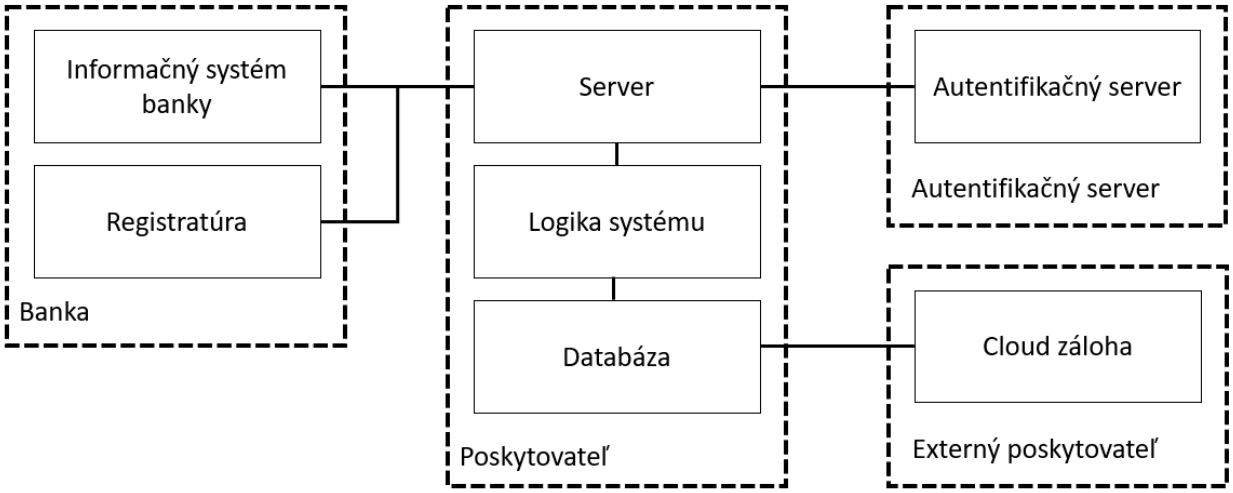
UPB – Zadanie 0

STRIDE, DFD, hrozby



Informačný systém banky – Softvér, ktorý spravuje bankové účty, prevody, informácie o majiteľoch účtov, etc.

Registratúra – Elektronická registratúra, ktorá zaznamenáva všetky pohyby na účtoch ako aj platby zákazníkov

Server – Server aplikácie (backend)

Logika systému – Sprostredkovateľská vrstva, ktorá ma na starosti komunikáciu medzi serverom a databázou

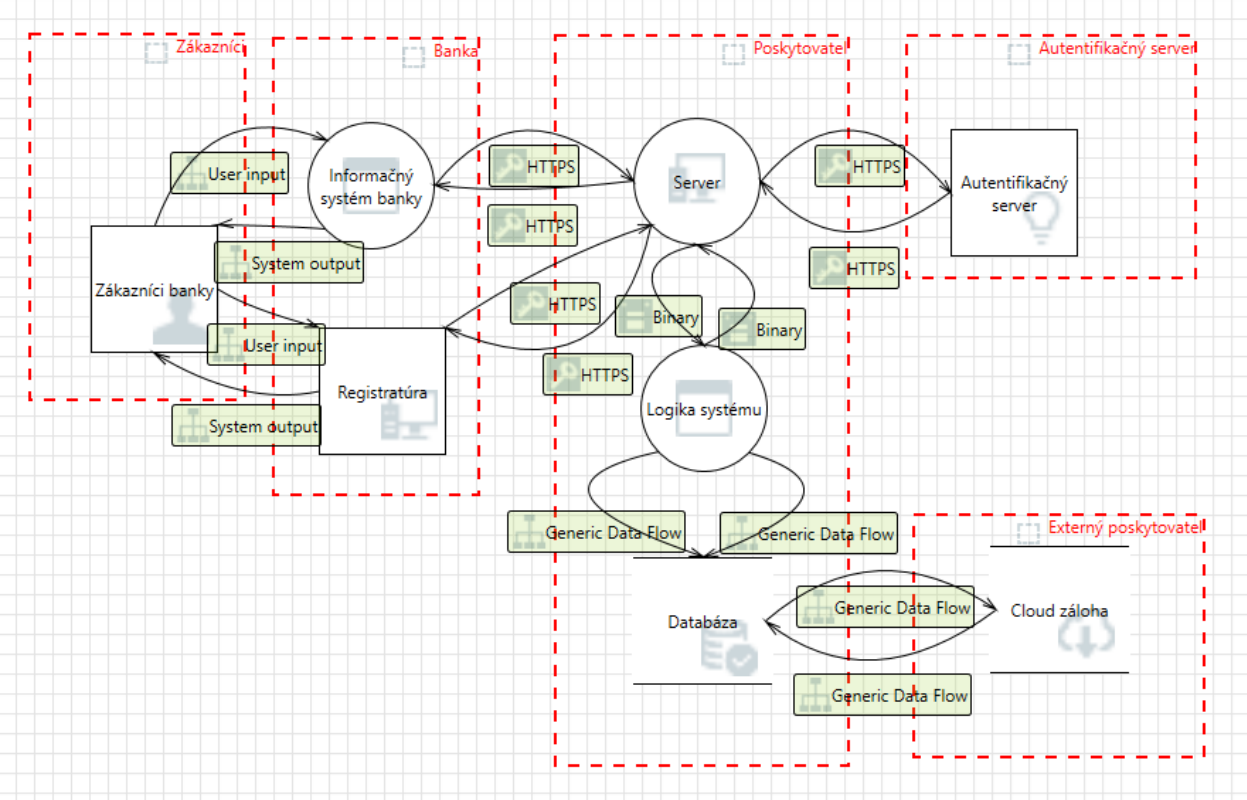
Databáza – Úložisko všetkých údajov z informačného systému

Autentifikačný server – Bezpečnostné overenie identity používateľov

Cloud záloha – záloha databázy na cloudovom úložisku

Hrozby nie sú všetky, zbytok je v .html súbore

Trust boundaries



Zákazníci – Zákazníci, ktorí už majú v banke vytvorený účet a využívajú systém

Banka – Systém sa nachádza v hlavnej pobočke danej krajiny

Poskytovateľ – Systém sa nachádza v najbližšej pobočke poskytovateľa, tak ako aj úložisko

Autentifikačný server – Bezpečnostné overenie identity používateľov

Externý poskytovateľ – Databázový server určený na uchovávanie histórie prevodov starších ako určité obdobie a taktiež zálohu aktuálnej databázy beží u externého poskytovateľa

Hrozby nie sú všetky, zbytok je v .html súbore

Hrozby

***S*poofing** nastáva vtedy keď proces alebo entita je niečo iné ako o sebe tvrdí, napríklad nahradenie procesu, súboru, stránky alebo sieťovej adresy. Dajú sa tak získať iné výhody alebo zmena identity s cieľom získať vyššie oprávnenia v systéme.

***T*ampering** je čin, pri ktorom sa menia bity v bežiacom procese, dajú sa tak zmeniť údaje medzi dvomi bežiacimi procesmi. Modifikácia dát umožňuje napríklad prihlásenie sa bez potreby účtu alebo poškodenie systému.

***R*epudiation** znamená zamietanie používateľa že niečo vykonali v systéme, napríklad pokus o prihlásenie do cudzieho účtu alebo odstránenie súboru. Jednoduchým riešením je zavedenie LOGs do systému.

***I*nformation disclosure** nastáva vtedy, keď informácia dokáže byť čítaná niekým kto by na ňu nemal mať prístup.

***D*enial of service** nastáva vtedy, keď proces alebo dátové úložisko nie je schopné vykonať všetky požiadavky. Môže dôjsť k zahlteniu systému alebo pádu.

***E*levation of privilege** nastáva vtedy, keď niekto získa vyššie oprávnenia ako by mal mať pomocou implementačného bugu.

Hrozby nie sú všetky, zbytok je v .html súbore

Zoznam hrozieb

Spoofing

- Spoofing of Source Data Store Databáza
- Spoofing of Destination Data Store Cloud záloha
- Spoofing of Source Data Store Cloud záloha

Riešenie pre všetky tri: *Využitie autentifikácie pre kvalitnejšiu identifikáciu rozdielnych entít.*

Tampering

- Cross Site Scripting

Riešenie: *Ošetriť vstupy od používateľov.*

- Potential SQL Injection Vulnerability for Databáza

Riešenie: *Ošetriť vstupy od používateľov.*

- Server Process Memory Tampered

Riešenie: *Zníženie počtu dát, ku ktorým sa pristupuje pomocou pointrov, pridanie validácie prichádzajúcich dát.*

Repudiation

- Data Store Denies Cloud záloha Potentially Writing Data
- Potential Data Repudiation by Server
- External Entity Autentifikačný server Potentially Denies Receiving Data

Riešenie pre všetky tri: *Spomínané logovanie aktivít.*

Information disclosure

- Data Flow Sniffing

Riešenie: *Šifrovanie dát.*

Denial of service

- Data Store Inaccessible

Riešenie: *Zabezpečenie dátového servera pred útokmi alebo dočasné núdzové prepnutie záložného cloud úložiska v prípade núdze.*

- Potential Excessive Resource Consumption for Logika systému or Databáza

Riešenie: Využíval by som deadlock pri zdrojových požiadavkách.

Elevation of privilege

- Elevation Using Impersonation

Riešenie: *Využitie validačných nastavení pomocou X.509 na tokenoch.*

- Server May be Subject to Elevation of Privilege Using Remote Code Execution

Riešenie: *Oddelenie servera pre vykonávanie kódu od zvyšku systému.*

Hrozby nie sú všetky, zbytok je v .html súbore