



Analýza hrozieb a rizík pre oblasť „Cloud Cyber Security“ v rámci SoA

ECTA, s.r.o.

Mgr. Monika Jaborníková

Senior Consultant, internal auditor

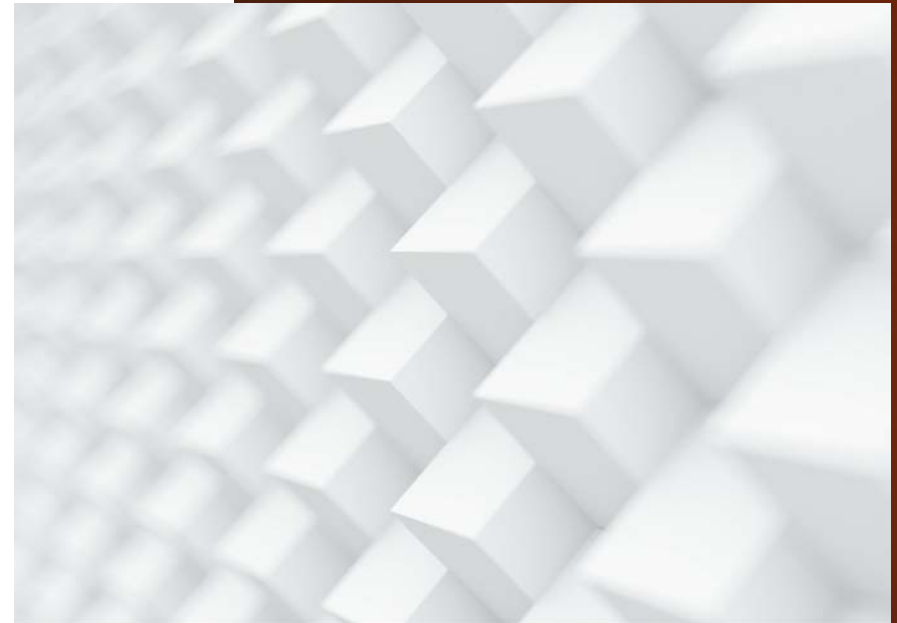
Obsah prednášky:

- Aplikácia požiadaviek kybernetickej bezpečnosti v oblasti cloudových služieb podľa ISO/IEC 27017 v praxi
- Aplikácia požiadaviek kybernetickej bezpečnosti na ochranu osobne identifikovateľných informácií (PII – personally identifiable information) vo verejných cloudoch vystupujúcich ako spracovatelia PII podľa ISO/IEC 27018

ISO/IEC 27017 Informačné technológie – Bezpečnostné techniky – Súbor postupov pre opatrenia bezpečnosti informácií pre cloudové služby založené na ISO/IEC 27002

Používanie cloud computingu zmenilo spôsob, ako by mali organizácie posudzovať a zmierňovať riziká bezpečnosti informácií z dôvodu podstatných zmien v tom, ako sú výpočtové zdroje technicky navrhnuté, používané a riadené.

Medzinárodná norma ISO/IEC 27017 poskytuje dodatočné pokyny k implementácii a poskytuje kontrolné opatrenia pre riešenie hrozieb bezpečnosti informácií a zvažovaní rizík špecifických pre cloudové prostredie.



ISO/IEC 27017

Riadenie rizík informačnej bezpečnosti pri cloudových službách

- Na rozdiel od všeobecnej použiteľnosti postupov pre riadenie rizík informačnej bezpečnosti má cloud computing svoje vlastné typy zdrojov rizík, vrátane hrozieb a zraniteľností, ktoré sú odvodené z jeho vlastností, napr. využitie sietí, škálovateľnosť a pružnosť systému, zdieľanie zdrojov, poskytovanie samoobslužných služieb, obmedzená viditeľnosť kontrolných opatrení,...
- Kontrolné opatrenia a pokyny k implementácii uvedené v kapitolách 5-18 a v Prílohe A tejto medzinárodnej normy, sa zaoberajú zdrojmi rizík a rizikami špecifickými pre cloud computing.

ISO/IEC 27017

- Norma je štruktúrovaná vo formáte podobnom ISO/IEC 27002 v kapitolách 5 až 18 a súvisiacimi podkapitolami a neoddeliteľnou súčasťou je Príloha A – Rozšírený súbor opatrení cloudových služieb.
- V rámci týchto kapitol sú jednotlivo uvedené dodatočné pokyny k implementácii špecifickej pre cloudové služby týkajúce sa kontrolných opatrení pod názvom „**Pokyny k implementácii pre cloudové služby**“.
- Jednotlivé pokyny sú rozdelené a uvedené zvlášť pre **Zákazníka cloudových služieb** a zvlášť pre **Poskytovateľa cloudových služieb**, v niektorých prípadoch je pokyn rovnaký pre oba subjekty.

- Celkovo 37 špecifických pokynov k implementácii pre cloudové služby.

ISO/IEC 27017

špecifické pokyny k implementácii pre cloudové služby

5.1.1 Politiky pre bezpečnosť informácií

6.1.1 Role a zodpovednosti informačnej bezpečnosti

6.1.3 Kontakt s autoritami

7.2.2 Povedomie, vzdelávanie a školenie o bezpečnosti informácií

8.1.1 Zoznam aktív

8.2.2 Označovanie informácií

9.1.2 Prístup k sieťam a sieťovým službám

9.2.1 Registrácia a zrušenie registrácie užívateľa

9.2.2 Zriadenie prístupu užívateľa

9.2.3 Riadenie privilegovaných prístupových práv

9.2.4 Riadenie tajných autentizačných informácií užívateľov

9.4.1 Obmedzenia prístupu k informáciám

9.4.4 Použitie privilegovaných obslužných programov

10.1.1 Politika použitia kryptografických opatrení

10.1.2 Správa kľúčov

11.2.7 Bezpečná likvidácia alebo opakované použitie zariadení

12.1.2 Riadenie zmien

12.1.3 Riadenie kapacít

12.3.1 Zálohovanie informácií

12.4.1 Zaznamenávanie udalostí formou logov

12.4.3 Logy o činnosti administrátorov a operátorov

12.4.4 Synchronizácia času

12.6.1 Správa a riadenie technických zraniteľností

13.1.3 Princíp oddelenia v sieťach

ISO/IEC 27017

špecifické pokyny k implementácii pre cloudové služby

14.1.1 Analýza a špecifikácia požiadaviek informačnej bezpečnosti

14.2.1 Politika bezpečného vývoja

15.1.1 Politika bezpečnosti informácií pre oblasť vzťahov s dodávateľmi

15.1.2 Riadenie bezpečnosti v rámci zmlúv s dodávateľmi

15.1.3 Reťazec dodávateľov informačných a komunikačných technológií

16.1.1 Zodpovednosť a postupy

16.1.2 Podávanie správ o udalostiach bezpečnosti informácií

16.1.7 Zhromažďovanie dôkazov

18.1.1 Identifikácia príslušnej legislatívy a zmluvných požiadaviek

18.1.2 Práva k duševnému vlastníctvu

18.1.3 Ochrana záznamov

18.1.5 Regulácie kryptografických opatrení

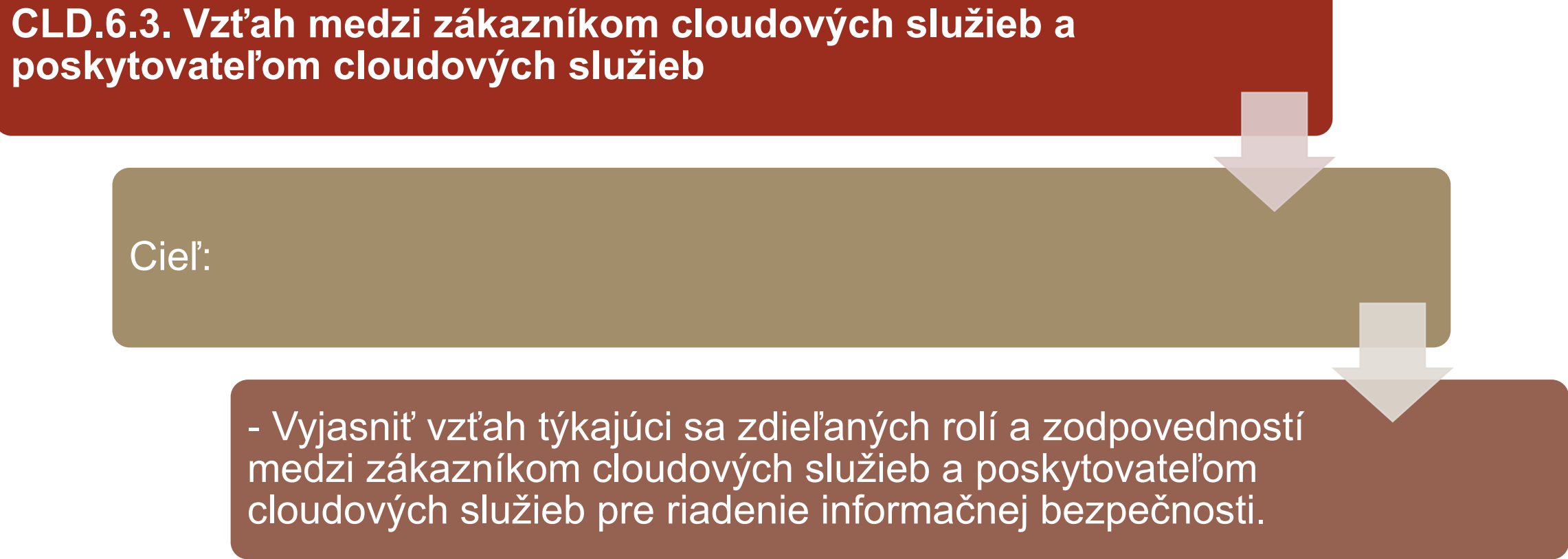
18.2.1 Nezávislé preskúmanie bezpečnosti informácií

ISO/IEC 27017

- Organizácie, ktoré majú v úmysle zaviesť opatrenia normy ISO/IEC 27017 v systéme riadenia informačnej bezpečnosti (ISMS), ktorý má byť komforntý s ISO/IEC 27001, by mala tiež **rozšíriť** svoje **Prehlásenie o aplikovateľnosti (SoA)** o nasledujúce opatrenia nachádzajúce sa v Prílohe A:



CLD.6.3. Vzťah medzi zákazníkom cloudových služieb a poskytovateľom cloudových služieb



```
graph TD; A[CLD.6.3. Vzťah medzi zákazníkom cloudových služieb a poskytovateľom cloudových služieb] --> B[Cieľ:]; B --> C[- Vyjasniť vzťah týkajúci sa zdieľaných rolí a zodpovedností medzi zákazníkom cloudových služieb a poskytovateľom cloudových služieb pre riadenie informačnej bezpečnosti.];
```

Cieľ:

- Vyjasniť vzťah týkajúci sa zdieľaných rolí a zodpovedností medzi zákazníkom cloudových služieb a poskytovateľom cloudových služieb pre riadenie informačnej bezpečnosti.

ISO/IEC 27017

Príloha A

CLD.6.3.1 Zdieľané roly a zodpovednosti v rámci prostredia cloud computing

- Zodpovednosti za zdieľané roly bezpečnosti informácií pri používaní cloudových služieb by mali byť pridelené identifikovaným stranám, dokumentované, komunikované a implementované ako zákazníkom cloudových služieb, tak aj poskytovateľom cloudových služieb.
- Roly a zodpovednosti sú v cloud computingu typicky rozdelené medzi zamestnancov zákazníka cloudových služieb a zamestnancov poskytovateľa cloudových služieb. V rámci pridelenia rolí a zodpovedností by sa mali vziať do úvahy dáta a aplikácie zákazníka cloudových služieb, pre ktoré sa poskytovateľ cloudových služieb stáva správcom.

ISO/IEC 27017

Príloha A

CLD.8.1 Zodpovednosť za aktíva

- Cieľ: Platí cieľ uvedený v 8.1 normy ISO/IEC 27001

CLD.8.1.5 Odstránenie aktív zákazníka cloudových služieb

- Aktíva zákazníka cloudových služieb, ktoré sa nachádzajú v priestoroch poskytovateľa cloudových služieb, by mali byť po skončení dohody o cloudových službách včas odstránené a v prípade potreby vrátené.

ISO/IEC 27017

Príloha A

CLD.9.5 Riadenie prístupu k dátam zákazníka cloudových služieb v zdieľanom virtuálnom prostredí

Cieľ:

Zmiernenie rizík bezpečnosti informácií pri používaní zdieľaného virtuálneho prostredia cloud computingu

CLD.9.5.1 Oddelenia vo virtuálnom prostredí

- Virtuálne prostredie zákazníka cloudových služieb prevádzkované na cloudových službách by malo byť chránené pred ostatnými zákazníkmi cloudových služieb a neoprávnenými osobami.

ISO/IEC 27017

Príloha A

Implementácia logických oddelení závisí od aplikovaných virtualizačných technológií:

- Konfigurácie sietí a úložísk možno virtualizovať, ak softvérová virtualizačná funkcia poskytuje virtuálne prostredie (napr. virtuálny operačný systém). Okrem toho, oddelenie zákazníkov cloudových služieb v softvérovo virtualizovaných prostrediach môže byť navrhnuté a implementované použitím segregačných funkcií softvéru.
- Ak je informácia zákazníka cloudových služieb uložená vo fyzicky zdieľanom priestore úložiska s „tabuľkou meta-dat“ cloudovej služby, oddelenie informácií od iných zákazníkov cloudových služieb môže byť implementované riadením prístupu k „tabuľke meta-dat“.
- Bezpečný viacnásobný prenájom a súvisiace pokyny uvedené v „ISO/IEC 27040 Information technology – Security techniques – Storage security“ možno aplikovať na prostredie cloud computingu.

ISO/IEC 27017

Príloha A

CLD.9.5.2 Zodolnenie virtuálneho zariadenia

Virtuálne prístroje v prostredí cloud computingu by mali byť odolné tak, aby spĺňali potreby činnosti organizácie.

Zákazníci a poskytovatelia cloudových služieb by mali pri konfigurácii virtuálnych strojov zaistiť zodolnenie príslušných aspektov (napr. len tie porty, protokoly a služby, ktoré sú potrebné) a uplatnenie vhodných technických opatrení (napr. anti-malware, zaznamenávanie do logov) pre každý používaný virtuálny stroj.

ISO/IEC 27017

Príloha A

CLD.12.1 Prevádzkové postupy a zodpovednosti

Cieľ: Platí cieľ uvedený v 12.1 normy ISO/IEC 27001

CLD.12.1.5 Prevádzková bezpečnosť administrácie

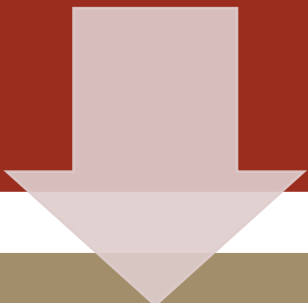
Mali by byť definované, dokumentované a monitorované postupy pre administratívne činnosti v prostredí cloud computingu.

Zákazník cloudových služieb	Poskytovateľ cloudových služieb
Zákazník cloudových služieb by mal zdokumentovať postupy pre kritické činnosti, pri ktorých môže zlyhanie spôsobiť neodstrániteľné škody na aktívach v prostredí cloud computingu. Príklady kritických činností sú: - inštalácia, zmeny a vymazanie virtualizovaných zariadení, ako sú servery, siete a úložiská - Postupy pri ukončení používania cloudových služieb - Zálohovanie a obnova. Tento dokument by mal stanoviť, že tieto činnosti bude sledovať dohľadový orgán.	Poskytovateľ cloudových služieb by mal poskytnúť dokumentáciu kritických činností a postupov zákazníkovi cloudových služieb, ktorí si ju vyžiadali.

ISO/IEC 27017

Príloha A

Cloud computing má výhodu rýchleho poskytovania a administrácie, tiež samoobslužných služieb na vyžiadanie. Tieto činnosti sú často realizované administrátormi zo strany zákazníka cloudových služieb a poskytovateľa cloudových služieb. Pretože ľudský faktor pri týchto kritických činnostiach môže spôsobiť vážne incidenty bezpečnosti informácií, mali by byť zvážené a v prípade potreby definované a implementované mechanizmy na zabezpečenie týchto činností.



Príklady vážnych incidentov zahŕňajú vymazanie alebo vypnutie veľkého počtu virtuálnych serverov alebo zničenie virtuálnych aktív.

ISO/IEC 27017

Príloha A

CLD.12.4 Zaznamenávanie formou logov a monitorovanie

Cieľ: Platí cieľ uvedený v 12.4 normy ISO/IEC 27001

CLD.12.4.5 Monitorovanie cloudových služieb

Zákazník cloudových služieb by mal mať schopnosť monitorovať určené aspekty fungovania cloudových služieb, ktoré zákazník cloudových služieb používa.



ISO/IEC 27017

Príloha A

CLD.13.1 Správa bezpečnosti siete

Cieľ: Platí cieľ uvedený v 13.1 normy ISO/IEC 27001

CLD.13.1.4 Koordinácia správy bezpečnosti virtuálnych a fyzických sietí

Po konfigurácii virtuálnych sietí by mala byť na základe politiky bezpečnosti siete poskytovateľa cloudových služieb overená konzistencia konfigurácií medzi virtuálnymi a fyzickými sieťami.

V prostredí cloud computingu postavenom na virtualizačných technológiách je virtuálna sieť konfigurovaná na virtuálnej infraštruktúre na fyzickej sieti. V takýchto prípadoch môže nekonzistencia sieťových politík spôsobiť výpadky systému alebo chybné riadenie prístupu.

V závislosti na type cloudových služieb sa môžu zodpovednosti za konfiguráciu virtuálnej siete presúvať medzi zákazníkom cloudových služieb a poskytovateľom cloudových služieb.

ISO/IEC 27018 - Informačné technológie – Bezpečnostné techniky – Súbor postupov na ochranu osobne identifikovateľných informácií (PII) vo verejných cloudoch vystupujúcich ako spracovatelia PII.

Obvykle organizácie implementujúce ISO/IEC 27001 chránia svoje vlastné informačné aktíva. V kontexte požiadaviek na ochranu **PII (osobne identifikovateľných informácií)** na poskytovateľov verejných cloudových služieb vystupujúcich ako spracovateľ PII však organizácie chránia informačné aktíva, ktoré mu zákazníci zverili.



ISO/IEC 27018

ISO/IEC 27018 má taktiež podobnú štruktúru ako ISO/IEC 27002 - kapitoly 5 až 18 a rozširuje opatrenia aby zodpovedali distribuovanej povahe rizika a existencie zmluvného vzťahu medzi **zákazníkom cloudových služieb** a **spracovateľom PII vo verejnom cloude**. Rozširuje ISO/IEC 27002 (resp. dokument SoA) dvomi spôsobmi:

- **Pokyny k implementácii použiteľné na ochranu PII vo verejnom cloude** pre niektoré opatrenia uvedené v ISO/IEC 27002
- **Príloha A** poskytuje sadu ďalších opatrení a pripojené pokyny, ktoré majú riešiť požiadavky na ochranu PII vo verejnom cloude, ktorými sa nezaoberá súbor opatrení ISO/IEC 27002.

ISO/IEC 27018

Príloha A

Príloha A – Súbor opatrení na ochranu PII rozšírený spracovateľom PII vo verejnom cloude

- špecifikuje nové opatrenia a pripojené pokyny k implementácii, ktoré v kombinácii s rozšírenými opatreniami (kapitoly 5-18), vytvoria súbor rozšírených opatrení k splneniu požiadaviek na ochranu PII, ktoré sa aplikujú na poskytovateľov služieb verejného cloudu, ktorí vystupujú ako spracovatelia PII.
- Tieto opatrenia sú rozdelené do nasledovných princípov súkromia:

ISO/IEC 27018

Príloha A

A.2 Súhlas a voľba

A.2.1 Závazok spolupráce týkajúci sa práv subjektov PII

- Spracovateľ PII verejného cloudu by mal zákazníkovi cloudových služieb poskytnúť prostriedky, umožňujúce plniť záväzok týkajúci sa zaistenia ľahšieho uplatnenia práv na prístup subjektov PII, úpravu a/alebo vymazanie PII s nimi spojených.

A.3 Legitimita a špecifikácia zámeru

A.3.1 Zámer spracovateľa PII vo verejnom cloude

- PII, ktoré majú byť spracovávané na základe zmluvy, by nemali byť spracovávané pre akýkoľvek účel nezávisle na inštrukciách zákazníka cloudových služieb.
- Inštrukcie môžu byť obsiahnuté v zmluve medzi spracovateľom PII vo verejnom cloude a zákazníkom cloudových služieb, zahŕňajúce napríklad cieľ a časový rámec, ktoré majú byť dosiahnuté danou službou.

A.3.2 Komerčné využitie spracovávateľa PII vo verejnom cloude

- PII spracovávané na základe zmluvy by nemali byť používané spracovateľom PII vo verejnom cloude na účely marketingu a reklamy bez výslovného súhlasu. Takýto súhlas by nemal byť podmienkou prijatia služby.

ISO/IEC 27018

Príloha A

A.5 Minimalizácia dát

A.5.1 Bezpečné vymazanie dočasných súborov

- Dočasné súbory a dokumenty by mali byť vymazané alebo zničené v rámci špecifikovaného dokumentovaného obdobia. Informačné systémy spracovávajúce PII by mali implementovať periodickú kontrolu, či sú nepoužívané dočasné súbory presahujúce špecifikovanú dobu životnosti vymazané.

A.6 Obmedzenie použitia, uchovávanía a sprístupnenia

A.6.1 Oznámenie o sprístupnenie PII

- Zmluva medzi spracovateľom PII vo verejnom cloude a zákazníkom cloudových služieb by mala vyžadovať, aby spracovateľ PII vo verejnom cloude informoval zákazníka cloudových služieb, v súlade s akýmkoľvek postupom alebo časovými úsekmi stanovenými v zmluve, o akejkoľvek právne záväznej požiadavke na sprístupnenie PII donucovacím orgánom (audítori vymáhajúci zákon), okrem prípadu, kedy je takéto sprístupnenie zakázané.

A.6.2 Zaznamenanie sprístupnenia PII

- Sprístupnenie PII tretím stranám by malo byť zaznamenané, vrátane informácií o tom, aké PII boli sprístupnené, komu a kedy.

ISO/IEC 27018

Príloha A

A.8 Otvorenosť, transparentnosť a upozornenia

A.8.1 Sprístupnenie subdodávateľského spracovávaní PII

- Využitie subdodávateľov spracovateľom PII verejného cloudu na spracovanie PII by malo byť sprístupnené príslušným zákazníkom cloudových služieb pred ich využitím.

A.10 Preukázateľná zodpovednosť

A.10.1 Oznámenia narušenie dát obsahujúce PII

- Spracovateľ PII vo verejnom cloude by mal okamžite upovedomiť príslušného zákazníka cloudových služieb o udalosti každého neautorizovaného prístupu k PII, alebo neautorizovaného prístupu k zariadeniam alebo vybaveniam na spracovanie vedúce k strate, odhaleniu alebo zmene PII.

A.10.2 Doba uchovávaní administratívnych bezpečnostných politík a smerníc

- Kópie bezpečnostných politík a prevádzkových postupov by mali byť uchovávané po určitú dobu a dokumentované pri výmene (vrátane aktualizácií).

A.10.3. Návrat , presun likvidácia PII

- Spracovateľ PII vo verejnom cloude by mal mať politiku týkajúcu sa návratu, presunu a/alebo likvidácie PII a mal by túto politiku sprístupniť zákazníkovi cloudových služieb.

ISO/IEC 27018

Príloha A

A.11 Bezpečnosť informácií

A.11.1 Dohody o zachovaní dôvernosti alebo mlčanlivosti

- Jednotlivé osoby s prístupom k PII by podľa opatrení spracovateľa PII verejného cloudu mali prijať záväzok zachovania mlčanlivosti.

A.11.2 Obmedzenie zariadenia hardcopy materiálu

- Zariadenie hardcopy materiálu, ktorý zobrazuje PII, by malo byť obmedzené.

A.11.3 Opatrenia na obnovenie dát a zaznamenávanie logov

- Mal by existovať postup pre snahu obnoviť dáta a jeho zaznamenávanie do logov.

A.11.4 Ochrana dát na pamäťových médiách mimo priestor organizácie

- PII na médiách mimo priestory organizácie by mali byť predmetom autorizačnej procedúry a nemali by byť prístupné nikomu inému než autorizovaným zamestnancom (napr. zašifrovaním dotýčnych dát).

A.11.5 Použitie nezašifrovaných prenosných pamäťových médií a zariadení

- Prenosné fyzické médiá a prenosné zariadenia, ktoré nedovoľujú šifrovanie, by nemali byť používané, okrem prípadu, kedy je to nevyhnutné, a každé použitie takéhoto prenosného média alebo zariadenia by malo byť zdokumentované.

ISO/IEC 27018

Príloha A

A.11.6 Šifrovanie PII prenášaných cez verejné dátové siete

- PII prenášané cez verejné dátové siete, by mali byť pred prenosom zašifrované.

A.11.7 Bezpečná likvidácia hardcopy materiálov

- Ak sú hardcopy materiály zničené, tak by mali byť zničené bezpečne pomocou mechanizmov ako je rozstrihanie, rozrezanie na malé kúsky, spálenie, skratovanie a pod.

A.11.8 Jedinečné použitie užívateľských ID

- Ak má prístup PII viac jednotlivých osôb, potom by mala mať každá z nich odlišné užívateľské ID pre identifikačné, autentizačné a autorizačné účely.

A.11.9 Záznamy autorizovaných užívateľov

- Aktualizovaný záznam užívateľov alebo profilov užívateľov, ktorí majú autorizovaný prístup k informačnému systému, by mal byť uchovávaný.



ISO/IEC 27018

Príloha A

A.11.10 Správa užívateľského ID

- Deaktivované alebo vypršané užívateľské ID by nemali byť pridelené ďalším jednotlivcom.

A.11.11 Zmluvné opatrenia

- Zmluvy medzi zákazníkom cloudových služieb a spracovateľom PII vo verejnom cloude by mali špecifikovať minimálne technické a organizačné opatrenia, zaisťujúce, že sú zavedené zmluvne viazané bezpečnostné opatrenia, a že dáta nie sú spracovávané pre akýkoľvek účel nezávisle na inštrukciách kontrolóra.

A.11.12 Subdodávateľské spracovanie PII

- Zmluvy medzi spracovateľom PII vo verejnom cloude a akýmkoľvek subdodávateľmi, ktorí spracovávajú PII, by mali špecifikovať minimálne technické a organizačné opatrenia, ktoré spĺňajú bezpečnosť informácií a záväzky týkajúce sa ochrany PII spracovávateľa PII vo verejnom cloude. Takéto opatrenia by nemali byť predmetom jednostranného obmedzenia zo strany subdodávateľa.

ISO/IEC 27018

Príloha A

A.11.13 Prístup k dátam v priestore používanom na ukladanie dát

- Spracovávateľ PII vo verejnom cloude by mal zaistiť, že kedykoľvek je zákazníkovi cloudových služieb pridelený priestor na uloženie dát, a akékoľvek dáta uložené skôr v tomto úložisku, nie sú pre tohto zákazníka cloudových služieb viditeľné.

A.12 Zhoda v oblasti súkromia

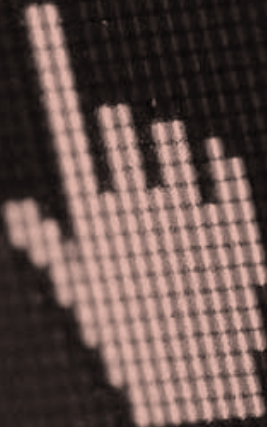
A.12.1 Geografické umiestnenie PII

- Spracovávateľ PII vo verejnom cloude by mal špecifikovať a dokumentovať krajiny, v ktorých by mohli byť PII eventuálne uložené.

A.12.2 Zamýšľané miesto určenia PII

- PII prenášané pomocou siete na prenos dát by mali byť predmetom príslušných opatrení, ktoré boli navrhnuté k zaisteniu, že dáta dosiahli zamýšľané miesto určenia.





Security

Ďakujem za pozornosť

ECTA, s.r.o.

Mgr. Monika Jaborníková
Senior Consultant, internal auditor

www.ecta.sk