Webstránky z pohľadu bezpečnosti a GDPR

Martina Javůrková, MBA

www.dimensions.sk

Obsah

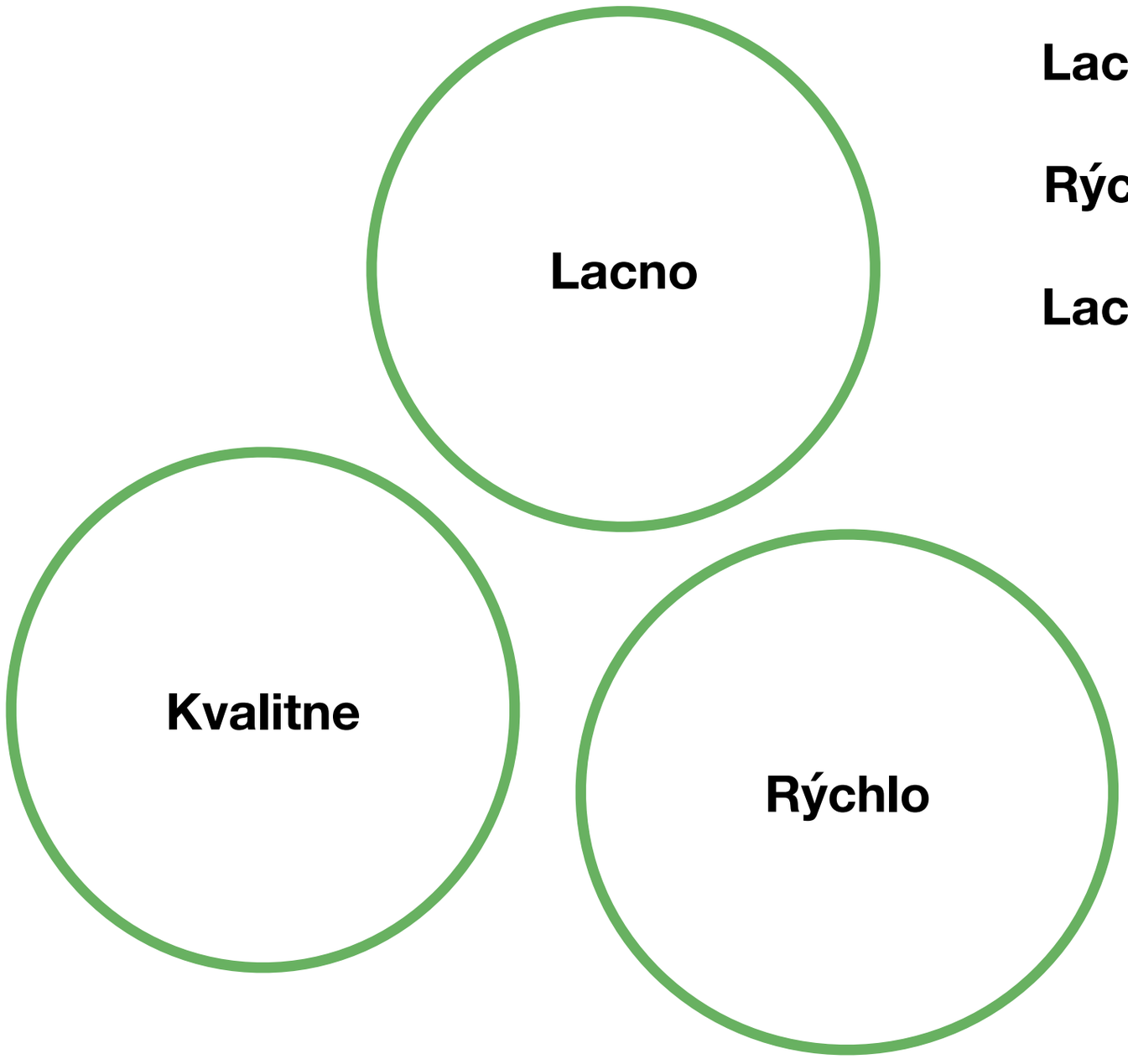
- Základné rozdelenie webstránok
- Ako získať svoju webovú stránku
- Hrozí mojej webstránke riziko?
- Open Source redakčné systémy a ich riziká
- Dobrá prax
- Ako si vybrať dobrého dodávateľa
- Najčastejšie porušenia GDPR na webových stránkach
- Na čo myslieť pri tvorbe webovej stránky

Základné rozdelenie webstránok

- **CMS** - webstránku môže vytvoriť aj laik bez znalostí programovania a v podstate zadarmo

- **Natívne** - vyžadujú programátorske znalosti a skúsenosti

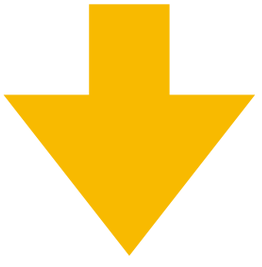
Ako získať svoju webovú stránku



Lacno a kvalitne = nebude to rýchlo

Rýchlo a kvalitne = nebude to lacné

Lacno a rýchlo = nebude to kvalitné



Bezpečnostné riziká

Zadarmo, bez vedomostí a skúseností

Čo všetko sa môže stať …

- Neautorizované prihlásenia
- Zastaraný základný softvér
- Nedefinované používateľské roly
- Zastarané šablóny a doplnky
- Malvér
- (SQL) Injekcie
- Spam s optimalizáciou pre vyhľadávače (SEO)
- Skriptovanie medzi stránkami
- Útoky odmietnutia služby
- Phishing
- Útoky na dodávateľský reťazec
- Hotlinking
- Falšovanie žiadostí medzi stránkami (CSRF)

… a aké to môže mať dôsledky

- Distribúcia phishing e-mailov
- Zneužitie vášho CMS neskôr na útok na ďalšie prepojené systémy
- Strata kontroly nad CMS
- Krádež údajov
- Nesúlad / porušenie GDPR s možnými sankciami

Kybernetické útoky mrhajú vašim časom, energiou a peniazmi. Môžu tiež ohroziť vašu autoritu a povesť, najmä ak sú útokmi ovplyvnení návštevníci vašich stránok.

– Jamie Juviler (HubSpot)

Hrozí vašej webstránke riziko?

- Dostupnosť CMS = viac rizikových používateľov, ktorí nepoznajú dobré bezpečnostné postupy

- (Ne)výhoda CMS: otvorený zdrojový kód

  - Výskumníci a vývojari k nemu majú prístup a testujú ho, čo umožňuje identifikovať bezpečnostné chyby

  - Prístup majú aj škodliví hackeri

Bezpečnostné riziká v číslach

- Adresár WordPress ponúka 56 000 oficiálnych doplnkov (pluginov) a tisícky ďalších sú dostupné od dodávateľov tretích strán.
- 13,7 milióna škodlivých žiadostí z 16 000 rôznych adries IP bolo zacielených na takmer 1,6 milióna webových stránok WordPress, uviedla bezpečnostná firma WordPress WordFence v správe zverejnenej 9. 12. 2021
- V roku 2020 Wordfence nameral viac ako 2 800 útokov za sekundu zameraných na WordPress
- Na WordPresse beží 43,2 % všetkých webových stránok
- V roku 2021 došlo k nárastu nahlásených zraniteľností o 150 % oproti roku 2020
- 29 % kritických chýb plugingoch pre WordPress vôbec nedostalo bezpečnostnú aktualizáciu
- Len 0,58 % zraniteľností sa nachádzalo v jadre WordPressu, zvyšok sa týkal šablón a pluginov, ktoré pochádzali z rôznych zdrojov a od vývojárov od tretích strán.
- 91,38 % chýb bolo odhalených v bezplatných pluginoch, platené prémiové doplnky pre WordPress tvorili iba 8,62 %
- približne 43 % webov na WordPresse využívalo v roku 2021 aspoň jeden zraniteľný komponent z priemerne 18 nainštalovaných

Zdroj: https://patchstack.com/whitepaper/the-state-of-wordpress-security-in-2021/

Dobrá prax pre bezpečnosť vášho webu

- Používať silné heslá a pravidelne ich aktualizovať
- Používať dvojfaktorovú autentifikáciu
- Pravidelne inštalovať aktualizácie WordPress-u (vychádzajú cca raz za 3 mesiace)
- Pravidelne inštalovať aktualizácie doplnkov (vychádzajú nepravidelne, čím viac doplnkov, tým viac a čatejších aktualizácií)
- Pravidelne vykonať audit doplnkov a ich využívania, deaktivovať a odinštalovať nepoužívané
- Pravidelne inštalovať aktualizácie šablóny a vymazať nepoužívané
- Prideliť užívateľom len nevyhnutné práva
- Vykonať pravidelne bezpečnostnú kontrolu škodlivého kódu
- Inštalovať kvalitné bezpečnostné doplnky
- Používať reCaptcha a iné bezpečnostné prvky
- Pridať watermarks na fotografie a obsah webu
- Vybrať si dôveryhodného poskytovateľa hostingu so silným technickým a bezpečnostným zázemím

(ne)Aktualizovanie

- CMS sa rýchlo vyvíja = nutné pravidelne aktualizovať doplnky (pluginy)
- Pravidelne sa vyhľadávajú a opravujú nové chyby zabezpečenia = je potrebné aktualizácie nainštalovať čo najskôr a často kontrolovať dostupné záplaty
- Pri výbere doplnkov (pluginov):
  - Uprednostňujte aktualizované doplnky
  - Uprednostňujte uznávané a široko používané doplnky
  - Pozorne sledujte vývoj každého doplnku použitého na vašom webe
  - Vykonajte analýzu bezpečnostných rizík
  - Vykonajte analýzu súladu s GDPR

Ako si vybrať dobrého dodávateľa

- Podpíše s vami zmluvu
- Dobre sa pýta
- Analyzuje vaše odpovede a potreby
- Má časový harmonogram a dodržiava termíny
- Komunikuje s vami tak, že mu rozumiete
- Vysvetľuje. Viete čo robí a prečo
- Píše vlastný kód na mieru pre vás
- GDPR nie sú len 4 otravné písmenka

Najčastejšie porušenia GDPR na webových stránkach

čo?

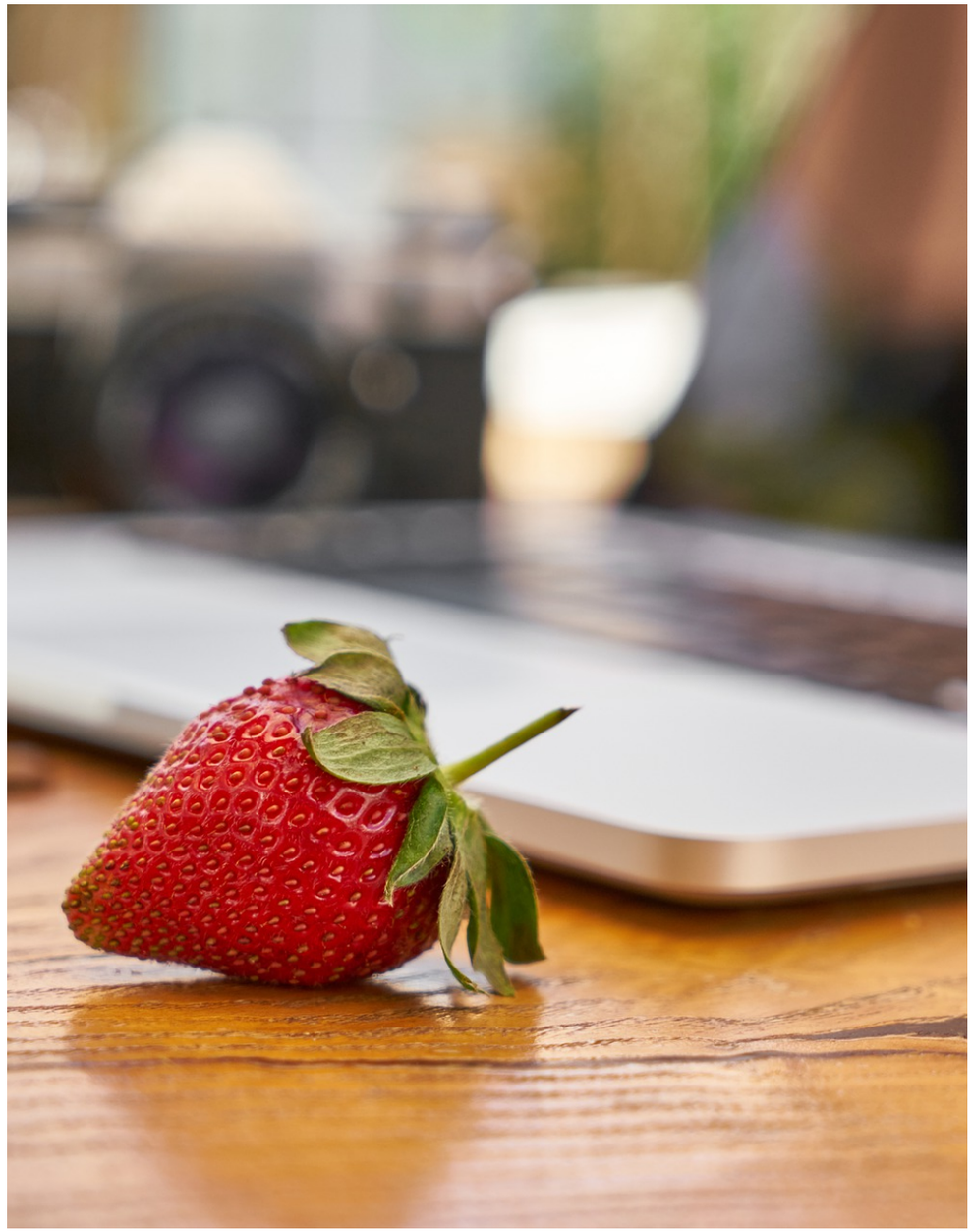
- ☑ SSL certifikát
- ☑ Cookie lišta
- ☑ Informačná povinnosť
- ☑ Súhlas

kde?

- ☐ Newsletter
- ☐ Formuláre
- ☐ Dokumenty na stiahnutie
- ☐ Rezervácie, kalendáre, platby
- ☐ Sociálne siete
- ☐ Referencie
- ☐ Fotografie
- ☐ Videá
- ☐ Kontaktné údaje
- ☐ Povinne zverejňované zmluvy
- ☐ Komentáre
- ☐ Prekliky na iné weby

Na čo myslieť pri tvorbe webovej stránky?

- **UX vs GDPR**
  - Na čo webstránka slúži?
  - Aké dáta spracúvam a na akých právnych základoch?
  - Dochádza ku prenosu osobných údajov do 3. krajín?
  - Informoval som dotknuté osoby správnym spôsobom?
  - Kto sú sprostredkovatelia?
  - Sprostredkovateľská zmluva a pokyny pre sprostredkovateľa
- **Sprostredkovateľská zmluva**
  - Záväzok mlčanlivosti
  - Kto je vlastník kódu?
  - Ako sú riadené prístupy?
  - Aké údaje Sprostredkovateľ spracúva a na aký účel?
  - Ktoré spracovateľské operácie môže vykonávať?
  - Aké technické a organizačné opatrenia musí prijať pred začatím spracúvania a ako ich skontrolujem?



Dimensions Consulting Services s.r.o.
Zámocká 18
811 01 Bratislava

Kontakt: office@dimensions.sk