UTÓLAG KÖNNYŰ OKOSNAK LENNI

MIKOR JÖHET JÓL AZ OFFENZÍV MEGKÖZELÍTÉS?

Veres-Szentkirályi András 2020-07-07

$ whoami

Veres-Szentkirályi András

- OSCP, GWAPT, SISE, HAREC
- Silent Signal társalapító (2009-)
- pentester, toolmaker
- 15 év tapasztalat

Menetrend

1. Offenzív biztonság
2. Offenzív CI/CD
3. Offenzív automatizált tesztelés
4. Offenzív konténerek

Egy fontos gondolat előszó helyett

“Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can’t break.”

– Bruce Schneier (1998. október 15.)
https://www.schneier.com/crypto-gram-9810.html#cipherdesign

Grand Brighton Hotel, 1984

“Today we were unlucky, but remember **we only have to be lucky once. You will have to be lucky always.**”

– Provisional IRA (1984. október 13.)
Taylor, Peter (2001). Brits: The War Against the IRA. Bloomsbury Publishing. p. 265. ISBN 0-7475-5806-X.

https://en.wikipedia.org/wiki/Brighton_hotel_bombing

ASAP

silent signal

Specifikációs hibák fájnak a legjobban minden értelemben:

“A US soldier in Afghanistan used a Precision Lightweight GPS Receiver—a “plugger”—to set coordinates for an air strike. He then saw that the “battery low” warning light was on. He changed the battery, then pressed “Fire.” The device was designed, on starting or resuming operation after a battery change, to initialize the coordinate variables to its own location. The resulting strike killed the user and three comrades”

`http://mcs.open.ac.uk/mj665/SeeMore3.pdf`

`https://web.archive.org/web/20130624110018/http:/www.gpsnavigatormagazine.com/gps-blamed-in-deadly-fire-event.html`

Tájékozottság

silent signal

- low hanging fruit: hol jönne be egy igazi támadó
- leltár: mink van egyáltalán?
- szoftver verziók
- dependency chain
- Equifax vs. Struts

„Van rá poliszink!”

silent signal

- mi mindenre lehet ám: jelszó, middleware/library blacklist/whitelist
- nem mindegy: műszaki kényszer vs. természetes nyelvű írott ajánlás
- formalizált-automatizált infra: folyamatos és automatikus kényszer

Menetrend

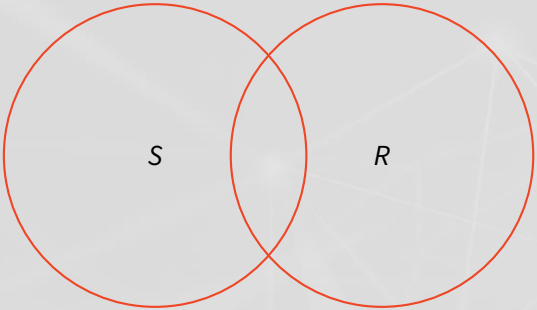
1. Offenzív biztonság
2. Offenzív CI/CD
3. Offenzív automatizált tesztelés
4. Offenzív konténerek

CI/CD alapok

silent signal

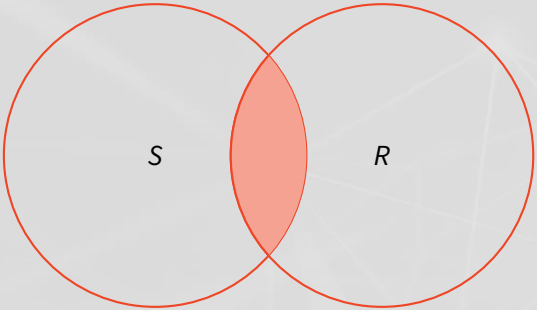
- nulladik lépés: forráskód menedzsment
- commit/push: automatikus build
- automatikus tesztek: cloud infrastruktúra adja magát
- build kimenet: automatikus deployment

Offenzív vs. defenzív megközelítés



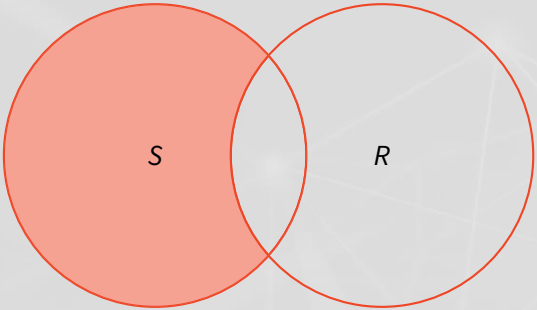
- *S* specifikáció
- *R* rendszer

Offenzív vs. defenzív megközelítés



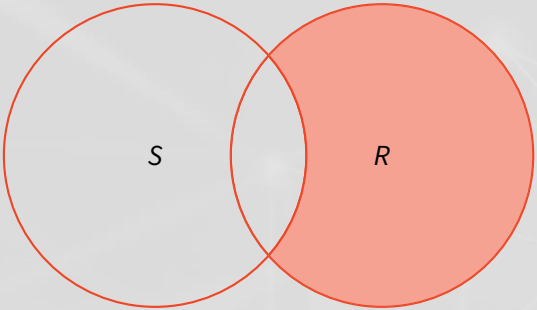
- S specifikáció
- R rendszer
- $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)

Offenzív vs. defenzív megközelítés



- S specifikáció
- R rendszer
- $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)
- $S - R$ specifikációban szereplő, de rendszer által **nem** nyújtott szolgáltatás
  - bug, funkcionális hiba

Offenzív vs. defenzív megközelítés



- S specifikáció
- R rendszer
- $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)
- $S - R$ specifikációban szereplő, de rendszer által **nem** nyújtott szolgáltatás
  - bug, funkcionális hiba
- $R - S$ specifikációban **nem** szereplő, de rendszer által nyújtott szolgáltatás
  - feature, potenciális biztonsági hiba

Menetrend

- Offenzív biztonság
- Offenzív CI/CD
3. Offenzív automatizált tesztelés
- Offenzív konténerek

Mi rossz történhet? (©HBO)

silent signal

Disclaimer

silent signal

- nem helyettesíti a manuális biztonsági vizsgálatot
- sőt, annak kimenete fontos visszacsatolás
- célpontok: low hanging fruit, regresszió, security baseline

1. példa: Erlang HTTP kliens

“It never even occurred to me that an http client would be insecure by default when connecting over https.”

```
$ curl https://self-signed.badssl.com/
curl: (60) SSL certificate problem: self signed certificate
More details here: https://curl.haxx.se/docs/sslcerts.html

3> httpc:request("https://self-signed.badssl.com/").
{ok,{{"HTTP/1.1",200,"OK"},
     [{"cache-control","no-store"},
      {"connection","keep-alive"},
      {"date","Tue, 07 Jul 2020 10:34:00 GMT"},
      ...
```

2. példa: integritásvédelem

- mindenki bemagolta a CIA triádot
- I = Integrity – kikényszeríti bárki?
- C = Confidentiality – elegendő önmagában?

https://xkcd.com/1181/

3. példa: invalidáció

silent signal

- API kulcsok – lehetséges-e egyáltalán, lásd JWT
- tanúsítványok – CRL, OCSP
- ellenőrzi bárki?

Menetrend

- Offenzív biztonság
- Offenzív CI/CD
- Offenzív automatizált tesztelés
4. Offenzív konténerek

Minimális környezet

silent signal

- mit talál egy támadó a gépen?
- mekkora része kell ennek a tényleges működéshez?
- “Cattle not Pets”
- shell hozzáférés (pl. SSH)
- kompromittált hosztról takarítás vs. nulláról újjáépítés
- configuration as code / “facade of immutability”

TTL

silent signal

- mennyi idő alatt lehet kitolni commitot?
- mennyi idő javítani egy sérülékenységet?
- deployment idő korrelál az automatizáltság, formalizáltság mértékével
- példa: Let’s Encrypt

Összefoglalás

silent signal

- Ne csak „magunk ellen” védjük a rendszert!
- Gondoljunk arra, hogy mindig lesz olyan, aki nem tartja be a játékszabályokat!
  - sőt, tőlük kellene igazán védenie a rendszernek
  - kezdettől fogva legyen része a tervnek!
- Nyessük le a plusz „feature”-öket!
- A biztonság is legyen része a formalizált-automatizált minőségbiztosítási rendszernek!
  - a sebezhető rendszer színtelen és szagtalan
  - formalizáltságból ered az automatizált kényszer
  - vö. “Liberty is Muscle that Must Be Exercised”

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t

silent signal