ITpedia .. vaše IT encyklopedie

A *AI hallucination*

Když generativní AI vymýšlí věrohodně znějící, ale zcela nepravdivé nebo smyšlené informace – často bez zřejmého důvodu.

Náš tip: Není to chyba ve smyslu výpočtu, ale důsledek predikce pravděpodobných slov. Lidé pak mylně věří, že AI ‚ví'. Ne, jen hádá, co by asi tak mělo následovat.

AI-native

Systém, který má AI jako základní součást architektury – nejen plugin. Využívá AI k rozhodování, personalizaci nebo řízení procesů, nikoliv jen ke kosmetickému vylepšení.

Náš tip: Hodně produktů se tak tváří, ale ve skutečnosti volají OpenAI API a čekají na prompt. AI-native znamená hlubší integraci a schopnost učit se z vlastních dat, kontextu i uživatelů.

B *BaaS*

Backup as a Service – služba, která vám umožní zálohovat data do cloudu bez nutnosti vlastní infrastruktury. Většinou jde o automatizovaný systém záloh s možností rychlého obnovení, správou verzí, šifrováním a geo-redundancí.

Náš tip: BaaS vypadá jednoduše, ale záleží na detailech: frekvence záloh, doba obnovení (RTO), maximální ztráta dat (RPO) a compliance (např. GDPR). Ne každá cloudová záloha je skutečně bezpečná a okamžitě dostupná.

Business continuity

Schopnost organizace udržet klíčové operace během krize nebo výpadku. Zahrnuje plány, procesy, technologie a lidi, kteří umožní chod firmy i za mimořádných okolností.

Náš tip: Nestačí mít jen zálohy – je potřeba vědět, kdo co dělá, jaké jsou alternativy a jak rychle obnovit služby. Krizový plán bez testování je jen složka v šuplíku.

C *CBOM*

Crypthography bill of material – je dokument nebo registr, kde přehledně evidujete veškeré kryptografické algoritmy, klíče a knihovny používané v systémech, aplikacích a produktech – tzv. „materiálový seznam“ vaší firemní kryptografie. Podobně jako SBOM slouží k auditům, migraci na PQC, eliminaci zastaralých algoritmů a k podpoře crypto-agility i v supply chain.

Náš tip: Bez CBOM budete při auditů, incidentů nebo migraci tápat „jak v kabelovém šuplíku“ – zavádějte verze, data expirace, odpovědné osoby a exportujte CBOM ke každému releasu, ať máte kryptografii pod kontrolou.

Cloud repatriation

Strategie, kdy firma přesune systémy nebo data zpět z veřejného cloudu do on-premise prostředí – často kvůli nákladům, výkonu nebo regulacím.

Náš tip: Je to jako rozvod s cloudem. Důvod bývá jednoduchý: přehnané účty za provoz, které nikdo nečekal. Zpět domů, ale s bolestí a refaktoringem.

Cluster

Cluster je soustava propojených počítačů (uzlů), které spolupracují tak, že se navenek chovají jako jeden systém, přičemž plánování a koordinaci úloh zajišťuje software. Používá se ke zvýšení výkonu a dostupnosti nákladově efektivněji než jeden velký stroj a škáluje od malých instalací po superpočítače.

Náš tip: Než stavět cluster, ujasněte si primární cíl (HA, HPC, load-balancing), nároky na síťový propoj a sdílené úložiště a eliminaci single-point-of-failure, protože tyto volby určují architekturu i provozní náklady**.**

CQRC

Kryptograficky (či cryptanalytically) relevantní kvantový počítač – stroj s takovou porcí qubitů a tak nízkou chybovostí, že zvládne lámat dnešní veřejně-klíčové algoritmy (RSA, ECC) „na jedno kliknutí“. Odborníci počítají, že první reálně nasaditelný CQRC dorazí během příští dekády, a proto už dnes musíme šifrovat post-kvantově.

Náš tip: Říkáte si „ještě je čas“? Útočníci už si vaše šifrované e-maily archivují a čekají, až je CQRC přehraje jako staré VHS. S migrací na PQC neotálejte – jinak budete číst vlastní historii v něčích novinách.

Crypto agility

Schopnost rychle a spolehlivě nahradit či upravit kryptografické algoritmy a související parametry bez narušení provozu napříč protokoly, aplikacemi a infrastrukturou. Klíčová vlastnost pro přechody na post-kvantové standardy a zvládnutí budoucích změn v kryptografii i bezpečnostních požadavcích.

Náš tip: Začněte inventurou kryptografie, oddělte algoritmy od byznysové logiky konfiguračně, připravte procesy a automatizaci pro výměny certifikátů a klíčů, a zapojte crypto-agilitu do Zero Trust a síťových kontrol. Pomůže to zvládnout i trend zkracování platnosti certifikátů a omezí riziko výpadků.

D *Data Mesh*

Moderní přístup ke správě dat v organizaci. Místo centralizovaného datového týmu se data rozdělují podle domén – každý tým spravuje „svá data“ jako produkt. Cílem je škálovatelnost a odpovědnost.

Náš tip: Zní krásně, ale bez jasné datové kultury to končí jako zmatek mezi týmy. Data mesh není nástroj – je to způsob myšlení, který vyžaduje i zralost v řízení přístupu, kvality a governance.

DDoS

Distributed Denial of Service – útok, který přetíží tvůj systém/firemní web takovým množstvím požadavků, že přestane fungovat. Typicky z botnetu tisíců zařízení. Cílem je výpadek nebo vydírání.

Náš tip: DDoS už nejsou jen „přestřelky hackerů“ – v dnešní době se s DDoS útoky setkávají větší instituce, oblíbeným cílem bývají úřady a instituce, ale stále častěji míří například na e-shopy nebo SaaS firmy. Mít jen firewall nestačí. Pomůže WAF, CDN a DDoS ochrana od poskytovatele. A hlavně – monitoring.

DevSecOps

Rozšíření konceptu DevOps o bezpečnost – tedy integrace security praktik do vývoje a provozu už od začátku. Zahrnuje automatizované testy, kontrolu závislostí, bezpečnostní scany v CI/CD a posílení odpovědnosti vývojářů za bezpečnost.

Náš tip: DevSecOps není o tom, že „bezpečnost už řeší vývojář“. Je to týmový sport – potřebujete nástroje, kulturu spolupráce a hlavně podporu vedení, jinak to skončí u jednoho checkboxu v pipeline..

E *Edge system*

Edge system označuje výpočetní a úložné zdroje umístěné blízko zdrojů dat a uživatelů, aby se snížila latence a omezily přenosy do centrálního datacentra či cloudu. Často souvisí s IoT a může využívat virtualizaci/kontejnerizaci na lokálních uzlech pro reakce v reálném čase i při omezené konektivitě.

Náš tip: Zajímejte se o požadavky na latenci a propustnost, konektivitu (např. 5G), datovou suverenitu a správu životního cyklu aplikací na edge uzlech, jinak se „edge“ míjí účinkem.

F *FWaaS*

Firewall as a Service (FWaaS) přesouvá funkci firewallu do cloudové služby a umožňuje jednotné řízení bezpečnostních politik bez ohledu na fyzickou lokaci uživatelů nebo aplikací. Tento přístup reflektuje realitu distribuovaných týmů a SaaS aplikací..

Náš tip: FWaaS dává smysl tam, kde je velký podíl vzdálených uživatelù a cloudových aplikací. V čistě on-premise sítích s vysokými nároky na latenci mùže být tradiční firewall stále efektivnější volbou.

H *Hyperautomation*

Propojení technologií jako RPA, AI, chatboty, data mining a další za účelem kompletní automatizace celých podnikových procesů. Nejde jen o jeden krok, ale o celé workflow.

Náš tip: Na papíře vypadá krásně, v realitě to často končí na výjimkách a nedokumentovaných procesech. Pokud nemáš v pořádku data a procesy, hyperautomation tě zmate spíš než spasí.

I *IaC*

Infrastructure as Code. Přístup, kdy infrastruktura (servery, sítě, storage) není nastavována ručně, ale pomocí konfiguračních souborů a skriptů. Pomocí nástrojů jako Terraform, Ansible nebo Pulumi se infrastruktura definuje, verzuje a nasazuje jako běžný kód.

Náš tip: IaC šetří čas a eliminuje „ruční chyby“, ale jen pokud se dodržuje disciplína – verzování, testování a code review. Pokud máte v IaC nepořádek, je to jen digitální obdoba šuplíku s kabely.

IIoT

Industrial Internet of Things - průsečík spolehlivého průmyslového světa (OT) a moderních datových technologií (IT a IoT). Znamená to obohacení fyzických strojů a výrobních linek o chytré senzory a konektivitu, aby bylo možné sbírat detailní telemetrii. Cílem je získat data pro prediktivní údržbu, optimalizaci výkonu a vzdálený monitoring, ideálně bez narušení kritického řízení samotného stroje.

Náš tip: Než začnete olepovat staré výrobní linky drahou elektronikou, vyřešte architekturu – jak bezpečně propasírovat data z přísně izolované OT sítě ven do cloudu (např. přes datové diody). Hlavně ale musíte předem vědět, jakou byznysovou akci na základě těch dat provedete, jinak skončíte s plným úložištěm zbytečných čísel a drahým projektem, který se nikdy nezaplatí.

K *K8s, Kubernetes*

Open-source platforma pro orchestraci kontejnerových aplikací. Umožňuje škálovat, nasazovat, spravovat a automatizovat chod mikroservisních systémů v cloudu i on-premise.

Náš tip: Super výkonný nástroj, ale taky komplexní bestie. Pokud máš tříčlenný tým a používáš K8s, možná přidáváš víc složitosti než užitku. Skvělý sluha, zlý pán.

L *Low-code / No-code*

Platformy umožňující tvorbu aplikací bez nutnosti psaní kódu, pomocí vizuálních nástrojů a předpřipravených komponent. Umožňuje rychlý vývoj byznys aplikací.

Náš tip: Funguje skvěle do první nestandardní logiky. Pak se vývoj zastaví, protože do systému se musí zasáhnout kódem, který už platforma neumí.

M *ML a AI*

Machine Learning (ML) je metoda, kdy počítač hledá vzory v datech, učí se z nich a vylepšuje se bez explicitního programování. Artificial Intelligence (AI) je širší koncept, který zahrnuje ML, ale i pravidlové systémy, NLP, počítačové vidění atd.

Náš tip: Rozdíl je v míře „samostatnosti“: ML je jako učedník – potřebuje data a úlohy. AI je mistr, kterému říkáte, co má dělat. Lidé často zaměňují pojmy, což vede k nerealistickým očekáváním.

N *NIS & NIS2*

NIS – Network and Information Security. NIS2 jako druhá verze evropské směrnice o kybernetické bezpečnosti zavádí přísnější povinnosti pro firmy z kritické infrastruktury, IT dodavatele i digitální služby. Týká se řízení rizik, incident reportingu, i governance bezpečnosti. Zásadní rozdíl mezi NIS a NIS2 tedy spočívá v rozsahu, na který se regulace vztahuje. NIS se zaměřovala primárně na kritickou infrastrukturu, zatímco NIS2 rozšiřuje pravidla na širší spektrum organizací, včetně středních podniků a dalších klíčových subjektů. Lze říci, že NIS2 zavádí vyšší standardy kybernetické bezpečnosti a přísnější sankce.

Náš tip: NIS2 není jen o IT. Vyžaduje zapojení vedení společnosti, právníků i compliance týmu. Připravte se na to, že se vás bude týkat i když si myslíte, že jste „jen dodavatel softwaru“. A pokuty? Ano, jsou tam.

NIST

National Institute of Standards and Technology – americký úřad, který stanovuje metr, vteřinu, i to, jak má vypadat bezpečný algoritmus. V srpnu 2024 vydal první tři finální post-kvantové standardy (FIPS 203–205) a v březnu 2025 přidal záložní šifru HQC, takže všem dodal jasný „jízdní řád“ na éru po CQRC. Více zde.

Náš tip: Nejste si jisti, kterou PQC knihovnu zvolit? Sledujte, co právě doporučuje NIST – ušetříte si kyber-Sophiinu volbu a body u auditorů máte v kapse.

NOC

Network Operations Center zajišťuje dohled nad dostupností a výkonem síťové infrastruktury a IT služeb. Je klíčový pro stabilní provoz a včasné odhalení provozních problémů, které mohou mít přímý dopad na byznys.

Náš tip: NOC má největší přínos pro organizace s nepřetržitým provozem nebo kritickými službami. U menších prostředí bez vysokých nároků na dostupnost může být rozsah NOC služeb zbytečně naddimenzovaný.

O Observability

Observability zahrnuje schopnost porozumět stavu systému pouze na základě výstupů – logů, metrik, tracingu a signálů. Oproti klasickému monitoringu jde o schopnost vidět i to, co nebylo explicitně definováno.

Náš tip: Skvělý buzzword, ale implementace je složitá. Nestačí mít nástroje jako Grafana nebo Prometheus. Potřebujete kulturu, která z nich čte smysluplné závěry a reaguje v reálném čase.

OT

Operational Technology - provozní technologie (OT) označuje hardware a software, který přímo monitoruje a řídí fyzická zařízení, procesy a události v průmyslu či infrastruktuře. Na rozdíl od klasického IT, které spravuje data, OT hýbe fyzickým světem (výrobní linky, elektrárny, vzduchotechnika) a jeho absolutní prioritou je provozní bezpečnost, nepřetržitý chod a reakce v reálném čase.

Náš tip: Počítejte s tím, že OT systémy mívají životnost desítky let a často vůbec nebyly navrženy pro připojení k internetu. Než je začnete integrovat s podnikovým IT světem, zaměřte se na striktní síťovou segmentaci, protože úspěšný kyberútok zde neznamená jen únik dat, ale zastavení výroby nebo fyzické ohrožení.

P *Private cloud*

Privátní cloud kombinuje výhody cloudu (škálovatelnost, samoobslužnost, metriky a billing) s vlastnictvím infrastruktury. Může běžet ve vlastním datacentru nebo být hostován třetí stranou, ale stále je „vaším“ prostředím.

Náš tip: Vendor často tvrdí, že dělá private cloud, i když ve skutečnosti jde o virtualizaci. Důležitým znakem je software-defined přístup – pokud se infrastruktura neřídí automaticky, není to skutečný cloud.

PQC

Post-Quantum Cryptography – kryptografické algoritmy navržené tak, aby odolaly útokům kvantových počítačů. Nejde o hardware, ale o software, který může nahradit dnešní RSA nebo ECC.

Náš tip: Většina firem zatím nepotřebuje okamžitý přechod, ale je dobré sledovat standardizaci NIST. Ptejte se, jaká je kompatibilita s existující infrastrukturou a jaký dopad má nasazení na výkon.

Q *Q-Day*

Q-Day je hypotetický „den D“, kdy kvantové počítače překročí hranici potřebnou pro reálnou kompromitaci běžných veřejných algoritmů (RSA, ECC). Prakticky je to klíčová událost v bezpečnosti a compliance – útočníci archivují dnešní šifrovanou komunikaci, aby ji po Q-Day mohli prolomit; migraci na PQC nestavte na poslední chvíli.

Náš tip: Sledujte NIST roadmapu a počítejte s tím, že „once Q-Day hits, it’s too late“ – plánujte strategii, hybridní migraci, obnovujte klíče, ať Q-Day pro vaši organizaci není startem kyber-křižovatky.

QKD

Quantum Key Distribution – metoda využívající kvantovou fyziku k bezpečnému sdílení šifrovacích klíčů. Pokud někdo odposlouchává, mění vlastnosti částic a komunikující strany to poznají.

Náš tip: Praktické nasazení je omezené na speciální linky a krátké vzdálenosti. Ptejte se, jaké jsou náklady na infrastrukturu a jestli by nestačila klasická, levnější kryptografie.

Quantum as a Service

Cloudový model, kde poskytovatel nabízí přístup ke kvantovým počítačům přes API. Umožňuje experimenty a vývoj algoritmů bez vlastního hardwaru.

Náš tip: Je to spíš sandbox než produkční řešení. Zajímejte se, kolik stojí běh jednou „jobu“, jaké jsou limity qubitů a jestli má projekt reálný přínos, nebo jen vypadá futuristicky.

Quantum ready

Softwarové nebo bezpečnostní řešení, které je připravené na éru kvantových počítačů – např. kvantově odolné šifrování nebo architektura vhodná pro kvantové výpočty.

Náš tip: Realita: většina systémů to nepotřebuje a kvantové počítače pro praktické nasazení zatím neexistují. Výraz slouží hlavně k tomu, aby projekt zněl futuristicky a důležitě.

R Resilience as a Service

Služba, která slibuje zotavení a pokračování provozu po selhání – ať už jde o výpadek serveru, chybu aplikace nebo útok. Většinou jde o kombinaci HA, DR, záloh, testování a orchestrace obnovy.

Náš tip: Když firma slíbí Resilience-as-a-Service, ptejte se: co je součástí? Kolik stojí testy? Je to jen SLA? Kdo odpovídá za návrat k provozu? Mnoho řešení je jen fancy název pro obyčejné disaster recovery.

S SASE

Secure Access Service Edge (SASE) kombinuje síťové a bezpečnostní funkce do jednotného cloudového modelu. Odpovídá na potřebu bezpečného přístupu k aplikacím v prostředí, kde tradiční síťový perimeter ztrácí význam.

Náš tip: SASE je vhodné zejména pro organizace s distribuovanými uživateli a vysokým podílem SaaS aplikací. Pro menší firmy s jednoduchou topologií může být jeho zavedení zbytečně komplexní.

SLA

Service Level Agreement (SLA) definuje měřitelné parametry poskytované služby, zejména dostupnost, dobu reakce a odpovědnosti. V oblasti bezpečnosti představuje důležitý nástroj řízení rizik a očekávání.

Náš tip: SLA by mělo odpovídat reálné kritičnosti služby. Příliš ambiciózní SLA bez odpovídajících procesů a nástrojů často zvyšuje náklady, aniž by přinášelo skutečný bezpečnostní přínos.

SOC

Security Operations Center – 24/7 velín kybernetické bezpečnosti, kde analytici sledují logy, popíjejí kávu a čekají, až SIEM pípne něco podezřelého. Úkolem je incident najít, rozpitvat a zastavit dřív, než se z jiskry stane PR inferno. SOC je klíčový prvek kybernetické bezpečnosti organizace, jehož cílem je chránit organizaci před kybernetickými útoky, zkracovat dobu reakce na incidenty a minimalizovat škody.

Náš tip: SOC nejsou jen drahé obrazovky se zelenými vlnkami. Dejte týmu pravomoc „vytáhnout šňůru ze zdi“, jinak z *Security Operations Center* vznikne „Sorry, Our Company …“.

SECaaS

Security as a Service, neboli bezpečnost jako služba umožňuje organizacím využívat moderní bezpečnostní technologie bez nutnosti jejich provozu ve vlastní infrastruktuře. Model SECaaS je typický pro cloudová a hybridní prostředí, kde je klíčová flexibilita, rychlé nasazení a průběžná aktualizace ochrany.

Náš tip: SECaaS je nejvhodnější pro organizace, které nemají rozsáhlé on-premise prostředí a provozují většinu aplikací v cloudu. Pro silně regulované provozy nebo prostředí s legacy systémy může být nutná kombinace s lokálními bezpečnostními prvky.

Secured by design

Přístup k návrhu systémů, kde je bezpečnost začleněná už od začátku – ne jako dodatečný doplněk. Zahrnuje bezpečný vývoj (secure coding), principy minimálních oprávnění, kontrolu vstupů, segmentaci systémů a ochranu dat už ve fázi návrhu.

Náš tip: Pokud vám někdo tvrdí, že má „secured by design“, ptejte se na threat modeling, code reviews a testování bezpečnostních scénářů. Je rozdíl mezi tím, že je to bezpečné, a tím, že to tak někdo nazval v prezentaci.

State of the Art

State of the Art znamená zavádět a udržet bezpečnostní opatření, která odpovídají aktuální úrovni technologií, hrozeb i oborových best practice – nestačí „mít něco“, musíte prokazatelně držet krok. Pojem je klíčovým standardem v NIS2 i ISO 27001, kde slouží auditorům nebo regulátorům jako laťka pro to, jestli si „kryjete záda“ a umíte obhájit své postupy před kontrolou.

Náš tip: Aktivně sledujte nové hrozby, dokumentujte živý SoA (Statement of Applicability), pravidelně testujte a aktualizujte bezpečnostní opatření – nestačí jednou splnit, musíte průběžně dokazovat, že vaše řešení je stále „state of the art“.

V *Vulnerability scan*

Automatizovaný proces, při kterém nasazený software plošně prohledává sítě, systémy nebo aplikace a porovnává je s databází známých chyb (např. chybějící aktualizace, nezabezpečené porty, špatné konfigurace). Je to jako poslat robota, aby obešel budovu a nahlásil, kde chybí zámek nebo je pootevřené okno.

Náš tip: Než scan u někoho objednáte, ujasněte si, co reálně dodá. Hodí vám na stůl jen vygenerované PDF, nebo vám pomůže s prioritizací a rovnou nabídne i řešení? Zvažte limity vlastního týmu – pokud na lidi vysypete report se stovkou zranitelností, opraví to z nedostatku času jen napůl a přínos bude nulový. Scan má navíc smysl hlavně jako pravidelná aktivita. Jen z porovnání výsledků v čase poznáte, jestli se reálně zlepšujete, nebo jen pravidelně splachujete peníze za reporty, které beztak nemáte kapacitu řešit.

X *XDR*

Extended Detection and Response (XDR) sjednocuje detekci a reakci na hrozby napříč více bezpečnostními doménami. Umožňuje lépe identifikovat komplexní útoky a zkracuje dobu od detekce k reakci.

Náš tip: XDR přináší největší hodnotu tam, kde již existuje více bezpečnostních nástrojů a dostatek dat ke korelaci. Bez navazujících procesů a kvalifikované obsluhy však zůstává jeho potenciál nevyužitý.

Z *Zero Trust*

Bezpečnostní přístup, který říká: nikdy nevěř implicitně žádnému zařízení nebo uživateli – vše musí být ověřeno, autorizováno a sledováno, pokaždé. Funguje napříč sítěmi, uživateli i aplikacemi.

Náš tip: Bez správného identity managementu, síťových segmentací a auditního zázemí je Zero Trust jen slogan. Implementace vyžaduje trpělivost a dobrou integraci technologií.

Zero Trust Architecture

Architektonický přístup postavený na principech Zero Trust – zahrnuje identity, zařízení, sítě, aplikace, data a pravidla přístupu. Vše je řízeno podle důvěryhodnosti a kontextu.

Náš tip: Implementace vyžaduje vícevrstvou koordinaci a řízení přístupu založené na riziku. Bez plánu a integrace s IAM a SIEM nástroji to nebude fungovat.

Vytvořila ITS akciová společnost