Vliv zabezpečení webových stránek na pořadí zobrazení pomocí webových vyhledávačů

Jitka Sochorová

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jitka Sochorová**
Osobní číslo:	**A16052**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Vliv zabezpečení webových stránek na pořadí zobrazení pomocí webových vyhledávačů**
Téma anglicky:	**The Impact of Website Security on Viewing Order by Web Search Engines**

Zásady pro vypracování:

1. **Rozepište problematiku zabezpečení webových stránek a s tím spojené terminologie.**
2. **Popište a rozeberte problematiku optimalizace webových stránek ve vazbě na prioritu zobrazení webovými prohlížeči.**
3. **Vyberte metody a nástroje pro testování bezpečnosti webových stránek a priority vyhledávání.**
4. **Proveďte implementaci webové stránky pro potřeby testování se zaměřením na bezpečnost webových stránek.**
5. **Vhodně reprezentujte výsledky a stanovte doporučení na základě získaných výsledků.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.**
2. **KUBÍČEK, Michal a Jan LINHART. 333 tipů a triků pro SEO: [sbírka nejlepších technik optimalizace webů pro vyhledávače]. Vyd. 1. Brno: Computer Press, 2010, 262 s. ISBN 978-80-251-2468-0.**
3. **GRAPPONE, Jennifer a Gradiva COUZIN. SEO =: Search Engine Optimization : ovládněte SEO a získejte výhodu před konkurencí: optimalizujte své webové stránky pro vyhledávací servery: přiveďte na své stránky zákazníky dříve, než to udělá konkurence.**
4. **STALLINGS, William a Lawrie BROWN. Computer security: principles and practice. Third edition. Boston: Pearson, [2015], 840 s. Always learning. ISBN 978-1-292-06617-2.**
5. **BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority : legislativní rámec elektronického podpisu : praktické aplikace. Olomouc: ANAG, 2008, 157 s. Právo. ISBN 978-80-7263-465-1.**
6. **BARNETT, David N. Brand protection in the online world: a comprehensive guide. London: Kogan Page, [2017], 268 s. ISBN 978-0-7494-7869-8.**
7. **SCHMIDT, Eric, Jonathan B. ROSENBERG a Alan EAGLE. Jak funguje Google. Vydání první. Autor úvodu Larry PAGE, přeložil Martin BEDNARSKI. Brno: Jota, 2015, 318 s. ISBN 978-80-7462-749-1**

Vedoucí bakalářské práce: **Ing. Petr Žáček**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **20. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 20. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá spojením zabezpečení webových stránek s optimalizací pro vyhledávače. Klíčovou částí práce je zkoumání vlivu zabezpečeného protokolu na pořadí zobrazení webové stránky ve výsledcích vyhledávání. Teoretická část zahrnuje možnosti zabezpečení webů s využitím SSL protokolů a certifikátů, vydávaných certifikačními autoritami. Součástí teorie je představení optimalizace pro vyhledávače, její role v online marketingu a popsání dostupných vyhledávačů. Praktická část je věnována převedení konkrétní webové stránky na zabezpečený protokol, analýze pomocí vhodných nástrojů a návrhu doporučení pro optimalizaci. Výstupem je zhodnocení působení zabezpečení webu na SEO.

Klíčová slova:

SEO, SERP, snippet, webové vyhledávače, zabezpečení webu, HTTPS, SSL certifikáty

ABSTRACT

Bachelor thesis concerns to connection of website security and search engine optimization. The aim is examine the effect of implementation secure protocol and order of view in SERP. There are two parts. First one is theoretical where possibilities of web pages security are described. As well as security SEO and it’s role in online marketing are described. It includes known search engines and their behaviour. In practical part of thesis there is transfer to security protocol and implementation of propriate tools. The resolution includes examination if there is any impact of website security on the order of view by web search engines.

Keywords:

SEO, SERP, snippet, search engine, website security, HTTPS, SSL certificates

Ráda bych poděkovala vedoucímu bakalářské práce Ing. Petru Žáčkovi za cenné rady, připomínky a trpělivost při vedení mé práce. Poděkování patří také mé rodině, mým blízkým a kolegům za poskytnutí prostoru, důvěry a motivace v průběhu zpracovávání bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Žijeme v době, kdy populace tráví většinu času ve společnosti elektronických zařízení. Společně s reálnými lidmi se musel celý svět přizpůsobit moderním technologiím. Ve světě marketingu je tomu také tak, a proto se z velké části přesunul do online prostředí. Online marketing současné doby je obrovsky rozvinutá disciplína, která se velmi rychle vyvíjí. Prodejci se sice stále předhánějí, kdo vyrobí lepší produkt, ale zároveň soutěží na poli webových stránek, sociálních sítí a PPC reklam.

Společně s přesunem do online prostředí vznikly nové hrozby, které číhají na uživatele Internetu. Mezi ty nejčastější patří zneužití citlivých údajů, ke kterým se řadí přístupové údaje do bankovních účtů, emailových schránek apod. Jsme nuceni se bránit. Stejně tak se musí bránit správci webových stránek. V současnosti jsou kladeny daleko vyšší nároky na zabezpečení webů. Proč? Z bezpečnostního hlediska, aby neunikaly údaje a nezneužívalo se jich. Z hlediska marketingového, aby byly weby pro uživatele vzhledově přívětivé, a na první pohled důvěryhodné. Za jakým účelem? Primárním cílem je zisk.

Jak spolu tyto dvě disciplíny souvisí? V online prostředí se vyskytují „giganti“, kteří se stali autoritami pro provozovatele webových stránek. Jsou jimi webové vyhledávače. Monopol mezi vyhledavači vlastní firma Google. Tato firma určuje pravidla hry. Právě Google v nedávné době přiložil do kotle všem marketérům a začal hodnotit webové stránky na základě jejich zabezpečení. Cílem je uživatelská přívětivost a jejich bezpečí. Stává se tedy zabezpečení webových stránek jedním z hlavních hodnotících kritérií pro zobrazení webu na předních příčkách ve výsledcích vyhledávání?

V teoretické části práce budou separovaně popsány principy zabezpečení webových stránek a optimalizace pro vyhledávače. Zabezpečení webových stránek zahrnuje popis využití HTTPS protokolu, jeho souvislost s SSL certifikáty a certifikačními autoritami. Marketingová část obsahuje představení současných postupů pro zlepšení vyhledatelnosti stránek, které se reálně využívají v praxi, a také popis současných webových vyhledávačů.

Cílem praktické části bakalářské práce je převedení webové stránky na zabezpečený protokol pomocí certifikační autority Let’s Encrypt a nastavení parametrů potřebných ke správnému zabezpečení. Podniknuté kroky budou vyhodnoceny pomocí online nástrojů pro zhodnocení bezpečnosti nasazeného protokolu. Současně budou navrženy doporučení vedoucí k optimalizaci stránky pro vyhledávače. V závěru bude vyhodnocen vliv certifikátu na zobrazení webové stránky ve vyhledávání.

I. TEORETICKÁ ČÁST

1 ZABEZPEČENÍ WEBOVÝCH STRÁNEK

Komunikace na internetu probíhá nejen při odesílání e-mailů, ale také při samotném prohlížení webových stránek. Výsledkem nezabezpečené komunikace jsou uniknutá data ve formě hesel k e-mailům či internetovému bankovnictví, v jiných případech se útočníci mohou zaměřovat na data úřadů a státu. O zabezpečení komunikace na internetu se starají SSL a TLS protokoly. [1]

Informace na webových stránkách si posílají klient a server. Klientem může být například internetový prohlížeč a server je ten, na kterém běží konkrétní webové stránky. Přenášené informace existují nejen ve formě obsahu webové stránky, ale také ve formě informací o pohybu uživatelů – například to, co uživatel vidí a dělá. Z toho důvodu je za potřebí komunikaci zabezpečit, protože jiní uživatelé by se mohli vydávat za její účastníky a jednoduše odposlouchávat informace. O bezpečnost webových stránek se starají TLS protokoly, které společně s protokolem HTTP vytvoří zabezpečený protokol HTTPS.

1.1 HTTP a HTTPS

Zkratka HTTP skrývá HyperText Transfer Protocol a využívá se ke komunikaci prohlížeče se serverem. Nicméně komunikace je otevřená a kdokoli ji může číst. Veškerá zadaná hesla či vyplněné formuláře je možné veřejně zobrazit. K zabezpečení citlivých údajů byl vyvinut protokol HTTPS, kde velké S na konci znamená Secure. [2, 3]

Nutnost zabezpečení je nejvíce vyžadována právě u e-shopů, při zadávání údajů o kartě, u webů využívajících kontaktní formuláře i u webových stránek, u kterých je nutná určitá důvěryhodnost.

HTTPS využívá protokol HTTP a TLS. Reálně přenáší nezabezpečený protokol pomocí TLS po šifrovaném tunelu a celý provoz běží na portu 443. Pro umožnění celého procesu je zapotřebí právě asymetrické kryptografie. [4, 5]

1.1.1 Asymetrická kryptografie

Funguje na principu dvou klíčů. Veřejného a privátního. Veřejný klíč se používá k zabezpečení, je volně dostupný, a proto může každý uživatel poslat zašifrovanou zprávu příjemci. Každopádně příjemcovu zprávu nemohou přečíst všichni. Privátní klíč se používá k odšifrování. Díky němu lze přečíst přijatou zašifrovanou zprávu. Asymetrická kryptografie

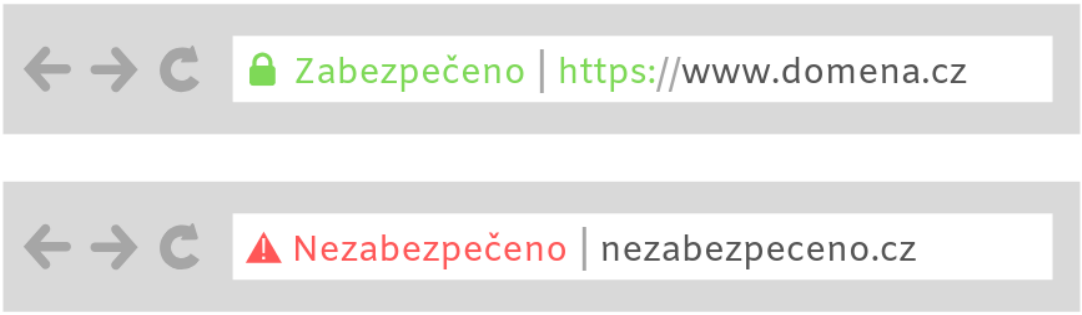
se vysoce podílí na principu funkce bezpečnostních certifikátů a bez jejího pochopení nelze činnosti SSL porozumět.

1.1.2 Důvody pro zabezpečení

Šifrování komunikace na internetu již není žádnou nadstandartní službou, ale neodmyslitelnou součástí každé kvalitní webové stránky. Důvodů pro zabezpečení je několik a mezi ty nejvýznamnější patří ochrana uživatelů. Bezpečný web chrání návštěvníky před odposlechem komunikace a zajišťuje jejich důvěru při pohybu na stránkách.

Se zabezpečením komunikace úzce souvisí odesílání formulářů na webu. V nich se často odesílají osobní údaje ve formě jména, příjmení, přihlašovacích údajů, hesel, čísla kreditních karet apod. Aby provozovatelé webových stránek zajistili bezpečnost v souladu s GDPR z roku 2018, nesmí žádný web s formuláři běžet na nezabezpečeném protokolu. [6]

V souvislosti s důvěryhodností webové stánky začaly dbát na protokoly HTTPS i internetové prohlížeče. Vše začalo pouhým rozlišením bezpečné stránky pomocí zámečku vedle doménového jména. Současná podoba se liší na základě použitého certifikátu. Nejvyšší certifikáty obsahují zelený zámeček a adresu firmy v adresním řádku. Google se v roce 2018 rozhodl posunout o krok dál a s verzí 68 prohlížeče Chrome začal označovat nezabezpečené weby červenou barvou za účelem zvýšení viditelnosti a případné odrazení uživatelů od používání stránek. Jedná se o důležitý bod z hlediska optimalizace pro vyhledávače, právě protože webové vyhledávače zabezpečený protokol zohledňují. [7]



Obrázek 1 - Zabezpečená vs. nezabezpečená doména [vlastní tvorba]

Nová verze internetového protokolu se nazývá HTTP/2. Jeho cílem je primárně urychlení načítání dat a celkové zrychlení plynulosti webových stránek. V současnosti se rozšiřuje po celém světě a je stále využívanější. Předpokládá se, že se zanedlouho stane standardem. Webová stránka může využívat HTTP/2 pouze ve chvíli, kdy využívá protokol HTTPS, což je dalším důvodem pro migraci. [8]

1.2 Bezpečnostní certifikáty

Certifikáty jsou veřejné dokumenty, které propojují doménové jméno s veřejným klíčem. Bezpečnostní certifikáty jsou vystavovány prověřenými certifikačními autoritami. Jejich obsahem jsou základní údaje ve formě:

- Jmény autority
- Názvu domény
- Veřejného klíče
- Údajů o platnosti
- Podpisu autority [5, 9]

Jednoduše lze certifikáty definovat jako dokumenty jednoznačně prokazující identitu webové stránky.

1.2.1 Typy certifikátů

Na trhu se nachází již velká nabídka bezpečnostních certifikátů. Pohybují se v různých cenových hladinách a nabízejí různé možnosti:

- **Základní certifikáty** - webovou stránku lze plnohodnotně zabezpečit již nejlevnějším typem certifikátů, jehož cena se pohybuje od dvou set korun. Používané certifikáty jsou RapidSSL či Comodo a dokáží zašifrovat komunikace, a dokonce i zmizí červené označení z adresního řádku. [10]
- **Zelené certifikáty** - nejdražší a nejdůvěryhodnější certifikáty, označují se EV a obsahují zelený název společnosti vedle názvu domény. Souhrnně se nazývají zelené certifikáty. Jejich cena neklesne pod dva tisíce korun. [11]
- **SAN certifikáty** – SSL certifikáty, zabezpečující několik domén najednou. Stránky lze přidávat až do skončení platnosti. Jejich ceny se pohybují v řádech tisíců. [12]
- **Wildcard** – typ certifikátu, který se jinak nazývá hvězdičkový. Jeho hlavní vlastností je, že pomocí něj lze zabezpečit hlavní doménu a všechny její subdomény. Počet subdomén je neomezený. [13]

Kromě výše zmíněných certifikátů existují na trhu certifikáty pro podpis kódu, které se nazývají Code signing. Slouží pro vývojáře aplikací nebo souborů, nacházejících se na webu. Setkat se lze také s osobními certifikáty pro ověření identity uživatele na internetu a používají se pro podpis smluv nebo emailů.

1.2.2 Druhy certifikátů dle ověření

Certifikáty se kromě typů dělí i podle ověření. Než je certifikát vystaven je nutné ověřit žadatele. Jedná se o proces validace, která je proveditelná třemi různými způsoby:

- **Ověření domény (DV)** – ověření pomocí domény je nejlevnější způsob a probíhá pouze elektronicky skrz emailovou komunikaci. Kromě nízké ceny je proces získávání certifikátu velmi rychlý. Z toho důvodu se vyplatí malým jednoduchým webům. Samotný certifikát neobsahuje žádné další informace o žadateli. [14]
- **Ověření společnosti (OV)** – certifikace ověření společnosti probíhá nejen elektronicky, ale i telefonicky. Žadatel musí kontaktovat společnosti vystavující certifikáty a prokázat, že se jedná o opravdu o provozovatele webových stránek. [14]
- **Rozšířené ověření (EV)** – certifikáty s rozšířeným ověřením poskytují nejvyšší stupeň zabezpečení. Validace probíhá důkladněji a tyto typy certifikátů jsou již standardem pro finanční instituce, velké firmy a v současnosti také e-shopy. Největší výhodou EV certifikátů je název společnosti zelenou barvou v adresním řádku. Uživatelé mohou na první pohled vidět, komu daná stránka patří. [14]

Obrázek 2 - Druhy certifikátů dle ověření [vlastní tvorba]

1.2.3 Certifikační autority

Certifikační autorita je nezávislý subjekt, který vydává TLS certifikáty. Ověřují pravost veřejného klíče. Autority musí splňovat podmínky CAB fóra, což je subjekt, který sdružuje certifikační autority. Jejich cílem je vytvoření pravidel a standardů, kterými se jednotlivé autority musí řídit. Kromě certifikačních autorit jsou členy fóra také tvůrci internetových prohlížečů. Patří mezi ně Apple, Google, Microsoft Corporation, Opera Software ASA a The Mozilla Foundation. [15]

Mezi nejznámější certifikační autority v České republice patří Comodo, Rapid SSL, Symantec a Thawte. [16]

1.2.4 Let's Encrypt

Současná nejpoužívanější autorita pro zabezpečení webových stránek zadarmo na nazývá Let's Encrypt. Na internetu působí od roku 2015 a poskytuje zdarma SSL certifikáty doménám. Často je navrhována provozovatelům webů přímo poskytovatelem webových serverů. Vzhledem k nulovým poplatkům za certifikát má v současnosti Let's Encrypt určitá omezení. Není jej možné poskytnout doménám třetího řádu, a také není podporován některými webovými prohlížeči a operačními systémy. Platnost certifikátu je omezená na tři měsíce. Poskytovatelé webhostingů nabízí bezplatné certifikáty uživatelům, kteří mají zakoupené domény druhého řádu. [17]

Proces získání certifikátu od Let's Encrypt probíhá přihlášením do administrace webhostingu a vyhledáním položky „HTTPS", kde se dá o SSL požádat.

1.3 SSL a TLS protokoly

Zkratka SSL znamená Secure Sockets Layer a jedná se o označení kryptografických protokolů pro ochranu internetové komunikace. V minulosti se využívaly protokoly SSL, nyní byly nahrazeny modernější verzí – TLS protokoly (Transport Layer Security). TLS 1.0 je nástupcem SSL 3.0 s několika vylepšeními. Ačkoliv se v praxi používá TLS protokol, zkratka SSL je již dlouho zažitá a používá se nadále. Mluví-li se tedy o SSL komunikaci, jedná se již vždy o TLS. [1, 2]

Certifikáty zajišťují bezpečnou komunikaci na internetu a jsou užitečné nejen v samotném zajištění bezpečnosti, ale i v optimalizaci pro vyhledávače.

1.3.1 SSL protokol

Protokoly SSL se využívají ze dvou hlavních důvodů:

- Identifikace
- Šifrování komunikace.

Identifikace zajišťuje jistotu klientovi i serveru, že komunikují spolu navzájem a nikdo cizí se nevydává za jednoho z účastníků komunikace. Šifrování zajistí bezpečnou výměnu klíčů a uplatnění šifrovacího algoritmu.

SSL certifikáty zajistí, že z adresního řádku zmizí označení „Nezabezpečeno“, objevující se u webů bez zabezpečení. Od nové verze Google Chrome jej prohlížeč zvýrazňuje červeně, čímž může způsobit horší uživatelský zážitek.

1.3.2 Druhy SSL certifikátů

Existuje několik druhů SSL certifikátů. Rozdíly mezi nimi se projeví jak v ceně daného certifikátu, tak v jeho podobě vedle adresního řádku. Podoba může mít vliv na důvěryhodnost webové stránky a tím pádem i dojem v očích uživatelů. [18]

1.3.2.1 Nejlevnější SSL certifikáty

Základní certifikáty se pohybují v řádech sta korun. Získání zmíněného typu je možné za pár minut a je k němu zapotřebí pouze zadání objednávky, její uhrazení a potvrzení emailu. V rámci certifikace je ověřena doména a její existence. Použitelné jsou jak pro webové stránky, tak pro intranety, zákaznické portály apod. Zmíněné typy odpovídají OV a DV certifikátům. [10]

1.3.2.2 Zelené SSL certifikáty

Nejdůvěryhodnějšími certifikáty v rámci zabezpečení webových stránek jsou zelené certifikáty. Nazývají se tak, protože v případě jejich použití, je v adresním řádku napsaný zeleně název firmy, které byl certifikát poskytnut. Odpovídají EV certifikátům. Uživatelé tak mohou jednoznačně identifikovat, zda se nacházejí na důvěryhodné stránce a nejedná se například o phisingový útok. V minulosti byly dominantou převážně finančních institucí – bank, internetových bankovnictví či větších firem s vyššími rozpočty. Certifikáty se dají pořídit od dvou či tří tisíc korun za rok. Na trhu jsou k dispozici zelené certifikace pro jednu či více domén najednou. [11]

1.3.3 Verze protokolů a jejich zranitelnosti

TLS protokol 1.0 byl nástupcem SSL 3.0. V současnosti je však tato verze již také zastaralá. Od léta 2018 nesmí být TLS 1.0 používána u webů s platebními branami. Její nadstavba 1.1 používá stejné algoritmy MD5 a SHA-1, které jsou již prolomené. Podporuje-li server stále verze 1.0 a 1.1 hrozí, že útočník může využít zranitelnosti, která se nazývá PoodleBleed a donutit ho místo novějších verzí 1.2 a 1.3 využít verze staré. [19] Rizikem je přečtení zašifrovaných dat z útočníkovi pozice Man-in-the-middle a řešením vypnout zastaralý SSLv3 protokol ve službách, které ho využívají a předejít tak úniku informací. [20]

Další bezpečnostní dírou v serverech je tzv HeartBleed. Jedná se o chybu v knihovně OpenSSL, která je klíčová při implementaci SSL a TLS protokolů. Zranitelnost HeartBleed umožní útočníkům zjistit podobu privátního klíče a tím komunikaci dešifrovat. Týká se verzí protokolů 1.0.1 až 1.0.1f a ochrana před ní je možná aktualizací OpenSSL knihovny. [21]
Mezi další známé zranitelnosti patří Crime, která umožní útočníkovi napadnout hrubou silou ověřovací cookies a jejím řešením je nevyužívat kompresi u SSL. [22]
Útok směřující přímo na protokol, a ne na identitu jako většina ostatních, se nazývá Beast a může dešifrovat HTTPS komunikaci. Útok donutí proces šifrování bloků zmanipulovat tak, aby se jednotlivé bloky šifrovaly stejným klíčem. Tento typ útoku postihuje SSLv3 a TLS 1.0. Současné verze TLS 1.1 a 1.2 jsou proti útoku chráněné, přechod na ně je řešením proti Beast útoku. [23]
Nejnovější verzí TLS protokolů je 1.3, která byla představena v roce 2018. Nová verze nepodporuje prolomené šifry a nebezpečné algoritmy. Mezi její další výhody patří zkrácení času pro handshake, protože verze 1.0, 1.1 i 1.2 využívaly komunikaci ve dvou cyklech, nazývaných 2-RTT. Zmíněný proces trval až půl sekundy. Handshake u 1.3 probíhá v jednom cyklu a nazývá se 0-RTT. Protokol tak zajišťuje rychlejší komunikaci mezi klientem a serverem. V současnosti je již možné novou verzi zapnout, nalézt ji lze hlavně v nejnovějších verzích internetových prohlížečů. [24]
Předejít využití téměř všech zranitelností útočníkem lze udržováním aktuálního operačního systému a pravidelnou aktualizací webového prohlížeče.

1.4 Migrace webové stránky na HTTPS

Při migraci webové stránky na zabezpečený protokol je pro správné převedení nutné dodržet několik zásadních bodů. Bez jejich splnění může být web špatně indexován nebo se mohou tvořit duplicitní webové stránky. Další chyby vyhledávače trestají penalizací a celkově lze úplně přijít o návštěvnost a zdroj zisku.

1.4.1 Přesměrování webu 1:1

Důležitá část samotného převodu webu je přesměrování stránek s kódem 301 z nezabezpečeného protokolu na zabezpečený. V praxi jde o nahrazení všech adres http:// na https:// v poměru 1:1. Poměr je důležitý kvůli indexaci webové stránky. Zároveň v adrese nesmí dojít například ke změně velikosti písmen. Přesměrování lze provést v konfiguračním souboru htaccess nebo pomocí pluginu. V případě redakčního systému

WordPress se jedná o pluginy Really Simple SSL nebo Better Search Replace. Přesměrování se týká také adres veškerých obrázků, JavaScriptů, kaskádových souborů, PDF a dalších multimédií. Žádoucí je také změnit adresy, které se nacházejí v článcích a na sociálních sítích. [25]

1.4.2 Zacyklení

Častou chybou při přesměrování je zacyklení adres. Vzniká ve chvíli, kdy jedna adresa směruje na druhou a na druhé je vytvořen redirect na první. Požadavek je tak odesílán neustále dokola a může vést ke spadnutí serveru. Samotné zacyklení dělá problémy také robotům, kteří se ztratí při indexaci webové stránky. Řešením je důkladná kontrola přesměrovávaných url adres. V praxi se používá tabulka v Excelu, obsahující staré adresy a k nim odpovídající nové.

1.4.3 Robots.txt a sitemap.xml

Starý web obsahuje vlastní soubor robots.txt s pravidly, kterými se řídili roboti na staré verzi webu. Je-li požadováno, aby se roboti chovali stejně při procházení zabezpečené verze webu je vhodné vytvořit soubor nový. V případě, že by se verze souboru na HTTP přesměrovala na verzi bez HTTPS, přestala by existovat a roboti by mohli získat přístup ke stránkám, které byly zakázané.

Mapu webu je vhodné vytvořit znovu pro novou verzi webu a adresu na verzi sitemap.xml s HTTPS připsat do souboru robots.txt.

1.4.4 Nasazení webu a indexace

Po zveřejnění nové verze webu proces nekončí. Je důležité kontrolovat správnost provedení. Indexaci lze uspíšit přidáním ideálně pěti nejdůležitějších url adres do vyhledávačů. Seznam i Google mají své vlastní nástroje pro ověření adres. Zmíněný krok lze interpretovat jako pozvání robotů na web, aby ho mohli zaindexovat.

Trvá několik dní i týdnů, než vyhledávače zareagují na změny. Doporučuje se sledovat výkonnost stránky pomocí analytických nástrojů. Počet zaindexovaných stránek je viditelný v nástrojích Google Search Console a Collabim.

1.5 WordPress a zranitelnosti webových aplikací

WordPress je jeden z nejpoužívanějších redakčních systémů na světě. Jeho použití je zdarma a v současnosti je využíván pro správu nejen malých blogů, ale i velkých webů. Pro jeho časté používání je terčem útočníků vyhledávajících bezpečnostní slabiny, kterých by zneužili.

Pro dosažení aplikační bezpečnosti se rozhodla nezisková organizace OWASP šířit povědomí o nejvyskytovanějších rizicích pomocí projektu Top 10. Jeho cílem je seznámit vývojáře s bezpečnostními problémy, které se běžně vyskytují v aplikacích, a předcházet jim. Projekt obsahuje popis deseti bezpečnostních rizik aplikací a jejich řešení. [26]

1. **Injection** (injektování) – týká se převážně dotazů v databázích, příkazech v operačním systému apod. Díky chybě lze aplikaci napadnout škodlivým kódem skrz neošetřený vstup. Řešením injektování je oddělit nedůvěryhodná data od dotazů a příkazů. [26]
2. **Broken Authentication** (chybná autentizace) – riziko využívající chybu vytvořenou při tvorbě ověřování uživatelů, cílem je zneužití identity uživatele. Prevencí je vytvoření silného řízení autentizace. [26]
3. **Sensitive Data Exposure** (expozice citlivých dat) – chyba způsobující odcizení citlivých údajů, vznikající při nedostatečném šifrování dat v průběhu komunikace. Prevencí proti zranitelnosti je využití bezpečného SSL certifikátu. [26]
4. **XML External Entities** (XXE - útok externí entity) – jedná se o útok proti aplikacím, který zneužívá zastaralé či nesprávně konfigurované soubory. Řešením je eliminovat nepotřebné XML a nahradit je například formátem JSON. [27]
5. **Broken Access Control** (nefunkční kontrola přístupu) – špatně ošetřenou kontrolou přístupu se může útočník jednoduše dostat k citlivým údajům. Problému dokáže předejít bezpečný autorizovaný modul. [28]
6. **Security Misconfiguration** (nezabezpečená konfigurace) – riziko způsobující neautorizovaný přístup útočníka k datům, vzniká při zanedbání aktualizací či nedostatků konfigurace systému. Řešením jsou pravidelná testování bezpečnosti, udržování aktuálnosti systémů a správná konfigurace. [26]
7. **Cross-Site Scripting (XSS)** – pomocí zranitelnosti dokáže útočník spouštět skripty v prohlížeči uživatele. Jedná se o nejrozšířenější chybu, jejímž řešením je oddělení nedůvěryhodných dat od aktivního obsahu. [26]

8. **Insecure Deserialization** (nezabezpečená deserializace) – jedná se o riziko, které je méně pravděpodobné, každopádně má velmi závažné následky. Hrozba umožňuje útočníkovi spuštění škodlivého kódu chybou způsobenou při převodu proudu bytů na kopii objektu. Riziko je možné snížit kontrolou integrity příchozích souborů. [27]
9. **Using Components with Known Vulnerabilities** (použití známých zranitelných komponent) – riziko vzniká nedostatečnou kontrolou použitých knihoven či pluginů. Útočník zneužije bezpečnostních děr v prolomených komponentech. [26]
10. **Insufficient Logging and Monitoring** (nedostatečné logování a monitorování) – základem pro úspěšný útok je pro útočníky nutné, aby zjistili, které bezpečnostní díry aplikace obsahuje. Z toho důvodu je nejdříve musí objevit. Aplikace by tak měly nabídnout notifikace v případě nestandartního chování systému, čímž by se dalo útokům předejít nebo je alespoň včas objevit. [27]

2 OPTIMALIZACE PRO VYHLEDÁVAČE (SEO)

Zkratka SEO z angličtiny znamená Search Engine Optimization. Z anglického jazyka lze search engine interpretovat jako softwarový program, který vyhledává na internetu. Pojem optimalizace pro vyhledávače je sice mylným překladem, ale již zavedeným a v praxi hojně využívaným. [29]

SEO je součást online marketingu a lze ji pochopit jako proces činností, které vedou k lepší nalezitelnosti webové stránky. Cílů optimalizace pro vyhledávače může být několik. Mezi ty základní patří zvýšení návštěvnosti, vyšší proklikovost ve výsledcích vyhledávání, zvýšení šancí pro nalezení webu uživateli, vyšší počet konverzí apod.

Kromě optimalizace pro vyhledávače patří do online marketingu další aktivity, které vedou k prodeji produktů a služeb na internetu. Jsou jimi webové stránky a internetové obchody, e-mail marketing a PPC reklama. [30]

Obrázek 3 - Online marketing a jeho části [vlastní tvorba]

SEO je soubor kroků směřujících k zobrazování webové stránky na vysokých příčkách ve výsledcích vyhledávání, a to i ve chvíli, kdy není zavedena placená reklama. Návštěvnost přivedená z vyhledávání, která nebyla podpořena PPC reklamou, se nazývá organická. Je-li uživatel přiveden na webovou stránku proklikem z vyhledávání, znamená to, že daná stránka obsahovala informaci, odpovídající vyhledávacímu dotazu uživatele. Tato informace se nazývá relevantní.

2.1 Pojmy používané v SEO

SEO je plné zkratek, zavedených slov z angličtiny nebo výrazů, které jsou si až příliš podobné. Výrazy spolu úzce souvisí. Prvním z nich je SERP (Search Engine Result Page) – výsledky vyhledávání. Jedná se o první stránku, kterou uživatel vidí po kliknutí na tlačítko „hledej“ ve vyhledávání. Se SERPem úzce souvisí Snippet, který se v něm zobrazuje a obsahuje titulek a meta description dané stránky, svým vzhledem může mít vliv na CTR. CTR (Click-through rate) je poměr mezi počtem zobrazení a počtem prokliků, překládá se jako míra prokliku. Využívá se převážně při vyhodnocování návštěvnosti.

Dalším hojně používaným pojmem je vyhledávací dotaz. Jedná se o slovo nebo skupinu slov, která uživatel zadává do vyhledávacího řádku. Často je zaměňován s klíčovým slovem a naopak. Klíčové slovo je slovo nebo skupina slov, na která PPC a SEO specialisté cílí. Více vyhledávacích dotazů může směřovat k jednomu klíčovému slovu.

2.2 On-page faktory

Faktory on-page jsou ty, které mohou být přímo ovlivnitelné autorem webových stránek. Nacházejí se přímo na webu a kromě viditelného obsahu se jedná také o technické aspekty. [31]

2.2.1 Technické SEO

Technické SEO se postupně stává velkou samostatnou disciplínou, která již má své vlastní specialisty. Jedná se o velmi obsáhlou část optimalizace pro vyhledávače, zabývající se technickými parametry webových stránek.

Dřívější dělení optimalizace je tak doplněno o technické SEO, které se sice převážně řadí do on-page faktorů, zasahuje ale také i do off-page faktorů. [32]

2.2.1.1 Indexace a Crawling

Aby se webová stránka mohla zobrazit ve výsledcích vyhledávání je nutné, aby ji roboti vyhledávačů zaindexovali. Stránky uložené v indexu se poté zobrazují uživatelům v SERPu. Důležité je, aby byly zaindexovány stránky, které mají unikátní a hodnotný obsah. Stránky s duplicitním obsahem, UTM parametry, url s nedůležitým obsahem apod. do indexu nepatří. Pro indexaci jsou důležité dva soubory. Prvním ze souborů je sitemap.xml. Představuje mapu webu, ve které jsou uvedeny stránky určené k procházení a indexaci. Soubory sitemap.xml lze rozdělit na několik souborů. Lze vytvořit separované mapy pro stránky, obrázky i videa. Roboti se o umístění souborů dozví uvedením adresy sitemapy

v souboru robots.txt, případně nahráním mapy do nástroje Google Search Console. Ve zmíněném souboru robots.txt je kromě adresy na mapu webu uvedeno, jaké části webu mohou roboti procházet a jaké nikoliv. Díky němu lze předejít zbytečnému procházení stránek a vytváření duplicit. Roboti tento soubor procházejí jako první. Umístěn by měl být v kořenovém adresáři webu. [32]

Pojem crawling představuje procházení webu robotem. Aby vyhledávače dokázaly nabídnout uživateli nejvíce relevantní obsah je nutné, aby udržovaly svou databázi aktuální. Pro stanovení priorit procházení vznikl crawl budget. Jedná se o čas, který roboti stráví na jedné webové stránce. Zahrnuje také počet stránek, které během návštěvy projde. [32]

2.2.1.2 Zabezpečení webu

Komunikace na webu funguje na principu dotazů a odpovědí. Využívá se při ní internetový protokol HTTP (Hypertext Trasfer Protocol), který slouží k výměně HTML souborů. Prohlížeč pošle dotaz na server, ten ho zpracuje a pošle odpověď. Bezpečnostní nevýhodou této komunikace je její snadná prolomitelnost. Může být jednoduše odchycena a případně i upravena. Pro bezpečný přenos komunikace slouží protokol HTTPS. [32]

Důležitým milníkem pro SEO byl rok 2014, kdy začal Google hodnotit webové stránky na základě přítomnosti protokolu HTTPS a od roku 2018 (od verze Chrome 68) označuje nezabezpečené stránky červeným nápisem „Nezabezpečeno“.

2.2.1.3 Rychlost načítání

Rychlost načtení webové stránky patří mezi hodnotící faktory vyhledávačů. Doporučovaná maximální rychlost by neměla klesnout pod čtyři sekundy. Pro dobrou uživatelskou zkušenost však platí, že čím rychleji je web načtený, tím lépe. Google pro měření rychlosti načítání nabízí bezplatný nástroj Google PageSpeed Insights, který zahrnuje nejen analýzu současného stavu, ale i doporučení pro zlepšení. Zmíněný nástroj je vhodný převážně k rychlé kontrole. Pro komplexnější hodnocení existují online nástroje WebPageTest.org nebo GTmetrix.com. [32]

2.2.1.4 Optimalizace pro mobilní zařízení

Přizpůsobení webových stránek pro mobilní zařízení, kterými jsou kromě telefonů také tablety, je dalším důležitým technickým aspektem pro zlepšení pozice ve vyhledávačích. Důvodem je stále vyšší podíl mobilních zařízení na návštěvnosti webových stránek.

Mobilní verze webů je nejčastěji řešena pomocí:

- responzivních designů,
- odlišnou mobilní a desktopovou verzí.

Nevýhodou druhé možnosti je, že se jedná o dvě různé url adresy a vyhledávače je mohou považovat za duplicitní obsah. Předcházet zmíněnému problému lze pomocí identifikace hlavního webu kanonickou značkou, která se vkládá do hlavičky zdrojového kódu:

<link rel="canonical" href=http://www.nazev.cz />

V minulosti vyhledávače procházely stránky primárně podle desktopové verze, ale v roce 2018 Google oznámil, že zavádí Mobile-First Index. Znamená to, že Google nejdříve prochází mobilní verzi a na jejím základě hodnotí weby. Úplně nejnovější technologie mobilních stránek jsou AMP (Accelerated Mobile Pages). Ve výsledcích vyhledávání jsou stránky odlišené ikonkou blesku, nacházející se vedle snippetu. Zmíněná AMP technologie je unikátní, protože dokáže načíst stránku za desetiny sekundy. [32]

Pro mobile friendly weby je vhodné dodržet několik základních kroků:

- konfigurace view portu v hlavičce kódu (meta tag s atributy name="viewport" a content="width-device-width"),
- odpovídající velikost písma, aby byl obsah dobře čitelný,
- dotykové a klikací prvky v dostatečné vzdálenosti od sebe – jedná se o častou chybu, na kterou upozorňuje Google Search Console,
- omezení výskytu vyskakovacích oken. [32]

2.2.1.5 Strukturovaná data

Strukturovaná data patří mezi rozšířené výsledky vyhledávání. Jedná se o informace uložené ve zdrojovém kódu webu. Vyhledávače jim rozumí a snadněji tak identifikují, co se na stránce nachází. Strukturovaná data se promítají do výsledků vyhledávání tak, že rozšiřují snippety o informace navíc. Ty mohou snáze zaujmout uživatele a zvyšovat tak pravděpodobnost prokliku.

Existuje několik způsobů, kterými strukturovaná data do kódu implementovat. Všechny vycházejí ze standardu schema.org. Mezi typy řešení patří:

- Kód ve formátu **JSON-LD**,
- **Mikrodata** v HTML kódu,

- Formát **RDF-a**, nacházející se také přímo v kódu,
- Posledním řešením je **manuální označení** pomocí zvýrazňovače dat v Google Search Console. [32]

2.2.2 Titulky, meta popisky a nadpisy h1

Velmi důležitou součástí, na kterou se při optimalizaci zapomíná, jsou titulky a popisky webu. Titulky se vkládají do párového tagu <title></title> a jsou obsaženy v hlavičce webu. Zobrazují se tučně ve snippetech. Popisky se vkládají také do hlavičky a do tagu <meta> s atributem description. Vkládá se do něj specifikace obsahu webové stránky. To stejné platí i pro titulek. Požadovaná délka titulku je cca 70 znaků a délka popisku cca 160.

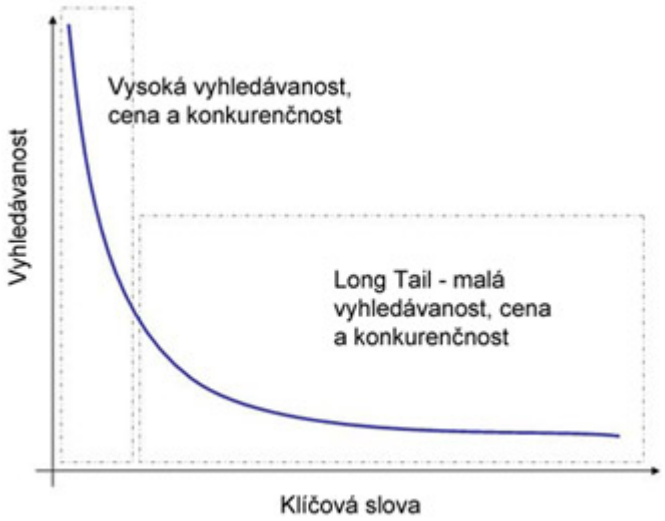
Jasně strukturované by měly být i jednotlivé nadpisy. Uvádí se, že každá stránka by měla obsahovat nadpis úrovně h1, který pomůže nejen uživatelům, ale i robotům při orientaci na webu.

2.2.3 Klíčová slova

Analýza klíčových slov je základem online propagace na internetu. Pro PPC i SEO je důležité si v úvodu stanovit cílovou skupinu a klíčová slova, na která chtějí být na internetu nalezitelná. Tato slova se v pay-per-click kampaních používají pro cílení a v optimalizaci pro vyhledávače při tvorbě obsahu na webu.

Klíčová slova se dají získat různými způsoby. Jedním z nich je samotná webová stránka a texty na ní obsažené, následují brandové výrazy, do kterých se řadí název firmy, a podnikatelský záměr. Existuje také software pro návrh klíčových slov. Přímo zabudovaný ho mají PPC systémy Skliku a Google Ads. Oba fungují na podobném principu, kdy po zadání určitého výrazu ho systém zobrazí včetně statistik hledanosti a míry konkurence, která značí, jak často ho inzerenti používají při propagaci. Návrh klíčových slov lze vytvořit také v softwaru Collabim, který nabízí možnosti získání slov, kdy se strojově procházejí texty webové stránky a na základě četnosti jejich výskytu se vytvoří seznam možných klíčových slov.

Long tail je specifický výraz pro klíčové slovo, které je velmi konkrétní. Mezi jeho vlastnosti patří sice nízká hledanost, ale vysoká relevance. Během analýzy klíčových slov se seřazují slova dle hledanosti, long taily se nacházejí na seznamu nízko, protože nejvíce vyhledávaná jsou obecná slova. Každopádně v případě, že je web optimalizován na vysoce relevantní výrazy, je větší pravděpodobnost, že uživatelé nakoupí. [33, 34]



Obrázek 4 - Long Tail [35]

2.2.4 Budování obsahu

Ve světě online marketingu se říká: „Content is king!“ Vlivem vysokého počtu informací, které se na internetu dají nalézt, je cílem tvořit kvalitní obsah na webové stránce. Ten se může definovat jako informace, která bude pro uživatele hodnotná a určitým způsobem jim něco přinese. Tím pádem se ze stránky stane důvěryhodný zdroj, na který se uživatelé rádi vracejí. Příkladem může být distributor mobilních zařízení. Na webové stránce bude mít sekci blog, ve které bude pravidelně přispívat články o nejnovějších mobilních aplikacích, rady a tipy pro údržbu zařízení nebo informace a recenze nových produktů přicházejících na trh.

2.3 Off-page faktory

Off-page faktory jsou narozdíl od výše popisovaných on-page faktorů hůře ovlivnitelné, a proto se jim přikládá vyšší váha. Důvodem je, že se nenacházejí na dané webové stránce. Mezi nejvýraznějšími off-page faktory jsou zpětné odkazy. V optimalizaci pro vyhledávače je hodnocená nejen jejich kvalita, ale také kvantita. Kvalita se určuje na základě toho, z jakého webu odkazují a co je textem samotného odkazu. Disciplína zabývající se budováním zpětných odkazů se nazývá linkbuilding. [36]

2.3.1 Zpětné odkazy

Zpětnými odkazy rozumíme hypertextové odkazy, které míří na web z jiné stránky. Platí, že vyšší množství odkazujících webů znamená lepší hodnocení. Neznamená to však, že se

vyhledávače spokojí pouze s kvantitou. Kvalita odkazů je velmi důležitá. Kritérii pro určení kvality zpětných odkazů jsou:

- Anchor text – část odkazu, na kterou lze kliknout
- Tématický soulad webů
- Důvěryhodnost webu
- Stáří odkazu
- Umístění odkazu na stránce

Kromě zmíněných bodů si vyhledávače všímají, jak často je web diskutován a zmiňován na sociálních sítích (Facebook, Twitter, apod.) Na základě četnosti je webům přidáváno hodnocení. [37]

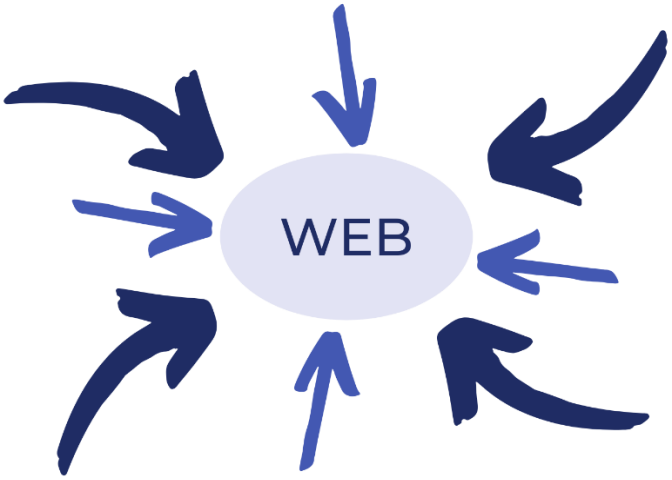
2.3.2 Linkbuilding

Linkbuilding je činnost delšího trvání, která má za cíl budování základny odkazů směřující na web za účelem zvyšování důvěryhodnosti. Do českého jazyka se překládá jako budování zpětných odkazů. U konkrétních odkazů záleží na tom, z jakého jsou zdroje, kam směřují a jaký je jejich text. [34]

V rámci linkbuildingu se rozlišují tři typy odkazů:

- Interní
- Odchozí
- Externí

Interní odkazy se nacházejí napříč jedním webem a směřují na jinou část webu nebo na publikovaný článek. Důležité je, aby textem odkazu byla relevantní informace. Ideální je v odkazech uvádět tu informaci, na kterou je odkazováno. Odchozí odkazy směřují z webu na jiný a externí odkazy naopak. [38]



Obrázek 5 - Zpětné odkazy mířící na webovou stránku [vlastní tvorba]

2.4 Webové vyhledávače

Webové vyhledávače vznikly za účelem třídění dat. Vlivem zvyšujícího se množství informací, které se na internetu nacházejí, byla potřeba umět v nich rychle vyhledávat. První použitý webový vyhledávač se jmenoval Archie a byl vytvořen v roce 1990. Sloužil k prohledávání FTP serverů. [39]

V současnosti existuje řada webových vyhledávačů. Mezi nejznámější vyhledávače v České republice patří Seznam.cz, Google, Bing a Yahoo.

2.4.1 Google

Vyhledávač od Googlu je v současnosti nejpoužívanějším vyhledávačem na světě. Vlastní ho stejnojmenná firma. Navržen byl v roce 1998 studenty Sergeyem Brinem a Larrym Pagem, kteří ho v rámci výzkumu na univerzitě vyvinuli pro ověření svého algoritmu, který hodnotil webové stránky na základě PageRanku. PageRank je číslo, které označuje hodnocení každé url. V praxi jej lze považovat za ukazatele důvěryhodnosti stránky. V době, kdy byl algoritmus navržen jeho úroveň výrazně převyšovala kvalitu tehdejších vyhledávačů, a proto se Google stal prioritním vyhledávačem. Od té doby se zdokonaluje a je neustále vyvíjen a vylepšován. Aktuálně je Google komerčním produktem, a proto je o jeho architektuře zveřejněno velmi málo informací. Vyhledávač je však rozdělen do několika datacenter, která jsou rozmístěna po celém světě a běží na vysoce výkonných počítačích. V současnosti je Google gigantem na trhu, který dělá vše dle vlastních pravidel. Počet zaměstnanců se blíží číslu sto tisíc. [40, 41]

2.4.2 Seznam

Seznam byl prvním českým internetovým vyhledávačem, který založil Ivo Lukačovič v roce 1996. Původně sloužil jako jednoduchý katalog, doplněný o další služby. O rok později od založení se z něj stal fulltextový vyhledávač, který svého času předčil i monopol mezi vyhledávači – Google. Kromě webového vyhledávače je součástí Seznamu také zbožový vyhledávač Zboží.cz. Hodnotící ukazatel webových stránek se jmenuje S-Rank a svým způsobem se jedná o podobnou hodnotu jako Page Rank u Google. Hodnota se pohybuje mezi 1-10, každopádně mechanismus S-Ranku je neveřejný. Indexace na Seznamu je pomalejší než na Google. V případě zveřejnění nové stránky nebo webu je možné, že nebude zaindexován okamžitě. Pro tyto situace existuje nástroj „Přidání nového odkazu“, s jehož pomocí lze požádat vyhledávač, aby zadanou stránku prošel. [42]

2.4.2.1 Google vs. seznam

Vyhledávač od Seznamu je v České republice velkým konkurentem Googlu. Od roku 2014 vypracovává agentura eVisions průzkum zastoupení jednotlivých vyhledávačů v rámci přivádění návštěvnosti. Údaje získávají na základě dat z účtů necelých sto klientů. V roce 2014 byl podíl organické návštěvnosti v poměru 43 % ku 53 % s vedením Seznamu. Na konci roku 2018 se poměr výrazně změnil ve prospěch Googlu a výsledky ukázaly 75 % ku 25 %. Nutno zmínit, že z celkového počtu návštěvnosti přivedly Google se Seznamem dohromady 96 % lidí. Zbylá procenta si rozdělily vyhledávače Bing, Yahoo a Yandex. Zajímavostí jsou statistiky z jednotlivých zařízení. Například na desktopech v roce 2014 v době průzkumu byla ze Seznamu návštěvnost 54 % a Google 46 %, avšak v druhé polovině roku Google Seznam předehnal. Při aktuálním měření v roce 2019 je Google stále majoritní a zabírá 70 %. Největší rozdíly ve vyhledávačích jsou patrné na mobilních zařízeních, kdy měl Google navrch již v roce 2014 s 56 % návštěvnosti. Při nejnovějším průzkumu je na mobilech v Google vyhledáváno v 81 % případů a v 19 % na Seznamu. [43]

Na základě výzkumu je patrné, že Seznam ztrácí na síle a uživatelé se z velké části přesouvají na Google. Důvodem může být množství služeb, které Google nabízí zadarmo, jeho výskyt v Android zařízeních nebo například poskytování vlastní aplikace prohlížeče, ve které je vyhledávač domovskou stránkou. [43]

Zajímavostí je, že existují pouze čtyři země na světě, které mají silného konkurenta Googlu. Kromě ČR, kde se Seznam drží na 30 %, se jedná o Čínu, Japonsko a Rusko. [44]

2.4.3 Ostatní vyhledávače

Podíl dalších vyhledávačů v rámci návštěvnosti je velmi nízký. Průzkumy ukázaly, že jejich podíl je okolo 4 %. [45]

Jedním ze známých vyhledávačů je Bing od společnosti Microsoft. Spuštěn byl v roce 2009 a nahradil tehdejší produkt Live.com. V současnosti je Bing nejčastěji využíván ve firmách, kde je používán software společnosti Microsoft, protože je nainstalován jako výchozí vyhledávač. [46]

Dalším významným vyhledávačem je Yahoo. Ačkoliv původně pochází z Ameriky, nejvíce se zaběhl v Japonsku, kde s 30 % návštěvnosti konkuruje Googlu. [44]

V Číně je Google zakázaný, a proto je zde minoritní vyhledávač Baidu. Z něj proudí 80 % návštěvnosti a o zbylá procenta se dělí Haosa, Shenma a Soga. Zajímavostí je, že český Seznam v Číně zablokovaný není. [44]

Ruský Yandex vznikl již v roce 1990 a stále si před Googlem udržuje náskok. Důvodem je podpora rozdílné abecedy. V současnosti je Yandex rozšířený kromě Ruska také v Bělorusku, Kazachstánu, Kyrgyzstánu a v pár procentech i v Turecku. [44]

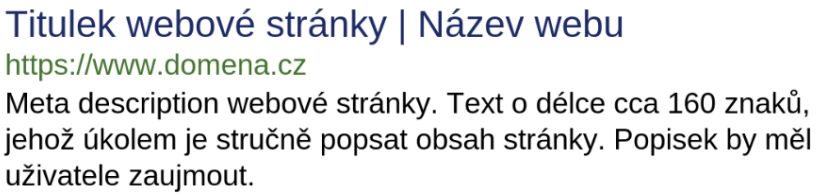
2.5 Hodnotící faktory pro pořadí zobrazení ve výsledcích vyhledávání

Webové vyhledávače hodnotí stránky na základě spousty kritérií. Samotné společnosti nemají přímo specifikované veškeré podmínky pro dobré umístění webové stránky. Na základě zkušeností si však specialisté předávají informace o úpravách, které fungovaly pro zlepšení umístění ve výsledcích vyhledávání a zvýšení organické návštěvnosti.

V rámci technického SEO jsou výraznými hodnotícími faktory již výše zmíněné zabezpečení webu a rychlost načítání stránky. Vyhledávače vždy upřednostňují bezpečnost a pohodlí uživatelů. Další z technických faktorů je responzivní design webu. Vzhledem ke zvyšujícímu se trendu mobilních zařízení jsou upřednostňovány stránky, které jsou optimalizované pro mobilní zařízení pomocí responzivního designu nebo stránky AMP (Accelerated Mobile Pages).

Autorita stránky a domény jsou známými kritérii pro dobré umístění. Důležité je proto tvořit kvalitní základnu příchozích i odchozích odkazů. Kromě autority je také hodnoceno samotné stáří webové stránky. Mladý web má nižší šanci zobrazit se na vyšších příčkách než starší web. Závisí samozřejmě také na relevanci a kvalitě obsahu. [47]

Mezi méně známé hodnotící faktory patří dwell time. Jedná se o čas, který uživatel stráví na stránce před tím, než se vrátí zpět do výsledků vyhledávání. S tím, kolik času uživatelé webu věnují, souvisí kvalita obsahu a relevantnost k vyhledávacímu výrazu. Z toho důvodu je nutné tvořit kvalitní obsah, který bude mít pro uživatele skutečnou hodnotu. K vyhledávacím dotazům musí být relevantní klíčová slova použitá v titulcích a popiscích stránek. Se zvyšujícím se procentem prokliků na stránky skrz výsledky vyhledávání se také zvyšuje hodnocení webové stránky očima vyhledávačů. [48]



Obrázek 6 - Příklad snippetu ve výsledcích vyhledávání

3 NÁSTROJE PRO SEO A TESTOVÁNÍ BEZPEČNOSTI

Výsledky optimalizace pro vyhledávače a správného zabezpečení webových stránek lze získávat pomocí různých nástrojů. Některé nástroje jsou online a jejich použití je značně jednoduché, jiné programy je potřeba instalovat a případně zakupovat licence.

3.1 Nástroje pro testování bezpečnosti

Nástroje pro testování bezpečnosti webové stránky zkontrolují správnost nasazení SSL certifikátů. Nejznámějším a nejpoužívanějším nástrojem v praxi je zahraniční online nástroj Qualys. Z českých nástrojů se používá SSL tester.

3.1.1 Qualys

Nástroj Qualys se zabývá hlubší analýzou SSL serveru a hodnotí pomocí písmen od A do F. Existuje také hodnocení písmenem T, které je přiřazeno stránce bez SSL certifikátu. Hodnocení je komplexnější a odvíjí se od několika různých faktorů. Stránky získávají číselné skóre, na jehož základě je přiřazováno hodnocení dle tabulky.

Tabulka 1 - Kritéria pro hodnocení dle nástroje Qualys [49]

Hodnocení	Známka
≥ 80	A
≥ 65	B
≥ 50	C
≥ 35	D
≥ 20	E
< 20	F

Písemné ohodnocení je základním vypovídajícím ukazatelem kvality SSL certifikátu. Rozbor je však důkladnější a zaměřuje se na tři základní kritéria. Jsou jimi podpora protokolu, výměna klíčů a síla šifrování. Síla šifrování představuje 40 % z hodnocení a další dvě kritéria 30 %.

Na podpoře protokolu závisí procentuální ohodnocení. Různým verzím jsou přiřazena jiná procenta. Důvodem jsou bezpečnostní mezery starších protokolů.

Tabulka 2 - Hodnocení podpory protokolu [49]

Verze protokolu	Skóre
SSL 2.0	0 %
SSL 3.0	80 %
TLS 1.0	90 %
TLS 1.1	95 %
TLS 1.2	100 %

Výměna klíčů se provádí pomocí Diffieho-Hellmanova kryptografického protokolu, který vytváří šifrované spojení mezi účastníky komunikace. Její hodnocení je opět vyjádřeno v procentech. Důležité je tedy používat silné klíče například 2048 bitové. [50]

Tabulka 3 - Hodnocení výměny klíčů [49]

Výměna klíčů	Skóre
Slabý klíč	0 %
Výměna klíče bez ověření	0 %
Klíč <512 bitů	20 %
Klíč <1024 bitů	40 %
Klíč <2048 bitů	80 %
Klíč <4096 bitů	90 %
Klíč ≥4096 bitů	100 %

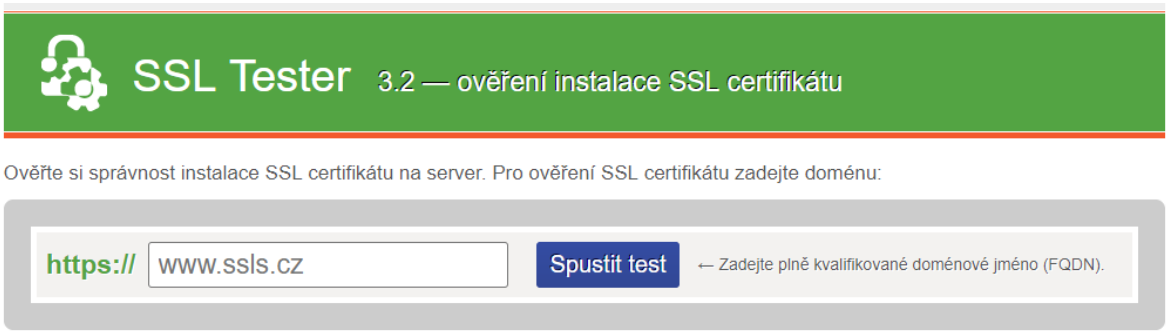
Posledním ze tří hlavních kritérií je síla šifry. Jelikož útočníci mohou využít symetrických šifer pro narušení komunikace, je použití slabých šifer penalizováno. Síla šifrování se vyjadřuje v bitech a vypočítá se součtem nejsilnější a nejslabší šifry vyděleným 2.

Tabulka 4 - Hodnocení síly šifrování [49]

Síla šifry	Skóre
0 bitů (bez šifrování)	0 %
< 128 bitů	20 %
< 256 bitů	80 %
≥ 256 bitů	100 %

3.1.2 SSL Tester

Český nástroj SSL Tester se využívá k ověření správnosti instalace SSL certifikátů. Poskytován je na webu ssls.cz společnosti Alpiro s.r.o. Dokáže detekovat podporované verze certifikátů, ověřuje správnost samotné instalace SSL a zahrnuje také kontrolu důvěryhodnosti certifikační autority. Mezi hlavní výhody patří detekce zranitelností PoodleBleed, Crime, Drown apod. Výstupem nástroje je shrnutí a případné návrhy na vylepšení. [51]



Obrázek 7 - SSL Tester

3.1.3 Security Headers

Bezpečnostní hlavičky specifikují pravidla v rámci komunikace serveru s prohlížečem. Mezi jejich funkce patří povolení nebo úplné zakázání některých funkcí, které by mohly ohrozit bezpečnost uživatelů webových stránek. [52]

- **HTST** – zajišťuje komunikace pouze na HTTPS protokolu, funguje jako prevence proti man-in-the-middle typu útoku [52]
- **CSP** – informuje o povolených zdrojích, které se mohou načítat, lze povolit či zakázat jednotlivé typy souborů [52]
- **X-Frame Options** – předchází zneužití obsahu útočníkem omezením zobrazení webové stránky pouze na konkrétní doménu [52]
- **X-XSS Protection** – hlavička umožňuje nastavení XSS filtru, který se nachází v prohlížeči a díky němu pomáhá předcházet cross-site-scripting útokům [52]
- **X-Content-Type-Options** – ověřuje, zda je nastavení formátů zdrojových souborů správné [52]
- **Referrer-Policy** – pomáhá chránit uživatele před zjištěním identity při sdílení odkazu nebo může omezit sběr analytických dat za účelem zvýšení bezpečnosti uživatelů [52]

- **Feature-Policy** – použitím hlavičky lze povolit či zakázat určité funkce prohlížeče, v současnosti není podporovaná všemi prohlížeči [52]

Přítomnost bezpečnostních hlaviček a jejich nastavení lze analyzovat pomocí nástroje securityheaders.com, který hodnotí web na škále od A do F.

3.2 Vyhodnocování optimalizace pro vyhledávače

SEO lze definovat jako dlouhodobý proces vedoucí ke zvýšení organické návštěvnosti webové stránky. Z toho důvodu neexistuje nástroj, který by dokázal ověřit správnost implementovaných kroků instantně. Stejně jako celý průběh optimalizace pro vyhledávače je vhodné monitorovat výsledky dlouhodobě.

3.2.1 Nástroje společnosti Google

Google poskytuje širokou nabídku nástrojů pro tvůrce a správce webových stránek. Nástroje spolu komunikují a lze je vzájemně propojit. Nejvýznamnějším z nich je Google Analytics, který se zaměřuje na sledování návštěvnosti stránek. Jeho obsahem jsou data o návštěvnících webu a pro SEO má význam ve sledování organické návštěvnosti. Kromě návštěvnosti lze v nástroji pozorovat podrobná data o prodejích, jednotlivých zdrojích návštěvnosti a chování uživatelů.

Vložení nástroje na stránku lze pomocí měřícího kódu, který se vkládá do zdrojového kódu webu přímo do tagu <head></head>.

```
<!-- Global Site Tag (gtag.js) - Google Analytics -->
<script async
src="https://www.googletagmanager.com/gtag/js?id=GA_TRACKING_ID"></script>
<script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
          gtag('js', new Date());
           gtag('config', 'GA_TRACKING_ID');
</script> [https://support.google.com/analytics/answer/1008080]
```

Řetězec GA_TRACKING_ID je nahrazen ID měření, které je vygenerováno po registraci účtu a stránky v Google Analytics.

Nasazení měřícího kódu na web lze ručně přímo ve zdrojovém kódu nebo pomocí nástroje Google Tag Manager, jenž slouží pro správu více měřících kódů. Tag Manager lze na web

implementovat také pomocí pluginu. Při jeho nasazení není nutné více zasahovat do zdrojového kódu, a zároveň mít na webu vyšší počet měřících kódů.

Cílem technického SEO je nastavení webu tak, aby byl dobře indexovatelný a tím pádem nalezitelný ve výsledcích vyhledávání. Indexaci webové stránky je možné kontrolovat pomocí nástroje Google Search Console, který se jinak nazývá Webmasters. Vyhodnotí počet zahrnutých i vyloučených stránek z indexace. Upozorňuje také na chyby a problémy – například na výskyt stránek 404 a duplicit. V přehledu nástroje lze zobrazit vyhledávací dotazy, skrz které se uživatelé proklikli na web.

Službu Webmasters lze s webovou stránkou spárovat několika různými způsoby. První z nich je pomocí Google Analytics, pokud je web již má. Ověřit stránku je možné také vložením HTML značkou s měřícím řetězcem do hlavičky webu, pomocí Google Tag Manageru nebo pluginem ve WordPressu.

3.2.2 Collabim

Český nástroj pro správu a sledování pozic klíčových slov se nazývá Collabim. Využívá se pro měření pozic konkrétních klíčových slov, dokáže monitorovat PPC reklamy a porovnávat pozice konkurentů. Collabim nabízí správu jedné webové stránky zdarma, pro sledování vyššího počtu webů je možné pořídit placené balíčky.

Kromě přehledu klíčových slov obsahuje také možnosti využití jednorázových analýz, které slouží k vytvoření přehledu různých dat. Analyzovat lze jak samotná klíčová slova, tak url adresy a celé weby.

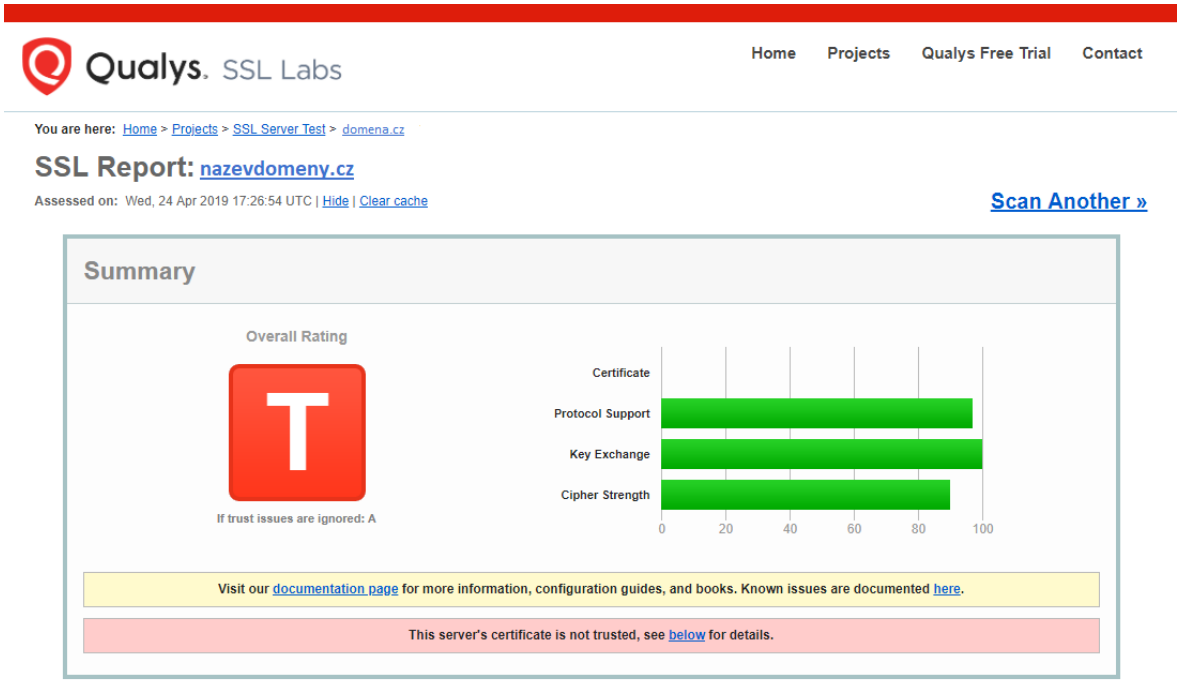
II. PRAKTICKÁ ČÁST

4 ZABEZPEČENÍ WEBOVÉ STRÁNKY

Teoretická část práce obsahuje převedení webové stránky na zabezpečený protokol. Součástí procesu je prvotní analýza nezabezpečené stránky pomocí nástrojů pro testování bezpečnosti. Cílem je převést na zabezpečený protokol pomocí certifikační autority Let's Encrypt a získat nejlepší možné hodnocení v rámci testovacího nástroje Qualys.

4.1 Úvodní analýza webu

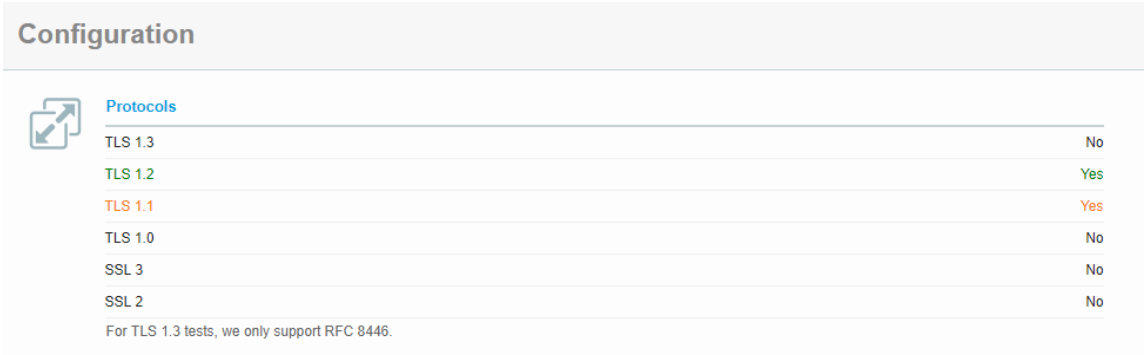
Webová stránka pro účely migrace je postavena na serveru poskytovatele Endora.cz. Využívaným redakčním systémem je WordPress. Stránka je nezabezpečená a komunikace není šifrována. Analýza před převedením je provedena pomocí nástrojů SSL Tester a Qualys.



Obrázek 8 - Úvodní analýza pomocí Qualys

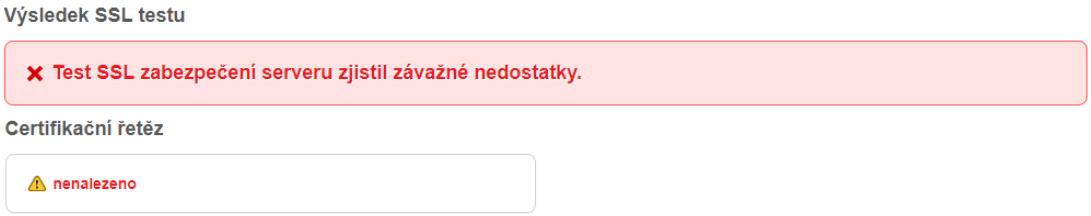
Nástroj Qualys udělil webu nejhorší možnou známku, kterou v hodnocení lze dostat. Výsledek byl očekávaný z důvodu absence zabezpečeného protokolu, kterou znázorňuje chybějící křivka u položky Certificate.

Analýza také ukázala, že mezi podporovanými protokoly se nachází TLS 1.1, která je v současnosti považována za nedůvěryhodnou.



Obrázek 9 - Podporované protokoly

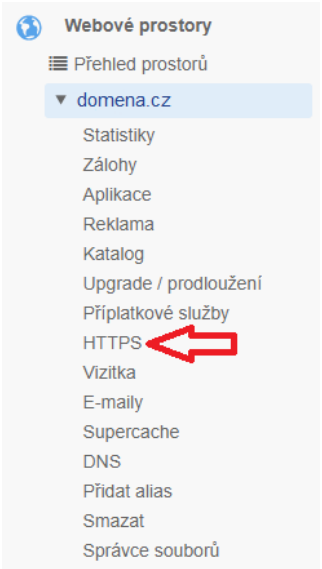
Nástroj SSL Tester také ukázal chybějící certifikát. Objevilo se hlášení, že test SSL zabezpečení serveru zjistil závažné nedostatky. Certifikační řetěz nebyl nalezen.



Obrázek 10 - Výsledek testování pomocí nástroje SSL Tester

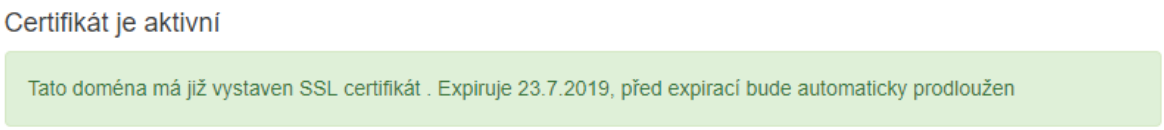
4.2 Migrace na zabezpečený protokol

Poskytovatel serveru nabízí zabezpečený protokol k objednání zdarma. Jedná se o certifikát společnosti Let's Encrypt, jehož doba platnosti je tři měsíce. Služba se po vypršení certifikátu sama aktualizuje.



Obrázek 11 - Objednání certifikátu u poskytovatele domény

Žádost o certifikát je jednoduchý proces. V menu u webového prostoru se vlastník webu proklikne do položky „HTTPS“, kde jediným stisknutím tlačítka o SSL certifikát zažádá. Zobrazí se hlášení, že do třiceti minut bude certifikát vydán. Ve chvíli, kdy je služba aktivní, objeví se informace o vystavení, expiraci a automatickém prodloužení.



Obrázek 12 - Hlášení o aktivním certifikátu

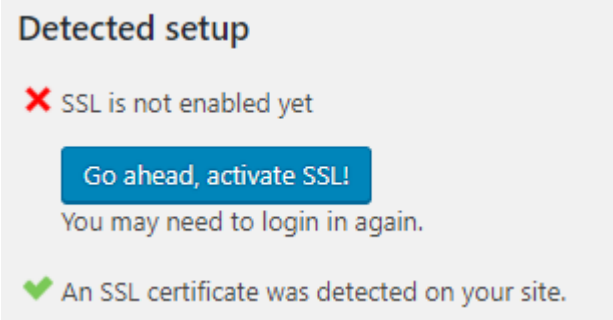
Aktivací certifikátu proces převedení webové stránky nekončí. Důležitou součástí je úprava HTTPS před názvem domény přímo v redakčním systému a přesměrování stránek.

Obrázek 13 - Protokol a doménové jméno před změnou

Zakoupením certifikátu se protokol sám nezmění, a proto je nutné provést úpravy ručně. Změna doménového jména se provádí přímo ve WordPressu v základním nastavení webové stránky. Klíčový je přepis protokolu http na https.

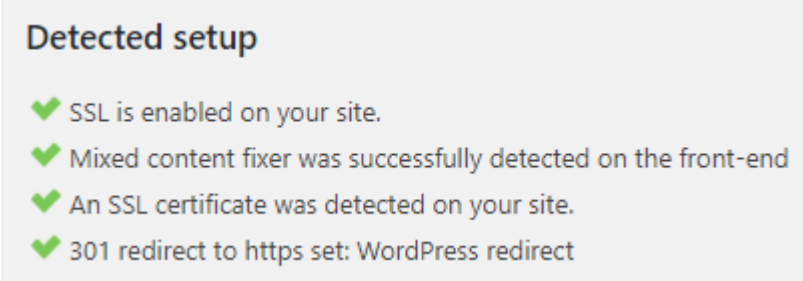
Obrázek 14 - Protokol a doménové jméno po změně

Přesměrování stránek je možné za pomocí nejrůznějších pluginů. Mezi nejznámější pluginy patří Better Search Replace nebo Really Simple SSL. Pluginy zajistí přesměrování stránek na zabezpečený protokol tak, aby se při načítání webové stránky provedlo přesměrování z http na https. Při migraci byl použit protokol Really Simple SSL.



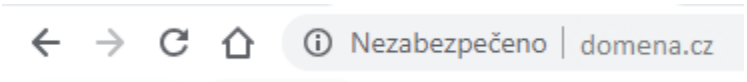
Obrázek 15 - Really Simple SSL před aktivací

Stažení pluginu je možné v redakčním systému v položce „Instalace pluginů“. Vyhledání a stažení pluginu je první část procesu. Druhá část je samotná jeho aktivace.



Obrázek 16 - Really Simple SSL po aktivaci

Po aktivování pluginu jsou přesměrovány stránky pomocí 301 redirect, což je oznámení prohlížečům, že se stránka nachází na jiné adrese. V tomto případě se jedná o přesměrování z konkrétní nezabezpečené stránky na její zabezpečenou verzi.

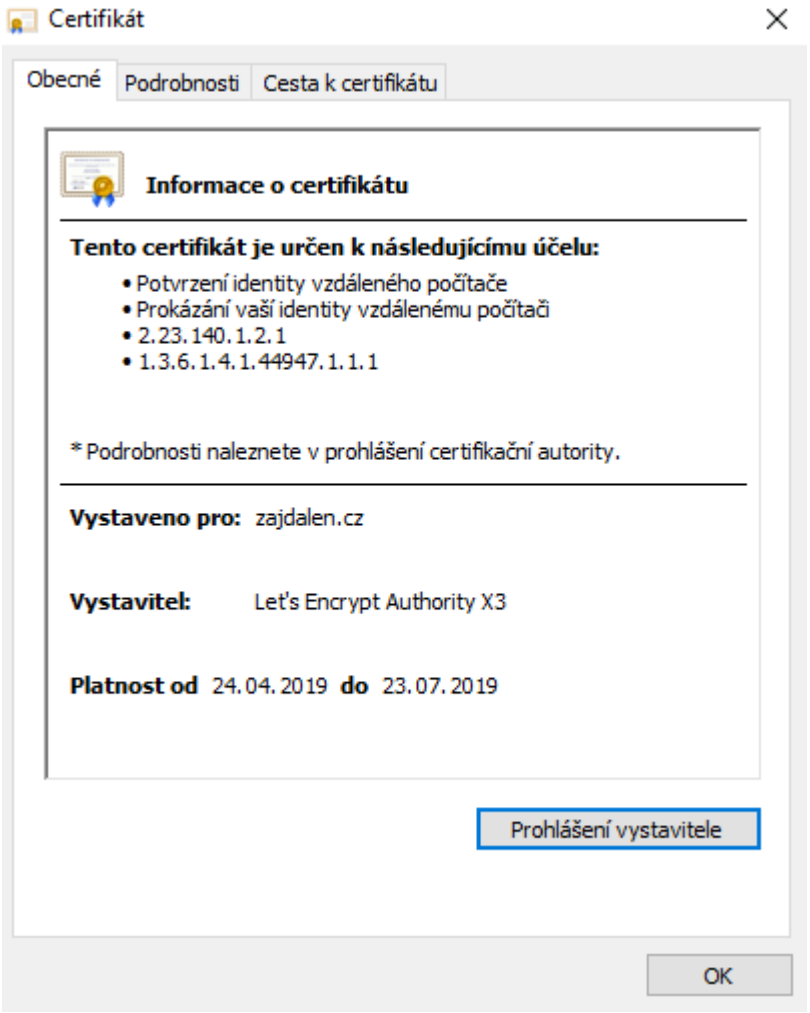


Obrázek 17 - Adresa webu před zabezpečením

Před přepsáním doménového jména a aktivací pluginu obsahovala doména v adresním řádku znak informace v kroužku a hlášku „Nezabezpečeno“.

Obrázek 18 - Adresa webu po zabezpečení

Aktivací přesměrování je nyní doména zabezpečena a v adresním řádku se objevuje protokol https a symbol zámku, značící přítomnost bezpečnostního certifikátu. Jeho rozklikutím se zobrazí informace o certifikátu, souborech cookies a nastavení webu. Informace o certifikátu jsou veřejně dostupné a lze si je kliknutím na certifikát zobrazit. V obecných informacích je možné zjistit účel certifikátu, jeho platnost, certifikační autoritu a prohlášení vystavitele. V podrobnostech se nachází verze, sériové číslo, algoritmus podpisu či kryptografický otisk.

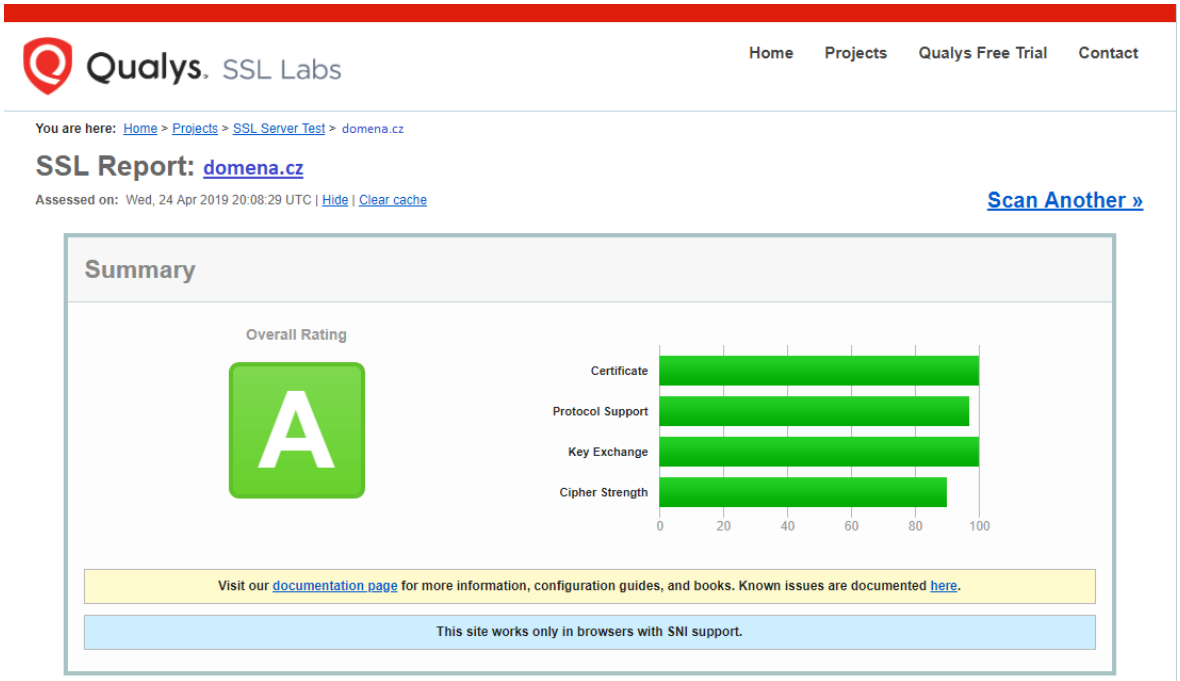


Obrázek 19 - Informace o certifikátu

4.3 Analýza webové stránky po migraci

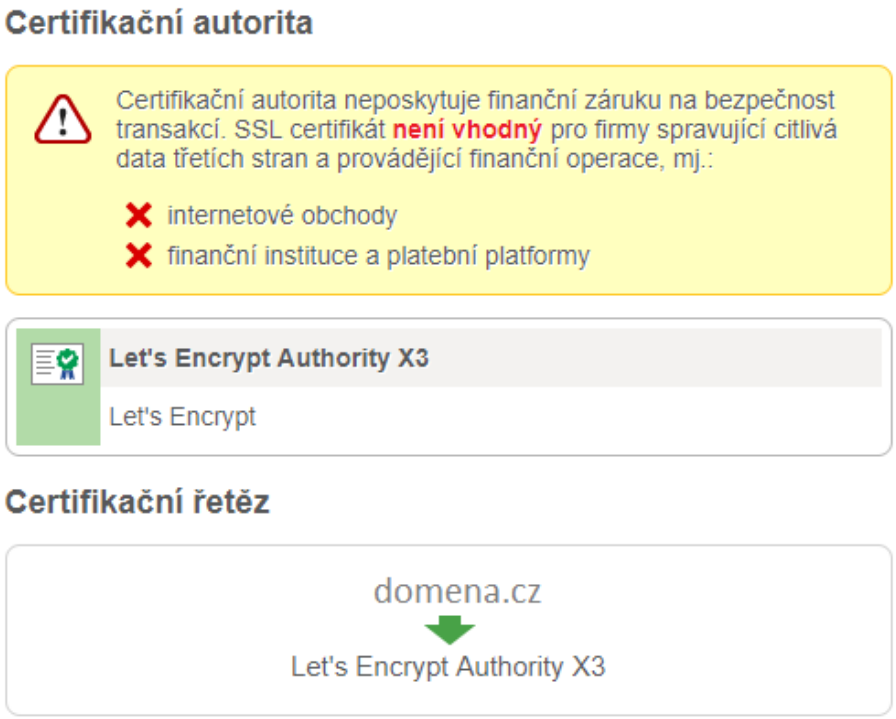
Převedení stránky proběhlo kompletně se všemi kroky, které byly potřeba. Součástí migrace je otestování správnosti instalace SSL certifikátu. Použity jsou stejné nástroje, kterými byla stránka analyzována v úvodní fázi.

Výsledky pomocí Qualys ukázaly nejlepší možnou známku A. Křivka znázorňující přítomnost certifikátu je na nejvyšší možné úrovni. Drobné nedostatky jsou stále k nalezení v podpoře protokolu TLS 1.1 a v síle šifrování.



Obrázek 20 - Analýza po zabezpečení pomocí Qualys

Testování pomocí SSL Testeru dopadlo také úspěšněji než v první fázi. Nástroj rozpoznal přítomnost certifikátu a výstupem byly informace o certifikační autoritě, podporovaných protokolech a zranitelnostech. Nástroj upozornil, že certifikát od Let's Encrypt není vhodný pro internetové obchody a finanční instituce, protože neposkytuje finanční záruku na bezpečnost transakcí.



Obrázek 21 - Analýza po zabezpečení pomocí SSL Testeru

Výstupem obou testů byl seznam zranitelností, jež by mohly být v rámci bezpečnosti webových stránek uplatněny a zhodnocení, zda je testovaný web náchylný k uplatnění hrozeb z nich vycházejících.

BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)

Obrázek 22 - Zranitelnosti a jejch možné uplatnění dle Qualys

Podle nástroje Qualys je web chráněn proti nejčastějším hrozbám, stejně tak, jako podle nástroje SSL Tester.

Zranitelnosti

PoodleBleed (CVE-2014-3566)	OK
HeartBleed (CVE-2014-0160)	OK
CRIME (CVE-2012-4929)	OK
DROWN (CVE-2016-0800)	OK
Podpora RC4	✔ ne
Secure renegotiation	✔ ano
Smíšený obsah (http & https)	✔ ne
Malware nebo podezřelý kód	OK

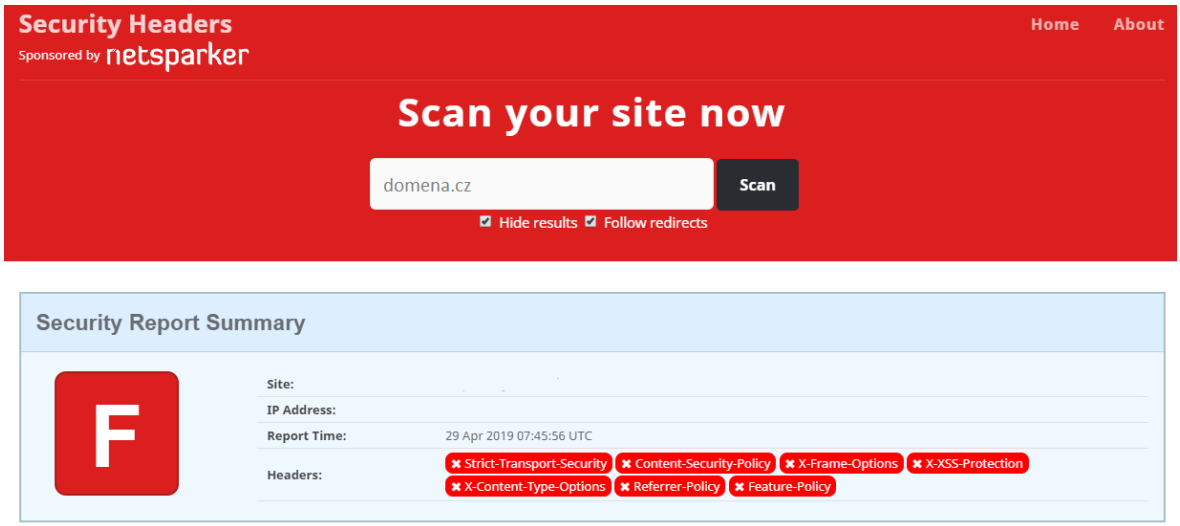
Obrázek 23 - Zranitelnosti a jejich možné uplatnění dle SSL Testeru

Závěrečná analýza webu ukázala, že protokol od společnosti Let's Encrypt je dostačující a zabezpečení webu funkční. Pouze v případě, že by se web zabýval prodejem či chtěl získat vyšší důvěryhodnost, byla by požadována placená autorita.

4.4 Nastavení Security Headers

Součástí zabezpečení webových stránek je nastavení bezpečnostních hlaviček – tzv. Security Headers. V rámci vylepšení zabezpečení webových stránek byly přidány hlavičky do kódu webové stránky. Úpravy je možné provést v ftp souborech webu v položce functions.php. Pro kódování konfiguračních souborů webových stránek na WordPressu je využíván programovací jazyk php.

V úvodu proběhla analýza webu pomocí online nástroje Securityheaders.com, jehož hodnocení bylo F.



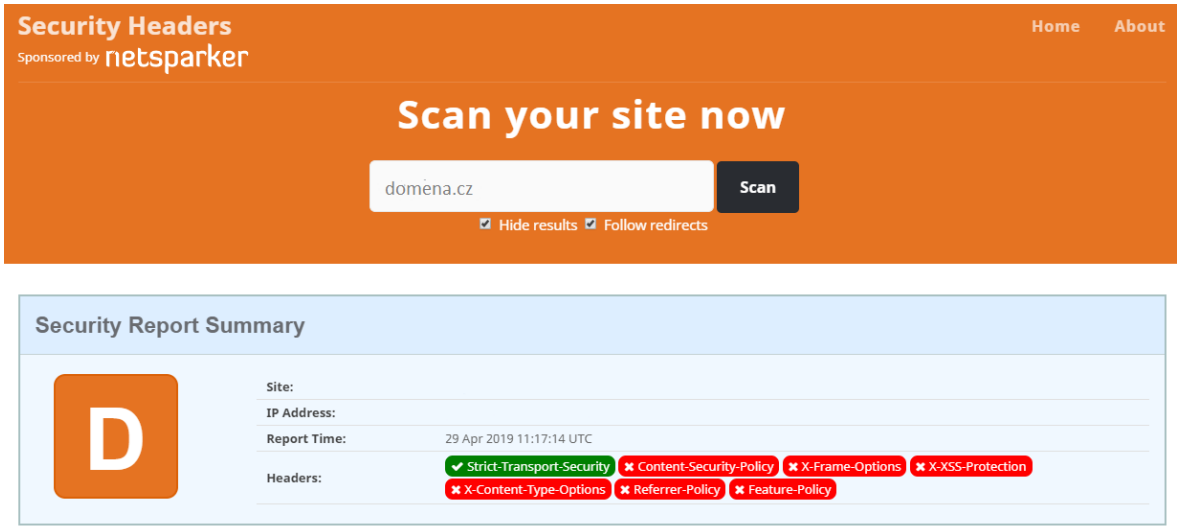
Obrázek 24 - Úvodní analýza webové stránky

První implementovanou hlavičkou byla HSTS, jejíž parametrem max-age je počet sekund, v jejichž průběhu má prohlížeč komunikovat pouze přes zabezpečený protokol.

```
header( 'Strict-Transport-Security: max-age=10886400' );
```

Obrázek 25 - Kód HSTS hlavičky

Analýza stránky po vložení první hlavičky ukázala zlepšení o jeden stupeň na D a upravená hlavička byla zvýrazněna zelenou barvou.



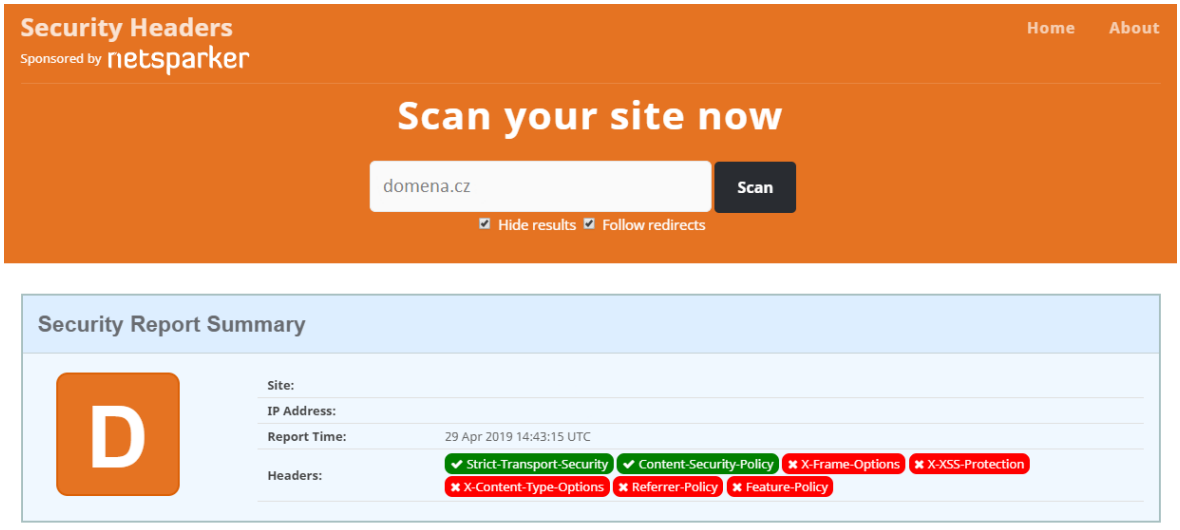
Obrázek 26 - Analýza po vložení hlavičky HSTS

Druhou vloženou hlavičkou byla CSP, která nastavuje práva jednotlivým typům souborů. Do konfiguračního souboru byl vložen kód s parametry self povolující soubory z vlastní domény a soubory šifrované pomocí sha256.

```
header("Content-Security-Policy: script-src 'self' 'sha256-".base64_encode(hash('sha256', 'alert("allowed");', true))."'");
```

Obrázek 27 - Kód pro vložení CSP hlavičky

Potvrzením úprav a následnou analýzou v nástroji Security Headers byla známka stránky stále D, každopádně report zvýraznil hlavičku CSP zeleně.



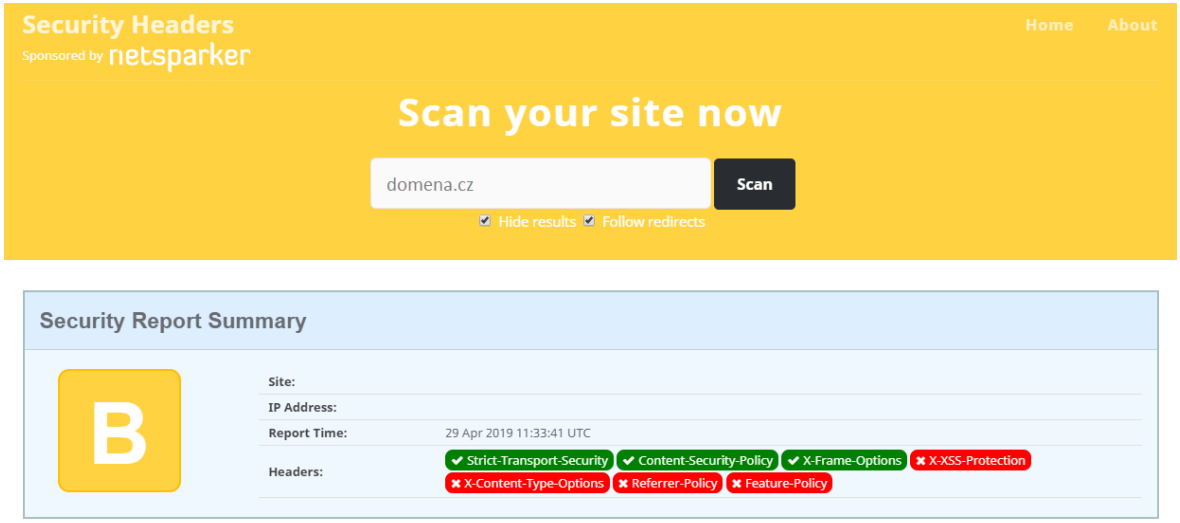
Obrázek 28 - Výsledky analýzy po konfiguraci hlavičky CSP

Třetí nastavenou bezpečnostní hlavičkou je X-Frame-Options, jejímž úkolem je omezení načítání webové stránky pouze na rám na vlastním webu.

```
header('X-Frame-Options: SAMEORIGIN');
```

Obrázek 29 - Kód pro konfiguraci X-Frame-Options hlavičky

Nastavením X-Frame-Options se změnilo hodnocení až na známku B a hlavička byla označena zeleně.



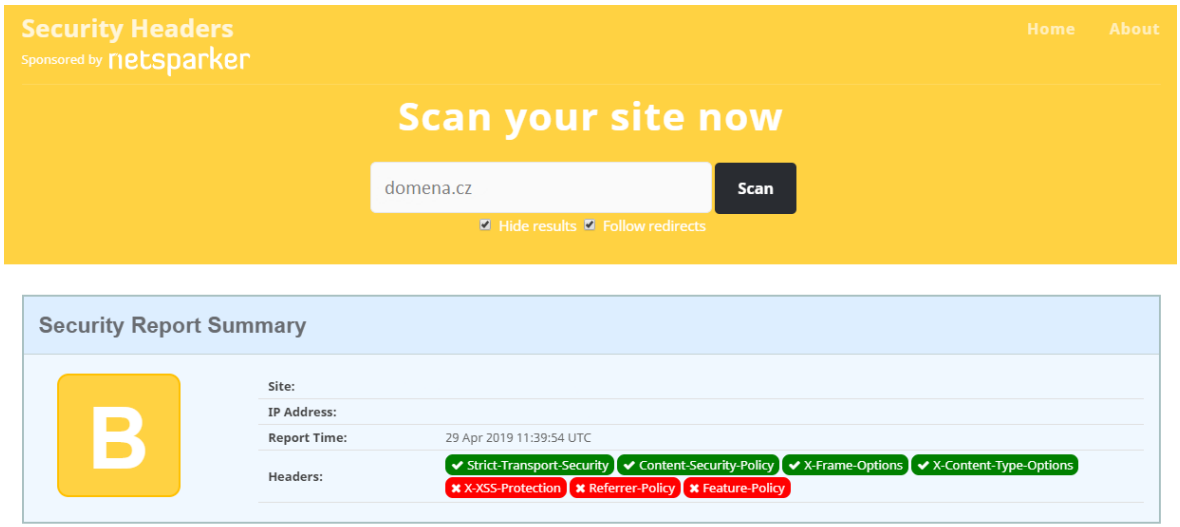
Obrázek 30 - Výsledky analýzy po konfiguraci hlavičky X-Frame-Options

Následující ze Security Headers je X-Content-Type-Options. Hlavička slouží jako ochrana proti XSS a funguje tak, že ověřuje správnost typu souboru .css.

```
header("X-Content-Type-Options: nosniff");
```

Obrázek 31 - Kód pro konfiguraci X-Content-Type hlavičky

Po implementaci se hodnocení webové stránky nezměnilo a stále odpovídalo hodnocení B.



Obrázek 32 - Výsledky analýzy po konfiguraci hlavičky X-Content-Type

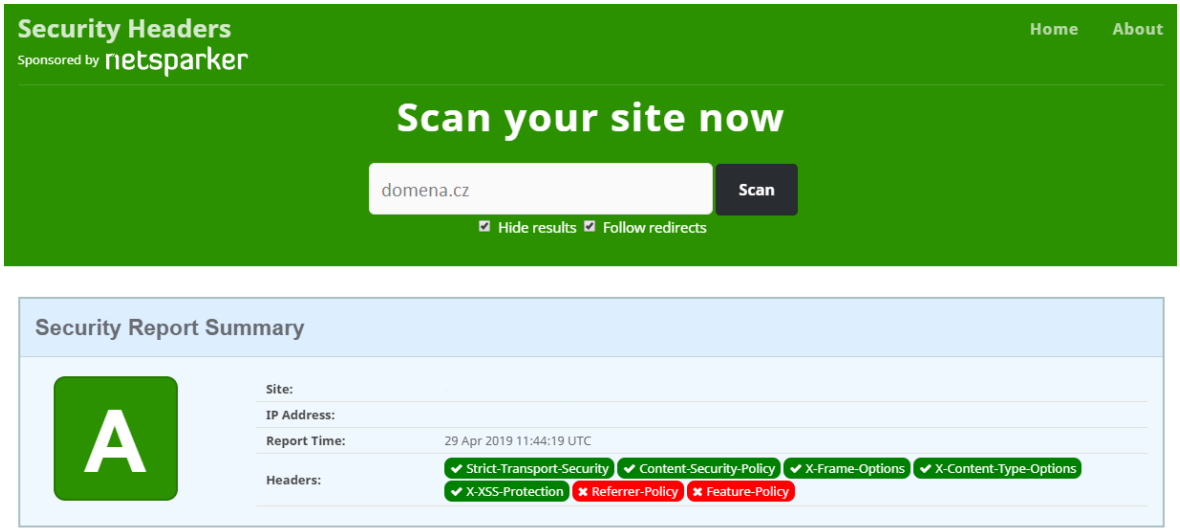
Pátou bezpečnostní hlavičkou je X-XSS-Protection, jejíž název napovídá, že opět chrání proti XSS. Stačí mít v konfiguračních souborech nastavený následující kód.

```
header('X-XSS-Protection: 1; mode=block');
```

Obrázek 33 - Kód pro konfiguraci X-XSS-Protection hlavičky

XSS filtr se v některých prohlížečích nachází defaultně, ale je možné, že byl uživatelem vypnut. Díky nastavení hlavičky se před načtením webové stránky zkontrolují CSS soubory a v případě detekování útoku zamezí prohlížeč její načtení.

Nastavením X-XSS-Protection hlavičky se hodnocení webové stránky v Security Headers změnilo na známku A.



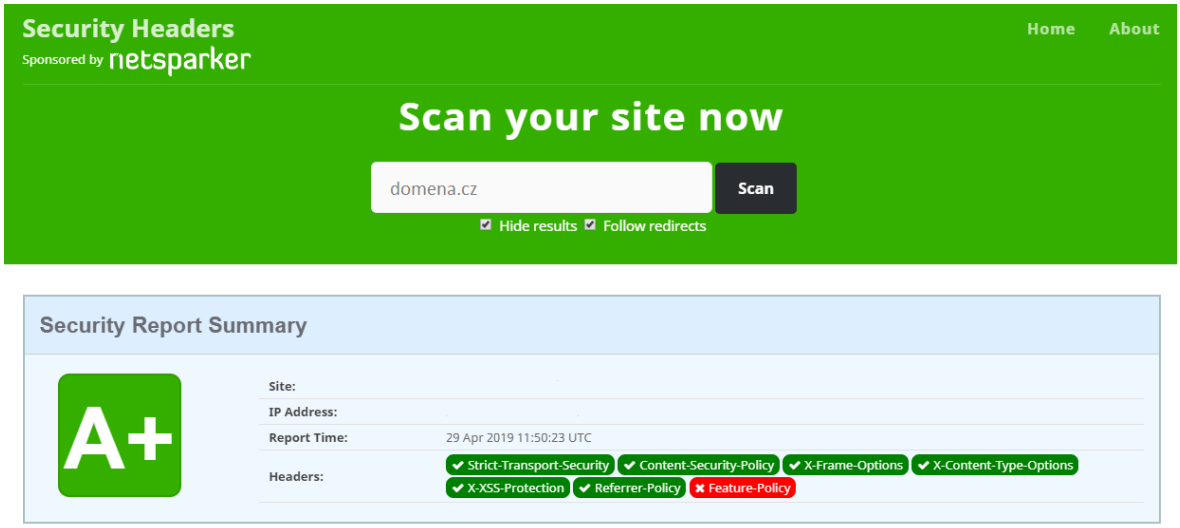
Obrázek 34 - Výsledky analýzy po konfiguraci hlavičky X-XSS-Protection

Následující hlavičkou je Referrer-Policy, která má za úkol chránit uživatele omezením sběru analytických dat.

```
header('Referrer-Policy: no-referrer');
```

Obrázek 35 - Kód pro konfiguraci Referrer-Policy hlavičky

Jejím nastavením se hodnocení webové stránky posunulo z A na známku A+, která je v rámci analýzy Security Headers nejvyšší. Nástroj označil nastavené hlavičky zeleně a zbývající jedna je stále červeně.



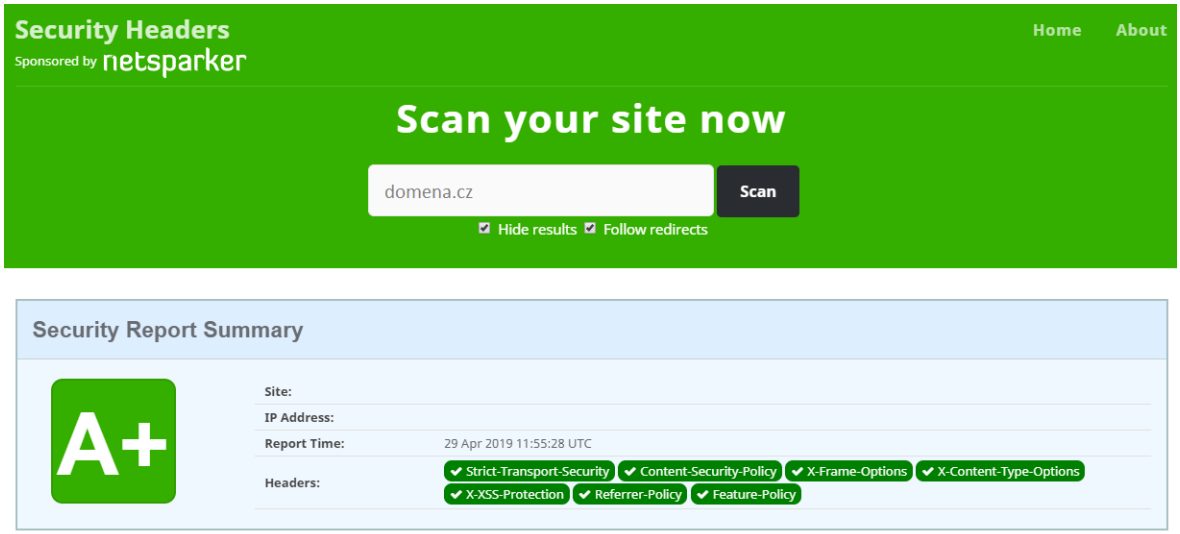
Obrázek 36 - Výsledky analýzy po konfiguraci hlavičky Referrer-Policy

Pro dokonalé hodnocení je požadováno nastavit také Feature-Policy hlavičku, která povoluje nebo zakazuje přístup k určitým aplikacím.

```
header('Feature-Policy: geolocation none;midi none;notifications none;push none;sync-xhr none;
microphone none;camera none;magnetometer none;gyroscope none;speaker self;vibrate none;fullscreen self;payment none;');
```

Obrázek 37 - Kód pro konfiguraci Feature-Policy hlavičky

Implementací hlavičky se hodnocení A+ zachovalo a všechny bezpečnostní hlavičky byly označeny zelenou barvou.



Obrázek 38 - Výsledky analýzy po konfiguraci hlavičky Feature-Policy

Nastavení bezpečnostních hlaviček je důležité, aby byl prohlížeč informován, jak se má chovat na webové stránce. Jejich implementace je jednoduchá, a zároveň užitečná pro bezpečnost uživatelů. Z toho důvodu je vhodné docílit nejvyšší možné známky v rámci hodnocení.

5 OPTIMALIZACE WEBOVÉ STRÁNKY PRO VYHLEDÁVAČE

Zabezpečení webové stránky by mělo být základním stavebním kamenem pro její úspěšnost. Další kroky v rámci optimalizace pro vyhledávače budou implementovány po převodu na HTTPS. SEO zahrnuje plán konkrétních kroků, které webové stránce pomohou při optimalizaci nalezitelnosti. Tyto kroky jsou doporučeními, jimiž by se vývojáři a správci webu měli řídit při jeho tvorbě a v průběhu. Body jsou zařazeny do tří kategorií a seřazené na základě priorit.

5.1 Úvodní analýza webové stránky

Optimalizace začíná úvodní analýzou, která se jinak nazývá marketingová mapa a přehledně shrnuje jednotlivé kroky a jejich aktuální stav. Úvodní shrnutí je vytvořeno na nezabezpečené webové stránce, ještě před převedením na nezabezpečený protokol.

Tabulka 5 - Úvodní analýza optimalizace pro vyhledávače

Faktory	Konkrétní kroky	Optimalizováno		
On-page		**Ne**	**V procesu**	**Ano**
	Indexace a crawling	•		
	Zabezpečení webu	•		
	Rychlost načítání	•		
	Responzivní design			•
	Strukturovaná data	•		
	Titulky, popisky a nadpisy		•	
	Klíčová slova	•		
	Budování obsahu	•		
Off-page	Zpětné odkazy	•		
	Linkbuilding	•		
Nástroje	Google Tag Manager	•		
	Google Analytics	•		
	Collabim	•		
	Google Search Console	•		

Z tabulky je patrné, že webová stránka není optimalizovaná vůbec. Jediné kroky, které web splňuje v základu je responzivní design, protože je stránka postavená na redakčním systému

WordPress, který má optimalizaci pro mobilní zařízení zahrnutou v šabloně. Druhým krokem jsou titulky, jejichž vyplnění redakční systém v základu také požaduje.

Nezabezpečená webová stránka byla v úvodu nahrána do softwaru Collabim a měřily se pozice webu ve výsledcích vyhledávání na zadaná klíčová slova. Úvodní analýza přinesla výsledky viz Tabulka 6.

Tabulka 6 - Pozice nezabezpečeného webu ve vyhledávání

Klíčové slovo	Pozice Google CZ
obor btsm	22
konference btsm	22
den otevřených dveří na fai	27
btsm utb zlín	33
skupina btsm	39
ústav bezpečnostního inženýrství	47
utb zlín	60+
magisterské studium	60+
fai utb	60+
bakalářské studium	60+
bezpečnostní studia	60+
fakulta aplikované informatiky	60+
btsm	60+
studium bezpečnosti	60+
btsm zlín recenze	60+

Nejlepší pozice se nachází až na třetí stránce výsledků vyhledávání. Z pozic lze usoudit, že nalezitelnost webu není ideální a uživatelé se k němu při hledání pravděpodobně nedostanou.

5.2 Doporučení v rámci optimalizace pro vyhledávače dle priorit

SEO doporučení se v praxi často řadí dle priorit. Některé kroky mají při optimalizaci vysoký dopad na hodnocení a některé nižší. Z toho důvodu jsou rozdělení do tří skupin podle důležitosti.

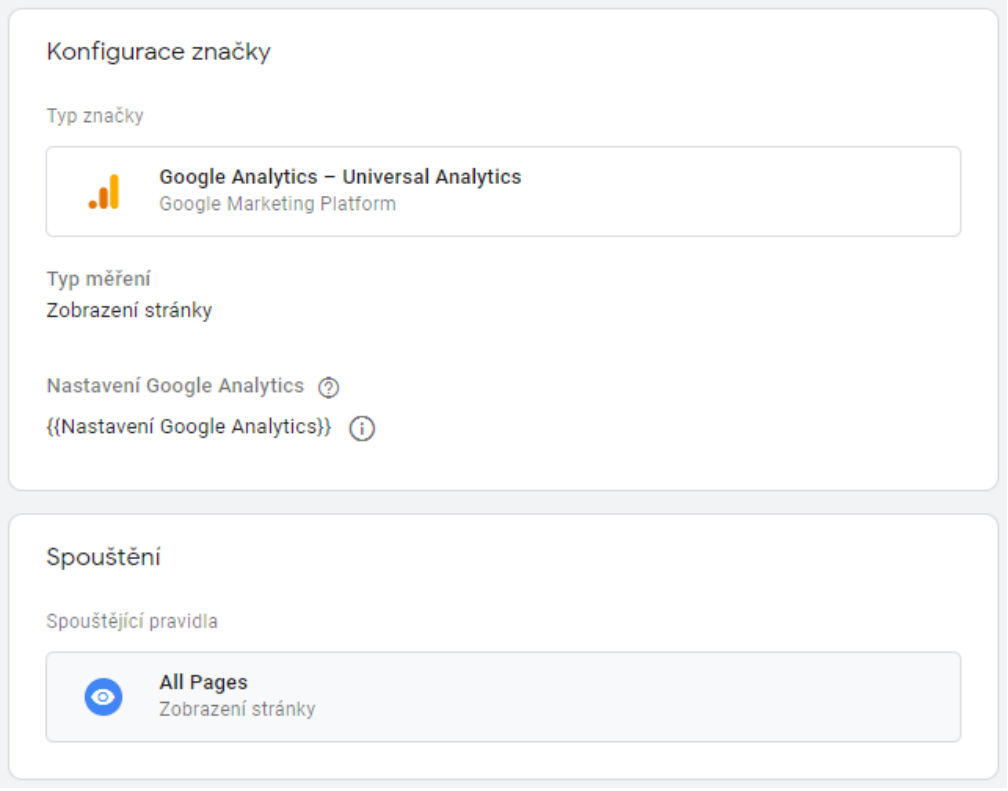
Některé kroky jsou specifické tím, že požadují soustavnou dlouhodobou péči, další se naopak optimalizují jednorázově.

Tabulka 7 - SEO doporučení seřazené podle priorit

Nejvyšší priorita	Zabezpečení webu
	Nasazení analytických nástrojů
	Analýza klíčových slov
	Robots.txt a sitemap.xml
	Rychlost načítání webové stránky
Střední priorita	Titulky, popisky a nadpisy
	Tvorba obsahu
	Linkbuilding
Nízká priorita	Optimalizace stránky 404
	Profil firmy v Google My Business a Firmy.cz
	Strukturovaná data

Nejvyšší prioritu má zabezpečení webové stránky. Jedná se o krok, který má vysoký dopad na uživatele a hodnocení. Proces zabezpečení je prakticky proveden v kapitole 4.

Nasazení analytických nástrojů je jednorázovou záležitostí. Pomocí Google Tag Manageru se na web implementuje analytický nástroj Google Analytics.



Obrázek 39 - Konfigurace nástroje Google Analytics ve správci značek

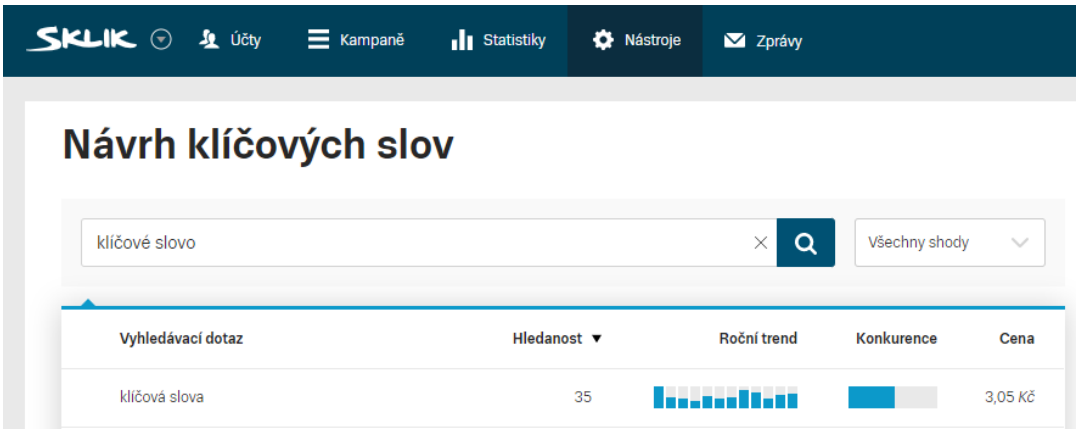
Nasazení se provádí pomocí vytvoření značky. Typ měření udává, kdy se má daná funkce vykonat a spouštění specifikuje stránky, na kterých se nástroj uvede do provozu. V případě měření návštěvnosti je zvolena možnost spouštění na všech stránkách webu.

Tag Manager a Google Search Console jsou na stránku vloženy pomocí pluginů ve WordPressu. Plugin Yoast by SEO umožňuje nasadit nejen Google Webmasters, ale vytvoří také soubory robots.txt a sitemap.xml. Plugin Metronet Tag Manager zajistí implementaci Google Tag Manageru na webovou stránku.

Obrázek 40 - Vložení Google Tag Manageru pomocí pluginu ve WordPressu

Nástroj Collabim nabízí správu jedné webové stránky zdarma, stačí založit uživatelský účet a danou webovou stránku zařadit do sledování. Implementací klíčových slov je možné sledovat pořadí webu na vložené výrazy.

Analýza klíčových slov je základním stavebním kamenem pro textaci webu, tvorbu obsahu i případnou placenou propagaci. Její tvorbu je vhodné začít brainstormingem a následným použitím nástrojů pro návrh klíčových slov. Ten je součástí nástrojů pro placenou propagaci. Výstupem analýzy je tabulkový soubor v Excelu, který zahrnuje vyhledávané fráze roztříděné do kategorií dle témat, obsahující statistiky vyhledávání, úrovně konkurence a průměrné ceny za kliknutí.



Obrázek 41 - Plánovač klíčových slov v Skliku

Střední prioritu mají kroky, na kterých je třeba pracovat soustavně. Zahrnují textaci webu a tvorbu relevantního obsahu na blog, která je součástí kvalitních webových stránek. Obsah odpovídá tématu webové stránky a je přidanou hodnotou pro uživatele. Články by měly mít vzdělávací či informativní charakter. V rámci tvorby textů a článků je vhodné zahrnout interní i externí odkazy, které budou relevantní k dané stránce.

Titulky a popisky webu jsou pro domovskou stránku a hlavní stránky z menu tvořeny ručně. Ostatní popisky a titulky jsou generovány z prvního odstavce textu na stránce.

Doporučeními s nízkou prioritou je vhodné se zabývat až po vyladění dvou předchozích kategorií. Jsou mezi nimi však kroky, které mohou pomoci hodnocení a organické návštěvnosti na webu. Založení profilu firmy v Google My Business a Firmy.cz je zadarmo a pomůže uživatelům a případným zákazníkům s vyhledáním základních informací. Strukturovanými daty se dají lépe specifikovat informace o webu, firmě či událostech tím, že je vyhledávače snadněji pochopí. Díky nim může být webová stránka lépe viditelná ve výsledcích vyhledávání.

```
<script type="application/ld+json">
{
    "@context": "http://schema.org",
    "@type": "WebPage",
    "name": "Název webové stránky",
    "description": "Meta popisek webové stránky."
    }
}
</script>
```

Obrázek 42 - Strukturovaná data pro WebPage

Smazané stránky se stavovým kódem 404 se nacházejí na každém webu. Jejich počet by však měl být co nejnižší. Uživatelsky přívětivým krokem je úprava stránky 404 tak, aby korespondovala s designem celého webu a případně dokázala uživatele motivovat na webu zůstat.

5.3 Analýza stránky po zabezpečení a zapracování doporučení

Při zapracování doporučení pro optimalizace pro vyhledávače se stránka může stát přívětivější pro uživatele a lépe hodnocenou v očích robotů. Implementací bodů nejvyšší priority má web potenciál být správně zaindexovaný vyhledávači a jednoduše nalezitelný uživateli na relevantní klíčová slova.

Tabulka 8 - Analýza webu po zapracování SEO doporučení

Faktory	Konkrétní kroky	Optimalizováno		
On-page		**Ne**	**V procesu**	**Ano**
	Indexace a crawling			•
	Zabezpečení webu			•
	Rychlost načítání		•	
	Responzivní design			•
	Strukturovaná data	•		
	Titulky, popisky a nadpisy		•	
	Klíčová slova			•
	Budování obsahu		•	
Off-page	Zpětné odkazy		•	
	Linkbuilding		•	
Nástroje	Google Tag Manager			•
	Google Analytics			•
	Collabim			•
	Google Search Console			•

Vložením analytických nástrojů, zabezpečením webu, analýzou slov a instalací pluginu pro SEO jsou hotové jednorázové kroky v rámci optimalizace. Jejich zapracováním je pravděpodobné zlepšení hodnocení webu vyhledávači.

Kroky, na kterých je žádoucí pracovat neustále, jsou tvorba obsahu, odkazů a ladění titulků a popisků u nově tvořených stránek. Tyto kroky mohou v čase zvyšovat kvalitu webové stránky a upevňovat její pozici na vysokých příčkách ve výsledcích vyhledávání. Optimalizace pro vyhledávače je dlouhodobým procesem, který má však smysl a z dlouhodobého hlediska může mít vliv na výkonnost webových stránek.

Zabezpečení webu mělo dopad i na pozice ve výsledcích vyhledávání. Převedená verze stránky opět byla měřena v Collabimu a její umístění se u určitých klíčových slov změnila. Měření bylo povedeno po dvou týdnech od implementace bezpečnostního certifikátu.

Tabulka 9 - Pozice zabezpečeného webu ve výsledcích vyhledávání

Klíčové slovo	Pozice Google CZ
obor btsm	2
konference btsm	4
den otevřených dveří na fai	10
btsm utb zlín	20
skupina btsm	2
ústav bezpečnostního inženýrství	60+
utb zlín	60+
magisterské studium	60+
fai utb	60
bakalářské studium	60+
bezpečnostní studia	60+
fakulta aplikované informatiky	60+
Btsm	39
studium bezpečnosti	60+
btsm zlín recenze	15

Na základě dat z Tabulky 9 lze zhodnotit, že zabezpečení stránky mělo pozitivní vliv na její pozice ve výsledcích vyhledávání.

6 SHRNUTÍ VÝSLEDKŮ A ZÁVĚREČNÁ DOPORUČENÍ

V průběhu praktické části byla webová stránka převedena na zabezpečený protokol implementací certifikátu od společnosti Let's Encrypt. Ve výsledném hodnocení nástrojem Qualys pro testování bezpečnosti byla udělena známka A. Současná úroveň zabezpečení je pro jednoduchou webovou stránku dostatečná. V případě, že by byla požadována vyšší úroveň zabezpečení, je vhodné upravit podporované protokoly a zaměřit se na sílu šifrování.

Nastavení bezpečnostních hlaviček bylo provedeno v konfiguračních souborech pomocí programovacího jazyka PHP. Docíleno je finálního hodnocení A+ v nástroji Security Headers. Jedná se o nejvyšší možnou známku. Pro úpravu pravidel chování serveru a prohlížeče je možné změnit parametry jednotlivých bezpečnostních hlaviček. Jejich nastavení závisí na požadavcích provozovatelů webů.

Na základě výsledků optimalizace pro vyhledávače lze potvrdit vliv zabezpečení webové stránky na pořadí zobrazení pomocích webových vyhledávačů. Pozice webu na zadaná klíčová slova byly měřeny softwarem Collabim. V úvodu zaznamenala nezabezpečená verze nejlepší zobrazení až na třetí stránce výsledků vyhledávání.

Tabulka 10 - Rozdíly pozic ve výsledcích vyhledávání

Klíčové slovo	Pozice Google CZ
obor btsm	+ 20
konference btsm	+ 18
den otevřených dveří na fai	+ 17
btsm utb zlín	+ 13
skupina btsm	+ 37
ústav bezpečnostního inženýrství	- 13
utb zlín	60+
magisterské studium	60+
fai utb	+ 1
bakalářské studium	60+
bezpečnostní studia	60+
fakulta aplikované informatiky	60+
Btsm	+ 21
studium bezpečnosti	60+
btsm zlín recenze	+ 45

Na základě údajů z Tabulky 10 je patrné, že se převedená stránka začala zobrazovat na některá klíčová slova již na první stránce. Údaje se změnily po indexaci nové verze webu, dva týdny po jejím převedení. U poloviny klíčových slov se pozice posunuly směrem nahoru, u dalších šesti zůstaly stejné a u jednoho slova došlo ke zhoršení. K výsledkům je nutno doplnit, že pozice klíčových slov se mění každým dnem v závislosti na zaindexovaném obsahu. Pozice 60+ značí, že analyzovaná webová stránka není na tato slova vhodně optimalizovaná. Řešením je úprava textace a tvorba obsahu, který bude obsahovat daná klíčová slova a k nim relevantní informace. Za nízkými pozicemi může být také celkové stáří webové stránky nebo neodpovídající název domény.

Vliv certifikátu na optimalizaci pro vyhledávače lze měřit i dalšími způsoby. První z nich je měření návštěvnosti webu, kterou je vhodné vyhodnocovat v horizontu půl roku a více. Druhou možností je sledovat pozice stránky na vyhledávací dotazy v Google Search Console. Pro dostatečné množství dat je nezbytné sledovat pozice minimálně několik týdnů. Celkově lze zhodnotit, že SEO není jednorázová záležitost, ale dlouhodobý proces, a proto se pozice webu mohou neustále vyvíjet.

ZÁVĚR

Práce spojuje zabezpečení webových stránek s optimalizací pro vyhledávače. Popisuje způsob, jakým spolu zmíněné oblasti souvisejí a jak se dají uplatnit v online marketingu. Celá práce je rozdělena na dvě hlavní části, první z nich je teoretická a druhá praktická.

V úvodu práce byly představeny možnosti zabezpečení webových stránek. Následně jsou popsány internetové protokoly, SSL certifikáty a certifikační autority. Technická část zahrnuje redakční systém WordPress a typické zranitelnosti webových aplikací. Specifikována byla také problematika optimalizace pro vyhledávače, jejích částí a představení současných webových vyhledávačů. SEO část je zakončena kritérii hodnocení pro zobrazení stránek na předních příčkách ve výsledcích vyhledávání.

Část teorie byla věnována nástrojům, pomocí kterých se testuje úroveň zabezpečení webové stránky. Vybrány byly také online nástroje prakticky využívané v současném online marketingu pro sledování návštěvnosti, indexace a klíčových slov. Nástroje jsou následně využity v praktické části pro analýzu implementované webové stránky.

V praktické části práce je implementován zabezpečený protokol pomocí certifikátu od společnosti Let's Encrypt a následné nastavení bezpečnostních hlaviček. Ty slouží k posílení bezpečnosti webové stránky. Úroveň zabezpečení byla upravována tak, aby v nástrojích pro hodnocení úrovně zabezpečení dosahovala webová stránka nejvyšší možné známky. V nástroji Qualys získal web hodnocení A, v nástroji pro testování bezpečnostních hlaviček A+. Navrženy byly kroky ke zlepšení vyhledatelnosti webové stránky, jejichž implementací má stránka potenciál ještě zvýšit svoji kvalitu v očích vyhledávačů. Díky jejímu zabezpečení byl položen základní kámen úspěšné optimalizace. Výsledky ze zkoumání pozic klíčových slov naznačily, že zabezpečený protokol měl vliv na pořadí webu ve výsledcích vyhledávání. Její další optimalizování a zkoumání vlivu na pozice ve vyhledávání je vhodné k dalšímu výzkumu. Do budoucna je tak vhodné nadále pokračovat ve zkoumání vlivu certifikátu na web a pracovat na případných úpravách, které si nové technologie žádají. Vyzkoušet lze jinou certifikační autoritu pro poskytnutí certifikátu a v rámci SEO dlouhodobě měřit návštěvnost webové stránky.

Bakalářská práce je vzhledem k její struktuře vhodná pro začínající vývojáře zabývající se tvorbou webových stránek pro komerční využití nebo pro online marketéry, zajímající se o optimalizaci stránek pro vyhledávače. Systematické popsání stránek z hlediska bezpečnosti webových stránek a spojení se SEO může poskytnout ucelený přehled o souvislosti dvou

popisovaných oblastí. Praktická část může sloužit jako návod pro zabezpečení webové stránky a její převod na protokol HTTPS zároveň se základním nastavením optimalizace pro vyhledávače.

SEZNAM POUŽITÉ LITERATURY

[1] HANÁK, Jiří. Vysvětlení SSL certifikátů: Co jsou, jak fungují a proč je používat. Master [online]. 2016 [cit. 2019-04-29]. Dostupné z: https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod

[2] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

[3] Co je to HTTP / HTTPS. SSLS.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.ssls.cz/https.html

[4] STALLINGS, William a Lawrie BROWN. Computer security: principles and practice. Third edition. Boston: Pearson, [2015], 840 s. Always learning. ISBN 978-1-292-06617-2.

[5] 3.0 ČESKO. Komu to věříme? Pohled mezi důvěryhodné certifikační autority [online]. [cit. 2019-04-29]. Dostupné z: https://www.petrkrcmar.cz/prednasky/certifikacni_autority.pdf

[6] 5 důvodů proč nasadit SSL certifikát a HTTPS na web. Web security blog [online]. 2019 [cit. 2019-04-29]. Dostupné z: https://blog.sslmentor.cz/clanky/5-duvodu-proc-nasadit-ssl-certifikat-a-https-na-web/

[7] Hypertext Transfer Protocol -- HTTP/1.1 [online]. 1999 [cit. 2019-04-29]. Dostupné z: https://tools.ietf.org/html/rfc2616

[8] MICHÁLEK, Martin. Rychlý protokol HTTP/2: S nasazením na weby na nic nečekejte. Vzhůru dolů [online]. 2019 [cit. 2019-04-29]. Dostupné z: https://www.vzhurudolu.cz/prirucka/http-2

[9] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority: legislativní rámec elektronického podpisu: praktické aplikace. Olomouc: ANAG, 2008, 157 s. Právo. ISBN 978-80-7263-465-1.

[10] Nejlevnější SSL certifikát. SSLmentor.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.sslmentor.cz/ssl/nejlevnejsi-certifikaty

[11] Zelený EV SSL certifikát. SSLmentor.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.sslmentor.cz/ssl/ev

[12] Multidoménové SSL certifikáty (UCC/SAN). SSLmentor.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.ssls.cz/certifikaty/san

[13] SSL WildCard SSL certifikát. SSLmentor.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.sslmentor.cz/ssl/wildcard

[14] Přehled DV, OV, EV SSL. SSLmentor.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.sslmentor.cz/ssl/druhy-overeni

[15] CAB Forum (Certification Authority Browser Forum). ZONER software, a.s. [online]. [cit. 2019-04-29]. Dostupné z: https://www.sslmarket.cz/ssl/cab-forum/

[16] Certifikační autorita. SSL-cerfifikaty.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.ssl-certifikaty.cz/o-certifikatech/certifikacni-autorita/

[17] SSL pomocí Let's Encrypt - HTTPS zdarma. ENDORA.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.endora.cz/vlastnosti/https-zdarma-ssl-lets-encrypt

[18] SSL certifikát - HTTPS certifikát. SSLmentor.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.sslmentor.cz/ssl/ssl-certifikaty

[19] Vypněte TLS 1.0 a 1.1 už dnes. Michal Špaček [online]. 2018 [cit. 2019-04-29]. Dostupné z: https://www.michalspacek.cz/vypnete-tls-1.0-a-1.1-uz-dnes

[20] PoodleBleed zranitelnost. SSLS.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.ssls.cz/poodle.html

[21] OpenSSL Heartbleed. SSLS.cz [online]. [cit. 2019-04-29]. Dostupné z: https://www.ssls.cz/heartbleed.html

[22] Protokol SSL/TLS - slabé šifry, zranitelnosti a jejich testování. Samuraj [online]. 2014 [cit. 2019-04-29]. Dostupné z: https://www.samuraj-cz.com/clanek/protokol-ssl-tls-slabe-sifry-zranitelnosti-a-jejich-testovani/

[23] SSL v ohrožení: komunikaci je možné dešifrovat. Root.cz [online]. 2011 [cit. 2019-04-29]. Dostupné z: https://www.root.cz/clanky/ssl-v-ohrozeni-komunikaci-je-mozne-desifrovat/

[24] TLS 1.3 – Seznamte se s novým bezpečnostním standardem. Blog SSL Market [online]. 2018 [cit. 2019-04-29]. Dostupné z: https://blog.sslmarket.cz/inpage/tls-1-3-seznamte-se-novym-bezpecnostnim-standardem

[25] HLAVINKA, Jaroslav. Co si pohlídat při přechodu na HTTPS?. Jak dělat SEO [online]. 2018 [cit. 2019-04-29]. Dostupné z: https://jakdelatseo.cz/checklist-pro-prechod-z-http-na-https

[26] OWASP Top 10 [online]. 2013 [cit. 2019-04-29]. Dostupné z: https://www.owasp.org/images/f/f3/OWASP_Top_10_-_2013_Final_-_Czech_V1.1.pdf

[27] 10 nejzávažnějších zranitelností webových aplikací podle OWASP [online]. [cit. 2019-05-14]. Dostupné z: https://www.zdrojak.cz/clanky/10-nejzavaznejsich-zranitelnosti-webovych-aplikaci-podle-owasp/

[28] Top 10-2017 Top 10 [online]. [cit. 2019-05-14]. Dostupné z: https://www.owasp.org/index.php/Top_10-2017_Top_10

[29] GRAPPONE, Jennifer a Gradiva COUZIN. SEO - Search Engine Optimization. Přeložil Roman SKŘIVÁNEK, přeložil Dana BALAŠTÍKOVÁ. Brno: Zoner Press, 2007. Encyklopedie webdesignera. ISBN 978-80-86815-85-5.

[30] Online marketing [online]. [cit. 2019-04-24]. Dostupné z: https://www.optimal-marketing.cz/slovnicek/online-marketing

[31] On-page faktory [online]. [cit. 2019-04-24]. Dostupné z: https://www.evisions.cz/on-page-faktory-cs

[32] VELIČKA, Matěj, Richard KLAČKO a David BRENNER. Ochutnejte technické SEO [online]. [cit. 2019-04-24]. Dostupné z: https://taste.cz/ebook-technicke-seo

[33] KUBÍČEK, Michal a Jan LINHART. 333 tipů a triků pro SEO: [sbírka nejlepších technik optimalizace webů pro vyhledávače]. Vyd. 1. Brno: Computer Press, 2010, 262 s. ISBN 978-80-251-2468-0.

[34] Linkbuilding pro e-shopy. ContentKing [online]. [cit. 2019-04-24]. Dostupné z: https://www.contentkingapp.cz/akademie/linkbuilding-e-shopu

[35] Long tail. Adaptic, s. r. o. [online]. [cit. 2019-04-24]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/long-tail

[36] Off-page faktory. Adaptic, s. r. o. [online]. [cit. 2019-04-24]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/off-page-faktory

[37] Off-page faktory. MioWeb [online]. [cit. 2019-04-24]. Dostupné z: https://www.mioweb.cz/slovnicek/offpage-faktory

[38] SEO: Užitečné tipy – část 3. InPage [online]. [cit. 2019-04-24]. Dostupné z: https://blog.inpage.cz/inpage/seo-uzitecne-tipy-cast-3

[39] Historie internetových vyhledávačů a katalogů [online]. [cit. 2019-05-18]. Dostupné z: https://www.webcesky.cz/historie-internetovych-vyhledavacu-a-katalogu

[40] SCHMIDT, Eric, Jonathan B. ROSENBERG a Alan EAGLE. Jak funguje Google. Brno: Jota, 2015, 318 s. ISBN 978-80-7462-749-1.

[41] Historie Google [online]. [cit. 2019-05-18]. Dostupné z: https://businessworld.cz/cio-bw-special/historie-google-6729

[42] Co je Seznam.cz [online]. [cit. 2019-05-18]. Dostupné z: https://www.mioweb.cz/slovnicek/vyhledavac-seznam

[43] Infografika: Podíl vyhledávačů Google a Seznam na českém internetu #2019 [online]. [cit. 2019-05-18]. Dostupné z: https://www.evisions.cz/blog-2019-01-24-infografika-podil-vyhledavacu-google-a-seznam-na-ceskem-internetu-2019

[44] Chraňme si náš Seznam.cz – je totiž na světě jedinečný [online]. [cit. 2019-05-18]. Dostupné z: http://www.czechfreepress.cz/podoteky/chranme-si-nas-seznam-cz-je-totiz-na-svete-jedinecny.html

[45] Google vs. Seznam - infografika [online]. [cit. 2019-05-18]. Dostupné z: https://ceskeinfografiky.cz/google-vs-seznam-infografika

[46] Bing, nový vyhledávač Microsoftu, je online. Ohrozí Google? [online]. [cit. 2019-05-18]. Dostupné z: https://www.zive.cz/Bleskovky/Bing-novy-vyhledavac-Microsoftu-je-online-Ohrozi-Google/sc-4-a-147274/default.aspx

[47] 10 klíčových SEO faktorů ovlivňující výsledky na Googlu [online]. [cit. 2019-05-18]. Dostupné z: https://blog.netpromotion.cz/10-klicovych-seo-faktoru-googlu

[48] Dwell time: Důležitá metrika stojící v pozadí [online]. [cit. 2019-05-18]. Dostupné z: https://getfound.cz/blog/dwell-time-dulezita-metrika-stojici-v-pozadi

[49] SSL Server Rating Guide [online]. 2018 [cit. 2019-04-29]. Dostupné z: https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

[50] Logjam: jak vyřešit nově objevenou zranitelnost. SSL Market [online]. 2015 [cit. 2019-04-29]. Dostupné z: https://blog.sslmarket.cz/inpage/logjam-jak-vyresit-nove-objevenou-zranitelnost

[51] SSL Tester 3.2 - ověření instalace SSL certifikátu. SSLS.cz [online]. 2015 [cit. 2019-04-29]. Dostupné z: https://www.ssls.cz/ssltest.html

[52] Časté otázky k Security Headers. [online]. [cit. 2019-04-30]. Dostupné z: https://securityheaders.cz/faq

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AMP	Accelerated Mobile Pages
CTR	Click-through rate
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
PHP	Hypertext Preprocessor
PPC	Pay Per Click
SEO	Search Engine Optimization
SERP	Search Engine Results Page
SSL	Secure Socket Layer
TLS	Transport Layer Security
UTM	Urchin Tracking Module

SEZNAM OBRÁZKŮ

SEZNAM TABULEK