Szakdolgozati témák IT-biztonsági aspektusainak megvitatása a ChatGPT-vel/Copilot-tal ezen robot-vélemények kritikai értelmezése céljából

(Discussing IT security aspects of thesis topics with ChatGPT/Copilot to critically interpret these robot opinions)

Pitlik László, anonim Hallgatók (MY-X team)

# Bevezetés

A feladat rel. egyszerű: egy feltételezett vizsgakérdést adjunk át elsőként a Chatgpt/Copilot számára, majd a kapott válaszokban keressünk anomáliákat (pl. rendszerszinten: ÉS-használatának tiltása felsorolásokban, kihagyás- és átfedés-mentesség, sorrendiség vs. halmazelemek felsorolása, stb.).

# Esettanulmány

Prompt: Milyen IT biztonsági aspektusai vannak a következő témának? Ajánlatkérési folyamatok automatizálása RFQ alkalmazással: Tervezés, Fejlesztés és Integráció

ChatGPT 3-mini-high

*„Az RFQ alkalmazással történő ajánlatkérési folyamatok automatizálása során az IT biztonsági szempontok széles spektrumát kell figyelembe venni. Ezeket három fő fázisban lehet összefoglalni:*

***1. Tervezés***

* ***Kockázatelemzés (1)***
* ***biztonsági követelmények meghatározása: (2)*** *Azonosítani kell a rendszer potenciális sebezhetőségeit, például adatszivárgás, jogosulatlan hozzáférés vagy manipuláció lehetőségét. Ezen felül a biztonsági célokat (pl. rendelkezésre állás, adatvédelem, integritás) korai szakaszban definiálni kell.*
* ***Adatvédelmi (3)***
* ***megfelelőségi szabályozások: (4)*** *Figyelembe kell venni az érvényes adatvédelmi előírásokat (például GDPR) és iparági szabványokat (pl. PCI-DSS, ha pénzügyi tranzakciókról van szó). Ezek beépítése a rendszertervezésbe kritikus a jogi és üzleti kockázatok minimalizálása érdekében.*
* ***Biztonsági architektúra kialakítása: (5)*** *A rendszer tervezése során meg kell határozni, hogyan védjük az adatokat és a kommunikációs csatornákat. Ide tartozik például a hálózati szeparáció (DMZ, tűzfalak) és a rendszer rétegelt biztonsági megoldásainak (defence in depth) kialakítása.*
* ***Hozzáférés-szabályozás tervezése: (6)*** *Már a tervezési fázisban definiálni kell a felhasználói szerepköröket, jogosultságokat és a hitelesítési mechanizmusokat, például erős jelszópolicy, többfaktoros hitelesítés (MFA) és szerepkör alapú hozzáférés-kezelés (RBAC).*

***2. Fejlesztés***

* ***Biztonságos kódolási gyakorlatok:*** *A fejlesztés során elengedhetetlen a secure coding irányelvek betartása, például az input validáció, kimeneti szűrés, SQL-injekció, XSS vagy CSRF támadások elleni védelem. Ezek segítenek csökkenteni a szoftverben rejlő sebezhetőségeket.*
* ***Titkosítás alkalmazása:*** *Mind az adatok tárolása, mind az átvitel során biztosítani kell a titkosított kommunikációt (például SSL/TLS használata). Ezen kívül az érzékeny adatok tárolását is titkosítani kell.*
* ***Kódellenőrzés és sebezhetőség tesztelés:*** *Rendszeres kód auditok, statikus és dinamikus elemzések, valamint penetrációs tesztek szükségesek a hibák és biztonsági rések feltárásához még a rendszer élesítése előtt.*
* ***Naplózás és eseménykövetés:*** *A fejlesztés során implementálni kell egy részletes audit naplózást, amely lehetővé teszi a rendszerben történt biztonsági események, anomáliák és hibák nyomon követését.*

***3. Integráció***

* ***Biztonságos API és interfész kezelése:*** *Az RFQ alkalmazás gyakran kommunikál külső rendszerekkel. Az integráció során elengedhetetlen a megfelelő API hitelesítés és autorizáció (például OAuth, token alapú megoldások), továbbá a kommunikáció titkosítása.*
* ***Adatcsere és kommunikáció biztonsága:*** *A rendszerek közötti adatcsere során biztosítani kell, hogy az adatok titkosított csatornákon (például VPN, SSL/TLS) keresztül közlekednek, így védve az adatok integritását és bizalmasságát.*
* ***Harmadik fél rendszereinek biztonsági auditja:*** *Ha az RFQ alkalmazás külső szolgáltatásokat vagy partnereket is integrál, ezek biztonsági szintjét auditálni kell, hogy ne legyenek a rendszer gyenge láncszemei.*
* ***Rendszerintegritás és rendelkezésre állás:*** *Biztosítani kell a rendszer redundanciáját, rendszeres biztonsági mentéseket, valamint az incidensek gyors és hatékony kezelését, hogy a szolgáltatás folyamatosan elérhető legyen.*
* ***Folyamatos monitorozás:*** *Az integráció után is fontos a rendszer állapotának és biztonsági eseményeinek folyamatos monitorozása, beleértve a behatolásészlelő rendszerek (IDS/IPS) alkalmazását és a rendszeres log-elemzést.*

***Összefoglalva***

*Az RFQ folyamat automatizálása során a biztonságot a rendszer teljes életciklusában szem előtt kell tartani. A tervezési fázisban meghatározott biztonsági stratégiának, a fejlesztési szakaszban alkalmazott biztonságos kódolási eljárásoknak és a biztonságos integrációs megoldásoknak együtt kell működniük annak érdekében, hogy a rendszer ellenálljon a modern IT fenyegetéseknek, és megfeleljen a szabályozási előírásoknak.*

*Ezzel a megközelítéssel biztosítható, hogy az automatizált ajánlatkérési folyamatok nemcsak hatékonyak, de biztonságosak is maradnak a teljes rendszer életciklusa alatt.”*

Prompt: A fázisokon belüli pontok időrendiséget jelöl?

*„Indokolt a következőhöz: 5 másodperc*

*Nem, a fázisokon belüli pontok nem egy szigorú időrendi sorrendet, hanem az adott szakaszban figyelembe veendő kulcsfontosságú biztonsági aspektusokat jelölik. Ezek a pontok inkább a figyelembe veendő területeket és feladatokat mutatják be, amelyek a tervezési, fejlesztési és integrációs fázis során egyaránt fontosak, de nem feltétlenül egymás után kell őket végrehajtani. Más szóval, bár a projekt egész életciklusában vannak olyan lépések, amelyek időben egymást követik, az itt felsorolt pontok célja az átfogó biztonsági szemlélet és a legfontosabb területek kiemelése, nem pedig egy konkrét ütemterv megadása.”*

o3-mini-high

**Prompt:**

Az első fázist írd át időrendi sorrendbe, ha szükséges átírni.

2/2

Reasoned for 12 seconds

„*Az alábbiakban az első fázis (Tervezés) lépéseit időrendi sorrendbe rendezzük, feltételezve, hogy az egyes tevékenységek egymásra épülnek:*

1. ***Kockázatelemzés és biztonsági követelmények meghatározása:*** *A projekt kezdeti szakaszában feltérképezni kell a rendszer sebezhetőségeit és potenciális fenyegetéseit, majd ennek alapján meghatározni az alapvető biztonsági célokat (pl. adatvédelem, integritás, rendelkezésre állás).*
2. ***Adatvédelmi és megfelelőségi szabályozások felmérése:*** *A kockázatelemzés eredményeinek tükrében át kell tekinteni az érvényes jogi és iparági előírásokat (például GDPR, PCI-DSS), hogy a tervezett megoldás megfeleljen a vonatkozó szabályozásoknak.*
3. ***Biztonsági architektúra kialakítása:*** *Az előző lépésekben meghatározott követelmények és szabályozások alapján meg kell tervezni a rendszer biztonsági architektúráját. Ez magában foglalja a hálózati szeparáció (pl. DMZ, tűzfalak) és a rétegelt védelmi megoldások kialakítását, valamint az adatok titkosítását.*
4. ***Hozzáférés-szabályozás tervezése:*** *Végül, az architektúra kialakítását követően definiálni kell a felhasználói szerepköröket, jogosultságokat és hitelesítési mechanizmusokat (pl. erős jelszópolicy, többfaktoros hitelesítés, RBAC), amelyek a rendszer biztonságos működését biztosítják.*

*Ez a sorrend logikusan építi fel a tervezési folyamatot, ahol az alapvető kockázatok és követelmények meghatározása megalapozza a további, részletesebb biztonsági megoldások kialakítását.”*

o3-mini-high

**Prompt:**

Fordított sorrendben ugyanilyen logikus lenne a végrehajtás?

Reasoned for 8 seconds

„*A végrehajtás fordított sorrendje nem lenne logikus, mivel az egyes lépések egymásra épülnek. Például:*

1. ***Hozzáférés-szabályozás tervezése*** *Ez a lépés feltételezi, hogy már meghatároztuk a rendszer általános biztonsági architektúráját és kockázatait. Ha ezt fordított sorrendben végeznénk, nem rendelkeznénk a szükséges alapokkal a felhasználói jogosultságok és hitelesítési mechanizmusok meghatározásához.*
2. ***Biztonsági architektúra kialakítása*** *Az architektúra megtervezése során az előzőleg elvégzett kockázatelemzés és megfelelőségi vizsgálat eredményei alapján dolgozunk. Fordított sorrendben ez sem lenne megalapozott, mivel a kockázatok és jogszabályi követelmények ismerete nélkül nehéz lenne megfelelően kialakítani a rendszer védelmét.*
3. ***Adatvédelmi és megfelelőségi szabályozások felmérése*** *Ez a lépés segít azonosítani azokat a szabályokat és előírásokat, amelyekre a rendszernek épülnie kell. Ha ezt a lépést későbbre halasztanánk, a később kialakított architektúra nem biztos, hogy összhangban lenne a jogi követelményekkel.*
4. ***Kockázatelemzés és biztonsági követelmények meghatározása*** *Ez az alaplépés, amely nélkül nincs értelme megtervezni a továbbiakat, hiszen a rendszer sebezhetőségeinek és fenyegetéseinek azonosítása nélkül nem tudnánk meghatározni a megfelelő biztonsági intézkedéseket.*

*Tehát a visszafelé történő végrehajtás nem biztosítaná a megfelelő alapokat a rendszer védelméhez, mivel az egyes lépések egymásra építése nélkül a teljes biztonsági koncepció nem lenne megalapozott.”*

o3-mini-high

**Prompt:**

Vannak olyan pontok, amelyek párhuzamosan is végezhetők?

Reasoned for 17 seconds

*Igen, bizonyos pontok párhuzamosan is elvégezhetők, de fontos, hogy a párhuzamos munkavégzés során a kritikus információáramlás és a szinkronizáció ne sértse a logikai sorrendet. Például:*

* ***Adatvédelmi és megfelelőségi szabályozások felmérése*** *Ez a feladat párhuzamosan elvégezhető a részleges kockázatelemzéssel, hiszen az előírásokkal kapcsolatos információk begyűjtése függetlenül történhet a rendszer sebezhetőségeinek feltérképezésétől. Fontos azonban, hogy a végleges kockázatelemzés eredménye beépüljön a megfelelőségi követelmények végső meghatározásába.*
* ***Biztonsági architektúra kialakítása*** *Amennyiben az alapvető kockázatok és megfelelőségi elvárások már részben ismertté váltak, az architektúra tervezése egyes elemeiben párhuzamosan is dolgozható, például a hálózati szeparáció és az adatátvitel titkosításának részleteinél. Itt a kockázatelemzés folyamatos visszacsatolása szükséges, hogy az architektúra minden kritikus területre kiterjedjen.*

*Tehát bár a kockázatelemzés alapvető lépés, amire a további feladatok épülnek, az adatvédelmi megfelelőség és bizonyos architektúrális elemek kidolgozása bizonyos mértékben párhuzamosan is végezhető, feltéve, hogy a projekt menedzsment megfelelően koordinálja az egyes tevékenységeket.”*

o3-mini-high

**Prompt:**

Ha egytől négyig számozzuk a pontokat, akkor mutassa két ütköző pontot.

Reasoned for 27 seconds

*„Igen, két pont ütközhet, ha nem megfelelően koordináljuk őket. Például:*

* ***3. Biztonsági architektúra kialakítása*** *Ez a pont határozza meg a rendszer alapvető technikai és hálózati kereteit, ideértve a titkosítási protokollokat, a hálózati szeparációt és a rétegelt védekezést.*
* ***4. Hozzáférés-szabályozás tervezése*** *Ennek a feladatnak az a célja, hogy a felhasználók jogosultságait, hitelesítési mechanizmusait és szerepköröket szabályozzuk.*

***Ütközés forrása:*** *Ha a hozzáférés-szabályozás tervezése párhuzamosan vagy akár előbb történik, mint a biztonsági architektúra kialakítása, előfordulhat, hogy a hozzáférési szabályok nem illeszkednek az architektúra által meghatározott technikai paraméterekhez (például a hálózati szeparáció, titkosítási elvek). Ez inkompatibilitáshoz és biztonsági réseket eredményezhet, mert a hozzáférési megoldásoknak az architektúra adta korlátok és lehetőségek alapján kell kialakulniuk.”*

Prompt: Milyen IT biztonsági aspektusai vannak a következő témának? Ajánlatkérési folyamatok automatizálása RFQ alkalmazással: Tervezés, Fejlesztés és Integráció

Copilot

*Az ajánlatkérési folyamatok automatizálása RFQ (Request for Quotation) alkalmazással számos IT biztonsági kihívást és szempontot vet fel. Íme néhány fontosabb aspektus:*

1. ***Adatvédelem és adatbiztonság****: Az RFQ alkalmazások nagy mennyiségű érzékeny adatot kezelnek, beleértve a szállítók árajánlatait, szerződéseit és egyéb üzleti információkat. Fontos, hogy az adatok titkosítva legyenek mind az átvitel, mind a tárolás során.*
2. ***Hozzáférés-kezelés****: Az alkalmazásnak biztosítania kell, hogy csak az arra jogosult felhasználók férhessenek hozzá az érzékeny adatokhoz. Ez magában foglalja a felhasználói hitelesítést, az engedélyek kezelését és a naplózást.*
3. ***Integritás és hitelesség****: Az adatok integritásának és hitelességének biztosítása érdekében fontos, hogy az alkalmazás támogassa a digitális aláírásokat és az audit nyomokat. Ez segít megelőzni az adatok manipulálását és biztosítja, hogy az adatok megbízhatóak legyenek.*
4. ***Rendszerbiztonság****: Az RFQ alkalmazás fejlesztése és integrációja során figyelmet kell fordítani a rendszerbiztonságra, beleértve a sebezhetőségek felderítését és javítását, a rendszerfrissítések és a biztonsági javítások rendszeres alkalmazását.*
5. ***Kockázatkezelés****: Az IT biztonsági kockázatok azonosítása és kezelése kulcsfontosságú. Ez magában foglalja a kockázatfelmérést, a kockázatkezelési stratégiák kidolgozását és a folyamatos kockázatmonitoringot.*
6. ***Szállítói együttműködés****: Az RFQ folyamatok automatizálása során fontos, hogy a szállítók is betartsák az IT biztonsági előírásokat. Ez magában foglalja a szállítói együttműködési platformok biztonságos használatát és a szállítói auditokat.*

*Ezek az IT biztonsági szempontok segítenek biztosítani, hogy az ajánlatkérési folyamatok automatizálása biztonságosan és hatékonyan valósuljon meg.”*

Prompt: A számok sorrendiséget jelölnek?

*„Igen, a számok sorrendiséget jelölnek a felsorolt IT biztonsági szempontok között. Ezek a számok segítenek rendszerezni és áttekinthetővé tenni az információkat. Szeretné, ha bármelyik pontot részletesebben kifejteném? Vagy esetleg van más kérdése a témával kapcsolatban? „*😊

**Prompt:** Milyen IT biztonsági aspektusok merülnek fel a következő szakdolgozati téma esetén? főcím: Az adminisztratív hatékonyság növelése alcím: A Microsoft Azure SDK alkalmazása az Azure DevOps felületén történő adminisztratív feladatok egyszerűsítésére

**Válasz:** Ez egy izgalmas és releváns szakdolgozati téma! Az IT biztonsági aspektusok, amelyek felmerülhetnek a Microsoft Azure SDK és az Azure DevOps használata során, a következők lehetnek:

1. **Hitelesítés és engedélyezés**: Az Azure DevOps-ban a felhasználók hitelesítése és engedélyezése kritikus fontosságú a biztonság szempontjából. Fontos, hogy csak az arra jogosult felhasználók férjenek hozzá az adminisztratív feladatokhoz.
2. **Adatvédelem és titkosítás**: Az adatok védelme érdekében az Azure SDK és az Azure DevOps titkosítási mechanizmusokat alkalmaz. Az adatok titkosítása mind a tárolás, mind az átvitel során elengedhetetlen.
3. **Biztonsági szabályzatok és megfelelőség**: Az Azure DevOps-ban alkalmazott biztonsági szabályzatok és megfelelőségi követelmények betartása biztosítja, hogy az adminisztratív feladatok végrehajtása során ne sérüljenek a biztonsági előírások.
4. **Hozzáférés-ellenőrzés és naplózás**: Az adminisztratív feladatok végrehajtása során fontos a hozzáférés-ellenőrzés és a tevékenységek naplózása. Ez lehetővé teszi a gyanús tevékenységek azonosítását és a biztonsági incidensek gyors kezelését.
5. **DevSecOps gyakorlatok**: A DevSecOps megközelítés integrálása az Azure DevOps-ba biztosítja, hogy a biztonsági szempontok már a fejlesztési folyamat korai szakaszában figyelembe legyenek véve.

Ezek az aspektusok mind hozzájárulnak ahhoz, hogy az adminisztratív feladatok biztonságosan és hatékonyan legyenek végrehajtva az Azure DevOps felületén. Ha további részletekre van szükséged, szívesen segítek!

**Prompt:** Az első pontban tárgyalt hitelesítés és engedélyezés felcserélhető sorrendileg?

**Válasz:** Igen, a hitelesítés és engedélyezés sorrendje felcserélhető, mivel mindkettő kritikus szerepet játszik az IT biztonságban. Általában a hitelesítés az első lépés, amely során a rendszer ellenőrzi a felhasználó személyazonosságát, és ezután következik az engedélyezés, amely meghatározza, hogy a hitelesített felhasználó milyen erőforrásokhoz és műveletekhez férhet hozzá. De a sorrend felcserélhető, mivel mindkettő ugyanazt a célt szolgálja: a hozzáférés biztonságának biztosítását.

# Konklúziók

Az emberi kritikai gondolatok egyrészét prompt-tá konvertálva kimutatható, ha a ChatGPT/Copilot irracionálissá válik. A ChatGPT és a Copilot válaszainak eltérései egymástól önmagukban s gyanúra adnak okot.