26. 4. 2024

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Kyberkriminalita a její vliv na obchodní společnosti

Informační technologie se za poslední desetiletí staly nedílnou součástí společnosti, a to tak, že si bez nich nedokážeme život už ani představit. Toto období otevírá dveře k nesčetným možnostem a v mnohých ohledech nám usnadňuje každodenní fungování. Zároveň s sebou přináší i nové hrozby, které s technologickým pokrokem přicházejí.

Změnil se způsob, jakým komunikujeme, jak pracujeme, jak trávíme volný čas, ale také se pozměnil obrázek současné trestné činnosti. S rozvojem technologií se tak rozšířila i paleta způsobů, jakými se dá páchat trestná činnost, a vyvstaly i nové cíle, na které se pachatelé zaměřují. Vedle „tradičních" trestných činů se tak stále častěji setkáváme s trestnými činy spojenými s kyberprostorem. Například za rok 2022 vzrostl oproti roku 2021 počet trestných činů spáchaných v kybernetickém prostoru téměř o 95 %, což představuje zhruba 10 % celkové registrované kriminality.[1] Přičemž v těchto statistikách jsou zahrnutí i podnikatelé a obchodní společnosti, kteří se také stávají terčem kyberútoků. To může mít dopad nejen na poškození reputace a nemalé finanční ztráty, ale může to vést i k narušení provozu společnosti a poškození práv třetí strany. Na tuto problematiku se blíže podíváme v tomto článku.

Co je to kyberkriminalita?

Kybernetická kriminalita je pojem odvozený od pojmu kybernetický prostor, což je dle § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti: *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*". Možno ještě doplnit, že právě ona výměna informací a propojení těchto systémů je to, co tento prostor také tvoří a nejen to, k čemu slouží. Kybernetická kriminalita se tedy jako pojem vycházející z kybernetického prostoru vymyká standardnímu rozdělení trestné činnosti a kategorizaci trestných činů. Není vázaná na konkrétní území, předměty a ani objekty útoku. Není tedy možné ji striktně brát za samostatné právní odvětví, naopak v ní můžeme spatřovat určité rysy podobné jiným trestněprávním odvětvím.

Pokud bychom hledali ryzí definici kybernetické kriminality, najdeme ji jen stěží. Otázkou je, zdali je vůbec možné kybernetickou kriminalitu nějak definovat. Tento pojem se neustále vyvíjí a reaguje na dynamické změny v kybernetickém prostoru. Pokud bychom se ji pokusili nějakým způsobem závazně definovat, v době dopsání by již mohla být tato definice zastaralá. To by mohlo způsobit potíže jak pro orgány činné v trestním řízení, tak pro společnost jako takovou, která se jako terč této kriminality musí snažit držet s pachateli krok v oblasti prevence a ochrany.

S oficiální definicí či nějak vymezeným obsahem kybernetické kriminality nepracuje ani naše legislativa. Lze ji tedy pozitivně popsat jako *„trestná jednání, jejichž společným jmenovatelem je, že v nich vystupuje počítač jako nositel hardwarového a softwarového vybavení a dat, a to buď jako předmět útoku nebo nástroj pachatele."*[2]

Pojmy jako počítačová, informační či internetová kriminalita se mohou jevit jako synonyma právě ke kybernetické kriminalitě, ale ve skutečnosti skrývají důležité nuance. Jedná se kupříkladu o odlišné

nástroje a objekty útoků, ale i o odlišný způsob prevence či odhalování.

Hrozby pro podnikatele

V posledních letech se počet kybernetických útoků dramaticky zvýšil a firmy všech velikostí a oborů čelí riziku krádeží dat či nejrůznějším hackerským útokům. Pachatelé mohou svým počínáním ochromit jejich chod do takové míry, že kolabují systémy, dílčí funkce vykazují chyby, a tím tak dokáží celou společnost vyřadit z provozu. To s sebou nese několik specifických hrozeb v závislosti na tom, čím se daná společnost zabývá a jaké má zaměření. Pachatelé mohou znemožnit fungování platební brány, nabourat se do databází či vypnout systémy, jejichž úkolem je uchování nějakého materiálu v příslušné kvalitě (např. chladící zařízení či zařízení zaručující udržení určitého hygienického standardu). Škody se tedy mohou pohybovat jak v řádech „zanedbatelných částek", tak i v řádech milionů či miliard.

V českém právním řádu nenajdeme s ohledem na problematické vymezení pojmu kybernetické kriminality zvláštní skutkovou podstatu, pod kterou by všechny trestné činy spojené s kyberprostorem spadaly. Máme sice trestný čin **neoprávněného přístupu k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací** dle § 230 trestního zákoníku (dále jako „**TrZ**"), trestný čin **opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat** podle § 231 TrZ či trestný čin **neoprávněného zásahu do počítačového systému nebo nosiče informací z nedbalosti** v § 232 TrZ, ale jiné kybernetické trestné činy podřazujeme pod skutkové podstaty, jejichž znaky kyberprostor zásadně neobsahují. Lze hovořit například o **sabotáži** (§ 314 TrZ), **poškození cizí věci** (§ 228 TrZ), **podvodu** (§ 209 TrZ), **vydírání** (§ 175 TrZ) nebo o **neoprávněném nakládání s osobními údaji** (§ 180 TrZ) a o **poškození cizích práv** (§ 181 TrZ). Nyní se detailněji podíváme na některé konkrétní formy kybernetické kriminality, které se mohou týkat obchodních společností.

Šíření malwaru

Malware je zkratka pro malicious neboli škodlivý software, který je navržen tak, aby způsoboval škody v počítačích a počítačových sítích. Mezi jeho nejčastější podoby patří viry, červi, trojské koně, spyware či ransomware. Malware se ve všech svých podobách může šířit nejrůznějšími způsoby, mezi které patří například e-mail, umístění infikovaného odkazu na web nebo sociální sítě, navštívení samotné infikované stránky, infikované disky vložené do počítače či „prosté" sociální inženýrství.

Nakažení počítače malwarem se může projevovat jeho zpomalením, samovolným vypínáním či restartem, ztrátou dat či vyskakováním doposud neznámých dialogových oken.

Z hlediska zaměření tohoto článku je nejproblematičtější vlastností malwaru právě jeho dostupnost. Tím, že stačí prosté kliknutí na na první pohled bezpečně vyhlížející odkaz, mohou omylem firemní počítač a systém snadno nakazit i samotní zaměstnanci, kterým přijde například podvodný e-mail.

DDoS útoky

DDoS útoky neboli Dsitributed Denial of Service jsou jedním z druhů kybernetické kriminality, který si klade za cíl zahltit server nebo síť takovým množstvím provozu, že se stane nedostupným pro svoje uživatele. Útočníci skrze síť infikovaných počítačů odesílají velké množství falešných požadavků na cílový server, a tím ho ochromují. Rozlišujeme několik typů DDoS útoků, a to volumetrické, které se zaměřují právě na zahlcení serveru velkým množstvím dat, protokolové, které zneužívají slabin v síťových protokolech k zahlcení serveru a aplikační útoky, které cílí na specifické aplikace běžící na serveru.

Příklad DDoS útoku lze uvést třeba v souvislosti se zveřejněním nějakého nového produktu na e-shopu. Jako podnikatel máte toto zveřejnění naplánované a v moment, kdy se tak stane, se na váš web nahrne velké množství zákazníků. Ačkoli může docházet ke zpoždění odezvy serveru z důvodu velkého náporu zájemců o tento nový produkt, tak jste na to připraveni a server tzv. „nespadne“. Najednou ale začne server dostávat enormní množství falešných požadavků. Ty zahltí server a znemožní mu zpracovávat reálné objednávky od vašich reálných zákazníků. To vede k nedostupnosti e-shopu, následné finanční ztrátě, a pokud to dovedeme až do krajních důsledků, pachatelé mohou během DDoS útoku ukrást i citlivá data, na což navazuje další podkapitola.

Únik a zneužití osobních údajů

Únik a zneužití osobních údajů má dopady nejen na obchodní společnost jako možný terč útoku, ale především i na její klienty, zaměstnance či dodavatele nebo jinou třetí stranu. Opět zde záleží na tom, čím se daná společnost zabývá. Určitý typ osobních údajů schraňují kupříkladu stavební společnosti a jiné zase společnosti působící na poli zdravotnictví. Ať už se ale jedná o jakékoli zaměření, je únik a následné zneužití osobních údajů bez pochyby závažným činem, který ovlivňuje i osoby na první pohled nijak nespojené s danou společností.

Únik dat může být příčinou činnosti hackerů, kteří se tzv. nabourají do počítačových systémů společnosti a data odcizí. Dalším způsobem může být již výše zmiňovaný malware či ransomware. Nelze opomenout ani lidský faktor, kdy únik dat může být následkem lidské chyby. Zaměstnanec může omylem odeslat tato data nesprávné osobě, může z nedbalosti ztratit zařízení, na kterém jsou osobní údaje uchovávána, či umožní únik dat nedodržováním bezpečnostních pravidel a opatření, čímž pachatelům značně usnadní práci.

Společnost může takovýto únik stát nejen dobrou pověst, ztrátu klientely či případné spory v občanskoprávní rovině, ale může to být i shledáno jako porušení GDPR. GDPR aneb **nařízení Evropského parlamentu a Rady 2016/679** z roku 2016 **o ochraně osobních údajů** stanovuje pravidla pro ochranu tohoto typu údajů a vztahuje se na všechny firmy, které osobní údaje fyzických osob zpracovávají v Evropském hospodářském prostoru. Úřad pro ochranu osobních údajů může společnosti uložit pokutu až ve výši 20.000.000 EUR nebo 4 % celosvětového ročního obratu. Zároveň je nutné dodržet předepsaný postup nahlášení úniku dat, informovat subjekty, jejichž data byla odcizena, a provést nápravná opatření.

Právnická osoba jako pachatel kyberkriminality

Právnická osoba nemusí být pouze terčem kybernetického útoku, ale i pachatelem, jak vyplývá z negativního výčtu v § 7 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim (dále jako „**TOPO**“).

Zároveň ale není možné, aby trestný čin spáchala právě právnická osoba, jelikož s ohledem na absenci schopnosti právně jednat za ni (resp. v jejím zájmu či v rámci její činnosti) vždy musí jednat fyzická osoba. V § 8 odst. 1 TOPO jsou jako tyto fyzické osoby uvedeny statutární orgán nebo jeho člen, osoba vykonávající vedoucí či řídící činnost nebo kupříkladu zaměstnanec při plnění pracovních úkolů.

K této problematice, tedy k přičitatelnosti jednání fyzických osob, se tuzemský právní řád vyjadřuje v § 8 odst. 2 TOPO. **Právnické osoby mohou páchat v zásadě vše výše uvedené, ať už se jedná o neoprávněné nakládání s osobními údaji, neoprávněný přístup k počítačovému systému či šíření počítačového viru.**

Ochrana společnosti před kyberkriminalitou

S prostředkem ochrany přichází v současnosti Evropská unie v podobě bezpečnostní směrnice NIS 2.

Tu má do českého právního řádu transponovat **novela zákona o kybernetické bezpečnosti**. Tato směrnice, která vstoupila v platnost na začátku roku 2023 a navazuje na již existující směrnici NIS, je zaměřená na kybernetickou bezpečnost proti hackerským útokům uvnitř organizací a mimo jiné si klade za cíl zvýšení jejich odolnosti. **Tato směrnice přichází oproti své předchozí verzi s přísnějšími požadavky na organizace. Jedná se o pravidelné posuzování rizik, implementaci bezpečnostních opatření nebo o ohlašovací povinnost. NIS 2 zároveň dopadá na větší počet organizací. Může se týkat nejen společností v kritické infrastruktuře, jako je energetika, doprava nebo zdravotnictví, ale například i poskytovatelů poštovních služeb, výrobců a dodavatelů klíčových produktů a služeb či se může týkat společností podnikající v oblasti odpadového hospodářství.**

Nejlepší obranou proti kybernetické kriminalitě je tedy **dostatečná ochrana a prevence. Každá společnost by tak měla dbát na správnou implementaci technických a organizačních opatření. To v sobě zahrnuje zejména**:

- **antivirové softwary**, adekvátní šifrování dat a pravidelnou aktualizaci softwaru společnosti, aby se zbytečně nevystavila hrozbám z důvodu své zranitelnosti,
- **školení zaměstnanců** o kybernetické bezpečnosti, o hrozbách, které práce s technologiemi přináší a také o správném nakládání s citlivými daty. Zaměstnanci by tak měli být schopni v základech rozeznat podvodný e-mail či webovou stránku, měli by být poučeni o tvorbě silných hesel a jejich správě, která spočívá například v jejich pravidelné změně a v neposlední řadě je důležité klást důraz na bezpečný pohyb na internetu na firemních zařízeních.
- **pravidelné zálohování dat**, aby data mohla být případně obnovena,
- neustálý zájem o trendy v trestné činnosti v kyberprostoru, aby tomu mohla přizpůsobovat svá opatření,
- „**krizový plán**“ s přesně stanoveným postupem jak jednat a jak reagovat v případě, že by se společnost stala terčem kybernetické kriminality.

Závěr

Kybernetická kriminalita představuje stále větší hrozbu. Vývoj technologií neustále rozšiřuje škálu možného nebezpečí, a to vyžaduje stálé vyhodnocování možných rizik a zvažování propracovanějších prostředků ochrany. Následky kybernetického útoku mohou pro právnické osoby spočívat nejen v ztrátě dobré reputace, ale především ve finančních ztrátách a možných sankcích kupříkladu ze strany Úřadu pro ochranu osobních údajů. Vzhledem k těmto okolnostem je téma kyberkriminality pro obchodní korporace klíčové. Právo obchodních korporací tak musí reflektovat tuto hrozbu a poskytovat firmám nástroje pro prevenci a řešení kybernetických útoků. Na závěr si tedy dovolujeme apelovat na pravidelné reflektování současných rizik jak v interních firemních dokumentech, tak v prováděných školeních a v nastavení dostatečných bezpečnostních opatření.[3]

Mgr. Lucie Špičková,
advokátka

Eva Hrdličková,
právní praktikantka

Advokátní kancelář Vych & Partners, s.r.o.

Lazarská 11/6
120 00 Praha 2

Tel.: +420 222 517 466
Fax: +420 222 517 478
e-mail: office@ak-vych.cz

---

[1] Zpráva o činnosti státního zastupitelství za rok 2022 [online]. Nejvyšší státní zastupitelství. 22. 6. 2023. [cit. 26. 2. 2024]. K dispozici >>> zde.

[2] Kuchta, J. Aktuální problémy počítačové kriminality včetně její prevence. Časopis pro právní vědu a praxi. 2016, roč. 24, č. 1, s. 6.

[3] Při psaní tohoto článku bylo mimo jiné vycházeno ze Studentské vědecké a odborné činnosti autorky Evy Hrdličkové na téma „Kyberkriminalita z trestněprávního pohledu“, 2024.

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí

- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory