

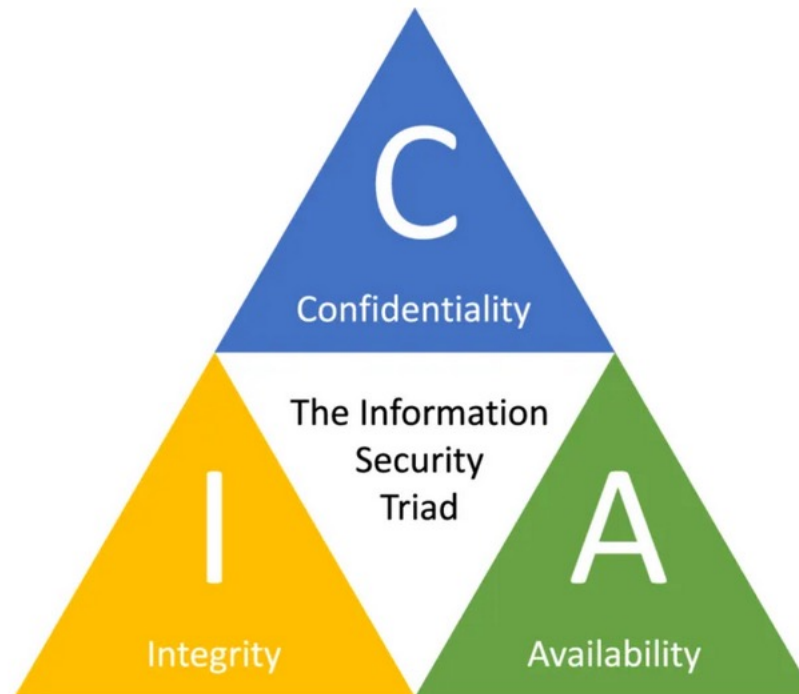


Integrita dat

Kybernetická a informační bezpečnost II

Vladimír Lazecký

vladimir.lazecky@viavis.cz



<https://kobalt.io/blogpost/confidentiality-integrity-and-availability-in-cyber-security/>

- ✓ Prolomení důvěrnosti = neoprávněný přístup k datům (přístup, zcizení...)

- ✓ Překážky pro útočníka – využití pro obranu
 - ✓ Zjistit, kde daná data jsou (architektura systému, distribuce dat)
 - ✓ Získat neoprávněný přístup do systému (autentizace, autorizace)
 - ✓ Logistika dat – jak data dostat ze systému ven (logování, nastavení práv)
 - ✓ Časový tlak (expirace přístupů, bezpečnostní procesy, monitoring)
 - ✓ Stopy – zvláště elektronické stopy (analýza stop, uchovávání, log management)

- ✓ **Techniky útoků - nápady?**

- ✓ **Technické:**
 - ✓ Útoky na autentizaci, neoprávněné přístupy
 - ✓ Odposlechy provozu
 - ✓ Zálohy a datové nosiče
 - ✓ Využití zranitelností

- ✓ Netechnické:
 - ✓ Socio útoky na uživatele
 - ✓ Head Hunter Attacks
 - ✓ Nápady nemají limity

✓ Integrita = shoda dat uložených s daty přečtenými

- ✓ Během přenosu dat nedošlo k jejich změně
- ✓ Transakce nad daty jsou autorizované a korektní

✓ Integrita = kompletnost dat

- ✓ Relační vazby v databázi např. vazba osoba x doklad x bydliště je úplná a jednoznačná

✓ Integrita = využitelnost dat pro dané použití

- ✓ *Zamyslete se nad příklady problematiky integrity?*
- ✓ *Výhody/nevýhody?*
- ✓ *Proč je integrita součástí bezpečnosti informací?*

✓ Mobilním telefonem uděláte fotku...

✓ Uložíte si ji

✓ Jak zajistíte její integritu?

✓ U sebe

✓ Na zálohách

✓ Sdílením na sociálních sítích

✓ Odesláním mailem

✓ Z hlediska bezpečnosti:

✓ *Co je narušením integrity?*

✓ *Jak může být integrita dat narušena?*

✓ *Jak ji detekujete?*

✓ Nezáměrné:

- ✓ Chybou algoritmů
- ✓ Technickým selháním
- ✓ Chybou uživatele

✓ Záměrné:

- ✓ Kyber incidenty
- ✓ Hybridní útoky

✓ **Ověřování shody:**

✓ **Zdrojová data = ověřovaná data**

✓ **Předpoklady:**

✓ **Spolehlivost zdrojových dat (záruka jejich integrity)**

✓ **Zaručený, opakovatelný spolehlivý způsob ověřování**

- ✓ Minulá přednáška
 - ✓ Kontrolní součty
 - ✓ Hashovací funkce
 - ✓ Samodetekční a samoopravné kódy

✓ Základní předpoklad:

✓ Integrita zdrojových dat

✓ *Jak ji zajistíte na cloudu, v mobilním telefonu?*

✓ Ověřování nesmí samo o sobě narušit integritu dat

✓ *Jak tomu rozumíte?*

✓ *Jak byste ověřili integritu sady fotek stažených z disku?*

- ✓ **Zajištění integrity se stává větším problémem než zajištění důvěrnosti a dostupnosti**
 - ✓ **(CIA Triad – Confidentiality, Integrity, Availability)**
- ✓ **Techniky ověřování integrity - předpokládají**
 - ✓ Zdrojová data – etalon ověřování pod kontrolou
 - ✓ Metody a procesy ověřování pod kontrolou
- ✓ **Problém všeho sdíleného – cloud, aplikace, uložení s nekontrolovaným přístupem**

- ✓ Dostupnost = data jsou k dispozici v čase potřeby
- ✓ Dostupnost = zdroje jsou k dispozici v rozsahu a čase potřeby
- ✓ *Co rozumíte „zdroji“?*

✓ DoS – Denial of Service

- ✓ Zařízení je zahlceno požadavky
- ✓ Útok je veden z „jednoho zdroje“
- ✓ Řešení – zablokování zdroje
- ✓ Integrovaná řešení na úrovni infrastruktury

✓ Neúmyslné incidenty:

- ✓ Technická chyba
- ✓ Chyby v SW
- ✓ Uživatelské chyby

- ✓ Připravená infrastruktura, škálovatelnost, detekovatelnost, blokace, zálohování

✓ DDoS – Distributed Denial of Service

- ✓ DoS útok vedený z více zdrojových zařízení
- ✓ Botnet – roBOT NETwork – síť infikovaných zařízení (proto řešit např. i domácí routery)
- ✓ Obrana – sofistiková řešení se zapojením širší infrastruktury (Cloudflare, Radware apod)

✓ Ransomware

- ✓ Blokace dat zdrojů např. šifrováním
- ✓ Odblokování za výkupné
- ✓ Šíření – trojské koně, červi, phishing, využití zranitelností, sociotechniky

✓ **Šifrovací ransomware** – obvykle asymetrická kryptografie

✓ **Nešifrovací ransomware** – admin ovládnutí systému a jeho zamčení

DOWNLOAD DECRYPTION TOOLS

Choose ransomware type

Our free ransomware decryption tools can help decrypt files encrypted by the following forms of ransomware. Just click a name to see the signs of infection and get our free fix.

AES_NI

Alcatraz Locker

Apocalypse

<https://www.avast.com/ransomware-decryption-tools#mac>

✓ Obrana:

- ✓ Zabezpečený perimetr a prostupy – FW, SIEM, antivir
- ✓ Zabezpečená infrastruktura
 - ✓ Segmentace sítě
 - ✓ Bezpečnostní zóny
 - ✓ Prostupy
- ✓ Zálohování
 - ✓ Systémy, data, procesy, princip 3x2x1
 - ✓ 3 nezávislé zálohy ve 2 nezávislých lokalitách, z toho aspoň jedna offline
- ✓ BCP a DRP plány a jejich důsledné otestování
- ✓ Práce s uživateli – práva, školení, testování, motivace

✓ Zotavení po útoku:

- ✓ Neničit stopy – vracíme se k integritě
- ✓ Analýza vektoru útoku, typu a času útoku
- ✓ Záloha zašifrovaných dat (obnova na nové datové nosiče)
- ✓ Šance využití prolomení šifrování (i v budoucnu)

✓ Útoky na dostupnost zdrojů

✓ Lidské zdroje – *jak byste útočili?*

✓ Technické zdroje – nedostupnost náhradní techniky, útoky na logistiku

- ✓ **Jste IT firma, máte unikátní nápad a vyvíjíte SW**
 - ✓ AI, která umí předvídat budoucnost
 - ✓ 5 kamarádů, z toho 2 vlastníci
 - ✓ Máte investora (mne):
 - ✓ 1. Kolik od něj potřebujete na vybudování firmy a rok života
 - ✓ Uvědomte si, co vše budete platit
 - ✓ **Přesvědčte mne**
 - ✓ 2. Peníze dostanete, kolik si řeknete, stanovte jejich rozdělení
 - ✓ Sestavte organizaci a odpovědnost ve firmě, co budete dělat sami, co nakoupíte

✓ Navrhněte řešení bezpečnosti

- ✓ Využijte vše, co víte
- ✓ Jde o váš životní nápad

✓ Zpracujte písemně a v prezentaci

✓ Nechte si je pro sebe ve skupině

- ✓ Objevila se konkurence, tušíte, že může být dál
- ✓ Neštítíte se ničeho – nemáte zábrany
- ✓ Rozhodnete se, že zaútočíte s cílem:
 - ✓ Zjistit jejich know how, vědět, jak jsou daleko, ušetřit na vývoji, předstihnout je
 - ✓ Pokud jsou dále, než vy, zpomalit, zastavit je
- ✓ **Naplánujte a provedte útok**
- ✓ **Udělejte to vzájemně**



Prostor pro vaše dotazy

Prostor pro vaše dotazy...

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký