Publikace je mimořádně povedeným dílem a velice přehledně zpracovává vybraná témata z oblasti kybernetické bezpečnosti. Její autoři jsou respektovaní odborníci nejen na domácí, ale také mezinárodní scéně a jejich široký záběr a zkušenost jsou znát zejména v praktických částech a doporučeních u jednotlivých kapitol.

Záběr publikace je ovšem mnohem širší, než jak by mohl napovídat její název, o čemž svědčí i téměř 230 stran kvalitně napsaného textu k řadě témat souvisejících s problematikou kybernetických incidentů. Dokonce je možné tvrdit, že žádná jiná publikace na českém trhu nepředstavuje v takové granularitě a komplexitě odpovědi na tolik otázek, které si právníci i technici musí na denní bázi klást v rámci prevence i řešení kybernetických incidentů. Spektrum čtenářů, jimž je tato publikace primárně určena tvoří manažeři kybernetické a informační bezpečnosti, pověřenci pro ochranu osobních údajů, architekti či auditoři kybernetické bezpečnosti, případně advokáti asistující regulovaným subjektům v oblasti informační compliance, ale ostatně všichni, kteří se zajímají o správné nastavení organizačních, technických a procesních pravidel.

Dokonce by se dalo bez nadsázky konstatovat, že pojednání k různým tématům zde v přehledné formě najdou také členové statutárních orgánů, kteří se mají v řadě oblastí, informační bezpečnost nevyjímaje, rozhodovat informovaně a s péčí řádného hospodáře. Zejména ti pak díky publikaci lépe pochopí, jak vnímat kybernetický incident z hlediska struktury compliance či řízení a mohou zpracovat kvalitní podkladovou dokumentaci pro účely tzv. defence file.

Z obsahové struktury je možné vyzdvihnout přehledně, uceleně a v rozumné míře detailu zpracované pojmosloví, ve kterém se mnohdy při tvorbě interní řídící dokumentace, jakkoliv by se to mohlo zdát nepravděpodobné, v praxi nezřídka chybuje. Nelze než ocenit propojení s problematikou ochrany a zpracování osobních údajů nejen v kontextu GDPR. Tolik skloňované standardy a normy pro řízení kybernetických incidentů jsou pak obsahem druhé části publikace, na kterou logicky navazuje stať popisující mj. analýzu rizik, opatření ke snížení rizika či kontroly a hodnocení compliance systému.

Díky skvěle formovanému autorskému kolektivu pak není divu, že na své si při čtení přijdou i právníci, jimž je představena velká množina témat vztahujících se k regulaci, povinnostem relevantním pro kybernetický incident, jakož i oznámení kybernetických incidentů či přehledně sumarizované požadavky na řízení dodavatelů (tzv. vendor management, jež doznal značného vývoje i v samotných vyhláškách o kybernetické bezpečnosti).

Nespornou přidanou hodnotou publikace je její čtvrtá kapitola, jež poskytuje klíč k pochopení praktických aspektů řízení kybernetických incidentů – podpora vedení organizace, pojištění kybernetické bezpečnosti, outsourcing, a tak dále. Výhodou je, že text není jen obecnou ochutnávkou diskutovaných témat, ale pravidelně nabízí plnohodnotné zamyšlení v souvislostech, které i experti působící dlouhodobě v prostředí kybernetické bezpečnosti bezesporu ocení. V neposlední řadě je potřeba také kladně hodnotit fakt, že publikace vyniká mimořádnou a špičkově promyšlenou skladbou, kdy je čtenáři umožněno s publikací pracovat interaktivně. Vysvětlující diagramy, navigační tabulky či přehledové grafiky jsou pak jen pomyslnou třešničkou na již tak řemeslně perfektně zpracované publikaci.

Nelze jinak než shodnout se s autory, kteří uvádí, že cílem publikace je nabídnout komplexní pohled na různé souvislosti spojené s kybernetickými incidenty a představit tolik potřebnou kuchařku, jak takovým incidentům předcházet, a tudíž eliminovat či zásadně minimalizovat možné negativní dopady. Tuto knihu vřele doporučuji těm, kteří s tématy kybernetické bezpečností teprve začínají, ale také všem, kteří se s jednotlivými nástrahami kyberprostoru vypořádávají na denní bázi v rámci jejich pracovních povinností.

Autor recenze: JUDr. Tomáš Ščerba, Ph.D., advokát, Local Partner White&Case, s.r.o., advokátní kancelář