NA CO SI DÁT POZOR PŘI IMPLEMENTACI POŽADAVKŮ VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

16.-17. května 2022, Hradec Králové
TLP: GREEN

Hana Kroupová
Odbor kontroly

Organizační část

Nejčastější problémy v organizační části I.

- Bezpečnostní dokumentace
  - Nereflektuje požadavky konkrétní organizace
  - Nedodržování interně stanovených postupů
  - Není platná, řízená, úplná, aktuální

- Systém řízení bezpečnosti informací
  - Žádný či nevhodně stanovený rozsah systému řízení bezpečnosti informací
  - Neprobíhá pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací

- Řízení aktiv a rizik
  - Nevhodná identifikace a evidence primárních a podpůrných aktiv a nezohlednění vazeb mezi nimi
  - Neexistující nebo neaktuální hodnocení rizik
  - Hodnocení rizik je mnohdy vytvořeno pouze za účelem shody se ZKB

Nejčastější problémy v organizační části II.

- Prohlášení o aplikovatelnosti, plán zvládání rizik
  - Neexistence
  - Nepochopení účelu dokumentů
  - Nereflektují výsledky provedeného hodnocení rizik
  - Dokumenty nejsou aktuální

- (Ne)Řízení dodavatelů
  - Nedostatečná kvalita uzavíraných smluv – kdo je za co zodpovědný
  - Neprobíhá kontrola dodržování stanovených pravidel, směrnic a politik

- Nedostatečná podpora vedení organizace v oblasti kybernetické bezpečnosti

- Organizační bezpečnost
  - Nedostatečné personální obsazení v oblasti kybernetické bezpečnosti
  - Nevhodné organizační zařazení kybernetické bezpečnosti v organizaci

Nejčastější problémy v organizační části III.

- Nízké bezpečnostní povědomí o kybernetické bezpečnosti napříč organizací
  - Neprobíhají školení

- Řízení kontinuity činností
  - Nejsou definovány důležité procesy, činnosti organizace a cíle kontinuity činností pro případ neočekávané události
  - Neexistence strategie kontinuity činností a havarijních plánů
  - „Testujeme až naostro“
  - Do testů nejsou zapojeny všechny významné zainteresované strany - vedení s dostatečnou rozhodovací pravomocí, dodavatel, atp.)

Technická část

Nejčastější problémy v technické části I.

- Segmentace a řízení komunikace
  - Nevhodně rozdělené segmenty (např. podporované i nepodporované typy systémů ve stejném segmentu)
  - Není blokována nežádoucí komunikace (blacklisting, firewall apod.)
  - Neprobíhá pravidelná kontrola prostupů

- Identity a autentizace
  - Nevhodně nastavená délka a komplexita hesel nebo nastavení politiky hesel v rozporu se schválenou politikou organizace
  - Používání sdílených účtů
  - Přidělování privilegovaných účtů osobám, které je nepotřebují

- Vyhodnocení kybernetických bezpečnostních incidentů
  - Nákup technologie z důvodu požadavku ve VKB bez zajištění odborných personálních kapacit
  - Neprobíhá zaznamenávání událostí u všech důležitých aktiv
  - Chybí zaznamenávání některých informací o událostech (např. časové pásmo)

Nejčastější problémy v technické části II.

- Dostupnost
  - Není zajištěna redundance aktiv nezbytných pro zajištění dostupnosti
  - Nejsou k dispozici náhradní zdroje napájení (UPS, dieselagregáty)
  - Není prováděno testování náhradních zdrojů napájení
  - Nepravidelné zálohování, nevhodné uchovávání záloh
  - Není prováděna kontrola použitelnosti provedených záloh

Děkuji za pozornost

h.kroupova@nukib.cz