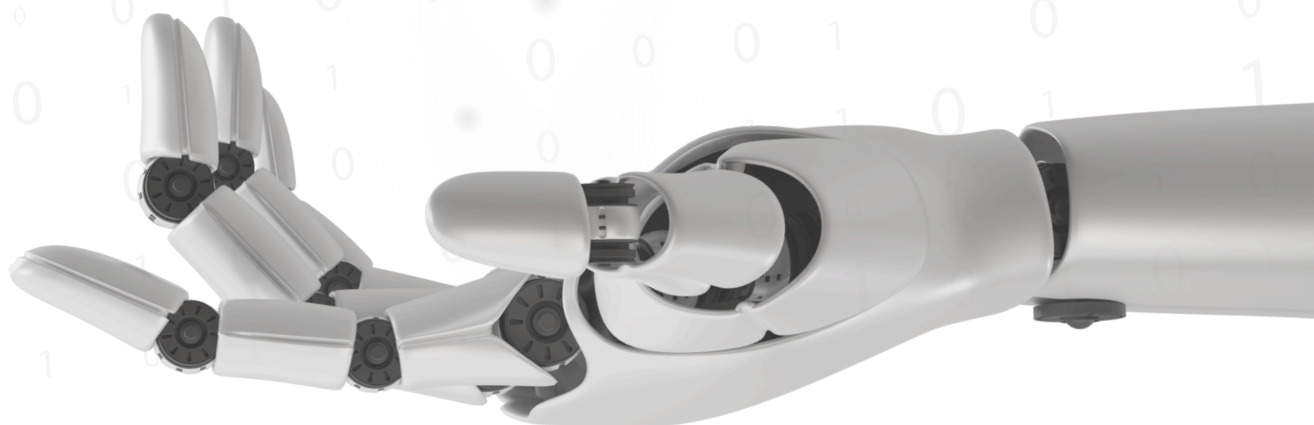


AUTOMATIZUJTE, VYUŽÍVEJTE AI, ALE BEZPEČNĚ!

Výběr správného online nástroje pro podporu podnikání může být pro běžného uživatele nadlidským výkonem. Tato výzva s sebou přináší i bezpečnostní rizika, kterým se lze vyhnout. Připravili jsme pro vás průvodce, který vám pomůže seznámit se s low-code, no-code (LCNC) řešeními a zároveň získat cenné rady, jak zůstat v bezpečí.



NIKOLAS STRAKA

Lowcodin

MARTIN KONEČNÝ

GUARDIANS^{CZ}

Autoři

Nikolas Straka

Mou misí je ukázat malým a středním podnikům možnosti moderních online nástrojů a naučit je vytěžit z nich maximum. V korporátním prostředí jsem vedl tým pracující s low-code/no-code technologiemi, který během dvou let pomohl stovkám kolegů a ušetřil miliony korun.

Vystudoval jsem systémové inženýrství a získával zkušenosti na různých IT pozicích – od testera, přes projektového manažera a produkt ownera, až po solution architekta. Věřím, že právě malé a střední podniky mohou z technologií low-code/no-code nejvíce profitovat, a to i bez velkých týmů a vysokých rozpočtů.



Martin Konečný

Působím jako konzultant a auditor kybernetické a informační bezpečnosti v Guardians.cz. Ačkoliv se zaměřuji zejm. na oblasti managementu informační a kybernetické bezpečnosti, na zákon o kybernetické bezpečnosti a na související ISMS, je mi jasné, že u svých klientů nesmíme podceňovat ani bezpečnost při implementacích low-code/no-code a AI, s čímž se jim snažím pomáhat.

Vystudoval jsem management podnikové infrastruktury a praxi získával postupně v rámci působení na NÚKIB a později v komerčním sektoru v rolích Privacy & Information Security Manager a CyberSecurity Manager, odkud jsem se rozhodl vydat cestou vlastního businessu.



Čtyři úrovně využití

Úroveň 1 - Běžný uživatel

Používáte online nástroje pro své podnikání?

Jednou z prvních úrovní používání online nástrojů pro vaše podnikání jsou tzv. krabicové nástroje. Ty si pořizujete za konkrétním účelem a jsou to nástroje, které vám na začátku vašeho „digitálního“ podnikání pomohou nejvíce.

Co si můžete představit pod pojmem “krabicový systém”?

- Na fakturaci, účetnictví a další účetní funkce, zvolíte např. Fakturoid nebo iDoklad.
- Pro řízení projektů použijete např. nástroje jako Trello nebo Asana.
- Jako CRM si zvolíte např. Raynet nebo Pipedrive.
- Pro ukládání dokumentů používáte např. Google Drive nebo Dropbox.
- Samostatně používáte nástroje umělé inteligence (ChatGPT, Dall-e, Gemini AI,...).
- Dokumenty k podpisu posíláte např. přes DigiSign.
- Mailový marketing řešíte přes Smartemailing.
- Schůzky s klienty plánujete přes Calendly.
- V aplikaci Notion uchovávejte know-how své firmy.
- Atd.

Každý z těchto nástrojů platíte za určitým účelem a každý z nich vám přináší určitou hodnotu. Je důležité mít na paměti, že tím možnosti vaší online produktivity nekončí.

Úroveň 2 - Integrátor

Dokážete propojit své krabicové nástroje?

Věděli jste, že většinu krabicových řešení můžete propojit sami, zvýšit tak jejich použitelnost a ušetřit vašemu týmu spoustu času?

K propojení vašich krabicových řešení používáme integrační platformy, jako jsou Zapier, Make.com, n8n nebo stále populárnější relay.app. Tyto nástroje poskytují uživatelská rozhraní pro práci s API a umožňují tak běžným uživatelům dělat to, co bylo před několika lety možné jen s pomocí programátora.

V praxi to pak může vypadat tak, že místo ručního přepisování dat z jednoho nástroje do druhého se data přepisují sama bez ručního zadávání.

Například když klient vyplní formulář na webu, automaticky se vytvoří záznam v CRM, vytvoří se složka klienta na Google disku a zároveň se vytvoří klient v Asaně. Do procesu můžeme zapojit i nástroje umělé inteligence, a tak již budete mít přehled o tom, co klient dělá v CRM na základě jeho webu.

Kombinací krabicového systému a LCNC integrační platformy jste vytvořili LCNC řešení. Možností, jak takového řešení dosáhnout jsou téměř neomezené. Jenom make.com má víc jak 1300 napojených aplikací a i když vaši aplikaci v seznamu nevidíte, můžete se napojit přes API.

Úroveň 3. - Systémový inženýr

Máte svůj jednotný zdroj pravdy?

Při kombinaci krabicových řešení může dojít k tomu, že platíte 10 nástrojů a přitom každý z nich využíváte jen na 20 %. Postupně se začnete ztrácet ve vašich datech a zbytečně platíte za funkcionality, které nevyžíváte.

Existují nástroje, ve kterých dokážete vytvořit relační databázi a tím si vytvořit nástroj přesně pro vaše potřeby. Můžete si to představit jako "Excel na steroidech". Tímto způsobem dokážete jednak nahradit některá krabicová řešení, ale hlavně si vytvořit nástroj, který bude pro vás ten hlavní. Nástroj ve kterém vždy najdete aktuální informace a jeho spuštění bude první věc po příchodu do práce.

Využít se k tomu dají platformy jako Airtable, SmartSuite, Clickup nebo české Tabidoo.

Po vytvoření jednotného zdroje pravdy s přicházejícími službami jako Zapier Central (v době psaní článku v Beta verzi) jsme jen krok od napojení vlastního AI asistenta a ještě efektivnějšímu využívání našich obchodních dat.

Úroveň 4. - LCNC Guru

Máte svůj klientský portál?

Výše zmíněné 3 úrovně jsou procesně zaměřené, převážně podporující interní procesy a chod společnosti. Jaké ale existují možnosti pro zlepšení vztahu se zákazníkem?

Pomocí nástrojů jako Softr, Glide nebo Noloco se dokážete napojit na svůj jednotný zdroj pravdy a zpřístupnit zákazníkům v omezeném zobrazení a funkcionalitě potřebná data. Když zákazník např. potřebuje zjistit, v jaké fázi se projekt, který mu zajišťujete právě nachází, otevře si portál a vše potřebné zjistí, aniž by proběhla jakákoliv komunikace.

Pomocí nástrojů jako Bubble, FlutterFlow nebo Adalo si můžete vytvořit vlastní webovou nebo mobilní aplikaci. Tady už se ale dostáváme do řešení, která vyžadují vysokou úroveň dovedností a na to, aby přinášela hodnotu, je potřeba se k řešení postavit metodicky jako k tradičnímu vývoji. Zmíněné platformy, nám jen dávají možnosti, které před pár lety ještě neexistovaly. Každá platforma má své výhody a nevýhody a jen jejich porovnání by bylo na samostatný ebook.

Každý business je jedinečný a každý business má jiné potřeby a preference. Na trhu existují tisíce nástrojů, které lze využít a existuje nespočet možných kombinací, jak tyto nástroje propojit. Je důležité myslet na to, že online nástroje jsou zde, aby nám pomohly a podpořily rozvoj našeho business-u a ne proto, abychom kupovali projev inovace. Je důležité vytvořit si ze svých interních procesů systém, který je efektivní, neobsahuje zbytečné kroky a jen se „opírá“ o online nástroje.

Využitím LCNC v porovnání s tradičním programováním získáváme větší flexibilitu dělat změny, zvyšujeme rychlost jakou se přizpůsobujeme trhu a snižujeme závislost na specializovaných IT personálech. Tato kombinace je klíčovým faktorem pro získání konkurenční výhody.

Vybraná bezpečnostní rizika

V rámci shrnutí uvádíme několik možných scénářů relevantních rizik:

- Získání přístupu do integrovaných / automatizovaných aplikací skrz uživatelské rozhraní LCNC.
- Zneužití funkčních integrací skrz LCNC platformu (zneužití propojení k emailu, AI, datům a jiným účtům a aplikacím).
- Únik dat.
- Zneužití kreditů (např. u AI nástrojů).
- Zneužití ovládnuté LCNC platformy k páčání trestné činnosti.
- Zneužití technických zranitelností v AI, LLM.

Chyby uživatelů

Jakých chyb se dopouští uživatelé, kteří se nejčastěji, logicky, soustřeďují na výstupy, než na bezpečnou cestu k potřebným výstupům?

- Deaktivovaná multifaktorová autentizace (MFA) k účtům.
- Využívání jednoho účtu na vše – k běžné práci i integracím.
- Vysoké oprávnění u účtů pro běžnou práci.
- Nevhodně uchovávané, případně nebezpečně sdílené API klíče.
- Žádná rotace klíčů.
- Žádné zálohy dat.
- Nevhodné zacházení s daty (např. při automatizaci analýzy osobních údajů způsobem porušujícím GDPR nebo AI Act).
- Nedostatečné povědomí o tom, jak funguje využívání API, webhooků a AI z hlediska bezpečnosti.

Chyby vývojářů

Jakých chyb se mohou dopouštět vývojáři?

- Vývoj zranitelných API u AI a LCNC.
- Vývoj bez zohlednění bezpečnostních aspektů (SSDLC).
- Nevhodně navržená architektura integrace z hlediska bezpečnosti.
- Data v otevřené formě (např. v query parametrech u webhooků – IČO či jiné identifikátory).
- Nevhodná práce s API klíči - např. sdílení, výměna nezabezpečenou formou.



Bezpečnostní aspekty LCNC a AI / LLM

AI nástroje a jiné LLMs, ale i LCNC platformy se stávají každodenní součástí našich životů. Zatímco nám pomáhají se zajištěním automatizace procesů a dosažením vyšší produktivity obecně, je zapotřebí zaměřit se i na bezpečnost při využívání a implementaci těchto nástrojů a služeb. Bez zohlednění bezpečnostních aspektů se z aplikace AI a LCNC může stát i noční můra – pakliže skrz ně nastane bezpečnostní incident (např. kybernetický útok). Obava z kybernetického útoku by ale rozhodně neměla být důvodem k tomu, abychom se k moderním technologiím obrátili zády. Raději se soustředíme na to, jak tyto technologie implementovat a používat tak, aby to bylo bezpečné a náš business byl tím pádem i dlouhodobě udržitelný.

Jedním z hlavních bezpečnostních rizik je, že uživatelé se často zaměřují jen na výstupy a požadované funkce a zabývají se otázkou zda automatizace, kterou si naklikali v LCNC platformě funguje. Nezapovídají se, jak je to bezpečné. Přitom ale mnohdy používají jeden účet “na všechno”, bez zapnuté MFA (např. shodný účet k firemnímu emailu i k LCNC platformě). V LCNC platformě si pak nastaví spojení přes API do emailu, do banky, do sdíleného úložiště, do fakturačního systému, do chatGPT účtu, do CRM atd.). Pro útočníky jsou pak účty do LCNC platformem bez zapnuté MFA snadný cíl. V momentě, kdy se útočník dostane k platformě, lehce např. provede export dat z propojených systémů, zneužije funkční propojení na email uživatele a aniž by si toho uživatel všiml, využívá platformu k útokům založených na principu BEC (business email compromise) atd.

Dále je vhodné upozornit, že mnoho uživatelů a firem si neuvědomuje, že nástroje, které jsou dostupné zdarma často neumožňují řadu bezpečnostních funkcí, někdy ani MFA. Častěji jsou mezi pokročilými bezpečnostními funkcemi např. volby data regionů, SSO integrace, ukládání logů, pokročilá správa uživatelů atp. Využití takových nástrojů nás může vystavit riziku porušení GDPR a jiných regulací.

Z technického hlediska tu pak máme řadu rizik, která mohou doprovázet využívání SaaS, API, AI / LLM, ať z hlediska chybné implementace a integrace, nebo z hlediska možných zranitelností.

Vybraná bezpečnostní doporučení

Mějte prosím na paměti, že se jedná o obecná doporučení. Ke konkrétním doporučením na základě efektivního posuzování rizik IA/LLM a LCNC je vždy nutné znát celý kontext a detailní business proces. Také technologie (např. konkrétní API, SaaS), data a jejich objem, která jsou zpracovávána prostřednictvím "integrace".

Pokud jde o zajištění informační a kybernetické bezpečnosti, je vhodné zmínit, že zde platí i obecná bezpečnostní doporučení, i když se bavíme o AI nebo LCNC platformách, případně o využití SaaS. Z obecných bezpečnostních aspektů, které je nutné zvážit jsou např.:

- Řízení identit a přístupových oprávnění
- Bezpečnost API
- Správa klíčů + rotace klíčů
- Bezpečná autentizace
- Bezpečnostní doporučení pro využití SaaS a outsourcingu (+ LCNC platforma nebo AI řešení by mělo být ve správě firmy, nikoliv externích konzultantů)
- Bezpečnostní testování
- Bezpečnost dat

Ze specifických doporučení je vhodné zmínit např.:

- Doporučení od OWASP k LLM – OWASP Top 10 for Large Language Model Applications - LLM AI Cybersecurity & Governance Checklist (<https://owasp.org/www-project-top-10-for-large-language-model-applications/>)
- Modelování hrozeb relevantních pro ML / LLM s využitím dat o taktikách, technikách a procedurách z pohledu útočníka – MITRE ATLASTM (Adversarial Threat Landscape for Artificial-Intelligence Systems) (<https://atlas.mitre.org/matrices/ATLAS>)

Zvolení správné platformy z pohledu bezpečnosti

- Ujistěte se, že vybraná platforma je určena pro firemní využití a umožňuje výše zmíněné bezpečnostní funkce.
- Ujistěte se, že vybraná platforma šifruje vaše data - jak v rámci zpracovávání (min. 256-bit SSL/TLS), tak v klidovém stavu (např. Algoritmem AES-256).
- Ujistěte se, že vybraná platforma splňuje best practices – zjistíte to např. tím, že má certifikaci ISO/IEC 27001, nebo SOC 2 Type II Report (a v budoucnu certifikaci podle ISO/IEC 42001:2023).
- Také by vás mělo zajímat umístění datových center / data regiony. To může mít důsledky pro výkon, dodržování předpisů (např. GDPR), suverenitu dat a obnovu po havárii.

POTŘEBUJETE PORADIT?



Potřebujete poradit v oblasti automatizací a integrací pomocí LCNC a AI? Nebo hledáte podporu v oblasti bezpečnosti a řízení rizik těchto řešení? Autoři tohoto white paperu vám rádi pomohou.

Automatizace, integrace

Ing. Nikolas Straka

Lowcodin.com

nikolas@lowcodin.com

[LinkedIn](#)

Bezpečnost

Ing. Martin Konečný, MBA, CISM

Guardians.cz

GSM: +420 736 709 865

martin.konecny@guardians.cz

[LinkedIn](#)

Lowcodin

GUARDIANS 

