KYBERBEZPEČNOST A NATO

Jak Severoatlantická aliance chrání svůj kyberprostor

Kyberprostor je již od summitu NATO ve Walesu v roce 2014 považován za klíčovou oblast pro zajištění kolektivní obrany a fungování Severoatlantické aliance. Kyberprostor a informační technologie dnes zajišťují funkčnost ozbrojených sil a propojují všechny oblasti boje. Na summitu ve Varšavě v roce 2016 Aliance přijala kyberprostor jako možnou pátou dimenzi vedení boje (kromě země, moře, vzduchu a blízkého vesmíru), takže i na tomto poli musí být schopna se efektivně bránit. Závěrečné komuniké varšavského summitu explicitně uvádí, že „kybernetické útoky stejně ničivé pro moderní společnost jako konvenční útok". NATO se proto rozhodlo vybudovat adekvátní schopnosti k provádění operací v kyberprostoru, včetně vytvoření efektivního modelu spolupráce s různými národními aktéry ze zemí NATO.

Role NATO spočívá zejména v:

1) ochraně aliančních síťových systémů
2) asistenci členským zemím, jež jsou odpovědné za ochranu svých národních sítí.

Mezi temné stránky využití kyberprostoru patří i ilegální aktivity. Máme-li na mysli především činnost jednotlivců či organizovaných skupin páchanou např. za účelem obohacení, lze mluvit o kyberkriminalitě a související **kyberbezpečnosti (cybersecurity)**.

Kyberprostor však může být využíván nestátními (teroristické a zločinecké organizace, ale i aktivisté typu Anonymous) či státními aktéry i za účelem špionáže, propagandy či narušení nepřátelských počítačových systémů **ve smyslu vojenských operací**. Pokud je kyberprostor použit jako zbraň, jedná se o kyber-konflikt či kyber-válku a mluvíme o potřebě **kyberobrany (cyberdefence)**.

Nejznámějšími kybernetickými incidenty na mezinárodní scéně jsou:

- **útoky na Estonsko v roce 2007** - Domácí ruská menšina se rozhodla dát formou občanských nepokojů najevo svůj nesouhlas s odstraněním sovětského monumentu bronzového vojáka. Během občanských nepokojů došlo k masivním kyber-útokům na webové stránky estonských ministerstev, premiéra, politických stran, estonských bank, společností a médií.
- **užívání hybridní taktiky během konfliktu vedeného Ruskem na Ukrajině od roku 2014** - např. útok na ukrajinský sčítací volební elektronický systém, útok na ukrajinské dopravní sítě aj.
- **malware Stuxnet**, který poškodil íránský jaderný program kolem roku 2010

Kromě ohrožení bezpečnosti mohou kybernetické útoky sledovat i kriminální cíle a stávají se postupně výnosným byznysem – celosvětově jsou ztráty kvůli kyberkriminalitě odhadové na 500 miliard dolarů, do roku 2019 by to mohlo být již 2,1 bilionu dolarů. Nejslabším místem je přitom nedostatečně silné heslo.

Bezpečnost a obrana kyberprostoru

Trend digitalizace či robotizace život v mnohém usnadňuje, zároveň však přináší nová rizika i hrozby. Závislost společnosti na digitálních informačních systémech se stále zvětšuje a kybernetické útoky se zároveň stávají běžnějšími, sofistikovanějšími a závažnějšími. Přitom narušení komunikace či zneužití dat může ovlivnit procesy rozhodování a následně ohrozit například život nebo majetek obyvatel či dokonce států. Ochrana informačních systémů před zneužitím, ať už softwarovým či hardwarovým, nebo odcizením informací v těchto systémech uložených, je proto klíčem k zajištění bezpečnosti v kyberprostoru. **Zajištěním bezpečnosti a obrany v kyberprostoru, tedy ochranou informací, systémů a infrastruktury, se proto stále intenzivněji zabývají jak odborné instituce, tak na nejvyšší úrovni i vlády a Severoatlantická aliance.**

Factbox natoaktual.cz je vydáván Informačním centrem o NATO v Praze jako přehled informací a zdrojů k vybraným tématům.
Není oficiálním vyjádřením NATO ani žádné jiné české nebo zahraniční vládní instituce.
V případě dotazů se neváhejte obrátit na IC NATO na adrese info@natoaktual.cz.

Centrum NATO v Estonsku

Estonsko se v roce 2007 stalo terčem kybernetických útoků, které měly fatální dopad na fungování celého státu, stopy útoku navíc vedou do sousedního Ruska. Poprvé se tak naplno ukázaly potenciální slabost institucí i společnosti členské země NATO po narušení informačních a komunikačních kanálů kybernetickými útoky. I proto se právě Estonsko dnes profiluje jako alianční lídr v oblasti kybernetické bezpečnosti, mj. otevřením **Centra excelence NATO pro kybernetickou obranu** v Tallinnu v roce 2008. Toto centrum má na starosti výzkumné, vzdělávací či konzultační aktivity v rámci celé Severoatlantické aliance.

Náklady na kyberbezpečnost rostou

Citlivost tématiky a roztříštěnost institucí věnujících se kyberbezpečnosti nedovolují přesně vyčíslit, kolik peněz státy či firmy na kybernetickou bezpečnost vydají. Relativně otevřené jsou USA - prezident Barack Obama v návrhu rozpočtu na rok 2017 alokoval více než 19 miliard dolarů na kybernetickou bezpečnost, což je o 35 % více než v roce 2016.

Česká stopa

Česká republika se ke kybernetické bezpečnosti vážněji postavila v roce 2011, kdy vláda ustanovila Národní bezpečností úřad státní autoritou pro oblast kybernetické bezpečnosti, což vedlo ke vzniku **Národního centra kybernetické bezpečnosti** (NCKB), které nyní koordinuje spolupráci na národní a mezinárodní úrovni. Pod NCKB funguje také vládní CERT (Computer Emergency Response Team) zaměřující se na ochranu kritické informační infrastruktury, významných informačních systémů a orgánů veřejné správy.

Kromě toho zde na národní úrovni působí také CSiRT.CZ (Computer Security Incident Response Team) starající se o řešení bezpečnostních incidentů v počítačových sítích provozovaných v ČR a dále složky v rámci ministerstva vnitra (např. policie řešící kybernetickou kriminalitu) a ministerstva obrany (kyberobrana, vojenské zpravodajství).

ČR: 200 incidentů měsíčně

Národní centrum kybernetické bezpečnosti (se 30 zaměstnanci) řeší v ČR zhruba 200 incidentů za měsíc - za rok 2015 to bylo téměř dva a půl tisíce incidentů (z toho jen 600 ohlášených).

Bibliografie a zdroje k tématu:

» Národní centrum kybernetické bezpečnosti (https://www.govcert.cz/cs/)

» Cyber Defence – NATO Library (http://www.natolibguides.info/cybersecurity/articles/archives)

» Boháček, Petr (2016): Kybernetická válka je další formou rusko-ukrajinského konfliktu. *natoaktual.cz*, 18.4.2016 (http://www.natoaktual.cz/kyberneticka-valka-je-dalsi-formou-rusko-ukrajinskeho-konfliktu-phv-/na_analyzy.aspx?c=A160418_151213_na_analyzy_m02)

» Doležel, Martin (2011): NATO svazuje kyberprostor. *natoaktual.cz*, 12.12.2011. (http://www.natoaktual.cz/nato-svazuje-kyber-prostor-druha-cast-dxs-/na_analyzy.aspx?c=A111212_091109_na_analyzy_m02)

» Fertasi, Nadja El – De Vivo, Diana (2016): Cyber resilience: protecting NATO's nervous system. *NATO Review*. (http://www.nato.int/docu/review/2016/Also-in-2016/nato-cyber-resilience-security/EN/index.htm)

» Jirovský, Václav (2007): *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

» Národní bezpečnostní úřad (2016): Národní strategie kybernetické bezpečnosti na období let 2015 až 2020. (https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf)

» Národní centrála proti organizovanému zločinu [2016]: Kyberkriminalita. (http://www.policie.cz/clanek/kyberkriminalita.aspx)

» natoaktual.cz (2016): Kyberútok na jednoho může být útokem na všechny, varují spojenci. *natoaktual.cz*, 15.6.2016 (http://www.natoaktual.cz/kyberutok-muze-spustit-realci-cele-aliance-fk2-/na_zpravy.aspx?c=A160627_105109_na_zpravy_m00)

» Pavelová, Alexandra (2016): Přehled: Národní strategie kybernetické bezpečnosti České republiky 2015-2020. *Security Outlines*, 20.11.2016. (http://www.securityoutlines.cz/narodni-strategie-kyberneticke-bezpecnosti-ceske-republiky-na-obdobi-let-2015-2020/)

» Schmitt, Michael N. (2013): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. (https://ccdcoe.org/research.html)

» Světnička, Lubomír (2016): Tady se pálí ostrými! Hackeři na cvičení vykolejili vlak s jaderným odpadem. *natoaktual.cz*, 25.10.2016. (http://www.natoaktual.cz/cviceni-cyber-czech-proti-hackerum-dtg-/na_zpravy.aspx?c=A161027_125335_na_zpravy_m00)

» Veenendaal, Matthijs - Kaska, Kadri - Brangetto, Pascal (2016): *Is NATO ready to cross the rubicon on cyber defence?* Cyber Policy Brief. Tallin: NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf)

Pokud budete mít zájem o další informace k tomuto tématu, neváhejte se obrátit na:
Informační centrum o NATO
Jungmannova 17, 110 00 Praha 1
info@natoaktual.cz
tel.: 221-506-758