NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Bezpečné aplikace pro stát

Mikulov 2021

Vladimír ROHEL

Historie – příklady publikovaných problémů

- Roku 2013 turecká hackerská skupina RedHack prolomila vládní web „Istanbul Special Provincial Administration“, aby vymazala dluhy lidí za elektřinu, vodu, plyn, a internetové připojení. K útoku útočníci využili jednoduše zranitelnosti SLQ Injection, díky které obešli přihlašovací stránku webu.
- Vývojáři nepoužili prakticky žádnou ochranu proti **SQL Injection** – programátoři se k psaní kódu stavěli nezodpovědně a proměnné vkládali přímo do SQL dotazu, nepoužili ani starší ochrany ošetřením proměnných tzv. escapováním – každopádně vůbec neměli proměnné vkládat do SQL dotazů ale používat tzv. parametrizované dotazy, zanedbali jakoukoliv ochranu na straně databáze nastavením oprávnění uživatele atp. I velmi snadný bezpečnostní test by podobnou chybu odhalil – proto lze usuzovat, že takto důležitý web nikdy nebyl před útokem bezpečnostně testován.
- Zdroj: https://www.ehackingnews.com/2013/06/istanbul-special-provincial.html

NAKIT

Historie – příklady publikovaných problémů

- Počátkem roku 2014 se kyberzločinci nabourali do online aukčního webu a získali hesla, e-mailové adresy, data narození a fyzické adresy 145 milionů uživatelů. Pozitivní je, že finanční informace ze sesterského webu PayPal byly uloženy odděleně od informací o uživatelích v rámci praxe známé jako segmentace sítě. To mělo za následek omezení útoku a zabránilo zločincům dostat se ke skutečně citlivým platebním informacím.
- Vývojáři nezodpovědně zpracovávali, ukládali či přenášeli data, dostatečně data neklasifikovali, nešifrovali a obecně **zanedbali téma zabezpečení dat již při návrhu** aplikace. Důkladný bezpečnostní test či audit by podobný nedostatek jistě odhalil.
- Zdroj: https://www.malwarebytes.com/data-breach

Historie – příklady publikovaných problémů

- V roce 2017 odhalili bezpečnostní výzkumníci podvod na SEO, který postihl více než 300 000 webových stránek WordPress. Podvod se soustředil kolem pluginu CAPTCHA pro WordPress s názvem Simply WordPress. Po instalaci Simply WordPress otevřel zadní vrátka a umožnil správcovský přístup k postiženým webům. Odtud hacker zodpovědný za tuto službu vkládal skryté odkazy na své podvodné webové stránky s výplatou půjček (odkazování jiných webových stránek na vaše webové stránky je skvělé pro lepší SEO).
- Vývojáři nezodpovědně použili do SEO (search engine optimization), resp. do CMS (content management systém) **nedůvěryhodný plugin z cizího zdroje**. Nejlepší obranou v tomto případě je ujistit se, že jakékoli aplikace a zásuvné moduly, které vyberete, pocházejí z důvěryhodného zdroje. U webů by zmíněný případ odhalil i snadnější bezpečnostní test, který by zkoumal původ implementovaných pluginů.
- Zdroj: https://www.malwarebytes.com/backdoor

NAKIT

Historie – příklady publikovaných problémů

- British Airways - druhá největší letecká společnost ve Spojeném království - čelila v roce 2018 úniku dat. Únik se týkal 380 000 rezervačních transakcí v období od srpna do září 2018. Hackerská skupina Magecart – zaměřená zejména na skimming karet pro útok využila zranitelnosti XSS (cross-site scripting) v JavaScriptové knihovně Feedify. Útočníci upravili webovou stránku (resp. JavaScriptový soubor) tak, že formulářové údaje si nechali zasílat na vzdálený server.
- Opět i v tomto případě vývojáři příliš **důvěřovali kódu z cizího zdroje**, knihovnu neprověřili a neučinili protiopatření – buď knihovnu neměli používat, nebo měli provést její opravu. Opět i v tomto případě pravděpodobně nebyl proveden bezpečnostní test, který by zranitelnost odhalil.
- Zdroj: https://readwrite.com/2020/11/30/3-dangerous-cross-site-scripting-attacks-of-the-last-decade/

NAKIT

Co nás k tématu vedlo?

Stát používá a vyvíjí velké množství aplikací „na klíč“

Aktuální trend je poskytování služeb občanům cestou portálových řešení nebo i například mobilních aplikací

Občas je velký tlak na dodávání nových funkcionalit a služeb často v krátkém čase

Stává se, že zadání není dostatečně detailní a dopracovává se „cestou“

Jsou špatně definovaná rizika

Aktuálně není jasná regulace vývoje pro stát a pravidla pro bezpečný vývoj aplikací

NAKIT

Co říká vyhláška č. 82/2018 Sb.?

§ 25

Aplikační bezpečnost

(1) Povinná osoba provádí penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva, a to

a) před jejich uvedením do provozu a

b) v souvislosti s významnou změnou podle § 11 odst. 3.

(2) Povinná osoba dále v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací a transakcí před

a) neoprávněnou činností a

b) popřením provedených činností.

NAKIT

AP NSKBČR 2021 – 2025 – pozitivní směr

C. ODOLNÁ SPOLEČNOST 4.0

	Kód	Úkol	Odpovědný subjekt	Časový rámec
ZABEZPEČENÍ DIGITÁLNÍ VEŘEJNÉ SPRÁVY	79.	Dle přístupu „security by design" navrhnout proces zabezpečení systémů e-Governmentu, a to již od počátku vytváření a realizace jednotlivých prvků.	MV NÚKIB Vládní zmocněnec pro IT a digitalizaci	Q4 2021
	80.	Již od počátku realizace jednotlivých systémů e-Governmentu zajistit dodržování navržených procesů určených k zajištění jejich kybernetické bezpečnosti.	MV NÚKIB Vládní zmocněnec pro IT a digitalizaci	Od Q1 2022 průběžně
	81.	Vytvořit metodiku bezpečného kódu pro státní správu s cílem podpořit vývoj bezpečného software.	MV ve spolupráci s: NÚKIB	Q4 2021

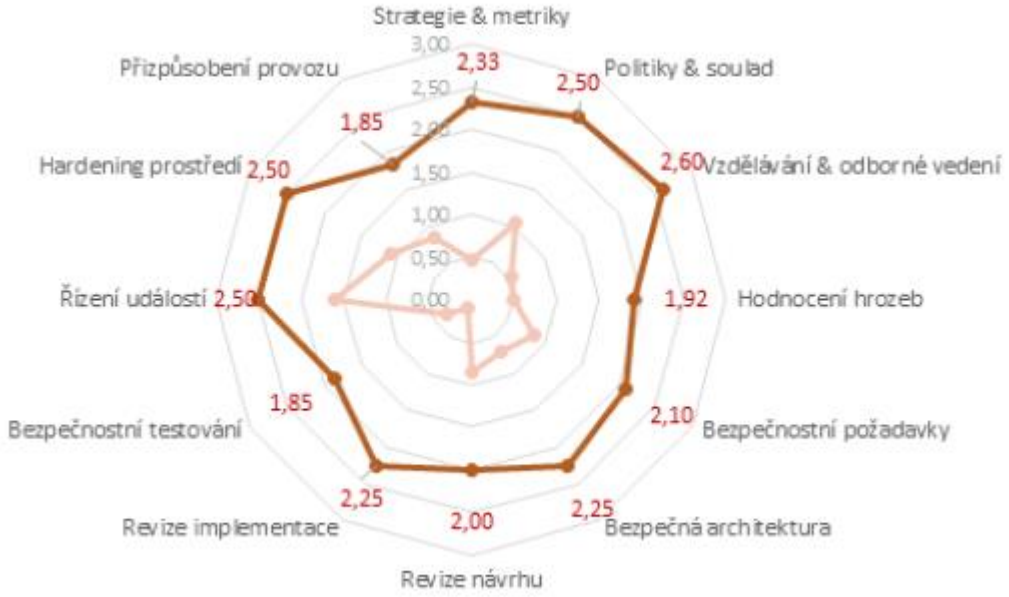
NAKIT

Reakce - Bezpečný vývoj v NAKIT

- 2019 – diskuse o nových přístupech k vývoji a bezpečnosti
- 2020 – vytvoření nové metodiky bezpečného vývoje v NAKIT
- 2021 – zahájen projekt zavádění metodiky do praxe
- Průběžné zlepšování stávajících projektů podle závěrů metodiky

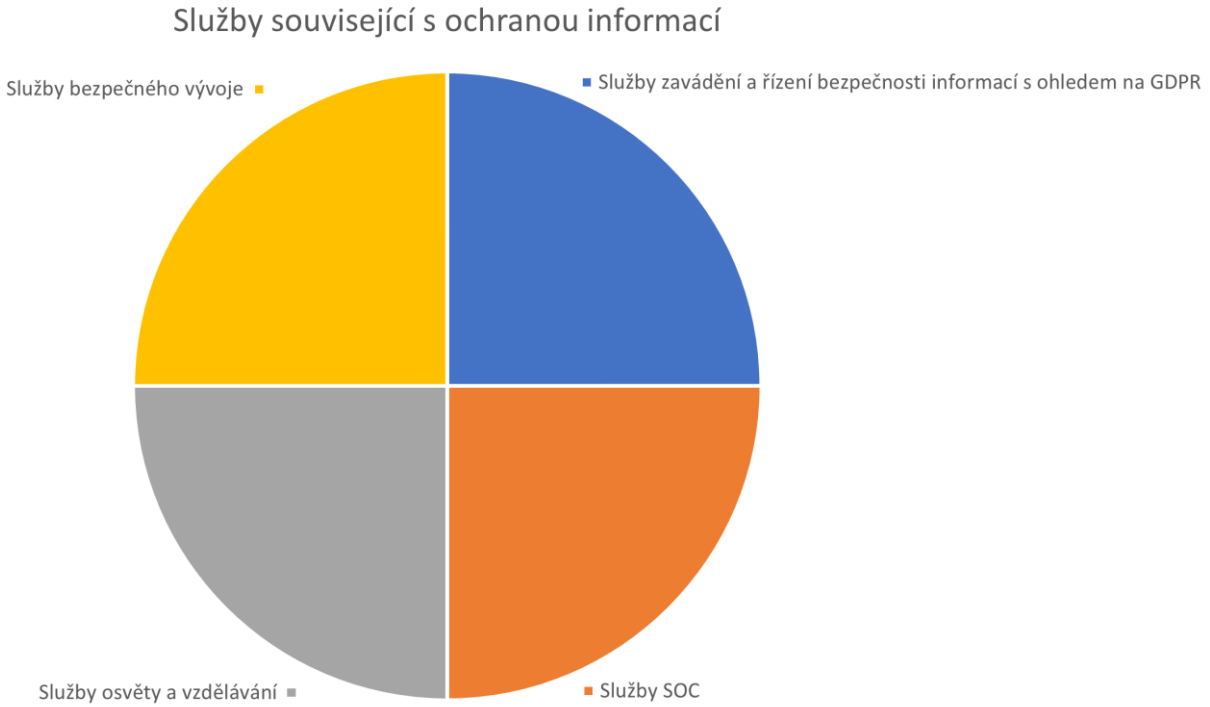
NAKIT

Příklad sledování aplikace metodiky



NAKIT

Služby bezpečnosti NAKIT



NAKIT

Závěr

- **Bezpečný vývoj v NAKIT** doplnil mozaiku oblastí našich bezpečnostních služeb, které budeme nadále rozvíjet do další formy služeb dodávky bezpečnosti pro stát a eGovernment

- Pár odkazů na závěr
  - a) **Minimální bezpečnostní standard**
    - https://nakit.cz/experti-z-nukib-nakit-a-ministerstva-vnitra-spojili-sily-kvuli-zabezpeceni-mensich-organizaci/
  - b) **Bezpečnostní standard pro videokonference**
    - https://nakit.cz/predstavujeme-bezpecnostni-standard-pro-videokonference/
  - c) **Doporučení pro bezpečné nakládání s e-identitou**
    - https://nakit.cz/pruvodce-svetem-elektronicke-identity/
  - d) **Ransomware: Doporučení pro mitigaci, prevenci a reakci**
    - https://www.nukib.cz/download/publikace/podpurne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf
  - e) **Kurzy KB pro správce ICT a nadstavba pro správce ve zdravotnictví**
    - https://csirt.muni.cz/about-us/news/muni-a-nakit-pripravily-kurzy-kyberbezpecnosti-pro-it-profesionaly
    - https://bootcamp.nc3.cz/

NAKIT

Děkuji

Q&A

Vladimír Rohel

E: vladimir.rohel@nakit.cz
M: +420 725 755 418

W: www.nakit.cz

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.