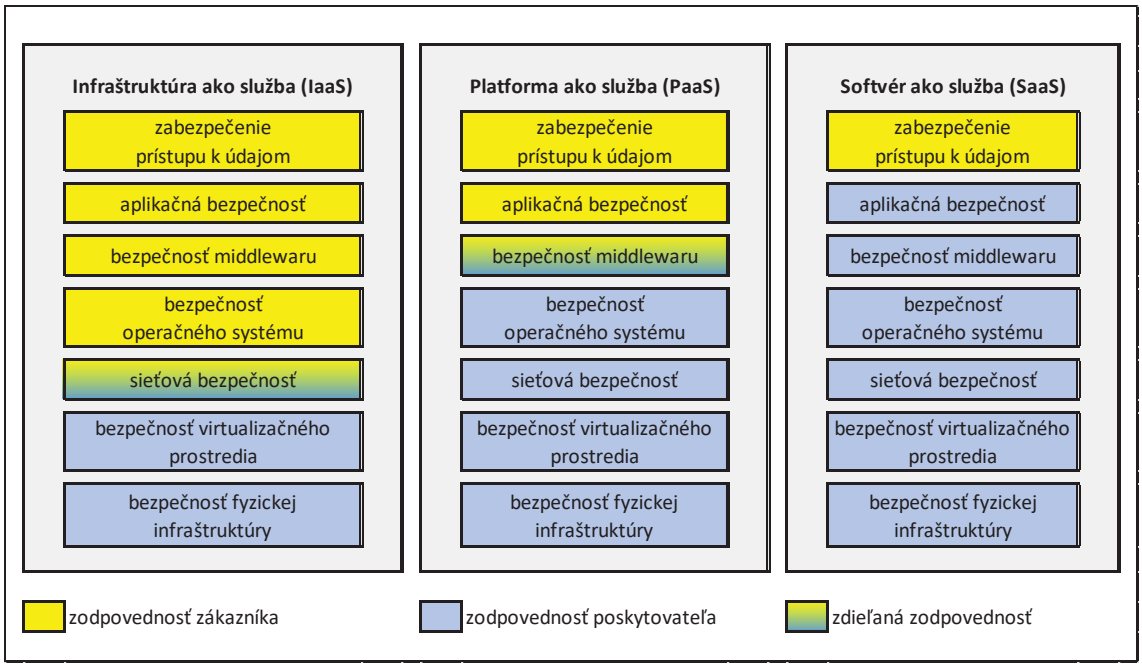
Bezpečnosť v cloude

Bezpečnosť a súkromie sú najdôležitejšie problémy, ktoré je treba riešiť pri navrhovaní spoľahlivého a dôveryhodného výpočtového prostredia. Pre každý počítačový systém je teda dôležitá jeho bezpečnosť a cloud nie je výnimkou. Používatelia cloudových služieb očakávajú, že poskytovateľ (CSP, Cloud Service Provider) zabezpečí dohodnutú úroveň služby (SLA, service-level agreement). Zákazníci migrujúci do cloudu potrebujú istotu, že výpočtové zariadenia a predovšetkým dáta, ktoré zverujú poskytovateľom cloudu, sú chránené. Toto je kritické pre spoločnosti, ktoré doteraz pracovali so svojimi dátami na svojich systémoch vo vlastných centrách a chránili si ich tradičnými spôsobmi (firewall, aplikačná brána, IDS/IPS...). Keďže sú dáta a dátové ložiská outsourcované tretej strane, zákazník stráca priamu kontrolu nad správou dát a stáva sa závislým na poskytovateľovi cloudu, ktorý nemusí byť vždy spoľahlivý. Po migrácii do cloudu sa časť zodpovednosti za bezpečnosť prenáša na práve na poskytovateľa cloudu [SB17, IMZ16].



Obrázok 0-1 Model zdieľania zodpovednosti za bezpečnosť v cloude [CD19].

Cloud computing prináša množstvo nových možností, ale rovnako ako iné nové technológie prináša aj isté bezpečnostné riziká. Tieto riziká je možné prekonať, vyžaduje si to však ich správne pochopenie.

Tak ako už uvádza 0, pre prostredie a formu cloud computingu je možné použiť rôzne modely. Zákazník musí najskôr pochopiť, ktorý z nich je pre jeho potreby najvhodnejší. Správna voľba modelu služieb cloudu (IaaS, PaaS, SaaS) a konkrétneho poskytovateľa cloudu znižuje bezpečnostné riziká spojené s migráciou do cloudu.

Tradičné počítačové systémy používajú na vytvorenie bezpečnostného perimetra firewall. Firewall tak vytvára kontrolný bod na hranici medzi chránenou vnútornou LAN a vonkajšou sieťou. Blokuje všetku komunikáciu a povoľuje iba definované výnimky (politika *default deny*), prípadne blokuje iba definovanú komunikáciu, inak všetko povoľuje (politika *default allow*). Druhý prístup má zmysel iba ak sú všetky aplikácie a dáta v niektorom bezpečnostnom perimetri. Cloud uvedené prístupy prekonáva. Výpočtové prostriedky, aplikácie a dáta sa presúvajú do prostredia cloudu, kde sú používateľom prístupné vzdialene vo vonkajšej sieti, a preto sa tradičný koncept hranice zabezpečenia už nepoužíva. Zmena prístupu ku zdrojom vyvoláva potrebu novej filozofie, ktorá zaručí bezpečnosť výpočtových prostriedkov aj v prostredí cloudu [SB17].

Význam bezpečnosti v cloude narastá aj s nástupom internetu vecí (IoT, Internet of Things). Obrovské množstvo cenovo lacných zariadení s nízkou spotrebou produkuje dáta, ktoré sa ukladajú a spracovávajú v cloude. Pre IoT zariadenia je typické zameranie iba na samotnú aplikáciu. Bezpečnosť je riešená minimálne. Často je prístup k zariadeniu chránený iba jednoduchým heslom, ktoré sa nedá zmeniť. Prípadne je zabezpečenie iba v rámci štruktúry siete snímačov a už nie pri prenose dát do cloudu. Pritom na základe dát z IoT zariadení sa často robia rozhodnutia, ktoré môžu viesť až k ohrozeniu majetku, zdravia a dokonca k úmrtiam ľudí. Napríklad kompromitovaný systém riadenia vzduchotechniky v nemocnici môže viesť k ohrozeniu zdravia pacientov. Do pozornosti sa tak aj pri internete vecí dostáva otázka bezpečnosti cloudových služieb, obzvlášť pri práci s citlivými dátami v zdravotníctve.

S cloudovými službami však rastie aj riziko ohrozenia súkromia. Hoci sú osobné dáta zbierané z rôznych zdrojov, už nie sú ako kedysi uložené a spracovávané na množstve izolovaných systémov, ale všetky končia v cloude [SPB+16, CRA+17].

Základné princípy

Jedným z najpopulárnejších modelov informačnej bezpečnosti je trojica označovaná ako CIA:

- dôvernosť (Confidentiality),
- integrita (Integrity),
- dostupnosť (Availability).

Útočník, ktorý sa snaží dôvernosť dát narušiť, chce zvyčajne dáta aj ukradnúť a predať. Útočník pokúšajúci sa narušiť integritu dát chce dáta zmeniť. Útočník, ktorý sa snaží narušiť dostupnosť dát, ich chce zneprístupniť, prípadne aspoň dostať do režimu off-line.

Model cloud computingu je tvorený vrstvami objektov, kde funkčnosť a zabezpečenie vyššej vrstvy závisí na nižších vrstvách. IaaS model zahŕňa vrstvu fyzickej infraštruktúry cloudu (úložisko, siete a servery), vrstvu virtualizácie (hypervízory) a vrstvu virtualizovaných zdrojov (VM, virtuálne úložisko, virtuálne siete). Model PaaS pokrýva vrstvy platformy (aplikačné servery, webové servery, IDE a ďalšie nástroje) a vrstvy API a služieb. Vrstva v PaaS závisí na virtualizácii zdrojov dodaných IaaS. Model SaaS zahŕňa aplikácie a služby ponúkané ako služba pre koncových používateľov. Vrstva v SaaS závisí na vrstve platforiem pre hosťovanie služieb a na vrstve virtualizácie. Takáto previazanosť objektov na rôznych vrstvách komplikuje problém zabezpečenia cloudu, pretože bezpečnosť každého objektu/vrstvy závisí od zabezpečenia nižších objektov/vrstiev.

Akékoľvek narušenie bezpečnosti akéhokoľvek cloudového objektu má dopad aj na bezpečnosť celej cloudovej platformy. Každá cloudová vrstva/objekt má osobitné požiadavky na bezpečnosť a špecifické zraniteľnosti, takže zabezpečenie celej služby si vyžaduje sadu bezpečnostných kontrol. Výsledkom je obrovské množstvo bezpečnostných kontrol, ktoré je potrebné spravovať. Navyše, správa heterogénnych bezpečnostných kontrol je komplexnou úlohou zohľadňujúcou konflikty medzi bezpečnostnými požiadavkami a bezpečnostnými opatreniami na každej vrstve. Uvedená skutočnosť môže viesť k nekonzistentnému bezpečnostnému modelu. Preto je potrebný jednotný modul riadenia bezpečnosti, ktorý bude koordinovať a integrovať bezpečnostné kontroly rôznych vrstiev na základe potrieb zabezpečenia [MGM10].

Analytická spoločnosť Gartner zverejnila v roku 2008 správu s názvom "Vyhodnotenie bezpečnostných rizík cloud computingu"[21]. Správa sa zamerala na sedem bezpečnostných problémov, ktoré by mali byť analyzované počas migrácii do cloudu. Týchto sedem problémov je možné považovať za základné prvky tvorby dobrej bezpečnostnej politiky v oblasti výpočtovej techniky. Zákazníci by mali od dodávateľa cloudovej služby požadovať riešenia uvedených problémov, čím dosiahnu zvýšenie ochrany a bezpečnosti svojich údajov v cloude. Správa uvádzala nasledovné problémy:

1. *Privilegovaný používateľský prístup*: pod "používateľom" v tomto prípade treba rozumieť používateľa-administrátora spravujúceho cloud. Pri migrácii do cloudu sa všetky dáta, vrátane citlivých, presunú do cloudu a ich majiteľ vo všeobecnosti stratí fyzickú kontrolu nad ich bezpečnosťou. Zákazníci teda musia od poskytovateľa cloudu požadovať konkrétne informácie týkajúce sa ľudí spravujúcich cloud. Napríklad "k akým dátam majú prístup" alebo "ako sú prístupy kontrolované" a podobne.
2. *Dodržiavanie predpisov*: aj keď poskytovatelia cloudov ukladajú a spravujú dáta svojich zákazníkov, v konečnom dôsledku sú to zákazníci, ktorí zodpovedajú za integritu a súkromie svojich vlastných dát. Mali by sa preto rozhodnúť pre takých poskytovateľov cloudu, ktorí získali bezpečnostné certifikáty od renomovaných

[21] https://www.gartner.com/en/documents/685308/assessing-the-security-risks-of-cloud-computing

audítorských spoločností a audity sú pravidelne opakované. Podľa spoločnosti Gartner, nesmú zákazníci poskytovať svoje citlivé dáta tým poskytovateľom služieb, ktorí odmietajú podstúpiť bezpečnostný audit.

3. *Umiestnenie dát*: dáta v cloude sú uložené v dátových centrách poskytovateľa cloudu rozložených po celej planéte. Zákazníci zvyčajne nemajú žiadne znalosti o tom, kde sú ich dáta fyzicky uložené. Takéto znalosti zvyčajne ani nepotrebujú. Sú však prípady, keď zákazník požaduje uloženie svojich dát na území konkrétnej oblasti alebo krajiny. Napríklad, v zmysle legislatívy svojej krajiny môže ukladať a spracovávať svoje dáta iba na území konkrétnej krajiny. Spoločnosť Gartner radí zákazníkom pýtať sa aj na takúto možnosť.
4. *Segregácia dát*: cloud computing je zdieľaná služba. Dátové úložisko je v cloude spravované v zdieľanom prostredí, kde sú dáta rozdielnych zákazníkov uložené na rovnakom mieste. Toto môže predstavovať bezpečnostné riziko. Poskytovatelia cloudových služieb musia implementovať mechanizmy logicky oddeľujúce uložené dáta rôznych zákazníkov. Šifrovanie je jednou z možností ako predísť narušeniu dôvernosti. Kľúčovou požiadavkou je však, aby implementované techniky boli dôkladne testované. Inak by nežiadúca nehoda mohla spôsobiť problémy.
5. *Obnova*: ďalším zásadným problémom je obnova dát pri akejkoľvek havárii. Poskytovatelia cloudu musia vydať prehlásenie, čo sa stane s dátami v takýchto prípadoch a ako dlho bude trvať obnova dát a dostupnosti služieb. Pre úplnú obnovu musí poskytovateľ udržiavať dátovú a aplikačnú infraštruktúru na geograficky oddelených miestach.
6. *Spolupráca s vyšetrovacími orgá*nmi: vyšetrovanie nezákonnej činnosti môže byť v prostredí cloudu veľmi náročné. Dôvodom je predovšetkým to, že údaje sú organizované a ukladané v neustále sa meniacej štruktúre dátových úložísk. Ďalším problémom je spoločné ukladanie dát od viacerých spotrebiteľov na rovnaké fyzické úložisko. Zákazníci by mali byť informovaní ako poskytovateľ cloudu v minulosti spolupracoval pri vyšetrovaní nelegálnych aktivít svojich klientov a ako má pre takéto situácie nastavené pravidlá a postupy.
7. *Dlhodobá životnosť*: v ideálnom prípade žiadny poskytovateľ cloudových služieb nezruší a ani nepredá svoj obchod. Pokiaľ sa to predsa len stane, vynára sa otázka čo sa stane s dátami zákazníkov. Budú dostupné? Zostane zachovaná ich dôvernosť? Zákazníci by mali byť podrobne informovaní čo sa bude diať v takýchto situáciách.

Renomovaní dodávatelia cloudových služieb sú schopní dosiahnuť uspokojivé výsledky pri riešení týchto problémov a ponúknuť zabezpečené cloudové prostredie [SB17].

Na problematiku bezpečnosti v cloud computingu je možné nazerať z dvoch uhlov pohľadu: zodpovednosť poskytovateľa cloudu (či už poskytujúceho SaaS, PaaS alebo

IaaS) a zodpovednosť zákazníka služby. Poskytovateľ musí zaistiť bezpečnosť svojej vlastnej infraštruktúry a aj dát a aplikácií svojich klientov. Na druhej strane zákazníci sa musia uistiť, že poskytovateľ použil všetky možné bezpečnostné opatrenia na ochranu služieb. Skúsenosti a odborné znalosti poskytovateľa hrajú v tejto súvislosti významnú úlohu.

Rovnako významnú úlohu zohráva aj vzájomný vzťah a dôvera medzi poskytovateľom a zákazníkom služby. Obe strany musia mať jasnú predstavu o svojej zodpovednosti ohľadne manažmentu bezpečnosti. Na pochopenie rizík v zmysle aké bezpečnostné opatrenia implementoval poskytovateľ cloudu, môže spotrebiteľ najať externých expertov [SB17].

Ako už bolo uvedené v časti Zodpovednosť v modeloch služieb cloudu, za bezpečnosť fyzickej infraštruktúry je plne zodpovedný poskytovateľ cloudu. Bezpečnosť fyzickej infraštruktúry dosiahne použitím prostriedkov fyzickej bezpečnosti, ako biometrická kontrola prístupu, fyzické tokeny, detektory pohybu, detektory požiaru a podobne. To isté platí, ak poskytovateľ ponúka virtualizované prostredie, zodpovednosť za izoláciu prostredí rôznych zákazníkov je v zodpovednosti poskytovateľa. Poskytovateľ sa musí postarať o to, aby v prostredí zdieľanej virtualizácie nemohol používateľ jedného virtuálneho počítača čítať pamäť iného virtuálneho počítača ak oba virtuálne počítače sú prevádzkované na jednom fyzickom serveri. Pri sieťovej bezpečnosti modelu IaaS už deliaca čiara vymedzujúca zodpovednosť medzi poskytovateľom a zákazníkom nie je taká ostrá, preto aj ju Obrázok 0-1 zobrazuje ako prelínajúcu. Poskytovateľ cloudu má svoju vlastnú sieť, za ktorú je zodpovedný a nad ňou je virtuálna sieť a je zodpovednosťou zákazníka vytvoriť a zabezpečiť v rámci nej bezpečnostné zóny.

Bezpečnosť operačného systému je obyčajne jednoduchá: pri IaaS je to zodpovednosť zákazníka, pri PaaS a SaaS je zodpovedný poskytovateľ cloudu. Pre middlewari, ako vrstvu medzi operačným systémom a aplikáciou, je zodpovednosť za bezpečnosť pri modeli PaaS opäť často zdieľaná, Obrázok 0-1. Poskytovateľ cloudu môže zabezpečovať inštaláciu aktualizácií a záplat, ale bezpečná konfigurácia aplikačného servera, implementácia šifrovania (web server a certifikát) a podobne je na zákazníkovi.

Pri modeli SaaS je za zraniteľnosť v aplikačnej vrstve zodpovedný poskytovateľ. Na druhej strane, za bezpečnosť prístupu k dátam je takmer vždy zodpovednosťou zákazníka.

Bezpečnostné hrozby v cloude

Na úspešné zavedenie cloudových služieb je rozhodujúce porozumieť bezpečnostným problémom cloud computingu a navrhnúť účinné riešenia. Korene príčin mnohých bezpečnostných incidentov boli v chybnom predpoklade zákazníka, že poskytovateľ cloudu niečo zabezpečuje, hoci v skutočnosti si to mal zabezpečiť sám, alebo navyše objednať u poskytovateľa. Napríklad, z Amazon Web Services Simple Storage Service (AWS S3) vinou nesprávneho pochopenia zdieľanej zodpovednosti unikli počas volieb v USA v 2016 údaje o 198 miliónoch registrovaných voličov. Podľa reportu spoločnosti Barracuda Networks z 2017 77 % IT manažérov je presvedčená, že poskytovatelia cloudu

sú zodpovední za bezpečnosť dát svojich zákazníkov a 68 % verí, že poskytovatelia sú zodpovední aj za bezpečnosť klientskych aplikácií. Pritom podľa bežných SLA to nie je pravda.

Hlavné bezpečnostné hrozby a zraniteľné miesta spojené s cloud computingom je možné zoskupiť do niekoľkých kategórií: sieťová bezpečnosť, bezpečnosť virtualizačného prostredia, správa prístupu a bezpečnosť dátového úložiska [IMZ16].

Sieťová bezpečnosť

Problémy súvisiace s bezpečnosťou v cloud computingu zahŕňajú jednak problémy, ktoré existujú aj v tradičnom výpočtovom prostredí, ale aj problémy špecifické pre cloud [IMZ16]. V cloudoch nie je hranica medzi vnútornou a vonkajšou sieťou taká zrejmá ako v tradičnom prostredí. Vyvstávajú tu rôzne otázky a nejasnosti, ako napríklad“ Je pri používaní modelu databáza ako služba táto služba vo vnútornej alebo vonkajšej sieti? A ak je štruktúra multicloudová a distribuovaná po celej planéte, na ktorej strane bezpečnostného perimetru siete sa jej prvky (cloudové služby) nachádzajú?

Vysoká variabilita modelov služieb cloudu, ktoré môžu byť využité pri budovaní aplikácie, prináša nejasnosti v kontrole sieťového prístupu. Je preto potrebné pristupovať ku každému modelu osobitne:

- Prostredie IaaS je najbližšie k tradičným prostrediam, oproti nim však prináša výhodu segmentácie aplikácií.
- Prostredie založené na kontajneroch a spravované špecializovaným orchestračným nástrojom. Príkladom je kontajnerový systém Docker a orchestračný systém Kubernetes. Ak sú aplikácie dekomponované až na mikroslužby, je možné sieťovú kontrolu v rámci aplikácie ladiť jemnejšie.
- Aplikačné prostredia PaaS, ako napríklad komerčne dostupné Cloud Foundry, Elastic Beanstalk a Heroku. Líšia sa počtom dostupných ovládacích prvkov siete. Niektoré umožňujú izoláciu jednotlivých komponentov, iné vôbec nemusia poskytovať konfigurovateľné funkcie firewallu.
- Serverless prostredie alebo FaaS (Function-as-a-Service) fungujú v zdieľanom prostredí, ktoré nemusí poskytovať možnosti sieťovej kontroly, alebo poskytujú možnosť kontroly len na strane klienta. Príkladom sú AWS Lambda, OpenWhisk, Azure Functions, a Google Cloud Functions.
- SaaS prostredie. Kým niektoré komerčne dostupné riešenia modelu SaaS poskytujú jednoduché sieťové ovládacie prvky (napríklad prístup iba cez VPN alebo zo zoznamu povolených IP adries), iné riešenia túto možnosť neobsahujú.

Mnoho aplikácií navyše používa viac ako jeden z uvedených modelov doručenia služby ako súčasť celkového riešenia. V jednej aplikácii je možné napríklad použiť kontajnery aj tradičné IaaS alebo kombináciu vlastného kódu so SaaS. To znamená, že niektoré komponenty klientovej aplikácie môžu mať lepšie možnosti kontroly sieťového prístupu

prvkami sieťovej bezpečnosti (ako firewall, WAF, IPS a pod.) ako iné. Preto je dôležité brať do úvahy celé spektrum hrozieb a rizík pre aplikáciu.

V prostredí cloudu boli odhalené mnohé sieťové útoky známe už z tradičného prostredia:

- *Wrapping attack* (útok obalením). Podpisy XML sa všeobecne používajú na účely autentifikácie a integrity správ SOAP (Simple Object Access Protocol). Protokoly, ktoré používajú podpisy XML, sú zraniteľné útokom nazývaným útok obalením podpisu XML alebo jednoducho útok obalením. Všeobecne to platí pre webové služby, a teda aj pre cloud computing. Aby sa zabezpečila integrita správy, preddefinovaná časť alebo viaceré časti správy SOAP sa podpíšu pomocou podpisu XML. Správa obsahuje bezpečnostnú hlavičku s podpisovým prvkom, ktorý odkazuje na jednu alebo viac častí podpísanej správy. Útok obalením podpisu XML využíva skutočnosť, že prvok podpisu neposkytuje žiadne informácie o odkazovanej časti správy. Útočník môže ľahko upraviť telo správy a vložiť škodlivý kód bez zneplatnenia podpisu. Útočník tu prakticky obalí podpis XML okolo škodlivého kódu a odovzdá ho, akoby išlo o autentickú správu.
- *Flooding attack* (útok zahltením). Jedným z najstarších typov tohto útoku je SYN flood, keď útočník posiela veľké množstvo žiadostí o vytvorenie TCP spojenia (TCP segment so SYN príznakom) z falošných zdrojových IP adries na cieľovú IP adresu. Cieľ na každú žiadosť reaguje rezervovaním zdrojov na nové sieťové spojenie a odoslaním TCP segmentu s príznakmi SYN a ACK. Cieľom útočníka je zahltením znefunkčniť cieľ. Iným príkladom útoku zahltením je, ak útočník vygenerovaním obrovského množstvo falošných žiadostí na web server určitého zákazníka vyvolá nárast požiadaviek na výpočtové zdroje. Cloud následne spúšťa ďalšie inštancie virtuálnych strojov a tým sa aj navyšuje zákazníkova konečná cena za prevádzku danej služby. Sila útoku môže rásť až do dosiahnutia limitov na výpočtové zdroje definované v zmluve medzi zákazníkom a poskytovateľom cloudu, čím príde k znefunkčneniu webovej služby. Útok vedený so zámerom znefunkčniť cieľ, ktorým môže byť napríklad server, služba alebo sieť, sa označuje ako DoS (Denial of Service). Pri útoku zahltením je útok vedený z veľkého množstva zväčša kompromitovaných zariadení (počítače, IP kamery, domáce úložiská..) z rôznych lokalít, preto sa označuje ako DDoS (Distributed Denial of Service).
- *Malware Injection Attack*. Tento typ útoku spočíva v tom, že sa do cloudového systému virtuálnych strojov, inštancií alebo obrazov vloží malware. V prostredí SaaS alebo PaaS je cieľom útočníka vytvorenie vlastnej implementácie služby obsahujúcej škodlivý kód a nasadenie tejto služby v cloude tak, aby vyzerala ako legitímna služba. Medzi dopady tohto útoku patrí odpočúvanie komunikácie, modifikácia dát, neoprávnený prístup k zdrojom cloudu, únik prístupových údajov používateľa, zmeny funkčnosti a blokovanie služby. Rovnakým spôsobom môžu útočníci v prostredí IaaS vytvárať virtuálne stroje obsahujúce a šíriace

malware. Kľúčovou výzvou tu nie je len detekcia vloženia malwaru, ale aj určenie inštancií virtuálneho stroja, ktoré útočník používa na šírenie malwaru.

- *Insecure APIs*. Zákazníci v cloude zvyčajne používajú na správu a interakciu s cloudovými službami sadu rozhraní API. Poskytovanie služieb, správa aplikácií, monitorovanie, povoľovanie bezpečnostných funkcií a podobne sa vykonávajú prostredníctvom týchto rozhraní. Tieto API sú rozhodujúce pre bezpečnosť a dostupnosť cloudových služieb. Nezabezpečené, ale aj zle navrhnuté API môžu organizáciu vystaviť rôznym bezpečnostným hrozbám, ktoré ovplyvnia dôvernosť, integritu a dostupnosť.
- Pri útoku *Cross Site Scripting (XSS)* útočník vloží do webového obsahu svoj škodlivý kód, ktorý sa vykoná na počítačoch návštevníkov webu. Na vloženie škodlivého kódu sa zvyčajne využije zraniteľnosť webovej aplikácie, webového servera, alebo jeho pluginu. Vo výsledku úspešný útočník získa prístup ku všetkým dátam, s ktorými pracuje prehliadač.

Hoci sieť v cloude prináša niektoré nové črty, stále je v cloudových prostrediach relevantných aj veľa tradičných konceptov, ktoré sa však môžu používať mierne odlišným spôsobom. Koncept kontroly prístupu založený na whiteliste a blackliste je jedným z nich.

Whitelist je zoznam povolených vecí (protokolov, IP adries, domén, portov …), pričom všetko ostatné je zakázané. *Blacklist* je naopak špecifickým zoznamom vecí, ktoré sú odmietnuté, pričom umožňuje všetko ostatné. Vo všeobecnosti sa za lepší (bezpečnejší) prístup považuje whitelist.

V mnohých cloudových prostrediach sú systémy poskytujúce službu pravidelne vytvárané a rušené a zákazník má len malú kontrolu nad pridelenými IP adresami. Z tohto dôvodu môžu zdrojové alebo cieľové IP adresy na whiteliste vyžadovať oveľa širší rozsah, ako by bolo akceptovateľné v tradičnom prostredí. Môžu byť dokonca špecifikované ako „0.0.0.0/0“ (čo predstavuje ľubovoľnú IP adresu), ktoré správcovia tradičných firewallov nepovoľujú.

S rozmachom sietí na doručovanie obsahu (content delivery network) a s používaním globálnych loadbalancerov (GSLB, Global Server Load Balancers) sa rozsahy dôveryhodných IP adries stávajú pre niektoré typy filtrovania komunikácie, ako napríklad kontroly odchádzajúcich pripojení, menej použiteľné, pretože sieťové adresy sa menia. To môže viesť k blokovaniu oprávnených spojení. Napriek tomu majú whitelisty a blacklisty stále svoje miesto v cloudovej bezpečnosti, len je potrebné rešpektovať ich obmedzenia.

Koncept delimitarizovanej zóny (DMZ) je možné implementovať do prostredia mnohých cloudov, ktoré poskytujú IaaS. Je to oblasť siete v cloude ohraničená firewallom, v ktorej sú umiestnené zdroje sprístupnené návštevníkom. V prípade kompromitácie sú zdroje izolované od ostatných zdrojov siete v cloude. V prípade iných modelov doručenia služby využívaných v cloudoch nemá implementácia DMZ zmysel, alebo je priamo vylúčená.

Proxy služby zabezpečujú prijatie požiadavky, jej odoslanie na ďalší komponent a preposlanie spracovanej odpovede odosielateľovi požiadavky. V cloudovom prostredí sa častejšie používa model *reverznej proxy služby*, keď proxy server preberá požiadavky od používateľov a tieto požiadavky odosiela na backendové servery. Proxy servery môžu byť užitočné jednak pre rôzne funkčné požiadavky (napríklad loadbalancer) a jednak pre bezpečnosť.

Firewally patria k najznámejším prvkom sieťovej bezpečnosti. Pomocou nich sa rozdeľujú siete do separátnych zón. Implementujú blacklistové a whitelistové zoznamy IP adries. Často plnia aj ďalšie funkcie ako VPN brány, či NAT (Network Address Translating). Môžu pracovať na rôznych vrstvách komunikačného modelu. V prostredí cloudu sa zvyčajne používa plnohodnotné virtuálne zariadenie ako ekvivalent fyzického firewallu. Tieto firewally sa označujú ako *next-generation firewall* a kombinujú funkcionalitu ďalších prvkov sieťovej bezpečnosti ako IDS (Intrusion Detection System), IPS (Intrusion Prevention System) a WAF (Web Application Firewall). Príkladom sú Barracuda CloudGen Firewall alebo CheckPoint CloudGuard. Poskytovatelia cloudov poskytujú aj vlastné riešenia kontroly sieťového prístupu formou sieťových zoznamov na riadenie prístupu (Access Control Lists, ACL). Pomocou nich zákazník jednoducho definuje pravidlá povoľujúce prístup k určeným zdrojom.

Bezpečnosť virtualizačného prostredia

Virtualizácia je jednou z hlavných zložiek cloud computingu, ktorá pomáha organizáciám cenovo efektívnym spôsobom optimalizovať výkon aplikácií. Túto technológiu je možné použiť aj ako bezpečnostný komponent; napríklad na zabezpečenie monitorovania virtuálnych strojov, uľahčovanie riadiacich úloh, ako je správa výkonnosti, správa cloudovej infraštruktúry a riadenie plánovania zdrojov. Hypervízor funguje ako abstrakčná vrstva poskytujúca potrebné funkcie správy zdrojov, ktorá umožňujú zdieľanie hardvérových prostriedkov medzi virtuálnymi počítačmi. Tieto technológie síce prinášajú veľké výhody, ale predstavujú aj ďalšie bezpečnostné hrozby [IMZ16].

- *Zraniteľnosti samotného Hypervízora*. Hypervízor umožňuje izolovaný beh viacerých hosťujúcich virtuálnych strojov na jednom fyzickom stroji. Kompromitácia hypervízora vedie k možnosti ovládať beh virtuálnych strojov a cez možnosť čítať zdieľanú pamäť a dátové úložiská aj k úniku dát vrátane prístupových údajov k jednotlivým virtuálnym strojom. Uvedená skutočnosť robí hypervízor veľmi zaujímavým cieľom pre útočníkov.
- *VM Escape*. Virtualizácia je navrhnutá tak, aby hostiteľ a virtuálne počítače boli robustne izolované. Ale chyby v tejto izolácii umožňujú útočníkovi vložiť do obslužných procesov škodlivý kód a tým izoláciu prelomiť a vyskočiť z virtuálneho počítača. Útočník sa tak dostane do hostiteľského systému odkiaľ môže realizovať ďalšie útoky.

- *Rozširovanie VM (VM sprawling)* je príznakom akejkoľvek rýchlo rastúcej virtuálnej infraštruktúry. Keď sa ktorékoľvek oddelenie spoločnosti rozhodne spustiť svoje špecifické aplikácie na vyhradených serveroch, môže to urobiť vďaka virtualizácii. Virtuálne stroje sú často nastavené na dočasné použitie, ako testovacie alebo vývojové laboratóriá, a po použití na ne môžu vlastníci zabudnúť a už ich nepoužívajú. Čím viac virtualizovaných aplikácií v spoločnosti existuje, tým je pravdepodobnejšie, že sa v infraštruktúre spoločnosti objaví „virtuálny odpad" a spôsobí rozrastanie virtuálnych strojov. Dalo by sa povedať, že toto je moderná verzia fenoménu „server pod stolom" z minulých rokov.
- *Cross VM Side Channel Attack*. Postranný kanál je forma úniku informácií, ktorá hrozí pri zdieľaní vyrovnávacej pamäte. Útok cez postranný kanál využíva takéto úniky na odcudzenie citlivých informácií, napríklad kryptografických kľúčov. Takéto útoky sú v cloud computingu klasifikované ako veľmi sofistikovaný útok.

Správa prístupu

Spravovanie identít (autentifikácia, autorizácia, roly) a poskytovanie bezpečného a efektívneho prístupu (IAM, Identity and Access Management) k rozsiahlym dátovým úložiskám je dôležitým prvkom cloud computingu. Vo väčšine organizácií je najdôležitejšie zabezpečenie dát a ochrana osobných údajov. Preto je spoľahlivá stratégia riadenia identity a prístupu nevyhnutným predpokladom strategického využívania bezpečných služieb cloud computingu [IMZ16].

Identita a manažment prístupu sa často uvádzajú spolu, ide sa však o dva odlišné pojmy:

- každá entita (napríklad používateľ, administrátor, systém) potrebuje identitu. Proces overenia identity sa nazýva autentifikácia,
- manažment prístupu je o zabezpečení toho, aby entity mohli vykonávať iba tie úlohy, na ktoré majú oprávnenie. Proces kontroly oprávnení entít pri prístupe k objektom sa označuje ako autorizácia.

V oblasti bezpečnosti IT sa často tieto dva pojmy prekrývajú. Napríklad je možné pre niekoho vytvoriť identitu (s priradenými prístupovými údajmi, ako je meno a heslo) a potom implicitne povoliť, aby ktokoľvek s platnou identitou mal oprávnenie na prístup k všetkým údajom v systéme. Prípadne je možné prístup niekoho odvolať odstránením jeho identity.

Mnoho poskytovateľov cloudových služieb ponúka služby IAM bezplatne ako súčasť cloudovej služby. IAM potom umožňuje mať jedno centrálne miesto na správu identít administrátorov cloudových služieb v celej organizácii pre prístup ku všetkým službám, ktoré poskytovateľ cloudu ponúka. Zákazník má prehľad o tom, akú úroveň prístupu daná osoba (zamestnanec, klient, kontraktor …) má. A v prípade, že ukončí spoluprácu s organizáciou, je možné spoľahlivo zrušiť všetky prístupy používané danou osobou.

Príkladmi komerčne dostupných služieb identity na autentifikáciu správcov cloudu pomocou služieb poskytovateľa cloudu sú Amazon IAM, Azure Active Directory B2C a Google Cloud Identity.

Okrem identít, ktoré zákazník poskytovateľa cloudu používa pre prístup k službám cloudu, je potrebné spravovať aj identity koncových používateľov, či už ide o vlastných zákazníkov alebo zamestnancov. Realizované to môže byť jednoducho v rámci aplikácie bežiacej v cloude. Prístupové údaje sú uložené v rovnakej databáze ako dáta, s ktorými pracuje aplikácia. Uvedené riešenie je však pre koncových používateľov menej prívetivé, pretože si musia pamätať prístupové údaje k ďalšiemu účtu. Inou možnosťou je použiť existujúcu službu identifikácie. Môže to byť služba vnútornej identity vlastných zamestnancov alebo zamestnancov zákazníka. Pre koncových zákazníkov to môže byť aj externá služba, ako napríklad Facebook, Google alebo LinkedIn. Vyžaduje si to však dôveru k tejto službe identity, aby bolo možné používateľov správne autentifikovať.

Najlepším spôsobom ochrany pred ukradnutím prístupových údajov je *viacfaktorová autentifikácia*. Najčastejšie sa definuje ako niečo čo používateľ vie, napríklad heslo, niečo čo má, napríklad hardvérový token, mobil, a niečo čím je, napríklad snímka sietnice oka, otlačok prsta. V cloudovom prostredí sa najčastejšie implementuje *dvojfaktorová autentifikácia* (2FA, two-factor access). Prvým "faktorom" je heslo a druhým môže byť:

- Doručená SMS na mobilný telefón, podmienkou je dostupná mobilná sieť, aby mohla byť SMS doručená. Zároveň je tu riziko krádeže telefónneho čísla pomocou klonovania SIM karty alebo zachytenia SMS.
- Časovo obmedzené jednorazové heslo (TOTP, Time-based One-time Passwords). Táto metóda vyžaduje, aby sa mobilnému zariadeniu poskytlo počiatočné „tajomstvo“ (zvyčajne prenášané pomocou 2D čiarového kódu). Tajomstvo, ktoré sa používa na výpočet jednorazového hesla každú minútu. Jednorazové heslo sa musí uchovávať v bezpečí iba minútu alebo dve, ale počiatočné tajomstvo umožňuje každému zariadeniu generovať platné heslá, a preto by sa malo po použití vymazať alebo dať na bezpečné miesto. Po prenose počiatočného tajomstva sa pre mobilné zariadenie nevyžaduje prístup k sieti ako pri SMS, ale iba synchronizácia hodín.
- Push notifikácie. Metódou push notifikácie sa už overená klientska aplikácia na mobilnom zariadení pripája k serveru, ktorý podľa potreby cez toto spojenie pošle jednorazový kód klientskej aplikácii. Je to bezpečné, pokiaľ je autentifikácia pre už autentifikovanú klientsku aplikáciu bezpečná, ale vyžaduje pripojenie do internetu.

Autentifikácia sa používa aj pri prístupe na API. API heslo je podobné heslu pri autentifikácii používateľa, s tým rozdielom, že k autentifikácii API je potrebné len heslo. API heslo by mal byť dlhý reťazec náhodných znakov. Pri prístupe k API nie je možné použiť viacfaktorovú autentifikáciu, aplikácia nemá mobilný telefón ani otlačok prsta. To

znamená, že s autentifikačným heslom k API je potrebné narábať veľmi opatrne. Tu je niekoľko základných princípov pre prácu s nimi:

- heslá by sa mali dať ľahko meniť v pravidelných intervaloch a vždy, keď existuje podozrenie, že mohli uniknúť. Ak zmena hesla znamená, že treba aplikáciu stiahnuť a na mnohých miestach ju ručne zmeniť, je to problém.
- Heslá by vždy mali byť šifrované.
- Treba minimalizovať počet ľudí, ktorí vedia heslo.
- Systém, na ktorom sú uložené heslá, by mal byť dobre zabezpečený.
- Granulovať prístupy do čo najvyššej miery.
- Všetky použitia hesla aj jeho zmeny, by mali byť logované.

V roku 2016 unikli spoločnosti UBER dáta o 57 miliónov jej vodičov a zákazníkov, pretože v zdrojových kódoch jej aplikácie boli niektoré prístupové heslá k AWS. Aplikácia potrebovala tieto heslá na svoju funkcionalitu, ale nemali byť viditeľné v zdrojových kódoch. Toto je veľká chyba z dvoch dôvodov:

- Úložisko zdrojového kódu pravdepodobne nie je určené primárne na utajenie informácií. Jeho primárnou funkciou je ochrana integrity zdrojového kódu – napríklad zabránenie neoprávnenej modifikácii vložením zadných dvierok (backdoor). Úložisko zdrojového kódu môže byť v mnohých prípadoch sprístupnené programátorom tretích strán, alebo aj hocikomu v rámci komunitných stretnutí dobrovoľných programátorov (coding days).
- Aj keď je úložisko zdrojového kódu úplne bezpečné, je veľmi nepravdepodobné, že každý, kto má prístup k zdrojovému kódu, má aj oprávnenie poznať heslá použité v produkčnom prostredí.

Najčastejším riešením je odstrániť heslá zo zdrojového kódu a umiestniť ich niekde inde, napríklad na dedikovaný server so systémom správy hesiel.

Vo väčšine prípadov bude nasadenie aplikácie pozostávať z troch častí:

- kód aplikácie,
- konfigurácia pre toto konkrétne nasadenie,
- heslá potrebné pre toto konkrétne nasadenie.

Uloženie všetkých troch častí do jedného balíka môže viesť k závažným bezpečnostným incidentom.

Bezpečnosť dátového úložiska

Koncept poskytovateľa služby dátového úložiska, označovaný aj ako data outsourcing, má rastúci trend. Dostupnosť, integrita a dôvernosť dát zákazníkov závisí od kvality poskytovateľa, ktorého úroveň môže byť rôzna. Zákazník nemá možnosť overiť

bezpečnosť služby. Musí sa spoľahnúť na výsledky auditu audítorských firiem. Ak vôbec poskytovateľ takýto audit absolvoval. Poskytovateľ rovnako neochotne zverejňuje aj prípadné incidenty, aby si nezhoršil reputáciu. Preto sa v oblasti výskumu venuje veľká pozornosť zaručeniu integrity dát uložených na nedôveryhodných serveroch [IMZ16].

Vo všeobecnosti je možné uvažovať o nasledovných bezpečnostných problémoch outsourcovaného dátového úložiska:

- *Dôvernosť údajov*. Dôvernosť sa týka obmedzenia prístupu k informáciám a ich sprístupňovania iba oprávneným používateľom alebo systému. Jednými zo základných zásad dôvernosti sú zásady „len ak potrebuje poznať“ a „najmenšie možné privilégium“. Prístup ku kriticky dôležitým a citlivým informáciám by sa mal obmedziť iba na tých jednotlivcov alebo systémy, ktorí majú špecifickú nevyhnutnosť získať alebo použiť potrebné informácie. V prostredí cloud computingu sa v dôsledku veľkého počtu zúčastnených strán, zariadení a aplikácií zvyšuje aj počet prístupových bodov. Preto sa zvyšuje aj riziko narušenia bezpečnosti dát. Dôvernosť dát uložených vo verejnom cloudu môžu ovplyvniť: 1) mechanizmy kontroly prístupu (autentifikácia a autorizácia), 2) schéma ochrany údajov, 3) použitý šifrovací algoritmus a 4) správa šifrovacích kľúčov.
- *Integrita dát*. V cloud computingu sa integrita dát považuje za jeden z najväčších problémov. Integrita znamená, že informácie sú presné a spoľahlivé a neoprávnená strana ich neupravila, nevytvorila alebo nevymazala.
- *Dostupnosť dát*. Očakáva sa, že dáta uložené do úložiska budú vždy v prípade potreby dostupné. Napriek použitiu architektúr navrhnutých pre vysokú spoľahlivosť a dostupnosť služieb môžu mať služby cloud computingu výpadky alebo spomalený výkon. Existuje pomerne veľa hrozieb, ktoré môžu spôsobiť nedostupnosť údajov. Po prvé, dostupnosť v sieti môžu ovplyvniť sieťové útoky ako napríklad útok odmietnutia služby (DoS alebo DDoS). Po druhé, vlastná dostupnosť poskytovateľov cloudových služieb môže byť zdrojom problémov. Okrem výpadkov služieb môžu veľké systémy úložných zariadení zaznamenať aj zlyhania diskov/sektorov, z ktorých niektoré môžu viesť k trvalej strate údajov.
- *Izolácia dát*. Zdieľané zdroje sú zásadnými charakteristikami cloud computingu. Zákazníci preto musia pred presunom svojich dát do cloudu zabezpečiť, aby všetky údaje v cloude boli úplne bezpečné a prístupné iba oprávneným používateľom. V cloudovom prostredí je obvykle požiadavka zákazníka spracovaná aplikáciou, ktorá je spustená s primeranými oprávneniami na prístup k akýmkoľvek údajom zákazníka. Táto aplikácia je zodpovedná za overenie a autorizáciu žiadosti. Keďže jediná ochrana je na aplikačnej úrovni, jediná zraniteľnosť na tejto úrovni ohrozuje údaje všetkých zákazníkov, čo by tiež mohlo viesť k úniku údajov medzi zákazníkmi.
- *Zdieľanie údajov*. Cloudové služby so zdieľaním dát sú vhodným modelom pre aplikácie, ako je online spracovanie textu, kalendár, blogovanie a sociálne siete.

Tieto aplikácie umožňujú viacerým používateľom upravovať svoje zdieľané zdroje súčasne, pričom sú škálovateľné a globálne prístupné. Tieto výhody môžu naopak ovplyvniť súkromie v dôsledku úniku informácií na strane servera a predstavovať značné riziko pre dôvernosť zdieľaných zdrojov. Aj opakujúca sa zmena členstva v skupine sťažuje zdieľanie údajov v prostredí viacerých majiteľov pri súčasnom zachovaní integrity a súkromia údajov.

- *Zálohovanie dát a redundancia*. Outsourcing dát do cloudového úložiska nemusí nevyhnutne znamenať, že údaje sú aj skutočne zálohované. Aby sa predišlo strate údajov a aby sa zachovala kontinuita činnosti, je potrebné zabezpečiť, aby boli zavedené správne zásady zálohovania. Z dôvodu ľahkej prevádzky môžu poskytovatelia služieb uprednostňovať spoľahlivé zálohovanie bez aktívneho súhlasu klientov. Tento prístup je nežiaduci, pretože dáta môžu byť v budúcnosti neočakávane zverejnené v dôsledku niektorých vonkajších alebo vnútorných útokov na cloud alebo nesprávneho životného cyklu zálohovacích dátových nosičov zo strany prevádzkovateľov cloudu.
- *Bezpečné mazanie dát*. Ide o zmazanie dát z úložiska, po ktorom už nie je možné zmazané dáta neskôr rekonštruovať. Vo verejnom cloudovom prostredí je základným záväzkom úplné vymazanie údajov (na žiadosť klienta) vrátane všetkých logovacích súborov a zálohových replík určených na obnovenie. Neodkladné zmazanie dát však môže byť náročné, pretože viaceré repliky údajov môžu byť rozptýlené v rôznych geografických lokalitách. Preto je ťažké zabezpečiť, aby poskytovateľ služieb spoľahlivo odstraňoval všetky záložné kópie údajov. Disk, ktorý je potrebné zničiť, môže navyše obsahovať údaje aj iných klientov. Niekedy môže byť zničenie samotného pamäťového média nevyhnutné na zabezpečenie úplného vymazania údajov.

Risk manažment v Cloude

Vo všeobecnosti, bezpečnostné riziko je možnosť, že určitá hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí organizácii škodu. *Risk manažment* sú potom koordinované činnosti pre vedenie a riadenie organizácie s ohľadom na riziká. Vo väčšine systémov na manažment rizika je úroveň rizika založená na kombinácii pravdepodobnosti, že určitá hrozba bude uskutočnená, t. j. nastane incident, a aký bude dopad incidentu. Napríklad, je veľmi pravdepodobné, t. j. úroveň rizika je vysoká, že útočník uhádne slovníkové heslo (napr. 123456) k administrátorskému účtu a následky budú veľmi negatívne, napr. poskytovateľ príde o zákazníkov. A naopak, niečo čo je málo pravdepodobné, t. j. úroveň rizika je nízka, napr. asteroid dopadne na záložné dátové centrum práve vo chvíli, keď to prvé zaplavila povodeň a následky budú katastrofálne (koniec biznisu).

Riziká môžu tiež vzájomne interagovať alebo agregovať. Môžu napríklad existovať dve riziká s relatívne nízkou mierou pravdepodobnosti a len nízkymi dopadmi, je však možné, že sa vyskytnú spoločne a potom výsledná kombinácia ich následkov bude

dramaticky vysoká. Napríklad dopad zlyhania jednej vetvy redundantného elektrického vedenia môže byť zanedbateľný, ale dopad zlyhania oboch vetiev môže byť naozaj zlý.

Vychádzajúc zo záverov množstva výskumov [IMZ16, KZ15] realizovaných v rokoch 2015 a 2016, možno vo všeobecnosti identifikovať niekoľko kritických rizík spojených s využívaním cloudu.

Únik údajov: Citlivé interné údaje organizácie sa môžu dostať do rúk konkurencie v dôsledku útokov postranným kanálom na virtuálnych strojoch. Napríklad útok môže byť navrhnutý tak, aby extrahoval súkromné kryptografické kľúče, ktoré sa používajú v iných virtuálnych strojoch umiestnených na rovnakom fyzickom serveri (rovnakom virtualizačnom podklade).

Strata údajov: O uložené údaje je možné prísť v dôsledku napríklad náhodného vymazania, straty šifrovacieho kľúča alebo fyzickej katastrofy, ako je povodeň, zemetrasenie, požiar atď.

Zneužitie účtu alebo služby: Phishing, podvody a zneužívanie softvérových zraniteľností uľahčujú útočníkom prístup k údajom o zákazníkoch, čo pomáha spustiť následné útoky.

Nezabezpečené rozhrania a API: API (Application Programming Interface) je sada protokolov a štandardov, ktoré definujú komunikáciu medzi softvérovými aplikáciami cez internet. Cloud API sa používajú na všetkých úrovniach infraštruktúry, platforiem a softvérových služieb na komunikáciu s inými službami. API pre model IaaS sa používajú na prístup a správu zdrojov infraštruktúry vrátane sietí a virtuálnych počítačov. API pre model PaaS poskytuje prístup k cloudovým službám, ako je napríklad úložisko. API pre model SaaS spája softvérové aplikácie s cloudovou infraštruktúrou. Zabezpečenie rôznych cloudových služieb závisí od zabezpečenia rozhraní API. Slabá sada API a rozhraní môže mať za následok veľa problémov so zabezpečením v cloude. Poskytovatelia cloudu vo všeobecnosti poskytujú svoje API tretím stranám na poskytovanie služieb zákazníkom. Slabé rozhrania API však môžu viesť k tomu, že tretia strana bude mať prístup k bezpečnostným kľúčom a kritickým informáciám v cloude. Pomocou bezpečnostných kľúčov je možné šifrované údaje zákazníka v cloude čítať, čo vedie k strate integrity, dôvernosti a dostupnosti dát. Zásady autentifikácie a riadenia prístupu môžu byť navyše porušené aj prostredníctvom nezabezpečených API.

Odmietnutie služby: Útočníci generujú obrovské množstvo falošných požiadaviek na určitý cloudový server, takže server je nútený spotrebovávať výkon procesora, pamäť, miesto na disku a šírku pásma siete. To nakoniec spôsobí spomalenie systému až za hranicu použiteľnosti a zabráni ostatným zákazníkom v používaní služby.

Zlomyseľný útočník zvnútra: Zlomyseľný útočník zvnútra (insider) je niekto, kto je zamestnancom cloudovej organizácie alebo obchodným partnerom s prístupom ku cloudovej sieti, aplikáciám, službám alebo údajom a zneužíva svoj prístup na vykonávanie neprivilegovaných aktivít. Správcovia cloudu sú zodpovední za správu

a údržbu kompletného prostredia. Majú prístup k väčšine údajov a zdrojov a môžu nakoniec zneužiť svoj prístup k vyneseniu týchto údajov.

Nedostatočná obvyklá opatrnosť (due diligence): Pojem due diligence pochádza z amerického práva a tamojšej praxe pri uzatváraní zmlúv. V preklade znamená obvyklú opatrnosť a starostlivosť vynakladanú v obchodnom styku podnikateľov. V európskych krajinách sa pod termínom due diligence rozumie najmä hĺbková previerka podniku v súvislosti s potenciálnou obchodnou transakciou akou môže byť napríklad kúpa akcií podniku [C10]. Cloud computing ponúka rozsiahle možnosti výpočtových zdrojov a rýchly prístup, vďaka čomu sa množstvo firiem presunie do cloudu bez toho, aby vyhodnotili riziká s ním spojené. Nedostatočné porozumenie prostredia poskytovateľa služieb a nesprávne posúdenie prevádzkových vstupov a výstupov môže viesť k tomu, že organizácia sa dostane do kritickej situácie. Z dôvodu komplexnej architektúry cloudu nie je možné v cloude použiť rovnakú bezpečnostnú politiku ako pred migráciou do cloudu. Zákazníci cloudu navyše nemajú predstavu o interných bezpečnostných postupoch, audite, logovaní, ukladaní dát a prístupe k nim, čo vedie k vytvoreniu neznámych rizík v cloude. V niektorých prípadoch si vývojári a dizajnéri aplikácií ani neuvedomujú možné efekty nasadenia ich aplikácií do cloudu, ktoré môžu vyústiť do prevádzkových a architektonických problémov.

Zraniteľnosti zdieľaných technológií: Cloud computing ponúka poskytovanie služieb zdieľaním infraštruktúry, platformy a softvéru. Rôzne komponenty však nemusia dostatočne napĺňať bezpečnostné požiadavky cloudu na dokonalú izoláciu. V posledných rokoch boli útočníkmi pri útokoch na cloud zneužité zraniteľnosti v technológiách zdieľania zdrojov. Jedným takýmto útokom je získanie prístupu k hypervízoru s úmyslom spustiť škodlivý kód, získať neoprávnený prístup ku cloudovým zdrojom, virtuálnym strojom a dátam zákazníkov. Zraniteľné miesta hypervízora, útoky na postranné kanále virtuálnych strojov, rozrastanie VM (VM sprawl) a mnoho ďalších možných hrozieb v dôsledku zdieľanej architektúry viacerých nájomcov môžu vystaviť celé prostredie kompromitácii.

Strata kontroly: Prenos údajov do cloudu znamená prenos kontroly na poskytovateľa cloudových služieb. V mnohých prípadoch to môže mať dopad na bezpečnosť.

Uzamknutie: Keďže neexistuje všeobecný štandard pre prenositeľnosť dát a služieb, závislosť od konkrétneho poskytovateľa cloudových služieb často sťažuje prechodu klienta od jedného poskytovateľa k inému.

Nedostatočne bezpečné zmazanie dát: Vymazanie dát z cloudového úložiska nezaručuje, že v budúcnosti nebudú tieto údaje znovu prístupné. V skutočnosti, ak poskytovateľ cloudovej služby dáta cielene bezpečne nezmaže alebo ak dáta nie sú šifrované priamo klientom, mohli by byť neskôr obnovené.

Reťazec dostupnosti: Poskytovateľ cloudových služieb môže delegovať časť svojej práce na tretiu stranu (subdodávateľa) alebo dokonca môže využiť službu iného

poskytovateľa služieb. Vytvára sa tak potenciál pre kaskádové zlyhanie, ktoré môže ovplyvniť dostupnosť služieb.

Zneužívanie cloudových služieb: Pojem zneužívanie cloudových služieb sa týka zneužívania cloudových služieb spotrebiteľmi. Väčšinou sa používa na popis akcií používateľov cloudu, ktoré sú nezákonné, neetické alebo porušujú ich zmluvu s poskytovateľom služieb. Výskum ukázal, že niektorí poskytovatelia cloudu nedokážu zistiť útoky spustené zo svojich sietí, v dôsledku čoho nie sú schopní generovať výstrahy alebo zastaviť útoky. Zneužívanie cloudových služieb je pre poskytovateľa služieb vážnejšou hrozbou ako pre používateľov služieb. Napríklad šírenie spamu z kompromitovaných virtuálnych strojov v cloude malo za následok zapísanie všetkých IP adries poskytovateľa cloudu na blacklist čo malo negatívny dopad na všetkých klientov poskytovateľa. Poskytovateľ služieb teda musí implementovať maximálne možné opatrenia na zabránenie týmto hrozbám.

V priebehu rokov boli škodlivými používateľmi prostredníctvom cloudu spustené rôzne útoky. Napríklad, Amazon EC2 služby boli použité ako riadiace servery pre botnet Zeus v roku 2009. Známe cloudové služby ako Twitter, Google a Facebook poslúžili ako riadiace servery na spustenie trójskych koní a botnetov. Ďalšími útokmi, ktoré boli spustené pomocou cloudu, sú útok hrubou silou na heslo, phishing, útok DoS a DDoS proti webovej službe, cross site scripting a SQL injection.

Cloud Security Alliance (CSA)[22], organizácia združujúca spoločnosti a odborníkov pôsobiacich v oblasti cloudových technológií, vypracovala v roku 2017 analýzu aktuálnych bezpečnostných problémov. Experti CSA identifikovali nasledujúcich 12 kritických problémov (zoradených podľa závažnosti podľa výsledkov výskumu):

1. Narušenie bezpečnosti dát (Data Breaches)
2. Slabý manažment riadenia prístupu (Weak Identity, Credential and Access Management)
3. Bezpečnostné chyby v API (Insecure APIs)
4. Zraniteľnosti na úrovni systému a aplikácií (System and Application Vulnerabilities)
5. Zneužitie účtu (Account Hijacking)
6. Zlomyseľní útočníci zvnútra (Malicious Insiders)
7. Pokročilá a trvalá hrozba (APTs, Advanced Persistent Threats)
8. Strata dát (Data Loss)
9. Nedostatočná obvyklá opatrnosť (Insufficient Due Diligence)

22 https://cloudsecurityalliance.org/

10. Zneužitie a nezákonné použitie cloudových služieb (Abuse and Nefarious Use of Cloud Services)
11. Útok odmietnutím služby (Denial of Service)
12. Zraniteľnosti v technológiách zdieľania (Shared Technology Vulnerabilities)

V roku 2019 analýzu zopakovali a dostali sa k mierne odlišným výsledkom, opäť zoradené podľa závažnosti:

1. Narušenie bezpečnosti dát (Data Breaches)
2. Chyba v konfigurácii a nedostatočná kontrola zmien (Misconfiguration and Inadequate Change Control)
3. Nedostatky v návrhu bezpečnostnej architektúry cloudu (Lack of Cloud Security Architecture and Strategy)
4. Nedostatočný manažment riadenia prístupu a správy kľúčov (Insufficient Identity, Credential, Access and Key Management)
5. Zneužitie účtu (Account Hijacking)
6. Hrozba od útočníkov zvnútra (Insider Threat)
7. Nezabezpečené rozhrania a API (Insecure Interfaces and APIs)
8. Slabá úroveň kontroly (Weak Control Plane)
9. Zlyhania metaštruktúry a štruktúry aplikácií (Metastructure and Applistructure Failures)
10. Neprehľadné používanie cloudových služieb (Limited Cloud Usage Visibility)
11. Zneužitie a nezákonné použitie cloudových služieb (Abuse and Nefarious Use of Cloud Services)

Cloud Security Alliance publikuje tieto reporty s cieľom zvyšovať povedomie o kritických bezpečnostných problémoch, ako sú narušenie údajov, nesprávna konfigurácia a správa identity a prístupu. Ostatné hrozby poukazujú na problémy nedostatočnej kontroly, napríklad pri multicloudových službách, neprehľadnosť aká časť služby beží v akom cloude. Cloud je svojou komplexnosťou miestom, kde útočník ľahko ukryje svoju prítomnosť, ako aj svoje ďalšie aktivity.

O tom, že sú riziká úniku dát z cloudu reálne sa presvedčilo množstvo spoločností. V roku 2019 spoločnosť Voipo, telekomunikačná spoločnosť, ktorá poskytuje služby Voice over Internet Protocol (VoIP), neúmyselne sprístupnila do Internetu milióny protokolov hovorov zákazníkov, textových správ (SMS) a ďalších dokumentov. Mnoho súborov obsahovalo podrobné záznamy hovorov (kto s kým volal, čas volania atď.). Celkovo spoločnosť Voipo sprístupnila viac ako 7 miliónov protokolov hovorov, 6 miliónov textových správ a ďalšie interné dokumenty obsahujúce nezašifrované heslá,

ktoré, ak sa použijú, by mohli útočníkovi umožniť získať prístup do vnútorných podnikových systémov.

V roku 2018 spoločnosť Level One Robotics, inžinierska spoločnosť špecializujúca sa na priemyselnú automatizáciu, sprístupnila vysoko citlivé patentové informácie, ktoré patria viac ako 100 výrobným spoločnostiam (Volkswagen, Chrysler, Ford, Toyota, General Motors, Tesla a ThyssenKrupp a ďalšie). V tomto prípade chybne nakonfigurovanou službou bol rsync server, ktorý umožňoval neautentifikovaný prenos údajov akémukoľvek rsync klientovi.

28. septembra 2018 Facebook oznámil významný únik dát o viac ako 50 miliónov účtov. Podľa správy bola do kódu Facebooku v júli 2017, teda viac ako o rok skôr, zanesená zraniteľnosť umožňujúca krádež prístupových údajov. Spoločnosť pripustila, že nevedela, aké informácie boli ukradnuté, ani koľko ďalších používateľských účtov bolo v dôsledku úniku ohrozených.

V roku 2017 technologický a cloudový gigant spoločnosť Accenture priznal, že neúmyselne zanechal obrovské dátové úložiská s citlivými dátami v štyroch nezabezpečených Amazon Web Services S3 storage bucket, čím odhalil vysoko citlivé heslá a šifrovacie kľúče, ktoré mohli spôsobiť značnú škodu spoločnosti a jej zákazníkom. Dáta mohol bez hesla stiahnuť každý, kto poznal webové adresy S3 bucketov.

Účtovná firma Deloitte priznala závažný únik dát 25. septembra 2017. Spoločnosť oznámila, že zistila kompromitáciu svojho globálneho e-mailového servera z dôvodu zle zabezpečeného e-mailového účtu správcu. Ku kompromitácii došlo v marci 2017 a údajne poskytoval útočníkom privilegovaný a neobmedzený prístup „do všetkých oblastí“. Účet správcu vyžadoval iba jedno heslo. 244 000 zamestnancov spoločnosti Deloitte využíva cloudovú službu Microsoft Azure na ukladanie prichádzajúcich a odchádzajúcich e-mailov. Okrem e-mailov útočníci mohli mať potenciálny prístup k používateľským menám, heslám a zdravotným informáciám. Niektoré e-maily obsahovali prílohy s citlivými údajmi o zabezpečení a dizajne.

V apríli 2010, chyba XSS na serveroch Amazon umožnila krádež prístupových údajov.

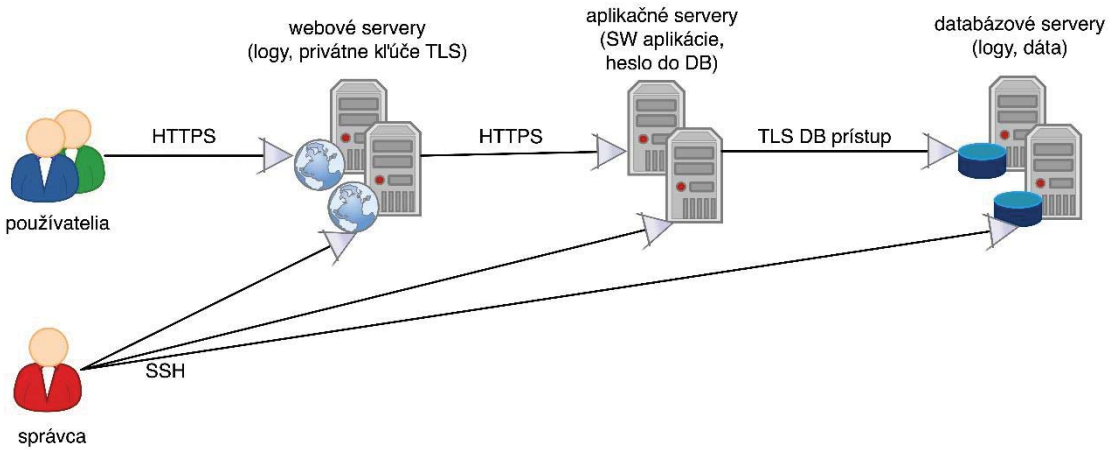
Po získaní predstavy o známych rizikách je možné:

- predísť riziku, napríklad vypnúť službu, ktorú nie je možné zabezpečiť
- zmierniť riziko, napríklad obmedziť prístup na administrátorský účet len z administrátorovho zabezpečeného počítača
- presunúť riziko na iný subjekt, ktorému sa za to zaplatí
- prijať riziko, po analýze celkovej úrovne rizika sa rozhodnúť akceptovať riziko a nepodnikať ďalšie opatrenia.

Ktorýkoľvek z uvedených krokov môže byť rozumný. Základnou podmienkou však je absolvovať analýzu rizík a zváženie ich následkov.

Identifikácia aktív

Vo všeobecnosti, aktívum je čokoľvek, čo má hodnotu pre jednotlivca, organizáciu alebo verejnú správu. V rámci risk manažmentu je potrebné identifikovať a klasifikovať aktíva. V prostredí cloudu môžeme za aktíva považovať jednak dáta (od informácií o zákazníkoch, prístupové údaje, logy, až po dáta zákazníkov), ako aj cloudové technológie, pomocou ktorých sa s dátami pracuje (dátové úložiská, fyzické aj virtuálne servery a pod.). Zjednodušene sú to *dátové aktíva* a *cloudové aktíva*.



Obrázok 0-2 Identifikované aktíva a zodpovednosť za ne v rámci jednoduchého modelu webovej aplikácie.

Pre získanie predstavy o dátových aktívach je možné vychádzať z obrázku, ktorý ukazuje jednoduchý model webovej aplikácie, Obrázok 0-2. Počas analýzy sa identifikujú napríklad nasledovné dátové aktíva:

- logy na webovom serveri, ktoré môžu obsahovať informácie identifikujúce návštevníka stránky
- softvér aplikácie
- konfiguračné súbory webovej aplikácie, ktoré obsahujú prístupové údaje do databázy
- privátny kľúč TLS certifikátu na webovom serveri
- dáta v databáze, ktoré obsahujú aj prístupové údaje administrátora webovej aplikácie a ďalších registrovaných používateľov, ako aj všetky ďalšie dáta, ktoré aplikácia spracováva.

Vzhľadom na to, že zdroje nie sú neobmedzené, je potrebné aktíva zoradiť, klasifikovať ich. Každá organizácia je iná, ale nasledujúce pravidlá poskytujú dobrý a jednoduchý východiskový bod na posúdenie hodnoty dát, a teda aj riziko narušenia ich bezpečnosti:

1. *nízke*, aj keď informácie v tejto kategórii môžu alebo nemusia byť určené na zverejnenie, ak by boli zverejnené, vplyv na organizáciu by bol veľmi nízky alebo zanedbateľný. Niekoľko príkladov:

- verejné adresy IP serverov,
- aplikačné logy bez citlivých údajov.

2. *stredné***,** tieto informácie by sa nemali zverejňovať mimo organizácie bez riadnych dohôd o mlčanlivosti. V mnohých prípadoch (najmä vo väčších organizáciách) by sa tento typ údajov mal zverejňovať iba na základe nevyhnutných informácií v rámci organizácie. Vo väčšine organizácií bude väčšina informácií spadať do tejto kategórie. Niekoľko príkladov:

    - podrobné informácie o tom, ako sú navrhnuté informačné systémy, ktoré môžu byť pre útočníka užitočné,
    - informácie o personáli, ktoré by mohli útočníkom poskytnúť informácie potrebné pri útokoch typu phishing alebo scam.

3. *vysoké*, tieto informácie sú pre organizáciu životne dôležité a ich zverejnenie by mohlo spôsobiť značné škody. Prístup k týmto údajom by mal byť obmedzený a mal by obsahovať viac bezpečnostných opatrení. Niekoľko príkladov:

    - informácie o budúcej stratégii alebo finančné informácie, ktoré by poskytovali významnú výhodu pre konkurentov,
    - obchodné tajomstvá,
    - prístupové údaje administrátorov,
    - citlivé informácie zákazníkov

Treba poznamenať, že zákony a priemyselné regulácie môžu účinne určovať, ako klasifikovať niektoré informácie. Napríklad všeobecné nariadenie Európskej únie o ochrane údajov (GDPR, General Data Protection Regulation) má mnoho rôznych požiadaviek na zaobchádzanie s osobnými údajmi, takže pomocou tohto nariadenia by sa mohli klasifikovať všetky osobné údaje ako „stredné“ riziká a podľa toho ich chrániť. Toto nariadenie sa môže vzťahovať na osobné údaje ktoréhokoľvek občana Európskej únie alebo Európskeho hospodárskeho priestoru bez ohľadu na to, kde vo svete sa údaje nachádzajú. GDPR vyžaduje, aby sa katalogizovali, chránili a auditoval prístup k „všetkým informáciám, ktoré sa týkajú identifikovateľnej osoby, ktorú možno priamo alebo nepriamo identifikovať najmä odkazom na identifikátor.“

Niektorí poskytovatelia cloudových služieb poskytujú doplnkové služby, ktoré môžu pomôcť pri klasifikácii a ochrane údajov. Napríklad Amazon ponúka Amazon Macie. Macie je bezpečnostná služba, ktorá využíva strojové učenie na automatické vyhľadávanie, klasifikáciu a ochranu citlivých údajov v AWS. Macie rozpoznáva citlivé údaje, ako sú informácie umožňujúce identifikáciu osôb (PII, Personally Identifiable Information) alebo duševné vlastníctvo. Zákazník má k dispozícii dashboard s informačnými panelmi a výstrahami, ktoré poskytujú prehľad o tom, ako sa k týmto údajom pristupuje alebo ako sa presúvajú.

Bez ohľadu na to, aký klasifikačný systém dát sa použije, je dôležité opísať definíciu každej klasifikačnej úrovne a jej príklady. Ďalej je dôležité, aby každý, kto vytvára, zhromažďuje alebo chráni údaje, rozumel tomuto klasifikačnému systému.

Cloudové aktíva zahŕňajú prvky technológií pre prenos, spracovanie a ukladanie dát používané v cloude. Záleží, či sa zákazník rozhodne pre IaaS, PaaS alebo SaaS. Vo všeobecnosti je možné za cloudové aktíva orientované na prenos považovať:

- *Siete na doručovanie obsahu* (CDN, Content Delivery Network), ktoré sa využívajú na globálne šírenie obsahu. Samotný obsah zvyčajne neobsahuje utajované dáta. Prípadný útočník však môže obsah pozmeniť, doplniť ho o malvér s cieľom ťažiť crypto meny, získať citlivé informácie o obetiach a následne ich vydierať, alebo k ďalším útokom, napríklad k útoku distribuovaným odmietnutím služby (DDoS, distributed denial-of-service).
- *DNS záznamy*, ktoré tiež nie sú utajené. Prípadný útočník ich však môže pozmeniť tak, aby ukazovali na jeho server, ktorý imituje vzhľad a správanie originálneho servera. Cieľom môže byť krádež prípadne zmena dát, ktoré návštevník v dobrej viere pošle na útočníkov server miesto na originálny server.
- *TLS certifikáty* a *súkromné kľúče*. TLS certifikát od dôveryhodnej certifikačnej autority je najlepším spôsobom ako sa chrániť pred podvrhnutím útočníkovho servera. Preto je certifikát s privátnym kľúčom zaujímavým cieľom pre útočníka. S ukradnutým certifikátom sa podvrhnutý server útočníka stáva dôveryhodným.
- *Prvky pre sieťovú bezpečnosť*. Virtualizované firewally, WAF (Web Application Firewall) a ďalšie aplikačné brány, virtuálne prepínače, smerovače. Ale aj reverzné proxy a load balancery. Jedná sa o ekvivalenty fyzických zariadení.

Podobne cloudové aktíva orientované na úložiská vo všeobecnosti zahŕňajú nasledovné:

- *Blokové úložiská*, ktoré sú cloudovou verziou hard disku v počítači. Napríklad AWS Elastic Block Storage, Azure Virtual Disks alebo Google Persistent Disks.
- *Súborové úložiská* sú cloudovým ekvivalentom súborového systému. Komerčne dostupné príklady sú AWS Elastic File System, Azure Files, Google Cloud Storage FUSE.
- *Obrazy*. Jedná sa o dávku informácií zahŕňajúcu všetko čo je potrebné pre spustenie virtuálneho počítača (vrátane operačného systému), kontajneru, alebo aplikačnej platformy (PaaS deployment). Pri spustení sa najskôr vytvorí kópia obrazu označovaná ako inštancia, a tá sa spustí. Ak je to možné, obrazy by nemali obsahovať citlivé informácie ako heslá alebo kľúče k API, pretože nie každý kto má oprávnenie na vytvorenie obrazu alebo jeho editáciu má zároveň aj oprávnenie pre prístup k citlivým informáciám. Obraz by mal byť

nakonfigurovaný tak, aby pri spustení jeho kópie, táto kópia zároveň získala aj citlivé informácie zo zabezpečeného umiestnenia, ku ktorému je obmedzený prístup.

- *Cloudová databáza*. Zjednodušene je možné hovoriť o relačných a nerelačných databázach. Väčšina cloudových poskytovateľov ponúka niekoľko rôznych variantov relačných aj nerelačných databáz. Všetky cloudové databázy môžu poskytovať riadenie prístupu na databázovej vrstve a niektoré databázy môžu poskytovať jemnejšiu kontrolu dát v databáze. Výber databázy môže mať výrazný vplyv na bezpečnosť celej aplikácie. Napríklad niektoré databázy zabudované v pamäti, ktoré sa používajú na rýchly výkon, natívne neponúkajú šifrovanie, čo môže byť v závislosti od typu uložených dát riziko.
- *Špeciálne úlo*žiská ako napríklad úložisko certifikátov, úložisko hesiel a podobne. Charakteristické pre ne je, že obsahujú kritické dáta. Kompromitácia môže kaskádovo viesť ku kompromitácii všetkých zákazníkov poskytovateľa cloudových služieb.

Výpočtové aktíva spravidla zoberú dáta, spracujú ich a pošlú ďalej. Orientujú sa na spracovanie dát. Vo všeobecnosti ide o:

- *Virtuálne počítače* (VM, Virtual Machine, ale aj VPS, Virtual Private Server) sú najznámejším cloudovým aktívom. V porovnaní s fyzickým počítačom je virtuálny odlišný v jednom zásadnom bode, virtuálne stroje rôznych zákazníkov bežia na rovnakom fyzickom systéme. Toto môže viesť k tomu, že jeden zákazník využívajúci všetok procesorový čas, sieťovú kapacitu a prenosovú kapacitu úložiska ovplyvní výkon virtuálnych strojov ostatných zákazníkov. Virtuálny stroj má vždy vlastný operačný systém, na ktorom sú nainštalované aplikácie poskytujúce požadované služby. Toto prináša potrebu riešiť prípadné zraniteľnosti (Vulnerability Management), správu používateľov a ich oprávnení (Access Management) a správu konfigurácií (Configuration Management).
- *Kontajnery*, podobne ako virtuálne počítače na nich beží kód aplikácií (napríklad webová aplikácia, databázová aplikácia). Na rozdiel od virtuálnych strojov však neobsahujú operačný systém. Kontajnery zdieľajú jadro operačného systému virtuálneho stroja na ktorom bežia. Jedným z najznámejších kontajnerových systémov je Docker a systém na správu kontajnerov Kubernetes. Pri nasadzovaní Kubernetes sú primárnymi aktívami klastre na ktorých bežia pod-y (zoskupenie kontajnerov, ktoré zdieľa úložisko, sieť a špecifikáciu pre spustenie kontajneru), v rámci ktorých bežia kontajnery, na ktorých bežia Docker kontajnery, ktoré sú bežiacimi kópiami obrazov.
- *aPaaS* – application-Platform-as-a-Service umožňuje nasadiť kód aplikácie bez nutnosti riešiť virtuálny stroj. Príkladom komerčne dostupných služieb je

AWS Elastic Beanstalk. Klient dodá webovú aplikáciu, ktorá beží v cloude a využíva služby cloudovej databázy. Pri tomto aktíve je bezpečnosť veľmi špecifická vzhľadom na to, že aplikácia zákazníka beží na tom istom virtuálnom stroji ako aplikácie iných zákazníkov.

- *Bezseverové funkcie* (serverless) sú spôsobom ako spustiť kód len keď je treba. Príkladom sú AWS Lambda, Azure Functions alebo Google Cloud Functions. Ponuky serverless funkcií sa líšia od ponúk aPaaS v tom, že v cloude zákazníkovi nič nebeží, kým nepríde požiadavka o jeho službu. To znamená, že zákazník nemusíte riešiť obrazy, inštancie, virtuálne stoje, ani kontajnery, pretože neexistujú žiadne dlhodobé inštancie. Aktívami v serverless je len kód samotnej funkcie. A rieši sa len zraniteľnosť v kóde a prístup k funkcii.

Možnosti ochrany aktív

Väčšina poskytovateľov cloudu, podobne ako systémy na správu kontajnerov, akým je napríklad Kubernetes, používajú koncept tagov (značiek). Tag je zvyčajne kombináciou mena alebo kľúča a hodnoty. Tagy sa dajú použiť na mnohé účely, od kategorizácie zdrojov v inventári, cez rozhodnutia o prístupe, až po určenie reakcie na definovanú udalosť, resp. incident. Príkladom tagu je:

- datatype = PII.

Názov kľúča je v tomto príklade "datatype" a jeho hodnota je PII (Personally Identifiable Information). Potom každý zdroj, ktorý má priradený tento tag je treba chrániť ako aktívum, pomocou ktorého je možné identifikovať osobu. Tagovaním je možné vyjadriť aj klasifikáciu aktíva:

- dataclass = low,
- dataclass = moderate,
- dataclass = high.

Pre používanie tagov je dôležité, aby sa používala jednotná sada tagov naprieč organizáciou. Sada musí obsahovať vysvetlenie každého tagu, aby nedošlo k nesprávnemu použitiu tagu. Poskytovatelia cloudu zvyčajne umožňujú vytvoriť 15 až 64 tagov pre jeden cloudový zdroj. Niektorí poskytovatelia poskytujú možnosť automatickej kontroly správnej aplikácie tagov na zdroje. Vďaka tomu je možné odhaliť netagované alebo nesprávne tagované zdroje.

Šifrovanie je jedným z najúčinnejších nástrojov na ochranu dátových aktív. Dáta môžu byť zašifrované:

- počas prenosu cez sieť (napríklad SSH, HTTPS),
- počas spracovania (šifrovaná operačná pamäť),
- počas uloženia na dátovom úložisku (zašifrovaný súbor, databáza, atď.).

Šifrovaniu ako ochrane dát počas prenosu sa venovalo miesto v časti Sieťová bezpečnosť. Problematika ochrany spracovávaných dát šifrovaním je v oblasti cloudov

relatívne nová. Nejde však o novú myšlienku. Tvorcovia operačného systému OpenBSD prišli už v roku 2000 s myšlienkou šifrovania virtuálnej pamäte[23]. Od verzie 3.9 je virtuálna pamäť rozdelená na mnoho malých blokov, pričom každý je zašifrovaný vlastným kľúčom. Ak dáta v bloku už nie sú potrebné, zmaže sa príslušný šifrovací kľúč.

Niektorí poskytovatelia cloudu (Amazon Web Services, Google Compute Platform a ďalší) poskytujú službu správy kľúčov (KMS, Key Management Service). KSM využíva dve úrovne šifrovacích kľúčov:

- kľúč na šifrovanie dát (data encryption key),
- kľúč na šifrovanie kľúčov (key encryption key).

Zašifrovaný kľúč na šifrovanie dát je uložený pri zašifrovaných dátach. Prácu s kľúčmi je možné zjednodušene opísať nasledovne: keď je treba dáta šifrovať, zašifrovaný kľúč na šifrovanie dát sa pošle do KSM, kde je dešifrovaný pomocou kľúča na šifrovanie kľúčov. Dešifrovaný kľúč sa následne použije pri šifrovaní dát. Po skončení šifrovacích operácií sa kľúč zabudne. Používanie KSM niektorí poskytovatelia cloudu označujú aj ako šifrovanie na strane servera (Server-side Encryption). Výhodou je prenesenie zodpovednosti na stranu poskytovateľa. Zároveň je možné využívať aj ďalšie služby poskytovateľa ako je vyhľadávanie v dátach, indexovanie dát, testovanie dát antivírusovým programom a podobne. Na druhej strane, chyba v službe dátového úložiska potenciálne umožňuje neoprávnenému používateľovi požiadať službu dátového úložiska o dešifrovanie dát. Z toho dôvodu je šifrovanie vo vlastnej réžii, označované aj ako šifrovanie na strane klienta (client-side encryption), považované za bezpečnejšie. Dáta sú odosielané do cloudu už zašifrované a poskytovateľ ich nemôže prečítať pretože nemá šifrovacie kľúče. Nevýhodou šifrovania je to, že môže znížiť výkon v dôsledku dodatočného času potrebného na šifrovanie a dešifrovanie údajov.

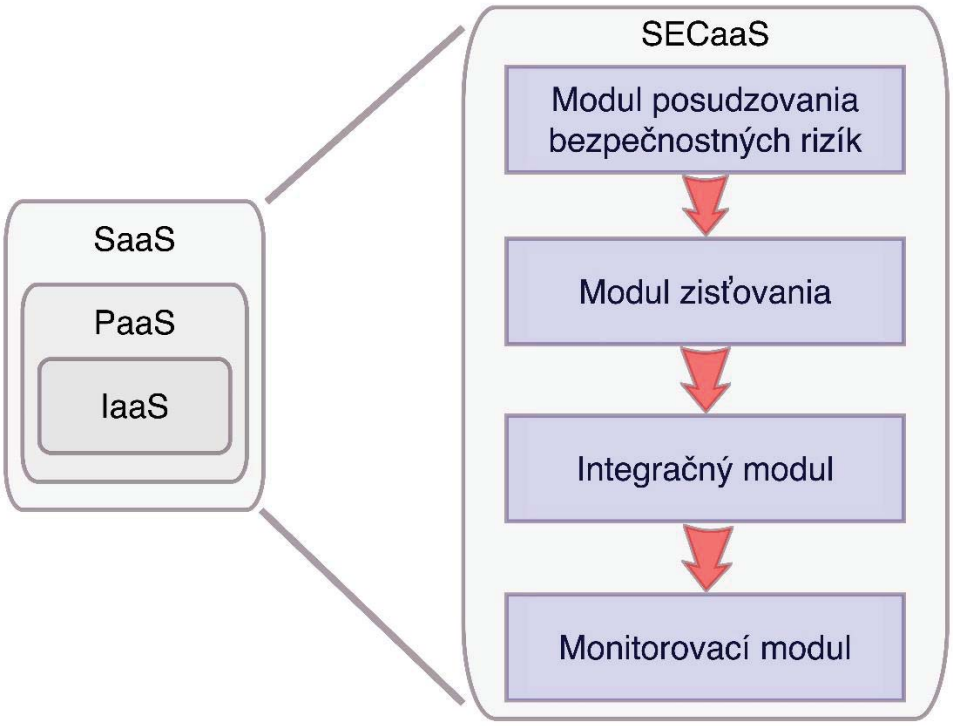
Security-as-a-Service (SECaaS) v Cloude

19. júna 2011 používatelia Dropboxu zistili, že sa na svoje účty dostanú aj po zadaní nesprávneho hesla. Je nevyhnutné pochopiť, aké sú možnosti ochrany dát a zdrojov pred narušením bezpečnosti v cloude, ktorý poskytuje zdieľané platformy a služby. Je veľmi dôležité mať k dispozícii vhodné mechanizmy, ktoré bránia poskytovateľom cloudových služieb využívať údaje zákazníkov spôsobom, ktorý nebol zmluvne dohodnutý. Za účelom splnenia kritických bezpečnostných požiadaviek používania cloudových služieb sa v niekoľkých posledných rokoch vynaložilo veľké úsilie na navrhovanie bezpečnostných služieb, ktoré by sa mohli poskytovať ako cloudové služby v modeli *Security-as-a-Service* (SECaaS). Niektoré zo služieb, ktoré ponúkajú poskytovatelia SECaaS svojim zákazníkom, sú systémy detekcie narušenia a systémy prevencie pred prienikom (Barracuda, CheckPoint), antivírusové programy a antimalware (Eset, McAfee), bezpečnosť e-mailov (Proofpoint), ochrana webových aplikácií (Oracle Cloud

23 https://www.openbsd.org/papers/swapencrypt.ps

WAF, BigIP F5), správa identít a prístupov (okta, Oracle IAM), šifrovanie (Oracle key management), monitorovanie integrity a správa udalostí (SIEM, Splunk), atď.

Tieto bezpečnostné služby majú veľký vplyv na bezpečnosť spoločností akejkoľvek veľkosti a prinášajú výhody, ktoré by inak neboli dostupné najmä pre malé firmy. SECaaS umožňuje dodávať bezpečnostné kontroly a funkcie novými spôsobmi. Spoločnostiam tiež umožňuje používať aj také bezpečnostné technológie, ktoré by inak boli pre ne cenovo nedostupné. SECaaS tak umožňuje zníženie nákladov na bezpečnostné kontroly a riešenie nových bezpečnostných problémov, ktoré prináša cloudové prostredie.



Obrázok 0-3 Security-as-a-Service [ZCD+17].

Aby sa SECaaS považovala za praktickú cloudovú službu, musí zákazníkom poskytovať možnosť vytvoriť si vlastné bezpečnostné politiky a rámec riadenia rizík. Zákazníci cloudových služieb musia byť schopní charakterizovať, hodnotiť, merať a určovať priority svojich systémových rizík. Poskytovatelia cloudu musia ponúkať bezpečnostné služby nezávislé od akejkoľvek platformy a prispôsobiteľné neustále sa meniacim cloudovým prostrediam a tiež zabezpečiť, aby ich bezpečnostné opatrenia neboli príliš zložité na efektívne uplatňovanie. Pred použitím cloudovej služby musia zákazníci určiť, aké bezpečnostné opatrenia poskytuje a aké ďalšie bezpečnostné služby sú potrebné na riešenie prípadnej zraniteľnosti. Zákazníci môžu na základe týchto analýz identifikovať bežné bezpečnostné služby, ktoré môžu zveriť poskytovateľom služieb. V závislosti od modelu poskytovania cloudu sa cloudová služba môže porovnávať so súborom bezpečnostných ovládacích prvkov, aby sa určilo, ktoré ovládacie prvky už

existujú, poskytované spotrebiteľom alebo poskytovateľom cloudových služieb a ktoré ovládacie prvky je potrebné požadovať od iných poskytovateľov cloudových služieb.

Ako ukazuje Obrázok 0-3 navrhovaný rámec obsahuje štyri hlavné komponenty: modul posudzovania rizika, modul zisťovania, integračný modul a monitorovací modul.

Modul posudzovania bezpečnostných rizík je zodpovedný za identifikáciu a vyhodnotenie rizík a dopadov rizika a za odporúčanie bezpečnostných kontrol na riešenie týchto rizík. Prostredníctvom komplexnej analýzy rizík zákazník identifikuje, aké bezpečnostné kontroly a aplikácie sú potrebné na zabezpečenie organizácie. Potom zákazník určí, ktorá bezpečnostná aplikácia sa bude prevádzkovať na lokálnych systémoch zákazníka a aké bezpečnostné aplikácie budú bežať u poskytovateľov cloudových služieb.

Modul zisťovania je určený na nájdenie vhodných poskytovateľov služieb, ktorí poskytujú požadované bezpečnostné služby identifikované modulom na posudzovanie bezpečnostných rizík. To je možné dosiahnuť pomocou verejného repozitára zoznamu služieb a ich funkcií, ku ktorým majú zákazníci prístup. Pri hľadaní vhodných služieb by sa mali brať do úvahy interoperabilita, najnižšie náklady a kvalita výstupných reportov. Tento modul umožňuje zákazníkom porovnávať služby, ktoré ponúkajú rôzni poskytovatelia cloudu, a získať referencie na vybraných poskytovateľov. Výstupom modulu je skupina bezpečnostných služieb, pravdepodobne od rôznych poskytovateľov cloudových služieb.

Následne *integračný modul* prispôsobí vybrané bezpečnostné služby a integruje ich do konečného bezpečnostného riešenia. Výstupom tohto modulu je bezpečnostná architektúra systému, ktorá zahŕňa orchestráciu množstva bezpečnostných prvkov pokrývajúcich rôzne aspekty bezpečnosti.

Monitorovací modul je zodpovedný za nepretržité monitorovanie bezpečnostných služieb. Je to služba monitorovania bezpečnosti v reálnom čase. Monitoruje záväzky SLA. Zodpovedá tiež za riadenie kontinuity činnosti (business-continuity) a zvládanie incidentov. Aby sa zabezpečila kontinuita, mali by sa zvážiť problémy, ako sú priority obnovy, t. j. priority zákazníka týkajúce sa toho, čo sa má obnoviť v prípade incidentu, a závislosti, t. j. v akom poradí obnova prebieha. Správa incidentov a reakcia na ne sú súčasťou riadenia kontinuity činnosti. Cieľom tohto procesu je obmedziť dopad neočakávaných a potenciálne rušivých udalostí na úroveň akceptovateľnú organizáciou.

Trh SECaaS mal už v roku 2016 hodnotu viac ako 3 miliardy dolárov a neustále rastie. Mnoho organizácií začalo migrovať do cloud computingu bez adekvátnych vedomostí a zdrojov na zabezpečenie vlastnej bezpečnosti. Dôverovali poskytovateľom cloudu, že sa postarajú o bezpečnosť ich dát v cloude, ale nezohľadnili aspekty celej cloudovej infraštruktúry. Hrozieb je pritom veľa, strata dát, chyby konfigurácie, ukradnuté heslá, kompromitované API, APT, zneužité účty, DoS a DDoS. SECaaS poskytovateľ, označovaný aj ako MSSP (Managed Security Service Provider) môže pomôcť pokryť všetky uvedené hrozby bez nutnosti navyšovať vlastné IT zdroje.

Best practise v bezpečnosti cloudov

Viac ako polovica respondentov v externom prieskume spoločnosti Symantec [SR19] potvrdila, že ich postupy cloudovej bezpečnosti neboli dostatočne pripravené na splnenie požiadaviek rastúceho využívania cloudových aplikácií. A takmer tri štvrtiny z nich uviedli, že uvedená skutočnosť viedla k bezpečnostným incidentom v ich cloudovej infraštruktúre. Mnoho nesprávnych postupov zostáva nezistených z dôvodu neprehľadnej cloudovej infraštruktúry. Odhalia sa až pri následnej analýze incidentov s cieľom zlepšiť svoje postupy v oblasti cloudovej bezpečnosti. Avšak len polovica respondentov uviedla, že robia takúto analýzu incidentov. Vlastné údaje spoločnosti Symantec potvrdzujú, že 85 percent zákazníkov nevyužíva všeobecne odporúčané "best practise". Spoločnosti, ktoré migrujú do cloudu by mali zvážiť tieto kľúčové kroky:

- Budúcnosť podnikovej bezpečnosti spočíva v koncepčnom a architektonickom modeli *Zero Trust*, ktorý podporuje holistický prístup k informačnej bezpečnosti so zvláštnym zameraním na procesy a technológie. Tradičné postupy IT bezpečnosti zabezpečujú autentifikáciu a autorizáciu používateľov na perimetri chránenej siete. Pri modeli Zero Trust nikto v sieti nedostane voľný vstup. Model Zero Trust predstavuje mikrosegmentový prístup s granulovanými úrovňami ochrany aplikovanými na dáta a ovládacie prvky implementované vo všetkých prístupových bodoch systému vrátane mobilných zariadení a aplikácií v cloude. Dáta v mikroperimetroch sú klasifikované na základe citlivosti a samotná architektúra zodpovedá za kontinuálne zmeny, čo okrem iného umožňuje modifikáciu prístupových práv na základe skóra rizika správania a typu zariadenia. Okrem kontroly segmentácie a prístupu je všetka sieťová prevádzka skenovaná a monitorovaná na prítomnosť hrozieb pomocou nástrojov, ako sú e-mailové brány a webové brány. Segmentácia siete a izolácia údajov minimalizujú dopad akéhokoľvek možného narušenia bezpečnosti. Každé riešenie počítačovej bezpečnosti, ktoré vynucuje Zero Trust, by malo obsahovať funkcie automatizovanej orchestrácie, aby sa znížila prevádzková záťaž bezpečnostných tímov.
- Verejný cloud je už zo svojej definície zdieľaným bezpečnostným modelom s poskytovateľom cloudu, čo znamená, že organizácie musia prehodnotiť svoju úlohu a stať sa oveľa aktívnejšími v riadení bezpečnosti, ako tomu bolo v minulosti. Napríklad s IaaS sú poskytovatelia cloudových služieb zodpovední za ochranu svojich cloudov, zatiaľ čo zákazníci sa musia sústrediť na riešenie zraniteľností alebo zneužitia ich cloudových aplikácií. K tomu je potrebné prejsť na decentralizovaný model IT bezpečnosti, v rámci ktorého vlastníci aplikácií preberajú zodpovednosť za bezpečnostné politiky a postupy podľa dohodnutých usmernení. Organizácie by mali byť pripravené investovať do školení o bezpečnosti v cloude, aby sa zaistilo, že zamestnanci rozumejú oblasti cloud computingu a špecifikám bezpečnej práce v tomto prostredí.
- Rastúci počet bezpečnostných platforiem má zabudované prvky UI a strojového učenia, ktoré automatizuje úlohy a prináša vyššiu úroveň inteligencie pri riešení

bezpečnostných incidentov. Patrí sem analýza správania používateľov, ktorá sa používa na identifikáciu potenciálnych bezpečnostných rizík vytvorením rámca bežného správania v priebehu času na identifikáciu abnormálnej aktivity v cloude. Automatizácia behaviorálnej analýzy sieťových komponentov pomáha organizáciám ľahšie a efektívnejšie identifikovať a klasifikovať potenciálne hrozby. Údaje o incidentoch by sa mali analyzovať a automaticky roztriediť, aby organizácie mali prehľad o tom, či je udalosť problematická, či je výsledkom prerušenia obchodných procesov alebo jednoducho štandardného obchodného správania, ktoré si vyžaduje úpravu politiky. Vďaka tomu je možné výrazne zlepšiť presnosť a priorizáciu pri riešení incidentov a proces sa stáva oveľa efektívnejším, čím sa znižuje manuálne vyšetrovanie a bezpečnostný personál sa tak môže zamerať na skutočné incidenty.

- Bezpečnosť sa často rieši až na konci vývoja aplikácie a nie je integrovaná do celého procesu vývoja. Vzhľadom na rýchlosť celého procesu vývoja, vedie tento prístup k bezpečnostným problémom. Prístup DevOps (Development & Operation) umožňuje rýchlejšie zavádzanie nových funkčností (aplikácií, funkcionality, verzií, …) s menším počtom chýb a vyššou spoľahlivosťou, držať krok s inovatívnymi technológiami, ako sú kontajnery a mikroslužby, a zároveň podporovať užšiu spoluprácu medzi bežne izolovanými tímami. Efektívne DevOps zaisťuje rýchle a časté vývojové cykly (niekedy týždne alebo dni), ale zastarané bezpečnostné postupy môžu spôsobovať brzdenie vývoja. Preto je potrebné zavádzať spoluprácu systémov DevOps a SecOps (Security Operation) ako spoločnej zodpovednosti za bezpečnosť, ktorá je integrovaná v projekte od začiatku do konca vývoja. Pre tento prístup sa zaužíval termín „DevSecOps“. Avšak najdôležitejším nástrojom, ktorý umožňuje tieto zmeny v prístupe k vývoju aplikácií je IT automatizácia. IT automatizácia zahŕňa správu repozitárov zdrojových kódov, register kontajnerov, kontinuálnu integráciu a doručovanie (Continuous Integration and Continuous Delivery, CI/CD), manažment rozhraní API, orchestráciu a monitorovanie.
- Jedným zo základných nástrojov, ktoré sa dajú použiť na zaistenie zabezpečenia cloudu, je auditný záznam (audit trail, audit log). Ide o chronologický zápis aktivít v systéme, ktorý je dostatočný pre rekonštrukciu a spätné sledovanie a vyhodnotenie stavu prostredia a aktivít súvisiacich s operáciami a procedúrami od ich začiatku až ku konečnému výsledku.

Zhrnutie

S príchodom nových služieb, rozsiahlych dátových úložísk, prepájaním cloudových služieb cez ich API, spolu s notoricky známymi útokmi na súkromie, dôvernosť, integritu a dostupnosť, sú pre platformy cloud computingu potrebné škálovateľnejšie bezpečnostné riešenia.

Multicloudové prostredia vyžadujú interakcie medzi poskytovateľmi cloudu založené na vzájomnej dôvere. Hlavným obmedzením je spôsob, akým sa odvodí dôvera a aké mechanizmy možno použiť na vytvorenie dôvery. Určitá pozornosť sa vo výskume

venovala vývoju metriky dôvery na vyčíslenie požadovaných úrovní dôvery v perspektíve zachovania súkromia. Je potrebný ďalší výskum škálovateľných mechanizmov vytvorenia dôvery, ktoré možno použiť pre rôzne modely zavádzania cloudu vo viaczložkových prostrediach.

V cloude je hosťované veľké množstvo údajov a poskytovatelia cloudu musia zaručiť jeho autentifikáciu a integritu všetkým používateľom. Overenie pôvodného zdroja pre dáta z distribuovaných zdrojov, pribúdanie dát do hostingu veľkou rýchlosťou (napríklad nepretržitý prúd údajov z miliónov senzorov), zachovanie integrity dát v čase, keď s nimi pracuje veľká používateľská základňa, to všetko vyžaduje škálovateľné riešenia. Pre tieto problémy je potrebné preskúmať riešenia založené na proveniencii a modely na overenie integrity grafov založené na big data [TYP+15].

Pri porovnávaní zamerania výskumu akademickej obce a vývoja v priemysle, najvýraznejším rozdielom je skutočnosť, že výskumné práce zvažujú útoky zo strany zlomyseľných zákazníkov a aj zlomyseľných poskytovateľov cloudových služieb, zatiaľ čo zamerania poskytovateľov cloudov sa zväčša orientujú iba na prvú možnosť [HGK+17]. Poskytovateľ cloudu má zvyčajne plnú dôveru od zákazníka. Zmluvné podmienky medzi poskytovateľom a zákazníkom vo všeobecnosti hovoria, že poskytovateľ cloudu je zodpovedný za zabezpečenie dát svojich zákazníkov. Poskytovatelia cloudových služieb sú však podľa nich explicitne oslobodení od zodpovednosti za škodu v dôsledku kompromitácie.

Pretože poskytovatelia cloudov musia budovať obraz svojej dôveryhodnosti, akademická obec predstavuje dôležitý protipól k identifikácii slabých stránok bezpečnosti poskytovateľa cloudových služieb, ktoré by pre samotných poskytovateľov bolo nepríjemné zverejniť. V prípade hrozieb zo strany zlomyseľných zákazníkov, priemysel a akademická obec identifikovali niektoré rovnaké hrozby, ale prišli s rôznymi riešeniami. Napríklad veľa akademických prác sa venovalo úniku dôverných informácií cez virtuálne stroje prostredníctvom postranných a skrytých kanálov. Akademici navrhli niekoľko nových a sofistikovaných riešení. Väčšina poskytovateľov cloudov však tvrdí, že dobre skonštruované hypervízory by mali stačiť na izoláciu zákazníkov v zdieľanom prostredí. Niektorí poskytovatelia cloudov prijímajú ďalšie opatrenia, aby presvedčili zákazníkov, že sú chránení pred týmito hrozbami, ale tieto opatrenia sú stále technicky jednoduché v porovnaní s riešeniami pochádzajúcimi z akademickej oblasti. Hypervízor spoločnosti Joyent SmartOS ponúka dva nezávislé izolačné mechanizmy – SmartOS Zone (podobnú BSD jailu), ako aj izoláciu založenú na QEMU-KVM. Amazon, Fujitsu a SoftLayer svojim zákazníkom ponúkajú za príplatok špecializované virtuálne počítače, ktoré bežia na dedikovaných podkladoch. Zdá sa, že priemysel nezávisle vyvinul niekoľko ďalších riešení problému úniku medzi virtuálnymi strojmi. To naznačuje, že výskumné úsilie by sa malo zamerať na zistenie praktickosti útokov, ktoré využívajú únik z viacerých virtuálnych strojov a ukázať nakoľko sú realizovateľné a s akými nákladmi. Ak sa tieto útoky ukážu ako relatívne lacné a ľahko realizovateľné, potom budú musieť všetci poskytovatelia cloudových služieb pridať do svojej ponuky aj dedokovaný hardvér

ako alternatívu. Na druhej strane, ak sa takéto útoky ukážu ako veľmi nákladné alebo nepraktické, potom môžu dedikovaný hardvér využívať iba niektorí zákazníci s mimoriadne cennými informáciami [HGK+17].

Jedným zo spôsobov, ako môžu vedecké publikácie ovplyvňovať prax v priemysle, je demonštrovať realizovateľnosť konkrétnych útokov. Napríklad je opis hrozby úniku dôverných informácií prostredníctvom zdieľaných obrazov virtuálnych strojov v prostredí Amazon EC2 v odbornom článku [RTH+09]. Tieto hrozby boli potvrdené aj spoločnosťou Amazon.

Pri plánovaní cloudovej stratégie je potrebné zistiť, aké dáta budú v cloude. Je potrebné klasifikovať každý typ údajov podľa dopadu na organizáciu, ak by boli tieto dáta kompromitované, t. j. ak ich útočník prečíta, zmení alebo odstráni.

Pojem gridového počítania

Víziou gridového počítania je, aby boli výpočtové prostriedky k dispozícii pre používateľov rovnako ľahko, ako elektrická energia v elektrickej sieti. Hlavný motivačný rámec gridového počítania tvorí súčasný narastajúci počet koncových vysokovýkonných počítačových zariadení, ako aj obrovské množstvo informácií dostupných v globálne distribuovaných zdrojoch prepojených vysokorýchlostnými sieťami. Práve hladký prístup ku globálnym distribuovaným IT zdrojom dáva vedcom možnosť riešiť rozsiahle problémy v oblasti vedy a techniky. Gridové prostredie je projektované tak, aby pomohlo vyplniť existujúcu medzeru pri vzájomnom využívaní výpočtových prostriedkov a prepojilo dostupné zdroje dohromady, a tak poskytlo vedcom ľahký a transparentný prístup k novej integrovanej superpočítačovej infraštruktúre.

Gridové technológie sa v súčasnosti používajú v mnohých vedných oblastiach a zahŕňajú rôzne typy gridových prostredí, ako je výpočtový, dátový, či kolaboratívny grid. *Výpočtový grid*, napr. škandinávsky projekt *NorduGrid*[24] alebo projekt koordinovaný inštitúciou CERN *Worldwide LHC Computing Grid*[25], americký projekt *The Open Science Grid*[26], či česká Národná gridová infraštruktúra (NGI) MetaCentrum[27], zahŕňajú veľké množstvo vzájomne prepojených vysoko výkonných výpočtových stredísk, za účelom poskytnúť mimoriadnu výpočtovú kapacitu. Celkový súhrnný výpočtový výkon takýchto distribuovaných stredísk ďaleko prevyšuje výkon jedného výpočtového zariadenia lokalizovaného na jednom mieste a umožňuje vykonávanie výkonovo vysoko náročných aplikácií, príp. aplikácií s vysokou priepustnosťou. *Dátové gridy* sa zameriavajú skôr na správu a zdieľanie obrovského množstva dát pre globálne distribuované vedecké komunity, napr. projekt zameraný na nukleárnu fyziku *Particle Physics Data Grid*[28] alebo projekt *dCache.org*[29] zameraný na ukladanie obrovského množstva dát distribuovaných medzi veľké množstvo heterogénnych serverových uzlov pod jeden virtuálny stromový súborový systém. Iným typom gridového prostredia sú tzv. *spolupracujúce gridy*, ako napríklad EÚ projekt *Virolab*[30] – a virtual lab for decision

[24] http://www.nordugrid.org/
[25] http://wlcg.web.cern.ch/
http://wlcg-public.web.cern.ch/
[26] https://opensciencegrid.org/
[27] https://www.metacentrum.cz/cs/Sluzby/Grid/
[28] http://www.ppdg.net/
[29] https://www.dcache.org/
[30] https://www.virolab.org/

support in viral diseases treatment, ktorých cieľom je vytvoriť virtuálne laboratória za účelom poskytnúť geograficky vzdialeným vedcom výskumné prostredie pre vedeckú spoluprácu, akým je napr. diaľkové ovládanie zariadení, senzorov a iných nástrojov.

Motivácia

Výpočtové prostredia sa vyvinuli počínajúc od jedného používateľského prostredia, cez masívne paralelné procesory (MPP), klastre pracovných staníc a distribuované systémy až po súčasné systémy gridového počítania a cloudové služby. Každý prechod predstavoval určitý prelom, ktorý umožnil vedcom riešiť nové, komplexné problémy, príp. vykonávať sofistikované programy, ktoré nebolo možné skôr implementovať. Avšak každý prechod prináša ďalšie výzvy a problémy, rovnako ako nutnosť technickej inovácie. Vývoj počítačových systémov viedol k dnešnému stavu, v ktorom sú milióny počítačov prepojené prostredníctvom internetu s rôznymi hardvérovými a softvérovými konfiguráciami, s rôznymi danosťami, topológiou zapojenia, s rôznymi prístupovými politikami, atď. A práve impozantná kombinácia hardvérových a softvérových zdrojov na internete vyvolala záujem používateľov pri skúmaní nových spôsobov ako využívať, a obzvlášť bezpečne využívať, početné zdroje efektívne a ekonomicky, a ako celkovo prepojiť tieto distribuované zdroje tak, aby ich bola schopná efektívne využiť jediná aplikácia.

Gridové počítanie je vo svojej podstate diverzifikované a heterogénne, prekleňujúce viacero administratívnych domén, ktorých zdroje nie sú vo vlastníctve jedného držiteľa, resp. nie sú spravované jediným správcom. Uvedené danosti nastoľujú rôzne výzvy pre manažment gridových zdrojov, akými sú napr. otázka autonómie, otázka heterogénnosti prostredia, či politika rozšíriteľnosti a v neposlednej rade aj otázka bezpečnosti. Kľúčovými prvkami manažmentu gridového počítania sú: (i) *riadenie zdrojov* – grid musí vedieť, aké zdroje sú pre rôzne úlohy k dispozícii, (ii) *riadenie bezpečnosti* – grid musí dbať na to, aby mali k dispozícii a používali dostupné zdroje iba autorizovaní používatelia, (iii) *správa údajov* – údaje musia byť správne zaslané, vyčistené, rozdelené a spracované, (iv) *správa služieb* – aplikácie a používatelia musia byť schopní sa dotazovať v gride efektívnym spôsobom. Hlavný element pri riešení uvedených otázok v gridovom počítaní predstavuje softvérová vrstva nazývaná *middleware*.

Middleware poskytuje metódy na overovanie identity používateľa, ale aj zdrojov, umožňuje bezpečné vykonávanie, monitorovanie a riadenie operácii na zdieľaných prostriedkoch, a taktiež zahŕňa kolektívne služby ako sú sprostredkovateľské, monitorovacie, diagnostické, strategické služby. Hoci vrstva middleware umožňuje vykonávanie vlastného gridového počítania, používatelia sú naďalej vystavený istej zložitosti a to práve vďaka zložitosti samotnej vrstvy middleware. Táto záťaž vychádza z nutnosti mať určité znalosti rôznych súčastí vrstvy middleware, aby bolo možné čo najefektívnejšie využívať gridové zdroje. Tieto znalosti sa pohybujú od dopytovania sa na potrebné informácie od poskytovateľov informácií v gride, výber vhodných prostriedkov pre úlohy používateľa, vytváranie príslušných súborov typu JSDL (Job

Submission Description Language), zasielanie úloh gridovým zdrojom a samotná inicializácia spustenia výpočtovej úlohy.

Ústredným prvkom v gridovom počítaní je sprostredkovanie zdrojov (grid resource brokering), ktoré do istej miery odbremeňuje používateľa od zložitosti gridovej vrstvy middleware. Služba zameraná na sprostredkovanie zdrojov mapuje, ktoré gridové zdroje spĺňajú požiadavky používateľa na zasielanú úlohu. Uvedený proces môže v sebe zahŕňať prehľadávanie niekoľkých administratívnych domén, s cieľom nájsť jeden zdroj, ktorý je vhodný na vykonanie úlohy, alebo môže zahŕňať plánovanie danej úlohu s použitím viacerých zdrojov v rámci jedného alebo viacerých miest v gride.

Hlavným cieľom gridového počítania je poskytnúť nástroj výpočtu v zmysle stanovených požiadaviek používateľa. Služba sprostredkovania zdrojov sa tak orientuje na poskytovanie služieb so zameraním sa na používateľa. S viacerými používateľmi z rôznych strán súvisí aj ďalšia povinnosť, kde gridové prostredie musí riešiť prípady a adekvátne poskytovať zdroje viacerým používateľom, ktorí majú záujem o rovnaký zdroj v rovnakom čase bez znalosti o existencii druhého používateľa. Navyše, pre maximalizáciu výhod gridového počítania je dôležité, aby boli gridové služby schopné odhaliť všetky zdroje, ktoré sú pre grid prístupné, a namapovať zaslanú úlohu na najvhodnejší zdroj. Problém vyhľadávania zdrojov a zaslanie úlohy najlepšie zodpovedajúcemu zdroju znamená pre výpočtové gridové systémy veľkú výzvu, keďže sa v gridových prostrediach nachádza enormné množstvo zdrojov, a navyše je potrebné brať do úvahy ich rôznorodosť, dostupnosť, ale aj rozmanitosť atribútov zdrojov, ako je zaťaženie procesora a veľkosť diskového priestoru.

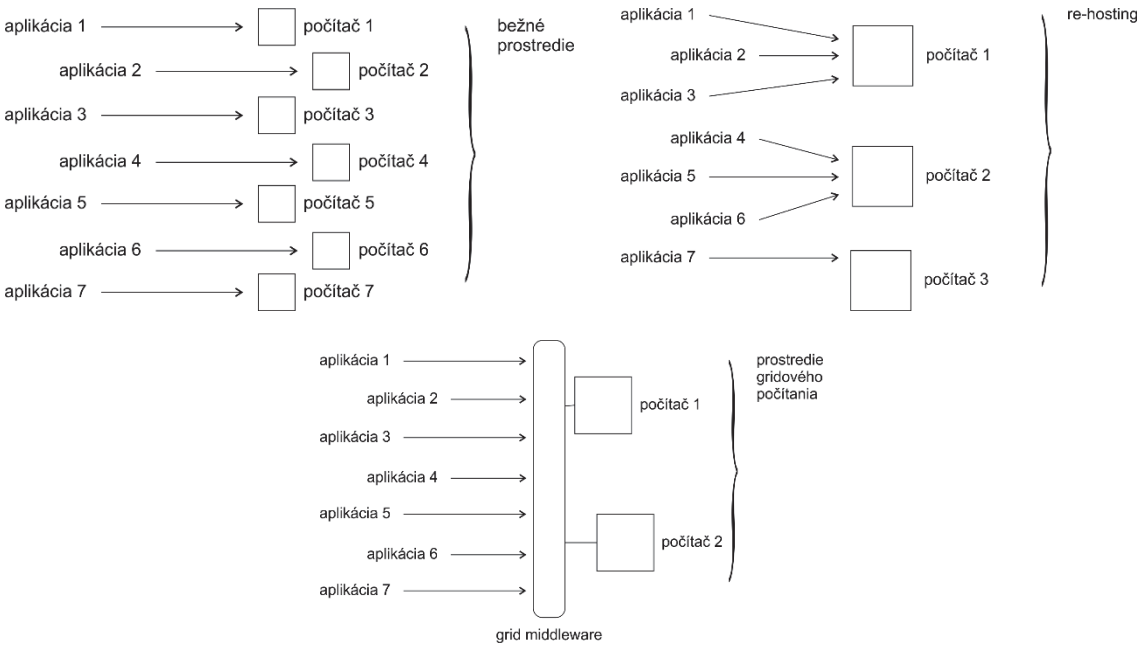
Gridové počítanie, tak ako aj cloud computing, využíva virtualizáciu. Virtualizácia zdrojov je abstrakcia serverových, úložných a sieťových prostriedkov tak, aby boli v rámci organizácie aj mimo nej dynamicky dostupné na zdieľanie. Virtualizácia je jedným z prvých krokov na ceste k viacúčelovému počítaniu, akým je práve gridové počítanie, a v kombinácii s ďalšími serverovými, úložnými a sieťovými prostriedkami umožňuje zákazníkom vybudovať IT infraštruktúru „bez“ pevných hraníc alebo iného obmedzenia. Avšak virtualizácia má o niečo väčší dôraz na miestne zdroje, zatiaľ čo gridové počítanie má väčší dôraz na geograficky rozložené zdroje z rôznych organizácií [M04]. Virtualizácia môže zahŕňať nasledujúce oblasti:

- Virtualizácia servera pre horizontálne a vertikálne škálované serverové prostredia. Virtualizácia servera umožňuje jeho lepšie využitie, zlepšenú úroveň služieb a zníženú réžiu správy.
- Virtualizácia siete, ktorú umožňujú inteligentné smerovače, prepínače a iné sieťové prvky podporujúce virtuálne siete LAN. Virtualizované siete sú bezpečnejšie a viac schopné podporovať nepredvídané výkyvy v požiadavkách zákazníkov a používateľov.
- Virtualizácia úložísk (server, sieť a diskové pole). Technológie virtualizácie úložísk zlepšujú využívanie súčasných úložných podsystémov, znižujú

administratívne náklady a chránia dôležité údaje bezpečným a automatizovaným spôsobom.

- Aplikačná virtualizácia umožňuje vykonávanie programov a služieb na viacerých systémoch súčasne. Tento výpočtový prístup súvisí s horizontálnym škálovaním, klastrami, gridovým počítaním a cloud computingom, v ktorých sú časti jednej aplikácie schopné byť vykonávaná na viacerých serveroch súčasne.
- Virtualizácia dátových centier, pričom skupiny serverov, úložných priestorov a sieťových zdrojov môžu byť poskytované alebo realokované za chodu tak, aby vyhovovali potrebám novej IT služby alebo zvládli dynamicky sa meniace pracovné zaťaženia.

Rovnako aj pri porovnaní gridového počítania s tzv. „rehostingom“ (prenosom aplikácie/systému na iný výpočtový systém), nasadenie gridového počítania nie je len rehosting. Ako ukazuje Obrázok 0-1, rehosting znamená redukciu typicky veľkého počtu serverov na menšiu množinu výkonnejších a modernejších serverov, zväčša z dôvodu optimalizácie a zvýšenia výkonu, priestoru a fyzickej údržby, či z dôvodu úspor. Avšak aplikácie sú stále priradené k špecifickým serverom. Na druhej strane, gridové počítanie umožňuje skutočnú virtualizáciu výpočtovej funkcionality. Aplikácie nie sú vopred priradené k určitým serverom, ale priradenie je vykonané za behu na základe rozhodnutia v reálnom čase. Navyše, aplikácie môžu byť priradené nielen lokálne, ale môžu byť využité zapojené zdroje z celého sveta [M04].



Obrázok 0-1 Porovnanie gridového počítania s rehostingom [M04].

Definícia gridového počítania

Na začiatok uvádzame definíciu gridového počítania, ktorá bola prevzatá od jedného z najväčších používateľov gridovej technológie a to organizácie CERN. Definícia je

uvedená na webovom portáli organizácie TWGrid zameranej na vytváranie medzinárodnej spolupráce v gridovom počítaní:

"Gridové počítanie je služba pre zdieľanie výpočtového výkonu a pre zdieľanie kapacity na ukladanie dát cez internet."[31]

Prvé inovatívne zavedenie pojmu grid bolo definované od autora Iana Fostera, tiež označovaného ako „otec gridu", a jeho kolegu Carla Kesselmana v knihe *The Grid: A Blueprint for a New Computing Infrastructure* [KF98]. Idea gridového počítania tu vychádza z už spomínanej predstavy, že výpočtový výkon by mal byť pre používateľov ľahko prístupný ako elektrický prúd z elektrickej siete (angl. Power Grid). Na tieto aspekty sa vzťahuje aj samotná počiatočná definícia gridového počítania od Fostera a Kesslemanna, kde je grid definovaný so zameraním sa na výpočtové aspekty, a to nasledovne:

„Výpočtový grid je hardvérová a softvérová infraštruktúra, ktorá poskytuje spoľahlivý, konzistentný, všadeprítomný a lacný prístup k špičkovému výpočtovému vybaveniu."

V roku 2003 autori Foster a Kesselman danú definíciu gridu prepracovali a zdokonalili, pričom špecifikovali pojem zdieľanie zdrojov v gridovom prostredí a s tým súvisiace otázky, najmä otázku koordinácie zdrojov a proces dohadovania sa pri zdieľaní. Definícia je uvedená v druhom vydaní knihy *The Grid 2: A Blueprint for a New Computing Infrastructure* [FK03]:

„Zdieľanie, ktoré berieme do úvahy, nie je primárne pre výmenu súborov, ale pre priamy prístup k počítačom, softvéru, dátam a ďalším prostriedkom, v rozsahu potrebnom pre spoločné riešenia problémov a stratégie sprostredkovania zdrojov, ktoré sa využívajú v priemysle, vo vede a ďalších inžinierskych odboroch. Toto zdieľanie je nevyhnutne prísne kontrolované, pričom je poskytovateľmi zdrojov a spotrebiteľmi jasne a dôsledne definované, čo je spoločné a kto má oprávnenie zdroje zdieľať, a podmienky, za ktorých k zdieľaniu dôjde. Množina jednotlivcov a/alebo inštitúcií, ktoré sú stanovené danými pravidlami pre zdieľanie, tvorí to, čomu hovoríme virtuálna organizácia."

Poznamenajme, že podstata myšlienky gridového prostredia sa líši od podstaty webových služieb tým, že gridové počítanie využíva internet na zdieľanie výpočtových a pamäťových zdrojov, zatiaľ čo web využíva internet pre zdieľanie informácií.

Gridové počítanie je založené na myšlienke, že vedci môžu prekonať svoje lokálne počítačové obmedzenia pomocou flexibilne definovaných zoskupení procesorov prepojených vysoko výkonnými sieťami a tak vytvoriť na vyriešenie určitého problému distribuované paralelné výpočtové prostredie. Veľkosť gridového prostredia môže variovať od malých gridov vytvorených len z niekoľkých kooperujúcich pracovných staníc, až po veľké gridy, na ktorých kooperuje množstvo spoločností a sietí. Vlastník výpočtových zdrojov v gridových systémoch a používateľ zdrojov v gridových systémoch zväčša nie je rovnaká osoba a zväčša ani nepatria do rovnakej administratívnej

[31] GRID, http://www.twgrid.org/en/index.php?option=com_content&task=view&id=159&Itemid=273

domény. Na grid možno pozerať ako na istú globálnu sieť výpočtových zdrojov, ktoré reprezentujú jedno rozsiahle výpočtové prostredie.

Základné vlastnosti gridového prostredia

Gridové počítanie sa objavilo ako nová paradigma pre distribuované výpočty. Tradične distribuované výpočty sú definované ako systém s pevným počtom uzlov. S príchodom gridového počítania sa však počet uzlov v distribuovaných systémov neustále mení a systém je označovaný ako *dynamický distribuovaný systém* a má nasledujúce vlastnosti [IF01, BDG04, Sto07]:

Heterogénne zdroje

Ponúkané zdroje v gridovom prostredí majú veľmi rôznorodé zloženie, t. j. rôzne architektonické platformy, rôzne rýchlosti dostupných CPU, rôzne rozloženie hierarchie pamäte a rôzne kapacity dostupných diskov, ako aj rôznu softvérovú konfiguráciu zdrojov.

Dynamická dostupnosť zdrojov

Absencia striktnej kontroly na pridávanie/odoberanie zdrojov v gridovom prostredí a dobrovoľnosť poskytovania zdieľaných zdrojov môže spôsobiť odpojenie zdroja od prebiehajúceho výpočtu kedykoľvek na prianie vlastníka zdroja. Prostriedky môžu byť nedeterministicky pridávané/odoberané z množiny dostupných zdrojov, čo znamená, že dané prostriedky môžu vstúpiť a opustiť grid kedykoľvek. Uvedená danosť na jednej strane robí gridové prostredie vysokokvalitným výpočtovým médiom, analogické s internetom ako vysokokvalitným komunikačným médiom. Na druhej strane však musí grid prispôsobovať svoje správanie tak, aby na získanie maximálneho výkonu maximálne využil dostupné zdroje.

Rozsiahlosť

Grid sa musí byť schopný vysporiadať s rôznym množstvom dostupných zdrojov, od malého počtu niekoľkých zdrojov, až po niekoľko miliónov. To nastoľuje veľmi vážny problém, ako sa vyhnúť prípadnému zníženiu výkonu gridu, ak sa zvýši jeho veľkosť.

Geografická distribúcia

Gridové zdroje môžu byť umiestnené na vzdialených miestach.

Zdieľanie zdrojov

Zdroje v gridovom prostredí patria mnohým rôznym organizáciám, ktoré umožňujú prístup k týmto zdrojom ďalším organizáciám, resp. používateľom. Programy jednej organizácie tak môžu využívať nelokálne zdroje inej organizácie, čo podporuje efektivitu a znižuje nákladovosť systému.

Rôzna administrácia

Každá organizácia môže vytvoriť rôzne bezpečnostné a administratívne politiky, na základe ktorých sú ich vlastné zdroje dostupné a použiteľné. V dôsledku nárastu zložitosti pri zohľadňovaní všetkých rôznych politík sa zvyšuje aj náročnosť konzistentného

zabezpečenia gridového prostredia. Jednou z požiadaviek kladených na gridové prostredie je použitie distribuovaných riadiacich mechanizmov.

Koordinácia zdrojov

Zdroje v gridovom prostredí musia byť koordinované s cieľom poskytnúť súhrnné výpočtové možnosti.

Transparentný prístup

Grid je možné vnímať ako jeden rozsiahly virtuálny počítač. Grid by mal umožniť svojim používateľom prístup k počítačovej infraštruktúre bez toho, aby museli byť dôverne oboznámení s architektúrou a topológiou gridového prostredia. Uvedená danosť je niekedy považovaná za najvýraznejší aspekt gridového počítania.

Spoľahlivý prístup

Grid musí zabezpečovať poskytovanie služieb v rámci stanovených požiadaviek na kvalitu služieb (QoS). Potreba spoľahlivých služieb je zásadnou požiadavkou, pretože používatelia požadujú ubezpečenie, že sa im dostane predvídateľný, trvalý a často vysoký výkon.

Konzistentný prístup

Grid musí byť postavený na štandardných službách, protokoloch a rozhraniach, ktoré skrývajú rôznorodosť zdrojov a zároveň umožňujú jeho rozšíriteľnosť. Bez týchto noriem by vývoj aplikácií, ako aj masívne využívanie nebolo možné.

Bezpečnosť

Základným rysom gridového prostredia je bezpečný prístup k zdrojom. Preto majú používatelia a aplikácie z pohľadu prístupu ku gridovým zdrojom vymedzený len stanovený počet oprávnení. Zjednodušene povedané, gridová bezpečnosť je jednou z prvých vecí, s ktorou sa reálni gridoví používatelia musia vysporiadať, a je nevyhnutná pre akýkoľvek gridový systém, ktorý zahŕňa niekoľko administratívnych domén.

Druhy gridových systémov

Nasledujúca kategorizácia rozlišuje gridy podľa typu aplikácií, ktoré sa na nich vykonávajú. Rozlišované sú tieto základné typy gridových systémov [KSD07]:

Výpočtový grid

Jedná sa o klasickú a najpoužívanejšiu formu gridu. Výpočtové zdroje, ako pracovné stanice, PC alebo aj PC klastre sú zlúčené do virtuálneho superpočítača, ktorý poskytuje oveľa viac zoskupeného výpočtového výkonu ako jediný klaster alebo pracovná stanica. V tomto type gridu prevažujú výpočtovo náročné aplikácie.

Dátový grid

Dátový grid integruje rôzne, väčšinou distribuované a heterogénne dátové zdroje do virtuálnej databázy. V tomto type gridu dominujú otázky týkajúce sa prístupu k dátam a ich integrácií. Dátový grid je charakterizovaný federáciou dátových sád na miestnej

úrovni pre správu, organizáciu, ukladanie a distribúciu, a to asynchrónne a aj v reálnom čase.

Scavenging grid

Scavenging grid sa typicky využíva pri veľkom počte používateľských staníc. Umožňuje používateľom využívať výpočtové prostriedky (napríklad cykly CPU) iných staníc a poskytovať vlastné nevyužité prostriedky ostatným. Najviac známym príkladom je projekt SETI@home[32] zameraný na hľadanie inteligentného mimozemského života vo vesmíre prostredníctvom analýzy vzoriek signálov z najväčšieho rádioteleskopu na svete v Arecibo. Objavujú sa však aj výhrady nazývať takéto štruktúry gridom, keďže riadenie a administrácia v systéme je striktne centrálna.

Vzorovým príkladom scavenging gridu sú projekty založené na nástroji BOINC (Berkeley Open Infrastructure for Network Computing). BOINC je softvér, ktorý umožňuje prevádzkovať projekty pre distribuované výpočty na počítačoch poskytnutých dobrovoľníkmi z celého sveta. SETI@home je jedným z najznámejších projektov využívajúcim BOINC. A práve úspech projektu SETI@home všetkých presvedčil, že distribuované výpočty sa môžu použiť aj pre mnoho iných výpočtovo náročných vedeckých projektov[33] a využívať tak inak nevyužitú kapacitu počítačov. Pôvodne veľká výpočtová úloha sa rozdelí na veľký počet malých samostatných jednotiek, ktoré potom analyzujú milióny počítačov na celom svete. V súčasnosti je spoločná výpočtová kapacita zapojených počítačov v infraštruktúre BOINC 28.599 PetaFLOPS[34], čo zodpovedá najvýkonnejším (nedistribuovaným) superpočí-tačom sveta v rebríčku Top500[35].

Sémantický grid/Znalostný grid

Tieto gridy využívajú sémanticky obohatené služby (napr. výpočtové a dátové služby s pridanými popismi, ktoré sú pre ľudí čitateľné a sú strojovo spracovateľné) pre maximálnu jednoduchosť použitia, zdieľanie, automatizáciu a opakované použitie. Hlavný cieľ je kladený na opakované použitie technológie v kontexte sémantického webu. Sémantický grid využíva technológie sémantického webu pre opis nielen statických dát, ale aj pre opis webových/gridových služieb a nimi spracovávaných dát, resp. na zistenie vedomostí z distribuovaných zdrojov na základe prístupov sémantických gridov.

Spolupracujúci grid

Poskytuje nové virtuálne prostredie pre spoluprácu geograficky vzdialených jedincov a skupín, alebo vzdialené ovládanie nástrojov a prístrojov.

---

[32] https://setiathome.ssl.berkeley.edu/
[33] https://boinc.berkeley.edu/projects.php
[34] https://boinc.berkeley.edu/
[35] https://www.top500.org/