Milyen veszélyeket hozhatnak

az elektronikus csatornákon folyó kommunikációra

a SOA alapú fejlesztések?

sőt:

SOA veszélyek - elhárítási feladatok az intézményben

Dr. Szenes Katalin CISA, CISM, CGEIT
szenes.katalin@nik.bmf.hu

Budapesti Műszaki Főiskola
Neumann János Informatikai Kar
Alkalmazott Informatikai Intézet

SOA - alk.fejlesztés veszély elhárítás elektronikus csatorna I.

fejlesztő :
akinek az Informatikai részéről feladata van az alkalmazások fejlesztésében

- a szereplők és a préda
- ötletadók: szakmai szervezetek
- védelmi megoldások' 2006
- "informatikusi" feladatok alkalmazásokat fenyegető veszélyek elhárításában, DE..
- az intézményi infokommunikációs rendszer integrált védelme
  - az informatikai biztonság 3 pillére
- mit várunk a szervezeti pillértől?
- és a szabályozástól?

És a technikától? **. / .**

SOA - alk.fejlesztés veszély elhárítás elektronikus csatorna II.

És mit várunk a technikától?

- az elektronikus csatornás alkalmazások kommunikációs útja
- mi köze a SOA architektúrának az elektronikus csatornákhoz?
- alkalmazásfejlesztési zavarok
- a kommunikáció rétegei infrastruktúrális elemenként
  - szereplők: emberek- mi, belsők, és ők, az ügyfelek
  - fizikai szint - itt szereplők a "fejlesztői" körből?
  - adatok, adatbázisok

  szereplők itt: elsősorban a programtervezők, programozók
- a kommunikáció infrastruktúrális elemeinek implementációja és karbantartása itt az üzemeltetés az illetékes
- a kommunikáció - információ - útja
- a kommunikáció infrastruktúrális elemeinek implementációja és karbantartása itt az üzemeltetés az illetékes
- bölcs tanácsok
- magyarázatok

A szereplők

- támadók
  - alkalmazott — haszon
  - partner — tudatlanság
    - szerződő fél: vevő, szállító — rosszindulat
  - versenytárs
  - hacker, cracker, diák, — szórakozás
  - bűnöző, kém, ügynök, terrorista — *mi a sorrend?*
- védők
  - munkaköri kötelességből
  - szakmai szervezetek, közösségek tagjai
  - és: a legjobb szakmai gyakorlat egyéb követői
- ötletadó
  - szintén: a szakmai szervezetek, internet, stb.

és a préda

mit lehet szerezni?
adatokat
- személyazonosságot
- titkokat
- előnyöket - másoknak hátrányokat, pl.
  - pénzt
  - versenytársat tönkretenni

célpont:
- magánemberek
- cégek
- állam

ötletadók: a szakmai szervezetek

- ISACA - Information Systems Audit and Control Association - CISA, CISM Manual
- ITGI - IT Governance Institute - ISACA - COBIT
- ISO - International Standards Organization 27000-es család, stb.
- nem szakmai, de hasznos: USA állami, egyéb források

"internetesek"
- W3C - World Wide Web Consortium

és (majdnem) SOA specifikusak
- OASIS - Organization for the Advancement of Structured Information Standards - www.oasis-open.org -e-business szabványok, non-profit
- OWASP - Open Web Application Security Project www.owasp.org - megbízható alkalmazások fejlesztése

Védelmi megoldások' 2006 (majdnem)

- rendezett és ellenőrzött fejlesztési munka
- sérülékenység befoltozása kívülről technikai eszközökkel
- csalásfelderítő alkalmazások futtatása - infrastruktúrális elem - szintenként

az elkészült mű próbája:

- tesztelés
- környezeti / támadás szimuláció
- szkennelés

Milyen legyen a védelem? - 2006-ban

milyen?	*mit?*	*hol?*
proaktív		
mindig figyelő	➔ adatok	➔intézményi hálózatban
módszeres		
összes komm. rétegre	➔ szolgáltatások	
szolg. **teljes életciklusára**		➔céghatáron túl is

"informatikusi" feladatok alkalmazásokat fenyegető veszélyek elhárításában, *DE...* az intézményben mindenkinek van feladata

"informatikus":

- rendszerszervező
  - felmérés
  - egyeztetés
  - rendszerterv
- programozó
  - a program készítésekor: ellenőrzési célok az adott eszközhöz
  - a specifikumok kihasználása, pl. osztály - típuskezelés
  - hibakezelés - fátum: pl. kifogyott a papír
  - kivétel kezelés - mi hibánk: pl. felületes típusellenőrzési gyakorlat
- tesztelő
- üzemeltető + ! incidensek kezelése

de: az egész intézménynek vannak feladatai: a(z elkötelezett !) vezetőségnek

- üzletnek
- támogatóknak

az intézményi infokommunikációs rendszer integrált védelme
- az informatikai biztonság 3 pillére

szervezet	*szabályozás*	*technika*
struktúra - SZMSZ	IBSZ	az IT infrastr. elemek:
jogok / felelősségek	- feladatok	- topológiája, elrendezése
elszámoltathatóság		
munkakörök	- jogosultságok	- implem., konfigurálás
kötelességelhatárolás	- naplózás	- karbantartás, felügyelet
tev. felügyelet	internetezés	
oktatással a	levelezés	védelmi rendszerek:
-tudatosság fejlesztése	adatvédelem	tűzfal, ID(P)S, ...
törvényekhez,	rendszerfejlesztési folyamat	
-iparághoz compliance	szabályozása (SDLC - ISO/IEC 12207	
	Informatika. Szoftveréletciklus-folyamatok)	

Dr. Szenes SOA - fejlesztés - elektronikus csatornák 10

mit várunk a szervezeti pillértől? - és kinek kell megcsinálnia?

követelmények	*szervezeti egységek*
rendelkezésre állás	legfelső vezetés
integritás	informatika
bizalmasság	fizikai,
hozzáférésvédelem	logikai IT biztonság (független kell legyen!)
jogi, hatósági megfelelés	belső ellenőrzés
funkcionalitás	jogi részleg
legjobb szakmai gyakorlat	
	külső audit

segítség:
- IT irányító bizottság
- kockázatkezelési segédszervezet

Dr. Szenes SOA - fejlesztés - elektronikus csatornák 11

mit a szabályozástól? - és ki írja ezeket a szabályzatokat?

Szabályozás, folyamatok:

rend, kötelességelhatárolás,

jogosultságok:
- hozzáférés ⇔ munkához szükséges
- ki / hol / mit / milyen jogosultsággal / mikor / hogyan / miért
- kell történeti jogosultságkezelés (Active Dir. info kevés)

oktatás:
- kapcsolatfelvétel csak óvatosan
- idegeneknek meggondolt felvilágosítás

rend a számítástechnikai alkalmazások fejlesztésében
változáskezelés, dokumentáció, üzletmenet folytonosság

Dr. Szenes SOA - fejlesztés - elektronikus csatornák 12

a 3. pillér

és mit várunk a technikától?

veszély:
a kommunikáció útja szerint — intézmény - ügyfél között
infrastruktúrális elemek szerint — elemenként
a kommunikáció eszközkészlete szerint — pl. http(s), xml

poén előre -
védelem:
megakadályozó / vizsgálati / kárenyhítő ("ellenőrzési") intézkedések
rendezett - tervezett fejlesztés
jogosultságkezelés, változáskezelés, DOKUMENTÁCIÓ

az elektronikus csatornás alkalmazások kommunikációs útja

intézmény és külső partner között:
- intézményi hálózat - intézményi informatika felelőssége
- külvilág - mindenki felelőssége,
  de elsősorban az alkalmazás felhasználójáé, az ügyfélé

részletek:
- legbelső, legfontosabb rendszerek
  bizalmas, fontos ➔ kihasználható ügyfél-, partner-, dolgozói, stb. adatok
- középső perimeter
  - a legbelső perimetertől és a legkülsőtől is !
    elválasztandó elektronikus csatorna és egyéb **!** feldolgozások,
  - távoli bejelentkezés fogadása, stb.
- esetleges további perimeterek
- a külvilágtól, "azaz az internettől" elválasztó perimeter
  elektronikus csatornás alkalmazásnál itt fontos védendő elem:
  a webszerver(ek) - a mögöttes adatbázisok beljebb lehetnek

mi köze a SOA architektúrának az elektronikus csatornákhoz?

- front-end: üzleti alkalmazások belépési pontja
- ➔ a "SOA" az alkalmazott "belépési pontja" lesz
- ➔ üzleti szakterületi alkalmazottak jogosultságát itt lehet kezelni

- csatorna kommunikáció:
  a legbelső rendszertől az intézményi hálózaton kívüli ügyfélig
  ➔ része a SOA-n belüli kommunikáció is
  ➔ a csatornára vonatkozó követelményeknek érvényesülnie kell(ene)

mi lehet probléma? . / .

mi köze a SOA architektúrának az elektronikus csatornákhoz?

baj viszont, ha:
- ellenőrizetlenül - ismeretlenül hívnak az üzleti rendszerek szolgáltatásokat a front-end-ből
- *ellenőrizetlenül* (azaz nem üzleti igény) nyílt, nem titkosított a kommunikáció
- rendezetlen az alkalmazásfejlesztés, és így a csatornás alkalmazásé is

ez mint alkalmazásfejlesztési probléma

alkalmazásfejlesztési zavarok

a számítástechnikai alkalmazások fejlesztése

életciklus, majd a fázisok teendőinek meghatározása	nem tudni: kinek, mikor, mi, ... a feladata mi van kész, és mi nincs, egyáltalán, hány %-ra kész?
teszt elés felelőseinek, módjainak meghatározása	funkcionalitás sérülése +! sérülékeny termék
új módszerekről álmodunk, de nem vagyunk még felkészülve	- " -
SOA, kapkodva	- " -

SOA - web-szolgáltatások sérülékenységei + hagyományos alkalmazási sérülékenységek:

a kommunikáció rétegei - infrastruktúrális elemenként - szereplők: emberek mi, belsők, és ők, az ügyfelek

1. réteg: az emberek - a szereplőink
dolgozók + ügyfelek ill. belülről + kívülről

veszély:

intézményben:
- social engineering
- egyedi felhasználóknak való kiszolgáltatottság
- és a szervezeti problémák

ügyfélnél:
- saját ostobaság
- phishing
- történetek
- adatkérő e-mail egy szolgáltató nevében
- "ingyenes" filmek, képek, pornó, játék, stb.
- web oldal hamisítás, stb.

a kommunikáció rétegei - infrastruktúrális elemenként - szereplők: emberek mi, belsők, és ők, az ügyfelek

védelem:
az intézményi oldalon:

szervezeti pillér
- tevékenységek pontos definíciója & felügyelete, kötelességelhatárolás,
- többi szervezeti pilléri elvárás

szabályozási pillér: teendők pontos és világos leírása
! ide tartozik a rendszerfejlesztési folyamat
- felhasználói leírás - üzleti szakterület
- üzemeltetési utasítás - informatikai szakterület
- többi szabályozási elvárás

ügyfél oldal: **. / .**

a kommunikáció rétegei - infrastruktúrális elemenként - szereplők: emberek mi, belsők, és ők, az ügyfelek

az ügyfél oldalán -
is van feladata az intézményi Informatikának:

- PIN kód, token, SMS, stb
- ügyfél oktatása:
  - patch
  - vírusvédelem, stb..
- ne bízzunk a tőlünk már letöltött kliensben ➔ szerver oldali ellenőrzések

miről van szó?
kliens: az a program, amit az ügyfél használ, a PC-jén
- otthon
- internet kávézóban,
- stb.

szerver: az, ami a klienssel tartja a kapcsolatot
- egy középső perimeterben (ld. komm. útja) kell elhelyezni, és
- ellenőrzéseket kell definiálni - milyeneket, pl.?

a kommunikáció rétegei - infrastruktúrális elemenként - szereplők: emberek mi, belsők, és ők, az ügyfelek

szerver oldali ellenőrzések **pl. elég gyakori a Java program** de más eset is hasonló
- megtervezett típuskezelés
- megtervezett kivételkezelés
- adatbeviteli ellenőrzések
  (Dashöfer - Informatikai biztonsági kézikönyv / COBIT)

hasznos alkalmazási ellenőrzési célok:
- 1. A forrásadatok előkészítése és hitelesítése
- 2. A forrásadatok összegyűjtése és bevitele
- 3. Pontossági, teljességi és hitelességi ellenőrzések
- 4. A feldolgozás sértetlensége és helyessége
- 5. Az output felülvizsgálata és a legjobb szakmai gyakorlat szerint való kezelése, az adatok egyeztetése. Hibakezelés
- 6. A tranzakciók sértetlensége és hitelessége

saját:
- 7. A közlekedő adatok bizalmassága

ezekhez kellenek ellenőrzési intézkedések

a kommunikáció rétegei - infrastruktúrális elemenként - fizikai szint
- itt szereplők a "fejlesztői" körből?

2. réteg: a fizikai
erre szabályzatot a rendszerszervezők írnak - jó esetben
- az egész épület
- a gépterem
- dokumentumok, bármilyen közegen, főleg:
- a nyomtatványok – a profi is kukázik

fizikai biztonsági védelem:
- ajtók zárva tartása
- kártya / kulcs őrzése
- piggy – backing megakadályozása
- ajtónyitó kód bizalmas kezelése
- idegenek kikérdezése
- adattárolók ügye – az adat különféle állapotaiban!
- laptop, mozgatható periféria, pl. USB-t, stb. ki/be vinni/hozni

a kommunikáció rétegei - infrastruktúrális elemenként - adatok, adatbázisok
szereplők itt: már *előtérben* a programtervezők, programozók

3. réteg: az adatok - adatbázisok - mi érheti az adatot?
- másolás, lopás
- törlés, egyéb rongálás
- módosítás

és miért, mi volt a baj?
néhány példa:
/1 SQL injection - oka:
ellenőrizetlen adatok inputja, pl.
- web oldalon a szövegdobozba
- ügyfél PC-n futó Java klienstől az intézményi Java szerverhez

eredménye:
- értékes info-k lekérdezése, felülírása
- új felhasználók felvétele
- jelszavak kiküldése mail-ben a támadónak, stb.

a kommunikáció rétegei - infrastruktúrális elemenként - adatok, adatbázisok
szereplők itt: elsősorban a programtervezők, programozók

/2. cross-site scripting - oka:
beolvasunk ellenőrizetlen adatot,
ami rosszindulatú Java script,
ezt a támadó web oldalon kiíratja, végfelhasználó beolvassa, gépe végrehajtja

/3. HTML paraméterek rosszindulatú módosítása - oka:
ellenőrizetlen paraméterek beolvasása HTML formokból
és ezek kerülnek be HTTP request-be

/4. URL módosítás - oka:
a támadó módosítja az URL string-et, és így juttatja be saját adatát
a védendő adatbázisba

stb.

a kommunikáció infrastruktúrális elemeinek implementációja és karbantartása itt az üzemeltetés az illetékes

4. réteg: az infrastruktúrális elemek karbantartása - ezt az üzemeltetéstől várjuk persze

mi a sérülékeny:

- operációs rendszerek
  - kliensfarm
  - szerverfarm
  - hálózati eszköz - switch, router
  - védelmi eszköz
    - tűzfal
    - IDS / IPS
  - web szerver
  - célgép
    - ATM
    - sorszámosztó, stb,
- adatbázisok

a kommunikáció infrastruktúrális elemeinek implementációja és karbantartása itt az üzemeltetés az illetékes

az infrastruktúrális elemek tipikus hiányosságai,
amelyek sérülékenységet okoznak:

operációs rendszer:

- felesleges szolgáltatások - hardening kell
- elavult verziók
- rossz konfiguráció
- jogosultsági problémák:
  - gyári jelszavak változatlanul hagyása, és / ill.
  - közös jelszavak
- stb.

adatbázisok:

- hiányzó patch
- rossz konfiguráció
- jogosultságok - ahogy operációs rendszernél

és mindehhez sokszor korrektív ellenőrzési intézkedés sincs

a kommunikáció - információ - útja

5. réteg: az információ útja
fizikai / elektronikus formában

		info		
intézmény		=>		felhasználó
	fizikai	<=	publikus	
	}	forma	{	
	elektronikus		magán	

pl.:

legbelső rendszer	- középső perimeter	- web szerver
belső hálózat	közbülső logika	első kapcsolati pont

- ellenőrizetlen
- szervezetlen
- illetéktelenek hozzáférése ellen nincs biztosíték

bölcs tanácsok, és nemcsak SOA komponenseket fenyegető veszélyek ellen

- az informatikai folyamatokhoz *ellenőrzési célok* hozzárendelése
- az ellenőrzési célok elérése alkalmas *ellenőrzési intézkedések / eljárások* meghatározása
- megakadályozó – vizsgálati – kárenyhítő intézkedések:

rendezettség, fegyelem, karbantartás,
a rendszerfejlesztés egész életciklusa alatt legjobb szakmai gyakorlat követése
(rendszerszervezési, programozási, tesztelői, kulcsfelhasználói feladatok)

tesztelés, szkennelés,
naplózás, csalásfelderítés,megelőző vizsgálatok,
titkosítás, digitális aláírás - PKI

Magyarázatok

hacker - Wikipédia nyomán - guru, varázsló
programozó, aki program kód, vagy erőforrások módosításával próbál valami sérülékenységet kihasználni
lehet olyan informatikai biztonsági szakértő, aki jól ismeri a számítógép, a számítógéphálózatok biztonsági lehetőségeit, és

- felhívja a figyelmet gyengeségeikre, vagy
- megpróbálja ezeket kihasználni

cracker: a "feketekalapos", a rosszindulatú hacker
- néha fordítva van – a cracker a jó, hacker a rossz

Magyarázatok

infrastruktúrális elem
- amit sérülékenység szempontjából érdemes megkülönböztetni:
- Az informatikai infrastruktúra komponensei. Maga a számítógép is infrastruktúrális elem, a rajta futó szoftverrel, az adatbázis kezelő rendszerrel, a számítógépes kommunikációt biztosító hálózati elemekkel, az informatikai szolgáltatás megfelelő minőségét, sértetlenségét és bizalmasságát biztosító védelmi elemekkel (azok részeivel - infrastruktűrális elemeivel) és persze az ezek segítségével működő, az üzleti folyamatokat szolgáló alkalmazói programrendszerekkel együtt.