POUŽITÁ TERMINOLOGIE

3D tisk (aditivní výroba) je proces tvorby trojrozměrných hmotných objektů na 3D tiskárně. 3D objekty jsou tvořeny zpravidla vrstvu po vrstvě, postupným přidáváním souvislých vrstev materiálu (nejčastěji jde o termoplasty, kovy či pryskyřice), 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.

Bezpečnost ICT je souhrn opatření, kontrol a postupů používaných v systémech informačních a komunikačních technologií (ICT) s cílem zajistit integritu (neporušenost; aby nebylo možné s daty nepozorovaně manipulovat), pravost, dostupnost a důvěrnost údajů a systémů (tzn. k informacím či datům mají přístup pouze oprávněné osoby). Bezpečnost ICT zahrnuje např. také vývoj ochranného softwaru pro firmu (antivir, antispam, firewall) či analyzování bezpečnostních narušení a rizik nebo řešení bezpečnostních problémů.

Bezpečnostní dokumentace je obvykle sada dokumentů definujících opatření, postupy a procedury týkající se bezpečnosti ICT a ochrany důvěrných dat. Bezpečnostní dokumentace obvykle zahrnuje informace o způsobech a periodicitě školení zaměstnanců ohledně jejich povinností souvisejících s bezpečným používáním ICT, o bezpečnostních opatřeních v oblasti ICT, o hodnocení bezpečnostních opatření v ICT, jsou zde plány na aktualizaci bezpečnostních dokumentů ICT apod.

Elektronická objednávka je objednávka, odvolávka či jiná žádost o dodání zboží či poskytnutí služby, která obsahuje náležitosti nezbytné k realizaci obchodu (kupní smlouvy apod.) dle všeobecných či sjednaných obchodních podmínek a splňuje podmínky pro elektronické obchodování. Pro elektronické obchodování je rozhodující právě elektronické zadání nebo přijetí objednávek.

Elektronická výměna dat (EDI – Electronic Data Interchange) představuje komunikační technologii založenou na bezpapírovém obchodním styku. Je to elektronická komunikace 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).

Elektronické obchodování je nákup nebo prodej (objednávání nebo přijímání objednávek) přes internet nebo počítačovou síť (např. uzavřenou mezipodnikovou síť). Pro elektronické obchodování je rozhodující, že objednávka je uskutečněna (přijata nebo odeslána) elektronickou cestou. Rozhodující naopak není způsob placení ani způsob uskutečnění dodávky. Nezahrnují se nákupy (prodeje) realizované na základě objednávek, které byly připraveny z informací získaných na internetu, ale podány klasickou cestou (osobně, telefonicky, písemnou objednávkou) nebo prostřednictvím e-mailu. Elektronické obchodování může obíhat na webových stránkách či mobilních aplikacích elektronického obchodu (**web e-commerce**). Objednávka je vyplněna a odeslána přes internetové stránky e-shopu, přes on-line tržiště (e-marketplace), přes mobilní aplikace nebo přes extranet. Druhý způsob e-obchodování je prostřednictvím elektronické výměny dat (**EDI commerce**) při které dochází k výměně obchodních dokumentů (např. elektronických objednávek) mezi partnery elektronického obchodu.

IT odborníci jsou zaměstnanci, kteří jsou experty na hardware, software a služby v oblasti ICT, jejichž hlavní činností je podílet se na vývoji nových technologií a umožňovat využívání informačních a komunikačních technologií jiným osobám. IT odborníci zahrnují: analytiky, 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.

Konfigurace produktu/služby je možnost pro zákazníky navolit či přizpůsobit si standardně nabízené zboží či služby na míru podle jejich přání či požadavků. Např. volba složení, použitých materiálů, atd.

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).

Nedostupnost služeb ICT (např. útok typu Denial of Service (DoS, případně DDoS)) je typ útoku na počítač nebo síť, kdy server, na který je útok prováděn, po čase odmítne poskytovat své služby. Navenek se to projeví jednoduše tak, že na server se nemůžete dostat. DoS útok může provádět jeden uživatel, nebo může útok provádět více lidí současně, protože víc lidí snáze vytvoří zátěž, aniž by jakýkoli z nich potřeboval disponovat kapacitou nutnou k úspěšnému provedení útoku – to je právě případ Distributed Denial of Service. Pokud jde o distribuovaný útok, je rozložený na větší množství uživatelů.

Online tržiště (elektronické tržiště; marketlapce; e-marketplace) je webová stránka, na které prodejci mohou za domluvenou provizi nabízet své zboží nebo služby. Propagaci zboží nebo služeb, platební brány a zákaznický servis zastřešuje infrastruktura zavedeného prodejního portálu. Patří sem např. platformy jako Booking.com, damejidlo.cz, košík.cz, rohlík.cz nebo také partnerský prodej např. přes Mall.cz, Heureka Marketplace, Alza Marketplace nebo Facebook Marketplace.

Pevné připojení k internetu (Fixní broadband) 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). Patří sem hlavně technologie DSL, připojení přes kabelovou televizi, pevné bezdrátové připojení (Wi-Fi), pronajatý datový okruh atd.

Prozrazení důvěrných údajů je využívání různých technik manipulace a klamání lidí s cílem získat informace nebo se k nim dostat. **Phishing:** útočník se snaží vylákat důvěrné informace (např. heslo, PIN) prostřednictvím falešné identity – vydává se za banku, úřad, jinou firmu apod. **Pharming:** útočník ovládne identitu nebo webové stránky skutečné osoby/instituce a snaží se v přestrojení vylákat důvěrné informace.

Připojení přes mobilní sítě; internet v mobilu je připojení k internetu prostřednictvím datového tarifu od mobilních operátorů. Přístup na internet probíhá přes mobilní telefonní síť nejčastěji prostřednictvím datové SIM karty vložené do mobilního telefonu/smartphonu, příp. tabletu. Objem přenášených dat odpovídá sjednanému datovému tarifu. 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).

Ransomware je typ bezpečnostního útoku, který cílí na nedostupnost dat nebo celého systému (blokuje počítačový systém nebo šifruje data v něm zapsaná), a pak požaduje od oběti výkupné za obnovení přístupu.

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 (přičemž 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.

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

VPN síť (Virtual Private Network, česky **virtuální privátní síť**) zprostředkovává bezpečné propojení zařízení nebo sítí (např. poboček firmy) mezi sebou prostřednictvím 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 firmy 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).