

SECURITY 2012



20. ročník konference o bezpečnosti v ICT

Case study: Bezpečný vývoj aplikácie v praxi

Juraj Porubčan, AEC

Martin Žemlička, VUB





Trochu teórie o Secure SDLC

- Zo štatistík vyplýva, že:
 - 37% všetkých identifikovaných zraniteľností pochádza z webových aplikácií
 - 75% bezpečnostných incidentov vzniká v aplikáciách

Web Application Vulnerabilities
as a Percentage of All Disclosures in 2011 H1

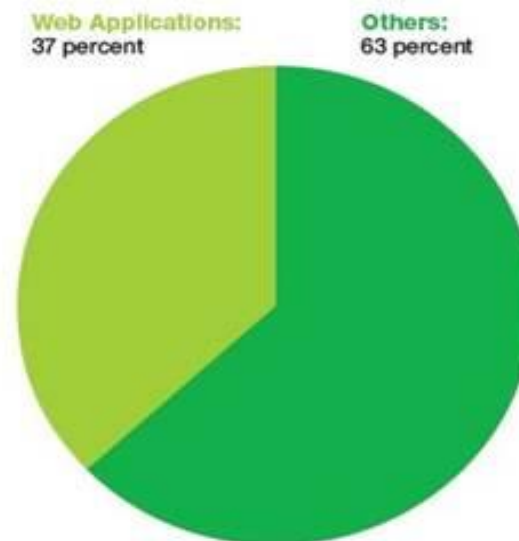


Figure : Web Application Vulnerabilities as a Percentage of All Disclosures in 2011 H1



Teória o SDLC, pokračovanie

- V minulosti boli útoky vedené väčšinou na vrstvu infraštruktúry, nie na aplikačnú vrstvu
- Aplikačná vrstva nebola napádaná, pretože obvykle nebola vystavená von
- Bezpečný vývoj aplikácie znamená časovú aj finančnú úsporu
- Je teda potrebné zabezpečiť všetky vrstvy systému ako celok

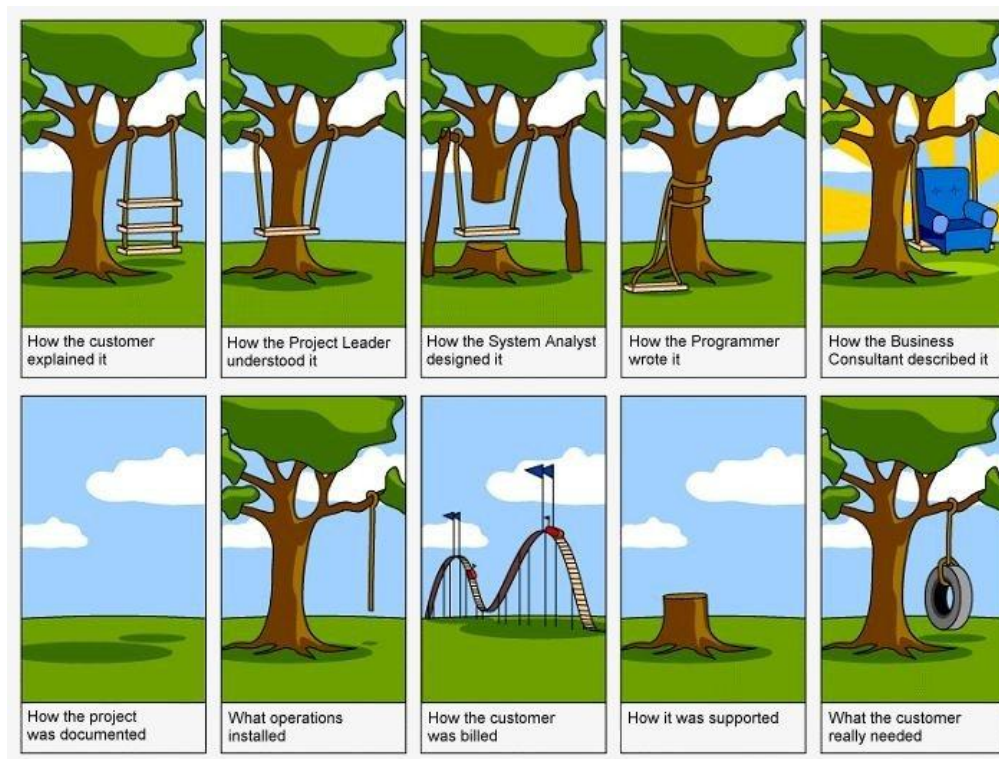




Trochu teórie o Secure SDLC

■ Naše členenie SDLC

- Analýza
- Návrh
- Vývoj
- Testovanie
- Nasadenie



Toto ale viete a je to štandardná teória. Teraz prax



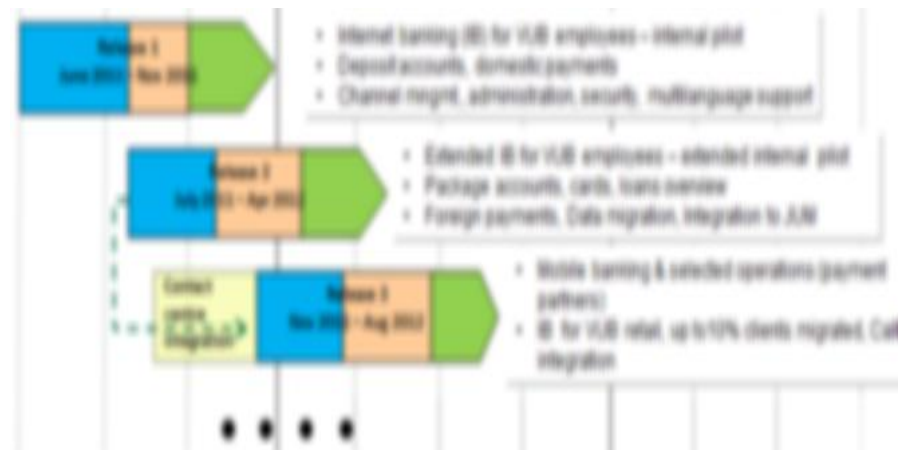
Predstavenie projektu

■ Čo je Multichannel

- Nové riešenie, ktoré má v budúcnosti integrovať všetky predajné a podporné kanály do jedného prostredia

■ Prečo je Multichannel

- Potreba reagovať na nové požiadavky klientov a trhu
- Potreba čeliť novým hrozbám v cyber-priestore





Projekt, pokračovanie

- Cieľ nášho snaženia
 - Implementovať riešenie, ktoré bude aj bezpečné
 - Zaviesť efektívne mechanizmy, ktoré umožnia eliminovať jednoduché a systematické chyby v návrhu a implementácii
 - Definovať mechanizmy, ktoré pomôžu udržať istú úroveň kvality celého riešenia
 - Mať prehľad o rizikách v riešení, aby boli riadené čo najefektívnejšie



Náš tím

- Role v projekte (nerobíme všetci všetko)
 - Dodávateľ aka Juraj
 - Revízia HFD, DFD, DTD a APD
 - Zákazník aka Martin
 - Analýza rizík
 - Akceptácia výstupov projektu a oponovanie návrhových dokumentov
 - Konzultant aka Marek
 - Pomoc pri dodržiavaní kvality riešenia
 - Pripomienkovanie dokumentov súvisiacich s bezpečnosťou
 - Všetci
 - Konzultácie pre jednotlivé projektové tímy





Ako sme si metodiky prispôsobili

■ Referenčné metodiky

- FIPS
- NIST



■ Výhody

- Všeobecne akceptované bezpečnostné štandardy
- Štandardy definujú štruktúru dokumentov (deliveráčov)
- Povinnosť riadiť sa štandardami VÚB a ISP
- Potreba prispôbiť štandardy požiadavkám lokálnych regulátorov a zákazníka

■ Nevýhody

- Vytvorené pre US prostredie (právne aj bezpečnostné)



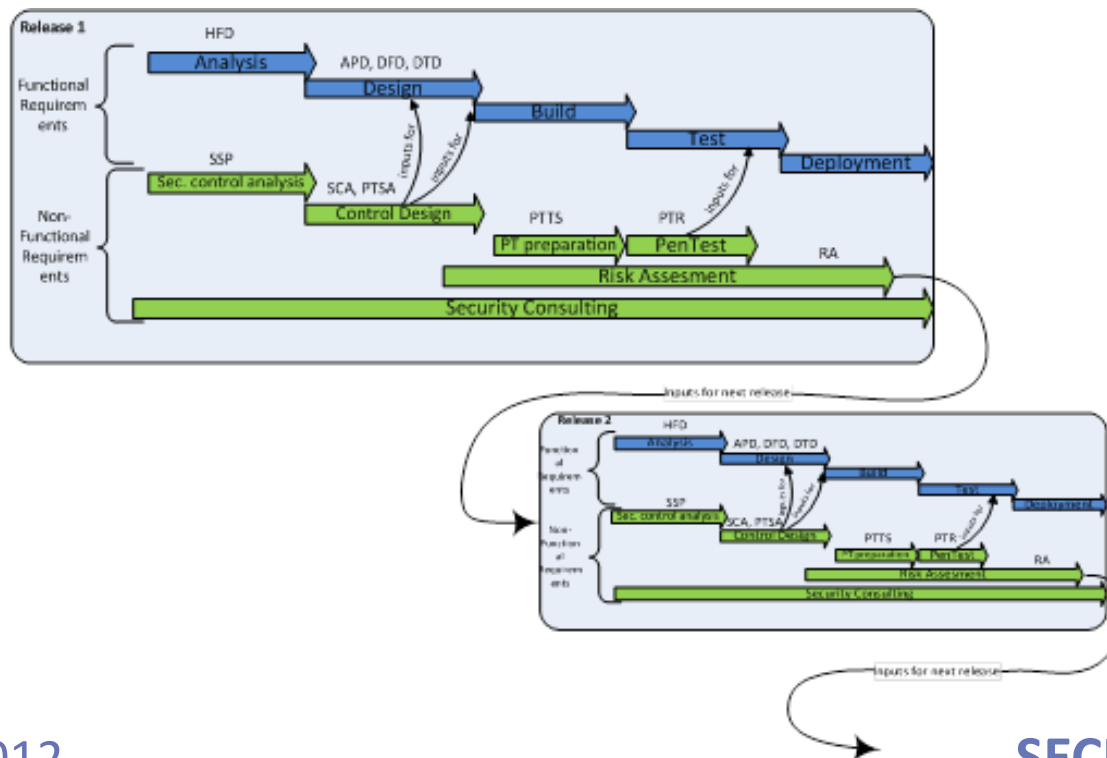
Metodiky, pokračovanie

- FIPS 200
 - Minimálne požiadavky na federálne informačné systémy
- NIST SP 800-30
 - Príručka riadenia rizík v IT systémoch
- NIST SP 800-53
 - Doporučené bezpečnostné opatrenia pre federálne informačné systémy
- NIST SP 800-64
 - Bezpečnosť vo vývojovom cykle systémov
- OWASP, OSSTMM
 - Testovanie webových aplikácií a infraštruktúry



Dokumenty a ich účel v projekte

- Metodický dokument
 - SQAP (Security Quality Assurance Plan)
 - Metodický dokument popisujúci úlohu a začlenenie bezpečnosti v projekte





Dokumenty, pokračovanie

- Architektonické dokumenty
 - SSP (System Security Plan)
 - Zoznam technických bezpečnostných opatrení
 - SCA (Security Control Architecture)
 - Architektonický dokument postavený na SSP. Detailne rozpracováva jednotlivé opatrenia na úrovni architektúry riešenia
 - SA (Security Architecture)
 - Detailný opis bezpečnostných vlastností Frameworku a celého riešenia



Dokumenty, pokračovanie

■ Testovacie

- PTSA (Penetration Tests Scope and Approach)
 - Metodický dokument popisujúci dva typy penetračných testov:
 - Interné projektové pre všetky releasy
 - Externé nezávislé pre releasy publikované do Internetu
- PTTS (Penetration Tests Testing Scenarios)
 - Detailné scenáre penetračných testov



Dokumenty, pokračovanie

- Analýza rizík
 - Vychádza z NIST SP 800-30
 - Vypracováva ju banka
 - Upravené metriky
 - Vybrané len niektoré hrozby z katalógu hrozieb
 - Upravená metodika hodnotenia rizika

The screenshot displays a risk assessment matrix with the following structure:

- Columns:** Threats, Vulnerabilities, Assets, and Risk Levels (Low, Medium, High, Very High).
- Rows:** A list of threats, including:
 - 1. Aggressive and/or malicious users (e.g., hackers, insiders, etc.)
 - 2. Malicious insiders (e.g., employees, contractors, etc.)
 - 3. Malicious outsiders (e.g., hackers, etc.)
 - 4. Malicious insiders (e.g., employees, contractors, etc.)
 - 5. Malicious outsiders (e.g., hackers, etc.)
 - 6. Malicious insiders (e.g., employees, contractors, etc.)
 - 7. Malicious outsiders (e.g., hackers, etc.)
 - 8. Malicious insiders (e.g., employees, contractors, etc.)
 - 9. Malicious outsiders (e.g., hackers, etc.)
 - 10. Malicious insiders (e.g., employees, contractors, etc.)
 - 11. Malicious outsiders (e.g., hackers, etc.)
 - 12. Malicious insiders (e.g., employees, contractors, etc.)
 - 13. Malicious outsiders (e.g., hackers, etc.)
 - 14. Malicious insiders (e.g., employees, contractors, etc.)
 - 15. Malicious outsiders (e.g., hackers, etc.)
 - 16. Malicious insiders (e.g., employees, contractors, etc.)
 - 17. Malicious outsiders (e.g., hackers, etc.)
 - 18. Malicious insiders (e.g., employees, contractors, etc.)
 - 19. Malicious outsiders (e.g., hackers, etc.)
 - 20. Malicious insiders (e.g., employees, contractors, etc.)
 - 21. Malicious outsiders (e.g., hackers, etc.)
 - 22. Malicious insiders (e.g., employees, contractors, etc.)
 - 23. Malicious outsiders (e.g., hackers, etc.)
 - 24. Malicious insiders (e.g., employees, contractors, etc.)
 - 25. Malicious outsiders (e.g., hackers, etc.)
 - 26. Malicious insiders (e.g., employees, contractors, etc.)
 - 27. Malicious outsiders (e.g., hackers, etc.)
 - 28. Malicious insiders (e.g., employees, contractors, etc.)
 - 29. Malicious outsiders (e.g., hackers, etc.)
 - 30. Malicious insiders (e.g., employees, contractors, etc.)
 - 31. Malicious outsiders (e.g., hackers, etc.)
 - 32. Malicious insiders (e.g., employees, contractors, etc.)
 - 33. Malicious outsiders (e.g., hackers, etc.)
 - 34. Malicious insiders (e.g., employees, contractors, etc.)
 - 35. Malicious outsiders (e.g., hackers, etc.)
 - 36. Malicious insiders (e.g., employees, contractors, etc.)
 - 37. Malicious outsiders (e.g., hackers, etc.)
 - 38. Malicious insiders (e.g., employees, contractors, etc.)
 - 39. Malicious outsiders (e.g., hackers, etc.)
 - 40. Malicious insiders (e.g., employees, contractors, etc.)
 - 41. Malicious outsiders (e.g., hackers, etc.)
 - 42. Malicious insiders (e.g., employees, contractors, etc.)
 - 43. Malicious outsiders (e.g., hackers, etc.)
 - 44. Malicious insiders (e.g., employees, contractors, etc.)
 - 45. Malicious outsiders (e.g., hackers, etc.)
 - 46. Malicious insiders (e.g., employees, contractors, etc.)
 - 47. Malicious outsiders (e.g., hackers, etc.)
 - 48. Malicious insiders (e.g., employees, contractors, etc.)
 - 49. Malicious outsiders (e.g., hackers, etc.)
 - 50. Malicious insiders (e.g., employees, contractors, etc.)
 - 51. Malicious outsiders (e.g., hackers, etc.)
 - 52. Malicious insiders (e.g., employees, contractors, etc.)
 - 53. Malicious outsiders (e.g., hackers, etc.)
 - 54. Malicious insiders (e.g., employees, contractors, etc.)
 - 55. Malicious outsiders (e.g., hackers, etc.)
 - 56. Malicious insiders (e.g., employees, contractors, etc.)
 - 57. Malicious outsiders (e.g., hackers, etc.)
 - 58. Malicious insiders (e.g., employees, contractors, etc.)
 - 59. Malicious outsiders (e.g., hackers, etc.)
 - 60. Malicious insiders (e.g., employees, contractors, etc.)
 - 61. Malicious outsiders (e.g., hackers, etc.)
 - 62. Malicious insiders (e.g., employees, contractors, etc.)
 - 63. Malicious outsiders (e.g., hackers, etc.)
 - 64. Malicious insiders (e.g., employees, contractors, etc.)
 - 65. Malicious outsiders (e.g., hackers, etc.)
 - 66. Malicious insiders (e.g., employees, contractors, etc.)
 - 67. Malicious outsiders (e.g., hackers, etc.)
 - 68. Malicious insiders (e.g., employees, contractors, etc.)
 - 69. Malicious outsiders (e.g., hackers, etc.)
 - 70. Malicious insiders (e.g., employees, contractors, etc.)
 - 71. Malicious outsiders (e.g., hackers, etc.)
 - 72. Malicious insiders (e.g., employees, contractors, etc.)
 - 73. Malicious outsiders (e.g., hackers, etc.)
 - 74. Malicious insiders (e.g., employees, contractors, etc.)
 - 75. Malicious outsiders (e.g., hackers, etc.)
 - 76. Malicious insiders (e.g., employees, contractors, etc.)
 - 77. Malicious outsiders (e.g., hackers, etc.)
 - 78. Malicious insiders (e.g., employees, contractors, etc.)
 - 79. Malicious outsiders (e.g., hackers, etc.)
 - 80. Malicious insiders (e.g., employees, contractors, etc.)
 - 81. Malicious outsiders (e.g., hackers, etc.)
 - 82. Malicious insiders (e.g., employees, contractors, etc.)
 - 83. Malicious outsiders (e.g., hackers, etc.)
 - 84. Malicious insiders (e.g., employees, contractors, etc.)
 - 85. Malicious outsiders (e.g., hackers, etc.)
 - 86. Malicious insiders (e.g., employees, contractors, etc.)
 - 87. Malicious outsiders (e.g., hackers, etc.)
 - 88. Malicious insiders (e.g., employees, contractors, etc.)
 - 89. Malicious outsiders (e.g., hackers, etc.)
 - 90. Malicious insiders (e.g., employees, contractors, etc.)
 - 91. Malicious outsiders (e.g., hackers, etc.)
 - 92. Malicious insiders (e.g., employees, contractors, etc.)
 - 93. Malicious outsiders (e.g., hackers, etc.)
 - 94. Malicious insiders (e.g., employees, contractors, etc.)
 - 95. Malicious outsiders (e.g., hackers, etc.)
 - 96. Malicious insiders (e.g., employees, contractors, etc.)
 - 97. Malicious outsiders (e.g., hackers, etc.)
 - 98. Malicious insiders (e.g., employees, contractors, etc.)
 - 99. Malicious outsiders (e.g., hackers, etc.)
 - 100. Malicious insiders (e.g., employees, contractors, etc.)



Podnet z praxe 1

- Podnet 1: Analýza rizík
 - Analýza rizík mala v prvom release meškanie
 - Návrhové dokumenty obsahovali málo informácií
 - V R1 bolo treba oponovať veľké množstvo návrhových dokumentov
 - Prijaté protiopatrenia
 - AR pre R1 bola dokončená dodatočne
 - V návrhu R2 boli použité čiastočné výsledky AR pre R1
 - Bonusy
 - Analýza rizík zohľadnila výsledky penetračného testu



Podnet z praxe 2

- Podnet 2: Security Architecture
 - Dokument mal byť vstupom do analýzy rizík
 - Pripraviť ho mohol len úzko špecifikovaný tím, ktorý mal prioritnejšie úlohy
 - Prijaté protiopatrenia
 - Žiadne
 - Dôsledky
 - Bezpečnostné chyby vo Frameworku sa objavajú až vo fáze testovania a penetračného testovania



Podnet z praxe 3

- Podnet 3: Security Control Architecture
 - Obrovský rozsah
 - R1 a R2 obsahujú takmer všetky bezpečnostné opatrenia spoločné aj pre ďalšie releases
 - Prijaté protiopatrenia
 - Nutná redukcia (len Technical Controls, vypustené politiky x-1)
 - Prioritizovanie (len P1 v R1 a ostatné do R2 a ďalších)
 - Po porade s vývojovým tímom
 - Bonusy
 - Rozpracovávali sme len najdôležitejšie opatrenia



Podnet z praxe 4

- Podnet 4: Bezpečnostné konzultácie a revízie návrhových dokumentov
 - V jednotlivých návrhoch sa začali nekontrolovaným spôsobom šíriť rôzne šifrovacie a iné heslá, ktoré by v produkcii boli takmer neudržiavateľné
 - Bezpečnostné operácie boli v rôznych častiach projektu implementované rôzne
 - Začal sa rozmáhať živelný spôsob migrácie údajov do nového systému



Podnet z praxe 4, pokračovanie

- Prijaté protiopatrenia
 - Bol navrhnutý a implementovaný mechanizmus zjednocujúci všetky kryptografické operácie
 - Bol zavedený jednotný mechanizmus na autentifikáciu, autorizáciu, riadenie prístupu a auditovanie
 - Pomohli sme správne navrhnuť a implementovať bezpečný spôsob migrácií citlivých údajov do nového riešenia.



Podnet z praxe 5

- Podnet 5: Penetračné testovanie
 - Predpoklady (asi naivné)
 - Stabilná aplikácia
 - Produkčná konfigurácia systémov a infraštruktúry





Podnet z praxe 5, pokračovanie

- Výsledky penetračných testov
 - Celkový prehľad:
 - 2 x Critical
 - 5 x High
 - 2 x Medium
 - 6 x Low
 - Zraniteľnosti na infraštruktúre a systémoch
 - Našli sa zraniteľnosti v aplikácii



Podnet z praxe 5, pokračovanie

- Navrhnuté protiopatrenia
 - Spraviť bezpečnostné školenie pre jednotlivé tímy
 - Do R2 doplniť hardening systémov a infraštruktúry
- Bonusy
 - Zraniteľnosti boli objavené ešte počas R1
 - Odstránia sa v R1 alebo R2, čo sú neverejné releasy



Podnet z praxe 6

- Podnet 6: Bezpečnosť pri vývoji a implementácii
 - Požiadavky na vzdialený vývoj a vzdialený prístup do prostredí
 - Zdieľanie a preposielanie projektových dokumentov
 - Práca mimo priestorov a zdrojov banky
 - Prijaté protiopatrenia
 - Definovali a formalizovali sme pravidlá a politiky na prácu a prístup k informačným aktívam banky
 - Zabezpečili sme povinné oboznámenie sa dodávateľa s týmito pravidlami
 - Výhody
 - Jasné pravidlá s dodávateľom
 - Bezpečnostné povedomie dodávateľa sa dá preukázať a je na úrovni interného zamestnanca



Podnet z praxe 7

- Podnet 7: Bezpečnostné požiadavky a vedľajšie náklady
 - V čase analýzy sa môže ukázať potreba implementovať dodatočné systémy, alebo riešiť celé projekty
 - Môžu mať významný dopad na rozpočet projektu, alebo na bezpečnosť riešenia
 - Protiopatrenia
 - Súčasťou prípravných prác bola analýza rizík
 - Bonusy
 - Infraštruktúrne a podporné projekty boli už súčasťou business case na Multichannel
 - Minimalizácia dodatočných vyvolaných nákladov na implementáciu bezpečnosti počas behu projektu



Záver

- Prax už po niekoľkých mesiacoch behu projektu ukázala, že aktívne zapojenie bezpečnosti do SDLC je prínosom
 - Veľa chýb a problémov bolo odstránených vo fáze návrhu
 - Časté testovanie je viac na osoh ako na škodu, aj keď komplikuje projektové plánovanie
- Konzultácie Security tímu výrazne zvýšili bezpečnostné povedomie v ostatných tímoch projektu

Děkujeme za pozornost.

Juraj Porubčan, AEC
Martin Žemlička, VUB

