PRINCÍPY BEZPEČNÉHO VÝVOJA SOFTVÉRU

Bezpečnosť má byť súčasťou všetkých fáz životného cyklu vývoja IT systémov. V posledných rokoch bol zavedený pojem „životný cyklus bezpečného vývoja systémov" (ang.: „Secure System Development Life Cycle" – SSDLC).

Bezpečný vývoj softvéru sa opiera o niekoľko základných zásad:

URČENIE POŽIADAVIEK

Bezpečnostné kritériá začlenené do každej fázy procesu vývoja softvéru, vrátane aplikačnej architektúry a koncepcie použiteľnosti softvérového produktu.

HĹBKOVÁ OCHRANA

Na ochranu pred rôznymi typmi hrozieb sú implementované viaceré vrstvy bezpečnostných opatrení. (ang.: „Defense in Depth")

ZÁSADA NAJNIŽŠÍCH PRÁVOMOCÍ

Používatelia a zariadenia majú prístup len k tým funkcionalitám v rámci informačného systému, ktoré sú nevyhnutné na plnenie príslušných úloh. (ang.: „Least Privilege")

ODDEĽOVANIE ZODPOVEDNOSTÍ

Jednotliví používatelia nemajú možnosť používať alebo upravovať informačné aktíva bez predchádzajúcej autorizácie, právomoci používateľov sú obmedzené, aby sa predišlo riziku zneužitia v dôsledku kumulácie. (ang.: „Separation of Duties")

ŠPECIFICKY NAVRHNUTÁ BEZPEČNOSŤ

Primerané technické a organizačné opatrenia sú prijaté už v čase určenia prostriedkov spracúvania, t.j. už vo fáze návrhu a vývoja IT systémov. (ang.: „Security by Design")

ŠTANDARDNÁ BEZPEČNOSŤ

Primerané technické a organizačné opatrenia sú trvalo udržateľné, t.j. IT systémy sú predvoleným spôsobom nakonfigurované s bezpečnými nastaveniami a voľbami. (ang.: „Security by Default")

RIADENIE ZRANITEĽNOSTÍ

Posudzovaním a záplatami je minimalizovaný počet známych zraniteľností a potenciálnych slabých miest v IT systémoch a infraštruktúre. (ang.: „Vulnerability Management")

LOGOVANIE

Správne nakonfigurovaný proces logovania bezpečnostných informácií napomáha včas zachytiť neobvyklé správanie softvéru, a systémové udalosti skôr, ako sa rozvinú do skutočného incidentu.

BEZPEČNÉ RÁMCE

Používajú sa iba najnovšie a najbezpečnejšie verzie nástrojov a komponentov na vývoj softvéru, softvérové knižnice komponenty sú aktívne podporované, majú pozitívne referencie a pochádzajú od dôveryhodných dodávateľov.

VALIDÁCIA VSTUPOV

Je správne nastavená stratégia syntaktického a sémantického overovania vstupov, kód je konzistentný a softvérové moduly neakceptujú žiadne nesprávne a neočakávané vstupy.

ODDELENÉ PROSTREDIA

Vývoj prebieha mimo produkčného prostredia a bez použitia "ostrých dát", s definovaným a riadeným procesom správy zdrojového kódu a verzií.

MANAŽMENT DIGITÁLNYCH IDENTÍT

V kontexte odporúčaní OWASP je zaručené používanie silných hesiel, je implementovaná viacfaktorová autentifikácia, v systéme je zabudovaná správa relácií (ang. „Session management") a implementovaná je správa cookies.

OCHRANA CITLIVÝCH ÚDAJOV

Na citlivé údaje (napr. heslá, osobné údaje, údaje o kreditných kartách, zdravotné záznamy, obchodné záznamy atď.) je aplikovaná vyššia úroveň ochrany, najmä šifrovaná ochrana informácií pri prenose a ukladaní údajov.

SPRACOVANIE VÝNIMIEK A CHÝB

Systém sa nezrúti ani pri výskyte chyby a spôsob, akým bude aplikácia reagovať na množstvo nepredvídateľných stavov sa opiera o súbor účinných núdzových scenárov.

PENETRAČNÉ TESTOVANIE

Potenciálne zraniteľné miesta systému vyplývajúce z chýb kódovania, alebo chýb konfigurácie sú odhalené testovaním, ešte pred nasadením do produkčného prostredia.

SÚLAD

Systém je navrhnutý tak, aby počas jeho budúcej prevádzky boli dodržané príslušné právne predpisy, požiadavky odvetvovej regulácie a technické normy týkajúcich sa informačnej bezpečnosti. (ang.: „Compliance)

Tieto odporúčania sú zoznamom hlavných zásad , ktoré by mali všetci vývojári dodržiavať s cieľom dodávať softvérové aplikácie odolné voči známym kybernetickým bezpečnostným hrozbám. Adoptovanie princípov bezpečného vývoja softvéru musí byť samozrejme predmetom hlbšieho štúdia a najmä udržateľnej najlepšej praxe v oblasti aplikačnej architektúry.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ISBN 978-80-69011-03-8

Verzia V.1

www.cybercompetence.sk