Izzivi varovanja aplikacijskih nastavitev in infrastrukturnih podatkov

Mitja Lenič

NKBM d.d.

OWASP
Education Project

Copyright 2007 © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

Zakaj smo tukaj?

- Kompleksni sistemi
- Popolna varnost je iluzija
- Grožnje na vsakem koraku
- Vsak sistem ima ranljivosti
- Širjenje dobre prakse

Vsebina

- Varovanje informacij
- Ocena tveganj
- Močno overjanje uporabnika
- Aplikacijske nastavitve
- Dnevniki in revizijska sled
- Povzetek

Varovanje informacij

- Varovanje informacij je proces
- Izhodišče standardi ISO/IEC27000
- Model „Načrtuj – Stori – Preveri – Ukrepaj“
- Neprenehno spremljanje in izvajanje

Cilji varovanja informacij

- Zaupnost
  - Ščitenje občutljivih informacij pred nepooblaščenim dostopom
- Neoporečnost
  - Varovanje točnosti in popolnosti informacij in programske opreme
- Razpoložljivost
  - Zagotavljanje, da so informacije in storitve na voljo uporabnikom

Obsega varovanja (OWASP)

- Informacijski viri
- Vendar ne pozabiti na
  - Ljudi,
  - Zgradbo in prostore,
  - Energija,
  - Opremo,
  - Komunikacijske povezave
  - ....

Ocena tveganj

- Identifikacija
  - Groženj
  - Ranljivosti
- Ocena
  - Verjetnosti dogodka
  - Kritičnost/vpliv

$$\text{Tveganje} = \left(\frac{\text{Grožnje} \times \text{Ranljivosti}}{\text{Kontrole, ukrepi}} \right) \times \text{Vrednost}$$

Identifikacija ranljivosti (na grožnje)

- Ranljivost je posledica pomanjkanja kontrol
- Zadostuje samo en izpostavljen šibek člen
- Vsak informacijski sistem je ranljiv
- Kako identificirati ranljivosti?

Potencialna mesta ranljivosti IS

Ocena tveganj v programski opremi

- Kako oceniti tveganje?
- Več 100 programskih komponent za delovanje ene aplikacije
- Informacijski sistem je skupek aplikacij
- Dovolj je ena (kritična) ranljivost
- Nestabilno stanje
- Neprenehne spremembe programske opreme
  - Nove funkcionalnosti,
  - Ukinitev/sprememba obstoječih
  - Kratek cikel razvoja rešitev

Zmanjševanje tveganj

- Različni (tehnični) ukrepi
- Procesne kontrole
- Varnostne politike
- Upravljanje sprememb
- Sledljivost
- Preizkušanje delovanja programske opreme (QA)
- Pregledovanje rešitev
- Uporaba nestandardnih rešitev?

Politika razvoja programske opreme

- Nadzorovan proces sprememb
- Kontrole v procesu razvoja
- Več okolij za različne namene
  - Razvoja
  - Testiranja
  - Produkcije
- Enostaven prehod komponent med okolji

Izpostavljenost napadom

- Pomemben je izpostavljen profil
- Potreben trud s strani napadalca
- Ekonomičnost napada
- Napad na programsko infrastrukturo

Programska infrastruktura

- Zelo širok pojem
- Podpora poslovni programski opremi
- Pospeši in poenostavi razvoj
- Zviša kakovost rešitev

Primeri programske infrastrukture

- Imeniške storitve
- Baze podatkov
- Aplikacijski dnevniki
- Overjanje
- Nastavitvene datoteke
- Revizijske sledi
- Knjižnice
- ....

Overjanje uporabnika

- Prvi korak pri dostopu do zaupnih informacij
- Avtorizacija na osnovi overitve
- Zelo zanimiva točka napada
  - Regularni dostop do aplikacije
  - Napad se lahko izvede izven sistema
  - Težka identifikacija zlorabe

Overjanje z geslom

- Neprimerna hramba
- Šibka gesla

Slabosti gesel

Overjanje uporabnika (2)

- Overitveni elementi
  - Vedeti (uporabniško ime, geslo)
  - Imeti (certifikat, fizično sredstvo)
  - Biti (vzorci, biometrične informacije)
- Grožnje
  - Nezadostno varovanje overitvenih elementov
- Napadi
  - Socialni inženiring
  - Uganitev overitvenih elementov (groba sila)
  - Prestrezanje overitvenih elementov
  - Kraja (overjene) seje

Zakonodaja (varnostni problem)

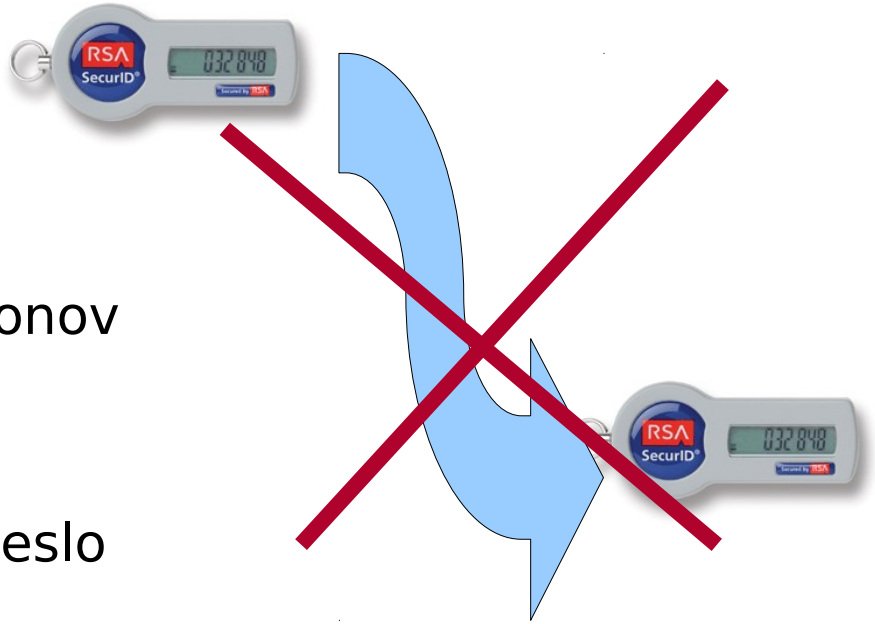
- Zadostujeta dva elementa
  - Imeti certifikat (nefizično sredstvo) izdan s strani CA
  - Vedeti geslo certifikata
- Informacija o identiteti se enostavno razmnoži
- Enostavno posredovanje tretji osebi
  - Računalniški virus/trojanec
  - Problem pridobitve gesla?
  - Lažna spletna stran (DNS spoofing, datoteka hosts)

Močno overjanje

- Uporabiti vsaj dva overitvena elementa
- Vedeti in imeti
  - Imeti sredstvo, ki ga je težko kopirati (ponarediti)
- Biometrija preko spleta?
- Uporabiti več kanalov
  - Splet
  - Papir
  - Telefon
  - (E)Pošta

Močno overjanje (2)

- Imeti nekaj, kar je težko kopirati
- Imeti fizično sredstvo
  - Npr. generator začasnih žetonov SecurID
- Kombinacija overjanj
  - Vedeti uporabniško ime in geslo
  - Vedeti PIN in imeti fizični generator žetonov
  - Potrditev po neodvisnih kanalih
- Visoki stroški sistema
- Težavnost uporabe



Programske nastavitve

- Vsaka aplikacija jih ima
- Vsebujejo informacije o okolju, potrebni infrastrukturi in (poslovnih) nastavitvah
- Tipična mesta:
  - Spremenljivke okolja
  - Parameter ukazne vrstice
  - Register
  - Nastavitvena datoteka
  - Baza podatkov (kako do baze?)
  - Imeniške storitve
- Različni formati
- Nestandardne lokacije

Vloga programskih nastavitve

- Parametrizacija rešitve
  - Poveča fleksibilnost
- Omogočajo nespremenljivost komponente
- Enostaven in transparenten prehod med okolji
- Kritičen vpliv na delovanje rešitve
- Dostopnost občutljivih informacij o infrastrukturi

Varnost programskih nastavitev

- Vsebujejo občutljive informacije
- Tarča napadalcev
- Privzeti računi in gesla
- Privzete (odvečne) funkcionalnosti
- V praksi sistemi z več 100 aplikacijami/storitvami
- Problem upravljanja nastavitev
  - Večje tveganje človeške napaka

Slaba praksa

- Fiksno „zapečene“ nastavitve
  - Izvorna koda, izvedljivi modul
  - Omejitve dostopa
  - Onemogočen prehod med okolji
  - Težavno upravljanje in spreminjanje nastavitev (npr. menjava gesel)
- „Javno“ dostopne nastavitve
  - http://demo.si/../../config.php
  - http://demo.si/app/app.properties
- Razpršenost nastavitev

Dobra praksa

- Standardni način shranjevanja
- Ločevanje odgovornosti in procesnih vlog
- Centralno upravljanje nastavitev
- Šifriranje občutljivih informacij
- Varnostni pregledi nastavitev

Dnevniki in revizijska sled

- Zakonodajne in regulatorne zahteve
  - ZVOP
- Politike sledenja delovanja sistemov
  - Napake v delovanju sistema
  - Pomoč pri iskanju napak
- Pomembna sled za rekonstrukcijo aktivnosti
  - Sistemski dogodki
  - Uporabniki s posebnimi privilegiji
- Forenzični dokazi
- Več mešanih aspektov
  - Ločeni dnevniki
- Dolgotrajna hramba

Osnovne lastnosti dnevnika

- Avtentičnost dnevnika
  - Vnosov ni mogoče spreminjati/brisati
  - Vnosa ni mogoče ponarediti
- Strukturirana vsebina
- Spremljanje vsebine dnevnika
  - Delovanje sistemov
  - Spremljanje performanc
  - Zaznava vdorov
- Osnova za avtomatsko obveščanje

Vsebina aplikacijskih dnevnikov

- Datum in ura nastanka dogodka (UTC)
- Izvorni sistem
- Vrsta dogodka
- Mesto dogodka
- Identifikacija (poslovnega) procesa
- Izvor dogodka
- Uporabniško ime
- Informacije o dogodku

Način zbiranja dnevnikov

- Porazdeljeni dnevniki
  - Vsaka aplikacija svoj dnevnik
  - Centralni sistemski dnevnik
- Izdvojen centralni sistem
  - Pošiljanje dnevnikov na centralni sistem
  - Spremljanje sporočil na poslovnem vodilu

Porazdeljeni dnevniki

- Problem spremljanja dnevnikov
- Težka rekonstrukcija porazdeljenih dogodkov
- Možnost manipulacije s strani uporabnikov s posebnimi privilegiji

Izdvojitev sistema beleženja dnevnikov

- Neodvisni sistem za zapis dnevnikov
- Visoka stopnja (tehničnega) varovanja
- Možnost spremljanja uporabnikov s posebnimi privilegiji
- Visoka stopnja razpoložljivosti
- Performančno problematično
- Ena točka izpada

Povzetek

- Veliko groženj
- Vsaka (programska) oprema ima ranljivosti
- Močno overjanje je nuja za varno poslovanje
- Nastavitve aplikacij so tipično slabo varovane
- Dnevnik in revizijska sled za forenzično analizo