ÓBUDAI EGYETEM

Kritikus infrastruktúra védelmi kutatások

TÁMOP-4.2.1.B-11/2/KMR-0001

ÚJ SZÉCHENYI TERV

Nagyméretű webes projektek a felhőben

Prém Dániel

Tanszéki mérnök

TÁMOP-4.2.1.B-11/2/KMR-0001

Résztvevők:

Dr. Kozlovszky Miklós, Dr. Schubert Tamás, Dr. Póser Valéria, Ács Sándor, Prém Dániel

Nemzeti Fejlesztési Ugynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZAG MEGUJUL

A projektek az Európai Unió támogatásával valósulnak meg.

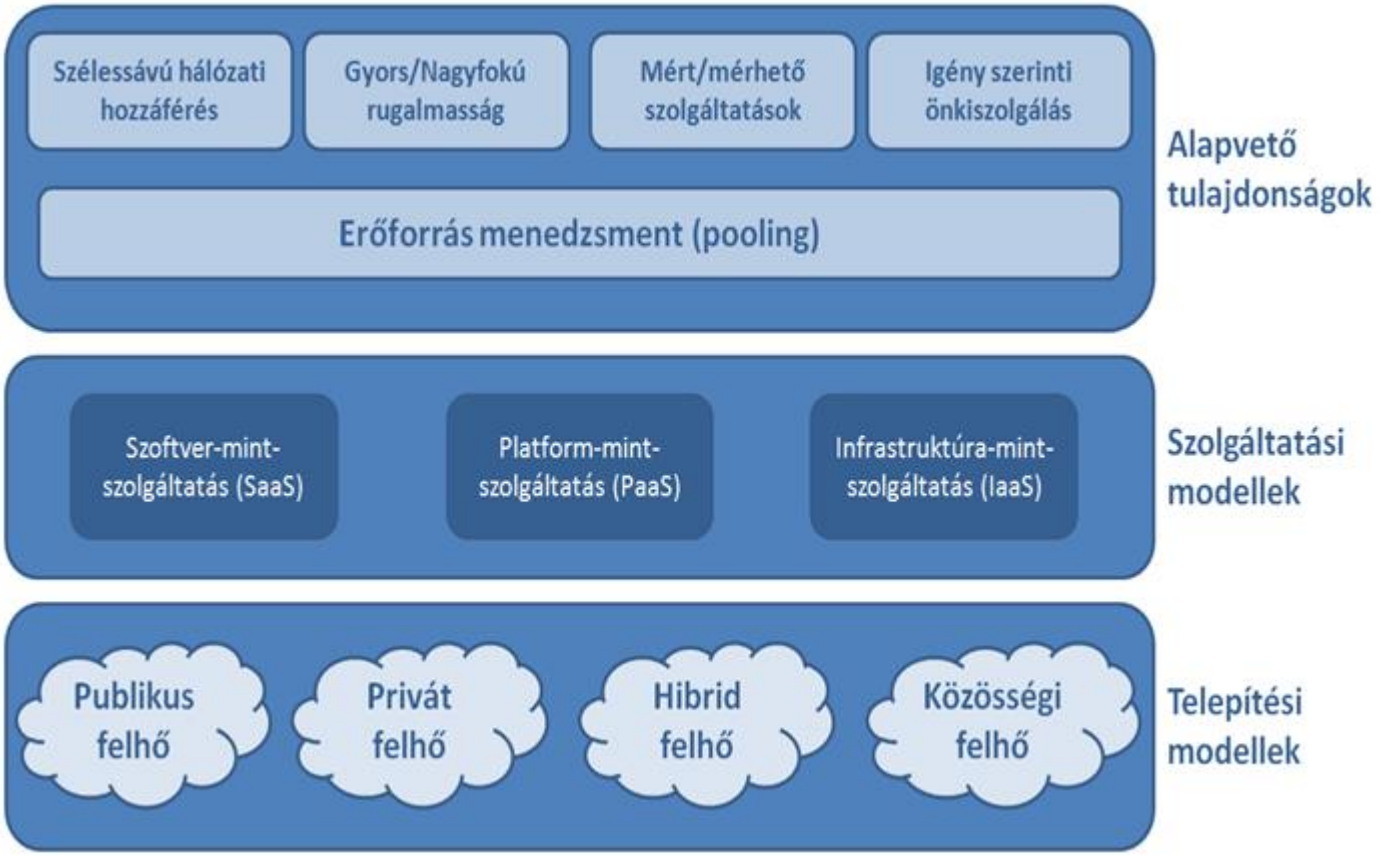
www.uni-obuda.hu

Cloud-Computing

National Institute of Standards and Technology definíciója:

A felhőszámítás olyan modell, amely lehetővé teszi konfigurálható számítási erőforrások (pl.: hálózatok, kiszolgálók, tárolók, alkalmazások és szolgáltatások) osztott készletének kényelmes, igény szerinti, hálózaton keresztül történő elérését, melyek gyorsan, kevés felügyeleti ráfordítással és szolgáltatói beavatkozással munkába állíthatók és eltávolíthatók.

Cloud-Computing



Infrastructure as a Service

- Virtuális gépek *(pl.: Amazon EC2, Amazon S3, GoGrid)*
- Számítási kapacitás bérbeadása
- Tárolókapacitás bérbeadása *(pl.: Amazon S3)*
- Teljes virtuális adatközpont bérbeadása *(pl.: Amazon VPC, Vmware vCloud, Cisco Virtual Multi-tenant Data Center)*
- A hálózat és a virtuális gépek tűzfallal védettek lehetnek, terhelésmegosztás lehetséges, redundáns eszközök alkalmazhatók
- Hozzáférés interneten keresztül

Sérülékenység vizsgálat

- A hálózati sérülékenység vizsgálat (Network Vulnerability Assessment) célja, hogy a belső és DMZ hálózaton lévő összes IP alapú host (számítógép, aktív eszköz, stb.) felismerésre kerüljön és kritikusság szerinti kategorizálása után az ismert sérülékenységekkel szembeni védelmét megállapítsuk.

- Egy publikus IaaS szolgáltató esetében hol és hogyan lehet ilyen sérülékenység vizsgálatot végezni?
- Egy megrendelő számra melyek lesznek a legfontosabbak?

Publikus IaaS modell komponensei

- Szolgáltató infrastruktúrája
  (fizikai / virtuális gépek, hálózat, kapcsolók, útválasztók, tűzfalak, stb.)
- Szolgáltató szoftveres komponensei
  (webes kezelőfelület, API kiszolgáló, ügyviteli rendszer, stb.)
- Bérlő (virtuális) infrastruktúrája
  (virtuális gépek, hálózat, tűzfalak, stb.)
- Külső hálózat
  (internet)

Honnan és mit ellenőrzök?

- Sok komponens, sok hely, sok irány…
  Sok kérdés:

- Egy belső vizsgálat során mihez férhetünk hozzá?
- Mihez nem férhetünk hozzá?
- Mi az aminek egyáltalán nincs értelme?
- Mi az amit figyelmen kívül kell hagyni?

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra				
Sz. Szoftver				
B. Infrastruktúra				
Internet				

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X			
Sz. Szoftver				
B. Infrastruktúra				
Internet				

- Ez az eset amikor a belső alkalmazott (pl.: operátor) a belső hálózatról támadást indít a szolgáltatói infrastruktúra ellen.
- Tipikusan egy DoS támadás vagy egy sérülékenység kihasználás az operációs rendszer vagy egy útválasztó ellen, esetleg MItM támadás.
- Mivel hozzáférés kell a szolgáltató fizikai infrastruktúrájához ezért körülményes. Sőt csak White-Box teszteléssel lehetséges.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X		
Sz. Szoftver				
B. Infrastruktúra				
Internet				

- Ez nagyon hasonlít az előző esethet, csak a belső alkalmazott jelenleg a szolgáltató szoftveres rendszerét vette célba.
- Belső nyilvántartás hamisítása, ügyféladatok megszerzése, jogkör bővítése, stb…
- Mivel hozzáférés kell a szolgáltató fizikai infrastruktúrájához ezért körülményes. Sőt csak White-Box teszteléssel lehetséges.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	
Sz. Szoftver				
B. Infrastruktúra				
Internet				

- Ismételten nagyon hasonló eset, azonban itt a cél a megrendelői infrastruktúra elérése és az ott tárolt adatok és információk megszerzése, vagy adott megrendelő rendszerének elérhetetlenné tétele.
- Hálózati forgalom lehallgatása, lemezképek beolvasása, módosítása, DoS támadás, stb.
- Mivel hozzáférés kell a szolgáltató fizikai infrastruktúrájához ezért körülményes. Sőt csak White-Box teszteléssel lehetséges.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver				
B. Infrastruktúra				
Internet				

- Ebben az esetben a belső alkalmazott eszetlenül támadja a külvilágot.
- Vagy sokkal reálisabb eset, hogy betörés történt és a szolgáltatói gépek egy Botnet / Zombi hálózat részévé váltak és támadásokat indítanak a külvilág ellen (további gépek megfertőzése, esetleg DoS támadás indítása céljából).
- Ez elsődlegesen nem lehet egy sérülékenységi teszt része, mivel ennek az iránynak akkor nincs értelme.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X			
B. Infrastruktúra				
Internet				

- A szolgáltató szoftveres rendszeréből indul támadás a szolgáltató infrastruktúrája ellen.
- Tipikusan az API vagy a Webes felületben található sérülékenység, melynek hatása az infrastruktúra kihat.
- Ezért a szolgáltató beleegyezése szükséges, mivel a teszt az infrastruktúra egyes elemeire kihathat.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-		
B. Infrastruktúra				
Internet				

- A szolgáltató szoftveres rendszeréből indul támadás egy másik szoftverkomponens ellen.
- IaaS sérülékenység vizsgálat esetén ennek nincs értelme, mivel ez minden tekintetben szoftveres szint és nem infrastrukturális.
- Emiatt „out of scope”…

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	
B. Infrastruktúra				
Internet				

- A szolgáltató API vagy Webes felületéről valamilyen sérülékenység hatására hozzáférhetőek a bérlői rendszer elemei vagy adatai.
- Egy sérülékenységi vizsgálat során jól tesztelhető, azonban mindenképpen a szolgáltató beleegyezése szükséges, mivel a teszt az infrastruktúra egyes elemeire kihathat.
- Erősen javasolt a teszt alatt egy saját bérlői rendszer kialakítása, hogy ne éles megrendelői adatokat tegyünk tönkre.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra				
Internet				

- A szolgáltató Webes vagy API felületéről támadás indítható egy webes külső erőforrás ellen.
- Ez elsődlegesen nem lehet egy sérülékenység vizsgálat része, mivel ennek az iránynak akkor nincs értelme.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X			
Internet				

- Egy bérlői infrastruktúrából támadás indítása a szolgáltató infrastruktúrája ellen.
- Ez egy igen jelentős veszélyforrás, s egyből látható hogy a lehetőségét meg kell vizsgálni.
- A teszt kimutatja, hogy egymástól mennyire jól szigetelt a bérlői és a szolgáltatói infrastruktúra.
- Azért van jelentősége, mert mi van akkor ha erre nem gondolt a szolgáltató? Internet irányból védekezik, de belső irányból nem?

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X		
Internet				

- Egy bérlői infrastruktúrából támadás indítása a szolgáltató szoftveres komponensei ellen.
  (Webinterfész, API, belső nyilvántartás, CRM, stb.)
- Egy sérülékenységi vizsgálat során jól tesztelhető, azonban mindenképpen a szolgáltató beleegyezése szükséges, mivel a teszt az infrastruktúra egyes elemeire kihathat.
- Megjegyzés: a belső szoftverek egy IaaS teszt esetén „out of scope” lesznek, de a webinterfész és az API „in scope”.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	
Internet				

- Egy bérlői infrastruktúrából támadás indítása egy másik bérlői infrastruktúra ellen.
- Egy sérülékenységi vizsgálat során jól tesztelhető. Ez egy igen jelentős veszélyforrás, s egyből látható hogy a lehetőségét meg kell vizsgálni.
- A teszt kimutatja, hogy egymástól mennyire jól szigeteltek a bérlői infrastruktúrák.
- Erősen javasolt a teszt alatt egy saját bérlői rendszer kialakítása, hogy ne éles megrendelői adatokat tegyünk tönkre.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet				

- Egy bérlői infrastruktúrából támadás indítása egy külső komponens ellen.
- Igazából akkor van értelme, ha a megrendelő az infrastruktúráját csak privát módon érheti el (pl.: VPN) és az infrastruktúrájának alapból nincs kapcsolata a külvilággal.
- A teszt arra irányulhat, hogy megoldható-e valamilyen módon, hogy mégis hálózatra és így internet hozzáférésre tegyünk szert.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet	X			

- Külső hálózatból támadás indítása a szolgáltatói infrastruktúra ellen.
- Tipikusan egy DoS támadás vagy egy sérülékenység kihasználása a hypervisor vagy útválasztó ellen, esetleg MItM támadás.
- Könnyű kivitelezni, azonban a szolgáltató beleegyezése szükséges, mivel az infrastruktúra egyes elemeit érintheti.
- Tipikusan Black-Box tesztelés.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet	X	X		

- Külső hálózatból támadás indítása a szolgáltató szoftveres komponensei (webinterfész, API, belső nyilvántartás, stb.) ellen.
- Könnyű kivitelezni, azonban a szolgáltató beleegyezése szükséges, mivel az infrastruktúra egyes elemeit érintheti és így a szolgáltatás minőségére kihathat.
- Tipikusan Black-Box tesztelés.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet	X	X	-	

- Külső hálózatból támadás indítása egy bérlői infrastruktúra ellen.
- Az életben teljesen valószerű példa lehet, de egy publikus IaaS szolgáltató esetében ez már nem az ő felelőssége, hanem a megrendelő felelőssége.
- Sőt ha be is törnek egy megrendelői gépre, akkor onnan
- Emiatt „out of scope”.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet	X	X	-	-

- Internetről támadunk internetet…
- Semmi közünk a szolgáltatóhoz és a bérlőhöz sem…
- Azaz nincs értelme, így kimarad.

Komponens mátrix

forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet	X	X	-	-

- Színek jelentése:
  - Amit mindenképpen javaslunk megvizsgálni
  - Amit javaslunk megvizsgálni, de megbeszélés tárgyát képzi, mivel nagyban függ a rendszertől, ráfordítható időtől, kihatástól. Ezen pontok esetében érdemes a szolgáltatóval konzultálni, hogy mely elemek kerüljenek a hatókörbe.
  - Azon elemek, amelyeket jó lenne megvizsgálni, de nagyfokú bizalom és felhatalmazás szükséges hozzá (black-box tesztelés) és a vizsgálat kihatása elég katasztrofális lehet, emiatt kiemelt figyelemmel kell eljárni.
  - Nincs értelme vizsgálni, vagy nem érint infrastrukturális elemet.

Komponens mátrix

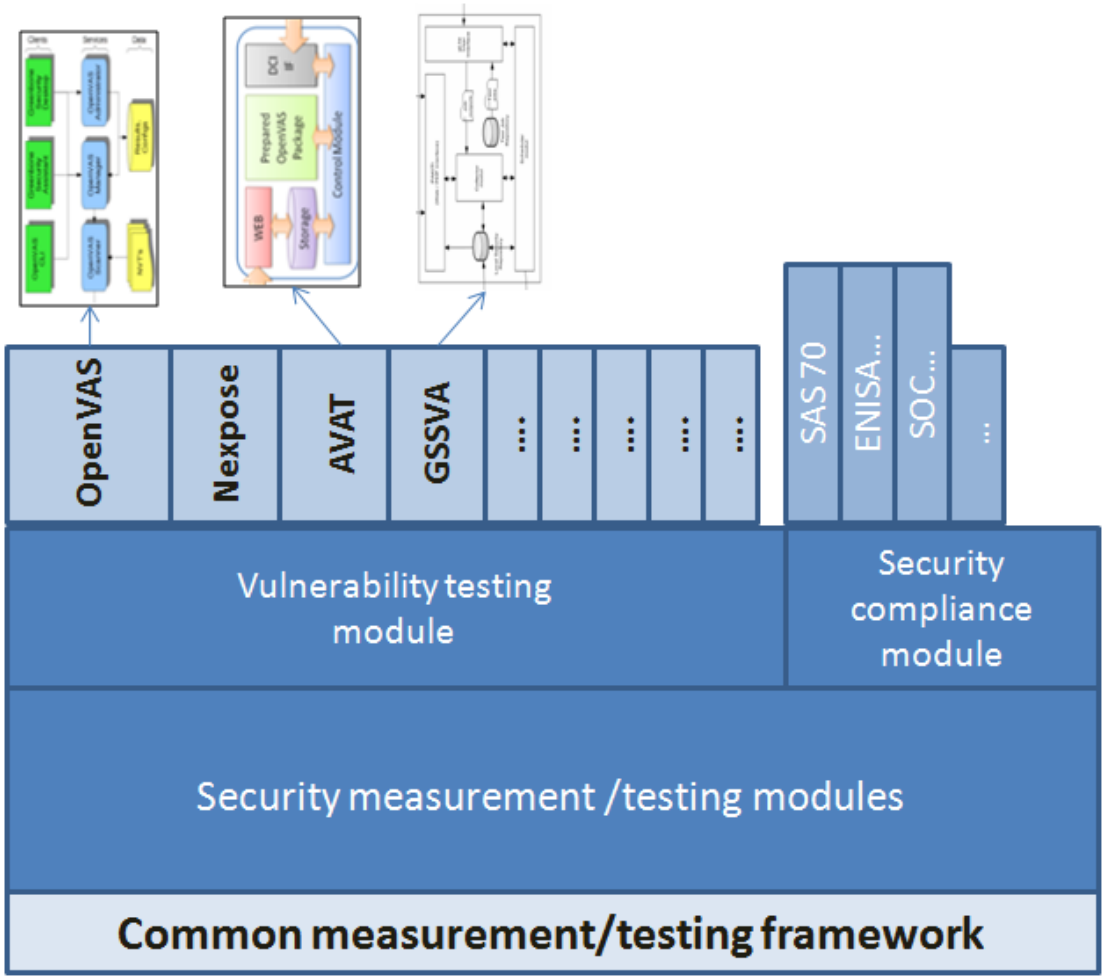
forrás \ cél	Sz. Infrastruktúra	Sz. Szoftver	B. Infrastruktúra	Internet
Sz. Infrastruktúra	X	X	X	-
Sz. Szoftver	X	-	X	-
B. Infrastruktúra	X	X	X	X
Internet	X	X	-	-

- Vizsgálati hatókör megállapítása:
  - Vegyük figyelembe a vizsgálatok elvégzéséhez szükséges időt, ugyanis ha mindent meg kell vizsgálni, akkor az nagyon sokáig tarthat…
  - Fontos, hogy ez nem egy Etikus Hackelés vagy egy Penetrációs Tesztelés. Itt a cél általános hibák, ismert sérülékenységek és a tervezési hibák feltárása.
  - A sérülékenységi vizsgálatot jó lenne valamilyen automata eszközökkel elvégezni, amelyek felmérik és alkalmazkodnak a változó környezetekhez.

Automata sérülékenység vizsgálat

- A cél egy olyan rendszer megvalósítása, amely:
  - Felméri az infrastruktúrát (kézi beavatkozást meg kell oldani)
  - Detektálja az eszközökön található operációs rendszereket és portokat
  - Megvizsgálja az infrastrukturális elemeket, milyen ismert sérülékenységekkel rendelkezik.
  - Majd minderről valamilyen jelentést készít teljesen automatikusan.

Automata sérülékenység vizsgálat



CLOUDSCOPE

Grid Site Software Vulnerability Analyzer

Advanced Vulnerability Assessment Tool

ÓBUDAI EGYETEM

www.uni-obuda.hu

Köszönöm a figyelmet!

Kérdések?

Köszönetnyilvánítás

Kritikus infrastruktúra védelmi kutatások

TÁMOP-4.2.1.B-11/2/KMR-0001

ÚJ SZÉCHENYI TERV

A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „*Kritikus infrastruktúra védelmi kutatások*” projektnek az előadáshoz végzet kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Nemzeti Fejlesztési Ugynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZAG MEGUJUL

A projektek az Európai Unió támogatásával valósulnak meg.

ÓBUDAI EGYETEM