Terminologie

(hesla jsou uvedena v abecedním pořádku)

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).

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 (e-commerce) 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 (resp. vytvoření a odeslání objednávky) může probíhat **na webových stránkách** (např. přes e-shop, přes extranet firmy; **web commerce**), přes mobilní aplikace nebo přes tzv. online tržiště (marketplaces). Druhý způsob e-obchodování je prostřednictvím **elektronické výměny dat** (**EDI commerce**). Jde o prodej, který probíhá mezi informačními systémy dodavatele a odběratele (prodejce a zákazníka), často přímo prostřednictvím systémů, jako jsou např. ERP nebo SCM. Při EDI dochází k výměně elektronických obchodních dokumentů (objednávek, rezervací, faktur, dodacích listů apod.), které mají dohodnutý formát (např. xml) umožňující jejich automatizované zpracování. Vytvořená objednávka se prodejci automaticky přenese do informačního systému, zákazníkovi se po jejím vyřízení data automaticky zapíší do skladového systému. Prodejce také v informačním systému vystavuje fakturu, která se přes EDI vyřizuje. Cílem je zjednodušit a automatizovat obchodní proces firem.

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.

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 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.

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 udávaná 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 sítě; internet v mobilu je připojení k internetu, které využívá mobilní sítě (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 rozložený 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 damejidlo.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 objednávky, platební brány, zákaznický servis a případné reklamace, expedici zboží má zpravidla na starosti partnerský prodejce.

Placená internetová reklama (inzerce) je jeden z nástrojů internetového marketingu využívaná např. k propagaci produktů či značky ve vyhledávačích, 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 (nahoře) ve vyhledávačích, 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 YouTubery, známými osobnostmi čili 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.

Pokročilá analýza textu (Text Mining), tzv. vytěžování textu nebo dobývání znalostí z textových dat. Jde o techniku práce s velkým množstvím dat pocházejícím z různých zdrojů (např. e-mailová korespondence, příspěvky ze sociálních sítí, recenze produktů, stížnosti zákazníků, novinové články, smlouvy, technické dokumenty a další). Výstupem je strukturovaný formát (báze znalostí), který umožňuje hlubší analýzu a pomáhá objevovat nové informace a vzory v textových datech.

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.

Robotická automatizace procesů (RPA) je využívání softwarových robotů k provádění úkolů, které se velmi často opakují a jsou náchylné k chybám. Patří sem také inteligentní automatizace procesů (IPA), což je pokročilejší technologie integrující umělou inteligenci a strojové učení k analýze dat, učení se z nich a informovanému rozhodování. Úkony, které mohou být vyřešeny díky RPA nebo IPA: automatické zpracování faktur, generování sestav, automatické odpovědi zákazníkům, přepis informací mezi systémy.

Rozpoznávání osob nebo objektů na základě obrazu umožňuje počítačům identifikovat nebo rozpoznat vzory nebo objekty v digitálních obrázcích. Díky tomu mají počítače schopnost identifikovat např. objekty, osoby nebo místa např. na fotografiích. Funkce rozpoznávání obrazu se používá např. v autonomních vozidlech nebo v bezpečnostních kamerách.

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

Strojové učení (Machine Learning) je podoblastí umělé inteligence a zabývá se algoritmy a technikami, které umožňují počítačovým systémům 'učit se'. Na základě naučených faktů a znalostí umí počítače vytvářet vlastní nové myšlenky a nápady a mezi daty nacházet vazby a souvislosti. **Hluboké učení (Deep Machine Learning)** učí počítače 'učit se' ze zkušeností, tj. např. 'pochopit' význam zkoumaného textového nebo zvukového dokumentu, rozpoznávání obličejů.

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) jsou stroje, programy a systémy vytvořené za účelem efektivního provádění úkolů a usnadnění lidské práce. Umělá inteligence umožňuje strojům reagovat na vnější podněty, samostatně se rozhodovat, řešit problémy a má potenciál se dále učit. Využívá se například ke zjednodušení administrativy a komunikace, ke zlepšení produktů i celých výrobních procesů, k předpovídání vývoje událostí nebo k podpoře strategického rozhodování při řízení firmy. Systémy umělé inteligence mohou být založeny čistě na softwaru (např. chatboty, strojové překlady, systémy pro rozpoznávání obličejů nebo lidské řeči, systémy, které generují obsah - tj. texty, obrázky, grafiku, zvuky nebo videa) nebo mohou být součástí strojů, zabudované v zařízeních (např. autonomní vozidla, roboti nebo drony).

Účet na sociálních médiích pro firmu znamená mít zde uživatelský profil 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 či

mikroblogy. Dalším typem sociálních médií jsou webové stránky sdílející multimediální obsah a také webové stránky typu „wiki“. Nejznámějšími aplikacemi sociálních médií používaných podniky jsou u nás Facebook, LinkedIn, Instagram, sociální síť X (dříve Twitter), či YouTube.

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).