

Alfa a Omega v Kybernetickej bezpečnosti (KB)

ATOS Cyber Security, Maro Duda

Stačí poznať týchto 60 jednoduchých hesiel a môžete ovládať botnet z pol milióna IoT zariadení

ponsored
aware to

Na naše školy denne útočia hackeri. Podľa auditu prvých troch

ODPORÚČAME

Kontrola sietí odhalila stovky nebezpečných útokov. Pokusov o prelomenie zabezpečenia bolo 122-tisíc.

dnes 00:00 Autor: Martin Hodás

13
zdieľaní

 Zdieľaj na Facebooku

V hornej časti zobrazenej strany sa objaví falošná inf
problém je údajne možné vyriešiť kliknutím na odk
podobným útokom zaistené, bezpečnosť webu nebo
CyberSecu

takto v noci zo soboty i

l DVRs were infected
at leading sites



ČO ROBIŤ?

Ako postupovať krok za krokom k lepšej KB?



Kam ideme?

**AUDIT
SECURITY
MANAGEMENT
- alebo -
Certifikačný
AUDIT**

**Čo potrebujeme
zobrať do úvahy?**

- Čas
- Postupy
- Technológie
- Ľudí
- Peniaze
- Zákony

**Ako sa tam
dostaneme?**

**Musíme pokryť
všetky
nedostatky
identifikované v
audite**

Aké sú míľniky?

**Zabezpečiť, že váš plán
je realistický a má
kontrolu kvality
pre každý definovaný
míľnik**

Prístup Atos-u

Pochopiť

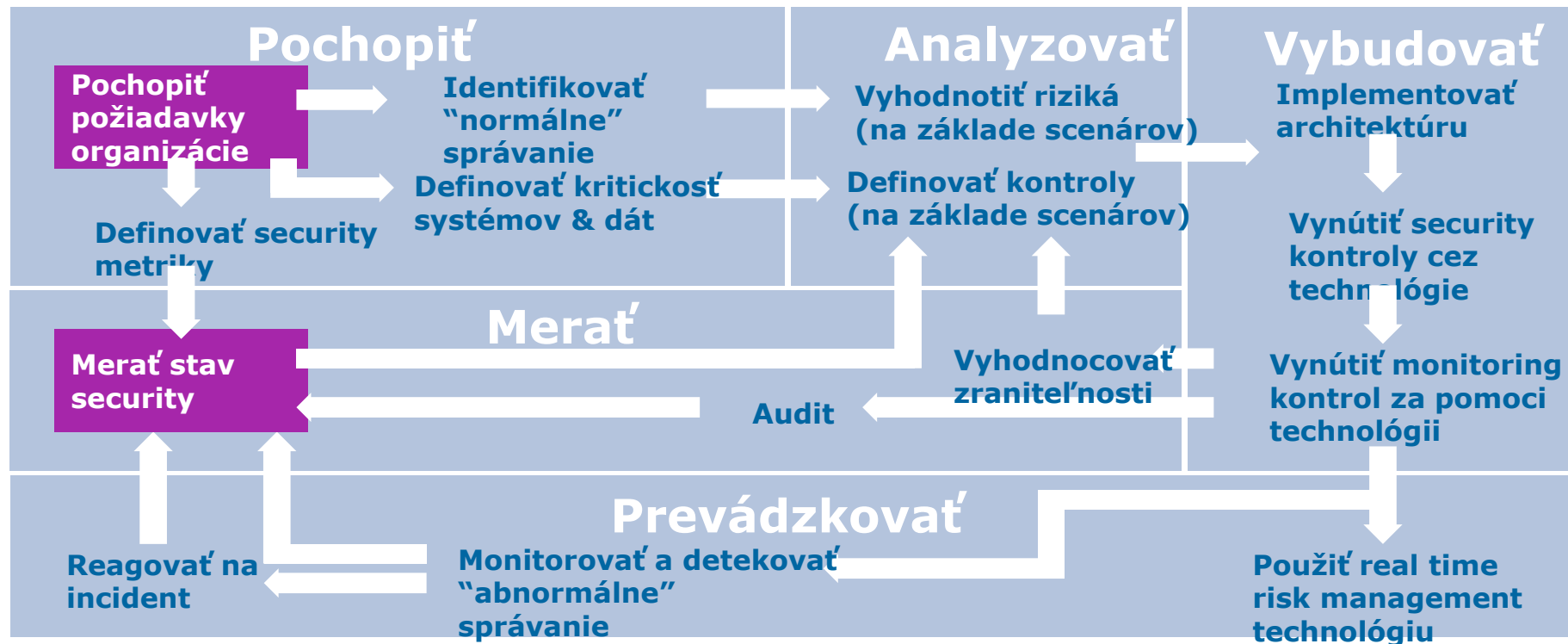
Analyzovať

Vybudovať

Merať

Prevádzkovať

...na základe "best practices"



3x “musíte” na ochranu IT systémov

Pochopiť

Musíte #1:

Definovať na mieru ušitý rámec pre kybernetickú bezpečnosť

Analyzovať

Vybudovať

Musíte #2:

Vybudovať kyber-bezpečnostné technologické kapacity

Merat'

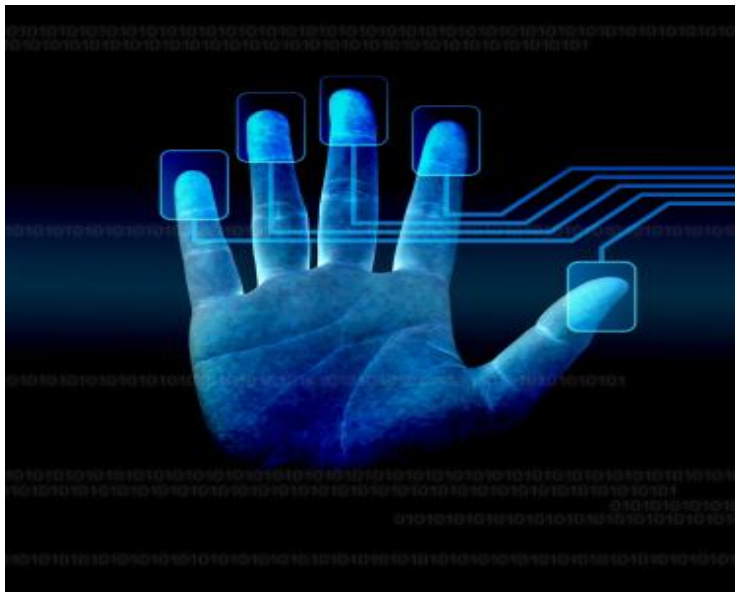
Musíte #3:

Prevádzkovať kyber-bezpečnostnú infraštruktúru

Prevádzkovať

Kybernetická bezpečnosť (KB)

10 krokov k lepšej KB?



1. IT Bezpečnostný Expert(i)
2. IDENTIFIKOVAŤ Všetky IT Aktíva
3. IDENTIFIKOVAŤ „Zlaté nugety“
4. IDENTIFIKOVAŤ Všetky KB RIZIKÁ
5. NAPLANOVAŤ Strategický & taktický PLÁN
6. Vypracovať a implementovať KB PROCESY
7. INVESTOVAŤ do KB technológií
8. IMPLEMENTOVAŤ metriky pre KB
9. Vypracovať a implementovať KB Procesy
10. Zvýšiť povedomie o KB

Ja to všetko?

ÁNO!

PRE ZAČIATOK!

Kyber-Bezpečnosť (KB) Minimum

Čo obyčajne chýba?

Zabezpečenie fyzického prístupu

Procesy

Politika Hesiel

KB pracovníci

Monitoring Kyber-Bezpečnosti

Segregácia rolí

RIEŠENIE PRE zdieľanie privilegovaných oprávnení (ROOT / Admin)

Centralizovaný monitoring KB udalosti a incidentov(SIEM)

Hardening systémov (vdďaka chýbajúcim baselinom ALEBO opatrení)

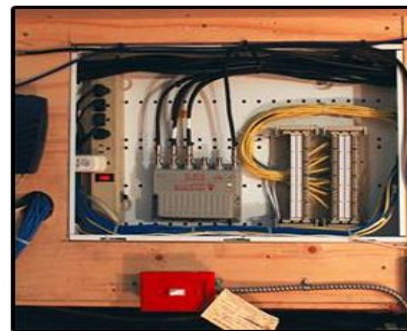
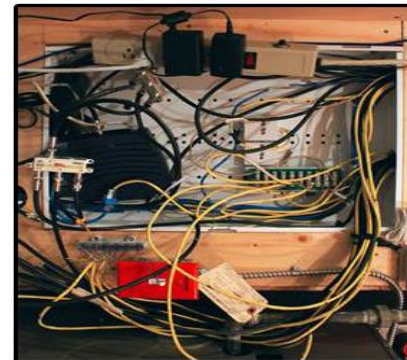
Antivírusová a Malware Ochrana

Sieťová Bezpečnosť

Zlé praktiky pri programovaní

SPRÁVNY prístup manažmentu a zamestnancov ku KB

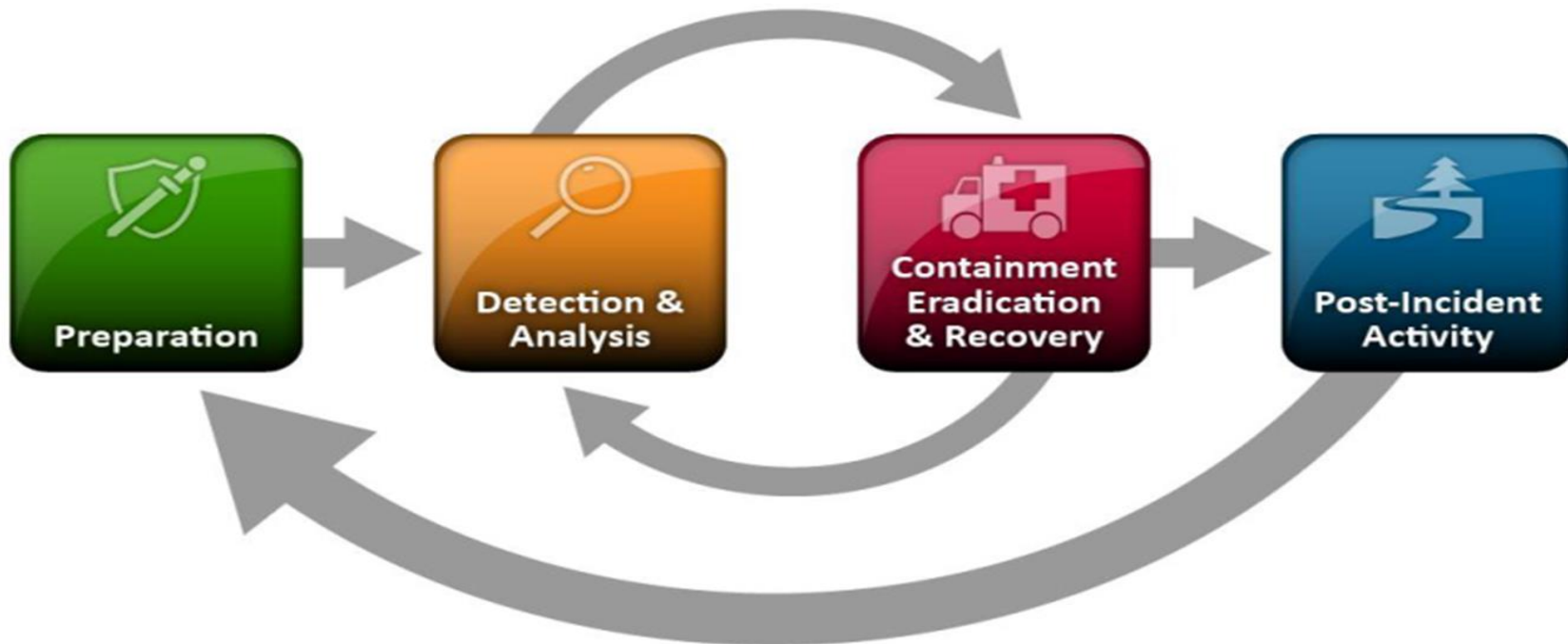
... OVEĽA VIAC ...



AtoS
CYBER
security



Životný cyklus IT Security Event/Incident



SOC/CSIRT/ ... ATOS MODEL

Security Operations Center – L1, 7x24 onsite

- Communication
- Monitoring, alarms investigation & response
- CSIRT P3/P4 incident handling, communication, coordination, for all CSIRT incidents
- Vulnerability reporting
- 1st line activities cross all other GSS services

AHPS

L2/L3

Atos High Performance Security

5x10 business onsite
7x24 standby

Customer
onboarding
projects

Infrastructure
maintenance

CSIRT

L2/L3

Cyber Security Incident Response Team

5x10 business onsite
7x24 standby

Computer
Forensics

Cyber
Security
Incident
Management

Threat
Management

Endpoint and Perimeter Threat Management L2/L3

5x10 business onsite
7x24 standby

Vulnerability Management L2/L3

5x10 business onsite
7x24 standby

Identity & Access Management L2/L3

5x10 business onsite
7x24 standby

DETEKCIA
SIEM monitoring

REAKCIA

OCHRANA
(Protection)
AV/Malware/IDS/
IPS/Proxy/NGFW

DETEKCIA

OCHRANA

Takže čo je Alfa a Omega v Kybernetickej bezpečnosti?

Alfa = uvedomiť si, že Kybernetická Bezpečnosť som Ja, ty, vy, komerčná firma, štátna firma, proste kybernetická bezpečnosť je o všetkom čo je/môže byť IT/ICT

Omega = Manažment Kyber-bezpečnosti

Dakujem

For more information please contact:

Marian Duda

M+ 421 903 416 694

marian.duda@atos.net

Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Unify, Yunano, Zero Email, Zero Email Certified and The Zero Email Company are registered trademarks of the Atos group. April 2016. © 2016 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

