Interní audit v digitálním světě aneb vazby interního auditu a IT bezpečnosti

Daniel Bican

Dan je zakládajícím partnerem společnosti DABRICON s.r.o., která se specializuje na poradenství v oblastech řízení rizik, compliance, kyberbezpečnosti a specializovaných datových analýz lokálním i mezinárodním klientům. Také se svým expertním týmem provádí forenzní a speciální šetření a pomáhá znesvářeným stranám řešit obchodní spory. Před založením DABRICONu byl 20 let konzultantem, manažerem, a nakonec partnerem oddělení forenzních služeb a řešení sporů globálních poradenských firem Andersen, Deloitte a EY ve střední a východní Evropě a se svými týmy pracoval na mezinárodních i lokálních projektech v mnoha zemích Evropy. Je absolventem VŠE a držitelem certifikací auditora a specialisty auditu, interního auditu, vyšetřování podvodů, proti praní špinavých peněz a projektového řízení.

Lubomír Pitter

Luboš je zkušený konzultant s více než 10 lety praxe. Pomáhá firmám řešit technologické výzvy a problémy. Zkušenosti sbíral prací pro širokou škálu klientů od malých rodinných firem až po nadnárodní společnosti. V rámci své kariéry pracoval jako datový analytik, byznys analytik, projektový manažer, a v neposlední řadě i jako produktový manažer v mezinárodních poradenských firmách a dalších nadnárodních společnostech. Manažerské dovednosti získával vedením menších týmů složených jak z technických, tak i netechnických specialistů. Vyjma technických oblastí se velmi dobře orientuje v oblasti procesů a jejich zdokonalování. Jeho zásadní přidanou hodnotou je schopnost propojování byznys světa a technologií.

V éře zintenzivňujícího se technologického pokroku, elektronizace a digitalizace se interní audit stává stále důležitějším prvkem v každé organizaci. Jeho role přesahuje tradiční hranice ověřování existence a nastavení kontrolních mechanismů interních procesů a rozšiřuje se také do komplexního hodnocení a ověřování kvality IT prostředí a kybernetické bezpečnosti. V tomto dynamickém prostředí, kde nové technologie přinášejí jak velké příležitosti, tak významné výzvy, se interní auditoři musí vybavit potřebnými nástroji a dovednostmi, případně spolehlivými partnery tak, aby mohli efektivně chránit citlivá data a systémy svých organizací.

Narůstající závislostí společností na digitálních technologiích se rozšiřuje i spektrum rizik – od sofistikovaných kybernetických útoků po interní bezpečnostní incidenty. Interní auditoři se tak musí po boku zástupců IT a kyberbezpečnosti stát strážci digitální kvality organizace. Jejich rozhodnutí pak mají zásadní význam pro ochranu a budoucí udržitelnost existence organizací. Tento přístup vyžaduje nejen hluboké porozumění technologickému prostředí, ale také schopnost rychle reagovat na neustále se měnící rizika či hrozby.

Digitální transformace přináší internímu auditu nové výzvy v podobě analýz velkých objemů dat, nutnosti pochopení komplexních IT systémů i aplikace umělé inteligence. Zároveň ale otevírá dveře k využití pokročilých technologických řešení, jako jsou automatizované auditní nástroje a cloudové platformy, které zvyšují efektivitu auditních procesů. Agilní přístup k auditu, který umožňuje rychlejší adaptaci na změny v prostředí

a efektivní řízení rizik, se stává nejen žádoucím, ale často i nezbytným.

„Digitální transformace přináší internímu auditu nové výzvy v podobě analýz velkých objemů dat, nutnosti pochopení komplexních IT systémů i aplikace umělé inteligence.“

Důležitost zapojení interního auditu do ověřování IT prostředí a kyberbezpečnosti organizace je ještě více podpořena aktuálními trendy ve vývoji standardů interního auditu. Právě probíhající aktualizace mezinárodního rámce IPPF (International Professional Practices Framework) zavádí tzv. *Topical Requirements*, které mají v rámci několika oblastí zvýšit konzistenci a kvalitu služeb interního auditu. Tyto požadavky odrážejí rostoucí význam a komplexitu IT a kybernetické bezpečnosti v prostředí moderních organizací. Zároveň posilují potřebu prohloubení znalostí a dovedností interních auditorů v oblasti kybernetické bezpečnosti a technologií. V tomto článku se proto zaměříme na to, jak interní audit může čelit těmto výzvám a jak může využít digitální transformaci k posílení své role a přispět k vytvoření bezpečnějšího a udržitelnějšího prostředí organizace. Představíme zde klíčové strategie, postupy a nástroje, které mohou auditoři používat k posílení procesů a kontrol IT a kybernetické bezpečnosti a jak mohou vytvářet synergie s IT oddělením, aby společně čelili digitálním výzvám budoucnosti.

Digitalizace a interní audit

Digitalizace představuje revoluční změnu ve způsobu, jakým organizace fungují. Přechod od tradičních procesů k digitalizovaným umožňuje zpracovávat a analyzovat velké množství dat rychleji a přesněji než kdykoliv předtím. Integrace pokročilých technologií, jako jsou umělá inteligence (AI) a strojové učení umožňují organizacím fungovat rychleji a efektivněji, avšak přináší i celou řadu nových výzev a rizik. Zařazení kybernetické bezpečnosti, jako jedné z hlavních oblastí zájmu interního auditu je tak nevyhnutelné.

Interní audit by měl v dnešní době využívat veškerá dostupná data v organizaci a zpracovávat je co nejefektivněji pomocí datových analýz. Využití **datové analytiky** a **big data technologií** umožňuje auditorům rozpoznat vzorce, trendy a anomálie, které by mohly naznačovat potenciální rizika nebo problémy. Zmíněné analýzy mohou také zahrnovat **prediktivní modelování** a analýzu chování, které pomáhají předvídat a minimalizovat rizika, a to nejen v oblasti kybernetické bezpečnosti. Při vytváření analýz by měla být vždy brána v potaz míra **automatizace**, s jejíž pomocí bude v budoucnu analýza dat efektivnější.

Výstupy datových analýz je dobré vizualizovat v rámci interaktivních **dashboardů**. Tyto nástroje umožňují auditorům hlubší vhled do složitých datových struktur a mohou zlepšit rozhodování a prezentaci zjištění auditu. Dashboardy je také možné napojit na živá (real-time) data, což podporuje tvorbu průběžných/kontinuálních kontrolních systémů. S ohledem na kybernetickou bezpečnost mohou být zmíněné techniky používány s využitím monitorovacích systémů typu SIEM (Security Information and Event Management), zejména při analýzách logů, výstupů systémů zabraňujících únikům dat (DLP – Data Loss Prevention) a dalších nástrojů generujících velké množství záznamů. Porozumění těmto datům a rychlá orientace napříč rozsáhlými datovými výstupy jsou nezbytnou součástí správného přístupu k provádění interního auditu nejen IT prostředí a kyberbezpečnosti v organizaci.

„Aplikace agilních metod se ukázala jako efektivní nejen ve softwarovém vývoji, ale i v tradičním podnikání.

Digitalizace přináší s sebou nejen nové druhy rizik a výzev, ale zároveň může podstatně zvýšit efektivitu procesů interního auditu. Tohoto zlepšení je dosaženo prostřednictvím nástrojů, které umožňují interním auditorům správně porozumět a detailně, rychle a kvalifikovaně analyzovat data. Tato schopnost je nezbytná pro identifikaci a řízení rizik ve světě, který se neustále vyvíjí a je technologiemi stále více ovlivněn.

Agilní audit

Rozmach digitalizace a s ním se zvyšující komplexita jednotlivých oblastí interního auditu nutí auditní týmy k opouštění tradičního modelu ročního plánování k pružnější a dynamické strategii, která umožňuje rychlou adaptaci na měnící se potřeby a rizika. Agilní přístup zahrnuje pravidelné, či dokonce ad hoc revize auditních plánů a prioritizaci úkolů na základě aktuálních rizik a výzev. Potřeba pružně reagovat je obzvláště markantní v IT bezpečnosti, kde jsou organizace, jejich data a sítě neustále vystavovány novým hrozbám od útočníků, kteří jsou většinou o krok napřed. Přestože by kybernetická bezpečnost měla být jedním ze základních stavebních kamenů organizace, většina společností nemá specializovaného auditora pro kybernetickou bezpečnost. Je tomu tak zejména kvůli dlouholetému a přetrvávajícímu nedostatku takových bezpečnostních expertů na pracovním trhu. Interní audit se tak stává klíčovým nezávislým orgánem, který je nucen tuto roli suplovat.

Využití agilních metod umožňuje interním auditorům efektivně reagovat na nově vznikající hrozby a zároveň podporuje lepší komunikaci mezi nimi

a ostatními odděleními. To vede k rychlejšímu šíření důležitých informací a zkušeností napříč organizací, a napomáhá tak zefektivnění chodu společnosti.

Příkladem může být společnost, která zavedla agilní audit v reakci na výrazný růst a neustále se zvyšující počet kybernetických útoků. V této společnosti interní audit tradičně připravoval roční plán auditů pro různá oddělení a procesy. S využitím metod agilního řízení se však přístup změnil:

1. **Flexibilní plánování:** Místo pevného ročního plánu začal auditní tým vytvářet seznam auditních úkolů, jejichž priority pravidelně ověřoval se zúčastněnými stranami (stakeholdery), a aktualizovat posloupnost jejich provádění.
2. **Pravidelné prioritizace:** Auditní tým začal pravidelně hodnotit a aktualizovat úkoly v závislosti na měnícím se podnikatelském prostředí, aktuálních potřebách organizace a nově identifikovaných kybernetických hrozbách.
3. **Přeshraniční spolupráce:** Zvýšila se spolupráce s jinými odděleními, jelikož se jejich zástupci stali účastníky pravidelných schůzek (ceremonií), což umožnilo lépe porozumět provozním rizikům a integrovat poznatky a potřeby do priorit jednotlivých úkolů.

Přestože zavedení agilního auditu představuje určité výzvy, jako je potřeba kontinuálního vzdělávání, rozvoje dovedností, a v neposlední řadě změny osobního přístupu a mentálního nastavení, přináší klientům výrazné výhody ve formě zvýšené reaktivity, efektivity a schopnosti řešit aktuální výzvy.

Outsourcing a partnerství v interním auditu

Organizace a jejich interní audit je v posledních letech vzhledem ke zmíněnému nedostatku bezpečnostních expertů na pracovním trhu a nedostatečným interním kapacitám či náročnosti technologického prostředí často motivován k využívání outsourcingu některých aspektů interního auditu, zejména v oblasti IT a kybernetické bezpečnosti.

„Budoucnost však směřuje spíše k trendu využívání generativní umělé inteligence, což umožní interním auditorům rychlejší zpracování výstupů a auditních zpráv, nebo pokládání dotazů v určitém kontextu napříč datovými strukturami organizace.“

Outsourcing umožňuje získat rychle přístup k nedostatkovým zdrojům a specializovaným dovednostem, které interní tým nemusí mít. Externí experti mají v kontextu kybernetické bezpečnosti přehled o aktuálních trendech, hrozbách, a v neposlední řadě i regulatorních požadavcích. Integrace externích dodavatelů do auditního procesu vyžaduje pečlivý výběr partnerů a jasně definované rámce spolupráce pro zajištění kvality a kontinuity auditu. Navázání spolupráce se silným a důvěryhodným partnerem umožní organizacím efektivněji využít interní týmy, které mohou pracovat za paralelní podpory dodavatele. Pro tento typ spolupráce je výhodné využít zmíněných agilních metod, kdy jsou externí partneři začleněni do interního agilního týmu, aby co nejrychleji získali potřebné informace a porozuměli chodu organizace. Interní týmy mohou od dodavatele získat velmi cenné know-how. Rozsah spolupráce se může v čase postupně snižovat a odpovědnosti mohou být postupně předávány interním zaměstnancům. Experti z partnerské společnosti pak mohou být využíváni na základě rámcové smlouvy pouze v ad hoc případech za účelem konzultace či revize výstupů interního auditu. Outsourcing se tak stává klíčovou strategií pro posílení kapacit interního auditu a zajištění vyššího zabezpečení organizace v rychle se měnícím a technologicky náročném prostředí.

Shrnutí

V tomto článku jsme se ponořili do klíčových aspektů, které formují současný a budoucí směr interního auditu, a to nejen v oblasti kybernetické bezpečnosti. Digitalizace přináší nové výzvy, ale zároveň otevírá dveře k novým příležitostem pro interní audit, nabízí podrobnější analýzu dat a poskytuje hlubší vhled do technologických hrozeb. Aplikace agilních metod se ukazuje jako efektivní nejen v softwarovém vývoji, ale i v tradičním podnikání. Implementace agilního přístupu v interním auditu umožňuje efektivně reagovat na dynamické prostředí a rostoucí kybernetické hrozby, přináší zvýšenou reaktivitu a efektivitu. Outsourcing se jeví být velmi vhodným prvkem pro posílení schopnosti organizací efektivně čelit technologickým výzvám vzhledem k nedostatku odborníků v IT bezpečnosti.

Do budoucna můžeme očekávat další a hlubší integraci pokročilých technologií, jako je umělá inteligence a strojové učení, do auditních procesů. Je důležité zmínit, že mnoho organizací již nástroje založené na nějaké formě umělé inteligence mnoho let využívá. Budoucnost však směřuje spíše k trendu využívání generativní umělé inteligence, což umožní interním auditorům rychlejší zpracování výstupů a auditních zpráv nebo pokládání dotazů v určitém kontextu napříč datovými strukturami organizace. Tato integrace přinese nové výzvy i příležitosti, včetně potřeby rozvoje dovedností a adaptace na rychle se měnící bezpečnostní hrozby. Interní audit a kybernetická bezpečnost tak musí pokračovat ve spolupráci a hledání nových cest pro zajištění bezpečnosti dat a infrastruktury organizací v neustále se vyvíjejícím digitálním světě. ■