HOSPODÁŘSKÉ NOVINY
KOMERČNÍ PŘÍLOHA HN
čtvrtek, 21. května 2020

OBRANA A BEZPEČNOST

ARMÁDA V ČASE KRIZE

VOJÁCI POMÁHAJÍ I S CHYTROU KARANTÉNOU

Marie Myslíková
autori@economia.cz

Události, které v březnu vyústily až k vyhlášení nouzového stavu, kromě mnoha jiných složek aktivovaly vládním nařízením také Armádu České republiky. Ozbrojené síly se tak mohly ihned zapojit do pomoci integrovanému záchrannému systému, včetně Policie ČR. Svůj první úkol dostala armáda 10. března, kdy nasadila deset tříčlenných týmů na velké hraniční přechody. Vojáci asistovali při odebírání biologických vzorků u lidí, kteří jevili klinické známky onemocnění covid-19.

Podle bývalého náčelníka Generálního štábu Armády ČR, armádního generála Petra Pavla, byla tato okamžitá reakce možná díky tomu, že armáda má v časech míru vyčleněné určité síly, jež slouží k podpoře bezpečnostních složek pro vnitřní bezpečnost. „Je to něco přes tisíc lidí s technikou pro specifické úkoly. Souhlas je předjednaný, takže akce může proběhnout skutečně rychle. Pokud by bylo potřeba nasadit více lidí, musí si je ministr vnitra vyžádat," říká a zároveň upozorňuje, že ministerstvo obrany ani náčelník Generálního štábu nemají v tomto ohledu volnou ruku. „Jejich činnost koordinuje a řídí vláda, respektive Ústřední krizový štáb."

Jen na ochranu hranic nakonec armáda nasadila téměř tři tisíce lidí. K dispozici dala své přepravní kapacity a účastnila se prvních dodávek ochranných prostředků. Absolvovala stovky cest s nákladními auty, vojáci vykládali letadla a rozváželi pomoc po celém Česku. Poskytuje i specializovanou pomoc, ať už zdravotnické prostředky či specialisty epidemiology.

Dalším úkolem, na němž armáda pracuje, je projekt takzvané chytré karantény. „Tam máme k dispozici 300 lidí, z nichž je momentálně nasazeno něco přes dvě stě. Jsou součástí centrálního řídicího týmu, který koordinuje nasazení veškerých prvků vojenského zdravotnictví. Dále tvoří mobilní odběrové týmy u lidí, kteří se nemohou dostat na odběrová místa, a naši medici pomáhají krajským hygienickým stanicím s trasováním kontaktů," vysvětluje brigádní generál Zoltán Bubeník, ředitel sekce vojenského zdravotnictví ministerstva obrany. Liberečtí chemici navíc pomáhají s dezinfekčními týmy krajským hasičům, další vojáci jsou k dispozici v domovech pro seniory.

Koronavirus přinesl dílčí změny

I přesto, že jsou čeští vojáci nyní spolu s civilními zdravotníky, policisty i hasiči součástí první linie a před propuknutím pandemie samozřejmě cestovali po světě pracovně i soukromě, nákaza se jim prozatím téměř vyhýbá. Generál Zoltán Bubeník se domnívá, že jedním z hlavních důvodů je, že armáda na blížící se nebezpečí reagovala dříve než civilní sektor. „V době, kdy vláda vydávala pouze doporučení, jsme sice nezakazovali odjezdy, ale aplikovali jsme bez pardonu tvrdou karanténu pro každého, kdo se vrátil ze zahraničí. Tato opatření a správná ochrana se zejména v začátcích, kdy se nemoc hodně šířila, ukázaly jako efektivní."

Armáda se také na základě získaných informací o nákaze mohla dobře připravit na další dny a týdny i na případnou druhou vlnu nákazy. Změnila systém organizace práce v útvarech, v kancelářích i ve výcviku vojáků, doplnila zásoby osobních ochranných pomůcek a i nadále sleduje doporučení ministerstva zdravotnictví a analyzuje poznatky, které získala.

TĚCHONÍN

Stát sice specializovanou infekční nemocnici v Těchoníně na Orlickoústecku během aktuální pandemie využil, ale jen v souvislosti s jejími personálními kapacitami, experty a výzkumem. Těchonín jako takový nebyl aktivován, i když se o tom několikrát uvažovalo. Důvodem, proč nakonec zůstal v neaktivním stavu, byla neefektivita – nemocnice má k dispozici 28 lůžek pro ty nejtěžší případy nákazy typu ebola. V případě koronaviru je mnohem efektivnější využít zkušenosti vojáků-zdravotníků v civilních nemocnicích, kde se od nich ostatní učí používat řádně ochranné pomůcky či zacházet s kontaminovaným materiálem.

ILUSTRAČNÍ FOTO: HN - LIBOR FOJTÍK (NA SNÍMKU DOBROVOLNÉ VOJENSKÉ CVIČENÍ VE VYŠKOVĚ)

Generál Petr Pavel soudí, že by takovou revizi měl udělat celý stát. „Měli bychom využít tento oddechový čas, kdy je epidemie na ústupu, pro zlepšení toho, co fungovalo hůře, než bychom si přáli, abychom byli dobře připravení, kdyby přišla druhá vlna," myslí si Pavel.

Do pomoci se zapojilo i NATO

Debaty ohledně pandemie se dostaly i na půdu NATO. Společná opatření například ve vztahu ke strategické přepravě se podle oslovených generálů ukázala jako flexibilní. Uspořádání, kdy všechny alianční země mohou využívat přepravní kapacity, třeba transportní letouny Antonov An-124 Ruslan, bylo podle nich klíčové.

V rámci aliančního projektu SALIS, umožňujícího rychlou vzdušnou přepravu těžkých nákladů po světě, má totiž členský stát zakoupen určitý počet letových hodin sloužící hlavně pro obranu. Pokud ale nastane urgentnější krize, mohou se prostředky použít i na zdravotnickou pomoc. Aliance však nejsou primárně vojenské jednotky, je to uskupení států fungující na základě politického konsenzu. Vojska jednotlivých aliančních států jsou pouze jedním z nástrojů řešení civilní nouzové připravenosti.

„Je proto nutné revidovat jednotlivé pandemické plány, vývoj a výrobu inovativních materiálů, které se potom dají použít jako ochranné prostředky," říká generál Bubeník. Petr Pavel, který v letech 2015 až 2018 působil také jako předseda vojenského výboru NATO, poukazuje i na propojení vědeckých pracovišť v rámci NATO.

„Je třeba sloučit zdroje na výzkum a vývoj do většího balíku, který už bude dávat smysl při vytváření efektivnějších protiepidemických opatření pro všechny členy NATO," vysvětluje generál Pavel.

ROZHOVOR

STRATEGIE TĚCH, KDO USILUJÍ O NABOURÁNÍ SOUKROMÍ
HACKER SI MŮŽE VYDĚLAT I ČISTĚ

KAROL SUCHÁNEK, EXPERT NA KYBERNETICKOU BEZPEČNOST

Michal Večeřa
autori@economia.cz

V 16 letech vyvinul svůj první bezpečnostní software, absolvoval speciální kyberbezpečnostní program na Massachusetts Institute of Technology (MIT), je držitelem bezpečnostní prověrky NATO. Posledních 10 let se stará o soukromí a bezpečnost firem a veřejně známých osobností po celém světě. „Třetí světová válka, která jednoznačně už v on-line světě probíhá, je bojem technologií a potažmo peněz. Kdo jich má víc, je napřed ve vývoji," tvrdí odvážně.

Kdy se stala kybernetická bezpečnost nedílnou součástí společnosti?
V obecné rovině tu byla už od 70. let minulého století, tedy dřív než většina lidí vůbec vlastnila počítač. Mediální zájem si tento fenomén získal hlavně kolem roku 2013 díky aféře Edwarda Snowdena. Ten jako zaměstnanec CIA zveřejnil informace o masivním a do té chvíle utajovaném celosvětovém sledování telefonů a elektronické komunikace ze strany bezpečnostních služeb USA. Během posledních let se pak o různých únicích dat a nabourání soukromí dozvídáme z médií téměř denně. A jde o závratná čísla co do počtu lidí, jejichž data se tak dostávají do nepovolaných rukou.

> Hotelová síť Marriott v roce 2018 zjistila, že jí někdo přes díru v IT infrastruktuře už celé čtyři roky krade data o zákaznících.

Můžete být konkrétní?
Třeba hackerský útok na americký registr dlužníků Equifax v roce 2017 se dotkl 147 milionů lidí, což bylo v té době 56 procent Američanů. Hackeři mají oproti jiným zlodějům velmi specifické postavení. Když vám někdo přes noc ukradne auto, ráno o tom víte a můžete to začít řešit. U útoků na informační systémy ale není výjimkou, když jsou data kontinuálně a bez povšimnutí kradena po dobu týdnů, měsíců, či dokonce let, podle sofistikovanosti celého postupu. Například hotelová síť Marriott zjistila v roce 2018, že jí někdo přes díru v IT infrastruktuře krade data o zákaznících už celé čtyři roky.

Velké firmy jsou tedy tou hlavní bezpečnostní dírou?
U velkých firem má hacker celkem logicky šanci na získání velkého množství dat, ovšem bývají zase zpravidla lépe zabezpečené než menší a střední firmy. A právě na ně se teď utočí více. Velmi citlivé jsou i vládní a státní organizace. Z mého pohledu kromě omezených rozpočtů na technologie a lidi hlavně proto, že jednotlivé instituce běží na nejednotné bezpečnostní infrastruktuře. Rozhodně by jim prospěla centralizace standardů a globální bezpečnostní strategie.

Například v energetice se právě z bezpečnostních důvodů mluví naopak o decentralizaci, aby nedošlo k blackoutu při napadení jednoho hlavního zdroje. Není lepší, když hackerským útokem padne jen jedno ministerstvo, a ne všechna?
Jde o propracovanost architektury a nastavení celého systému. Dnes už existují hodně pokročilé možnosti škálování, tak aby při případném útoku nespadl systém celý, ale jen určitá část. Vezměte si například Microsoft Cloud, který denně odráží miliony útoků a nikdy nepadl jako celek. Mnohem bezpečnější je využívat jednu platformu, nad kterou jsou centrálně řízené bezpečnostní standardy, než mnoho různých systémů s tím, že každý si řeší bezpečnost odděleně.

Jaká hrozba zasahuje v celospolečenském měřítku nejvíce lidí?
První linií jsou takzvané phishingové útoky. Tedy podvodná komunikace, nejčastěji e-mailová, která má za úkol vylákat od uživatele buď údaje, nebo rovnou i peníze. Pro hackery, kteří také zvažují své náklady, představuje ekonomicky zajímavý způsob práce. Řídí se trendy, jež v určitém momentě zajímají masu lidí – ať už to jsou Vánoce, volby, v Americe třeba zápasy Super Bowlu nebo dnes koronavirus. E-maily třeba s nabídkou zázračného léku na nemoc covid-19 pak mohou automatizovaně rozesílat na obrovské databáze kontaktů, protože téma rezonuje globálně. Čím větší množství, tím vyšší šance, že se nějaká rybička chytí a svá data poskytne. Může to znít triviálně a většina lidí si řekne, že podvodné e-maily přece rozpozná, ale není tomu tak. Jsou výsledkem stále propracovanějšího sociálního inženýrství, tzv. spear phishingu – podvodné elektronické komunikace zaměřené na konkrétní osobu, organizaci anebo firmu. Nezřídka se útočníkům podaří oblafnout i velmi zkušené uživatele. To byl i případ zásadního úniku dat z portálu Yahoo!, na který se sice přišlo v roce 2016, ale trval od roku 2013. Proto je dnes potřeba se učit dovednosti osobní digitální bezpečnosti.

Dnes jsou tedy útoky zaměřené spíš na to, aby přiměly uživatele k dobrovolnému poskytnutí dat než na instalaci viru?
Viry samozřejmě stále existují a dnes je velkým trendem takzvaný ransomware, který zablokuje počítač tím, že zašifruje jeho data a požaduje výkupné za opětovné zpřístupnění. Hackeři, kteří s tímto nástrojem pracují, jej umí vytěžit opravdu na maximum. Třeba se rozhodnete neplatit výkupné za rozšifrování dat na harddisku, protože je máte zálohovaná jinde. Pak následuje druhý stupeň, a sice vydírání, že vaše data budou zveřejněna. To už pro vás může být problém, zejména kvůli GDPR pokutě, jež vás rozhodně nemine.

„Navazování spolupráce s útočníky vidím jako dost problematické," říká Karol Suchánek.

FOTO: ARCHIV K. SUCHÁNKA

Je zřejmé, že lidská vynalézavost stále hraje i v této oblasti hlavní roli. Daří se také firmám a vládám obracet hackery na svoji stranu?
Jedná se o průmysl sám o sobě. Po celém světě existuje řada výzkumníků, kteří se věnují hledání bezpečnostních děr v jednotlivých systémech. Když na nějakou přijdou, mají dvě možnosti. Buď jít za tvůrcem systému a o chybě mu říct, za což většina hlavních hráčů na softwarovém trhu vyplácí tučné odměny. Nebo ty informace může prodat jiné straně. Stejně jako útočníci si je kupují i vlády – ať už za účelem napadení jiné země nebo vlastní ochrany. Když o díře v systémech vím, mohu si ji hlídat, případný útočník neuspěje a půjde jinam. Pak existuje třeba program Hacker One, propojující etické hackery s firmami, jimž pomáhají zvyšovat bezpečnost odhalováním jejich nedostatků. Ti nejšikovnější si tak přijdou na miliony korun, což je krásná ukázka toho, že si hacker může vydělat i čistě. Nicméně navazování spolupráce s útočníky vidím jako dost problematické z hlediska důvěry. Jak to ale funguje na úrovni bezpečnostních složek států, se můžeme jedině dohadovat. Je asi jasné, že o tom běžný smrtelník nemá tušení.

Jak moc se na kybernetické bezpečnosti, ale i na útocích podílí umělá inteligence?
Umělá inteligence se samozřejmě uplatňuje stále více. Dnes už dokáže hrozby rozpoznávat a sama na ně reagovat a učit se z chyb. Na to opět navazuje forma útoků, kdy se umělá inteligence bude snažit přimět napadený systém k tomu, aby své chyby neopravoval a neučil se z nich. Třetí světová válka, která jednoznačně už probíhá právě v on-line světě, je bojem technologií a potažmo peněz. Kdo jich má víc, je napřed ve vývoji. Velkou otázkou tedy zůstává, kdo jako první dokáže sestrojit kvantový superpočítač. S ním totiž ztratí význam hesla, jak je známe dnes, bude je louskat v reálném čase. Budou ale také vznikat hesla a šifry nová vytvořené právě kvantovým počítačem.