Audit kybernetické bezpečnosti aneb výchozí stav pro splnění požadavků NIS2

25.4.2024 - | PROTEXT

V dnešní digitální době jsou data jedním z nejcennějších aktiv podniků.

Organizace zaznamenávají své transakce do databází, ukládají dokumenty do síťových úložišť a při své činnosti se do značné míry spoléhají na technologie. S rostoucí závislostí podniků na těchto informačních technologiích a digitálních datech, v kontextu nutného úsilí o jejich ochranu včetně splnění nových zákonných povinností vyplývajících z bezpečnostní směrnice NIS2, nabývá jak u komerčních subjektů, tak organizací státní správy na důležitosti i tzv. audit kybernetické bezpečnosti.

Prevence je lepší než léčba

Kyberbezpečnostní audit je proces, v rámci kterého se hodnotí a analyzují bezpečnostní opatření, politiky a postupy organizace v oblasti informačních technologií a kybernetické bezpečnosti. Pravidelné audity tohoto typu jsou pro organizace nezbytné pro zajištění účinnosti jejich bezpečnostních opatření a pomáhají jim zejména dvěma způsoby:

Zaprvé umožňují posoudit, proaktivně identifikovat a následně řešit případná bezpečnostní rizika nebo nedostatky v bezpečnostních opatření, které mohou vyžadovat zlepšení či dodatečnou ochranu. Při testování zranitelností a hodnocení rizik lze identifikovat potenciální vstupní body pro kybernetické útoky, slabá místa v zabezpečení sítí a oblasti, kde mohou být ohrožena citlivá data, přičemž výsledky auditu umožňují organizacím vypracovat plán ochrany dat a zavést další bezpečnostní opatření a kontroly ke zmírnění zjištěných rizik.

Zadruhé představuje bezpečnostní audit pro společnost jakousi pojistku či ověření, že dodržuje právní předpisy a průmyslové normy týkající se ochrany dat, což zároveň zvyšuje její kredibilitu, neboť jí pomáhá prokázat její závazek k ochraně dat a dodržování předpisů zúčastněným stranám, jako jsou zákazníci, partneři a regulační orgány.

Mimo výše uvedené hrají audity kybernetické bezpečnosti zásadní roli i při vyvozování odpovědnosti jednotlivců za případné porušení zásad kybernetické bezpečnosti. To je důležité zejména s ohledem na chápání důležitosti ochrany dat a dodržování bezpečnostních politik ze strany zaměstnanců. Postupy pro zajištění kybernetické bezpečnosti organizací by měly být také pravidelně aktualizovány v souladu se změnami procesů řízení rizik a změnami v obchodních požadavcích, aktuálním vývoji v oblasti hrozeb a rozvoji technologického prostředí.

Nenahraditelný pomocník při auditu

I přesto, že bezpečnostní audit hraje klíčovou roli v ochraně citlivých podnikových dat, může být pro řadu organizací náročným, zdlouhavým a demotivujícím úkolem, kterému se vyhýbají. Nástroje v podobě klasických tabulkových a textových editorů, které často slouží jako nástroj k provedení auditu, mohou svojí omezenou funkčností audit komplikovat. Zejména při sběru, třídění a analýze dat vyžaduje užití těchto editorů zdlouhavou manuální práci, navíc s vysokou pravděpodobností lidské chyby, což vede nejen k frustraci, ale i zpomalování celého procesu auditu. Tento zastaralý způsob provádění bezpečnostního auditu bez automatizace ale může vést k ještě horšímu scénáři, a to neschopnosti organizace efektivně reagovat na změny v prostředí kybernetických hrozeb, díky

čemuž se dostane na mušku kyberzločincům. Řešením těchto problémů je moderní nástroj CSA vyvinutý specialisty v oblasti kybernetické bezpečnosti, který zmíněné nedostatky editorů nejen řeší, ale navíc nabízí i další přidanou hodnotu.

Cyber Security Audit 2.0

CSA od předního českého tvůrce a dodavatele informačních systémů společnosti Gordic je speciální aplikace pro analýzu bezpečnostních rizik a řízení procesních náležitostí kybernetické bezpečnosti z jednoho místa. CSA je nenahraditelným průvodcem pro organizace hledající jednoduché řešení požadavků vyplývajících ze Zákona o kybernetické bezpečnosti, normy ISO 27 000, směrnice NIS2 i nařízení DORA, přičemž v rámci komplexního přístupu poskytuje odpovědi na nároky české legislativy i mezinárodních standardů, umožňuje efektivní řízení aktiv, hodnocení rizik a implementaci opatření ke zvýšení bezpečnosti.

Aplikace CSA získala certifikát v souladu se Zákonem o kybernetické bezpečnosti (ZoKB) od renomované auditorské společnosti TAYLLORCOX, a je jediným nástrojem na analýzu rizik a řízení kybernetické bezpečnosti na českém trhu, který tento certifikát obdržel.

CSA v praxi

CSA usnadňuje řízení kybernetické bezpečnosti organizace v souladu se současnou českou i mezinárodní legislativou, přičemž obsahuje i specifické materiály a aktualizovaná doporučení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Poskytuje skutečný přehled o stavu kybernetické bezpečnosti organizace v reálném čase a umožňuje provádět analýzy v oblasti kybernetické bezpečnosti s nevídanou rychlostí, precizností a pohodlím, kterého lze jen těžko dosáhnout pomocí tradičních tabulkových a textových editorů.

Data jsou v rámci aplikace CSA dostupná nepřetržitě, je možné je kdykoliv upravit nebo stáhnout, a aplikace s využitím těchto dat nabízí široké spektrum možností, jakými lze podpořit bezpečnostní strukturu organizace. Pomáhá vytvářet, evidovat a hodnotit jak digitální, tak fyzická aktiva podniku a díky komplexnímu katalogu hrozeb a zranitelností umožňuje identifikovat potenciální rizika a využít mapy těchto aktiv k jejich detailnímu zobrazení. Hodnocení rizik je prováděno systematicky a efektivně, aby bylo možné včas přijímat kvalifikovaná rozhodnutí a adekvátně reagovat.

Aplikace CSA poskytuje i přehled o již proběhlých bezpečnostních událostech a incidentech, což usnadňuje rychlou a cílenou reakci. Jednou z jejích hlavních předností je funkce dlouhodobého sledování stavu kybernetické bezpečnosti v organizaci včetně jeho změn, díky čemuž lze snadno dohledat změny, které v systému kybernetické bezpečnosti proběhly, a jejich celkový dopad na chod podniku.

Na základě analýz nástroj generuje návrhy opatření a plánů pro zvládání rizik, aby organizace byla připravena na všechny možné bezpečnostní scénáře. Aby byla zachována transparentnost a soulad s předpisy, poskytuje i prohlášení o aplikovatelnosti a plány pro zachování kontinuity provozu. Výstupní analýzy a monitoring pak slouží nejen manažerům kybernetické bezpečnosti, vedoucím ICT, analytikům a auditorům jako podklady pro zlepšení úrovně kybernetické bezpečnosti organizace, ale také jako zdroj informací pro příslušné dozorové orgány. Více informací o nové generaci nástroje CSA 2.0 najdete na stránkách gordiccybersec.cz/csa/.

O tvůrci CSA

Společnost Gordic je předním českým tvůrcem a dodavatelem informačních systémů a nástrojů pro srozumitelnou komunikaci lidí a organizací. Jeho portfolio produktů a služeb zahrnuje informační

systémy určené pro veřejnou správu, včetně uznávané platformy GINIS, kterou využívá více než 6 000 organizací české veřejné správy; otevřené modulární informační systémy pro soukromý sektor, včetně DMS, řešení fyzické i kybernetické bezpečnosti a integrační platformy pro ovládání IoT technologií a efektivní sběr dat. Gordic je také iniciátorem a provozovatelem platformy KYBEZ, která je založena na dobrovolné spolupráci akademických, státních i komerčních a mediálních institucí z oblasti IT a telekomunikací a jejímž cílem je osvěta v oblasti kybernetické bezpečnosti a obrany.

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/audit-kyberneticke-bezpecnosti-aneb-vychozi-stav-pro-splneni-pozadavku-nis2/2510658