařízení až po automobily a přenositelné přístroje. Z tohoto důvodu byla v roce 2020 do seznamu CWE přidána podpora pro hardwarové slabiny.[38]

Od začátku je vytvoření seznamu komunitní iniciativou s cílem vyvinout konkrétní a stručné definice pro každý společný typ slabin, včetně související stromové struktury a v průběhu času jí vylepšovat. Využitím co nejširší možné skupiny zájemců je zajištěno, že je každá položka v seznamu náležitě popsána a diferencována.

Externí mapování pak umožňuje vytvářet skupiny, které souvisí i s jinými externími faktory nebo pohledy. Jako příklad by bylo možné uvést CWE VIEW pro Weaknesses in OWASP Top Ten (2017). Zde jde o specifickou stromovou hierarchii, kde skupiny OWASP Top Ten představují skupinové slabiny, které sdílejí společnou charakteristiku. Pod těmito položkami se nacházejí slabiny různé úrovně abstrakce a prezentují její konkrétní druh a dále následuje její varianta, která je již popsána velmi detailně a vztahuje se ke konkrétní technologii.

2.6.4.3 CVE

CVE je jedním z nejznámějších a nejpoužívanějších seznamů v informatice, obsahujícím unikátní identifikační čísla, s minimálně jedním veřejným odkazem na obecně známou zranitelnost nebo chybu v oblasti kybernetické bezpečnosti. CVE záznamy jsou mnohdy přímo implementovány v mnoha produktech a službách týkajících se kybernetické bezpečnosti z celého světa, včetně americké národní databáze chyb zabezpečení (NVD).

[38] Common Weakness Enumeration: A Community-Developed List of Software & Hardware Weakness Types [online]. MITRE, February 10, 2020 [cit. 2020-03-08]. Dostupné z: https://cwe.mitre.org/about/index.html

Položky CVE (označované jinak také jako „identifikátory CVE“ apod.) jsou jedinečné identifikátory pro veřejně známé zranitelnosti kybernetického zabezpečení.
Položky CVE jsou definovány následovně:

- CVE ID číslo se čtyřmi nebo více číslicemi v části ID sekvence (např. "CVE-1999-0067", "CVE-2014-12345", "CVE-2016-7654321")
- Stručný popis bezpečnostní chyby nebo expozice
- Jakékoli související odkazy (tj. informace o zranitelnosti a rady)

Iniciátorem a správcem je nezisková organizace MITRE, která se soustředí na spolupráci ve veřejném a vládním sektoru, v průmyslu i na akademické půdě. Věnuje se oblastem umělé inteligence, intuitivní vědě o datech, kvantové vědě o informatice, zdravotnické informatice, vesmírné bezpečnosti, politickým a ekonomickým expertizám, důvěryhodné autonomii, sdílení počítačových hrozeb a kybernetické odolnosti.

2.6.4.4 CAPEC

Projekt CAPEC (Common Attack Pattern Enumeration and Enumeration and Classification) poskytuje veřejně přístupný katalog známých vzorů útoků, který má uživatelům pomoci pochopit, jak lze dosáhnout zneužití slabin v aplikacích a dalších systémech obsahujících kybernetické hrozby. „Attack Patterns“ - (vzory útoků) jsou popisy společných atributů a postupů používaných k využití známých slabých stránek a možnosti ověření těchto postupů. Vzory útoků definují výzvy, kterým může tester čelit a návod, jak postupovat při jejich řešení. Vyplývají z konceptu návrhu vzorů aplikovaných spíše v destruktivním než konstruktivním kontextu a jsou generovány z hloubkové analýzy konkrétních příkladů jejich skutečného užití. Každý vzor útoku obsahuje znalosti o tom, jak jsou konkrétní části útoku navrženy a provedeny, a poskytuje také návod, jak zmírnit účinnost takového útoku. Vzory útoků pomáhají při vývoji aplikací nebo správcům systémů nebo funkcí zajišťujících kybernetickou komunikaci. Jejich pomocí lze lépe porozumět konkrétním prvkům útoku a možnostem ochrany před jejich působením[39].
Je možné je tedy využít pro praktickou simulaci útoku. Gestorem projektu je opět nezisková organizace MITRE, jako v případě CVE, uvedená v předchozí kapitole.

[39] CAPEC: About CAPEC [online]. MITRE, April 04, 2019 [cit. 2020-03-08]. Dostupné z: https://capec.mitre.org/about/index.html

3 Analytická část

Tato část obsahuje informace zjištěné v prostředí zkoumané organizace, tedy jak je architektonicky koncipována její infrastruktura a jak na ní navazuje dotčený informační systém. Jak je tento systém sám o sobě koncipován a z čeho se skládá. Následně je vybrána vhodná podoblast zvolené metodologie a je stanoven způsob a postup testování. Na konci jsou pak informace a výstupy z provedených testů, včetně doporučení zvážení rizik.

3.1 Architektura publikační infrastruktury organizace

Webový agendový systém, který je předmětem této analýzy je součástí širší informační platformy státní organizace, která je zřízena kompetenčním zákonem a která provozuje několik, jemu svěřených agend na základě speciálních zákonů. Celé informační prostředí organizace je značně rozsáhlé, heterogenní a vzájemně provázané. Předmětný systém je nejen sám součástí širší platformy, ale i on sám je integrátorem dalších jiných aplikací a služeb, ať již interních nebo externích. Pro potřeby oddělení jednotlivých informačních oblastí je třeba nejdříve odlišit infrastrukturní a aplikační vrstvu, a popis vybraného systému zasadit do jejich jednotlivých kontextů. Tento popis je nutný pro základní orientaci v implementaci systémů, ačkoli zde nebude řešena otázka funkční, tedy jak je systém provázán a využíván z pohledu obchodních procesů (tzv. bussiness view).

3.1.1 Aplikační vrstva

Zde analyzované systémy jsou většinou součástí portálového řešení vybrané organizace, které se skládá z několika samostatných komponent a představuje jednotný bod interakce s různorodými informacemi a obchodními procesy přizpůsobený individuálním potřebám jednotlivých uživatelů. Celá platforma je tvořena devíti samostatnými portály, přičemž každý z nich je buď celý veřejný nebo neveřejný nebo obsahuje svoji veřejnou a neveřejnou část. Pro potřeby autentizace a autorizace zde pro vybrané systémy existují reverzní proxy s technologií Apache, která centrálně filtruje a moderuje průchozí požadavky na jednotlivé komponenty portálů určené specifickou url. Obsažený autentizační agent analyzuje každý uživatelský požadavek a rozhoduje o nutnosti ověření identity. V případě potřeby je uživatel přesměrován na autentizační platformu, která dále využívá adresářových služeb (LDAP). Zde jsou definovány jednotlivé přístupy k aplikacím, přičemž každá aplikace využívá vlastní adresářovou strukturu, včetně specificky definovaných rolí.

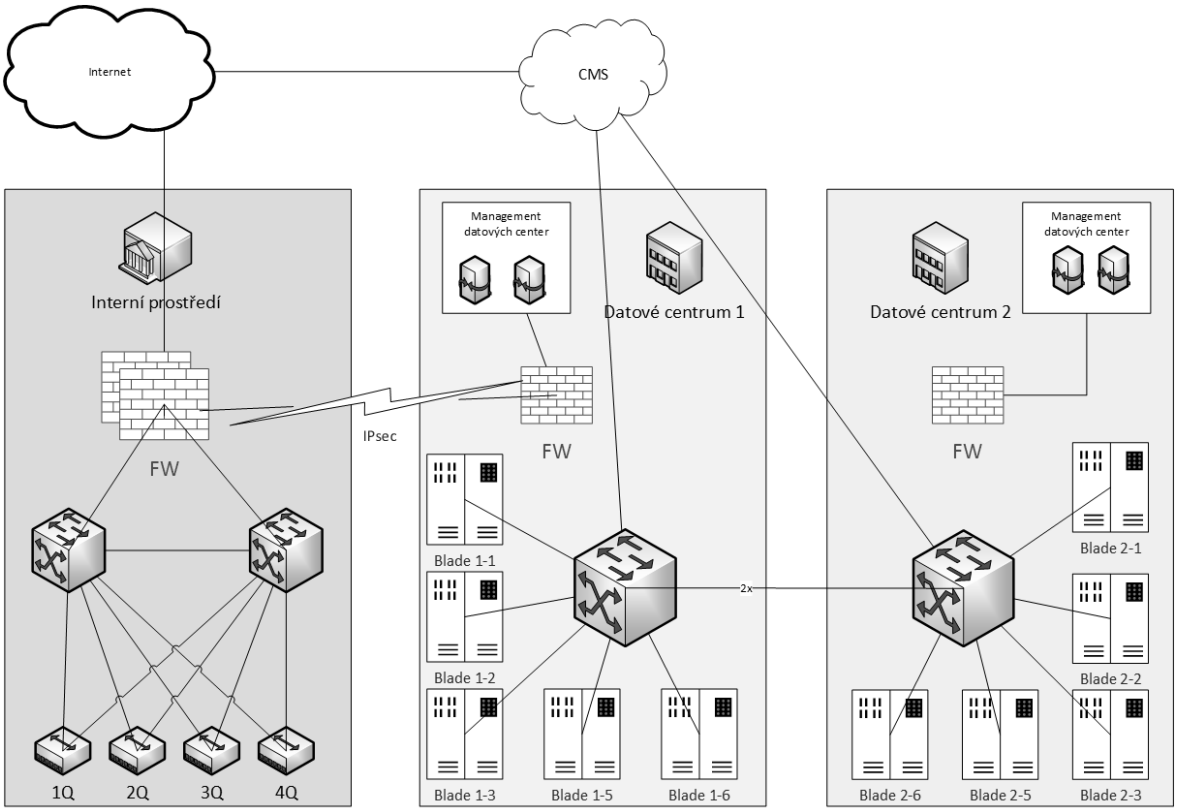
Část služeb, jako jsou speciální registry, a v tomto případě jde o jednu ze zkoumaných komponent – je samostatný dílčí portál, který slouží jako rozcestník, a to právě pro specifické aplikace a registry poskytované jednak odborné veřejnosti a registrovaným uživatelům.
Portál je budován již od roku 1990 a například v roce 2013 zde bylo 21 registrů a aplikací a pět klíčových služeb, poskytující veřejný web, evidenční systémy a aplikaci na podporu dotací[40].
Rozsah poskytovaných služeb se od té doby výrazně nezměnil. Samotný systém představuje pouze web se statickým obsahem a jako takový neposkytuje možnost editace nebo dynamizaci dat. Rozhodná data se vyskytují na rozhraní speciálních registrů, které je vždy definováno jako API s WSDL specifikací pro potřeby integrace s aplikacemi třetích stran nebo s vlastním prezentačním rozhraním. Obě tyto varianty přitom poskytují jak veřejně přístupná, tak neveřejná data. Celá platforma je pak podpořena CMS (Content Management System), tedy samostatnou správou obsahu a má svoji redakční část. Přihlašování uživatelů do prezentační části portálu je zajištěné pomocí výše zmíněného agenta. Redakční část je redaktorům publikována prostřednictvím Interního a Externího portálu. Ten opět zajistí přihlášení uživatele a redakční části předává jeho identitu.
Další variantou jsou samostatně publikované aplikace, které používají vlastní interní autentizační mechanizmus. Zkoumaný agendový systém využívá adresářových služeb obdobně, ale bez nutnosti existence autentizačního agenta na reverzních proxy a externích autentizačních portálových serverech. Požadavky procesuje napřímo, vlastními prostředky a konektivitou.

3.1.2 **Infrastrukturní vrstva**

Dotčená organizace státní správy provozuje informační služby ve vlastní gesci, kde většina technologického vybavení je soustředěna ve dvou datových centrech, uspořádaných jako geografický cluster. Propojení je realizováno zabezpečeně na linkové vrstvě L2 (viz referenční model ISO/OSI) pomocí standardu 802.1AE, známého též jako IEEE MAC Security standard (zkráceně MACsec). Na síťové vrstvě L3 jde o transparentní rozdělení. Připojení publikačních systémů do internetu je realizováno pomocí Centrálního místa služeb

[40] RYSOVÁ, Hana, Karel KUBATA, Jan TYRYCHTR, Miloš ULMAN, Martina ŠMEJKALOVÁ a Václav VOSTROVSKÝ. Evaluation of electronic public services in agriculture in the Czech Republic. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis [online]. 2013, 61(2), 473-479 [cit. 2020-03-30]. DOI: 10.11118/actaun201361020473. ISSN 1211-8516. Dostupné z: https://acta.mendelu.cz/61/2/0473/

(CMS2), provozovaného Ministerstvem vnitra, které mimo jiné slouží pro vzájemné propojení orgánů státní správy, a zajišťuje též služby konektivity a další, například bezpečnostní funkce. Uživatelské připojení z interního prostředí se však realizuje do internetu napřímo, do datových center pomocí IPSEC tunelu viz obrázek 4 níže.



Obrázek 4 - High level informační architektura organizace (autor)

Prezentační část portálu zajišťuje farma 2 aplikačních serverů v odděleném segmentu sítě (DMZ#internet) s předřazeným load balancerem pro zajištění vysoké dostupnosti a SSL terminátorem pro zajištění bezpečného šifrovaného spojení. Tato farma je přístupná z internetu na vlastní url adrese. Zde na aplikačním serveru běží zmíněný webový server Apache, obsahující modul pro zajištění SSO, který následně předává požadavky buď do samotné prezentační části portálu na technologii Oracle Weblogic, nebo do některé z integrovaných aplikací v jiné oddělené části sítě DMZ#aplikace. Load balancer je první organizací kontrolovaný prvek, na který dorazí HTTP, případně HTTPS požadavek uživatele z internetu. V případě, že se jedná o HTTPS komunikaci, zajišťuje balancer její terminaci. Dále jsou na balanceru nastavena základní pravidla přesměrování.

Aplikační servery pro prezentační část portálu jsou umístěné rovněž v DMZ#internet. Na serverech je nainstalován operační systém Red Hat Enterprise Linux a dále Oracle Weblogic

a Apache. MySQL Oracle Weblogic je java aplikační server, do něhož je publikována java aplikace jNetPublish, kdy tato aplikace zajišťuje publikaci samotné webové prezentace portálu. Apache na publikačních serverech obsahuje jednak autentizační modul. Tento modul kontroluje, zda je uživatel přistupující na definované url adresy přihlášen. Pokud ano, vkládá do http hlavičky novou hlavičku s vlastním parametrem, ve které je plně kvalifikované jméno uživatele v LDAP serveru. Pokud daný uživatel není přihlášen, zajišťuje jeho přesměrování na autentizační servery. Dále apache zajišťuje provoz reverzní proxy, která na základě url předává požadavek dále, a to buď do publikační části redakčního systému, nebo do některé z integrovaných aplikací. Nastavení proxy je v souboru /etc/httpd/conf.d/název_konfiguračního_souboru.conf, a zde jsou tedy rovněž uvedena přesměrování na registry provozované pod analyzovaným portálem.

Příklad výpis konfigurace apache pro přesměrování (anonymizováno)

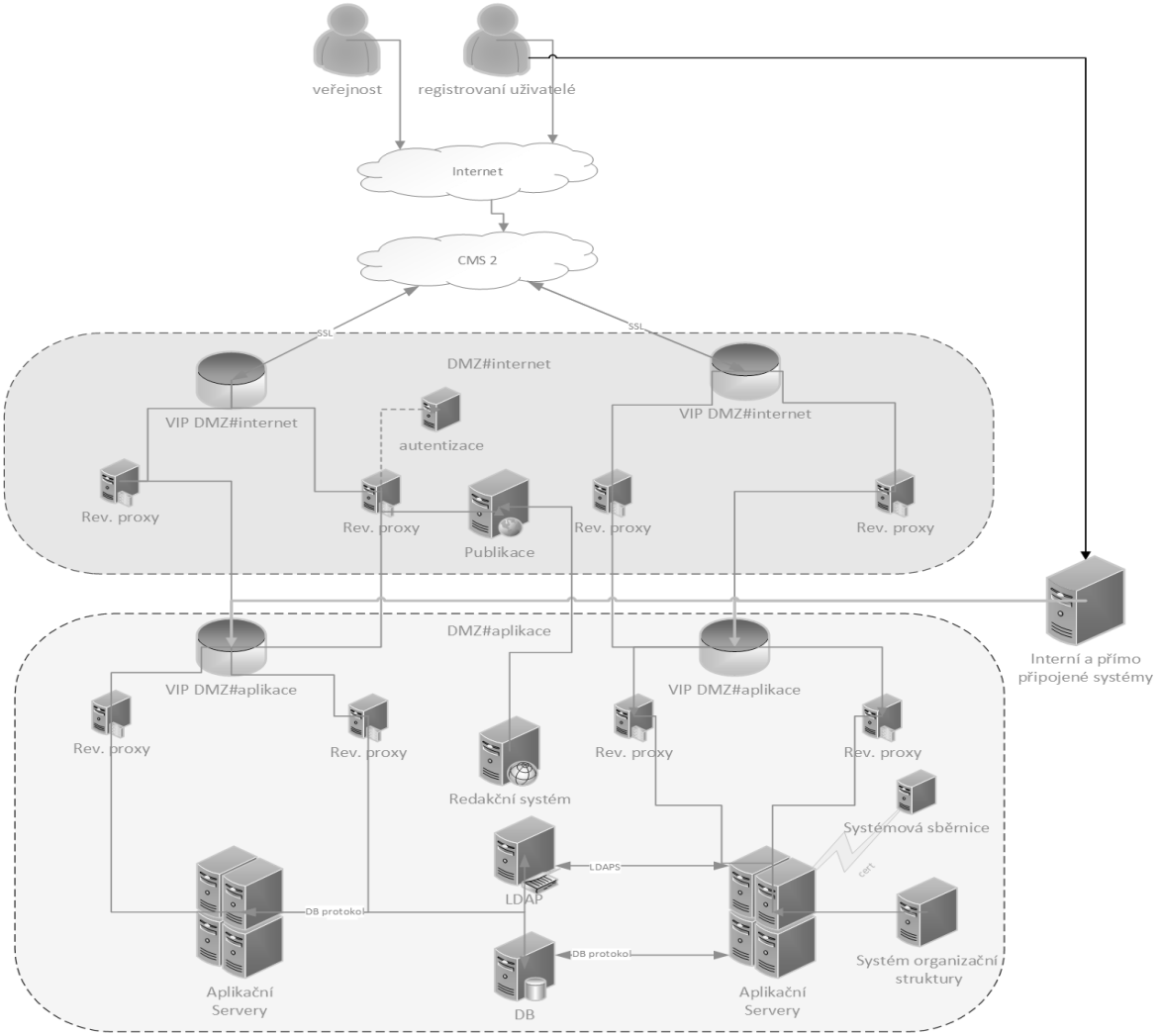
```
#Registr xxxxxxxx - FiPe - 2019/11/11 (CCV)
ProxyPass               /ssl/app/url_app                http://VIP-XX-1234.apl.dom.net:7778/ssl/app/url_app
ProxyPassReverse        /ssl/app/url_app                http://VIP-XX-1234.apl.dom.net:7778/ssl/app/url_app
```

Redakční část portálu je zajištěna virtuálním aplikačním serverem. Vysoká dostupnost redakční části je zajištěna pomocí funkcionality VMware HA. Přístup redaktorů k redakční části je zajištěn prostřednictvím Interního, případně Externího portálu. Jako databáze pro redakční část slouží instance na produkční infrastrukturní databázi. Na redakčním serveru je nainstalován operační systém Red Hat Enterprise Linux a dále Apache a Oracle Weblogic.
Apache na redakčním serveru zajišťuje pouze předávání příchozích http požadavků do Oracle Weblogic. Na rozdíl od prezentační části neobsahuje autentizační modul, neboť příchozí požadavky z Interního / Externího portálu v sobě již obsahují http hlavičku s dn uživatele. V Oracle Weblogic je shodně jako na prezentační části umístěna aplikace jNetPublish, zajišťující správu obsahu celé prezentace portálu. Jako datové úložiště je využita Oracle instance na produkční infrastrukturní databázi.
Portál ke své funkčnosti využívá další informační zdroje. Příkladem je adresářová služba LDAP, sloužící jednak ke zjišťování informací o přihlášeném uživateli, a dále jako zdroj kontaktů prezentovaných na portálu. Přístup k adresářové službě je realizován pomocí zabezpečeného protokolu LDAPS. Pro přístup je využíván dedikovaný servisní účet a pro správu uživatelů redakčního systému portálu je v adresáři vyhrazena samostatná organizační

větev. Informace o uživatelích jsou ze služby replikovány do vlastní databáze portálu. K replikaci dochází při každém novém přístupu uživatele do systému.

Dále komunikuje se samostatným systémem organizační struktury, který slouží k zjišťování informací o odděleních organizace, pro prezentaci organizační struktury a pro zobrazení kontaktních informaci jednotlivých oddělení, popřípadě pro prezentaci výčtové skupiny uživatelů zařazené do určité agendy. Dále se z této databáze využívá registr adresních míst a další číselníky. Pro přístup do Systému organizační struktury je v databázi portálu vytvořen databázový link se specifickým názvem a uživatelem.

Využívání webových služeb prostřednictvím systémové sběrnice je jediný způsob pro předávání dat mezi systémy organizace. Portálové registry se k systémové sběrnici připojují pomocí protokolu HTTPS. Autentizace je řešena pomocí klientského certifikátu. Portál využívá služeb systémové sběrnice přímo jako konzument (tedy volající systém), nebo též jako zprostředkující, tedy zde poskytuje informace a definice pro připojení na systémovou sběrnici veřejnosti nebo registrovaným uživatelům prostřednictvím aplikací konzumující webové služby.



Obrázek 5 - Publikační infrastruktura (autor)

3.2 Agendový systém

Organizace je ústřední orgán státní správy a v rámci svých kompetencí produkuje a zpracovává velké množství geografických dat. Jde o informace, které jsou vázány na geografické mapy a zde, v jednotlivých vrstvách, uchovává specifická data vyplývající z jeho věcné nebo kontrolní činnosti a také zpracovává data svých resortních organizací. Za tímto účelem provozuje několik agendových systémů, které slouží konkrétním potřebám v jednotlivých oblastech správy. Vybraný systém je ve fázi nasazení a poskytuje standardní funkcionality pro zobrazení, analýzu a editaci geografických dat. Jedná se o platformu GIS, jejíž využití se týká „Směrnice evropského parlamentu a rady 2007/2/ES ze dne 14. března 2007 o zřízení Infrastruktury pro prostorové informace v Evropském společenství (INSPIRE)“ a navazuje na Geoinfostrategii ČR a její další strategické dokumenty. Hlavními funkcemi je přidávání nových datových sad pomocí webových služeb nebo ruční editaci,

správa jednotlivých datových sad a zdrojů, jednotně i v samostatných databázích, správa prezentace dat pomocí portálu včetně tematických skupin, skupin obsahu, metadat rolí, přístupů a práv k publikaci. Tvorba map a mapových aplikací na základě widgetů a šablon, mapových kompozic a souvisejícího vzhledu, legend a popisků. Uživatelé pak pracují s jednotlivými aplikacemi, mapy nebo metadaty, a to zabezpečeně po přihlášení a konzumují informace vázané v kompozicích, a to dle příslušenství ve skupinách. Využívají funkcionalit widgetů nebo mapových nástrojů a v případě odpovídající úrovně oprávnění mohou editovat některá data. Dále systém slouží pro prezentaci informací v rámci otevřených dat (Opendata).

3.2.1 **Infrastruktura aplikace**

Pro běh aplikace je vytvořena samostatná VLAN umístěná v odděleném segmentu sítě DMZ#aplikace, s vlastním pojmenováním a číslem, s přiděleným rozsahem IP adres s maskou 255.255.255.0. K dispozici je zde tedy 254 zdrojově přidělitelných adres. V této síti jsou pak umístěny jednotlivé aplikační servery. Jde celkem o pět virtualizovaných serverů s různými rolemi na platformě Vmware s operačním systémem Windows Server 2016 Standard. Ty plní funkce webového adaptéru, portálu, mapového serveru, datastore a databáze. Operační systémy jsou vytvořeny z hardenovaného template (bezpečnostně upravený instalační datový obraz), tedy jsou zde ošetřeny známé konfigurační nekonzistence. Servery jsou připojeny do aktualizačního programu WSUS a jsou zařazeny v patchovací skupině se čtvrtletní periodou kontrol. Zálohování je na úrovni virtualizace a probíhá jednou denně. Co se týče publikace, je aplikace vystavena pomocí virtuální IP adresy (VIP) ve vnější části oddělené sítě DMZ#internet a je na ní i terminován SSL provoz. Dochází zde i k rozkladu zátěže, který je realizován pomocí technologie F5 a jeho funkcionalit. Ta též zajišťuje filtraci pomocí webového aplikačního firewallu (WAF). Autentizace je zajištěna na rozdíl od v předchozích kapitolách uváděného globálního portálového řešení vlastními prostředky a využívá SAML2. Zde se realizují požadavky uživatelů přistupujících z internetu. Druhá VIP je pak vystavena v jiné části oddělené sítě DMZ#aplikace a slouží pro přístup interních uživatelů.

3.2.2 **Aplikační komponenty**

Platforma využívá technologie IIS webového serveru, Microsoft .NET Framework 4.5.2, PostgreSQL 10.8 Windows x86-64 (64 bit) a vlastní komponenty – webový adaptér, mapový

server. Pro autentizaci používá propojení na LDAP. High level schéma je naznačeno v obrázku 5.

3.3 Výběr typu metodologie

V teoretické části, v kapitole týkající se standardů testování, bylo uvedeno několik metodik včetně projektů, které spravuje organizace OWASP fundation. Vzhledem k tomu, že jejich zaměření se týká předně webových aplikací a také se jedná o velmi rozšířený standard, byl zvolen i pro posouzení stanoveného systému. Bylo ale nutné rozhodnout, který projekt OWASP ze všech jeho možných bude vhodné použít pro potřeby této studie.

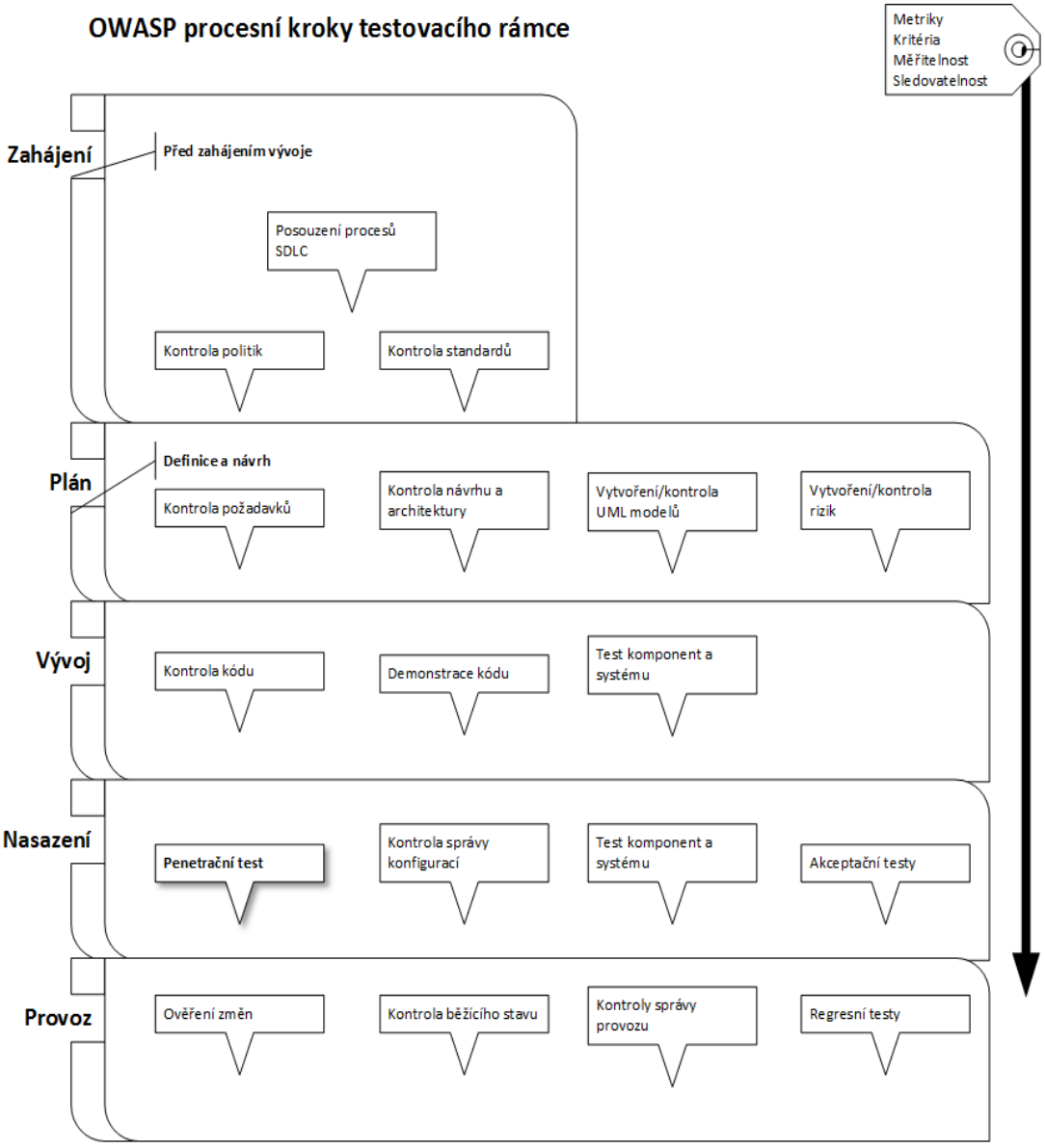
3.3.1 Posouzení projektů OWASP

Jako základ se často používá OWASP Top 10, jde ale o rychlou a jednoduchou variantu testování, která slouží spíše pro řešení akutních problémů a má zjistit, zda zranitelnost systému neodpovídá deseti nejzávažnějším chybám. Rozhodně se ale nejedná o komplexní testovací rámec, který by pokrýval celou problematiku zabezpečení webových aplikací. Průzkumem dokumentace ve vybrané organizaci bylo zjištěno, že existují krátkodobé roční plány bezpečnostních testů, které jsou pravidelně naplňovány. Většina v minulosti prováděných penetračních testů však nemá uvedený použitý standard nebo metodologii, případně se jedná právě o OWASP Top 10. V bezpečnostní politice není zakotvena povinnost realizovat penetrační testy dle existujících metodik.

V rámci OWASP existuje ASVS, který je velmi detailní a má ambice stát se základem pro certifikaci kvality v oblasti zabezpečení v organizacích vyvíjejících a dodávajících webová řešení. Jeho velká část se věnuje aplikovatelnosti, tvorbě a vývoji a znamená zapracování bezpečnostního hlediska do celého životního cyklu aplikace od jejího plánování a vzniku až po její zánik. Toto je zásadní pro stanovení rozsahu s ohledem na vybranou organizaci a systém. Jedná se o ústřední orgán státní správy, který má svoji svěřenou agendu představující její primární činnost, a nemá, tak jak je to také i u většiny ostatních správních úřadů, vlastní vývojové oddělení. Pořízení nových systémů řeší dodavatelsky, a přímo se na něm tedy nepodílí. Vlastní činnost zde může začínat až po implementaci a zavedení do provozu, pokud opomineme definici požadavků a součinnost při vývoji. Tato fáze, až do akceptace a předání, probíhá v odpovědnosti třetí strany. V tuto chvíli přechází systém do

majetku organizace a začíná provozní fáze, která je obvykle zajišťována pomocí smluvního partnera nebo vlastními silami.

S ohledem na rozsah a účel této práce byl rozsah stanoven pouze pro oblast ve vlastní odpovědnosti organizace, a na prostředí externích subjektů a dotčené předprodukční fáze zde nebude brán zřetel. Pro tyto účely se jeví jako vhodný OWASP Testing Guide (OTG) v jeho současné verzi 4.0. Ten má definován testovací rámec obsahující pět fází a obsahuje celý životní cyklus aplikace zde v terminologii OWASP SDLC (Software Development Life Cycle) a je tedy možné zvolit vhodnou oblast, která odpovídá aktuálnímu stavu vybrané aplikace. Ta byla v době přípravy testování ve fázi dodávky a před akceptačními testy. Všechny procesní kroky testovacího rámce jsou naznačeny v obrázku 5.



Obrázek 6 - OWASP Testing framework workflow (autor – zdroj OTG v.4)

3.3.2 Shrnutí výběru konkrétní podoblasti metodologie

Na základě skutečností uvedených v předchozí kapitole byl pro realizaci testů vybrán OWASP Testing Guide v. 4.0, který svou povahou nejlépe odpovídá typu, stavu a fázi projektu týkajícího se vybraného systému.

3.4 Způsob a rozsah testování

Tato kapitola obsahuje informace, jakým způsobem bude postupováno při testech a kde jsou hranice systému, tedy co bude předmětem testování a co nikoliv.

3.4.1 Postup testování

Dle OTG bude testování rozděleno do jednotlivých fází:

1. Sběr informací (Passive mode) – porozumění aplikační logiky, stanovení vektorů testování na základě architektury, pomocí http proxy – Burb comunity edition, získání hlaviček, parametrů a cookies.
2. Testování (Active mode) – provedení komplexní kontroly pomocí nástroje Nexpose a Zap proxy. Seřazení, porovnání a rozčlenění dle jedenácti podkategorií OTG.
3. Reporting – bude vytvořen výstup, členěný dle doporučení na tři kapitoly:
   - Manažerské shrnutí
   - Testovací parametry
   - Nálezy

3.4.2 Škála testovací úrovně

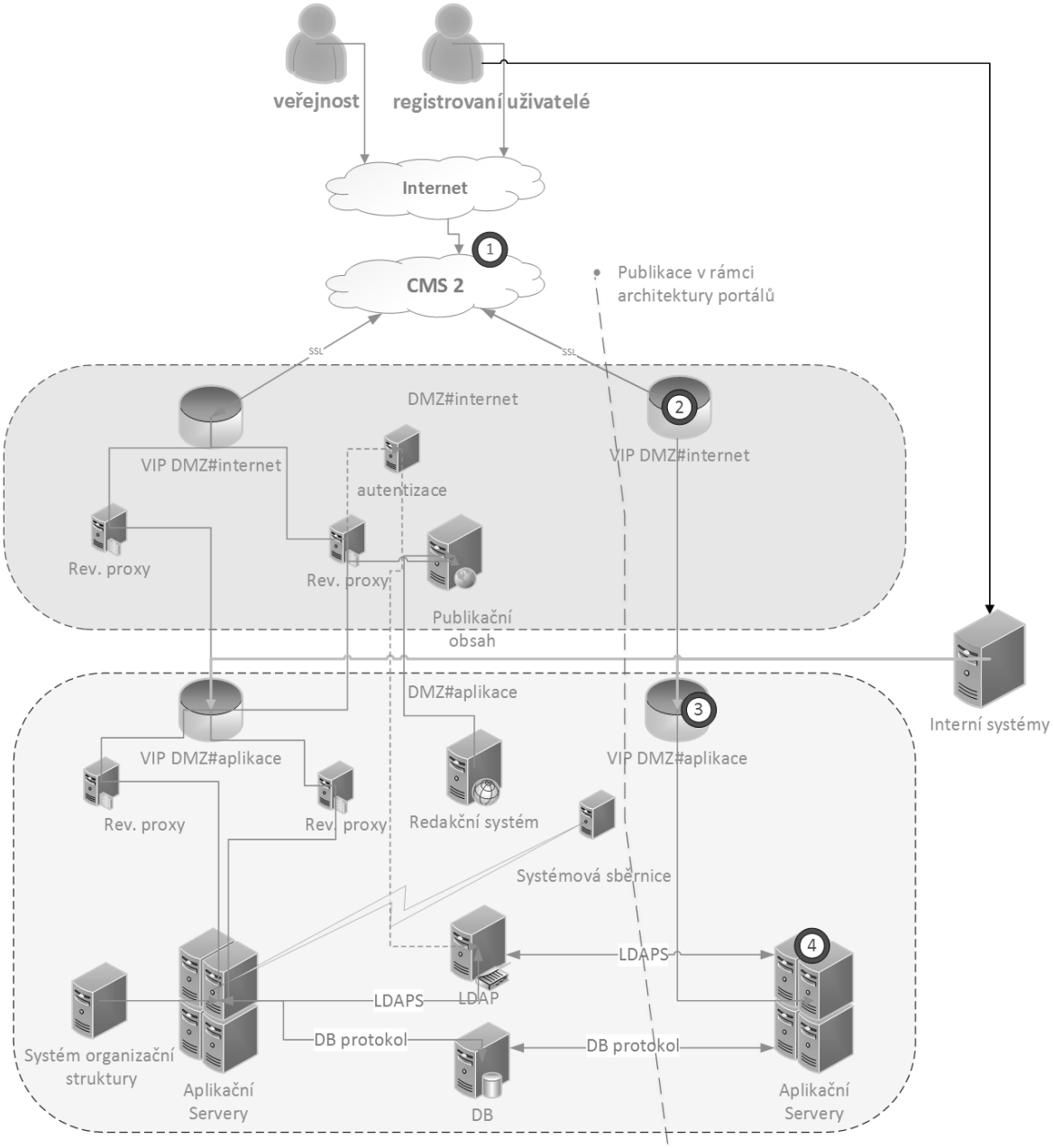
Rozměr testování je upraven pro potřeby této práce tak, aby obsahově odpovídal určenému rozsahu. Zaměřuje se tedy výhradně na vybranou aplikaci a přímo dotčené komponenty. Související infrastruktura je testována nebo zmíněna jen pokud funkčně přímo souvisí s předmětným systémem nebo je jeho součástí. Nebude samostatně testována adresářová služba a databázová vrstva.

3.5 Testy

Kapitola obsahuje popis, jak bylo postupováno při provádění manuálních kontrol a příprava a využití automatických nástrojů během testů.

3.5.1 **Vektory testování**

Vybraná aplikace, jak již bylo uvedeno v kapitole 3.1, je součástí celého portálového řešení organizace, má však samostatný design a vlastní způsob publikace a autentizace. Studiem a faktickým konfiguračním ověřením byly zjištěny konkrétní směry, které představují IP adresy v jednotlivých segmentech a komunikačních pásmech. Jedná se o čtyři vstupní body, tak jak je uvedeno na obrázku x. Vzhledem k tomu, že komunikace mezi bodem 1 a 2 je realizována v prostředí CMS2 a není tedy předmětem zkoumání případná filtrace nebo zde použité bezpečnostní technologie (tato oblast je ve správě Ministerstva vnitra), nebude vstupní bod 2 pro účely tohoto testování použit. Vektory testování jsou body 1, 3 a 4.



Obrázek 7 - Vektory testování (autor)

Vektor 1 představuje přístup z internetu a poskytuje pohled na aplikaci tak, jak ji vidí externí uživatel, například z řad veřejnosti. Je také nejvíce exponován a vzhledem k jeho přístupnosti může být cílem útoků z celosvětové sítě. Vektor 3 je přístupný pouze z vnitřní sítě a představuje omezený okruh systémů nebo uživatelů a pro kompromitaci by bylo nutné překonat omezení na perimetru. Vektor 4 je přístupný stejným způsobem, přístup na něj je filtrován a nejedná se přímo o publikační bod, jedná se o jeden z aplikačních nodů, bez rozkladu zátěže.

3.5.2 **Testovací sady**

Po stanovení jednotlivých vektorů testů je nutné stanovit konfigurace pro jejich provedení, tedy nejen to, co má být testováno, ale i podrobný návod nebo seznam, jakým způsobem bude postupováno. OTG uvádí několik různých nástrojů, které je možné za tímto účelem využít. Jejich výčet není konečný a v doporučení je uváděna vhodnost vlastního výběru a možnost kombinovaného užití. Přednosti tohoto přístupu spočívají ve schopnosti rozdílných technik vzájemně se doplňovat a pokrýt tak celou oblast testování. Zároveň poskytují schopnost vzájemného srovnávání. Pro tyto potřeby byl vybrán nástroj vyvíjený samotnou komunitou OWASP – Zed Attack Proxy (zkráceně ZAP). Jeho předností je integrace testů doporučovaných v OTG. Druhý nástroj je komerční software pro management zranitelností Nexpose od výrobce Rapid 7. Jedná se o alternativu všeobecně známějšího systému Nessus výrobce Tenable. Oba systémy byly nastaveny tak, aby pokryly všech jedenáct oblastí doporučených v OTG.

Tabulka 2 - OTG v. 4 testovací oblasti

OTG testovací oblasti (eng. original)	OTG testovací oblasti (překlad autor)
Information Gathering	Získávání informací
Configuration and Deploy Management Testing	Testování správy konfigurací a nasazení
Identity Management Testing	Testování řízení identit
Authentication Testing	Testování autentizace
Authorization Testing	Testování autorizace
Session Management Testing	Testování správy spojení
Input Validation Testing	Testování vstupní validace
Error Handling	Vypořádání chyb
Cryptography	Kryptografie
Business Logic Testing	Testování operační logiky
Client Side Testing	Testování strany uživatele

Konfigurační sada pro ZAP (politika pro aktivní sken):

Tabulka 3 - Konfigurační sada ZAP

OWASP ZAP PROXY Active scan policy	
SKUPINY/POLOŽKY	**PARAMETRY**
Client Browser	ano
Information Gathering	ano
Directory Browsing	ano
Source Code Disclosure - /WEB-INF folder	ano
Injection	ano
Buffer Overflow	ano
CRLF Injection	ano
Cross Site Scripting (Persistent)	ano
Cross Site Scripting (Persistent) - Prime	ano
Cross Site Scripting (Persistent) - Spider	ano
Cross Site Scripting (Reflected)	ano
Format String Error	ano
Parameter Tampering	ano
Remote OS Command Injection	ano
Server Side Code Injection	ano
Server Side Include	ano
SQL Injection	ano
Miscellaneous	ano
External Redirect	ano
Script Active Scan Rules	ano
Server Security	ano
Path Traversal	ano
Remote File Inclusion	ano

Konfigurační sada pro Nexpose:

Tabulka 4 - Konfigurační sada Nexpose

NEXPOSE – TEMPLATE FULL AUDIT	
SKUPINY/POLOŽKY	**PARAMETRY**
Asset Discovery	
Send ICMP "pings"	ano
Send ARP "pings"	ano
Send TCP packets to ports	21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080
Send UDP packets to ports	53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,5353,49152
Fingerprint TCP/IP stacks	
Service Discovery	ano
TCP Scanning	ano
SYN - porty	1-1040
UDP Scanning	ano
Discovery Performance	ano
Maximum retries	3
timeout interval	0,5-3s
Packets-Per-Second Rate	450-15000
Vulnerability Checks	
261 kategorií zranitelností	533071 jednotlivých zranitelností
Database Servers	
Oracle instances (SIDs) to connect to	ORCL,IASDB,OEMREP,XE,ixos,CTM4_0,CTM4_1,CTM4_6,CTM4_7,ARIS,MSAM,VPX,OPENVIEW,OVO,SA0,SA1,SA2,SA3,SA4,SA5,SA6,SA7,SA8,SA9,SAA,SAB,SAC,SAD,SAE,SAF,SAG,SAH,SAI,SAJ,SAK,SAL,SAM,SAN,SAO,SAP,SAQ,SAR,SAS,SAT,SAU,SAV,SAW,SAX,SAY,SAZ
Web Spidering	Viz Příloha V. Nexpose Web Spidering Parameters.

3.5.3 **Realizace testování**

Po stanovení jednotlivých vektorů byly dotčené IP adresy použity v konfiguracích pro realizaci testů. Testy byly naplánovány a provedeny 22. 2. 2020. V tomto kroku byly použity jak připravené testovací konfigurace pro ZAP Proxy, tak template pro produkt Nexpose. Testy v Nexpose byly nastaveny pomocí plánování úloh ve stanoveném provozním okně od 20:00 – 22:00. Pro potřeby testů byly vytvořeny dvě samostatné skenovací položky (Site), kterým byly přiřazeny jednotlivé IP adresy vybraných assetů ve zvoleném vektoru. Obě Site měly přiřazeny shodný zvolený konfigurační soubor (template) s obsahem položek jednotlivých prováděných testů. Testy v aplikaci ZAP proxy byly provedeny manuálně spuštěním aktivního skenu s vybranou politikou v provozním okně od 18:00 – 20:00. Konfigurace obou nástrojů tak obsáhly většinu kontrol doporučených v OTG, kromě

některých manuálních postupů. Jejich struktura a bodovací škály zranitelnosti jsou odlišné a následně bude nutná jejich normalizace, a tedy převedení na jednotnou škálu hodnocení zranitelností (severity).

4 Výsledky a diskuse

V této kapitole jsou informace k výsledkům testů a v úvodu vlastní interpretace, komentáře a upřesňující popis. Následuje výstup dle požadavku OWASP.

4.1 Výsledky testů

Výsledkem testů je řada nálezů, které mají různou úroveň závažnosti. Ta se vyjadřuje pomocí parametru Severity (z ang. severity – závažnost) a je odvozena ze schopnosti využít zjištěné zranitelnosti a pravděpodobného dopadu při jejím zneužití. Bohužel různé bezpečnostní projekty, systémy, a i výrobci používají rozdílné škály a názvy pro potřeby jejího vyjádření. Vzhledem k této skutečnosti bylo nutné porovnat úrovně Severity u nástrojů Nexpose a ZAP, jejichž výsledky jsou prezentovány. Vzájemný vztah jejich jednotlivých úrovní přehledně shrnuje tabulka 5.

Tabulka 5 - Porovnání závažnosti Nexpose/ZAP

Severity level compare	
Nexpose	**ZAP(OWASP)**
High	Critical
Medium	Severe
Low	Moderate
Informational	Info

Pro potřeby této studie je použita škála dle OWASP.

Další doplňující informací je skutečnost, že ZAP používá pro zpřesnění možnosti porovnání reference na CWE a WASC ve svém reportu (viz Příloha IV.). To znamená, že lze využít těchto katalogizačních systémů pro zjištění podrobností týkajících se konkrétních slabin nebo technik. Tím lze zpřesnit ohodnocení nálezů a dosáhnout výrazně lepších celkových výsledků testů.

Zásadní informací a výsledkem provedeného testu je zde fakt, že nebyla nalezena žádná zranitelnost, jejíž ohodnocení by bylo na úrovni závažnosti Critical. Nepodařilo se tedy ověřit, že by systém trpěl nějakou slabinou, jejíž přímé zneužití by mohlo mít vážné důsledky pro organizaci nebo uživatele, kteří jej využívají. Dá se ale konstatovat, že využití zvolené metodologie výrazně pomohlo definovat a uskutečnit tento test, především proto, že obsahuje pevnou strukturu pro jejich provádění a má definovaný výstup. Lze jej tedy pro využití doporučit. Shrnutí a další detailní informace budou prezentovány v dalších kapitolách, a to dle doporučení OTG.

4.2 **Report dle OTG**

Tato kapitola má doporučenou strukturu a obsahuje jednotlivé položky, tak jak to vyžaduje zvolená metodika.

4.2.1 **Manažerské shrnutí**

Výstupy projektu Bezpečnostní test systému Speciální registry[41]

(příklad patičky dokumentu s uvedením důvěrnosti informací)

Název dokumentu:	Zpráva z bezpečnostního testu Speciální registry	Verze:	1.0
Projekt:	365/22022020	Stádium:	Návrh
Autor/Autoři:	Bc. Roman Smetana	Důvěrnost:	DŮVĚRNÉ

Jméno souboru:	365_zprava_test_SR_v_1.0.docx	Počet stran:	69
Datum aktualizace:	22. 2. 2020	Strana:	76

Koncem měsíce února 2020 byly provedeny bezpečnostní testy aplikace Speciální registry. Kapitola dokumentuje nálezy, které byly výsledkem testů. Ty byly prováděny automatizovaně a částečně faktickým ověřením, profesionálními nástroji k tomu určenými s náležitou péčí a s předem definovanými parametry testů.

Celkem bylo prověřeno z pohledu aplikace tisíce zjištěných URL v kombinaci s mnoha parametry, ať již nativními, z titulu protokolů, nebo individuálními cookies a url parametry testované aplikace.

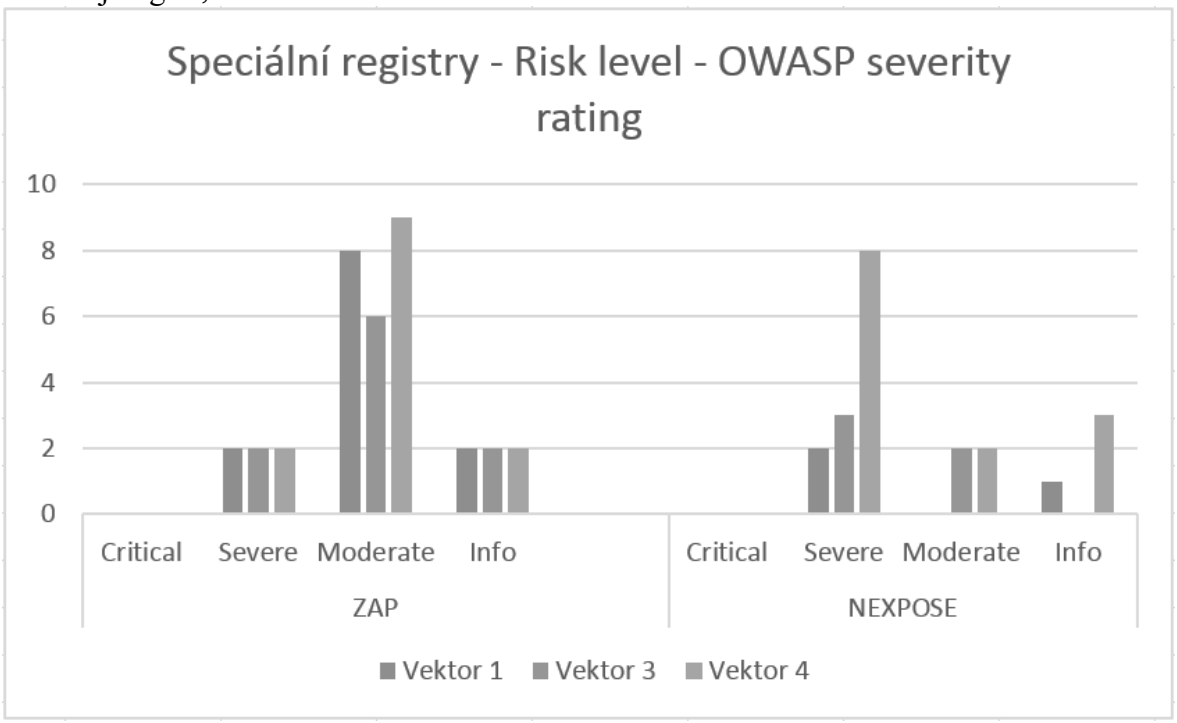
Vybrané vstupní body byly podrobně testovány jak legitimními hodnotami, tak účelově pozměněnými hodnotami pro zjištění limitů a chybového chování. Výsledkem jsou stovky tisíc aplikačních operací provedených a vyhodnocených. Nejzajímavější výsledky jsou uvedeny souhrnně níže a dále v následujících kapitolách. Dokumentace je zachycuje formou negativního výčtu. Jsou zde tedy uvedeny pouze ty, které mají informační hodnotu a mohou být použity pro zvážení a vyhodnocení rizik. Odstraněny byly duplicity, které by vedly ke stejnému zjištění a nerozšiřují informační význam sdělení.

Nálezy:

1. **Systém neobsahuje žádnou kritickou zranitelnost.**
2. **Systém obsahuje několik středně závažných zranitelností**
3. **Systém obsahuje několik zjištění s nízkou mírou zranitelnosti**

[41] Speciální registry – anonymizovaný název agendového systému

Počty nálezů rozdělených dle testovací technologie, závažnosti a vektoru testování, shrnuje následující graf, viz obrázek 8.



Obrázek 8 - Přehled zranitelností dle testovacích technologií a závažnosti (autor)

Shrnutí:

Nejzávažnějšími nálezy jsou Click Jacking, podpora TLS v1.0 a náchylnost na BEAST attack a nesprávné hodnoty Entity name v X.509 certifikátu a chybné nastavení pro X-Frame (rámce).

Doporučení:

- **U nálezů ze závažností typu „Severe“, a Moderate“ zvážit jejich odstranění.**
- **U ostatních nálezů akceptovat riziko zneužití, které je v tomto případě velmi nízké a s malými dopady. Nálezy včetně výsledku rozhodnutí zanést do technické dokumentace k systému.**

4.2.2 Testovací parametry

Cíl projektu – testování systému Speciální registry ověří, zda aktuálně publikovaná verze je dostatečně odolná na zneužití zranitelností, případně jaké slabiny se zde nacházejí. Dojde ke zvážení dopadů a bude určena jejich kritičnost jako podklad pro další rozhodování v oblasti rizik.

Rozsah projektu – testování se týká informačních bezpečnostních aspektů pouze vybrané aplikace a přímo související infrastruktury a bude provedeno ze zvolených vektorů. Zaměřuje se především na aplikační vrstvu modelu OSI a konfigurační nastavení a protokolovou komunikaci. Související infrastrukturou jsou myšleny prvky, komponenty a všechny další služby potřebné pro provoz systému.

Plán projektu – shrnuje jednotlivé kroky realizované v časové postoupnosti.

1. Příprava testování – 10-21 února 2020
2. Realizace testů – 22 února 2020
3. Vyhodnocení – 24-28 února 2020

Vektory a parametry – vektory testování byly zvolené přístupové body 1, 3 a 4 uvedené v kapitole 3.5.1. Pro testování byly použité testovací oblasti dle OTG viz tabulka 2 a vybrané konfigurační sady pro ZAP (politika pro aktivní sken) a skenovací template pro Nexpose viz tabulky 3 a 4.

Omezení – testy neberou v potaz bezpečnostní prvky umístěné v CMS2, tedy mimo působnost organizace. Testování bylo provedeno bez aktivní politiky WAF, tedy bez filtrace aplikační vrstvy na vstupním bodě. (WAF je možné použít pro eliminaci případných slabin nebo jako „virtual patching“ – virtuální aktualizace provedená na úrovni aplikačního firewallu).

Shrnutí zjištění – celkem bylo objeveno třicet nálezů ve třech kategoriích závažnosti.

Shrnutí doporučení – u nálezů se závažností typu „Severe“, a Moderate“ zvážit jejich odstranění, u ostatních nálezů akceptovat rizika. Jednotlivé doporučující opatření jsou uvedeny v následující sekci Nálezy.

4.2.3 **Nálezy**

Závažnost: Severe

OWASP ID: OTG-CRYPST-001

Node/URL: IPadresa xxx.xxx.xxx.xxx:443 (vektor1)

Nález: X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch). Položka certifikátu typu X.509 CN – název subjektu nesouhlasí se jménem hostitele (nesoulad běžného názvu certifikátu). Pole názvu subjektu (CN) v certifikátu X.509 neodpovídá názvu hostitele, předkládajícího certifikát. Před vydáním

certifikátu musí Certifikační autorita (CA) zkontrolovat totožnost subjektu žádajícího o certifikát, jak je vyžadováno certifikační praxí CA (CPS). Standardní postup ověřování certifikátů vyžaduje pole CN a jeho obsah musí odpovídat skutečnému jménu subjektu, který certifikát předkládá. Například v certifikátu předloženém „https://www.example.com/“, by CN mělo být „www.example.com“. Aby bylo možné detekovat útoky typu aktivní odposlech a zabránit jim, musí být ověřena platnost certifikátu, jinak by útočník mohl použít techniku man-in-the-middle a získat plnou kontrolu nad datovým tokem. Zde je právě důležitá platnost CN subjektu, který by měl odpovídat názvu entity (název hostitele). K neshodě s CN může docházet v důsledku chyby konfigurace, ale také z důvodu probíhajícího útoku. Mohlo by se též jednat o falešně pozitivní zprávu v případě serverů používajících SNI (Server Name Indication).

Doporučené řešení: Položka certifikátu typu X.509 CN – název subjektu by měl být opraven tak, aby správně reprezentoval název hostitele. Vygenerujte nový certifikát, který bude splňovat tuto podmínku, a to certifikační autoritou, které důvěřují obě strany, tedy klient i server.

Detaily: Název subjektu nalezený v certifikátu X.509 neodpovídá skenovanému cíli: Předmět CN „*.nalezenádoména.cz“ neodpovídá názvu webu. Subjekt CN „*.nalezenádoména.cz“ nelze přeložit na IP adresu pomocí DNS lookup. Také Subject Alternative Name „*.nalezenádoména.cz“ neodpovídá cílovému jménu zadaného webu. Alternativní název podskupiny „nalezenádoména.cz“ také neodpovídá názvu uvedenému na webu.

Závažnost: Severe
OWASP ID: OTG-CLIENT-009
Node/URL:
https://xxx.xxx.xxx.xxx/portal/home/webscene/viewer.html
https://xxx.xxx.xxx.xxx/portal/home/webmap/viewer.html

Nález: Click Jacking (http-generic-click-jacking)
Clickjacking je útok, známý také jako UI redressing (převlečení uživatelského rozhraní). Je to metoda, při které útočník používá k průniku více průhledných nebo neprůhledných vrstev.

Při kliknutí ve viditelném prostředí dojde fakticky ke kliknutí na tlačítko nebo odkaz v jiné stránce než v té, která je prezentována uživateli. Útočník tedy „ukradne“ klik a směruje uživatele na stránku nelegitimní.

Doporučené řešení: Nastavte konfiguraci tak, aby hlavička odpovědi obsahovala položku X-Frame-Options s instrukcí pro prohlížeč, který tak omezí použití rámců, tam kde není povolen.

Detaily:

Running HTTPS serviceHTTP request to
https://xxx.xxx.xxx.xxx/portal/home/webscene/viewer.html
HTTP response code was an expected 200
1: text/html
HTTP header 'Content-Type' was present and matched expectation
HTTP header 'Content-Security-Policy' not present
HTTP header 'X-Frame-Options' was present and matched expectation

Running HTTPS serviceHTTP request to
https://xxx.xxx.xxx.xxx/portal/home/webmap/viewer.html
HTTP response code was an expected 200
1: text/html
HTTP header 'Content-Type' was present and matched expectation
HTTP header 'Content-Security-Policy' not present
HTTP header 'X-Frame-Options' was present and matched expectation
…
(Dle koncepce OTG by dále v reportu následovalo uvedení všech nálezů z testů v naznačené struktuře. Z důvodu omezení rozsahu této práce jsou ostatní nálezy uvedeny v přehledných tabulkách v přílohách na konci.)

Závěr

Hlavní cíl této práce byl zaměřen na zabezpečení informačních systémů a zaobíral se skutečností, že připravovaná funkční řešení ve státních institucích, odvíjející se od legislativních předpisů a související s jejich věcnou působností, mají mnohdy přednost před řešením bezpečnostních aspektů. Často totiž nebývají plně součástí realizačních projektů nebo jsou řešeny jen v dílčích fázích životního cyklu, a to především z důvodu, že vývoj obvykle probíhá na straně dodavatele. Pro naplnění tohoto cíle bylo nutné posoudit úroveň informační bezpečnosti ve zvoleném orgánu státní správy a zjistit, zda se zde vyskytují problémové oblasti. Bylo nutné nejdříve sestavit literární rešerši na téma kybernetické bezpečnosti ve státní správě, včetně související problematiky dotýkající se jejích základních principů, a to i v historických a vývojových souvislostech. V této části byly řešeny otázky nejen v obecné rovině, ale i týkající se přímo užití a konstrukce informačních systémů. Od informační asymetrie k principu neoprávněného vzdáleného přístupu k zařízením a datům. Dále bylo nutné uchopit systém zákonů, orgánů a strategií, upravující tuto oblast a okrajově byly zkoumány i legislativní podmínky pro zabezpečení informačních systémů ve státní správě. Pro jejich kontrolu bylo nutné zaměřit se na způsoby, možnosti, standardy auditování a kontroly informační bezpečnosti, především z pohledu přístupů sdružených pod organizací OWASP fundation, se zaměřením na zvolení vhodného projektu, použitelného pro tyto účely ve státní organizaci.

V analytické části v kapitole 3.1 a 3.2 bylo zkoumáno informační prostředí organizace, její infrastruktura a také architektura aplikace. Tato znalost je zásadním předpokladem pro správné určení způsobu testování. Následně bylo nutné rozhodnout, kterou část zvolené metodologie a jak použít. V kapitole 3.3 Výběr typu metodologie byly posouzeny typy projektů OWASP a byl vybrán vhodný typ odpovídající povaze organizace a jejímu způsobu vývoje, respektive pořizování aplikací, a to OTG v.4. S ohledem na aktuální fázi životního cyklu aplikace byl zvolen penetrační typ testu. V kapitole 3.4 a 3.5 je podrobně popsáno, jakým způsobem byl zvolen druh testování, jak byly vybrány nástroje a parametry pro jeho provedení a určeny vektory testování. Došlo též k vybrání časového okna a jeho schválení managementem IT organizace. Doba a čas realizace byly dodrženy, z faktického testování byl zajištěn výstup. Získané informace byly roztříděny, vzájemně porovnány a vyhodnoceny. Ty prezentuje kapitola 4. a to prostřednictvím vytvořené závěrečné zprávy, obsahující manažerské shrnutí, testovací parametry a detaily, včetně ohodnocení závažnosti

a doporučení ke zvážení rizik a případnému odstranění slabin, tak jak to vyžaduje OTG. Zásadní informace se nacházejí v manažerském shrnutí, v kapitole 4.2.1. Tabulky a další detaily jsou uvedeny v přílohách práce. Zásadním zjištěním bylo, že vybraný systém neobsahuje kritické zranitelnosti a nevyžaduje bezodkladný zásah. Vedlejším zjištěním je fakt, že vybraná organizace sice provádí pravidelné bezpečnostní testy, ale nepoužívá standardizované postupy ani metodologie, nebo jen jejich základní zjednodušené varianty viz kapitola 3.3.1. Zde zvolený OTG je možné doporučit k použití a bylo by vhodné zvážit jeho pevné zavedení jako podmínky v systému řízení například zakotvením v bezpečnostní politice týkající se testování.

Je tedy možné konstatovat, že:

- Bylo zkoumáno informační prostředí a agendový systém v orgánu státní správy z pohledu kybernetické bezpečnosti
- Byly provedeny informační bezpečnostní testy s pozitivním výsledkem dle doporučení OTG (OWASP testing guide), včetně závěrečné zprávy
- Byly zjištěny nekritické slabiny a je možné přijmout nápravná opatření
- Byla vydána doporučení jako podklad pro rozhodování rizikových manažerů
- Byla ověřena možnost použití zvolené metodologie v orgánu státní správy

Přínosy lze spatřovat ve zlepšení realizace a řízení bezpečnostního testování, zvýšení informační bezpečnosti konkrétního systému i úřadu a tím zkvalitnění poskytování služeb. Při zajišťování bezpečnostního testování, ať již vlastními prostředky úřadu nebo prostřednictvím specializovaných odborných firem, je možné použít úspěšně OTG. Obsahuje komplexní sadu oblastí testování, vhodných pro provedení testů i jako podklad pro zadání výběrových řízení na jejich realizaci. Také může tento ověřený vlastní postup sloužit jako příklad k otestování a zvýšení úrovně bezpečnosti ve vlastní gesci. Kromě orgánů státní správy a ostatních úřadů je možné stejným způsobem postupovat i v případě jakékoli organizace. Uvedené zkušenosti lze aplikovat pro zadávání veřejných zakázek, i realizaci penetračních testů vlastními prostředky, a to jak ve státní sféře, tak na úrovni regionálních a místních samospráv. V této práci zpracovávané původní, neanonymizované výstupy, byly poskytnuty danému úřadu k vlastnímu využití. Předpokládá se, že návrhy a doporučení uvedené v manažerském shrnutí, pomohou odpovědným osobám dotčené organizace k rozhodnutí, které povede ke zvýšení úrovně zabezpečení u testovaného systému. Tím bude

v druhé řadě podpořena spolehlivost jím poskytovaných služeb, celého úřadu, a i obecně hodnověrnost státní správy ČR.

Seznam použitých zdrojů

ALTER, Steven. Defining information systems as work systems: implications for the IS field. European Journal of Information Systems [online]. 2017, 17(5), 448-469 [cit. 2020-03-24]. DOI: 10.1057/ejis.2008.37. ISSN 0960-085X. Dostupné z: https://www.tandfonline.com/doi/full/10.1057/ejis.2008.37

BARCELÓ, Marta a kol. OSSTMM 3 – The Open Source Security Testing Methodology Manual [online]. ISECOM, 2010 [cit. 2020-03-07]. Dostupné z: https://www.isecom.org/OSSTMM.3.pdf

BUCHALCEVOVA, Alena a Jan POUR. Business Informatics Management Model. Advances in Computer Science and Ubiquitous Computing [online]. Singapore: Springer Singapore, 2015, 2015-12-18, , 65-71 [cit. 2020-03-29]. Lecture Notes in Electrical Engineering. DOI: 10.1007/978-981-10-0281-6_10. ISBN 978-981-10-0280-9. Dostupné z: http://link.springer.com/10.1007/978-981-10-0281-6_10

BUCHALCEVOVA, Alena. Application of Methodology Evaluation System on Current IS Development Methodologies. International Journal of Information Technologies and Systems Approach [online]. 2018, 11(2), 71-87 [cit. 2020-03-29]. DOI: 10.4018/IJITSA.2018070105. ISSN 1935-570X. Dostupné z: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJITSA.2018070105

CAPEC: About CAPEC [online]. MITRE, April 04, 2019 [cit. 2020-03-08]. Dostupné z: https://capec.mitre.org/about/index.html

Common Weakness Enumeration: A Community-Developed List of Software & Hardware Weakness Types [online]. MITRE, February 10, 2020 [cit. 2020-03-08]. Dostupné z: https://cwe.mitre.org/about/index.html

ČESKO. § 25 odst. 1 písm. a) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 13. 3. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#p25-1-a

ČESKO. § 5b odst. 1 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 8. 2. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365#p5b-1

ČESKO. § 5a odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 2. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365#p5a-2

DOLEZEL, Michal, Alena BUCHALCEVOVA a Michal MENCIK. The State of Agile Software Development in the Czech Republic: Preliminary Findings Indicate the Dominance of "Abridged" Scrum. Research and Practical Issues of Enterprise Information Systems [online]. Cham: Springer International Publishing, 2019, 2019-12-13, , 43-54 [cit. 2020-03-29]. Lecture Notes in Business Information Processing. DOI: 10.1007/978-3-030-37632-1_4. ISBN 978-3-030-37631-4. Dostupné z: http://link.springer.com/10.1007/978-3-030-37632-1_4

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Pub., 2011. ISBN 9788074310508 s. 60

First - improving security together: Common Vulnerability Scoring System Version 3.1 Calculator [online]. 2019 [cit. 2020-03-08]. Dostupné z: https://www.first.org/cvss/calculator/3.1

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-2475457-4, s. 131-135

HARDY, Alexandre a Martin S OLIVIER. A Configurable Security Architecture Prototype. Data and Application Security [online]. Boston, MA: Springer US, 2001, 2002, , 51-62 [cit. 2020-03-30]. IFIP International Federation for Information Processing. DOI: 10.1007/0-306-47008-X_5. ISBN 978-0-7923-7514-2. Dostupné z: http://link.springer.com/10.1007/0-306-47008-X_5

IFTACH, Ian Amit. PTES: The Penetration Testing Execution Standard [online]. 2014 [cit. 2020-03-07]. Dostupné z: http://www.pentest-standard.org/index.php/Main_Page

ISSAF: Files [online]. 2005 [cit. 2020-03-08]. Dostupné z: https://sourceforge.net/projects/isstf/

KUBĚNKA, Pavel. Vzorové informační koncepce: Vzorová informační koncepce ústředního orgánu veřejné správy [online]. 2.8.2006, 46 [cit. 2020-04-02]. Dostupné z: https://www.mvcr.cz/soubor/informacni-koncepce-ustredniho-organu-verejne-spravy.aspx

LEPOFSKY, Ron. Web Application Vulnerabilities and the Damage They Can Cause. The Manager's Guide to Web Application Security [online]. Berkeley, CA: Apress, 2014, 2014-12-20, , 21-46 [cit. 2020-03-30]. DOI: 10.1007/978-1-4842-0148-0_3. ISBN 978-1-4842-0149-7. Dostupné z: http://link.springer.com/10.1007/978-1-4842-0148-0_3

MASNER, Jan, Pavel ŠIMEK, Eva KÁNSKÁ a Jiří VANĚK. Creation, Storage and Presentation of Information Content – Semantics, Sharing, Presentation, and Archiving. Agris on-line Papers in Economics and Informatics [online]. 2019, 11(01), 75-82 [cit. 2020-03-30]. DOI: 10.7160/aol.2019.110108. ISSN 18041930. Dostupné z: http://online.agris.cz/archive/2019/1/8

MOHASSEB, Alaa, Benjamin AZIZ, Jeyong JUNG a Julak LEE. Cyber security incidents analysis and classification in a case study of Korean enterprises. Knowledge and Information Systems [online]. [cit. 2020-03-30]. DOI: 10.1007/s10115-020-01452-5. ISSN 0219-1377. Dostupné z: http://link.springer.com/10.1007/s10115-020-01452-5

Národní strategie kybernetické bezpečnosti ČR 2015-2020. In: . Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2014, ročník 2015. Dostupné také z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

O úřadu. Národní úřad pro kybernetickou a informační bezpečnost [online]. Brno: NÚKIB Brno – Mučednická, 2017 [cit. 2020-01-24]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu

Působnost Úřadu. Úřad pro ochranu osobních údajů [online]. Praha: Úřad pro ochranu osobních údajů, 2013, 2019 [cit. 2020-01-24]. Dostupné z: https://www.uoou.cz/pusobnost%2Duradu/ds-1269/archiv=0&p1=1059

Rada vlády pro informační společnost. Ministerstvo vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky, 2019, 2020 [cit. 2020-01-24]. Dostupné z: https://www.mvcr.cz/clanek/rada-vlady-pro-informacni-spolecnost.aspx

RAO, Umesh Hodeghatta a Umesha NAYAK. The InfoSec handbook: an introduction to information security [online]. New York, New York: Apress, [2014] [cit. 2019-06-02]. Expert's voice in information security. ISBN 14-302-6382-2. Dostupné z: DOI: 10.1007/978-1-4302-6383-8

RYSOVÁ, Hana, Karel KUBATA, Jan TYRYCHTR, Miloš ULMAN, Martina ŠMEJKALOVÁ a Václav VOSTROVSKÝ. Evaluation of electronic public services in agriculture in the Czech Republic. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis [online]. 2013, 61(2), 473-479 [cit. 2020-03-30]. DOI: 10.11118/actaun201361020473. ISSN 1211-8516. Dostupné z: https://acta.mendelu.cz/61/2/0473/

SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada). ISBN 978-802-4730-516, s. 90-91

SYED, Mohamed A a spol. WASC Threat Classification: version 2.00 [online]. Verze 2. WEB APPLICATION SECURITY CONSORTIUM, 2010 [cit. 2020-03-08]. Dostupné z: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

ŠVARCOVÁ, Ivana a Tomáš RAIN. Informační management. Praha: Alfa Nakladatelství, 2011. Informatika (Alfa Nakladatelství). ISBN 978-80-87197-40-0, s 60

Top 10 Penetration Testing Certifications for Security Professionals. INFOSEC [online]. Herndon: Infosec Resources 2020, 2019 [cit. 2020-03-07]. Dostupné z: https://resources.infosecinstitute.com/top-5-penetration-testing-certifications-security-professionals/

TYRYCHTR, J., M. ULMAN a V. VOSTROVSKÝ. Evaluation of the state of the Business Intelligence among small Czech farms. Agricultural Economics (Zemědělská ekonomika) [online]. 2016, 61(2), 63-71 [cit. 2020-03-30]. DOI: 10.17221/108/2014-AGRICECON. ISSN 0139570X.

Veřejná správa: Strategický rámec rozvoje. Ministerstvo vnitra České republiky: o nás [online]. Praha: Ministerstvo vnitra České republiky, 2014 [cit. 2020-03-24]. Dostupné z: https://www.mvcr.cz/soubor/strategicky-ramec-rozvoje-verejne-spravy-v-cr-pro-obdobi-2014-2020.aspx, tabulka str. 84

VOSTROVSKY, V. a J. TYRYCHTR. Consistency of Open Data as Prerequisite for Usability in Agriculture. Scientia Agriculturae Bohemica [online]. 2018, 49(4), 333-339 [cit. 2020-03-30]. DOI: 10.2478/sab-2018-0040. ISSN 1805-9430. Dostupné z: https://content.sciendo.com/view/journals/sab/49/4/article-p333.xml

Přílohy

Příloha I. - Výsledky testů dle vektorů Nexpose (autor)
Příloha II. - Výsledky testů dle vektorů ZAP (autor)
Příloha III. - Zjištěné nálezy dle OTG charakteristik (autor)
Příloha IV. - ZAP report katalogizační reference (autor – zdroj report ZAP)
Příloha V. - Web spidering (autor zdroj Nexpose konfigurační template)

Příloha I. - Výsledky testů dle vektorů Nexpose (autor)

NÁSTROJ	VEKTOR/ZRANITELNOST	ZÁVAŽNOST
NEXPOSE	**Vektor 1**	
	X.509 Certificate Subject CN Does Not Match the Entity Name	Severe
	Click Jacking	Severe
	TCP timestamp response	Info
	Vektor 3	
	Click Jacking	Severe
	TLS Server Supports TLS version 1.0	Severe
	TLS/SSL Server is enabling the BEAST attack	Severe
	Diffie-Hellman group smaller than 2048 bits	Moderate
	TCP timestamp response	Moderate
	Vektor 4	
	X.509 Certificate Subject CN Does Not Match the Entity Name	Severe
	Untrusted TLS/SSL server X.509 certificate	Severe
	SMBv2 signing not required	Severe
	TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Severe
	Self-signed TLS/SSL certificate	Severe
	TLS Server Supports TLS version 1.0	Severe
	TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)	Severe
	TLS/SSL Server is enabling the BEAST attack	Severe
	TLS/SSL Server Supports The Use of Static Key Ciphers	Moderate
	TLS Server Supports TLS version 1.1	Moderate
	TLS/SSL Server Supports 3DES Cipher Suite	Info
	ICMP timestamp response	Info
	TCP timestamp response	Info

Příloha II. - Výsledky testů dle vektorů ZAP (autor)

NÁSTROJ	VEKTOR/ZRANITELNOST	ZÁVAŽNOST
ZED ATTACK PROXY	**Vektor 1**	
	X-Frame-Options Setting Malformed	Medium
	X-Frame-Options Header Not Set	Medium
	Cookie No HttpOnly Flag	Low
	Incomplete or No Cache-control and Pragma HTTP Header Set	Low
	Cookie Without Secure Flag	Low
	Cookie Without SameSite Attribute	Low
	Web Browser XSS Protection Not Enabled	Low
	X-Content-Type-Options Header Missing	Low
	Information Disclosure - Suspicious Comments	Info
	Timestamp Disclosure - Unix	Info
	Vektor 3	
	Application Error Disclosure	Medium
	X-Frame-Options Setting Malformed	Medium
	X-AspNet-Version Response Header Scanner	Low
	Incomplete or No Cache-control and Pragma HTTP Header Set	Low
	Server Leaks Information via "X-Powered-By" HTTP Response Header	Low
	Private IP Disclosure	Low
	Application Error Disclosure	Low
	Information Disclosure - Debug Error Messages	Low
	Timestamp Disclosure - Unix	Info
	Information Disclosure - Suspicious Comments	Info
	Vektor 4	
	Application Error Disclosure	Medium
	X-Frame-Options Setting Malformed	Medium
	X-AspNet-Version Response Header Scanner	Low
	Server Leaks Information via "X-Powered-By" HTTP Response Header	Low
	Incomplete or No Cache-control and Pragma HTTP Header Set	Low
	Private IP Disclosure	Low
	Application Error Disclosure	Low
	Information Disclosure - Debug Error Messages	Low
	Timestamp Disclosure - Unix	Info
	Information Disclosure - Suspicious Comments	Info

Příloha III. - Zjištěné nálezy dle OTG charakteristik (autor)

ZJIŠTĚNÉ NÁLEZY	OWASP Charakteristiky		
zranitelnosti	**GROUP (skupina)**	**ID (identifikační číslo)**	**ID DESC (popis ID)**
Application Error Disclosure	Information Gathering	OTG-INFO-008	Fingerprint Web Application Framework
Click Jacking	Client Side Testing	OTG-CLIENT-009	Testing for Clickjacking
Cookie No HttpOnly Flag	Session Management Testing	OTG-SESS-002	Testing for Cookies attributes
Cookie Without SameSite Attribute	Session Management Testing	OTG-SESS-002	Testing for Cookies attributes
Cookie Without Secure Flag	Session Management Testing	OTG-SESS-002	Testing for Cookies attributes
Diffie-Hellman group smaller than 2048 bits	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
ICMP timestamp response	Information Gathering	OTG-INFO-010	Map Application Architecture
Incomplete or No Cache-control and Pragma HTTP Header Set	Session Management Testing	OTG-SESS-004	Testing for Exposed Session Variables
Information Disclosure - Debug Error Messages	Configuration and Deploy Management Testing	OTG-CONFIG-002	Test Application Platform Configuration
Information Disclosure - Suspicious Comments	Configuration and Deploy Management Testing	OTG-CONFIG-002	Test Application Platform Configuration
Private IP Disclosure	Configuration and Deploy Management Testing	OTG-CONFIG-001	Test Network/Infrastructure Configuration
Self-signed TLS/SSL certificate	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Information Gathering	OTG-INFO-008	Fingerprint Web Application Framework

ZJIŠTĚNÉ NÁLEZY	OWASP Charakteristiky		
zranitelnosti	**GROUP (skupina)**	**ID (identifikační číslo)**	**ID DESC (popis ID)**
SMBv2 signing not required	Authentication Testing	OTG-AUTHZ-004	Testing for bypassing authentication schema
TCP timestamp response	Information Gathering	OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage
Timestamp Disclosure - Unix	Information Gathering	OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage
TLS Server Supports TLS version 1.0	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
TLS Server Supports TLS version 1.1	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
TLS/SSL Server is enabling the BEAST attack	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
TLS/SSL Server Supports 3DES Cipher Suite	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
TLS/SSL Server Supports The Use of Static Key Ciphers	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
Untrusted TLS/SSL server X.509 certificate	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
Web Browser XSS Protection Not Enabled	Input Validation Testing	OTG-INPVAL-002	Testing for Stored Cross Site Scripting
X.509 Certificate Subject CN Does Not Match the Entity Name	Cryptography	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
X-AspNet-Version Response Header Scanner	Information Gathering	OTG-INFO-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection

ZJIŠTĚNÉ NÁLEZY	OWASP Charakteristiky		
zranitelnosti	**GROUP (skupina)**	**ID (identifikační číslo)**	**ID DESC (popis ID)**
X-Content-Type-Options Header Missing	Configuration and Deploy Management Testing	OTG-CONFIG-002	Test Application Platform Configuration
X-Frame-Options Header Not Set	Client Side Testing	OTG-CLIENT-009	Testing for Clickjacking
X-Frame-Options Setting Malformed	Client Side Testing	OTG-CLIENT-009	Testing for Clickjacking

Příloha IV. - ZAP report katalogizační reference (autor – zdroj report ZAP)

Medium (Medium)	X-Frame-Options Setting Malformed
Description	An X-Frame-Options header was present in the response but the value was not correctly set.
URL	https:// xxxxxxxxxxxxxx/portal/home/webmap/viewer.html
Method	GET
Parameter	X-Frame-Options
Evidence	Allow
URL	https:// xxxxxxxxxxxxxx /portal/home/webscene/viewer.html
Method	GET
Parameter	X-Frame-Options
Evidence	Allow
Instances	2
Solution	Ensure a valid setting is used on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	https://tools.ietf.org/html/rfc7034#section-2.1
CWE Id	16
WASC Id	15
Source ID	3

Příloha V. - Web spidering (autor zdroj Nexpose konfigurační template)

Nexpose Web Spidering Parameters	
SKUPINY/POLOŽKY	**PARAMETRY**
Web Spidering	
Test cross-site scripting in a single scan	ano
Performance	
Maximum number of foreign hosts to resolve	100
Spider response timeout (s)	120
Maximum directory levels to spider	6
Maximum spidering time (minutes)	no limit
Maximum pages to spider	3000
Maximum retries for spider requests	2
Spider threads per Web server	3
HTTP daemons to skip while spidering	Virata-EmWeb, Allegro-Software-RomPager, JetDirect, HP JetDirect, HP Web Jetadmin, HP-ChaiSOE, HP-ChaiServer, CUPS, DigitalV6-HTTPD, Rapid Logic, Agranat-EmWeb, cisco-IOS, RAC_ONE_HTTP, RMC Webserver, EWS-NIC3, EMWHTTPD, IOS, ESWeb
Maximum link depth to spider	6
CIFS/SMB Account Policy	
Account lockout threshold	3
Minimum password length	6
Unix Policy	
Minimum account umask value	077