Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Obstarávanie, vývoj a údržba sietí, informačných systémov a aplikácií.

Pavol Dovičovič

21. október 2025

ČO HOVORÍ VYHLÁŠKA..

Bezpečnostné opatrenia (1/2)

- **Bezpečnostné opatrenia pre bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií podľa § 20 ods. 2 písm. f) zákona prijíma prevádzkovateľ základnej služby tak, že:**

  - je zabezpečené prepojenie procesov riadenia rizík a projektového riadenia počas celého životného cyklu projektov
  - je pravidelne, aspoň raz ročne vykonávaná kontrola a aktualizácia konfigurácie komponentov sietí, informačných systémov a operačných technológií podľa vývoja hrozieb; o kontrole sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia
  - sú definované a vykonávané procesy testovania bezpečnosti informačných systémov a operačných technológií
  - testovanie kybernetickej bezpečnosti je začlenené do životného cyklu vývoja a údržby sietí, informačných systémov a operačných technológií

Bezpečnostné opatrenia (2/2)

- **Bezpečnostné opatrenia pre bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií podľa § 20 ods. 2 písm. f) zákona prijíma prevádzkovateľ základnej služby tak, že:**
  - sú určené a uplatnené pravidlá bezpečného vývoja softvéru a informačných systémov
  - sú pri vývoji alebo získavaní aplikácií identifikované a naplnené relevantné požiadavky na kybernetickú bezpečnosť
  - sú riadené, monitorované a kontrolované činnosti súvisiace s vývojom programových prostriedkov a informačných systémov, ktoré sú dodávané treťou stranou
  - vývojové, testovacie a produkčné prostredia sú vzájomne oddelené a zabezpečené

VŠEOBECNÉ ZÁSADY RIADENIA DODÁVATEĽOV

- Organizácia musí implementovať formálny a zdokumentovaný proces, ktorým bude:
  - riadený spôsob výberu poskytovateľov služieb
  - riadený prípadný prenos činnosti k nim
  - dokumentované požiadavky na bezpečnosť informácií.

- Proces riadenia dodávateľov by mal pokrývať najmä nasledujúce oblasti:
  - Preverovanie budúcej dodávateľskej činnosti (**due dilligence**)
  - Definícia zmluvných záruk
  - Monitorovanie dodržiavania zmluvných podmienok
  - Pravidelný audit dodávateľov s cieľom poskytnúť komplexné záruky
  - Činnosti súvisiace s ukončením dodávateľského reťazca.



Spolufinancovaný Európskou úniou

ZAINTERESOVANÉ STRANY PRI RIADENÍ DODÁVATEĽOV

- Aby mohli byť splnené kľúčové záväzky, v závislosti od typu dodávateľa, kontextu a charakteru príslušných dodávateľských činností by mal proces riadenia dodávateľov **zahŕňať zástupcov z nasledujúcich oblastí**:
  - Príslušný vlastník procesu
  - Útvar zodpovedný za obstarávanie a riadenie dodávateľských vzťahov
  - Útvar zodpovedný za IT architektúru
  - Manažér kybernetickej bezpečnosti
  - Útvar zodpovedný za právne vzťahy



PRINCÍPY BEZPEČNÉHO VÝVOJA SYSTÉMOV (SSDLC)

ZÁSADY BEZPEČNÉHO VÝVOJA (SSDLC)

- **Secure Software Development Framework (SSDLC)**, vývojový rámec, ktorý sa zameriava na procesy súvisiace s integráciou bezpečnosti do existujúcich SDLC procesov
  - Vo všeobecnosti zahŕňa integráciu testovania bezpečnosti a ďalších aktivít do existujúceho vývojového procesu, aby sa zabezpečilo, že systém bude odolný proti bezpečnostným hrozbám a zraniteľnostiam
  - Opisuje vzťahy pri bezpečnom vývoji softvéru
  - Uvádza príklady ako dodržiavanie týchto postupov výrobcom softvéru pomôže:
    - znížiť počet zraniteľností v softvéri
    - zmierniť potenciálny dopad využívania nezistených alebo neadresovaných zraniteľností
    - zaoberať sa hlavnými príčinami zraniteľností, aby sa zabránilo opakovaniu v budúcnosti
  - Poskytuje spoločný slovník pre bezpečný vývoj softvéru
  - Zákazníci ho môžu používať na podporu komunikácie s dodávateľmi v akvizičných procesoch a iných riadiacich činnostiach

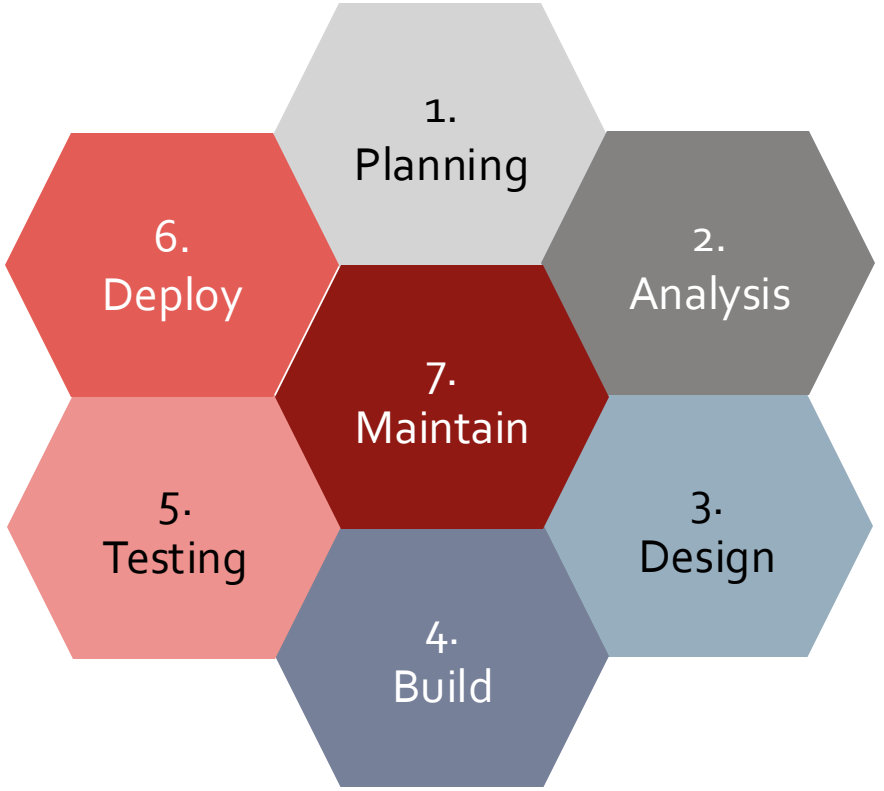


Zdroj: Microsoft SDL

ŽIVOTNÝ CYKLUS VÝVOJA SYSTÉMOV

Koncept životného cyklu vývoja systémov sa vzťahuje na celý rad hardvérových a softvérových konfigurácií, pretože systém sa môže skladať iba z hardvéru, iba zo softvéru alebo z kombinácie oboch.

- Tento cyklus má viacero typických fáz:
  - Preskúmanie opodstatnenosti
  - Analýza požiadaviek
  - Špecifikácia a návrh
  - Príprava prostredia
  - Vývoj
  - Testovanie
  - Implementácia, prechod
  - Dokumentácia
  - Prevádzka a údržba
  - Hodnotenie



Podľa techbeamers.com (2020)

BEZPEČNOSTNÉ OPATRENIA PODĽA SSDLC

- **Analýza požiadaviek:** Dopadové analýzy (BIA, DPIA),
- **Fáza plánovania:** Analýza rizík a hrozieb prostredia (TRA, GRA),
- **Fáza architektúry a dizajnu:** Posúdenie bezpečnostných rizík založené na dizajne, analýza architektúry,
- **Fáza vývoja:** Statická bezpečnostná analýza kódu (Secure Code Analysis),
- **Fáza implementácie:** Dynamická analýza kódu, testovanie bezpečnosti aplikácií (Dynamic Code Analysis),
- **Testovanie - Fáza pred nasadením:** Penetračné testovanie a analýza zraniteľnosti.

Cieľom je zabezpečiť bezpečný vývoj a eliminácia prenosu chýb do ďalšej fázy.

Zdroj: www.softwaretestinghelp.com

ZÁVER

- Ďakujeme za Váš čas
- Nasledujúci webinár na tému „ Bezpečnosť dodávateľského reťazca, riadenie súladu, audit a kontrola.“ 18.11.2025



NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.