Shrnutí konference Future of Cyber, únor 2026

Konference **Future Cyber Defence**, která proběhla v prostorách společnosti Cisco Systems, se zaměřila na kritické aspekty moderní bezpečnosti, od krizové připravenosti až po roli umělé inteligence (AI) v kybernetické obraně i útocích. Akce sloužila jako odborný úvod k nadcházející konferenci SCADA Security a podzimnímu Future Forces Forum.

Níže je podrobné shrnutí klíčových témat a závěrů z obou hlavních diskuzních panelů:

1. Krizové řízení a krizová připravenost

Hlavním tématem první části byl zásadní rozdíl mezi krizovým řízením a krizovou připraveností. Zatímco **krizové řízení** je reaktivní proces spouštěný v momentě vzniku problému, který je často doprovázen chaosem a neefektivní komunikací, **krizová připravenost** se buduje léta předem, aby následné řízení krize bylo efektivní.

• **Motto „Nebuďte nejslabším článkem“:** Účastníci zdůraznili, že každý subjekt – od jednotlivce přes firmy až po stát – musí převzít odpovědnost za svou vlastní odolnost.

• **Projekt 72 hodin:** Odborníci apelovali na potřebu soběstačnosti. V případě krize (např. výpadek energií či povodně) by lidé i firmy měli být schopni přežít prvních 72 hodin bez přímé pomoci záchranných složek, které se musí prioritně věnovat záchraně životů.

• **Problémy v praxi:** Častým neduhem firem je formální přístup k plánování. Plány krizové připravenosti jsou často aktualizovány až těsně před kontrolou („včera“), což znamená, že v reálné situaci nejsou funkční a lidé neznají své role.

• **Měření připravenosti:** V IT a bezpečnostním světě se připravenost měří pomocí metrik jako **Mean Time to Detect** (čas do detekce), **Mean Time to Respond** (čas na odpověď) a **Mean Time to Coordinate** (čas na koordinaci).

• **Legislativa a NIS 2:** Nový zákon o kybernetické bezpečnosti (implementující směrnici NIS 2) přináší zásadní změnu: **osobní a trestní odpovědnost manažerů** za zanedbání bezpečnosti, což by mělo motivovat vedení firem k reálnému zájmu o ochranu aktiv.

2. Umělá inteligence (AI) a bezpečnost

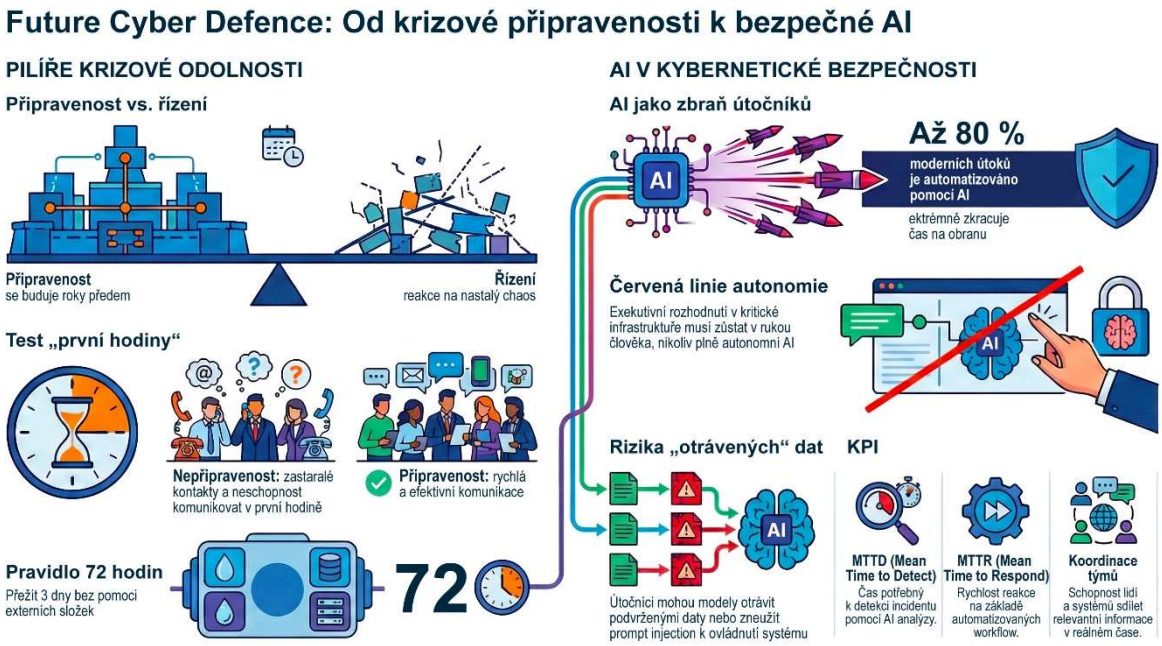
Druhý panel prozkoumal AI jako transformativní technologii, která mění pravidla hry v kyberprostoru. Diskutovalo se o její historii, současných hrozbách i budoucím potenciálu.

• **Rizika a útoky:** AI umožňuje extrémně rychlé škálování útoků. Objevují se hrozby jako **AI-driven malware**, autonomní agenti schopní samostatně prohledávat sítě, **Data Poisoning** (otrávení trénovacích dat) nebo **Prompt Injection** (zneužití modelu skrze vstupy).

• **Geopolitika a závislost:** Evropa je v oblasti vývoje AI vnímána jako „druhá liga“ za USA a Čínou. Existuje riziko závislosti na cizích modelech, které mohou v sobě nést kulturní a etické hodnoty svých tvůrců (např. čínské modely blokující politicky citlivá témata).

• **Příležitosti pro obranu:** AI má obrovský potenciál v prediktivní analýze a detekci hrozeb. Pomáhá zkrátit tzv. **Time to Patched Gap**, tedy dobu mezi objevením zranitelnosti a nasazením obrany.

• **Lidský faktor a „červená linie“:** Navzdory pokroku musí konečné rozhodnutí v kritických situacích (např. odstavení elektrárny) zůstat na člověku. AI může halucinovat nebo dělat chyby, za které nese právní odpovědnost člověk.



3. Výhled do budoucna (5–10 let)

Konference zakončila pohledem do budoucna, kde se očekává příchod **AGI (obecné umělé inteligence)** a rozvoj **kvantových technologií**.

• **Kvantové počítače:** Tyto stroje mohou v horizontu deseti let zásadně změnit možnosti šifrování a optimalizace obranných scénářů.

• **Integrace do fyzického světa:** AI se bude stále více přesouvat z kyberprostoru do fyzické reality (robotika, autonomní řízení), což přinese nové bezpečnostní výzvy.

• **Doporučení:** Jedinou cestou k přežití v takto rychlém prostředí je neustálé vzdělávání, využívání AI k vlastní obraně a zajištění, aby technologický pokrok neodstavil člověka z rozhodovacích procesů.

Konference byla uzavřena pozvánkou na další odborné akce, včetně březnové **SCADA Security** a podzimního **Future Forces Forum** v Letňanech, kde bude téma bezpečnosti dále rozvíjeno i v rámci specializované Live hacking zóny.