

TERMINOLOGIE

(hesla jsou uvedena v abecedním pořádku)

3D tisk (aditivní výroba) je proces tvorby trojrozměrných hmotných objektů na 3D tiskárně. 3D objekty jsou tvořeny zpravidla vrstvou po vrstvě, postupným přidáváním souvislých vrstev materiálu, podle digitální předlohy. 3D tisk se nejčastěji využívá k prototypové výrobě, příp. kusové malosériové výrobě složitějších výrobků nebo k výrobě 3D výrobních nástrojů a nejčastěji se uplatňuje v automobilovém, leteckém a jiném spotřebním průmyslu, dále pak v oblasti vědy, techniky, v lékařství či v architektuře.

3D tiskárna je zařízení, které dokáže podle digitálního počítačového 3D modelu nebo na základě již existující předlohy „vytisknout“ zcela nový trojrozměrný objekt. 3D tiskárna pracuje nejčastěji na principu tavení plastové struny a jejím následném nanášení ve vrstvách.

AI viz heslo **Umělá inteligence**.

Analýza dat je systematický proces sběru, analýzy a interpretace dat, při kterém jsou využívány softwarové nástroje jak pro základní úkony (např. tabulky, průměry, součty, jednoduché grafy v MS Excel), tak pro pokročilejší úkony (využití nástroje Tableau či jiných nástrojů Business Intelligence), databázové technologie, programovací jazyky (např. Python, R, SQL), nebo také nástroje umělé inteligence (např. strojové učení) a je prováděna s cílem získat informace, souvislosti, zlepšit rozhodování, zvýšit efektivitu, lépe porozumět zákazníkům nebo zvýšit ziskovost. Data mohou být pro analyzování získána jak z vlastních, tak z externích zdrojů (např. z účetnictví, od dodavatelů, zákazníků, státní správy).

Bezpečnostní dokumentace v oblasti ICT je sada dokumentů, které definují a popisují bezpečnostní opatření a postupy pro ochranu informačních a komunikačních technologií v organizaci. Bezpečnostní dokumentace typicky obsahuje bezpečnostní politiku firmy (hlavní zásady a cíle kybernetické bezpečnosti), analýzu rizik, plány jak reagovat na incidenty (popis postupů pro řešení kybernetických bezpečnostních incidentů), pravidla pro řízení přístupů k systémům a datům, programy pro vzdělávání zaměstnanců o bezpečnostních postupech, postupy pro zálohování a obnovu kritických dat a opatření pro ochranu fyzických zařízení a infrastruktury.

Blog (firemní blog, mikroblog) jsou internetové stránky, na nichž uživatelé (např. zaměstnanci) zveřejňují chronologicky uspořádané příspěvky v deníkové formě často společně s dalším multimediálním obsahem (obrázky, videi apod.). Tyto příspěvky pak mohou ostatní uživatelé komentovat nebo je dál sdílet. Právo měnit obsah má pouze "majitel" profilu na daném blogu. Sociální síť X (dříve Twitter) je v ČR sice nazýván sociální sítí, pro mezinárodní srovnání se však v tomto šetření považuje za tzv. mikroblog, tedy zmenšenou obdobu webového blogu sloužící k publikování textů omezené délky (např. max 160 znaků).

Business Intelligence (BI) je nástroj, který analyzuje a vizualizuje data, poskytuje strategické informace a slouží pro rozhodování. Nástroje BI sbírají data z různých zdrojů (např. z účetnictví, logistických systémů, z ERP, CRM) a využívají se např. pro řízení výkonnosti firmy. Ukazuje např. kolik firma vydělává, co se prodává nejvíce a jak se daří jednotlivým pobočkám nebo zaměstnancům.

CRM (Customer Relationship Management) je řízení vztahů se zákazníky. Shromažďuje data o zákaznících, např. kontaktní informace, nákupní preference nebo historii objednávek. Kromě toho CRM hlídá termíny, kdy se zákazníkovi ozvat, kdy dosáhne na bonusovou úroveň na slevu a podobně. CRM je často součástí nebo rozšířením ERP systému.

Elektronická fakturace je elektronické předávání účetních dokladů. Rozlišujeme dva typy faktur zasílaných elektronickou cestou: 1/ e-faktury zpracovatelné automatizovanými nástroji zpracování dat (tzv. standardizované faktury), v nichž jsou veškeré údaje v digitálním formátu a mohou být automaticky zpracovány. E-faktura je automaticky přenesena vnitropodnikovou fakturací od výstavce faktury či poskytovatele služeb přímo k příslušnému příjemci faktury nebo do jiných aplikací. Přenosovými formáty takovéto faktury mohou být XML, EDI nebo jiné formáty (v ČR např. formát ISDOC). 2/ elektronické faktury ve formátu neumožňujícím jejich automatické zpracování (nestrukturované faktury). Jedná se

například o faktury zaslané jako text klasickým e-mailem nebo faktury zaslané jako e-mailová příloha např. v PDF formátu.

Elektronická výměna dat (EDI – Electronic Data Interchange) je komunikační technologie založená na bezpapírovém obchodním styku. Jde o elektronickou komunikaci mezi dvěma subjekty, při které dochází k výměně obchodních dokumentů, dokladů (např. elektronických objednávek, faktur, elektronických upozornění na následující dodávky). Přenos dat probíhá výhradně elektronickou formou mezi dvěma počítačovými aplikacemi a je realizován v předem dohodnutém formátu datových zpráv. Datové zprávy mohou být založeny na standardech umožňujících jejich automatické zpracování (EDI, EDIFACT, XML, cXML apod.) nebo na proprietárních formátech, které nejsou standardizovány, ale strany se na nich dohodnou. Přenos datových zpráv je uskutečněn přes internet nebo jiné (privátní) počítačové sítě. Elektronická výměna dat může probíhat také prostřednictvím aplikací dostupných v informačních systémech ERP (Enterprise Resource Planning) nebo SCM (Supply Chain Management).

Elektronický prodej zahrnuje prodej zboží nebo služeb přes:

- a) **vlastní webové stránky firem (např. e-shop)** nebo **mobilní aplikace** určené k prodeji produktů;
- b) **web zprostředkovatele**, tj. na **online tržišti (marketplace)** nebo prostřednictvím **online partnerského prodeje** (nabízení zboží nebo služeb na webu resp. e-shopu velkého internetového prodejce);
- c) **elektronickou výměnou dat (EDI)** mezi informačními systémy dodavatele a odběratele, resp. prodejce a zákazníka.

Způsob placení ani způsob dodání není rozhodující. Zadávání objednávek prostřednictvím ručně psaných e-mailů se nepovažuje za elektronický prodej.

Elektronické sdílení informací s dodavateli či odběrateli **v rámci řízení dodavatelského řetězce** znamená výměnu všech forem elektronických informací s dodavateli a odběrateli (zákazníky). Předávané informace mezi obchodními partnery v celém dodavatelském řetězci slouží plánování a prognózování prodeje, koordinaci dodávek zboží a služeb, plánování a řízení výroby, řízení skladových zásob apod. Elektronická výměna informací může probíhat prostřednictvím internetu či jiných sítí (např. extranetu) nebo elektronické výměny dat (EDI).

ERP (Enterprise Resource Planning) je řízení a plánování podnikových zdrojů. Spadají sem systémy, ve kterých se spravuje např. účetnictví, finance, výroba, skladové hospodářství, logistika, správa majetku, systémy pro řízení lidských zdrojů. ERP tyto systémy integruje do jednoho centrálního systému.

Firemní informační systémy jsou aplikace, které podporují agendy a procesy v oblastech finančního řízení, řízení lidských zdrojů, výroby, skladového hospodářství, obsluhy a vyhledávání zákazníků nebo dodavatelského řetězce. Nejčastěji jde o systémy kategorie ERP, CRM, SCM, WMS, účetní programy a další.

Fixní připojení k internetu je externí připojení k internetu dodávané poskytovatelem v tzv. pevném místě včetně bezdrátového. Způsob dalšího rozvedení či sdílení připojení uvnitř firmy není v tomto šetření zjišťován. Nezahrnuje se zde připojení k internetu realizované prostřednictvím mobilních sítí (datový tarif od mobilních operátorů; mobilní připojení k internetu). Mezi fixní připojení patří především technologie DSL, optické připojení, připojení přes kabelovou televizi, pevné bezdrátové připojení (Wi-Fi) nebo pronajatý datový okruh.

Generativní AI je technologie, která dokáže vytvářet nový textový nebo multimediální obsah na základě zadání nebo vstupních dat (např. psaní článků, e-mailů, vedení konverzace, odpovídání na otázky, vytváření funkční kódů v různých programovacích jazycích, navrhování algoritmů, vytvoření obrázku podle textového popisu, úprava nebo doplnění částí obrázků, vytvoření videa podle textového popisu nebo obrázku, úprava hudební nahrávky nebo složení nové hudby). Patří sem také generování lidské řeči, tj. přirozeně znějícího hlasu.

Chatovací robot (chatbot) je program určený ke komunikaci se zákazníky. Chatboty komunikují na základě databáze s předem naprogramovanými scénáři komunikace, kde naleznou např. odpovědi na

nejčastější otázky zákazníků, tzv. FAQ, nebo komunikují díky využití umělé inteligence a schopnosti porozumění lidské řeči, kdy dokáží v komunikaci s člověkem reagovat na kontext situace.

IT odborníci jsou zaměstnanci, kteří jsou experty na hardware, software a služby v oblasti ICT. Jejich hlavní činností je podílet se na vývoji nových technologií a umožňovat využívání informačních a komunikačních technologií jiným osobám. IT odborníci zahrnují analytiku, vývojáře a programátory softwaru, databází, počítačových, webových a multimediálních aplikací, administrátory, správce počítačových sítí, databází, webu a zaměstnance zajišťující uživatelskou podporu provozu ICT. Zahrnují stálé i dočasné zaměstnance, kteří jsou v pracovním poměru k zaměstnavateli.

Internet věcí (IoT- Internet of Things) je označení pro síť vzájemně propojených fyzických zařízení (např. vozidel, strojů, elektroniky a jiných zařízení) vybavených snímači, senzory, čipy, programy či aplikacemi, pohyblivými částmi a síťovou konektivitou. Propojení těchto zařízení či jejich systémů do sítě jim umožňuje vzájemně spolu komunikovat (shromažďovat a posílat si navzájem data). Tato zařízení jsou často označována jako "chytrá, inteligentní či smart". Pro internet věcí je charakteristické, že "chytrá" zařízení lze vzdáleně přes internet sledovat, kontrolovat a řídit.

Kancelářské programy zahrnují obvykle textový procesor, tabulkový procesor, nástroj na tvorbu prezentací či databázový systém, někdy také grafické editory. Nejznámější je Microsoft Office (Word, Excel, PowerPoint, Access apod.), v poslední době získávají oblibu „open source“ kancelářské softwary, které jsou zcela zdarma (např. LibreOffice, dříve Open Office).

Konfigurace produktu/služby viz heslo **Personalizace (konfigurace) produktu**.

Kybernetická bezpečnost je klíčová pro ochranu osobních údajů, finančních informací a dalších citlivých dat před zneužitím. Jde o souhrn procesů, technologií a opatření, které chrání počítačové systémy, sítě a data před digitálními útoky. Cílem kybernetické bezpečnosti je zajistit důvěrnost (tzn. k informacím či datům mají přístup pouze oprávněné osoby), integritu (neporušenost; aby nebylo možné s daty nepozorovaně manipulovat), pravost, dostupnost informací a systémů. Hlavní oblasti kybernetické bezpečnosti jsou zabezpečení počítačových sítí proti neoprávněnému přístupu a útokům, zajištění bezpečnosti softwarových aplikací před zranitelnostmi, ochrana citlivých informací před krádeží nebo ztrátou, kontrola, kdo má přístup k systémům a datům, řešení a minimalizace dopadů kybernetických útoků, vzdělávání zaměstnanců o bezpečnostních postupech a hrozbách.

Maximální rychlost fixního připojení internetu je smluvně stanovená rychlost stahování dat (download) u fixního internetového připojení. Je udávána v Mbit/s.

Mobilní aplikace jsou vytvořeny speciálně pro malé obrazovky chytrých telefonů, tabletů a dalších mobilních zařízení a programovány tak, aby se daly jednoduše ovládat dotykem. Zahrnují se sem např. aplikace s věrnostním programem, aplikace, ve kterých mohou zákazníci udělat online objednávku nebo prostřednictvím kterých firmy zákazníkům poskytují zákaznickou podporu. Při koupi nového přenosného zařízení jsou již některé aplikace jeho součástí, jiné si může uživatel stáhnout volně nebo za poplatek v obchodech s aplikacemi. Mobilní aplikace jsou vyvíjeny pro konkrétní mobilní operační systémy (Android, iOS).

Mobilní připojení k internetu; připojení přes mobilní síť; internet v mobilu je připojení k internetu, které využívá mobilní síť (např. 3G, 4G, 5G) pro přenos dat. Připojit se uživatel může pomocí mobilního telefonu/ smartphonu nebo tabletu a prostřednictvím datového tarifu od mobilních operátorů. Mobilní operátoři nabízejí různé datové tarify podle objemu přenesených dat. V tomto šetření platí, že pokud firma poskytuje zaměstnancům mobilní připojení, jsou poplatky za internetové připojení nákladem firmy nikoli zaměstnanců (alespoň do výše předem dohodnutého limitu).

Nedostupnost služeb ICT (např. útok typu Denial of Service (DoS, případně DDoS)) je typ kybernetického útoku, při kterém se útočníci snaží narušit nebo poškodit webovou stránku, síť nebo jinou online službu tím, že ji přetíží velkým množstvím falešných nebo nevyžádaných požadavků, dokud nedojde k poklesu výkonu, omezení nebo výpadku služby. Pokud jde o distribuovaný útok (DDoS), je rozložen na větší množství uživatelů.

Online tržiště, také známé jako **marketplace**, je digitální platforma, která umožňuje různým prodejcům nabízet své produkty nebo služby na jednom místě. Na rozdíl od běžného e-shopu, kde prodává jeden

prodejce, zprostředkovává online tržiště prodej mezi mnoha různými prodejci a zákazníky. Patří sem např. platformy jako Booking.com, foodora (dříve damejdro.cz) nebo také partnerský prodej např. přes Mall.cz, Heureka Marketplace, Alza Marketplace nebo Facebook Marketplace.

Partnerský prodej je nabízení zboží nebo služeb na webu resp. e-shopu zavedeného internetového prodejce jako je např. Mall Partner nebo Heureka!shops. Prodejci zde mohou za provizi nabízet své zboží nebo služby. Infrastruktura prodejního portálu zastřešuje propagaci produktů, vyřízení objednávek, platební brány, zákaznický servis a případné reklamace, expedici zboží má zpravidla na starosti partnerský prodejce.

Personalizace (konfigurace) produktu je možnost pro zákazníky přizpůsobit si nabízené zboží/poskytované služby na míru podle jejich požadavků. U výrobků jde např. o volbu složení, výbavy, použitých materiálů, u služeb o volbu jejich rozsahu.

Placená internetová reklama (inzerce) je jeden z nástrojů internetového marketingu využívaná např. k propagaci produktů či značky ve vyhledávacích, sociálních médiích či jinde na internetu. Patří sem např. **kontextová reklama**, která se zobrazí ve výsledcích vyhledávání při hledání určitých slov. Zpravidla se zobrazuje na vyhrazeném místě (např. v podobě textu či grafického obsahu - banneru). Zahrnuje i situace, kdy podniky platí za to, že jejich reklamy jsou přednostně zobrazovány (nahore) ve vyhledávacích, v bannerech sociálních sítí apod. Dále sem patří **personalizovaná reklama**, která odpovídá předchozí internetové aktivitě uživatelů internetu a může přesněji cílit reklamní obsah. „Sledováním“ uživatele jsou získány informace o jeho chování na internetu (webu) pokročilými reklamními systémy (behavioral targeting). Data slouží k vyhodnocení jeho zájmů a potřeb a zobrazování odpovídajícího reklamního obsahu. Personalizovaná reklama zahrnuje také využívání souborů cookies, které slouží k zobrazování reklamního obsahu, který odpovídá předchozí internetové aktivitě uživatelů. Do placené internetové inzerce se řadí také **geolokační reklama**, která využívá geografickou polohu. Zobrazování této reklamy je možné nastavit jen na konkrétní oblast, např. v určité vzdálenosti od provozovny firmy. Pokud na ni uživatel klikne, dozví se podrobnosti, adresu, otevírací dobu apod. Internetová inzerce může probíhat také ve formě **placených reklamních článků**, videí, **placené spolupráce** s YouTube, známými osobnostmi či influencery.

Poskytování ICT zaměstnancům – za poskytnuté zařízení (např. počítač, notebook, tablet, mobilní telefon/smartphone) je v tomto šetření považováno takové, za které firma hradí výdaje s ním spojené tj. veškeré pořizovací výdaje a výdaje související s jeho provozem, např. poplatky poskytovateli za připojení k internetu.

Placené cloudové služby jsou nástroje, programy, servery nebo třeba úložný prostor, které firmy nakupují od poskytovatelů cloudu a tyto služby využívají přes internet. Výhodou cloudových aplikací je, že se nemusí nikde instalovat ani stahovat, k jejich používání stačí pouze webový prohlížeč a jsou přístupné z jakéhokoli zařízení a v jakémkoli místě s přístupem k internetu. Typickými cloudovými službami jsou např. e-mail na vlastní firemní doménu, kancelářské programy, datová úložiště, finanční nebo účetní programy, bezpečnostní SW (např. antivir), databázové systémy nebo výpočetní výkon. Pro cloud computing je charakteristické, že je poskytován prostřednictvím serverů poskytovatelů těchto služeb, služby jsou zpoplatněny, mohou být snadno měněny (např. počet uživatelů, velikost úložného prostoru), poskytovatelé služeb zajišťují aktuálnost softwaru, zabezpečení a funkčnost výpočetních prostředků. Může se jednat také o připojení přes virtuální privátní síť (VPN).

Pokročilá analýza dat (data analytics) zahrnuje metody a techniky, které jdou nad rámec základní analýzy dat (např. průměry, součty, jednoduché grafy) a umožňují porozumět historickým datům, udělat předpověď budoucího vývoje a udělat informované rozhodnutí založené na datech. Pokročilá analýza dat zahrnuje také práci s velkými objemy dat (Big Data), jejichž uchování a zpracování přesahuje možnosti tradičních nástrojů podnikových informačních technologií. K pokročilé analýze dat je využíván speciální software jako např. nástroje umělé inteligence (např. strojové učení, vytěžování textu), statistické modelování (např. SAS, SPSS, R), nástroje Business Intelligence (MS Power BI, Tableau), nástroje pro zpracování Big Data (Apache Spark, Hadoop) nebo programovací jazyky (např. Python, R, SQL).

Pokročilá analýza textu, např. vytěžování textu (Text Mining) pracuje s velkým množstvím existujících textových dat (např. e-mailová korespondence, faktury, smlouvy, technické dokumenty, příspěvky na

sociálních sítích, novinové články) objevuje v nich nové informace a souvislosti. Text Mining se používá např. při monitoringu médií a sociálních sítí, v zákaznickém servisu jako zdroj informací pro chatboty nebo k analýze zákaznických referencí, při zpracování dokumentů k tvorbě rešerší nebo shrnutí dlouhých textů, nebo také jako detekce plagiátů.

Prodej pomocí elektronické výměny dat (EDI) probíhá mezi informačními systémy dodavatele a odběratele (prodejce a zákazníka), často přímo prostřednictvím systémů, jako jsou např. ERP nebo SCM. Dochází při něm k výměně objednávek, rezervací, faktur, dodacích listů apod. Tyto dokumenty mají dohodnutý formát (např. xml), který umožňuje jejich automatizované zpracování. Znamená to např., že vytvořená objednávka se prodejci automaticky přenese do informačního systému a zákazníkovi se po jejím vyřízení data automaticky zapíší do skladového systému.

Prozrazení důvěrných údajů je využívání různých technik manipulace a klamání lidí s cílem získat informace nebo se k nim dostat. **Phishing** je typ kybernetického útoku, při kterém se útočníci snaží získat citlivé informace, jako jsou hesla, čísla kreditních karet nebo přihlašovací údaje, pomocí podvodných zpráv nebo webových stránek. Útočníci často předstírají, že jsou důvěryhodné instituce, jako jsou banky nebo známé webové služby, aby oběti přiměli k odhalení těchto informací. **Pharming** je podvodná technika používaná k získávání citlivých údajů od obětí útoku. Útočník pro pharmingu ovládne identitu nebo webové stránky skutečné osoby/instituce a snaží se v přestrojení vylákat důvěrné informace. Oběti často netuší, že byly přesměrovány na falešné stránky.

Ransomware je typ škodlivého softwaru (malware), který zašifruje data na počítači nebo jiném zařízení oběti a poté požaduje výkupné za jejich odemknutí. Útočníci obvykle hrozí, že data zůstanou trvale nedostupná, pokud oběť nezaplatí požadovanou částku. Ransomware se často šíří prostřednictvím infikovaných e-mailových příloh nebo škodlivých webových stránek.

Robot je stroj/zařízení pracující na principu senzorů (čidel) a snímačů. Je to automaticky řízený, opětovně programovatelný, víceúčelový manipulátor, který může být buď pevně upevněn na místě, nebo je mobilní.

- **Průmyslový robot** je stroj, který má programovatelný řídicí systém a provádí činnosti, které lze měnit na základě programu. Většina průmyslových robotů funguje jako robotické rameno s pevnou základnou. Toto robotické rameno se dokáže pohybovat v prostoru ve 3 a více osách. Průmyslové roboty jsou nejčastěji využívány pro zvýšení výrobní kvality, kapacity a produktivity. V odvětví zpracovatelského průmyslu jde často o robotizované automobilové výrobní linky. Průmyslové roboty jsou dále obvyklé v provozech s velkou sériovostí výroby, často se využívají na manipulační operace (průmyslové manipulátory).
- **Servisní robot** je stroj schopný samostatně vykonávat pohyb v prostoru a samostatně vykonávat pracovní úlohu, včetně rozhodování jak tuto úlohu vykonat (příčemž nejde o výrobní operace). Interpretovat, plánovat a uskutečňovat zadanou úlohu dokáže na základě činnosti svého řídicího systému a senzoriky. Servisní robot by měl být schopen bezpečně spolupracovat s lidmi i s jinými stroji nebo zařízeními. Dále pro něj platí, že dokáže pracovat na zemi, ve vzduchu nebo pod vodou a působí v prostředí, ve kterém je potřeba interagovat s okolím. Firmy je využívají např. ve skladech (robotický skladový systém, robotická paletizace a balení zboží), pro montážní práce, úklid, pro zajištění bezpečnosti (např. provádění ostrahy nebo kontroly budov prostřednictvím dronů, robotická protipožární ochrana), stavební práce či rekonstrukce budov či infrastruktury.

Robotická automatizace procesů (zkratka **RPA**) je technologie AI umožňující automatizovat rutinní úkony. Využívá k tomu softwarové roboty, kteří např. zadávají data do systémů, kopírují data nebo stahují přílohy z e-mailů. Patří sem také tzv. **inteligentní automatizace procesů**, kombinace 1/ robotické automatizace procesů (RPA) a 2/ technologií umělé inteligence. RPA umožňuje automatizovat opakující se úkony jako např. automatické zpracování faktur, třídění e-mailů, automatické odpovědi zákazníkům nebo přepis informací mezi systémy. AI (např. strojové učení) přidává schopnost „porozumět“ datům a na základě nich se rozhodovat.

Rozpoznávání lidské řeči je technologie AI, která převádí mluvenou řeč na text, např. zvukový záznam lidské řeči na text, který lze dále analyzovat nebo zpracovávat. Využívá se např. pro přepis rozhovorů, přednášek, automatické titulky, hlasové ovládání zařízení.

Rozpoznávání osob nebo objektů na základě obrazu - funkce počítačového vidění (rozpoznávání obrazu) se používá např. v účetnictví, logistice (např. automatické zpracování faktur, čtení objednávek a dodacích listů), v elektronickém obchodování (např. vyhledávání produktů podle obrázku), ve výrobě (např. kontrola kvality výrobků pomocí kamer), v bezpečnostních kamerách (např. detekce osob nebo podezřelého chování), ve zdravotnictví (např. analýza rentgenových snímků) nebo v autonomních vozidlech (např. rozpoznávání dopravních značek, chodců, překážek).

SCM (Supply Chain Management) je řízení dodavatelského řetězce. Nástroj SCM využívají zpravidla výrobní firmy. Pracuje s informacemi o skladování a o přesunech materiálů, polotovarů a hotových produktů z místa výroby do místa spotřeby. SCM je často součástí nebo rozšířením ERP systému.

Sociální média viz heslo **Účet na sociálních médiích**.

Strojové učení (Machine Learning) výrazně rozšiřuje možnosti analýzy dat, protože umožňuje modelům učit se z dat, odhalovat souvislosti v datech a na základě historických dat dokáže předpovídat budoucí vývoj. Vstupem pro strojové učení jsou často textová data vytěžená pomocí Text Mining (viz heslo Pokročilá analýza textu). Strojové učení je využíváno např. k detekci podvodných transakcí, k rozpoznávání spamu v e-mailech, k segmentaci zákazníků podle nákupního chování, k odhadu poptávky po konkrétních produktech, k monitorování strojů za účelem prediktivní údržby (předvídání poruch dříve, než nastanou) nebo k personalizaci obsahu nebo produktů na základě uživatelských dat (tzv. doporučovací systémy využívané např. v elektronickém prodeji). **Hluboké učení (Deep Learning)** se používá například při zpracování obrazu, zvuku, textu nebo časových řad.

Škodlivý software (malware) je program, který byl vytvořen s úmyslem vniknout do počítačového systému nebo jej poškodit. Patří sem počítačové viry, červy, Trojské koně.

Umělá inteligence (anglicky Artificial Intelligence, zkratka AI) označuje technologie umožňující strojům vykonávat úkoly, které dříve vyžadovaly lidskou inteligenci. AI se učí, resp. trénuje na velkém množství různých dat. Nejčastěji jde o texty z internetu, z knih, článků, obrázky (např. fotografie, rentgeny), zvuky (např. lidská řeč nebo hudba), videa nebo data z nejrůznějších senzorů. AI technologie existují buď v čistě softwarové podobě nebo jde o systémy integrované do strojů či zařízení, které se díky nim dokáží samostatně pohybovat a rozhodovat. Příklady AI v softwarové podobě:

- jazykové modely, které rozumí lidské řeči a vytvářejí texty či jiný obsah, odpovídají na otázky (tzv. generativní AI, např. ChatGPT, Copilot),
- modely umožňující učit se z dat a dělat předpovědi nebo rozhodnutí (strojové nebo hluboké učení),
- nástroje AI schopné rozpoznat obraz (např. obličeje, objekty nebo dokumenty) založené na technologii počítačového vidění,
- nástroje AI pro rozpoznávání lidské řeči založené na technologii, která převádí mluvenou řeč na text.

Příklady AI systémů integrovaných do strojů či zařízení:

- autonomní roboti používaní ve skladech, v průmyslové výrobě, k úklidovým činnostem apod.,
- autonomní drony používané k mapování terénu - těžko přístupné oblasti, ke sledování postupu výstavby, k hlídání objektů, ke kontrole infrastruktury apod.

Účet na sociálních médiích pro firmu znamená mít zde uživatelský profil/účet a možnost sdílet s ostatními uživateli informace, multimediální obsah, získávat jejich názory nebo například recenze svých produktů. Sociální média jsou online komunikační nástroje, které umožňují jejich uživatelům zakládat vlastní profily (uživatelské účty), jejichž prostřednictvím komunikují s ostatními uživateli, sdílejí s nimi informace či multimediální obsah. Nejznámějším a nejvyužívanějším typem sociálních médií jsou sociální sítě, dále sem patří firemní blogy. Dalším typem sociálních médií jsou webové stránky sdílející multimediální obsah a také webové stránky typu „wiki“. Nejznámějšími aplikacemi sociálních médií používanými podniky jsou u nás Facebook, LinkedIn, Instagram, síť X (dříve Twitter), Therads či YouTube nebo TikTok.

VPN síť znamená Virtual Private Network, česky virtuální privátní síť. VPN zprostředkovává bezpečné propojení zařízení nebo sítí (např. poboček firmy) mezi sebou prostřednictvím veřejné sítě (např. internetu). Umožňuje bezpečnou výměnu dat s šifrovaným přenosem.

Vzdálený přístup je možnost využívání pracovního e-mailu, firemních aplikací, dokumentů či souborů pro uživatele (zaměstnance) nacházející se mimo prostory firmy, obvykle formou zabezpečeného připojení prostřednictvím internetu.

Webové stránky prezentují firmu na internetu. Jejich obsah je pod kontrolou firmy (obsah uveřejněný na webových stránkách může oprávněná osoba měnit, upravovat). Za webové stránky firmy považujeme i stránky společné s jiným právním subjektem (např. webové stránky mateřské společnosti), pokud zde firma může alespoň částečně měnit/aktualizovat jejich obsah. Nepatří sem informace o subjektu zveřejněné pouze v internetových databázích firem (tzv. katalogy firem).