Lynt SERVICES

Modelování rizik s WordPress

Jak Vláďa Smitka přemýšlí o bezpečnosti

https://lynt.cz + https://webcheck.cz + https://smitka.me @smitka

Lynt SERVICES

Dobrý den, jsem bezpečnostní výzkumník a zároveň váš zákazník.

Žena mě požádala, abych **koupil nové zubní kartáčky**, ale místo toho jsem na vašem webu ### jsem narazil na **bezpečnostní chybu typu Reflected XSS**. Ta je způsobena nedostatečným ošetřením uživatelských vstupů a umožnuje na vašem webu vykonávat **škodlivý javascriptový** kód - XSS (cross site scripting). Reflected v tomto případě znamená, že pro její zneužití je třeba aby návštěvník webu kliknul na upravený odkaz.

Problém jsem nalezl v parametru "s" při vyhledávání, ale je možné, že se chyba nachází i na dalších místech.

Ukázka - následující odkaz nahradí na vašem webu všechny obrázky za obrázek **tlustého jednorožce**:

https://###/vyhledavani?s=%27;document.querySelectorAll(%27img%27).forEach(img%20=%3E%20img.src%20=%20%27https://tools.lynt.cz/u.png%27);%27

Reálný útočník by však mohl vykonat libovolný jiný kód, který by například mohl získat **citlivé údaje návštěvníka**, **přesměrovat ho na falešný web** se stejným vzhledem, nechat ho **stáhnout malware** a případě, kdyby na odkaz kliknul administrátor, tak by mohlo být možné získat i **kompletní kontrolu** nad webem.

Jaký by měl být další postup:

Tento e-mail byste měli předat lidem, kteří se u vás starají o web, případně dodavateli webu, aby chybu opravil. Jistě jim z popisu bude jasné, co mají dělat. Případně jsem k dispozici pro další konzultace.

Dále bych doporučoval zvážit odměnu za nalezení tohoto problému a jeho zodpovědné nahlášení (responsible disclosure). Na základě průmyslových standardů se tento typ chyby u webů, kde nejsou kritická data, typicky oceňuje v rozmezí 2000 - 10000,- Kč. Vzhledem k tomu, že u vás nakupuji, uvítám odměnu i formou nabízených produktů, například má 4 letá dcera miluje plyšové chobotnice, které máte také v nabídce 🙂.

Více o bezpečnostních problémech českých e-shopů si můžete přečíst v mém starším článku: https://datablog.reshoper.cz/studie-tretina-ceskych-e-shopu-ma-bezpecnostni-problemy/.

Aktuální problémy publikuji na svém anglickém blogu https://smitka.me.

Lynt SERVICES

vulnerability report - 4897

KM **Keyur Maheta**
komu Vladimír Smitka

so 04.03.2023 18:12

Byl detekován jazyk Angličtina. Chcete zprávu přeložit? Nyní nebo nikdy.

Hello Team
I Keyur Maheta found security issue in your system

TITLE :
`wp-config-setup`

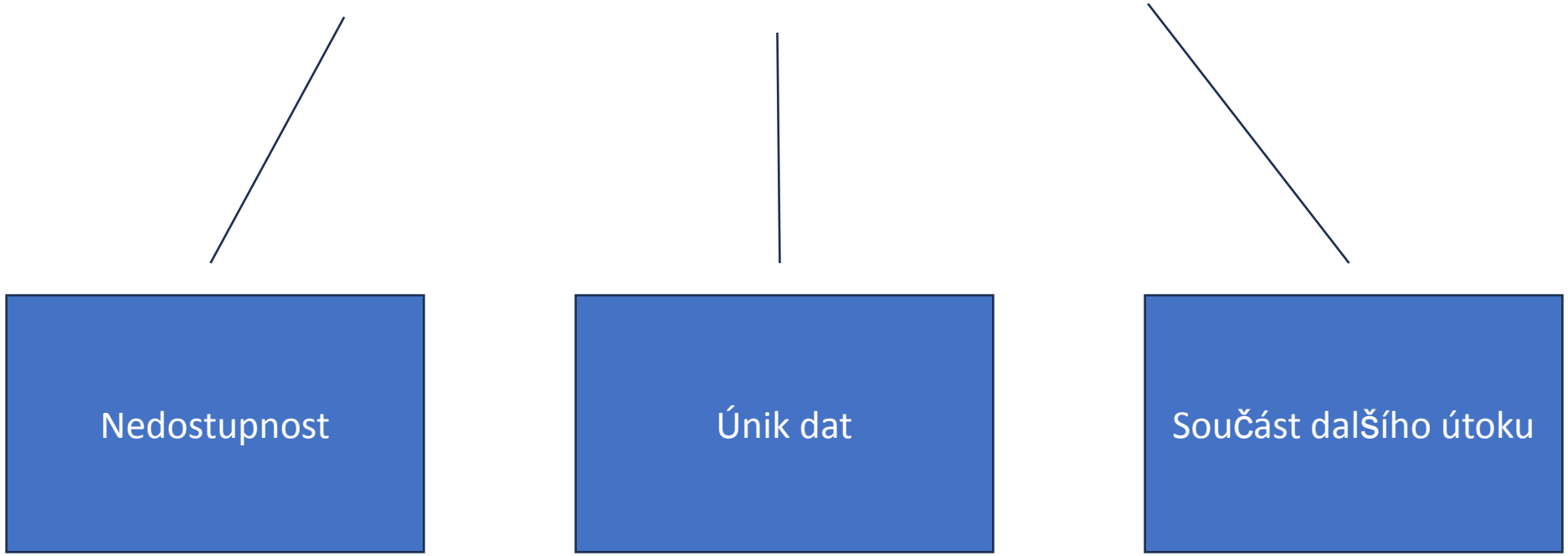
Step to rerpdouce
https://edu.lynt.cz/wp-admin/setup-config.php?step=1

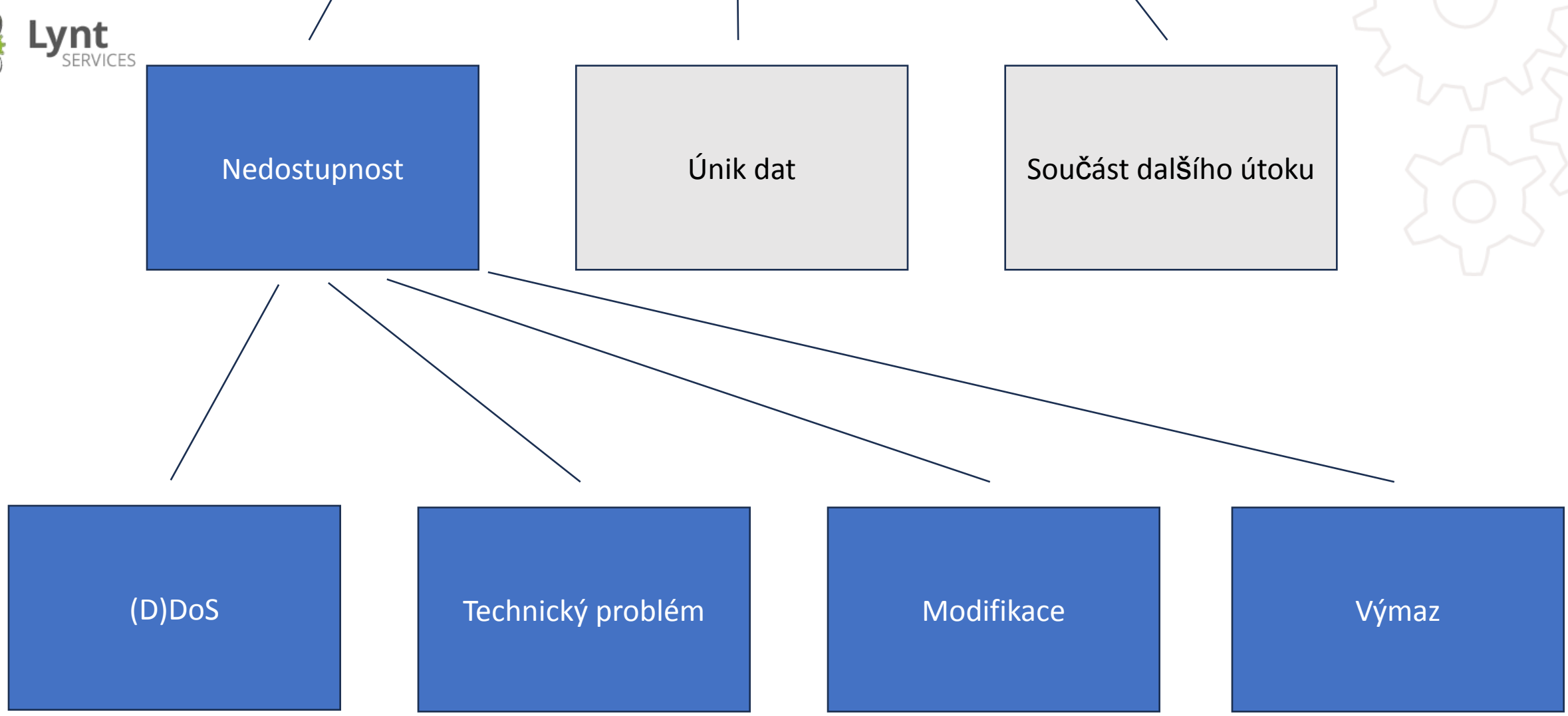
severity: high
reference: https://smaranchand.com.np/2020/04/misconfigured-wordpress-takeover-to-remote-code-execution/
tags: wordpress,setup

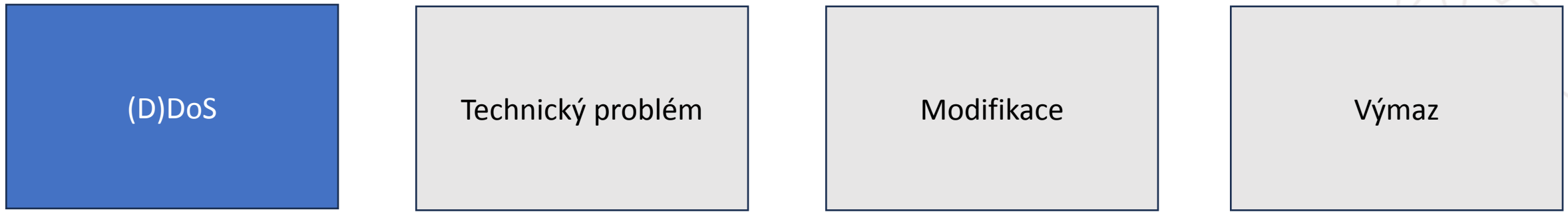
Best regards,
Keyur

Lynt SERVICES

Co mě může potkat?




Nedostupnost
Únik dat
Součást dalšího útoku
(D)DoS
Technický problém
Modifikace
Výmaz



- HA infrastruktura
- Rate limiting
- CloudFlare
- Vysoký výkon (cachovací plugin)

- Spuštení nouzové infra

Lynt SERVICES

(D)DoS	Technický problém	Modifikace	Výmaz

- Monitoring
- Logování

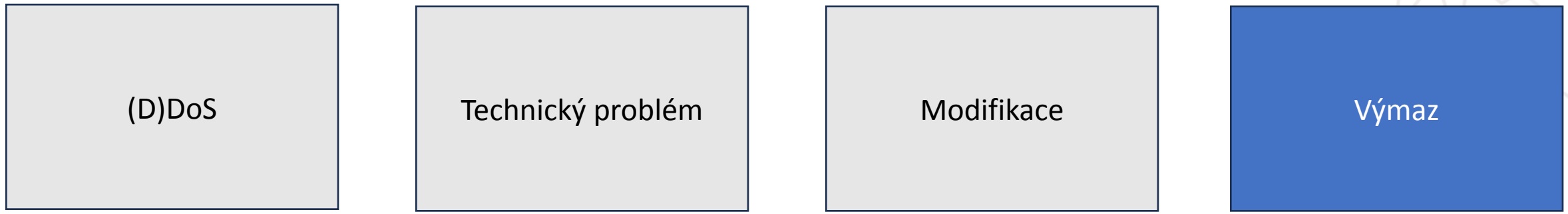
- Prověření logů
- Hotfix

Lynt SERVICES

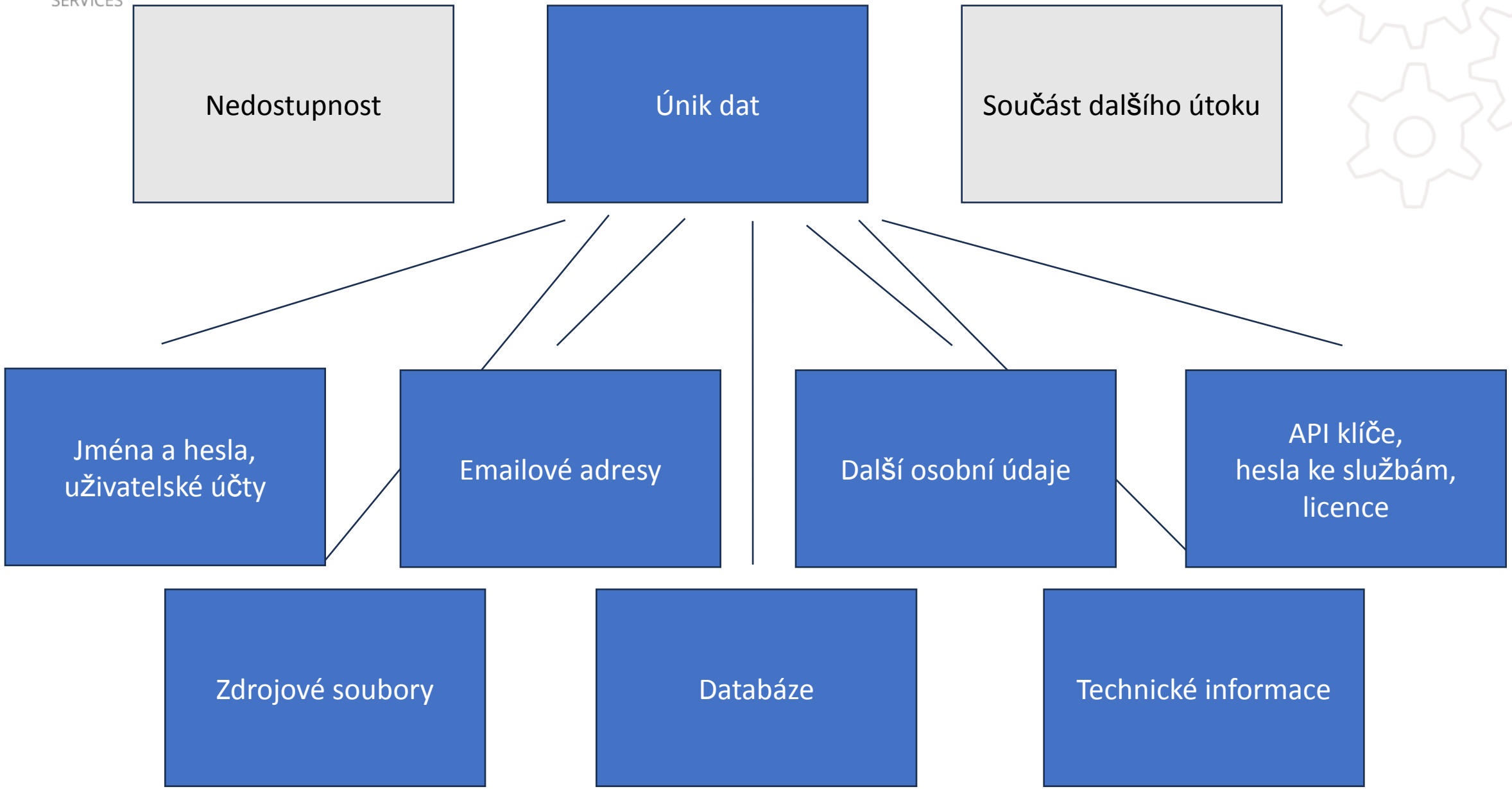
(D)DoS	Technický problém	**Modifikace**	Výmaz

- Zabezpečení *
- Zálohy

- Forenzní analýza
- Obnova zálohy



- Zálohy
- Obnova zálohy


Nedostupnost
Únik dat
Součást dalšího útoku
Jména a hesla, uživatelské účty
Emailové adresy
Další osobní údaje
API klíče, hesla ke službám, licence
Zdrojové soubory
Databáze
Technické informace

Lynt SERVICES

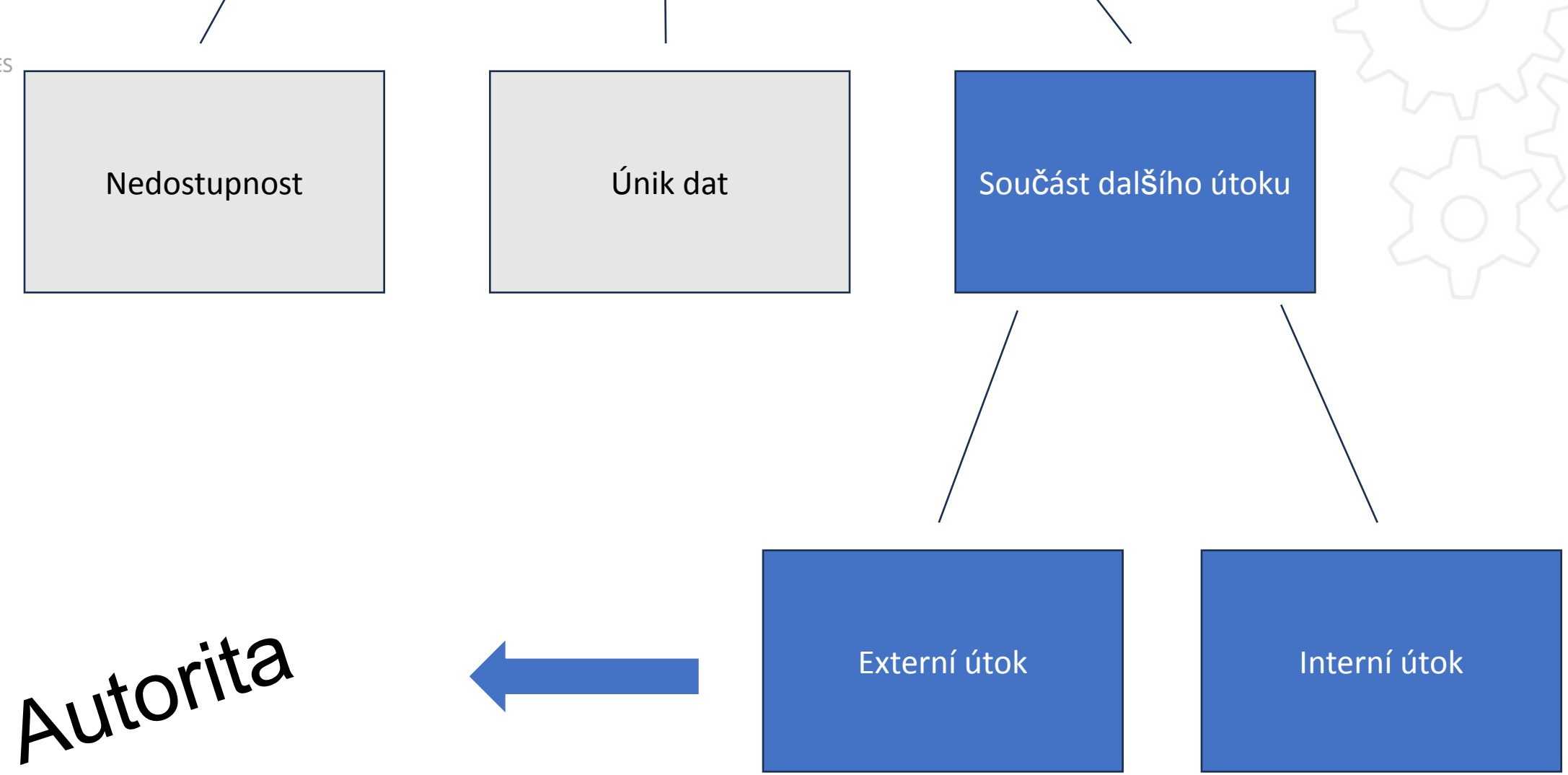
Co s daty?

- jména a hesla - přístup do adminu, zneužití v dalších službách
- emailové adresy - spam, profilování lidí
- další osobní údaje - profilování, podvody, prodej na černém trhu
- API klíče, hesla ke službám, licence - zneužití
- zdrojové soubory - hledání zranitelností a získání dat 👆
- celá databáze - získání informací 👆 zálohy
- technické informace – příprava na další útoky 👆

Jak data uniknou?

- zaměstnanec/vývojář (úmyslně nebo neúmyslně)
- zranitelnost
- další web na serveru
- postranní kanál

Lynt SERVICES



Lynt SERVICES

Jak si zabezpečit web?
Modelové příklady

1 – malý blog o whisky

2 – firemní web solárníků

3 – síť magazínů o investicích s několika autory

4 – střední eshop s rybářskými potřebami

5 – banka

Lynt SERVICES

Bezpečnost pro všechny

- Silná hesla a bezpečné chování
- Minimalizace počtu pluginů
- Důvěryhodné zdroje
- Aktualizace
- Zálohování
- Správné nastavení HTTPS
- Nedávat do prostoru hostingu neprodukční soubory
- Bezpečný hosting (to jde blbě poznat…)
- Blokace chybných přihlášení

Lynt SERVICES

popijenicko.cz

Osobní informační web, bez reklamy, sem tam affiliate odkaz. Zhruba jeden článek měsíčně.

Čeho se bojím?

- Bezpečnostní chyby v neaktualizovaných komponentách.
- Spam v komentářích.

Co doporučuji?

- Zapnout automatické aktualizace
- Zvážit bezpečnostní plugin nebo .htaccess firewall
- Antispamový plugin

Lynt SERVICES

sviticko.cz

Firemní web, který sbírá leady, velká konkurence.

Čeho se bojím?

- Na web se dostane malware, bude penalizovaný ve vyhledávačích.
- Web nebude fungovat.

Co doporučuji?

- Monitoring dostupnosti
- Bezpečnostní plugin s malware scanem
- Přístup do administrace jen z firmy

vydelavanicko.cz + cryptobuh.cz

Magazíny vydělávající na zobrazování reklamy, několik článků každý den.

Čeho se bojím?

- Na web se dostane malware, bude penalizovaný ve vyhledávačích.
- Web nebude fungovat nebo spadne pod náporem.
- Uniknou přístupy některého z autorů.

Co doporučuji?

- Minimalizace oprávnění, 2FA
- Hromadná správa aktualizací
- Audit log
- Cloudflare
- Vypnout gravatary nebo filtrace rest api
- Dobře izolované weby

Lynt SERVICES

krmenicko.cz

Woo eshop se 4000 produkty.

Čeho se bojím?

- Kvality doplňků.
- Únik dat.

Co doporučuji?

- Vlastní server se správcem, serverové bezpečnostní nástroje, spolehlivá služba na maily.
- 2FA, Bcrypt
- Kvalitní aplikační firewall, virtual patching.
- Zvážit CSP hlavičku.
- Audit, kde všude se data pohybují.
- Testovací prostředí.
- (Přejít na Shoptet 😀)

Lynt SERVICES

vasenasepenizky.cz

Je třeba opravdu dobrý plán 😉

Nástroje

- WordFence – kompletní bezpečnostní řešení
- 7G/8G Firewall – pravidla do .htaccess
- BBG Firewall – jednoduchý nenáročný blokátor
- WP Activity Log – audit log
- WP Armour – antispam
- CleanTalk – cloudový antispam
- Two Factor – 2FA
- UpdraftPlus - zálohování
- HetrixTools – monitoring dostupnosti a blacklistů
- Lynt Security Enhancer – naše bezpečnostní zlepšováky pro pokročilé

Lynt SERVICES

Uff!

A to je vše ☺️

Díky za pozornost a sledujte lynt.cz, smitka.me
a mě na x/twitteru @smitka