Služby v oblasti řízení rizik

Analýza a řízení rizik informační bezpečnosti

Vědět co musím chránit a proč

Co je analýza rizik informační bezpečnosti

Analýza rizik je základem pro efektivní řízení informační bezpečnosti v každé společnosti Kombinuje technické znalosti IT a bezpečnostních specialistů o stavu vašeho IT prostředí s pohledem business části vaší společnosti na její jednotlivé procesy a služby.

Spojením těchto dvou částí získá vaše společnost unikátní znalost toho, co je pro její chod důležité (business priority) a musí být tedy chráněno, a kde je nejzranitelnější, čili co jsou největší bezpečnostní rizika. Vaše informační bezpečnost tak dostane jasný signál, na co se zaměřit a kde bude mít její snaha největší přidanou hodnotu.

Co nabízíme

Postup založený na mezinárodně uznávaném standardu ISO 27005, který je zároveň v **souladu se zákonem o kybernetické bezpečnosti** a analýzou rizik dle ISO 27001

Komplexní podporu ve všech aktivitách od tvorby metodiky, přes analýzu samotnou až po nastavení procesu řízení rizik, ale **i samostatně v každé z těchto částí**

Pomoc při vyjednávání IT bezpečnosti **s TOP managementem** o nápravných opatřeních, ale **i při tvorbě komplexní strategie**, jak bezpečnost dále rozvíjet

Další **pomoc při eliminaci či zmírňování dopadů specifických rizik** informační bezpečnosti

Jednoduchý, prověřený nástroj pro vyhodnocování a řízení rizik, včetně **srozumitelného reportingu** pro různé druhy příjemců (TOP management, IT management, bezpečnost…)

Co získáte?

CISO - Co získáte:

- Komplexní zobrazení problémů i jejich příčin
- Odůvodnění pro nutné investice do bezpečnosti
- Oporu pro komunikaci s vrcholovým vedením
- Jednotný komunikační jazyk pro oblast řízení rizik

CIO - Co budete vědět:

- Která data jsou ve Vaší firmě nejcennější
- Jaká aktiva potřebujete k hladkému chodu firmy
- Co jsou největší rizika ve Vašem IT prostředím
- Na jaké problémy se máte prioritně zaměřit

CFO - Co získáte

- Znalost finančních dopadů rizik spojených s informační bezpečností
- Business case pro rozhodnutí, do kterých opatření investovat a do kterých nikoliv
- Znalost závislosti business procesů na informačních technologiích

pwc

www.pwc.cz/ras

Proč PwC?

Poskytujeme našim klientům praktické zkušenosti s řízením rizik informační bezpečnosti. Věříme, že proces řízení rizik je základním stavebním kamenem informační bezpečnosti, avšak v žádném případě to nemusí být proces složitý. Jednoduchost, praktičnost a efektivita jsou klíčové vlastnosti našich služeb.

Naše postupy i nástroje jsou zhotoveny na základě mezinárodně uznávaných standardů v informační bezpečnosti a jsou zároveň v souladu se zákonem o kybernetické bezpečnosti.

Kontakt

Tomáš Kuča
Partner
+420 251 152 054
tomas.kuca@pwc.com

Ondřej Linhart
GRC Expert
+420 732 633 893
ondrej.linhart@pwc.com

Naše nabídka služeb

Využíváme své zkušenosti, abychom dosáhli efektivního a úspěšného začlenění procesu řízení rizik informační bezpečnosti do vaší organizace a jejích cílů. Máme rozsáhlé zkušenosti s poskytováním asistence našim klientům ve všech oblastech řízení rizik:

Určení rozsahu analýzy

- Na základě společné dohody určíme, jaká část společnosti je součástí rozsahu analýzy rizik a jaká již do analýzy spadat nebude. Zohledníme také prostředí, ve kterém se společnost nachází, tzv. organizační kontext
- Společně s vámi identifikujeme budoucí uživatele výstupů z analýzy a zjistíme jejich očekávání a požadavky
- Stanovíme celkový plán a časový harmonogram analýzy, včetně aktivit, kde budeme potřebovat informace od vás nebo vašich kolegů

Metodika

- Stanovíme nejvhodnější a nejefektivnější metody a postupy pro provedení analýzy rizik ve vašem prostředí, výslednou metodiku vám pomůžeme formalizovat a zavést do běžného provozu
- Společně určíme důležité parametry pro analýzu rizik jako jsou škály pro hodnocení aktiv, zranitelností a hrozeb, nebo kritéria pro akceptaci rizik (tzv. risk apetit)
- Naše metodika je založena na mezinárodně uznávaném standardu pro analýzu rizik informační bezpečnosti ISO 27005:2018, je v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti

Identifikace a hodnocení aktiv

- Identifikujeme informační aktiva, na kterých je postaven chod vaší společnosti, a podpůrná aktiva, která zpracovávají nebo uchovávají zmíněná informační aktiva
- Pro informační i podpůrná aktiva určíme adekvátní úroveň granularity (pomocí agregace či slučování) tak, aby provedení analýzy bylo co nejefektivnější
- Určíme závislosti mezi informačními a podpůrnými aktivy a odpovědné vlastníky za každé identifikované aktivum
- S vlastníky informačních aktiv provedeme hodnocení důležitosti jejich aktiv pro chod vaší společnosti

Identifikace, hodnocení a zvládání rizik

- S vlastníky informačních aktiv identifikujeme nejpravděpodobnější hrozby, které aktiva ohrožují
- Se správci / vlastníky podpůrných aktiv identifikujeme jejich zranitelnosti
- Analyzujeme získané informace a určíme relevantní rizika pro vaši společnost, ohodnotíme je a pomůžeme vám nastavit efektivní opatření pro jejich ošetření.
- Dle vašich preferencí jsme schopni využít kvalitativních i kvantitativních metod (např. metoda ALE – Annual Loss Expectancy)
- Pomůžeme vám nastavit/zavést proces pro řízení rizik, vč. efektivního reportingu, podpoříme vás při prezentaci výstupů analýzy rizik ať už vašim kolegům z IT nebo nejvyššímu vedení

Cíle a vize

Naším cílem je poskytnout vám dostatečný detail na to, aby jste viděli, kde jsou problémy, které je třeba řešit, ale zároveň dostatečnou formu agregace, aby jste se neztratili ve stovkách identifikovaných rizik, bez jakéhokoliv propojení či priorit.

Vaši specialisté budou přesně vědět, co a jak chránit, a Váš management bude znát odpověď na otázku, proč je to důležité.

www.pwc.cz/ras