scademy
secure coding academy

Biztonságos szoftverek fejlesztése, a „by design” elv a gyakorlatban

Hétpecsét LXXXIV. Szakmai Fórum
2019. január 16.

Hornák Zoltán

20+ MILLIÓ PROGRAMOZÓ

EBBEN A PILLANATBAN IS

KEMÉNYEN DOLGOZIK:

SÉRÜLÉKENY PROGRAMOT FEJLESZT

EZ AKKORA MENNYISÉG

AMIRE NINCS ELEGENDŐ SZAKEMBER, HOGY KEZELJE

A TREND VILÁGOS ÉS EGYÉRTELMŰ

A KIBERBIZTONSÁG ROMLIK

NAPRÓL NAPRA

TÖBB PROBLÉMA SZÜLETIK, MINT MEGOLDÓDIK

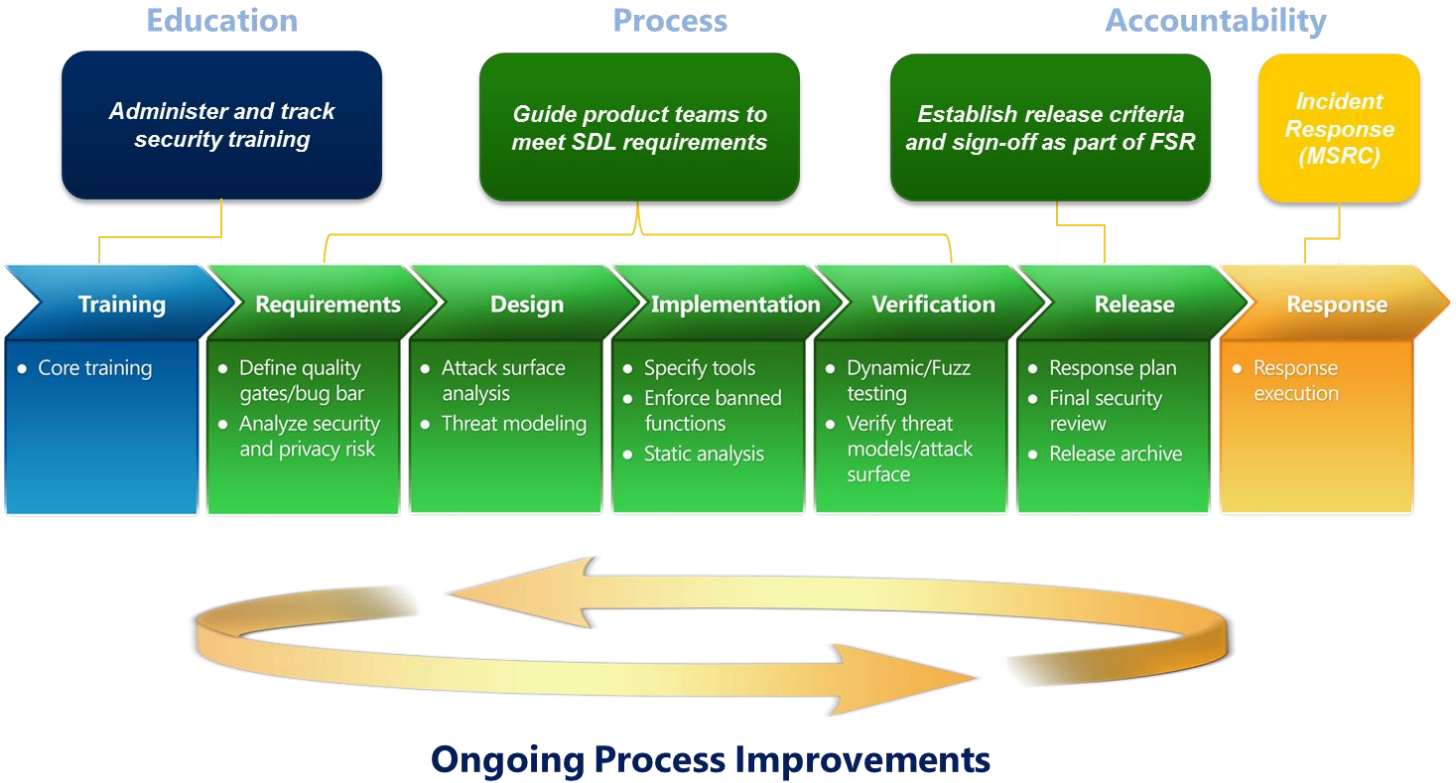
FOLYAMATOSAN

SÚLYOSBODIK A HELYZET

Biztonságos programok fejlesztése

Ez lenne a megoldás?

Microsoft Security Development Lifecycle (SDL)



SZAKEMBERHIÁNY

Forbes

Forbes CommunityVoice Connecting expert communities to the Forbes audience. What is This?

13,080 views | Aug 9, 2018, 07:30am

The Cybersecurity Talent Gap Is An Industry Crisis

Brian NeSmith Forbes Co
Forbes Technology Coun

POST WRITTEN BY

Brian NeSmith

Brian NeSmith is the CEO and Co-Founde
company, based in Sunnyvale, CA.

CSO FROM IDG

Home > Security

CYBERSECURITY SNIPPETS

By Jon Oltsik, CSO | JAN 11, 2018 11:53 AM PT

About

Jon Oltsik is a principal analyst at Enterpris
Group ESG and has been quoted in the Wi
Journal, Business Week, and the New York

ANALYSIS

Research suggests cybersecurity skills shortage is getting worse

New data from reveals growing skills gaps that represent an existential threat. What sh
organizations do?

CISION PR Newswire

The Severe Cybersecurity Professionals is a Key Risk to Our Nation's Security

NEWS PROVIDED BY
National Cyber Security Alliance →
Oct 09, 2018, 07:00 ET

NATIONAL CYBERSECURITY ALLIANCE

(ISC)² BLOG

18 October 2018

CYBERSECURITY SKILLS SHORTAGE SOARS, NEARING 3 MILLION

(ISC)²'s Cybersecurity Workforce Study, 2018

betanews

Cybersecurity faces a worldwide shortage of almost 3 million staff

By Ian Barker | Published 3 months ago | Follow

4 Comments | Like 18 | Share | G+ | Tweet

APRÓ PROGRAMHIBÁK

OKOZZÁK A LEGTÖBB
KIHASZNÁLHATÓ SÉRÜLÉKENYSÉGET

OLYAN IMPLEMENTÁCIÓS HIBÁK
AMELYEKET EL LEHETETT VOLNA KERÜLNI

BIZTONSÁGOS PROGRAMOZÁSI GYAKORLATTAL

Mennyire apró programhibák?
És mekkora problémát okoznak?

Ki tudja mi ez a szám?

3.14159265358979323846

Ki tudja mi ez a szám?

2.71828182845904523536

2.2250738585072012e-308

A legveszélyesebb lebegőpontos szám

2.2250738585072012e-308 avagy “The Double Bug”

- Ez a hiba több mint egy évtizedig lappangott!

- A **`parseDouble()`** metódus egy szöveg alakú számot konvertál double méretű lebegőpontos számmá
  - A probléma forrása, hogy a konverziós algoritmus közelítő lépésekkel keresi meg a decimális értékhez legközelebb álló bináris számot
  - Kettes számrendszerben a **`2.2250738585072012e-308`**
    - kisebb mint **`0x1.0000000000000p-1022`**
    - de nagyobb mint **`0x0.fffffffffffffp-1022`**
  - Ennek eredményeként a közelítő algoritmus oszcillálni kezd és **végtelen ciklusba kerül**

2.2250738585072012e-308 konverziós lépései

```
                                                                10110  22
                                                             11011110  222
                                                          100010110001  2225
                                                       101011011101010  22250
                                                    110110010100101011  222507
                                                 100001111100111010001  2225073
                                              101010011100001001110010  22250738
                                           110101000011001100010111001  222507385
                                        100001001001111111110111011000010  2225073858
                                     101001011100011111101010011100011001  22250738585
                                  110011110011100111100101000011111111010  222507385850
                               100000011000010000101111001010011111001011  2225073858507
                            101000011110010100111010111101000110111110000  22250738585072
                         110010100101111010001001101100011000101101100000  222507385850720
                      111111001111011000101100000111011110111000111000001  2225073858507201
0 10000110001 111110011111011000101100000111011110111000011100000100  2.225073858507201  E 15
0 10000101000 000000110000100001011110010100111110010110011001110  2.225073858507201  E 12
0 01101010011 010101001111110111010111111101110011101111110011101  2.225073858507201  E-52
0 00000000000 111111111111111111111111111111111111111111111111111  2.225073858507201  E-308
0 00000000001 000000000000000000000000000000000000000000000000000  2.2250738585072014 E-308
0 00000000000 111111111111111111111111111111111111111111111111111  2.225073858507201  E-308
0 00000000001 000000000000000000000000000000000000000000000000000  2.2250738585072014 E-308
```

A Double Bug kihasználása

- Egyetlen HTML lekérdéssel a Double Bug hatására elszállt **minden web szerver**, ami Tomcat alatt futott

- A HTML fejlécben van egy **`Accept-language`** mező
- Amelynek megadható egy `q` paraméter, amit lebegőpontos számként értelmez a szerver…
- Ennek eredményeként az alábbi kérés elküldésének hatására minden Tomcat szerver leállt:

```
GET / HTTP/1.1
Host: myhost
Connection: keep-alive
Accept-Language: en-us;q=2.2250738585072012e-308
```

2.2250738585072012e-308

WannaCry – és a hiba, amit mögötte volt

- Mindenki hallott a WannaCry-ról…
- Világszintű hatásról, a károkozás mértékéről
- De a háttérben lévő konkrét Windows biztonsági hibáról kevesebben

- Egyetlen betű hiba volt végső soron a felelős

- Ki tudja melyik betű volt az?

SPOT THE BUG BEHIND WANNACRY

```
int __stdcall SrvOs2FeaListSizeToNt(_DWORD *a1)
{
    _WORD *v1; v1 = a1;
    unsigned int v3;
    // ...
    *v1 = (_WORD)(v3 - v1);
    // ...
}
```

Leghatékonyabb módja a biztonság fokozásának az

OKTATÁS

Minden fejlesztőt úgy kellene képeznünk
hogy **Motivált Biztonságos Programozó** legyen

Biztonságos Programozás Oktatása

- Kötelező oktatás nem mindig éri el a célját
- Az eredményes képzés kulcsa a **motiváció**
- Szervezeti szintű oktatási program
  - Figyelemfelkeltő kampány programozóknak
  - Helyszíni tantermi oktatás
    - Gyakorlati példákkal
    - „Real-Life Hacking Fun”
  - Vizsgák
  - CTF: Capture-the-Flag csapatépítő játékok
- INSECAR: sérülékeny web és mobil alkalmazás
- TTT: Train-the-Trainer programok

Gyakorlati lebonyolítás

- Ideálisan minden programozónak célszerű lenne részt venni 3-5 nap gyakorlati képzésen
- A biztonságos programozás nem jelent többletmunkát, jelentős kód növekedést
- A kulcs a programozási **szokások** megváltoztatása
- A gyakorlati bevezetés legtöbbször lépésről lépésre valósul meg:
  - Cybersecurity szakemberek képzése
  - Security champions
  - Összes programozó

- A határvédelem, a falak, a várak építése jó ötlet volt
  - a középkorban
- Bárhol lehet kihasználható biztonsági lyuk
  - ahova külső input eljut
  - vagyis a gyakorlatban bárhol
- Biztonsági funkcionalitás
  - követelmény listák
- Kódminőség
  - a biztonságos programozás kulcsa

scademy
secure coding academy

SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

CCLAB

scademy
secure coding academy

Motivated Secure Coders

Thank you!

Zoltán Hornák

Zoltan.Hornak@scademy.com

www.scademy.com

Join the **Secure Coding Academy** group on LinkedIn and stay informed about our courses!

Essential security for all software engineers.