MASARYKOVA UNIVERZITA

Provozování integrovaného podnikového systému

Jaroslav Šmarda

Provozování IPS

- Implementace IS
- Formy využívání aplikací
- Software jako služba
- Zabezpečení IS
- Spolehlivost IS
- Servisně orientovaná architektura IS

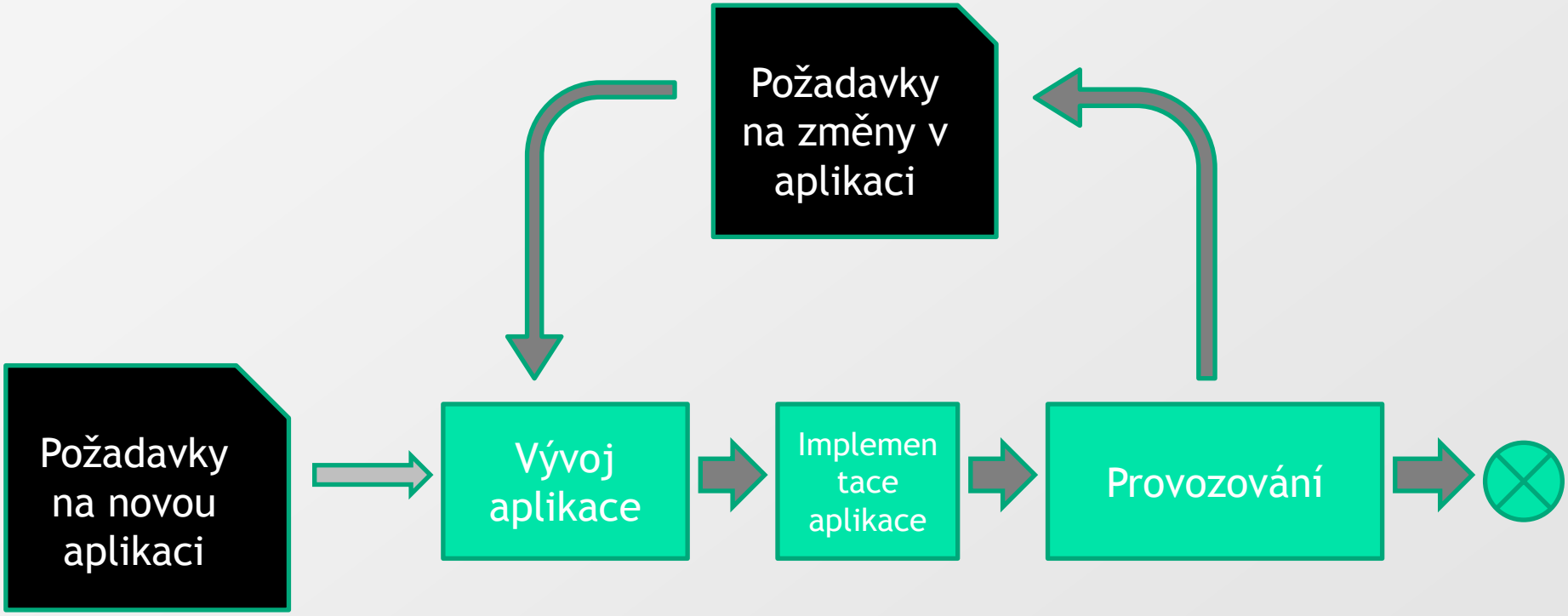
Implementace aplikace IPS

- Implementace je:
  - proces instalace nové aplikační komponenty do existujícího systému provozovaného v organizaci,
  - provedení všech požadovaných datových konverzí z jiných systémů a
  - převedení uživatelů do této aplikace

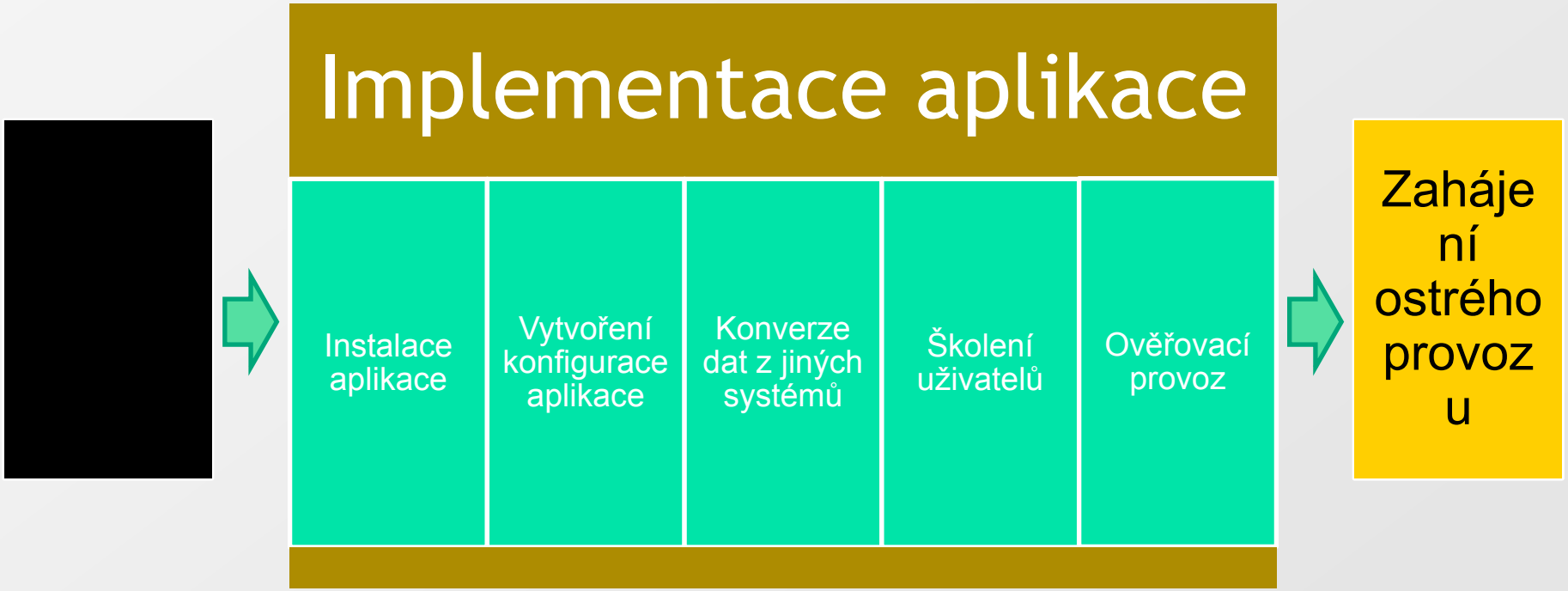
Dvě varianty implementace

- Velký třesk (cold turkey)
  - najednou v celé organizaci
- Postupná implementace (chicken method)
  - nejprve v jedné části organizace (organizačním útvaru)
  - teprve potom v dalších částech

Proces využívání aplikace



Implementace aplikace



Instalace aplikace

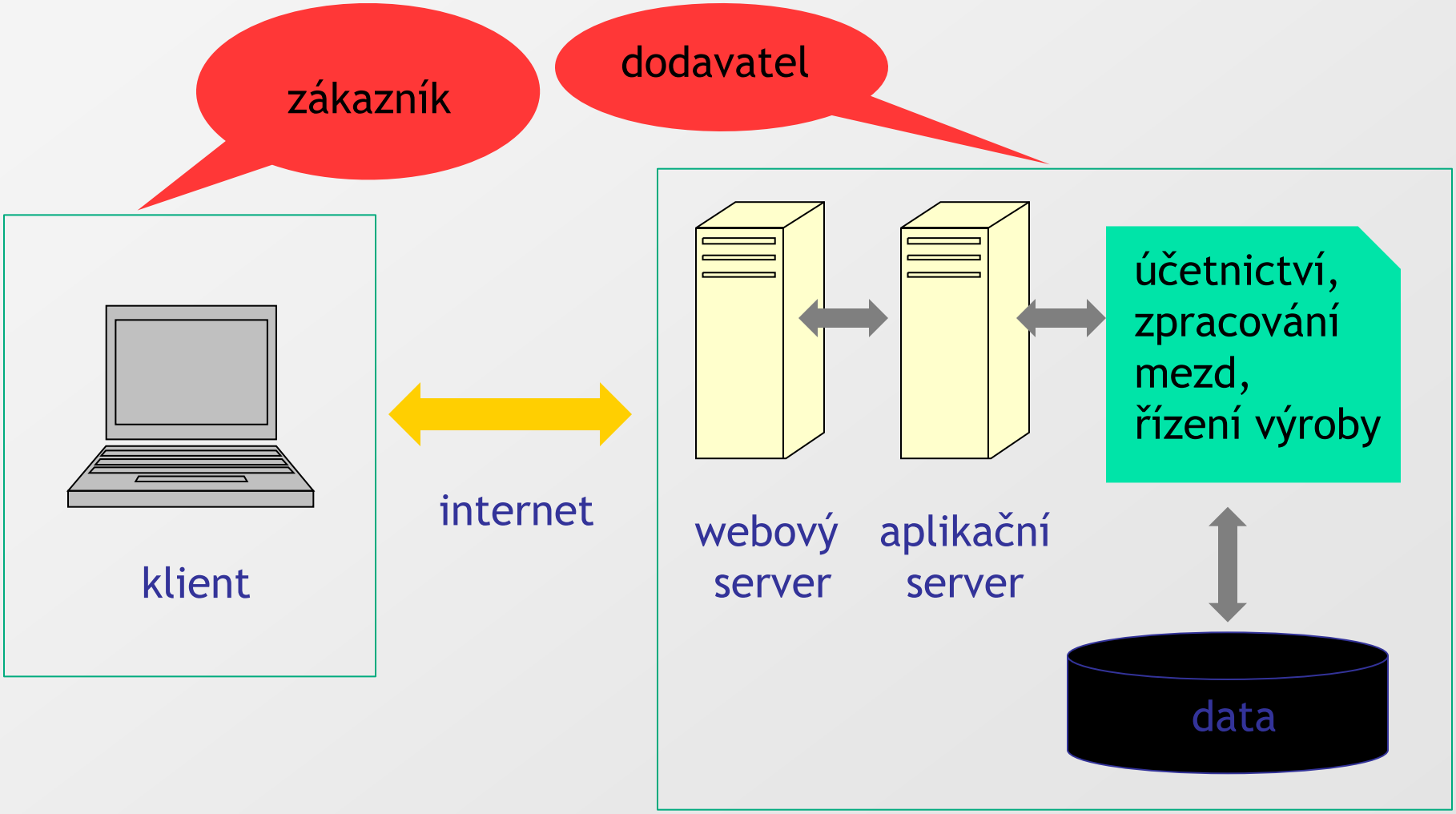
- Aplikace ve formě instalačního balíčku
  - .MSI pro Windows .DMG pro Mac OS X, .tar pro UNIX
- Instalace IS
  - na HW serveru (označujeme jako aplikační server)
  - někdy na stanicích, ale tam obvykle tenký klient - internetový prohlížeč

Vytvoření konfigurace aplikace

- Na začátku databáze prázdná nebo s předdefinovaným obsahem
- Nastavení konfiguračních entit
  - Konfigurační entity v databázi zpravidla definují organizaci
  - Konfigurační entity:
    - Struktura organizace
    - Seznam uživatelů
    - Účetnictví - tabulka bankovních účtů organizace, tabulka nákladových, výnosových, rozvahových účtů,…
- Konfigurace se během provozování **mění jen výjimečně**

Formy využívání aplikací

- Nákup licenčních práv k využívání aplikací
  - nákup a pak nákup nové verze za zvýhodněnou cenu
  - nákup a pak roční platba za využívání
  - instalace aplikace na serveru zákazníka
- Software formou služby (SaaS – Software as a Service)
  - pravidelná platba (měsíční, čtvrtletní) za službu
  - Instalace aplikace u dodavatele
  - SaaS jinak:
    - SW On Demand
    - ASP (Application Service Providing)


zákazník
dodavatel
klient
internet
webový server
aplikační server
účetnictví, zpracování mezd, řízení výroby
data

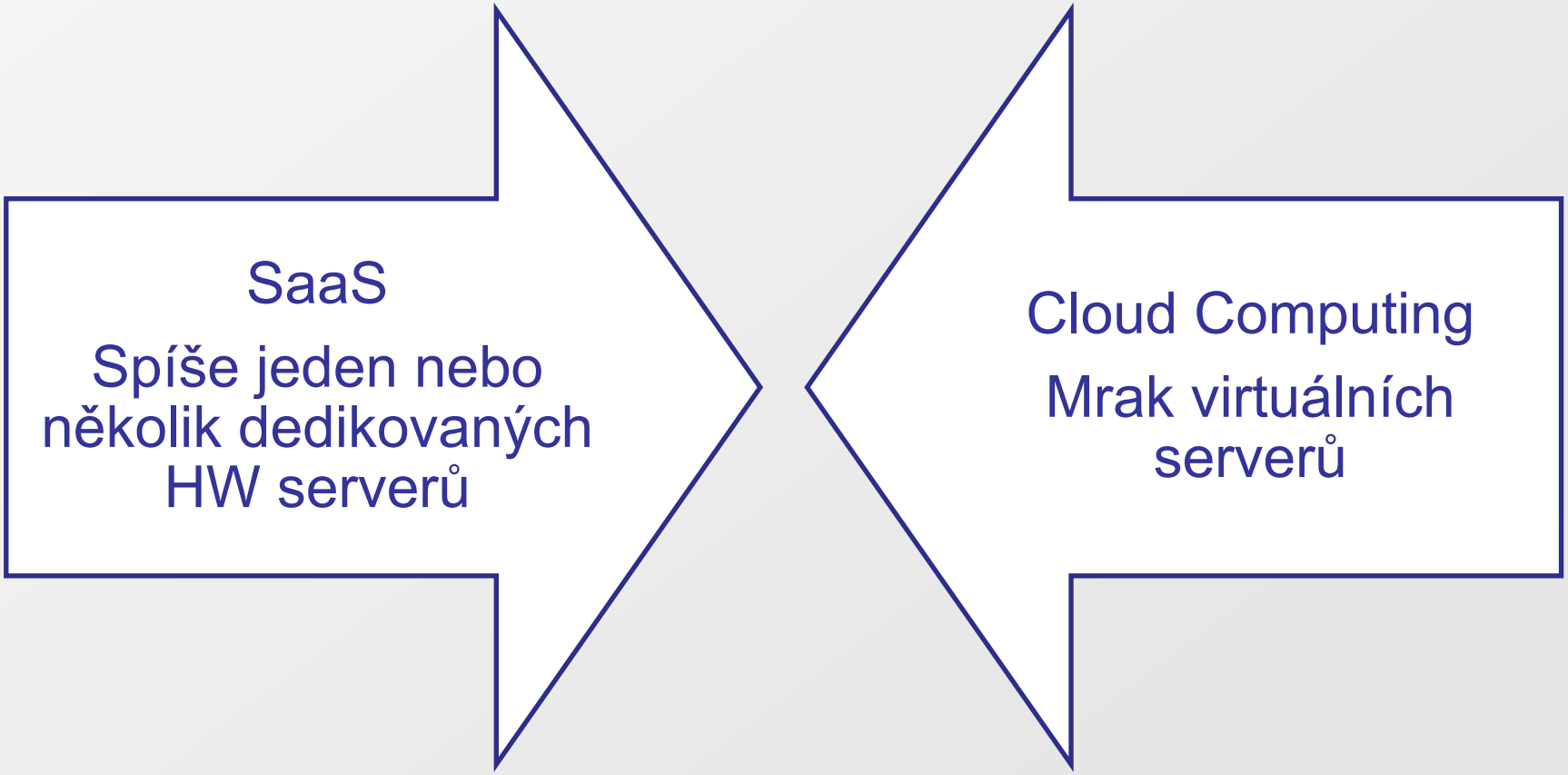
Výhody provozování aplikací formou SaaS

- Zákazník:
  - nepotřebuje HW server + OS + správce serveru
  - neinstaluje aplikační server
  - nestará se o archivace dat
  - nestará se o zabezpečení dat
  - využívá zabezpečený přístup přes internet (např. USB certifikáty)
  - služba na základě smlouvy (SLA Service Level Agreement)
- O toto všechno se stará dodavatel

SaaS a další podobné pojmy

- SW On Demand
- ASP (Application Service Providing)
- Cloud Computing

SaaS vs. Cloud Computing



Cloud Computing

- Datová centra – mraky serverů
- Multitenancy - více nájmů
  - Jedna instalace aplikace pro všechny zákazníky
- Škálovatelnost a elasticita
- Pay as you go
  - Kolik uživatel spotřebuje, tolik zaplatí
- Aktualizovatelnost (Up-to-date)
  - všechen software je automaticky aktualizovaný
- Přístup prostřednictvím internetového prohlížeče

Zabezpečení IS – základní principy bezpečnosti IS

- IS musí být chráněny tak:
  - aby k nim měly přístup pouze oprávněné osoby
  - aby se zpracovávaly nefalšované informace
  - aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
  - aby nebyly nekontrolovaným způsobem vyzrazeny
  - aby byly dostupné tehdy, když jsou potřebné

Narušení bezpečnosti IS lze provést například

- narušením soukromí či utajení informací
- vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií
- neoprávněným zvýšením svých privilegií přístupu k informacím
- modifikací privilegií ostatních osob
- zařazením se jako skrytý mezičlánek v konverzaci jiných subjektů
- pokažením funkcionality softwaru doplněním skrytých funkcí

Základní pojmy bezpečnosti IS

- Pojmem **autorizace** subjektu pro jistou činnost rozumíme určení,
  - že daný subjekt (aktivní entita - nejčastěji uživatel) je z hlediska této činnosti důvěryhodný. Udělení autorizace subjektu si vynucuje, aby se pracovalo s autentickými subjekty.
- **Autentizací** se rozumí
  - proces ověřování pravosti identity entity (subjektu, objektu, tj. uživatele, procesu, systémů, informačních struktur apod.).
- **Důvěryhodný IS** (subjekt nebo objekt) je
  - taková entita, o které se věří (je o tom podán důkaz), že je implementovaná tak, že splňuje svoji specifikaci vypracovanou v souladu s bezpečnostní politikou. Na důvěryhodnou entitu se můžeme spolehnout, chová-li se tak, jak očekáváme,že se bude chovat.

Zranitelné místo

- Slabinu IS využitelnou ke způsobení škod nebo ztrát útokem na IS nazýváme zranitelné místo.
- Podstata zranitelného místa může být:
  - fyzická (např. umístění IS v místě, které je snadno dostupné sabotáži a/nebo vandalismu, výpadek napětí)
  - přírodní (objektivní faktory typu záplava, požár, zemětřesení, blesk)
  - v hardwaru nebo v softwaru
  - fyzikální (vyzařování, útoky při komunikaci na výměnu zprávy, na spoje)
  - v lidském faktoru (největší zranitelnost ze všech možných variant)

Hrozba

- Zranitelná místa jsou vlastnostmi (součástmi) IS, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se IS provozuje, představují pro něj hrozby
- Pojmem **hrozba** označujeme možnost využít zranitelné místo IS k útoku na něj

Kategorizace hrozeb

- Objektivní
  - přírodní, fyzické (požár, povodeň, výpadek napětí, poruchy..., u kterých je prevence obtížná a u kterých je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy
  - fyzikální (např. elektromagnetické vyzařování)
  - technické nebo logické (porucha paměti, softwarová „zadní vrátka“, špatné propojení jinak bezpečných komponent, krádež, resp. zničení paměťového média, nebo nedokonalé zrušení informace na něm)
- Subjektivní (plynoucí z lidského faktoru)
  - neúmyslné (např. působení neškoleného uživatele / správce)
  - úmyslné (vnější útočníci (špioni, teroristi, kriminální živly, konkurenti, hackeři) i vnitřní útočníci (odhaduje se, že 80 % útoků na IT je vedeno zevnitř, útočníkem, kterým může být propuštěný, rozzlobený, vydíraný, chamtivý zaměstnanec); velmi efektivní z hlediska vedení útoku je součinnost obou typů útočníků)

Útok

- **Útokem**, který nazýváme rovněž **bezpečnostní incident**, rozumíme
  - buďto úmyslné využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo
  - neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech

Útočit lze:

- Přerušením
  - aktivní útok na dostupnost, např. ztráta, znepřístupnění, porucha periférie, vymazání programu, vymazání dat, porucha v operačním systému
- Odposlechem
  - pasivní útok na důvěrnost, kdy neautorizovaný subjekt si neoprávněně zpřístupní aktiva, jde např. o okopírování programu nebo o okopírování dat
- Změnou
  - aktivní útok na integritu, neautorizovaný subjekt zasáhne do aktiva, provede se např. změna uložených a/nebo přenášených dat, přidání funkce do programu
- Přidáním hodnoty
  - aktivní útok na integritu nebo útok na autenticitu, tj. o případ, kdy neautorizovaná strana něco vytvoří (podvržení transakce, dodání falešných dat)

Rozeznáváme útoky na:

- hardware
- software
- data

Útočník

- Útočník může být **vnější**, ale v organizaci se často vyskytuje i **vnitřní** útočník. Podle znalosti a vybavenosti rozeznáváme:
  - útočníky slabé síly
    - amatéři, náhodní útočníci, využívající náhodně objevená zranitelná místa
  - útočníky střední síly
    - hackeři, jejichž častým krédem je dostat se k tomu, k čemu nejsou autorizovaní
  - útočníky velké síly
    - profesionální zločinci, kteří mají původ obvykle mezi počítačovými profesionály

Bezpečnost IS

- **Bezpečnost IS**
  - zajištěnost proti nebezpečím, hrozbám, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití IS.
- **Bezpečný IS** je takový IS
  - který je zajištěn **fyzicky**, **administrativně**, **logicky** i **technicky**. IS je třeba zabezpečovat, protože se jedná o ochranu investic, neboť informace je zboží, nutí k tomu právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat.

Bezpečnost IS dána zajištěním:

- Důvěrnosti
  - k údajům mají přístup pouze autorizované subjekty
- integrity a autenticity
  - data, software a hardware smí modifikovat jen autorizované subjekty a původ informací je ověřitelný
- Dostupnosti
  - data nebo služby jsou autorizovaným subjektům do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo

Bezpečnostní funkce

- **Bezpečnostní cíle** jsou:
  - dílčí přínosy k bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity a dostupnosti. Pro jejich dosažení se aplikuje používání funkcí prosazujících bezpečnost, nazývaných rovněž bezpečnostní funkce nebo bezpečnostní opatření.
- **Bezpečnostní funkce** přispívá buďto ke splnění jednoho bezpečnostního cíle, nebo ke splnění několika bezpečnostních cílů.

Kategorizace bezpečnostních funkcí:

- Podle okamžiku uplatnění na:
  - Preventivní
    - např. odstraňující zranitelná místa nebo aktivity zvyšující bezpečnostní uvědomění
  - Heuristické
    - snižující riziko dané nějakou hrozbou
  - detekční a opravné
    - minimalizující účinek útoku podle schématu „detekce–oprava–zotavení“

Kategorizace bezpečnostních funkcí

- Podle způsobu implementace:
  - softwarového charakteru
    - mnohdy označované jako logické bezpečnostní funkce
  - administrativního a správního charakteru
    - výběr a školení důvěryhodných osob, hesla, autorizační postupy, přijímací a výpovědní postupy
  - hardwarového charakteru
    - technické bezpečnostní funkce (např. čipové karty)
  - fyzického charakteru
    - např. stínění, trezory, zámky,..

Bezpečnostní funkce

- identifikace a autentizace
- autorizace a řízení přístupu
- řízení opakovaného užívání objektů
- účtovatelnost, resp. prokazatelnost odpovědnosti získání záruky, že lze učinit subjekty zodpovědné za své aktivity
- audit
- zajištění nepopiratelnosti
- zajištění integrity
- zajištění důvěrnosti
- zajištění pohotovosti

Bezpečnostní mechanismy

- Bezpečnostní mechanismy jsou:
  - nástroje používané pro implementaci bezpečnostních funkcí.
- Bezpečnostní mechanismy mohou být:
  - administrativní (zákony, vyhlášky, výběr důvěryhodných osob)
  - fyzické (trezor)
  - logické (softwarové – šifrování)
  - technické (hardwarové – autentizační karta)

Příklady bezpečnostních mechanismů

- Hesla a osobní identifikační čísla
  - místo uchovávání hesel (osobních identifikačních čísel) v původní podobě uchovávají v počítači výsledky jejich zpracování jednosměrnými funkcemi
- Magnetické karty
  - poskytuje paměť přibližně pro řádově stovky bitů dat
- Čipové karty
  - obsahuje procesor, který je schopen realizovat výpočty

Teorie spolehlivosti

- Spolehlivost zařízení je:
  - pravděpodobnost, že zařízení bude vykonávat zamýšlenou funkci během specifikovaného časového intervalu za stanovených podmínek

Spolehlivost softwaru

- Spolehlivost IS závisí na spolehlivosti hardwaru, softwaru, operátorů a procesů
- Největší problém – spolehlivost softwaru
- Softwarová spolehlivost je výsledkem nepředvídaných výsledků softwarových operací
- I jednoduchý program může mít obrovskou kombinaci vstupů a stavů, které nelze otestovat

Spolehlivost softwaru

Metrika spolehlivosti softwaru

Počet chyb na tisíc řádků zdrojového kódu

Typy celostních vlastností

- Funkcionální
  - Objevují se v případě, že komponenty systému fungují společně za účelem dosažení daného cíle. Například vlastností kola je být dopravním prostředkem v případě, že všechny součásti kola jsou sestaveny tak, aby tvořily kolo.
- Nefunkcionální
  - Příkladem je spolehlivost, výkonnost, kvalita. Vztahují se k chování systému v operačním prostředí. Jsou často kritické také u informačních systémů.

Vlivy na spolehlivost systému

- *Hardwarová spolehlivost*
  - Jaká je pravděpodobnost poruchy hardwarové komponenty a jak dlouho bude trvat odstranění takové poruchy?
- *Softwarová spolehlivost*
  - Jaká je pravděpodobnost, že softwarová komponenta bude produkovat špatný výstup. Porucha softwaru je hůře odhalitelná.
- *Spolehlivost operátora*
  - Jaká je pravděpodobnost, že operátor udělá chybu?

Spolehlivostní vztahy

- Poruchy hardwaru mohou produkovat signály, které jsou mimo rozsah vstupů softwarových komponent.
- Softwarové chyby mohou vést k chybám operátorů.
- Prostředí, ve kterém je systém nainstalován, může ovlivnit spolehlivost systému.

Spolehlivostní inženýrství

- Vzhledem k vzájemným vazbám mezi komponentami se chyby mohou šířit systémem
- Systémové chyby se často objevují vzhledem k nepředvídaným vazbám mezi komponentami
- Je pravděpodobně nemožné předvídat všechny možné vazby mezi komponentami

Servisně orientovaná architektura (SOA) IS

- SOA je způsob vývoje distribuovaných systémů, ve kterých jsou komponenty **samostatné služby**
- Služby mohou být prováděny **na odlišných počítačích** od různých poskytovatelů
- Byly vyvinuty **standardní protokoly**, které podporují komunikaci a výměnu dat mezi službami
- Realizací SOA jsou **webové služby** (Web Services)

Výhody SOA

- Služby mohou být poskytovány lokálně nebo předány externím poskytovatelům
- Služby jsou systémově a jazykově nezávislé
- SOA automatizuje výměnu informací mezi organizacemi prostřednictvím jednoduchých protokolů

Standardy webových služeb