The usecase of Honeypots in the public administration sector

Ábel Gonda
Event Detection Specialist
abel.gonda@nki.gov.hu

National Cyber Security Center

CSIRT

PENTEST

EVENT DETECTION

NATIONAL
CYBER SECURITY CENTER
HUNGARY

AUTHORITY

AWARENESS

What are Honeypots?

Trap or decoy enviroment designed to emulate legitimate service or protocol in order to create interaction with cybercriminals.

What does it provide?

Security

- New network security layer
- Gains time for admins
- Alerting system

Canary tokens

Information

- Indicators
- Vulnerabilities
- Intelligence data

Honeynet

GovProbe

"Governmental Honeypot System"

HONEYPOT

Aims to help further sthrengthen the security of critical infrastrucures.

Network security:
- A second line of defence
- Easily provide firewall rules
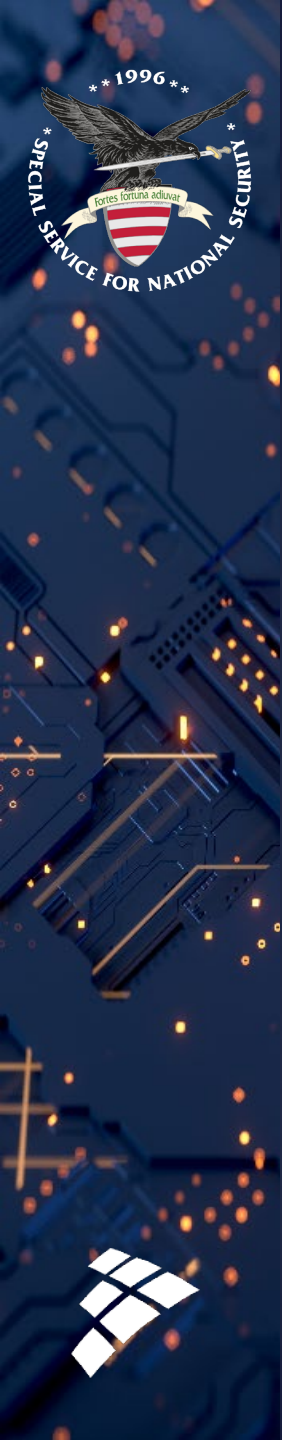- Intrusion alarm

Incident response:
- Enriches incident data from other sources (Firewall, IDS/IPS)
- Discovery of Zero Day vulnerabilities

Intelligence:
- Provides new indicators
- Helps in trend analysis

EWS

GovProbe Statistics

- 2.680.000 daily attack entries
- 6 high interaction sandbox enviroments
- 35 sets from ~ 3000 unique IP adresses a day
- a database of 486.000 passwords and 200.000 usernames
- 5 sensors

Thank you for your attention!

abel.gonda@nki.gov.hu

Learn more about the GovProbe Honeypot!

Podcast episode

LinkedIn Post

SPECIAL SERVICE FOR NATIONAL SECURITY

*** 1996 ***

Fortes fortuna adiuvat

NATIONAL
CYBER SECURITY CENTER
HUNGARY