#ANECT DOPORUČUJE 5 KROKŮ:

URGENTNÍ PREVENTIVNÍ OPATŘENÍ PRO KYBERNETICKOU OCHRANU

Kybernetické útoky zneužívají aktuální mimořádné situace a zásadně ohrožují chod společností, které jsou už nyní ve složité situaci.

Proveďte preventivně následující základní opatření pro svou kybernetickou ochranu (případně je znovu překontrolujte)!

1. **Správně a důsledně zálohujte!**

- Zkontrolujte, zda dochází k bezchybnému zálohování kritických systémů
- Otestujte obnovu ze záloh
- Oddělte zálohovací server se zálohami od zbytku infrastruktury
- Omezte a striktně kontrolujte problematické protokoly (především Samba protokol)
- Prověřte a omezte oprávnění pro zálohovací servisní účet, proaktivně změňte jeho heslo
- V případě aktivního Ransomware útoku – okamžitě odpojte zálohovací server od sítě

Co získáte? Jistotu, že zálohy jdou obnovit. Zálohování budete mít pod kontrolou a práva k zálohám bude mít pouze konkrétní servisní účet se silným heslem. Budete mít plán okamžité reakce při napadení Ransomwarem.

---

2. **Nalezněte a uzavřete rizikové porty a služby vystavené do veřejného internetu**

- Co nejdříve **oskenujte** své veřejné IP rozsahy/služby **a vyhodnoťte zranitelnosti** veřejně vystavených služeb ●
- V žádném případě veřejně nevystavujte služby typu vzdálená plocha (RDP), TeamViewer, databázový server atd.

Co získáte? Jednoduše uzavřete dveře nejčastějším banálním útokům zvenku, stanete se odolnější proti útokům na dostupnost vašich služeb a snížíte pravděpodobnost úniku dat.

---

3. **Chraňte účty a hesla uživatelů a správců!**

- Co nejdříve **zkontrolujte a vyhodnoťte** obsah výchozích skupin AD (Active Directory) – zejména **privilegované skupiny** typu Domain & Enterprise Administrators ● ●
- Nastavte nová a silná hesla u privilegovaných účtů (nezapomeňte na servisní účty!)
- Striktně oddělte používání uživatelských a administrátorských účtů
- Zakažte využívání administrátorských účtů k běžným operacím na koncových stanicích
- Zakažte ukládání hesel uživatelských účtů na koncových stanicích
- Vyžadujte silná hesla i u uživatelů
- Nastavte více-faktorovou autentizaci

Co získáte? Jistotu, že účty s vysokými oprávněními mají nové a silné heslo a že jsou použity jen tam, kde je to skutečně potřeba. Jistotu, že účtem běžného uživatele neovlivníte infrastrukturu. Snížíte také pravděpodobnost zneužití identity běžného uživatele či dokonce správce.

---

4. **Zabezpečte internetový provoz a emailovou komunikaci**

- Zkontrolujte nastavení filtrace webového provozu a zcela zakažte nebezpečné kategorie, jako jsou např. Phishing, Botnet, Malware, Hacking atd.
- Jednoduše přesměrujte zejména emailovou komunikaci přes cloudové technologie zamezující útokům nultého dne (Zero Day Attack)
- Zcela zakažte přímý přístup k internetu ze serverů, které jej nepotřebují (ideálně žádný vnitřní server!)
- Zaktualizujte ihned antivirové a antispamové filtry
- Zapněte kontrolu šifrovaného provozu (SSL)

Co získáte? Snížíte riziko zavlečení škodlivého kódu prostřednictvím běžného uživatele. Zabráníte přímé komunikaci serverů do internetu.

---

5. **Aktualizujte operační systémy a aplikace, aplikujte bezpečnostní záplaty**

- Co nejdříve **oskenujte** své vnitřní síťové prostředí a **vyhodnoťte zranitelnosti** na zařízeních, síťových prvcích a službách ● ● ●
- Připravte a otestujte plán pro nouzovou aplikaci kritických bezpečnostních záplat
- Izolujte nebo vyřaďte nepodporovaný HW a SW

Co získáte? Zásadně snížíte riziko zneužití bezpečnostních děr a šíření nákazy ve vnitřní síti, vedoucí nejčastěji k zašifrování stanic, serverů, databází a záloh.

● SOCA SCAN EXTERNÍ ZRANITELNOSTI. PORTY A PROTOKOLY

●● SOCA SCAN ÚČTY ADMINISTRÁTORSKÉ ÚČTY A HESLA

●●● SOCA SCAN INTERNÍ ZRANITELNOSTI. PORTY A PROTOKOLY

Nevíte si rady nebo nemáte odborné a finanční zdroje? Rádi pomůžeme #ANECT soca@anect.com