

WEALTH

MAGAZÍN

Report 2025

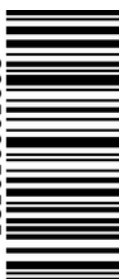
PŘEHLED
POSKYTOVATELŮ IT
A SOFTWAREVÝCH
ŘEŠENÍ PRO SPRÁVU
BOHATSTVÍ

REJSTŘÍK

Jmenný rejstřík
poskytovatelů IT
a softwarových řešení.

OBSAH MAGAZÍNU

Profily vybraných společností
s kontakty a přehledem služeb
IT a softwarových řešení.
Rozhovory s osobnostmi.





OBSAH

Editorial	3
Amenit	7
ANAFRA	10
Applifting	13
BDO	16
exTerra Services	21
MK-VISION	24
MyCom Solutions	27
Vertex	30
ZEBRA SYSTEMS	33
REJSTŘÍK	36

Digitální infrastruktura rodinného bohatství

Jaká IT a softwarová řešení jednotlivci či rodiny s vysokou hodnotou čistého jmění využívají?

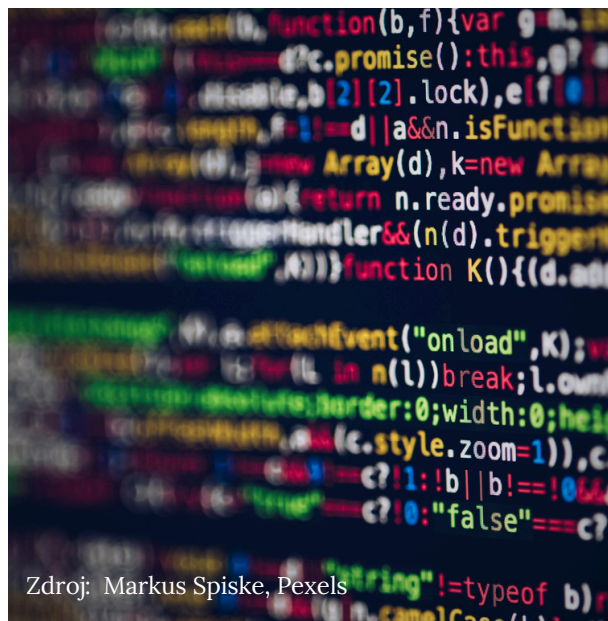
Editorial

V současné době se technologie stávají základem pro zachování i rozvoj rodinného jmění napříč generacemi. Do správy osobního i rodinného bohatství vstupují složité investiční struktury, měnící se regulace, důraz na kyberbezpečnost a generační očekávání. Digitalizace v oblasti správy rodinného bohatství tak není pouze módním trendem, ale nutností. S vývojem digitálních technologií proto roste poptávka na využití nejnovějších IT a softwarových řešení v oblasti správy bohatství.

Jednotlivci i rodiny s vysokou hodnotou čistého jmění hledají řešení zejména pro následující oblasti:

- Digitální identita, ochrana soukromí a kyberbezpečnost
- Finanční software, nástroje pro správu majetku, investic a digitálních aktiv
- Zabezpečená komunikace, síťové a cloudové služby
- Komunikační nástroje a nástroje pro Family Governance
- Personalizované poradenství a audit v oblasti technologií
- Správa a ochrana rodinného know-how a obchodních záležitostí
- Nástroje pro strategické plánování a správu nefinančních aktiv
- Automatizované systémy pro řízení byznysu a workflow

Mezi ta nejčastější IT a softwarová řešení pro správu majetku dnes však patří zejména kyberbezpečnost a ochrana digitální identity, správa investic, audit IT nebo nástroje pro Family Governance. „V současné době jsou prioritou dvě oblasti. Virtualizace, aktuálně řešíme klientům přechod z platformy VMware, kterou její majitel, Broadcom, úspěšně zabil cenovou a licenční politikou hraničící s vydíráním. Druhou oblastí je už několik let bezpečnost,“ upřesnil Petr Šantrůček, jednatel exTerra Services.



**Jaká IT a softwarová řešení v dnešní době
HNWI a movité rodiny nejčastěji vyhledávají?**

Digitální reporting a správa investic

Základem každého moderního Family Office nebo movité rodiny je robustní systém pro správu investic a finančního reportingu.

Tyto nástroje sdružují data o majetku napříč třídami aktiv, jurisdikcemi a správci. Umožňují tak nejen pravidelné výkazy pro jednotlivé členy rodiny, ale i pokročilé analýzy výkonnosti, rizik nebo plnění investičních cílů. Zvláště důležitá je schopnost integrovat různorodá data z bank, správcovských fondů, nemovitostních struktur či privátních investic do jedné bezpečné platformy. Transparentnost a možnost porovnávat vývoj portfolia v čase jsou zásadní pro informované rozhodování a strategické řízení bohatství. Na tento problém reagují i české společnosti, které se zaměřují na IT a softwarová řešení.

„Opakovaně jsme viděli, jak náročné je držet přehled o všech investorech, splátkách, emisích i související dokumentaci. Prostě řešit, byť i jednu menší emisi v excelovské tabulce, je ‚peklo‘. Chybovost se často stává problémem důvěryhodnosti a to je v oblasti financí naprosto zásadní,“ říká zástupce společnosti MK-VISION, která vyvinula software Bondsys.



Zdroj: Anyaberkut, Getty Images

Komunikační nástroje a řešení pro Family Governance

V prostředí vícegeneračních rodin hrají zásadní roli také technologie, které podporují interní komunikaci, sdílení dokumentů a řízení procesů v rámci Family Governance. Specializované nástroje umožňují bezpečné ukládání a sdílení dokumentace, jako jsou například zakladatelské

listiny, zápisy z rodinných rad či pravidla pro nástupnictví. Využívány jsou rovněž kalendáře rodinných událostí, hlasovací nástroje či vzdělávací platformy pro mladší generace. Podpora digitální komunikace a transparentního rozhodovacího procesu je důležitá zejména v případech, kdy členové rodiny žijí v různých zemích a časových pásmech.

Ochrana dat a kyberbezpečnost

S digitalizací správy bohatství přichází i zvýšené nároky na kybernetickou bezpečnost. Soukromé informace o majetku, právní struktuře či rodinných vztazích jsou vysoce citlivé a stávají se cílem dnes velmi sofistikovaných hrozeb.

9 nejčastějších kybernetických hrozeb podle společnosti Amenit:

- Telefon od „banky“ nebo „policie“, že máte akutní problém
- Podvodné QR kódy
- Ransomware
- Veřejné Wi-Fi sítě
- Zastaralé operační systémy
- Slabá hesla a špatná správa přístupových údajů
- Nepodporované nebo neznámé aplikace
- Absence záloh
- Neznalost

Z textů jednotlivých společností poskytujících IT a softwarová řešení pro správu bohatství pro Wealth Magazín - Report vyplývá, že právě kyberbezpečnost je v současné době jedním z nejdiskutovanějších témat. „Pro úspěšné podnikatele a rodiny s vysokým čistým jměním je velmi důležité nejen chránit osobní údaje, ale také

citlivé informace a firemní data,“ sdělili zástupci společnosti Vertix. Movití jednotlivci a rodiny proto investují do systémů pro šifrování dat, řízení přístupových práv, vícefaktorového ověřování nebo detekce narušení. „Zatímco průměrná škoda způsobená ransomwarem se v Evropě pohybuje kolem 80.000 €, dobře nastavená prevence a školení zaměstnanců stojí zlomek,“ doplnil představitel společnosti MyCom Solutions.

Samostatnou oblastí je školení rodinných příslušníků a personálu, tzv. „digitální hygiena“ se stává nedílnou součástí bezpečnostní kultury. „Uživatel může být tou nejdůležitější bezpečnostní vrstvou. Pokud ale není proškolen na nejnovější kybertrendy a triky, stává se rizikem – snadno naletí na falešný e-mail a umožní útočníkům překonat i zbývající bezpečnostní vrstvy,“ upřesnil Zdeněk Bínek, zakladatel Zebra Systems.



Zdroj: Formatoriginalphotos

V některých případech je kyberbezpečnostní infrastruktura navrhována a spravována srovnatelně důsledně jako ve finančních institucích. Vznikají tak nové bezpečnostní produkty a modely, které rodiny následují. Příkladem je Zero Trust Architecture. „Zero Trust je model kybernetické bezpečnosti založený na jednoduché, ale revoluční myšlence: žádný uživatel, zařízení ani služba nemá mít automaticky důvěru – bez ohledu na to, zda se nachází uvnitř nebo vně firemní sítě.

Každý požadavek na přístup k firemním systémům je považován za potenciální hrozbu, dokud není ověřen,“ vysvětlil pojem Marek Kovalčík, cybersecurity manager v BDO.

Nástroje pro strategické plánování a správu nefinančních aktiv

Vedle finančních toků a investic často HNW jednotlivci a rodiny spravují také další nefinanční majetek – sbírky umění, filantropické nadace, nemovitosti, jachty či rodinné firmy. Softwarové nástroje v těchto oblastech pomáhají sledovat hodnotu, provozní náklady, právní dokumentaci i dlouhodobé cíle spojené s těmito aktivy. Často bývají propojeny s portfoliem nebo integrované do širší platformy správy bohatství. Strategické plánování navíc zahrnuje nástroje pro simulaci budoucího vývoje majetku, daňové optimalizace či mezigenerační převody například formou trustů či nadací.

Personalizované poradenství a technologický audit

Rodiny s významným majetkem dnes čelí otázce, jak technologie využívat smysluplně a strategicky. Zvláště tam, kde se správa majetku opírá o vlastní Family Office nebo komplexní strukturu poradců, se proto stále častěji uplatňuje specializované technologické poradenství. Nejde jen o výběr správných nástrojů, ale především jejich propojení, nastavení bezpečnostních standardů a přizpůsobení konkrétním potřebám dané rodiny.

„Vytvořili jsme proto koncept hybridních týmů, jehož principem je sestavení pracovní skupiny z našich programátorů s týmem zákazníka. Ti vzájemně sdílejí své know-how a produkt vyvíjejí společně. Cílem je, aby klient vyvíjel aplikaci v domácím prostředí s použitím vlastních

nástrojů, procesů a lidí a bez závislosti na nás jako dodavateli,” popsali zástupci společnosti Applifting.

Součástí tohoto typu řešení bývá také tzv. audit digitální zralosti – tedy posouzení, nakolik systémy, které rodina využívá, odpovídají jejím cílům, způsobu života i rizikovému profilu. „Málokdo si uvědomuje, že i IT technologie je potřeba přizpůsobovat změnám, a to nejen interním, ale i externím. Růst, digitalizace, legislativa, kyberbezpečnost – to všechno jsou proměnné, které by měla vaše IT infrastruktura reflektovat,“ upřesnili specialisté ze společnosti ANAFRA.

Takový individuální přístup pomáhá vytvořit technologické zázemí, které neruší, ale naopak tiše slouží. Ať už jde o ochranu citlivých dat, sdílení know-how mezi generacemi, nebo o to, aby každý člen rodiny rozuměl své roli ve správě rodinného jmění.

Pro koho jsou tato řešení určená?

Technologická řešení v oblasti správy rodinného bohatství nejsou jen výsadou největších rodin. Oslovují široké spektrum movitých jednotlivců, rodin a jejich organizací.

Vícegenerační rodiny

Rodiny, které spravují majetek napříč třídami aktiv a kontinenty, ocení digitální nástroje pro přehled, komunikaci i kontrolu mezigeneračního předávání hodnot.

Majitelé rodinných firem

Ti, jež stojí před otázkou nástupnictví, hledají v technologiích nejen efektivitu, ale i způsob, jak formalizovat a přenést své know-how a rozhodovací procesy.

Jednotlivci a rodiny s vysokou hodnotou čistého jmění (HNWI a UNHWI)

HNWI využívají služeb externích poradců či bank a často chtějí mít přístup k datům, bezpečnou komunikaci i možnost auditovat správu svého jmění s vysokou mírou autonomie.

NextGen

Nová generace správců majetku, kteří často přistupují k bohatství jinak než jejich předchůdci, očekává digitální přehled, vzdělávací platformy, ESG analytiku a bezpečné komunikační kanály.

Single i Multi Family Offices

Rodinné kanceláře využívají sofistikované softwarové nástroje k řízení operativy, compliance, investiční strategie i vztahů s členy rodiny.

Na dalších stranách tohoto vydání publikace Wealth Magazín - Report naleznete bližší informace o společnostech, které poskytují IT a softwarová řešení pro správu rodinného bohatství. Věříme, že aktuální publikace pro vás budou přínosem.

Vážené čtenářky, vážení čtenáři,
přejeme vám příjemné čtení.



Eva Ulrichová

Eva Ulrichová
Šéfredaktorka



KONTAKT

TEL.: +420 556 706 203

E-MAIL: amenit@amenit.cz

WEB: www.amenit.cz



Ilustrační obrázek

Zdroj: Amenit

Amenit

Digitální komfort bez rizika? Bohužel mýtus.

Ve světě chytrých domů, luxusních hotelů a mezinárodního cestování si dnes málokdo z nás uvědomuje, že právě pohodlí, které nám technologie přináší, je často vykoupeno zásadními bezpečnostními riziky. Čím cennější jsou naše data nebo soukromí, tím větší hrozby nám hrozí. A právě proto by měl být základní přehled o digitálních hrozbách nedílnou součástí moderního životního stylu.

V následujícím krátkém článku pro vás shrneme hrozby, se kterými se dnes běžně setkáváme a které se mohou týkat každého z nás. Stačí jediná vteřina nepozornosti

a problém je na světě. Častým omylem přitom bývá domněnka, že cílem útoků jsou jen velké firmy nebo instituce. Opak je bohužel pravdou. Dnešní automatizované útoky míří právě na jednotlivce a menší subjekty, u kterých se útočníci spoléhají na velmi nízkou úroveň zabezpečení a mnohem menší pravděpodobnost dalšího šetření takového incidentu.

Když „banka“ nebo „police“ volá, že máte akutní problém

Představte si, že vám volá číslo, které se tváří jako vaše banka, nebo dokonce policie. Hlas na druhém konci zní profesionálně, ale naléhavě.

Upozorňuje na aktuální podezřelou transakci a žádá vás o spolupráci při domnělé záchraně vašich prostředků. Mluví rychle, abyste neměli čas přemýšlet. Dostáváte jasné instrukce. Za pár minut jste přišli o veškeré úspory. Tak jednoduché to je. A stává se to bohužel dnes a denně.

Veřejné Wi-Fi sítě – pohodlný přístup pro vás i pro útočníky

Hotel, kavárna, letiště. Bezpečné, protože mají přece heslo? Omyl. Sdílíte-li síť s útočníkem, dáváte mu tím možnost sledovat vaši aktivitu a potenciálně i získat citlivé údaje, jako jsou hesla nebo e-maily.



Ilustrační obrázek
Zdroj: Amenit

Podvodné QR kódy – když v sobě QR kód ukrývá více, než by měl

Stojíte na ulici, míříte na večeri a potřebujete zaplatit parkování. Naskenujete QR kód z automatu. Netušíte, že přes noc tam někdo přelepil falešný. Zadáte platební údaje a do několika minut mizí všechny peníze z účtu.

Ransomware – vaše data jako rukojmí

Otevřete zdánlivě neškodnou přílohu v e-mailu. V pozadí se nepozorovaně spustí software, který zašifruje veškeré vaše dokumenty, fotografie i zálohy. Následně se na obrazovce objeví výzva k zaplacení výkupného v kryptoměně. Když nezaplatíte, přijdete o všechno. Když zaplatíte, neexistuje žádná garance, že útočníci po zaplacení data rozšifrují.

Zastaralé operační systémy – otevřená brána pro útoky

Používáte starší tablet nebo telefon, protože se vám nechce všechno kopírovat na nový? Necháváte počítač měsíce bez aktualizací, „protože přece funguje“? Každý den tím riskujete, že někdo využije známé bezpečnostní chyby, které výrobce už dávno opravil.

Slabá hesla a špatná správa přístupových údajů

Kolik znaků mají vaše hesla? Mají alespoň 12 znaků, ideálně však 16 a více? Obsahují kombinaci malých a velkých písmen, číslic a speciálních znaků? Nebo spoléháte na snadno odhadnutelné fráze, jako je datum narození, číslo domu, přezdívká, nebo dokonce klasické „123456“? A co opakování hesel? Používáte

stejné přihlašovací údaje napříč různými účty a službami? A přidali jste si vůbec dvoufaktorové ověření (2FA/MFA), například potvrzení přístupu pomocí ověřovací aplikace? Když útočník prolomí jediné slabé heslo, často tím získá klíč i k vašim dalším účtům.

Nepodporované nebo neznámé aplikace

Nová aplikace nebo hra vypadá na první pohled super, doporučil vám ji přece známý. Už se nemůžete dočkat a během rychlé instalace ji bez přemýšlení udělíte všechna oprávnění, o která vás požádala – oprávnění ke kontaktům, mikrofonu a souborům. Takzvané „malicious“ neboli škodlivé aplikace pak sbírají data nebo dokonce zpřístupní celý váš telefon nezvaným hostům, kteří mohou klidně sedět na opačném konci světa.

Absence záloh

Stalo se něco? Smartphone spadl do vody? Zapomněli jste jej v kavárně a po rychlém návratu na místo už na stole není? Někdo ho ukradl! Ale vy nemáte zálohu? Nebo ji možná i máte, ale byla špatně nastavená a spousta dat se prostě nezálohovala. Nebo ještě lépe, neznáte heslo k úložišti se zálohou. Co teď?

Neznalost – největší riziko dneška

Možná vůbec nejvážnějším rizikem je fakt, že drtivá většina uživatelů netuší, čeho by se měla bát. Věří, že když používají iPhone, mají vyhráno. Že když mají antivirový software, jsou 100% chráněni. Skutečnost je ale mnohem složitější.

Na některé hrozby ani nejlepší nástroje světa nestačí. Útok je totiž mnohdy veden psychologicky, přímo na uživatele, který sám a dobrovolně útočníkům dá, co chtějí. Útočníci tak nemusí překonávat žádná hesla ani jiná bezpečnostní opatření. A právě neznalost a neopatrnost uživatelů dělá z digitálního prostoru potenciálně nebezpečné místo, kde se útočníkům snadno daří páchat všemožné podvody.

Ochrana, která dává smysl – bez složitosti

Dobrou zprávou je, že proti většině těchto rizik se lze efektivně bránit. Český výrobce s podporou fondu Mastercard je správnou volbou. Obrátte se na nás a řekneme vám více...

[Amenit s.r.o.](#) – 24 let zkušeností a mnoho spokojených zákazníků





KONTAKT

TEL: +420 773 745 727

E-MAIL: gabriela.chumchalova@anafra.cz

WEB: www.anafra.cz



Gabriela Chumchalová
IT Solutions sales director

ANAFRA

Audit IT – udělejte první krok k modernímu a bezpečnému IT

Odpovídá stav vašich IT technologií dnešním standardům a vašim potřebám? Jsou vaše data v bezpečí? Potýkáte se často s výpadky systémů a nedostupností dat? Odpovědi i příčiny vám odhalí audit IT.

Proč byste si tyto otázky měli položit?

Bez IT už se dnes neobejde nikdo, to všichni víme. Málokdo si však uvědomuje, že i IT technologie je potřeba přizpůsobovat změnám, a to nejen interním, ale i externím. Růst, digitalizace, legislativa, kyberbezpečnost – to všechno jsou proměnné, které by měla vaše IT infrastruktura reflektovat.

Klíčová je zejména bezpečnost dat, jelikož díky digitalizaci jsme na datech závislí a při jejich nedostupnosti či ztrátě se ocitneme v pasti. Počet útoků v kyberprostoru nejenže roste, ale díky nástupu AI se útoky stávají sofistikovanější a představují stále větší riziko. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) v roce 2024 zaznamenal dosud nejvyšší počet bezpečnostních incidentů. Je tedy zcela na místě klást si otázku, zda jsou vaše data dostatečně chráněna.

I časté výpadky systémů mohou způsobit značné komplikace a připravovat vás tím o zisk.

Znamená to, že stávající infrastruktura neodpovídá vašim aktuálním potřebám. Pokud vám poroste chodidlo, koupíte si o číslo větší boty. V malých botách prostě a jednoduše daleko nedojdete. U IT infrastruktury je to stejné. Je potřeba ji průběžně optimalizovat.



Jak postupovat, pokud chcete mít IT v pořádku?

Ideální je získat na vaše IT nezávislý odborný pohled. Díky auditu IT jsme schopni vám komplexně zmapovat softwarové a hardwarové technologie i IT procesy. Najdeme úzká místa, identifikujeme rizika a navrhujeme nápravná opatření. Zkontrolujeme licencování, zálohování dat i možný soulad s aktuálními právními normami a doporučíme kroky k celkové optimalizaci a modernizaci IT. Můžeme vám pomoci i s definováním IT směrnic a zpracováním výsledné dokumentace, pokud vám chybí. Nemusíte se pak hrozit toho, co se stane, až vás opustí váš „ajták“, který má jako jediný o vašem IT přehled.

Na co se při auditu zaměřujeme?

Audit jsme schopni provést pouze do té míry, do jaké nám bude umožněn přístup. Bez vaší součinnosti a administrátorského přístupu na server a k síťovým prvkům, jako jsou routery a switche, se moc hluboko nedostaneme.

Po získání přístupu důkladně analyzujeme tyto oblasti:

1. Typologie sítě

- Architektura
- Zařízení, která se v síti vyskytují
- Síťové prvky, koncová zařízení, tiskárny
- Docházkový systém, kamery
- Oprávnění a přístupy, VLAN apod.

2. Serverová část

- Počty a typy serverů, včetně služeb, které na nich běží
- Aktualizace a zálohy

3. Koncová zařízení

- Stanice, operační systém, parametry
- Oprávnění, hesla, zálohy

4. Audit licencí, antivirová zabezpečení

Auditem to pro nás nekončí

Jako nezávislý partner vám s celým auditem rádi pomůžeme. Problémy nebo nedostatky, na které během auditu narazíme, umíme rovnou i technicky vyřešit. Jsme poskytovatelem softwaru i dodavatelem potřebného hardwaru, který už téměř 20 let přijímá odpovědnost za IT našich klientů. Záleží nám na tom, abychom našli řešení, které dává smysl pro konkrétního zákazníka. Bezpečnost dat je pro nás prioritou, držíme je proto na serverech ve vlastním datacentru certifikovaném na stupeň TIER III a garantujeme bezproblémový a spolehlivý 24hodinový provoz. Naše technická podpora vám poskytne support 24/7. Stačí zavolat.



POŘIÐTE SI PŘEDPLATNÉ NAŠEHO TIŠTĚNÉHO ČASOPISU

včetně DPH a poštovného po České republice

**Pouze
1.000 Kč
ročně**



Více informací naleznete na
wmag.cz/predplatne-wealth-magazin-premium/





KONTAKT

TEL: +420 605 540 481

E-MAIL: info@applifting.cz

WEB: www.applifting.io



Vratislav Kalenda
CEO CZ & Founder

Applifting

Nezískáte jen software. Předáme vám i know-how, abyste byli nezávislí

IT sektor je vysoce konkurenční prostředí, kde si vývojářské firmy přirozeně chrání své know-how a snaží se být pro zákazníka nenahraditelné.

Klient zůstává závislý na dodavateli, který jediný může provádět dodatečné opravy a úpravy a inkasovat za to další peníze.

Co když to ale jde i lépe, aniž by na tom vývojářská firma trátila? Zákazník dostane potřebné know-how k tomu, aby mohl software provozovat a dále rozvíjet samostatně – bez závislosti na dodavateli. Odměnou jsou nadstandardní vztahy s klienty, dlouhodobá

partnerství i kladné reference. V Appliftingu máme ověřené už 11 lety praxe, že to funguje.

Úplná transparentnost? Základem je firemní kultura

Od začátku jsme měli jasno v tom, jak je pro nás důležitá svoboda klienta. Nechceme mu být pouhým dodavatelem služeb. Naopak je naším cílem plně jej zapojit do vývoje a dovést ho do fáze, kdy bude schopen aplikaci obsluhovat a vylepšovat již po vlastní ose. Nezávisle na nás. Tento přístup má kořeny v takzvané „tyrkysové“ kultuře, která je založená na volnosti, naprosté

otevřenosti a spokojenosti lidí. Takto ji alespoň definuje Frederic Laloux ve své knize Budoucnost organizací. Vymyká se tradiční hierarchii s množstvím manažerů, lidé zde dělají nezávislá rozhodnutí a nesou za ně odpovědnost.

Vliv na směřování firmy tak mají nejen zakladatelé, ale i pracovníci. Vyžaduje to naprostou důvěru v kolegy a současně z jejich strany vysokou míru odpovědnosti. Místo na dodržování finančních plánů se zde hledí na kreativitu a schopnost nalézat řešení problémů. A podobný princip jsme právě zavedli i ve spolupráci s klienty.

Hybridní týmy jako cesta k otevřené spolupráci

Vzájemná důvěra a otevřenost vedou ke snadnějšímu toku informací a přístupu přímo k jádru problému, a tak dokážeme být mnohem efektivnější. Zjistili jsme, že takové nastavení dělá členům týmu největší radost.

Zákazníkovi navíc přináší maximální hodnotu za jeho peníze, díky čemuž se k vám rád vrátí i doporučí ostatním.

Vytvořili jsme proto koncept hybridních týmů, jehož principem je sestavení pracovní skupiny z našich programátorů s týmem zákazníka. Ti vzájemně sdílejí své know-how a produkt vyvíjejí společně. Cílem je, aby klient vyvíjel aplikaci v domácím prostředí s použitím vlastních nástrojů, procesů a lidí a bez závislosti na nás jako dodavateli.

Porovnejte to se situací, kde klient dostane hotový software, aniž by měl ponětí, jak vlastně vznikl. S hlavními principy je seznámen v rámci několikahodinového školení, které jen těžko obsáhne všechny aspekty mnohaměsíčního procesu vývoje. A s aktualizacemi a změnami je závislý na původním dodavateli. Nepříliš lákavá představa, že? Přesto je toto každodenní realita, kterou spousta firem tiše toleruje.



Filip Kirschner
COO & Founder

Dvakrát měř, jednou řež platí i u vývoje

Další chyba, kterou firmy často dělají, je vývoj produktu bez dostatečného porozumění byznysu a reálným potřebám uživatelů. Věříme, že smysluplný produkt nevzniká náhodou. Už od začátku spolupráce proto investujeme čas do důkladné přípravy, ať už formou workshopů s klientem, nebo pomocí ověřených metod, jako je Design Sprint, který pomůže v rámci jediného týdne ověřit životaschopnost produktu. Cílem je vyhnout se slepým uličkám, minimalizovat riziko zbytečných nákladů a postavit něco, co má skutečnou šanci uspět. A jelikož si zakládáme na otevřenosti, výsledky těchto workshopů máte opět plně k dispozici. Je jen na vás, jak je využijete. Pokud se rozhodnete vyvíjet dál s námi, je celá tato příprava už v ceně.

Nejednou jsme se setkali s případy, kdy byl původní návrh až příliš ambiciózní, nebo naopak nedostatečný. Právě tato metoda, kdy si ve fázi validace nápadu oboustranně ujasníme směřování, může potenciálně zachránit cenné prostředky i čas. Příkladem z nedávné doby je vývoj vzdělávací platformy Skoala pro Nadaci České spořitelny, kde testování v rámci Design Sprintu pomohlo ujasnit směřování produktu, nebo aplikace Kuba English, digitálního učitele angličtiny poháněného umělou inteligencí.

S čím se na nás můžete obrátit?

Už více než 11 let pomáháme budovat komplexní digitální produkty. Spolupracujeme jak se startupy (např. Investown nebo Twigsee), tak s velkými hráči, jako jsou Jablotron, Česká spořitelna nebo kanadský Telus Health. Stojíme i za projekty, které zlepšují život nám všem – třeba systém digitálního ověřování identity BankID nebo platforma pro finanční edukaci dětí Skoala.

Řešíme celý životní cyklus produktu, od strategie a validace přes UX/UI design a vývoj až po implementaci AI a provoz infrastruktury nebo škálování a přípravy pro další růst.

Máte nápad na nový produkt nebo chcete digitalizovat svůj stávající byznys? Ozvěte se – rádi se s vámi potkáme.





KONTAKT

TEL: +420 241 046 111

E-MAIL: bdo@bdo.cz

WEB: www.bdo.cz



Marek Kovalčík

Cybersecurity Manager, Ethical Hacker & CISO v BDO

BDO

Zero Trust Architecture: Konec slepé důvěry v kyberprostoru

Digitální svět je dnes propojenější než kdy dřív. Zároveň však platí, že s každým novým zařízením, uživatelem nebo cloudovou službou roste i počet potenciálních vstupních bran pro kybernetické útočníky.

Tradiční bezpečnostní přístupy, které předpokládají, že vše uvnitř sítě je důvěryhodné, už zkrátka nestačí. A právě tady přichází ke slovu Zero Trust Architecture (ZTA) – strategie, která v kyberbezpečnosti hlásá jasné heslo: „Nedůvěřuj, vždy ověřuj.“

Co je Zero Trust?

Zero Trust je model kybernetické bezpečnosti založený na jednoduché, ale revoluční myšlence: žádný uživatel, zařízení ani služba nemá mít automaticky důvěru – bez ohledu na to, zda se nachází uvnitř nebo vně firemní sítě. Každý požadavek na přístup k firemním systémům je považován za potenciální hrozbu, dokud není ověřen.

Zatímco tradiční přístupy stavěly ochranu především na hranici sítě, Zero Trust počítá

s tím, že takový bezpečnostní perimetr už v éře cloudových služeb, vzdálené práce a mobilních zařízení vlastně neexistuje.

Na čem Zero Trust stojí?

Celá architektura Zero Trust stojí na třech základních pilířích:

1. Ověření identity – Každý uživatel musí být důkladně ověřen. Nestačí jedno přihlášení, identita je průběžně kontrolována.
2. Ověření zařízení – Zároveň je třeba prověřit, zda je zařízení bezpečné a oprávněné pro přístup.
3. Minimální práva (Least Privilege Access) – Uživatel má přístup pouze k těm zdrojům, které nezbytně potřebuje pro svou práci.

Dalšími klíčovými principy Zero Trust jsou:

- Mikrosegmentace sítě – Sít' je rozdělena na menší segmenty, čímž se omezuje možnost pohybu útočníka.
- Kontinuální monitoring a analýza chování – Vše, co se v síti děje, je sledováno v reálném čase.
- Šifrování dat a ochrana aplikací – Informace jsou chráněny nejen při přenosu, ale i v klidovém stavu.



Ilustrační obrázek
Zdroj: Guvendemir, Getty Images Signature

Proč Zero Trust nabývá na významu?

Zero Trust získává na popularitě především kvůli rostoucímu počtu bezpečnostních incidentů a rozpadu tradičních hranic sítí. S přechodem na cloudové služby, rozvojem hybridní práce a mobilního přístupu k datům již není možné spoléhat na bezpečnost uvnitř firemní infrastruktury. Navíc pokročilé technologie, jako strojové učení a umělá inteligence, umožňují v rámci Zero Trust monitorovat síťové chování a automaticky reagovat na podezřelé aktivity v reálném čase.



Ilustrační obrázek
Zdroj: Just_Super, Getty Images Signature

Proč by firmy měly Zero Trust zvážit?

Zero Trust Architecture je jedním z nejučinnějších nástrojů, jak dnes organizace mohou zvýšit svou kybernetickou odolnost. Zavedení tohoto přístupu má tyto výhody:

- Minimalizuje riziko narušení dat – díky průběžnému ověřování a omezení přístupu.
- Chrání před interními i externími hrozbami – uživatelé i zařízení musí neustále prokazovat svou důvěryhodnost.
- Umožňuje rychle detekovat a reagovat na incidenty – díky kontinuálnímu monitoringu a automatizaci.
- Pomáhá při auditech a plnění regulatorních požadavků – prokazatelně zajišťuje řízení přístupů.
- Přispívá k byznysové kontinuitě – bezpečnostní incidenty nezastaví chod firmy.

Přijetí Zero Trust architektury není bez překážek:

- Náročný přechod – Implementace může vyžadovat investice do technologií, školení a revizi stávajících systémů.
- Kompatibilita se staršími systémy – Legacy systémy často neumožňují pokročilé ověřování.
- Konzistence napříč organizací – Dodržování zásad Zero Trust i u partnerů a dodavatelů je výzvou.
- Uživatelská zkušenost – Příliš přísné ověřovací procesy mohou uživatele frustrovat.

Zero Trust proto není jen o technologiích, ale hlavně o strategickém plánování, nastavení procesů a průběžném řízení změn.

Jaké konkrétní technologie je nutné implementovat?

Neexistuje jedna černá skříňka, kterou by si organizace poříдила a jejím nasazením do firemní sítě mohla považovat naplnění ZTA strategie za hotové. Jedná se o komplexní pohled na bezpečnost, který musí zohledňovat bezpečnost všech používaných informačních kanálů. Vhodné nasazení bezpečnostních technologií, jako jsou Next-Gen firewally (NGFW), VPN, antivirový software, logování, nebo zálohování, hraje velmi důležitou roli v kybernetické odolnosti organizace. Nezaručují však neprostupnost pro potenciální útočníky a je nutné je doplnit o další vrstvy ochrany. Nápomocné může být například **ZTA desatero**.

Implementace ZTA strategie je výzvou pro firmy a také pro administrátory, jejichž odpovědností je zařídit bezproblémovou funkčnost a bezpečnost dílčích řešení.

Snadno se může stát, že systém nebude nakonfigurovaný zcela správně a bude vytvářet útočníkům příležitost ke kompromitaci sítě. Navíc technologie v čase zastarávají a nové bezpečnostní zranitelnosti jsou objevovány každý den. Pro odhalení i těch nejmenších bezpečnostních skulinek je nutné provádět periodické penetrační testování zkušenými profesionály.

Zero Trust Architecture desatero:

1. Řízení identit a přístupů – IAM (Identity and Access Management)
2. Vícefaktorová autentizace – MFA (Multifactor Authentication)
3. Rozhodování o přístupu na základě politik – ZTA Policy Engine / PDP (Policy Decision Point)
4. Vynucování přístupových pravidel v síti – PDP/PEP (Policy Enforcement Point)
5. Izolace částí sítě pro omezení pohybu útočníka – Network Segmentation
6. Kontrola stavu zařízení (aktualizace, EDR, šifrování...) – Device Posture Assessment
7. Neustálé ověřování a sledování chování – Continuous Authentication & Monitoring
8. Minimální potřebná oprávnění pro uživatele a zařízení – Least Privilege Access
9. Bezpečný přístup ke cloudovým aplikacím – SASE (Secure Access Service Edge)
10. Sdílená identita a jednotné přihlášení – Identity Federation / SSO (Single Sign-On)

V době, kdy kybernetické hrozby číhají za každým kliknutím, se koncept nulové důvěry stává klíčovým prvkem moderní bezpečnostní strategie. Přechod na Zero Trust je sice náročný, ale investice do něj je investicí do dlouhodobé stability a bezpečnosti každé firmy.



Zjednodušte si správu vášeho majetku pomocí inovativních technologií



Investujeme do technologií, které
vám díky automatizaci a přístupu
k informacím 24/7 umožní věnovat
více času tomu podstatnému.

eTRUST je digitální nástroj
a informační systém pro organizaci
rodiny, správu majetku i fondů.

www.etrust.cz





KONTAKT

TEL.: +420 602 119 906

E-MAIL: obchod@exterra-services.cz

WEB: www.exterra-services.cz



Petr Šantrůček
Jednatel společnosti

exTerra Services

„Nenabízíme zákazníkům nic, co bychom si sami nekoupili,“ říká Petr Šantrůček.

Jaké výzvy Petr Šantrůček se svým týmem nejčastěji řeší? A co je pro ně prioritou v rámci kybernetické bezpečnosti i dalších oblastí? To vše v rozhovoru zazní. A nechybí ani zmínka o trendech nebo nejčastějších mýtech v IT.

Jak byste představil Vaši firmu někomu, kdo Vás nezná?

Jsme kompaktní tým odborníků s mnohaletou praxí v IT. Máme zkušenosti jak s malými zákazníky, tak s velkými korporacemi. Dokáží postavit ad hoc tým rozšířený operativně o další specialisty. Zároveň umíme velmi rychle reagovat a začít pracovat s ohledem na situaci

i okamžitě a papírování, včetně smluvního, řešit souběžně nebo až po uhašení požáru. Stejně jako v práci samotné, tak i v obchodě se snažíme naplňovat zásadu Tomáše Bati popsanou takto: „Pod obchodní poctivostí rozumíme, že veškeré strany na obchodě zúčastněné musí být po provedení obchodu bohatší, než byly předtím.“

V čem se podle Vás Vaše společnost liší od ostatních v IT oboru?

Často nás oslovují klienti s problémy, na které si netroufli mnohem větší konkurenti. Pracujeme rychle a efektivně. Když to situace vyžaduje, obejdeme se bez formalit. Reference mluví za

nás. A v neposlední řadě nikdy nenabízím zákazníkům nic, co bych si sám nekoupil.

Můžete uvést příklad nějakého projektu, který Váš přístup ilustruje?

Velká německá pojišťovna čelila personální krizi, kdy jim odcházal poslední linuxový specialista. Na základě kontaktu tady v ČR jsem si s jejich evropským šéfem IT plácnul a dostali jsme za úkol převzít správu všech linuxových serverů (několik desítek) do vyřešení jejich personální krize. Jediné, co se papírově řešilo, byla NDA pro členy mého týmu. Během cca měsíce jsme převzali správu a ta dočasnost se protáhla na asi 4 roky. Celé to bylo postavené na podání ruky. V mém světě se dané slovo drží, a to podání ruky je dostatečné. Většinou, samozřejmě.



Jaké projekty nebo oblasti jsou pro Vás aktuálně nejdůležitější?

V současné době jsou prioritou dvě oblasti.

Virtualizace, aktuálně řešíme klientům přechod z platformy VMware, kterou její majitel, Broadcom, úspěšně zabil cenovou a licenční politikou hraničící s vydíráním. Druhou oblastí je už několik let bezpečnost. Dodávky technických řešení jsme rozšířili před 3 lety o školení základů kyberbezpečnosti pro uživatele, kteří jsou nejzranitelnější součástí IT. Máme v této oblasti velmi pochvalné reference.

Jak řešíte otázku kybernetické bezpečnosti a ochrany dat ve vašich službách?

To je natolik široká oblast, že ve zkratce mohu jen říci, že bezpečnost pojmáme jako komplexní úlohu a neomezujeme se jen na dílčí řešení. Zní to jako klišé, ale tohle je náš přístup.

Které technologie dnes považujete za zásadní pro růst firmy a proč?

Technologie je jen nástroj, používáme takové, které jsou pro zákazníka užitečné. S důrazem na slovo užitečné. Funkční a moderní řešení nabízí každý, my chceme, aby byla zároveň užitečná.

Jak se Vaše firma přizpůsobuje rychle se měnícím IT trendům a očekáváním klientů?

Slovy klasika, učit se, učit se, učit se. Celou svoji praxi se učím. A i moje firma se neustále učí.

Setkáváte se v praxi s nějakými mýty o IT, které byste chtěl vyvrátit?

Mám-li vypíchnout jeden, pak je to IT firmami často prodávané tvrzení, že jejich nástroj, služba či systém nějakou oblast vyřeší navždy. V IT totiž nic není navždy a je šarlatánství to tvrdit. Druhý, aktuální mýtus je, že firmy mají infrastrukturu převést do cloudu. Celou. Samozřejmě je cloud

užitečný, ale jen pro některé zákazníky a některé systémy. I zde razíme, že nástroje se mají používat jen na to, na co jsou vhodné. Móda „všechno do cloudu“ ostatně už na západ od nás ustupuje a firmy opět budují lokální IT.

Jakou roli podle Vás hraje zákaznická podpora ve světě IT?

Zásadní, ale to vám řekne každý. Naším přístupem je zákazníka znát, vědět, co je jeho podnikání, jak podniká, s kým obchoduje. Jen tak můžeme dodat službu kvalitního servisu a podpory. Zakládám si na tom, že máme se zákazníky dlouholeté vztahy, jeho IT známe a pomáháme s jeho rozvojem dlouhodobě.

Co Vás osobně motivuje každý den vést IT firmu?

Zodpovědnost a smysl pro povinnost. Povinnost vůči spolupracovníkům i vůči zákazníkům. Krátce, „duty first“.

Na co jste ve Vaší firmě nejvíc hrdý?

Na svoje spolupracovníky, kteří stojí za úspěchy firmy. Zakládám si na téměř nulové fluktuaci, protože stabilita týmu je zásadním předpokladem úspěchu. Z toho vyplývá druhá oblast, na kterou jsem pyšný, že za námi nezůstal jediný nevyřešený „pomníček“. A že šlo občas o situace, které vypadaly beznadějně.

Máte nějaký konkrétní případ takové vyřešené krize?

Kdybych měl vybrat opravdu velký „průser“, pak je to řešení obnovy systému pro zákazníka, který byl obětí kybernetického útoku. Celá infrastruktura, včetně hypervizorů, a dokonce záloh byla zničena nebo zašifrována. Původní dodavatel služeb odpovědný za správu IT si nevěděl rady. Začali jsme mezi vánočními svátky „na dobré slovo“ a 2.1. byly základní systémy funkční. Na tento případ a jeho řešení jsem opravdu pyšný.

Kdybyste dnes začínal znovu, udělal byste něco jinak?

Nevím, jestli bych vůbec znovu začínal. Ne, vážně, po bitvě je každý generál. Dnes bych měl zkušenosti, které jsem tehdy neměl. Omlouvám se, ale na tohle odpovědět asi neumím.

Práci už jsme probrali, ale jak odpočíváte? Čemu se věnujete, když máte čas?

Celý život mě zajímá historie, konkrétně nejvíce kastelologie, což je nauka o hradech. Takže mne lze potkat na místech, kde je pro laika jen pár kamenů a terénních nerovností. Druhou vášní je střelba a historické zbraně. Snažím se každý pátek uniknout IT na střelnici a urvat si dvě hodiny jen pro sebe. Je to dokonalé vyčištění mysli od práce a dalších starostí.





KONTAKT

TEL: +420 777 325 351

E-MAIL: info@mk-vision.cz

WEB: www.mk-vision.cz



Ilustrační obrázek
Zdroj: MK-VISION

MK-VISION

Když majetek roste, nemůže růst chaos

Jak technologie pomáhají zachovávat pořádek, přehlednost, bezpečnost a růst majetku

V prostředí, kde správci majetku, investoři i rodinné kanceláře operují s milionovými aktivy, je nejcennější komoditou čas – a hned po něm přehled. Mít jasně strukturovaný systém na správu finančních produktů, zejména dluhopisových emisí, je dnes nutností, ne luxusem. Přesto je realita často jiná. Excelové tabulky, ruční výpočty, nejednotná dokumentace, nepřehledná komunikace a díky tomu také vysoké riziko chyb.

Na tento problém reaguje český inovativní systém BondSys, určený pro efektivní správu

dluhopisových emisí, fondů a dalších finančních produktů. BondSys přináší do tohoto segmentu přehlednost, kontrolu, automatizaci – a tím i klid. Ačkoli by se mohlo zdát, že podobné řešení je čistě záležitostí robustních korporací, BondSys efektivně pomáhá i menším emitentům a společnostem, které chtějí spravovat své emise profesionálně a důvěryhodně.

Za systémem BondSys stojí vývojový tým agentury MK-VISION, která se kromě vývojových prací specializuje také na online marketingové služby pro klienty z finančního, právního i technologického sektoru. Právě v rámci dlouhodobé spolupráce s několika emitenty

vzešla potřeba takového systému přímo z praxe. „Opakovaně jsme viděli, jak náročné je držet přehled o všech investorech, splátkách, emisích i související dokumentaci. Prostě řešit, byť i jednu menší emisi v excelovské tabulce, je ‚peklo‘. Chybovost se často stává problémem důvěryhodnosti a to je v oblasti financí naprosto zásadní,“ říká zástupce MK-VISION. „Proto jsme vytvořili nástroj, který je přesný, praktický, bezpečný a velice přehledný.“



Ilustrační obrázek
Zdroj: MK-VISION

Jednoduchost, která skrývá sílu

BondSys funguje jako centrální mozek správy dluhopisů. Umožňuje evidenci emisí, investorů, platebních kalendářů, historii transakcí, generování potřebné dokumentace a obsahuje další spoustu z praxe vyplývajících užitečných funkcí. Vše v intuitivním webovém prostředí, ke kterému mají klienti přístup 24/7 v úrovních podle nastavených oprávnění.

Zásadní roli dnes hraje také bezpečnost. Systém běží na zabezpečených serverech v rámci EU, využívá vícestupňovou autentizaci, pravidelné zálohy a šifrovaný přenos dat. „Víme, že klienti, kteří spravují nebo emitují cenné papíry, kladou extrémní důraz na bezpečnost a diskrétnost.

Proto jsme BondSys stavěli s tímto požadavkem od samého začátku,“ doplňuje tým MK-VISION.

Technologie i důvěra

Jedinečnost BondSysu však nespočívá jen v samotném softwaru. Díky tomu, že ho vyvíjí společnost MK-VISION, která se dlouhodobě věnuje také prémiovému online marketingu, nabízí k systému BondSys rozšířený servis. Klienti tak mohou využít například tvorbu investorských webů, microsites pro konkrétní emise či projekty, emailové notifikace pro investory, nebo kompletní výkonnostní kampaně na podporu prodeje dluhopisů.

„Dnes nestačí mít jen produkt. Je potřeba ho správně prezentovat, vysvětlit a podpořit. Právě v tom je naše výhoda. BondSys není izolovaný nástroj, ale součást celého systému, ve kterém emitenti získají nejen pořádek, ale i profesionální prezentaci a důvěryhodnost,“ říká zástupce MK-VISION.

Otevřenost a budoucnost

BondSys je navržen jako modulární řešení s možností budoucího rozšiřování. Ať už se jedná o propojení na účetní software, clientské portály, nebo datové exporty pro auditory či regulátory. „Plánujeme také vývoj portálu pro investory, kde si každý držitel dluhopisů bude moci bezpečně zobrazit veškeré své údaje, historii transakcí či výplat. Pro větší emitenty chystáme i API integrace,“ dodává vývojový tým. Testujeme také implementace AI nástrojů, například pro prediktivní modely cashflow, hlídání klíčových termínů či automatické generování výkazů. Důraz však zůstává na bezpečnosti a jednoduchosti, aby mohl systém používat jak finanční analytik, tak správce malé emise rodinné firmy.

Proč právě teď

Na českém trhu dluhopisů dnes operují desítky firem, které čelí vyšším regulatorním i reputačním nárokům. Investoři jsou stále náročnější, sledují transparentnost, srozumitelnost i technické zázemí firem. Mít vlastní systém na správu emisí – a schopnost profesionálně komunikovat – je proto jasnou konkurenční výhodou, ale postupem času i nutností.

BondSys představuje řešení, které je rychle nasaditelné, bezpečné, a přitom přizpůsobitelné specifickým požadavkům. Pokud je pro vás důležitý přehled, efektivita a důvěryhodnost, může být právě systém BondSys tím, co vašemu dluhopisovému projektu nebo správě klientského portfolia vrátí klid, čas a systém.



Ilustrační obrázek
Zdroj: MK-VISION





KONTAKT

TEL.: +420 725 432 571

E-MAIL: frantisek.lehanka@mycom.cz

WEB: www.mycom.cz



František Lehanka
Sales Manager

MyCom Solutions

Kyberbezpečnost není otázkou zákonů, ale pudu sebezáchovy

Když vám někdo rozbije okno od auta, voláte policii. Když vám někdo rozbije firemní síť a stáhne zákaznická data, často o tom radši pomlčíte. Proč? Protože kyberútoky jsou neviditelné, nečekané – a pokud se na ně nepřipravíte, mohou firmu zlomit.

V MyCom Solutions s.r.o. máme jasno: kyberbezpečnost není jen compliance nebo odškrtnuté políčko ve směrnici. Je to otázka přežití. Data nejsou jen jedničky a nuly. Jsou to vztahy, důvěra a reputace.

NÚKIB ročně eviduje stovky případů ročně, ale je důležité si přiznat, že se jedná jen o zlomek

případů, které opravdu nastanou. Reálně jde o jednotky tisíc úspěšných kybernetických útoků na firmy každý rok a zároveň se toto číslo rok od roku zvyšuje. Nejedná se tak o zanedbatelné riziko, ale zcela reálnou hrozbu.

Ještě horší pak je propracovanost spojená s důsledky těchto útoků. Pryč jsou doby, kdy vám útočník zašifroval firemní prostředí a doufal, že data se vám nepodaří obnovit ze zálohy. Kybernetické útoky jsou dnes mnohem sofistikovanější, útočníci si dají práci s tím, aby vám znemožnili i přístup k zálohám a ještě vám citlivá data odcizí a budou vás vydírat jejich zveřejněním. V případě úspěšného útoku bude

nutné platit tak jako tak. Náklady na obnovení prostředí, výkupné útočníkům nebo pokuty úřadům...

Zákony vás donutí jednat. Strach vás donutí jednat rychle.

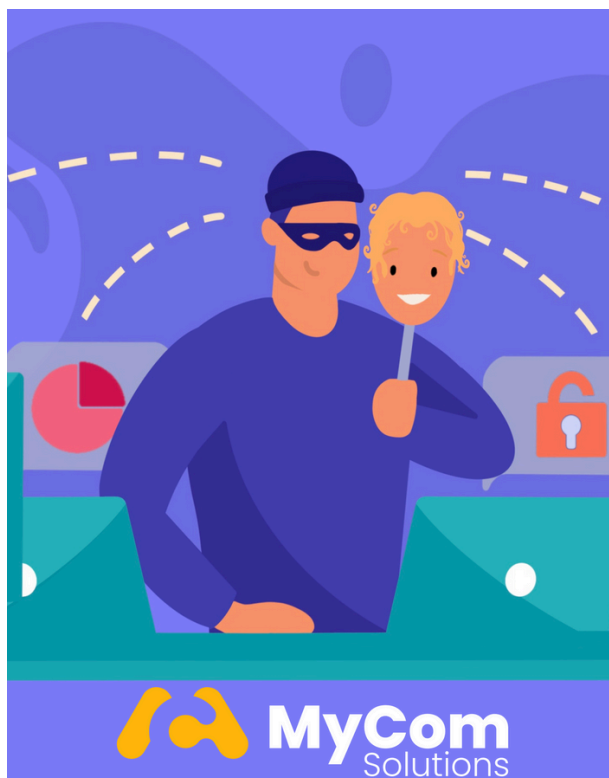
Zákony a směrnice typu NIS2 nebo GDPR jsou důležité. Ale realita je taková, že útočník nečeká, až budete připraveni. Zatímco vy ladíte interní dokumenty, on testuje vaše slabá hesla, otevřené porty a neaktualizované servery. Proto by otázka neměla znít „Musíme něco dělat?“, ale „Chceme přežít?“

Prevence je levnější než výkupné

Zatímco průměrná škoda způsobená ransomwarem se v Evropě pohybuje kolem 80.000 €, dobře nastavená prevence a školení zaměstnanců stojí zlomek.

V MyCom Solutions stavíme bezpečnost na čtyřech pilířích:

- Monitoring 24/7 – protože útočník nečeká na pracovní dobu
- Vzdělávání lidí – protože nejslabším článkem je často lidská chyba
- Reálné testy zranitelnosti – protože simulace je lepší než realita
- Prevence – každá společnost vlastní řadu bezpečnostních technologií, jen je nevyužívá, nebo je využívá špatně



Digitální svět je divoký západ. Nepodceňujte ho.

Mít silné heslo a antivir už dávno nestačí. Kyberzločinci používají umělou inteligenci, phishingové kampaně jsou stále sofistikovanější a vaše firemní data se můžou ocitnout na darknetu dříve, než se stihnete nadechnout. Nepanikařte. Ale jednejte.

Zabezpečte se dřív, než vás někdo „hackne“ k akci.

Jsme MyCom Solutions. Chráníme firmy, data a lidi. Protože kyberbezpečnost není otázkou zákona. Je to otázka pudu sebezáchovy.



WEALTH CLUB PREMIUM

- ✓ Články
- ✓ Video
- ✓ Networking
- ✓ Archiv záznamů
- ✓ Akce

VSTUP NA DVA MEZINÁRODNÍ EVENTY

PŘEDPLATNÉ WEALTH MAGAZÍN - PREMIUM

ZÁZNAMY PŘEDNÁŠEK KONFERENCÍ

REKLAMA V TIŠTĚNÉM ČASOPISE

A DALŠÍ VÝHODY



včetně DPH na 12 měsíců

24.900 Kč



Více informací naleznete na
www.wmag.cz/registrace-do-wealth-clubu-premium



KONTAKT

TEL.: +420 776 199 818

E-MAIL: michal.houdek@vertix.cz

WEB: www.vertix.cz



Ilustrační obrázek
Zdroj: Pixelshot

Vertix

Kyberbezpečnost pro jednotlivce a rodiny s vysokým čistým jméním (HNWI)

V digitálním věku je ochrana vašeho soukromí a majetku nezbytná pro zajištění dlouhodobé bezpečnosti. Pro úspěšné podnikatele a rodiny s vysokým čistým jméním je velmi důležité nejen chránit osobní údaje, ale také citlivé informace a firemní data. V tomto článku se dozvíte, jaké kybernetické hrozby vám mohou hrozit, jak se jim bránit a jak vybrat správného partnera pro kybernetickou ochranu.

1. Kybernetické hrozby, kterým čelíte

Phishing a podvody

Phishing je jedním z nejběžnějších způsobů, jak získat vaše citlivé informace.

Falešné e-maily nebo telefonáty se mohou tvářit jako důvěryhodné žádosti o osobní údaje.

Prevence:

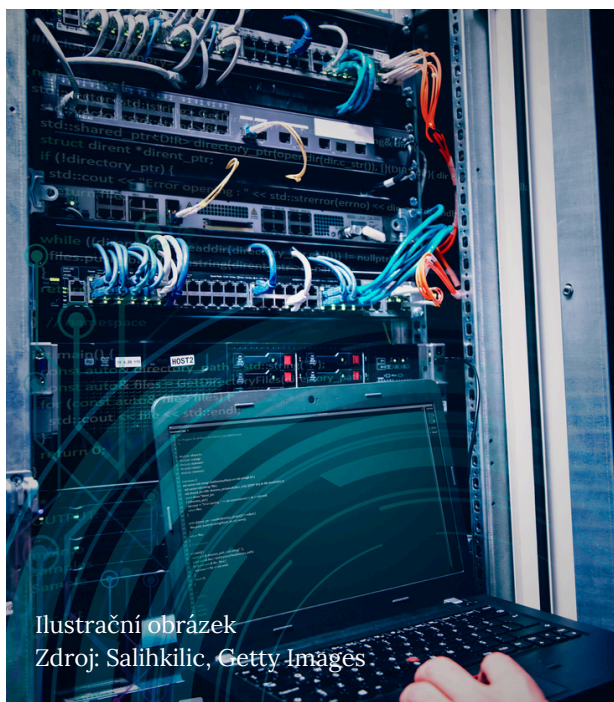
- Školení a obezřetnost: Neotevírejte podezřelé e-maily a neklikejte na neznámé odkazy.
- Dvoufaktorová autentifikace (2FA): Aktivujte 2FA pro důležité účty.

Ransomware

Ransomware šifruje vaše data a požaduje výkupné. Tento útok může mít vážné následky pro vaše osobní i firemní informace.

Prevence:

- Zálhování dat: Pravidelně zálohujte všechna důležitá data.
- XDR nástroje: Nasazení XDR (Extended Detection and Response) poskytuje komplexní ochranu na více úrovních a chrání vaše zařízení proti novým hrozbám. Běžný antivir už dnes nestačí.



Ilustrační obrázek
Zdroj: Salihkilic, Getty Images

Sociální inženýrství a podvody

Útočníci využívají manipulace k získání přístupu k vašim citlivým informacím. Pomocí informací z veřejných profilů mohou například vymyslet falešné žádosti o přístup k firemním nebo osobním údajům.

Prevence:

- Omezte sdílení osobních informací na sociálních sítích a před poskytnutím citlivých údajů vždy ověřte identitu osoby, která je požaduje.

AI a deepfake technologie

Umělá inteligence dnes umožňuje tvorbu falešných videí a telefonátů (deepfake),

kteé mohou být použity k manipulaci s informacemi nebo krádeži identity.

Prevence:

- Ověřujte zdroje: Ujistěte se, že obsah, který dostáváte, je ověřený. Používejte nástroje pro detekci deepfake.
- Ochrana biometrických údajů: Zabezpečte své biometrické údaje, jako jsou otisky prstů nebo rozpoznávání obličeje, které mohou být zneužity.

2. Jak se chránit před kybernetickými hrozbami**Silná hesla a pravidelné aktualizace**

Používejte silná, unikátní hesla pro každý účet. Ideálně využívejte správce hesel, který vám pomůže spravovat složitá hesla a pravidelně je měnit. Nezapomeňte na pravidelnou aktualizaci operačních systémů a aplikací, protože aktualizace často opravují bezpečnostní zranitelnosti.

Firewall a zabezpečení sítě

Firewall je klíčovým nástrojem pro ochranu vaší domácí i firemní sítě. Pomůže vám detekovat a blokovat podezřelý síťový provoz, který by mohl vést k útoku.

Prevence:

- Používejte kvalitní firewall a VPN (virtuální privátní síť) pro šifrování internetového připojení, zejména na veřejných Wi-Fi sítích.

Rizika IoT zařízení

IoT (Internet of Things) zařízení, jako jsou chytré kamery, termostaty, chladničky, žárovky nebo zámky dveří, mohou být snadno zneužita, pokud nejsou správně zabezpečena.

Prevence:

- Aktualizujte IoT zařízení pravidelně a nastavte silná hesla. Umístěte je do samostatné sítě, oddělené od vašeho hlavního zařízení, pro lepší ochranu.

Monitoring a dohled

Pro ochranu vašich zařízení a firemních systémů je klíčový 24/7 monitoring a pravidelné audity.

XDR nástroje umožňují efektivní detekci a reakci na kybernetické hrozby v reálném čase.

Prevence:

- Implementujte XDR pro lepší ochranu a provádějte pravidelné penetrační testy, abyste odhalili zranitelnosti v systémech a sítích.

3. Jak si vybrat správného partnera pro kybernetickou ochranu

Při výběru partnera na kybernetickou ochranu se ujistěte, že má zkušenosti s kybernetickou bezpečností a odpovídající certifikace (např. ISO 27001).

Partner by měl poskytovat pravidelný dohled, audity a reagovat na incidenty 24 hodin denně.

Prevence:

- Pojištění proti kybernetickým útokům může být užitečné pro minimalizaci finančních ztrát při kybernetických útocích.
- Ujistěte se, že poskytovatel má v nabídce pravidelné audity bezpečnosti, které zajistí, že vaše data budou chráněna i proti novým, neznámým hrozbám.

Závěr

Kybernetické hrozby jsou stále sofistikovanější a jejich dopady mohou být devastující. Ochrana vašich dat, financí a soukromí je nezbytná pro zajištění bezpečnosti. Kybernetická bezpečnost by měla být součástí každodenního života a zahrnovat nejen technologická opatření, ale i vzdělávání a prevenci.

Spolupráce s odborníky a nasazení moderních nástrojů vám pomůže zajistit dlouhodobou ochranu vašich osobních a firemních informací.





KONTAKT

TEL: +420 596 912 961

E-MAIL: info@zebra.cz

WEB: www.zebra.cz



Zdeněk Binek
CEO ZEBRA SYSTEMS

ZEBRA SYSTEMS

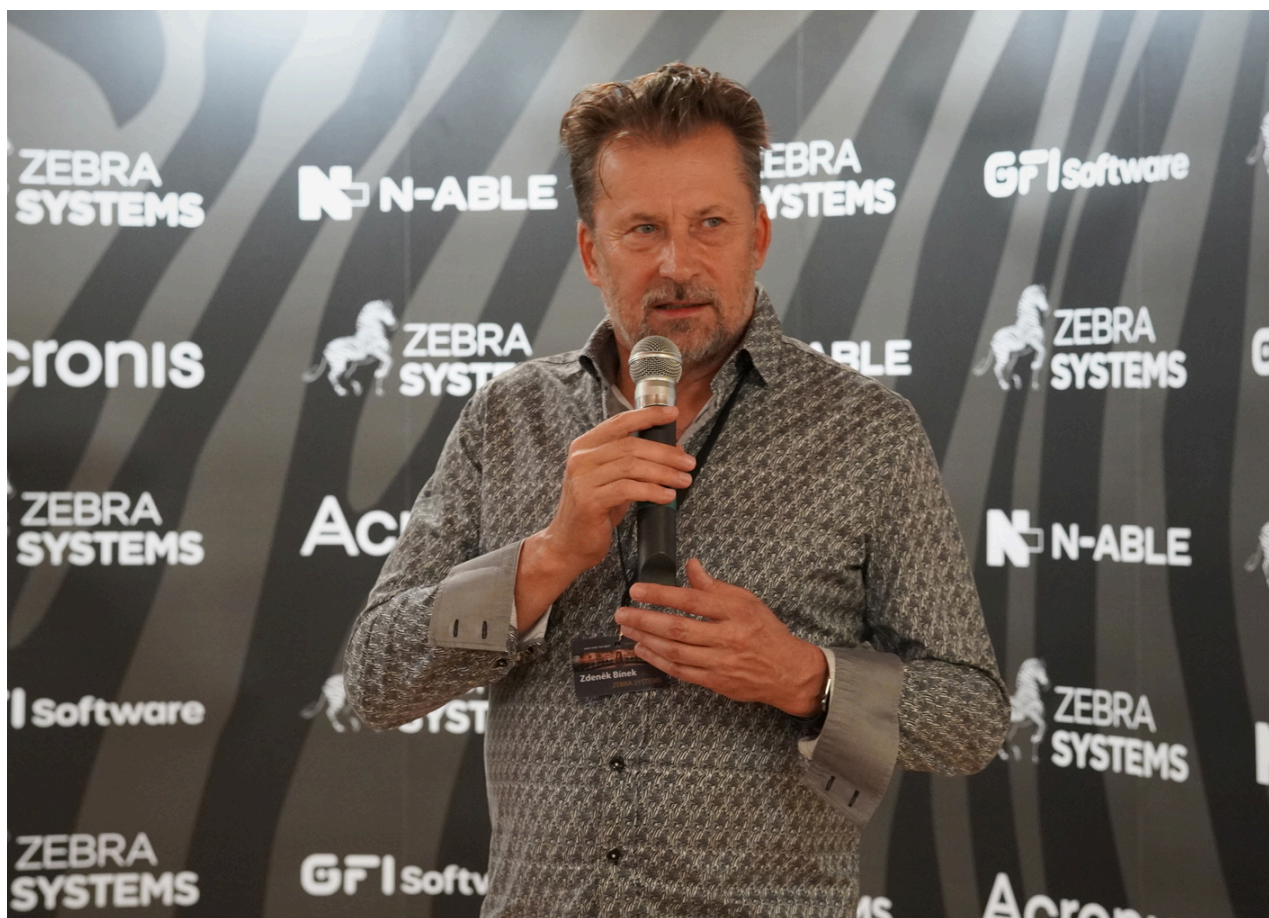
Bezpečné útočiště v kybernetické džungli

Digitální revoluce přinesla firmám a organizacím neuvěřitelné možnosti rozvoje jejich podnikání a zvýšení produktivity. S pozitivy se ale pojí i negativa – digitalizace přináší také nemalá rizika ztráty důležitých dat a hackerských útoků, které při současné závislosti na kybernetických technologiích znamenají hrozby vážných až kritických následků na provoz firmy a její finance. Jednou z nejohroženějších skupin jsou rodinné podniky a SMB firmy. Společnost ZEBRA SYSTEMS, jako jedna z typických rodinných podniků, dobře chápe jejich výzvy a nabízí účinné nástroje k maximálnímu zabezpečení IT systémů v dnešní kybernetické džungli.

Proč vlastně hovoříme o „kybernetické džungli“, když jde o firemní IT technologie?

Podle většiny průzkumů je situace v kybernetickém prostoru čím dál divočejší. Například společnost Acronis letos zjistila ohromující nárůst útoků vedených přes e-maily – o téměř 200 % v porovnání se stejným obdobím roku 2023. Ze všech typů e-mailových útoků je se 74% podílem dominantní phishing – tedy metoda sociálního inženýrství umožňující útočníkům získat přístup do kritických systémů a ke kritickým datům. V březnu pak firma GFI Software varovala, že podle aktuálních údajů z katalogu zjištěných zranitelností CVE bylo

v loňském roce zaznamenáno rekordních 40 297 softwarových zranitelností, tedy o 39 % více než v roce 2023. Pojem „kybernetická džungle“ je podle našeho názoru tím správným popisem toho, co se dnes děje.



Proč jsou ohroženy právě rodinné firmy?

V rodinných firmách, jak už to bývá, se o většinu rolí starají rodinní příslušníci a málokdy si najímají vysoce odborné specialisty. A to platí i pro oblast kybernetické bezpečnosti, protože provozovat IT oddělení se vším potřebným hardwarem, softwarem a sítěmi na korporátní úrovni je časově náročné a velmi nákladné. Malé a střední společnosti (SMB) na to nemají kapacity, jejich systémy mají bezpečnostní mezery a stávají se častým terčem kybernetických útoků. Navíc nemají ani čas na proškolení svých zaměstnanců a u těch je pak větší pravděpodobnost, že podlehnou například phishingovým útokům zmíněným výše.

Jakým způsobem těmto firmám pomáháte se zabezpečením jejich IT systémů?

Pomáháme se zajištěním nejen systémů, ale obchodní kontinuity, protože pokud dnes dojde k výpadku systému, často dojde k zastavení celé firmy. Zabezpečení musí proto obsahovat více vrstev. V první fázi je třeba ochránit data, bez kterých dnes nemůže žádná organizace existovat. Základní obrannou vrstvou je pravidelné zálohování dat, a to ideálně ve 3 kopiích a alespoň s jednou kopií mimo firmu (např. v cloudu). Zde například dodáváme oceňované řešení Acronis pro zálohování a obnovu po havárii.

Druhou vrstvou je zajištění kybernetické bezpečnosti, tj. zabezpečení organizace před kyberútoky. Jedním z nejčastějších způsobů, kterým útočníci pronikají do systémů, jsou zmíněné zranitelnosti. Ty jsou důsledkem stále větší komplexnosti IT infrastruktur a jejich závažnost pak zvyšuje laxnost uživatelů, kteří ignorují instalace potřebných oprav. Zde dodáváme řešení společnosti GFI Software, které umožňuje skenování zranitelností (včetně vzdálených zařízení) a automatizovanou správu záplat (patch management).

Dalším aktuálním příkladem je technologie ochrany koncových bodů (EDR), která v současnosti nahrazuje antiviry díky širším možnostem detekce podezřelé aktivity a podrobné analýzy v reálném čase. Tady nabízíme poskytovatelům služeb řešení od společnosti N-able, kteří je pak formou služby nabízejí koncovým zákazníkům.

Poskytujete svým zákazníkům také školení uživatelů?

Uživatel může být tou nejdůležitější bezpečnostní vrstvou. Pokud ale není proškolen na nejnovější kybertrendy a triky, stává se rizikem – snadno naletí na falešný e-mail a umožní útočníkům překonat i zbývající bezpečnostní vrstvy. Proto od loňského roku nabízíme možnost inovativní metody školení ve virtuální realitě Company (Un)Hacked. Jedná se o technologii umožňující školení ve virtuální realitě formou zážitků a realistických zkušeností, na které uživatel jen tak nezapomene. Je mnohem účinnější než tradiční školení formou prezentací či e-learningu.

Jak vidíte nejbližší budoucnost IT bezpečnosti?

Svět je a bude stále složitější – ten reálný i ten virtuální. Tak jako se chráníme zamčenými dveřmi a zabezpečovacím zařízením, tak i v kybernetickém prostoru se dnes potřebujeme chránit s pomocí vícero bezpečnostních vrstev a opatření. Teprve kombinace vrstev ochrany dat a kybernetické bezpečnosti nám poskytne ucelenou kybernetickou ochranu a minimalizuje rizika v dnešní digitální džungli. Naše společnost ZEBRA SYSTEMS již více než 30 let úspěšně chrání systémy a data stále více zákazníků, aby se mohli nerušeně věnovat svému současnému i budoucímu byznysu s pomocí špičkových a přitom cenově dostupných technologií na trhu.



REJSTŘÍK

SEZNAM OSLOVENÝCH POSKYTOVATELŮ IT A SOFTWAREVÝCH ŘEŠENÍ PRO SPRÁVU BOHATSTVÍ

A

ABAS IPS Management™
ABIS ITS, s.r.o.
Able
Abra Software, a. s.
Ackee
ACMARK s.r.o.
ACREA CR, spol. s r.o.
Actinet Informační systémy s.r.o.
ADC Systems s.r.o.
Administrátoři.cz s.r.o.
Algotech, a.s.
AMBICA s.r.o.
AMComputers s.r.o.
Amenit s.r.o.
Amikon.CZ s.r.o.
ANAFRA s.r.o.
ANASOFT, s.r.o.
Annex NET, s.r.o.
APEX Computer, s.r.o.
Apollo Data s.r.o.
Applifting
AR-NET Services s.r.o.
Arbes Technology
Arion
Arit s.r.o.

A

ASANA
assiX s.r.o.
ASYS IJD, spol. s r.o.
AT Computers a.s.
Atlas Group
ATOMIX technology s.r.o.
Auriga Systems s.r.o.
AWEA s.r.o.
AZ Facility
AZ Solutions, s.r.o.

B

Balcom s.r.o.
BAUER COMPUTER
BDO
BERÁNEK, spol. s r.o.
bezva IT partner s.r.o.
Blue Dynamic
BlueOne
Bohumil Dach
Bohuslav Ludvík - PROLOG
Bondsyst
Bootiq
BORPAS, s.r.o.
BRAIN computers s.r.o.

B

Brandcloud s.r.o.

BRITRES s.r.o.

C

CALL Servis s.r.o.

CALYX, spol. s r.o.

CASNET s.r.o.

CDC Data

Centurion

Certero IT Solutions s.r.o.

Certicon

Cleevio

CNS a.s.

COM Group

COMES, spol. s r.o.

Comimpex

ComIT services s.r.o.

COMP-any ICT s.r.o.

COMPARA systems

Complex technology s.r.o

COMPUTER PARTNER s.r.o.

ComSource

Coolhousing s.r.o.

Corpus Solutions a.s.

Creatiweb

CS21 Nextnet, s.r.o.

CSKA Karviná, spol. s r.o

Ctibor Bujdoš

CTS Trade It

CYBER GLOBAL, s.r.o.

Cyber Rangers s.r.o.

Cybrela

D

Data Force, s.r.o.

DATA-INTER spol. s r.o.

D

Datafest, spol. s r.o.

Digital Resources a.s.

Digitální strážce s.r.o.

Digitalsys s.r.o.

Digitdatarch

Digitree

DLNK s.r.o.

Doktor Online

Dr. Digital

E

e-BAAN Net s.r.o.

eABM s.r.o.

Edgy.Digital

eForum spol. s r.o.

ELO Digital Office ČR s.r.o.

ELSIN spol. s r. o.

ELSO PHILIPS SERVICE, spol. s r.o.

ELZY ConNet s.r.o

EPONA s.r.o.

Etnetera Core

Eviden

EXIRTA s.r.o.

EXPERIA GROUP

exTerra Services s.r.o.

F

Faster CZ spol. s r.o.

eFLEXTRON electronic, s.r.o.

Foxnet s.r.o.

Freelance Developers s.r.o.

G

GAIA Connections, s.r.o.

Geetoo Technology s.r.o.

GNOME.CZ

G

Gordic

H

HCV group a.s.

HERO Computers s.r.o.

Hexatech Technologies

HiTES CE s.r.o.

Hostuj to s.r.o.

CH

Cheops s.r.o.

I

ICT Group

ICT NWT s.r.o.

IDEAL AS

INSIO software s.r.o.

INTIO IT, s.r.o.

INVENTI

iPodnik Cloud

Iquest

ISG9

IT Active s.r.o.

IT AWACS SOLUTION s.r.o.

IT Consulting CZ s.r.o.

IT Prime s.r.o.

IT-Kovář s.r.o.

ITBUSINESS, s.r.o.

ITS Office Technology, s.r.o.

J

JA IT

Jan Hübner

K

K - system. CZ s.r.o.

KAKTUS Software, spol. s r.o.

KETNET s.r.o.

K

Kinet s.r.o.

Koala42

KOPOS technik, spol. s r.o.

Krueck

KSP Computer & Services, s.r.o.

KVTČVŠM spol. s r.o.

KyBez

L

LANETE, spol. s r.o.

LinuxBox.cz, s.r.o.

LITHIUM a.s.

LLP Group

Lukáš Souček

Lupasoft s.r.o.

M

Master DC

MeguMethod

MEMOS

MICROCOMP Plus s.r.o.

MICROWARE (tm), s.r.o.

Mitel

MK-VISION

vMONET+,a.s.

MOROSYSTEM

MyCom Solutions, s.r.o.

N

NanoCom IT Services s.r.o.

Nerit

NetSERV, s.r.o.

NetTech s.r.o.

New Logic

O

OK SOFT

OsPe Consulting s.r.o.

O

OneCore

P

PATRON-IT s.r.o.

Perpsia a.s.

Petr Pilin

Pixelmate

Plus Care

Primelux, s.r.o.

PT Computers s.r.o.

Q

Q – COM, spol. s r.o.

R

RCOMP, s.r.o.

Regfor (Cysensic)

Rexonix s.r.o.

Richard Charvát

Richit Solutions, s.r.o.

RNDr. Adam Kučera

RON Software

RSM CZ a.s.

S

S2 STUDIO, s.r.o.

SCIT s.r.o.

SEFIRA spol. s r.o.

Selecoss

Sestra Emmy

Seyfor

Shift2Cloud

SinguliT s.r.o.

SmartDORLAND, a.s.

SOFTMASTER s.r.o.

Softo s.r.o.

S

SP-IT Limited s.r.o.

SUMA spol. s r.o.

SUNSEC s.r.o.

Svět IT, s.r.o.

System4u a.s.

T

TEXI Dačice s.r.o.

The Cloud Provider s.r.o.

TORAS Marketing s.r.o.

TranSoft a.s.

truconneXion, a.s.

Trusted Network Solutions, a.s.

V

VAHAL, s.r.o.

VERTIX s.r.o.

VOS Health

W

Webfusion

Westercom

Westercom, s.r.o.

WOIT s.r.o.

X

X9.cz s.r.o.

Xevos IT Solutions

Z

Zebra Systems

Zymestic Solutions

OSTATNÍ

lclick

2N

4clouds s.r.o.

WEALTH

magazín

Vydavatel nepřebírá odpovědnost za škodu způsobenou použitím *Wealth Magazín - Report* nebo informací v něm obsažených. Každý investor je povinen provést vlastní analýzu rizik z hlediska právních, daňových a účetních konsekvencí, aniž by se výlučně spoléhal na informace v tomto dokumentu.

Informace uvedené ve *Wealth Magazín - Report* nemohou být považovány za nabídku k nákupu či prodeji jakéhokoliv investičního nástroje, nebo jinou výzvu či pobídkou k jeho nákupu či prodeji. Tento dokument není investičním doporučením dle nařízení Evropského parlamentu a Rady (EU) č. 596/2014, o zneužívání trhu, ani nepředstavuje investiční poradenství dle zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů. Dle zákona č. 240/2013 Sb., o investičních společnostech a investičních fondech se dle §272 tohoto zákona může stát akcionářem fondu kvalifikovaných investorů výhradně kvalifikovaný investor.

www.wmag.cz

Vydavatel Wealth Magazín s.r.o.
Šéfredaktor Eva Ulrichová
Grafika Dana Halušková
Redakce redakce@wmag.cz
Adresa Jindřišská 901/5, Praha 1
Vydání Číslo 12-2/2025



269506850525