**Témou mojej prezentácie je šifrovanie dát v službe Google Cloud.**

Ako prvé si povedzme aké druhy šifrovania máme vo všeobecnosti. Môžeme hovoriť o šifrovaní v troch rôznych **podobách**: šifrovanie v „**pokoji**“, šifrovanie pri **prenose** dát a šifrovanie pri **využívaní** dát.

Šifrovanie v „**pokoji**“ je to, čo používame na ochranu dát v prípade exfiltrácie, napríklad ak dôjde k odcudzeniu zariadenia.. Je to základná vrstva ochrany v zariadení.

Šifrovanie pri **prenose** chráni dáta keď sú presúvané medzi dvoma rôznymi lokáciami – spočíva z autentifikácie koncových bodov, zašifrovania informácií, skontrolovania prenosu a odšifrovania informácií keď prenos prebehol úspešne.

Šifrovanie pri **využívaní** dát ochraňuje dáta pri ich spracovávaní serverom – je to pomerne nový koncept v krypto-komunite.

**Pozrime sa ďalej akým spôsobom je možné chrániť dáta v súčasnosti:**

**Menšie** podniky a start-upy, bez dostatočnej infraštruktúry na manažovanie šifrovania, dáta často nešifrujú vôbec, alebo sa spoliehajú, že to za ne spraví ich cloud-provider.

**Väčšie** spoločnosti väčšinou majú spôsob ktorým spravujú šifrovacie kľúče, anglicky „key management service“ alebo KMS. Zaoberá sa generovaním, výmenou, uchovávaním, ...atd. šifrovacích kľúčov.

**Sofistikovanejšie** spoločnosti zvyčajne mávajú oveľa komplexnejšie hierarchiu kľúčov – na ochranu dát nepoužívajú iba jeden kľúč, ale viacero vrstiev kľúčov – teda samotné kľúče sú ďalej šifrované ďalšími kľúčmi. Pri tomto spôsobe šifrovania sa môže práca s nimi stať náročnou, hlavne ak sa pracuje s veľkým objemom dát. Preto býva využívaný tzv. „hardware security module“ alebo HSM, fyzické zariadenie, ktoré stráži a spravuje digitálne kľúče a ponúkajú účinnú autentifikáciu.

**Ako šifruje údaje Google?**

Google údaje uložené užívateľom šifruje automaticky, bez potreby nijakého dodatočného nastavenia. Pre väčšinu bežných údajov je toto šifrovanie úplne dostačujúce.

Druhý spôsob šifrovania dát sú „zákazníkom spravované šifrovacie kľúče“ (cusomer managed encryption keys) alebo CMEK, využívajúce Cloudový KMS systém. Je to verejne dostupný spôsob ochrany dát. Umožňuje generovanie kľúčov, ich využívanie, rotáciu, atd... Je to ideálne pre ľudí, ktorí chcú byť schopní sami si spravovať vlastné šifrovacie kľúče.

Tretí spôsob, ktorý je zatiaľ ponúkaný jedine Googlom, sú „zákazníkom dodávané šifrovacie kľúče“ (customer supplied encryption keys) alebo CSEK. Pri tomto spôsobe Google neukladá zákazníkom poskytnuté informácie nikde u seba.

**Rozoberme si teda „default-né“ šifrovanie od Googlu:**

Na pochopenie šifrovania Googlom je potrebné najskôr rozumieť ako ukladá informácie. Keď je nejaký objekt nahraný na úložisko Google Cloud, Google ho rozdelí na menšie časti „chunk-y“, a každý „chunk“ dostane lokálne generovaný a jedinečný šifrovací kľúč, tzv. DEK. Tento kľuč sa líši pre každý „chunk“, aj v prípade že patrí jednému užívateľovi, alebo aj keď tieto časti tvoria súčasť toho istého súboru. Prístup k týmto častiam je spravovaný takzvaným „access controll list-om“.

Tieto časti sú v Googli uchovávané pre prípad obnovy dát, ale nedochádza pri tom k ich odšifrovaniu – sú uchovávané zašifrované. Keby teda niekto chcel prísť do Googlu a ukradnúť informácie, ukradnúť hardware, musel by najskôr vedieť kde sú jednotlivé chunky do ktorých bol súbor rozdelený uložené, čo je takmer nemožné, pri tom s akým množstvom údajov Google pracuje, musel by mať prístup ku všetkým chunkom, a musel by mať tiež prístup ku všetkým kľúčom, ktoré tieto chunky šifrujú.

**Takže kde sú tieto kľúče uchovávané?**

Sú ukladané v podstate vo forme „hlavičky“ daného data chunku. Samozrejme ale nie sú zapísané vo forme plain textu, ale sú šifrované tzv. KEK, „key encryption key“. Tieto sú uložené v interných KMS systémoch Googlu. Má nízku latenciu, vysokú dostupnosť a teda v praxi to znamená, že beží na desiatkach tisícoch produkčných mašinách v datacentrách Googlu.

**V praxi to teda funguje tak, že:**

Predstavme si že máme troch aktérov – službu, ktorá využíva dáta, úložný systém, ktorý šifrované dáta ukladá, a KMS, ktorý ukladá šifrovacie kľúče šifrovacích kľúčov. Služba si vyžiada od úložného systému určitý objekt, ten verifikuje, že služba má mať umožnený prístup k tomuto objektu, zistí v ktorých chunkoch je tento objekt uchovávaný a potom vytiahne šifrovacie kľúče uložené v chunkoch a posunie ich ešte zašifrované do KMS. KMS potom verifikuje či úložný systém má právo pristupovať ku šifrovacím kľúčom daných šifrovacích kľúčov, odšifruje šifrovacie kľúče a posunie ich naspäť odšifrované úložnému systému. Úložný systém potom odšifruje dáta týmito kľúčmi a posunie ich službe, ktorá si ich vyžiadala.

**Toto bolo v skratke ako funguje Google úložisko.**