**TISKOVÉ ODDĚLENÍ**

**MINISTERSTVA OBRANY ČESKÉ REPUBLIKY**

**Datum**: 20. května 2021

##### Téma: Unikátní cvičení kybernetické bezpečnosti pro strategické firmy obranného průmysluOčekávané události ve dnech 1. až 9. května 2021

Ministerstvo obrany spolu s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) uspořádalo cvičení kybernetické bezpečnosti pro firmy účastnící se platformy Ministerstva obrany pro kooperaci strategických společností obranného průmyslu ČR a státu. Účastníci z řad top managementu i zaměstnanců těchto firem, pracovníci obou zmíněných institucí a dále Ministerstva průmyslu a obchodu museli řešit nejen samotné kybernetické útoky, ale také vše, co s kybernetickou bezpečností souvisí, to znamená nejen technické, ale také právní či mediální aspekty a provázanost s krizovým managementem.

Cílem cvičení bylo prověřit připravenost klíčových firem obranného průmyslu na hrozby související s kyberprostorem. Proto byl scénář cvičení připraven na míru, aby se účastníci museli vypořádat se situacemi, s nimiž se mohou reálně setkat a které jsou zasazeny do jim známých kulis. Scénář je koncipován jako hybridní kampaň zahrnující celou škálu hrozeb, které má na svědomí neznámý státní aktér.

**Proměna bezpečnostního prostředí a nutnost spolupráce státu a soukromého sektoru**

V poslední dekádě došlo k zásadní proměně bezpečnostního prostředí. Zvýšil se počet útoků na poskytovatele strategických produktů, technologií a služeb ze soukromého sektoru. Tyto útoky se staly rozšířenou alternativou ke konvenčnímu válčení a prakticky mažou hranici mezi národní bezpečností a situací v soukromém sektoru, který se v tomto ohledu stává důležitým aktérem národní bezpečnosti. Aby bylo možno tomuto novému typu hrozeb čelit, je třeba úzká spolupráce mezi státem a soukromým sektorem.

 „Obranný průmysl je klíčovým prvkem českého hospodářství s mnohaletou tradicí a světovými kvalitami. Jsem rád, že jsou to právě firmy našeho obranného průmyslu, které si uvědomují závažnost současné situace a jako první se zapojují do této iniciativy zorganizované společně Ministerstvem obrany a Národním úřadem pro kybernetickou a informační bezpečnost,“ říká náměstek sekce průmyslové spolupráce ministerstva obrany Tomáš Kopečný.

Právě za účelem systematické spolupráce mezi státem a strategickými firmami soukromého sektoru byla vybudována platforma pro cvičení tohoto typu. Jejich smyslem je kooperace mezi státem a nejvyšším managementem českých strategických společností s cílem navýšení odolnosti celé české společnosti. Tu zajistí bezpečné, stabilní a konkurenceschopné strategické společnosti k čemuž jim maximálně pomůže stát. Platforma buduje spolupráci na třech úrovních, kterými jsou výměna bezpečnostních informací, edukační workshopy o bezpečnostních hrozbách a simulace útoků.

**Kybernetické hrozby mají mnoho dimenzí**

Cvičení mělo dále ukázat multidimenzionální charakter kybernetických hrozeb. „Jde nám o to předvést cvičícím realitu. V té by nejspíš nešlo jen o kyberútok, ale velmi pravděpodobně by spolu s ním šly i další útoky, například dezinformační. Naším cílem je prověřit, zda je obranný průmysl na takový scénář připraven, a také ukázat, že kyberhrozby nejsou jen technická záležitost, ale že jde o komplexní disciplínu, které musí věnovat pozornost nejvyšší vedení jakékoli organizace,“ vysvětluje ředitel NÚKIB Karel Řehka.

Podstatné je například to, zda krizové plány organizace s takovou situací počítají, znalost právního prostředí a také schopnost efektivně komunikovat s veřejností, případně s dalšími subjekty, jako jsou subdodavatelé či odběratelé. To všechno je pro úspěšně zvládnutí kybernetického útoku naprosto zásadní. V tomto konkrétním případě se jako podstatná ukázala i samotná existence platformy Ministerstva obrany pro kooperaci strategických společností obranného průmyslu ČR a státu, neboť umožňuje efektivní koordinaci všech podstatných subjektů.

**Cílem cvičení není vyhrát, ale umět si představit reálnou situaci a správnou reakci**

Cvičení bylo koncipováno jako netechnické a prakticky k němu stačil papír a tužka. Podstatný je u podobných cvičení scénář založený na postupné eskalaci situace. První části cvičení se účastnili ti pracovníci, kteří by nastalou situaci řešili jako první. Ve druhé polovině nastoupil top management zúčastněných institucí, který měl na základě dostupných informací přijmout rozhodnutí na nejvyšší úrovni. Cvičení se také účastnila řada odborných pozorovatelů, kteří byli připraveni cvičícím v diskuzi poskytnout svoji expertízu.

Vzhledem k průběhu a koncepci cvičení nelze mluvit o tom, zda někdo vyhrál, nebo ne. Podstatné je, že si všichni odnesli informace o tom, jak mohou kybernetické hrozby vypadat a jaké kroky je nezbytné přijmout pro zajištění co nejvyšší míry bezpečnosti. Podobná cvičení také zlepšují kooperaci všech zainteresovaných subjektů a posilují vzájemnou výměnu informací, což je samo o sobě důležitou součástí kybernetické bezpečnosti státu.

Autor: Jana Zechmeisterová, OK MO a Jiří Táborský, NÚKIB