Defense in Depth

- Strategie "Defense in Depth" (Obrana ve hloubce) je koncept v oblasti kybernetické bezpečnosti, který se zaměřuje na vrstvenou ochranu IT infrastruktury prostřednictvím použití různých bezpečnostních mechanismů na více úrovních a místech, aby se zvýšila celková úroveň bezpečnosti. Tato strategie se zakládá na přesvědčení, že jedna jediná bezpečnostní vrstva nebo opatření nemusí být dostatečná pro ochranu systémů a dat před hrozbami, a proto je nutné použít více různých opatření na různých úrovních, aby se zvýšila odolnost proti různým typům útoků.

Běžné součásti firemní bezpečnostní politiky zahrnují:

- Politiku silných hesel: Stanovení požadavků na silná hesla pro všechny uživatele a pravidelnou změnu hesel, aby se minimalizovalo riziko neoprávněného přístupu.
- Politiku přístupových práv: Omezení přístupu uživatelů pouze na nezbytně nutné systémy, aplikace a data na základě jejich pracovních rolí a odpovědností.
- Politiku zálohování a obnovy: Stanovení pravidel pro pravidelné zálohování důležitých dat a systémů, jejichž obnova by měla být testována a dokumentována.
- Politiku aktualizace a správy zranitelností: Definování postupů pro pravidelnou aktualizaci software, aplikací a systémů a správu zranitelností, včetně monitorování a opravování známých zranitelností.
- Politiku šifrování: Stanovení požadavků na šifrování dat a komunikace, zejména u citlivých informací přenášených přes veřejné sítě.
- Politiku správy zařízení: Definování pravidel pro správu zařízení připojených k síti organizace, včetně mobilních zařízení, s cílem minimalizovat riziko ztráty nebo odcizení dat.
- Politiku monitorování a detekce hrozeb: Definování postupů pro sledování a analýzu síťového provozu, logů a indikátorů hrozeb za účelem rychlé detekce a odpovědi na bezpečnostní incidenty.

- Politiku školení a povědomí uživatelů: Stanovení požadavků na pravidelné školení uživatelů o kybernetických hrozbách, bezpečnostních postupech a politikách organizace, s cílem zvýšit povědomí o bezpečnosti a minimalizovat riziko chyb způsobených lidským faktorem.

Příklady opatření podle doporučení NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) zahrnují:

- Dvojí ověření (2FA/MFA): Používání dvojího ověření při přístupu k důležitým systémům a službám, což zvyšuje úroveň ochrany před neoprávněným přístupem.
- Aktualizace a správa zranitelností: Pravidelné aktualizace software, aplikací a systémů a správa zranitelností za účelem minimalizace rizika úspěšného využití známých zranitelností.
- Zálohování a obnova: Pravidelné zálohování důležitých dat a systémů a provádění testů obnovy, aby byla zajištěna možnost obnovy dat a služeb v případě havárie nebo ztráty dat.
- Monitorování a detekce hrozeb: Sledování a analýza síťového provozu, logů a dalších indikátorů hrozeb za účelem detekce potenciálních bezpečnostních incidentů a hrozeb.
- Omezení privilegovaného přístupu: Omezení přístupu s vysokými privilegii pouze na nezbytně nutných místech a pro nezbytné osoby, aby se minimalizovalo riziko zneužití privilegovaných účtů.
- Antivirová ochrana: Používání aktualizované antivirové ochrany na všech systémech a zařízeních, která jsou připojena k síti, s pravidelnými aktualizacemi a skenováními.
- Firewall: Konfigurace a správa firewallů pro ochranu sítě a systémů před neoprávněným přístupem zvenčí a vnitřního pohybu dat.
- Šifrování: Používání šifrování dat a komunikace, zejména při přenosu citlivých informací přes veřejné sítě.
- Školení a povědomí uživatelů: Pravidelné školení uživatelů o kybernetických hrozbách, bezpečnostních postupech a politikách organizace, aby se zvýšilo povědomí o bezpečnosti a snížilo riziko chyb způsobených lidským faktorem.

Tato opatření slouží k ochraně IT infrastruktury a dat organizace před různými typy kybernetických hrozeb a jsou důležitou součástí komplexního přístupu k zajišťování informační bezpečnosti v organizaci. Tyto opatření by měly být implementovány jako součást firemní bezpečnostní politiky, která stanovuje zásady, postupy a pravidla pro zabezpečení informačních aktiv organizace.