Czy nie ma bata na cyberatak?

Gerard Frankowski, Dział Bezpieczeństwa ICT PCSS

Konferencja „Bezpieczeństwo w Internecie – odpowiedzialne korzystanie z mediów społecznościowych”

Poznań, 8.02.2018

Czym jest PCSS?

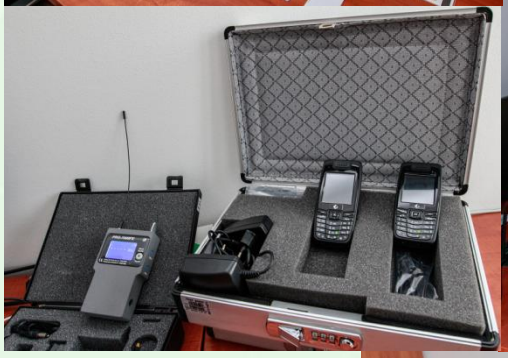
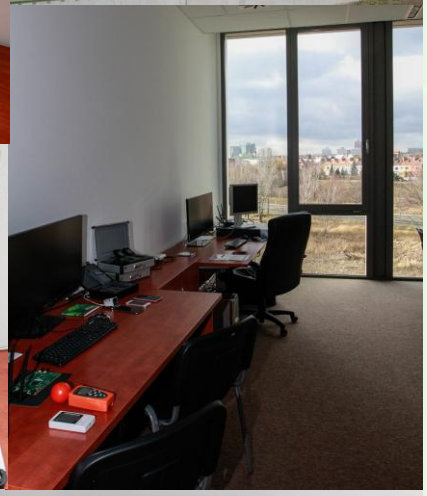
Czy to „Po Co Się Spieszyć”? ;)

- Jednostka naukowo-badawcza
- Centrum **superkomputerowe**
- Operator **sieci** naukowej PIONIER
- Ciekawe badania – współpraca z naukowcami, przedsiębiorcami, instytucjami publicznymi…
- Główne obszary zainteresowań
  - Sieci nowej generacji
  - Zaawansowane aplikacje
  - Usługi Internetu Rzeczy
  - **Bezpieczeństwo** sieci i systemów

Czym zajmuje się Dział Bezpieczeństwa?

- Zabezpieczanie własnych sieci oraz systemów
- Zadania bezpieczeństwa w projektach naukowo-badawczych
- Konferencje, szkolenia
- Współpraca zewnętrzna
- Własne badania w dziedzinie bezpieczeństwa IT




Specjalista cyberbezpieczeństwa musi wiedzieć bardzo wiele (i coraz więcej!)

Zwykły użytkownik nie musi wiedzieć aż tyle

Kilka najważniejszych porad dla Was:

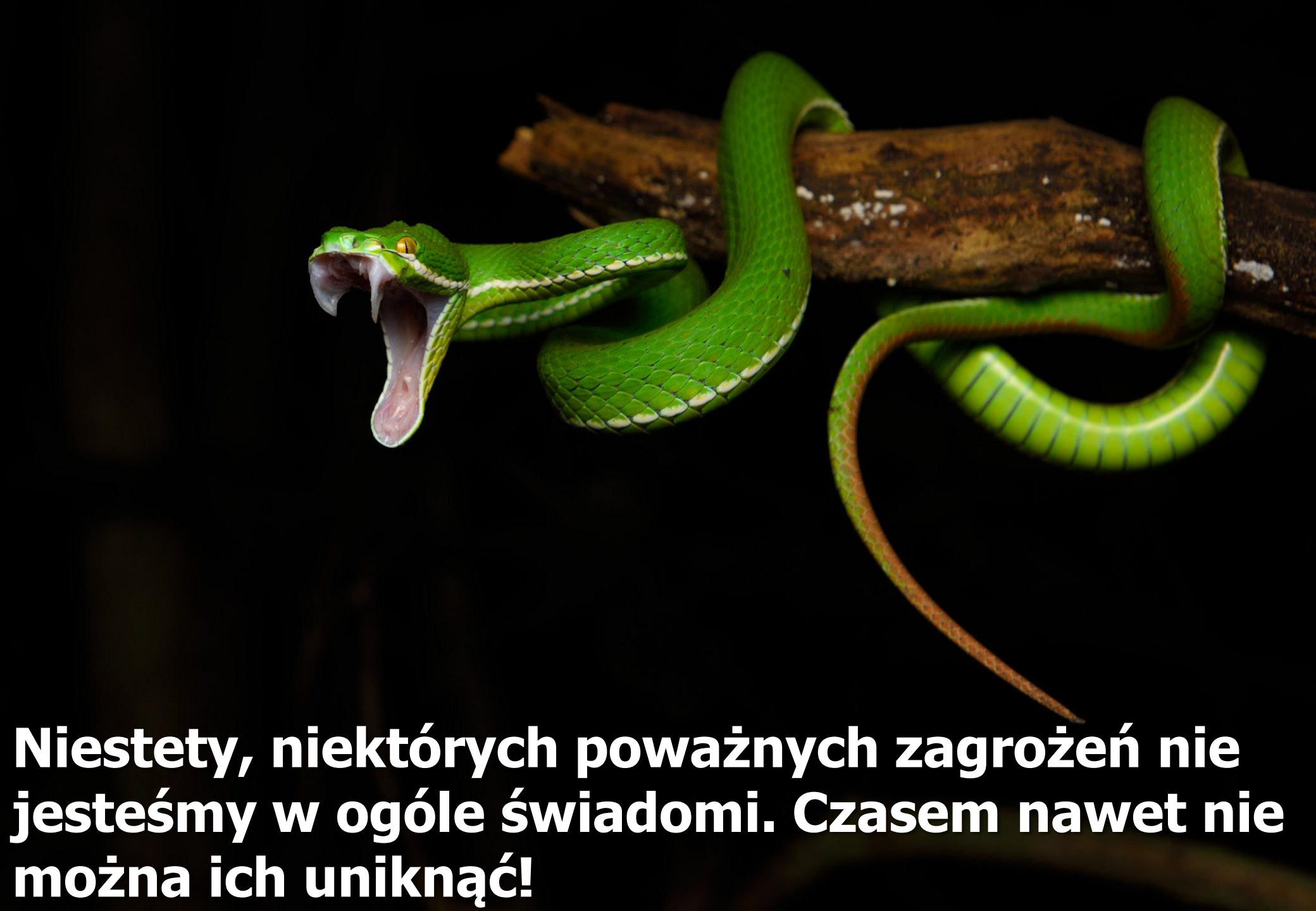
Mam silne hasła i nikomu ich nie ujawniam

Mój komputer ma zainstalowany aktualny system i programy, w tym systemy zabezpieczeń

Potrafię chronić swoją prywatność

Jestem świadomy: nie klikam dziwnych linków, uważam na załączniki i maile od nieznajomych

Mój smartfon i tablet to też cele ataku – muszę uważać tak samo, jak na komputerze



Niestety, niektórych poważnych zagrożeń nie jesteśmy w ogóle świadomi. Czasem nawet nie można ich uniknąć!

Przykład 1: StageFright

Wystarczyło, że dostałeś MMS, a jego nadawca mógł przejąć kontrolę nad Twoim telefonem

Wystarczy jeden MMS, aby przejąć kontrolę nad prawie wszystkimi z dzisiejszych smartphonów działających pod kontrolą systemu Android. Ofiara nie musi wykonywać żadnej akcji — co gorsza, nawet nie zorientuje się, że została zaatakowana, bo udany atak spowoduje skasowanie swoich śladów z telefonu ofiary...

StageFright — wystarczy, że ktoś zna twój numer telefonu

O błędzie, któremu nadano kryptonim **Stagefright** (tak, jest też logo!) poinformowała dziś firma Zimperium zajmująca się bezpieczeństwem mobilnym.

95% telefonów z Androidem można zhakować MMSem i trudno się przed tym zabezpieczyć

Autor: Adam dnia 27 lipca 2015 | 18 komentarzy

Wystarczy odtworzenie odpowiednio spreparowanej wiadomości MMS by zainfekować dowolny telefon z Androidem w wersji 2.2 i nowszej. Co gorsza, by załatać tę lukę, trzeba czekać na aktualizację od producenta telefonu....

Czytaj dalej

Źródło: zaufanatrzeciastrona.pl, niebezpiecznik.pl

Przykład 2: włamanie do... procesora

Można *zhakować* komputer, który jest wyłączony?

Można!

Security

How to remote hijack computers using Intel's insecure chips: Just use an empty login string

Exploit to pwn systems using vPro and AMT

By Chris Williams, Editor in Chief 5 May 2017 at 19:52 75 SHARE ▼

Znamy już szczegóły krytycznych błędów w wielu procesorach

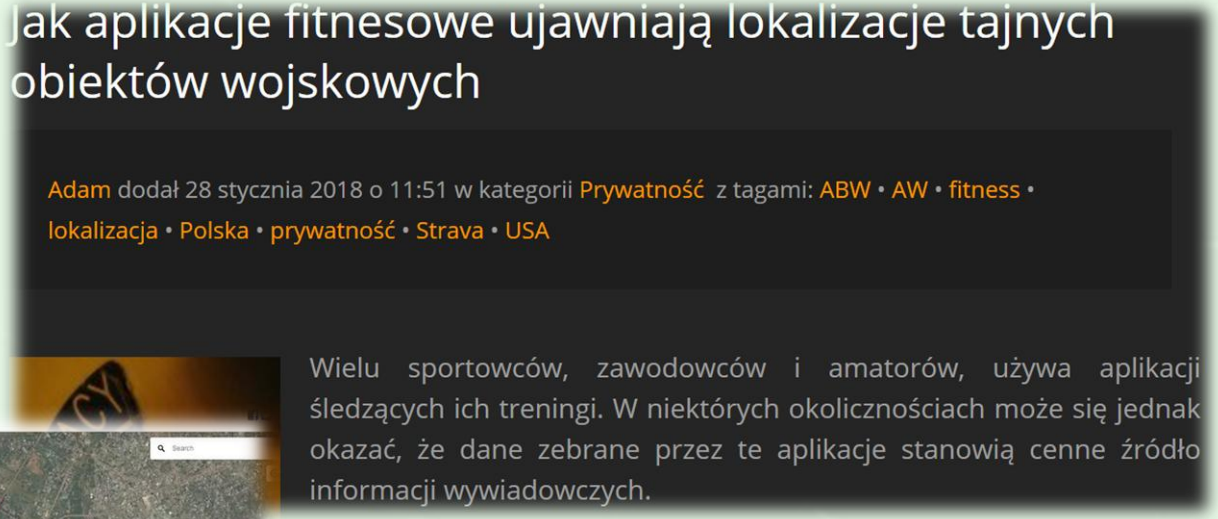
Adam dodał 4 stycznia 2018 o 00:28 w kategorii Top z tagami: AMD • ARM • Intel • Meltdown • Spectre

Szczegóły błędów, o których mówi cały świat bezpieczeństwa, zostały ujawnione wcześniej, niż się spodziewaliśmy. Ataki nazwane Meltdown oraz Spectre są faktycznie niebezpieczne i dotyczą wielu rodzin procesorów.

Źródło: zaufanatrzeciastrona.pl, www.theregister.co.uk

Przykład 3 – powiem Ci, gdzie jestem

Używanie urządzeń i aplikacji, które ujawniają miejsce naszego pobytu (albo inne wrażliwe dane)



Źródło: zaufanatrzeciastrona.pl

Co robimy, żeby to zmienić?

- **Szkolimy użytkowników, administratorów, programistów…**
- **Oceniamy bezpieczeństwo już gotowych systemów**
- **Pomagamy projektować od początku bezpieczne rozwiązania**
- **Tworzymy własne systemy zabezpieczeń**

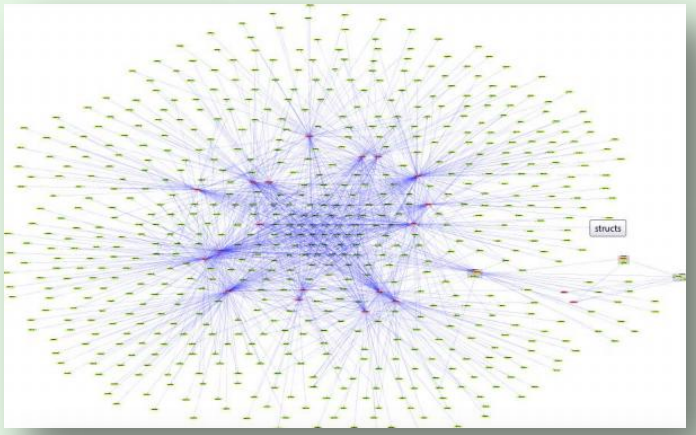
Zagrożenia możemy wykryć na dwa sposoby:

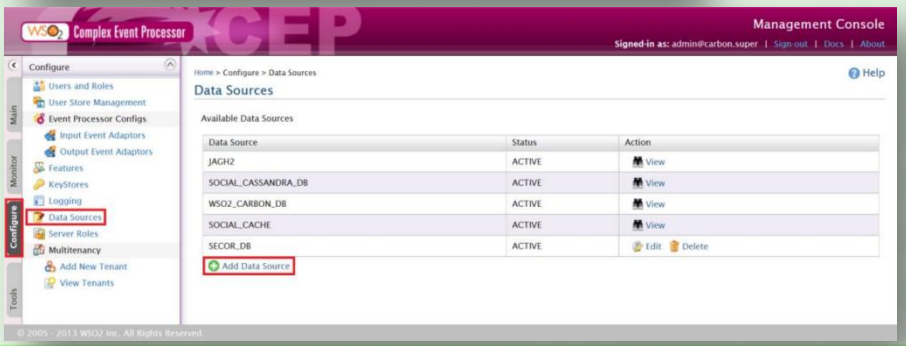
Analiza sygnaturowa

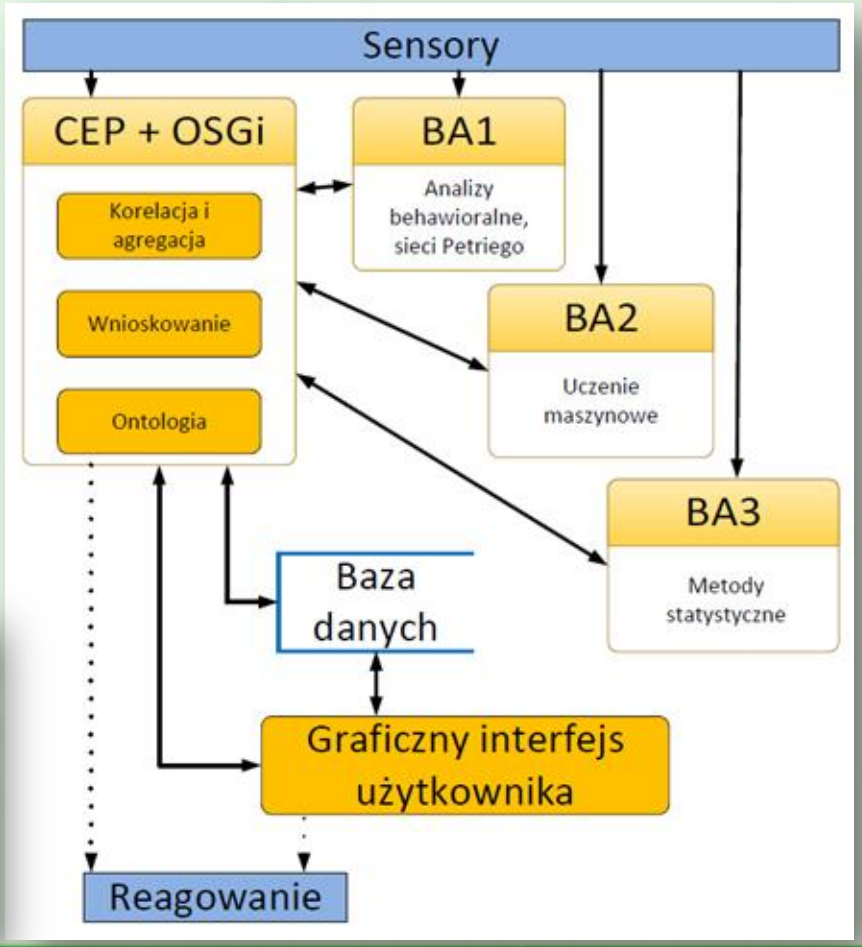
Analiza behawioralna (detekcja anomalii)

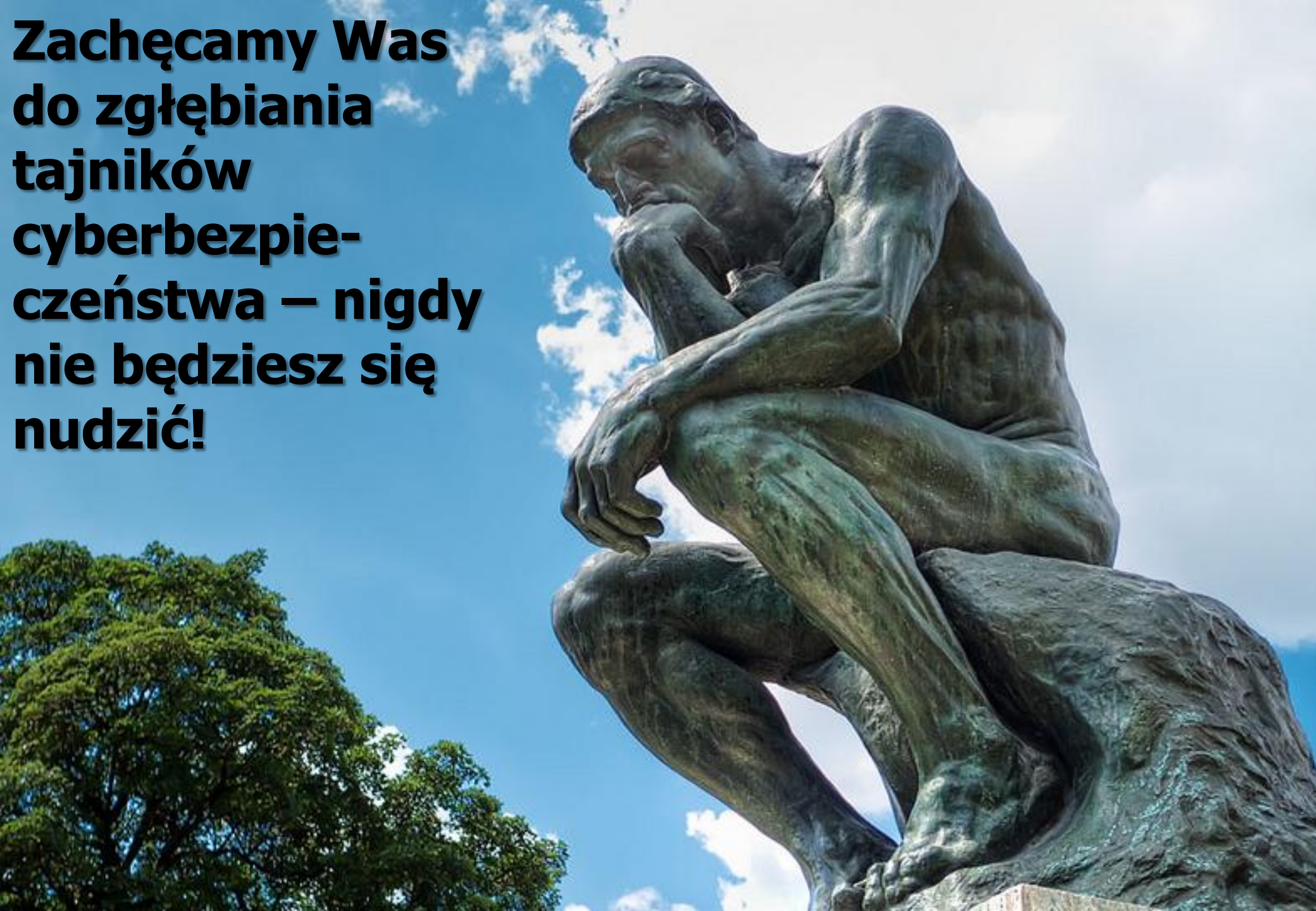

Detekcja anomalii nie jest idealną metodą, ale tylko ona pozwala wykryć ataki, które wcześniej nie były stosowane

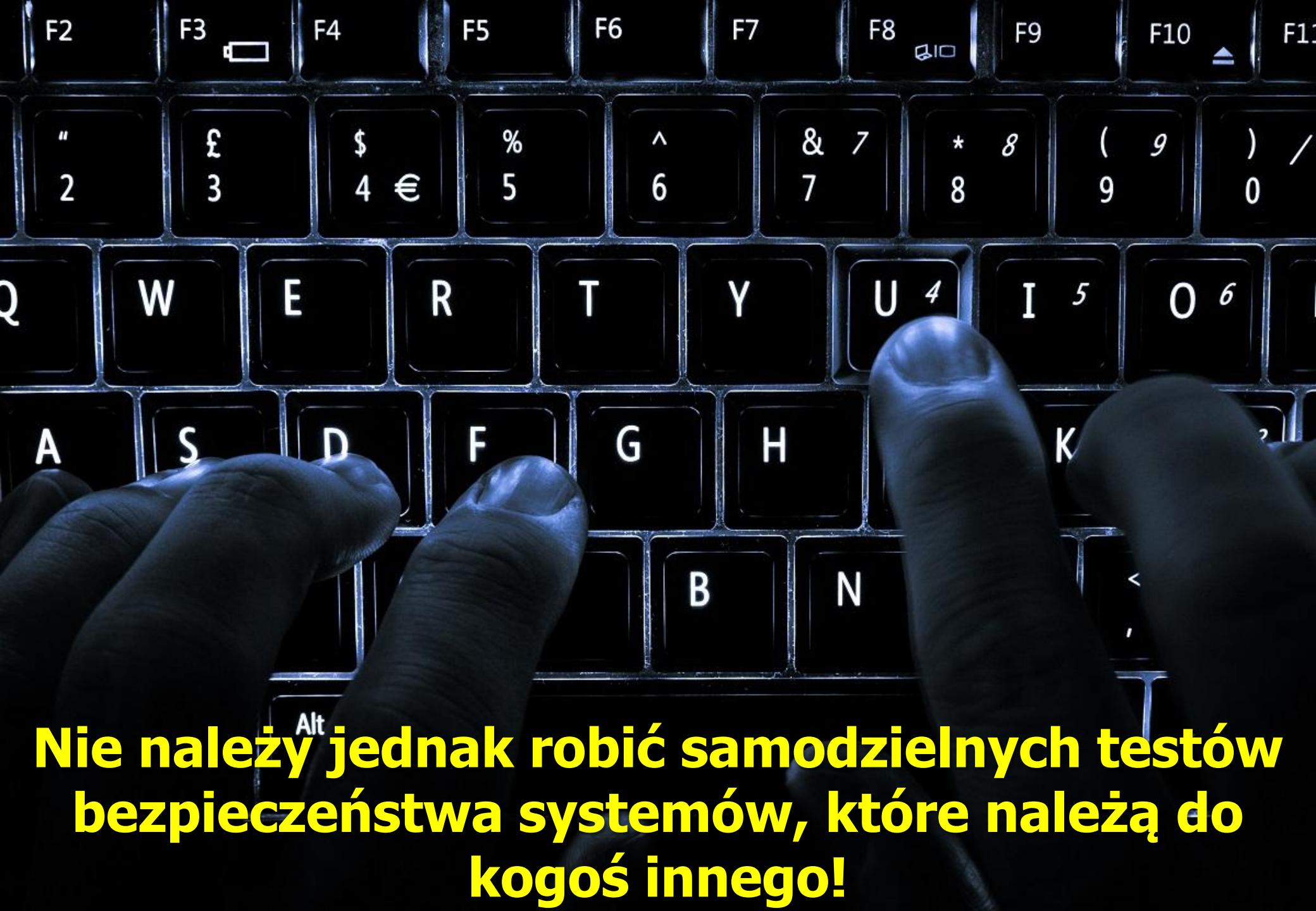
Przykład opracowanego systemu w ramach projektu naukowego SECOR








Zachęcamy Was
do zgłębiania
tajników
cyberbezpie-
czeństwa – nigdy
nie będziesz się
nudzić!


Nie należy jednak robić samodzielnych testów bezpieczeństwa systemów, które należą do kogoś innego!

Nie atakuj innych!

- Prowadzone **bez zezwolenia** testy bezpieczeństwa mogą grozić **odpowiedzialnością karną**!

- Art. 267-269 KK: grozi grzywna, ograniczenie lub pozbawienie wolności
  - Próba przełamania zabezpieczeń: do 2 lat
  - Podsłuchiwanie informacji w sieci: do 2 lat
  - Uniemożliwienie dostępu do usługi (DoS/DDoS) – do 3 lub nawet 5 lat

- Policja może skutecznie namierzyć większość napastników

Chcesz o coś zapytać?

- Autor prezentacji
  - gerard.frankowski@man.poznan.pl
- Więcej o naszym Dziale Bezpieczeństwa ICT:
  - security@man.poznan.pl
  - http://security.psnc.pl

- Więcej o cyberbezpieczeństwie po polsku – np.:
  - https://zaufanatrzeciastrona.pl
  - https://sekurak.pl/
  - https://niebezpiecznik.pl/
  - https://www.cert.pl/ouch/