CYBERGYM® EUROPE
EXPECT THE UNEXPECTED

Dopady Průmyslu 4.0 na kybernetickou bezpečnost

Ing. Tomáš Přibyl
Ing. Michal Kohút

Průmysl 4.0 – Kyberneticko-fyzicko-sociální revoluce

- Zásadním způsobem mění povahu průmyslu, energetiky, obchodu, logistiky a dalších částí hospodářství
- V centru stojí průmyslová výroba
- Jádrem je spojení virtuálního kybernetického světa se světem fyzické reality
- **Zcela nová filosofie přinášející celospolečenskou změnu (standardizace, bezpečnost, právo,…)**
  - Dojde k propojení senzorů, strojů a IT systémů mimo hranice dané firmy
  - Tyto CPS budou komunikovat na bázi Internetu, budou předvídat poruchy a konfigurovat samy sebe

Průmysl 4.0 a bezpečnostní rizika

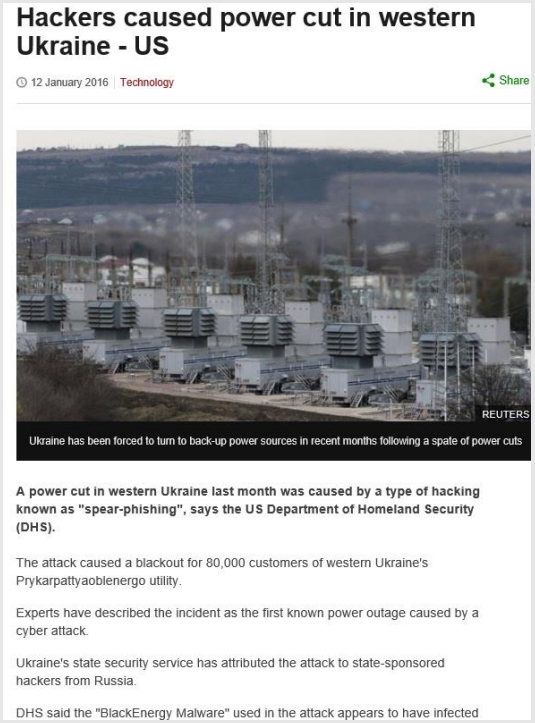
- Motivace útočníků
  - Konkurenční boj (dnes 9%) - zcizení duševního vlastnictví, zničení výroby
  - Cyber jako bojový nástroj (dnes 5%) - vyvolání chaosu, ztráty na životech, ekologické katastrofy
  - Finanční motivace - zcizení peněz z účtu podniků
- Průmysl 4.0 zvyšuje „operační prostor“ útočníkům
  - Pestrost vektorů vedení útoku díky propojeným systémům
  - Sběr informací o potencionálních cílech útoků z „chytrých“ zařízení
  - Očekává se významný nárůst ekonomicky motivovaných útoků na výrobní infrastrukturu
  - Očekává se nárůst útoků, kde bude zneužito kybernetického prostoru jako bojového nástroje

Průmysl 4.0 – rizikové oblasti

- Průmyslové sítě (otevřená a nešifrovaná komunikace, budou se dále otevírat vnitřní integraci a vnějšímu světu)
- Dodavatelsko –odběratelský řetězec (díky horizontální propojitelnosti systémů)
- Průmyslové řídící systémy (PLC, SCADA, HMI)
  - Zastaralé a neošetřené provozní operační systémy
  - Modifikace či zničení SW v PLC zařízení
  - Podvržení informací o stavu regulovaných veličin v HMI zařízeních
- Člověk jako nejslabší článek bezpečnosti
  - Jeho chování v rizikovém prostředí
  - Chybovost ve vývoji SW, správě technologií

Průmysl 4.0 – dopady kybernetických útoků

- Ztráta ovladatelnosti systémů
- Ztráta systémové dostupnosti
- Zhoršení výkonu
- Manipulace a ztráty dat
- Poruchy s dopadem na lidské zdraví
- Poruchy s dopadem na životní prostředí
- Finanční ztráty



Hackers caused power cut in western Ukraine - US

12 January 2016 | Technology

Share

REUTERS

Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

A power cut in western Ukraine last month was caused by a type of hacking known as "spear-phishing", says the US Department of Homeland Security (DHS).

The attack caused a blackout for 80,000 customers of western Ukraine's Prykarpattyaoblenergo utility.

Experts have described the incident as the first known power outage caused by a cyber attack.

Ukraine's state security service has attributed the attack to state-sponsored hackers from Russia.

DHS said the "BlackEnergy Malware" used in the attack appears to have infected

Průmysl 4.0 – komplexní pohled na bezpečnost I.

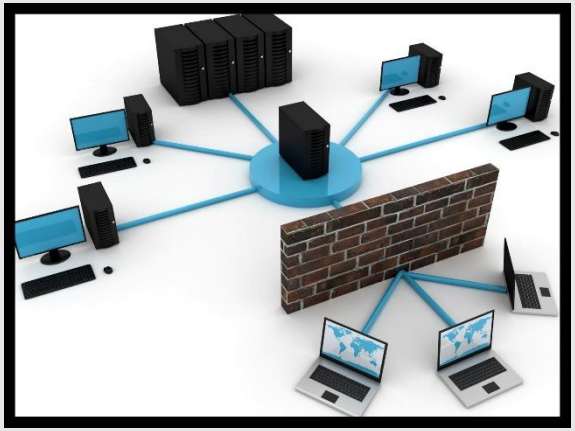
- Bezpečnost musí součástí projektové dokumentace systémů Průmyslu 4.0 „Security by Design“
- Opatření v procesní rovině
  - Ukotvení a zprovoznění procesů spojených s řízením bezpečnosti (každý podnik bude nucen – povinen mít bezpečnostní management)
  - Funkční procesy obnovy ze záloh, řízeného odstavení a efektivního krizového rozhodování
  - Bezpečnostní dohled – CERT/CSIRT
  - Certifikace komponent a bezpečnostních řešení (úroveň, kompatibilita)

Průmysl 4.0 – komplexní pohled na bezpečnost II.

- Technologické hledisko
  - Doplnění bezpečnostních technologií do systémů pro prevenci a detekci bezpečnostních incidentů
  - Doplnění systémů pro behaviorální analýzy
  - Přidělení a užívání unikátního identifikátoru pro každý element systému („Security Passport“)
- Práce s lidským faktorem
  - Posílení celkové vzdělanosti – prevence ve správě, vývoji
  - Zvýšení detekčních schopností kybernetických incidentů
  - Kompetence spojené s minimalizací škod a ztrát způsobených incidenty
  - Bezpečnost jako součást firemní kultury

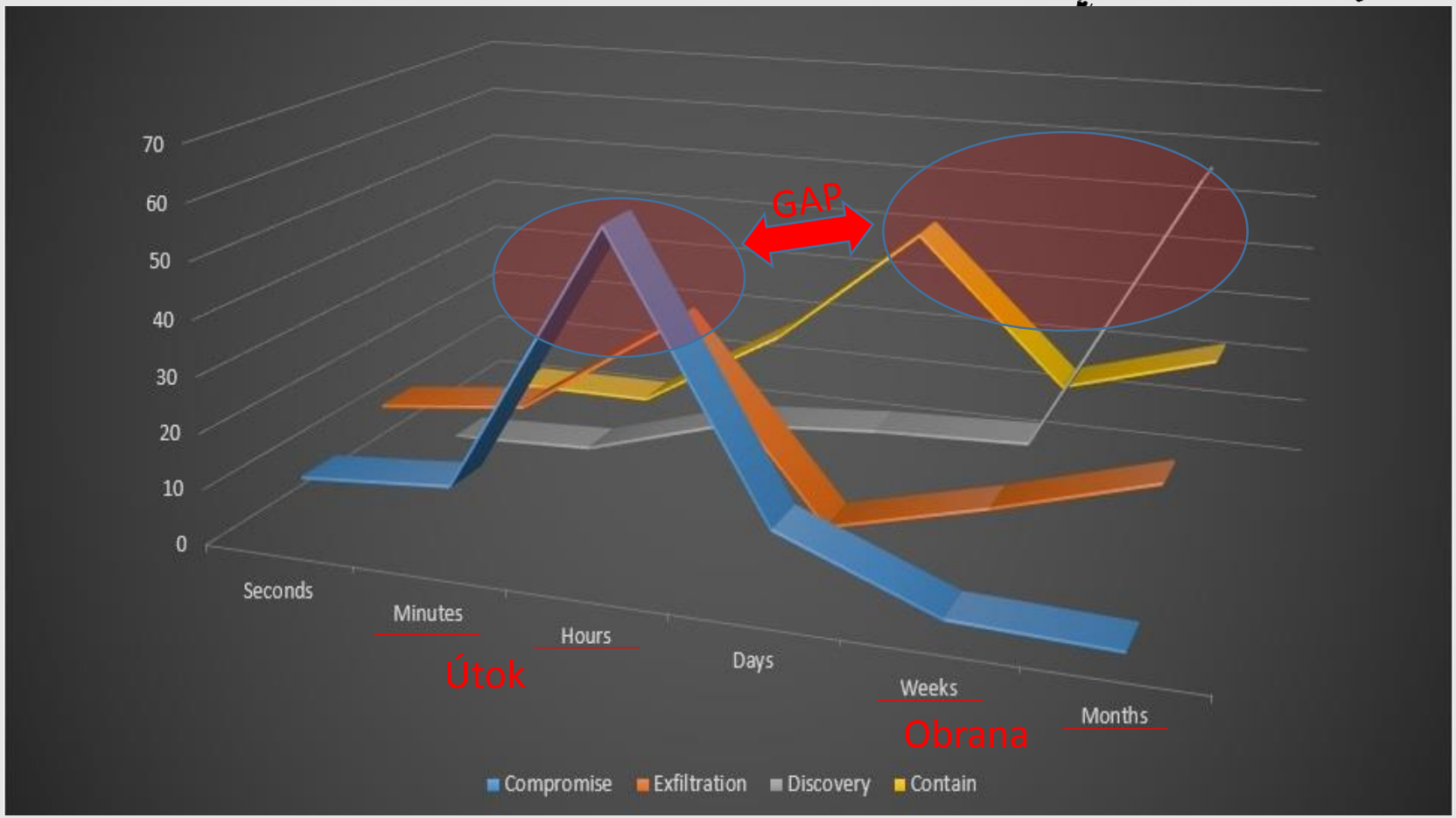
Člověk je největší slabinou

- Bezpečnost se stala **technologicky orientovanou** – útočníci si vždy najdou cestu
- Podle studie PWC: 95% budgetů jde na bezpečnostní technologie, 85% útoků využívá lidského faktoru



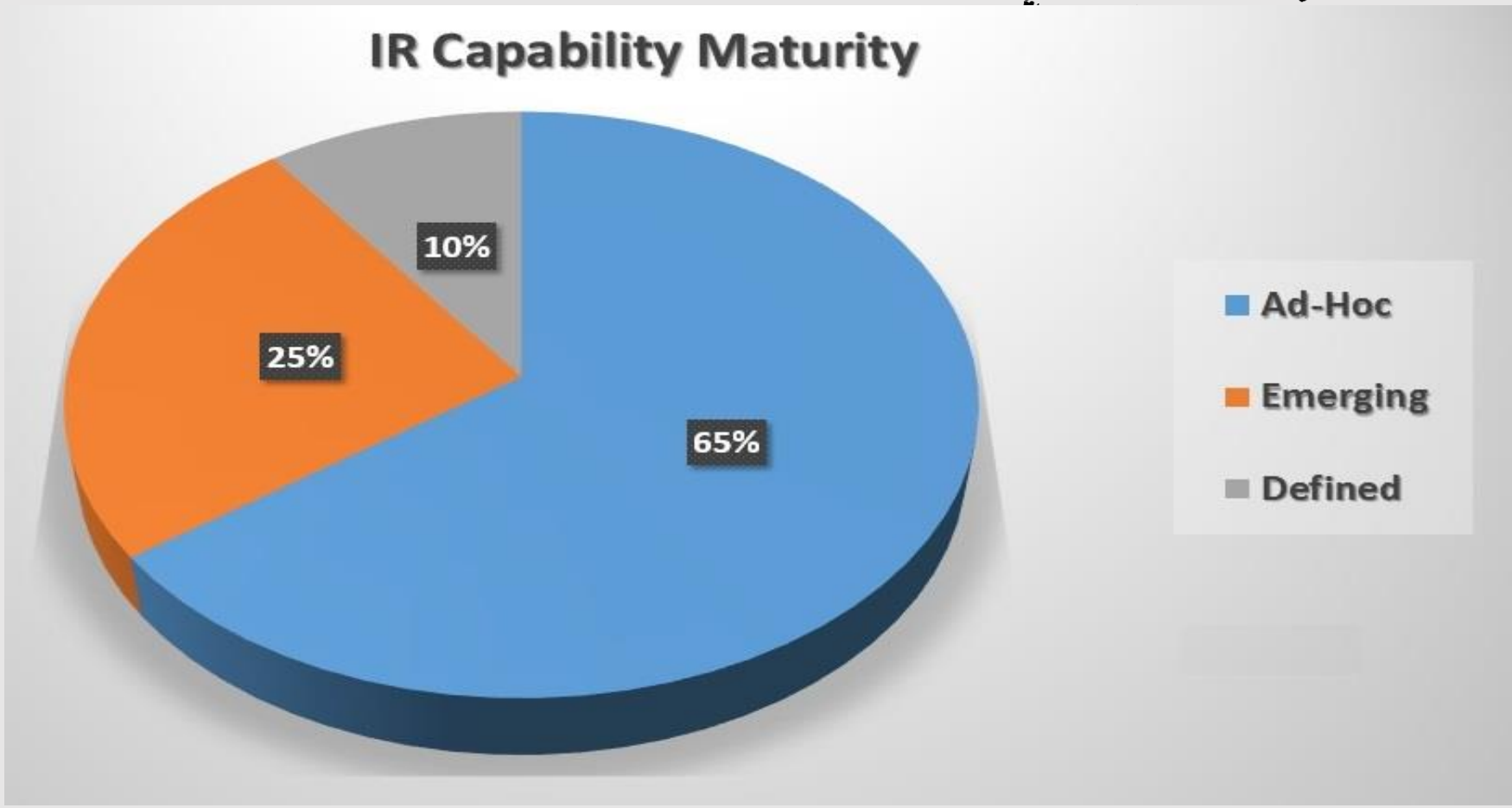
- Člověk je **zdroj chyb v IT**
  - Vývoj technologií
  - Vývoj aplikací
  - Provoz informačních systémů
- Člověk je **nástrojem vedení útoků**
- Člověk je **klíčový článek** v kybernetické obraně
  - V okamžiku, kdy útočník překoná bezpečnostní systémy

Výzvy v moderní kybernetické obraně



Source: Verizon report

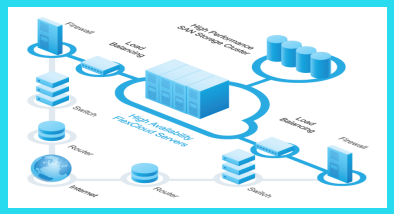
Schopnosti zákazníků v oblasti Incident Response



Source: Verizon report

Základní filosofie tréninkového konceptu

Schopnost emulace Zákaznické infrastruktury (procesů) pro všechny fáze dle CKM



Špičkoví hackeři (**Red tým**) používající scénáře s vojenským pozadím, trénující zákaznický tým.

1

2

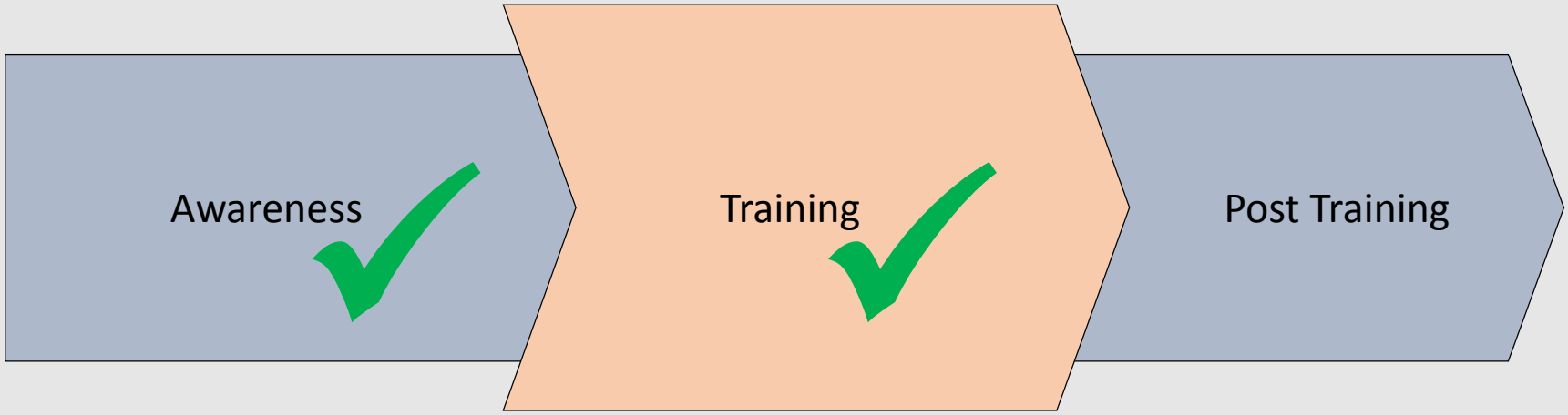
3

4

Metodika pro nabytí dovedností zákazníka ve schopnosti detekovat a minimalizovat ztráty z útoků

Báze **profesionálních scénářů** (s armádním pozadím) pro trénování obranných týmů.

Základní produktová nabídka CyberGym Europe



- **Cyber Defense Excercise pro IT specialisty**
- **Cyber Defense Excercise pro IT security**
- **Manažerský workshop**

- **CyberGym Trénink (Detekce a Incident Response)**

- **Security Roadmap**
- **Nastavení a zavedení SIEM**
- **Zavedení SOC**
- **SOC Team outsourcing**
- **Security „as a service“**
- **Další služby: Forenzní analýzy, IR scénáře, revize architektur, Q&A služby**

Změna přístupu ke kybernetické bezpečnosti

Human centric ?

- Bezpečnost jako součást firemní kultury
  - Týmová obrana
  - Metodika
  - Změna přemýšlení lidí

Compliance ?

- NIS, NIST, National Cyber Strategy, Cyber Act
  - Kritická infrastruktura
  - Auditní zprávy

Product centric ?

- Existující bezpečnost založená na produktech
  - SIEM, IDS, IPS..
  - Rozpočty x Rizika

Průmysl 4.0 – role státu v bezpečnosti Průmyslu 4.0

- Obecně posílení regulace kybernetického prostoru
- Speciální pozornost tam, kde jsou dopady na lidské zdraví či životní prostředí
  - Nutno realizovat řadu opatření legislativních, normalizačních, technických i organizačních na straně státu
- Nutno rozšířit definici kritických infrastruktur
  - Fyzické systémy (datové sítě, centra, objekty robotického charakteru)
  - Virtuální systémy (sociální sítě, SW pro fyzické systémy)
  - Autonomní systémy (autonomní funkce na základě SW)
  - Systémy s umělou inteligencí (samostatné rozhodování)

Průmysl 4.0 – role státu v bezpečnosti Průmyslu 4.0

- Certifikace bezpečnostních řešení používaných Průmyslem 4.0
  - Bezpečnostní složky musí mít možnost ověřovat zavedení a dodržování standardů
- Podpora práce silových resortů pro práci s kritickou infrastrukturou
  - Nutno realizovat řadu opatření legislativních, normalizačních, technických i organizačních na straně státu
  - Technické vybavení pro efektivní zapojení IZS
- Oficiální doporučené postupy pro bezpečnost Průmyslu 4.0
- Stát musí být připraven a schopen provádět ve vynucených případech zásahy do systémů, jejich dozor a kontrolu

CYBERGYM® EUROPE
EXPECT THE UNEXPECTED

Buďte připraveni na „EXPECT THE UNEXPECTED“!