VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

DIGITÁLNÍ FORENZNÍ ANALÝZA PROSTŘEDÍ HYBRIDNÍHO CLOUDU

DIGITAL FORENSICS OF THE HYBRID CLOUD ENVIRONMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **ANNA KRČÁLOVÁ**
AUTHOR

VEDOUCÍ PRÁCE **doc. Ing. ONDŘEJ RYŠAVÝ, Ph.D.**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Zadání bakalářské práce

157013

Ústav: Ústav informačních systémů (UIFS)
Studentka: **Krčálová Anna**
Program: Informační technologie
Název: **Digitální forenzní analýza prostředí hybridního cloudu**
Kategorie: Bezpečnost
Akademický rok: 2023/24

Zadání:

1. Nastudujte existující metody forenzní analýzy hybridních cloudových prostředí.
2. Pro vybranou cloudovou aplikaci (Google, Office365, AWS), vytvořte vhodné experimentální prostředí.
3. Prostudujte možnosti auditu aktivit uživatelů a dalších funkcí, které prostředí nabízí a jsou použitelné pro digitální forenzní analýzu.
4. Navrhněte a realizujte různé situace zneužití cloudového prostředí vhodných pro digitální forenzní analýzu.
5. Navrhněte a demonstrujte postup získávání a analýzy důkazů z cloudového prostředí.
6. Vytvořte metodologii pro postup digitální forenzní analýzy hybridního cloudové prostředí.
7. Vyhodnoťte a demonstrujte navrhnutou metodologii na vhodných případech užití.

Literatura:

- Agbedanu PR, Wang P, Nortey RN, Odartey LK. Forensics in the Cloud: A Literature Analysis and Classification. *Proc - 5th Int Conf Big Data Comput Commun BIGCOM 2019*. Published online 2019:124-132. doi:10.1109/BIGCOM.2019.00027
- NIST. NIST - Draft NISTIR 8006 - NIST Cloud Computing Forensic Science Challenges. *Nist*. Published online 2014. Dostupné na: http://safegov.org/media/72648/nist_digital_forensics_draft_8006.pdf
- Yankson B, Davis A. Analysis of the current state of cloud forensics: The evolving nature of digital forensics. *Proc IEEE/ACS Int Conf Comput Syst Appl AICCSA*. 2019;2019-Novem. doi:10.1109/AICCSA47632.2019.9035336

Při obhajobě semestrální části projektu je požadováno:
Body zadání 1-4.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Ryšavý Ondřej, doc. Ing., Ph.D.**
Vedoucí ústavu: Kolář Dušan, doc. Dr. Ing.
Datum zadání: 1.11.2023
Termín pro odevzdání: 9.5.2024
Datum schválení: 30.10.2023

Abstrakt

Práce pojednává o digitální forenzní analýze hybridního cloudu v kombinaci Google Cloudu a Nextcloudu. V práci je rozvedeno několik příkladů událostí, při jejichž řešení by byla analýza vhodná, a to od původní identifikace problému, přes zadržení dat, až po forenzní analýzu a výstup z ní. Součástí práce je i zkrácený postup nastavování hybridního cloudu a logování.

Abstract

The bachelor thesis deals with the digital forensic analysis of the hybrid cloud in the combination of Google Cloud and Nextcloud. Several examples of events in the solution of which analysis would be appropriate are detailed in the thesis, from the initial identification of the problem, through the retention of data, to the forensic analysis and its output. The work also includes a shortened procedure for setting up the hybrid cloud and logging.

Klíčová slova

Digitální forenzní analýza cloudu, cloud, vzdálené úložiště, hybridní cloud, metodika, artefakty, zneužití cloudu

Keywords

Cloud Digital Forensics, Cloud, Remote Storage, Hybrid Cloud, Methodology, Artifacts, Cloud Abuse

Citace

KRČÁLOVÁ, Anna. *Digitální forenzní analýza prostředí hybridního cloudu*. Brno, 2024. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce doc. Ing. Ondřej Ryšavý, Ph.D.

Digitální forenzní analýza prostředí hybridního cloudu

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně pod vedením doc. Ing. Ondřeje Ryšavého, Ph.D. Uvedla jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpala.

.....
Anna Krčálová
15. května 2024

Poděkování

Předně bych chtěla poděkovat svému vedoucímu doc. Ing. Ondřeji Ryšavému Ph.D. za jeho čas a trpělivost. Dále také své rodině, příteli a kamarádům za psychickou podporu v průběhu nejenom psaní této práce, ale i celého studia.

Obsah

Seznam obrázků

Kapitola 1

Úvod

Podle článku[1] využívá hybridní řešení cloudů až 80 procent organizací. Jeho používání může otevřít spoustu nových cest například při sdílení dat mezi organizacemi. Toto číslo je již teď značně vysoké a v budoucnu se bude pravděpodobně stále zvyšovat. Stále více však stoupá i motivace útočníků získávat data právě odsud. Proto, aby se dalo útokům předcházet, je potřeba správně zabezpečit svoje cloudové řešení, nejlépe i znát možnosti zneužití, a správně monitorovat a auditovat veškerou aktivitu. V případě hybridního řešení je důležité znát všechny části cloudu, veřejnou i soukromou část, jeho síťové propojení a vědět, kde v případě potřeby hledat samotné digitální důkazy o konkrétních aktivitách, kterými může být třeba jenom přihlášení uživatele. Prostředí hybridního cloudu nabízí komplexní, bohaté, zároveň i ne úplně prozkoumané prostředí pro forenzní vyšetřování. Jelikož je forenzní analýza cloudů disciplínou, se kterou se začalo teprve nedávno, je potřeba v ní pokročit a být krok napřed před možnými útočníky.

Cílem této práce je vytvořit metodologickou příručku k získávání artefaktů z hybridního cloudu. Jelikož není možné analyzovat všechny možné technologie, byla pro toto řešení vybrána kombinace `Nextcloudu` a `Google Cloudu`. Příručka byla vytvořena tak, aby dle ní mohli postupovat jak zkušenější jedinci, jako forenzní analytici, tak i nezasvěcení jednotlivci, kteří se jen zajímají o to, co se děje v jejich cloudovém úložišti.

V jednotlivých kapitolách této práci budou nejprve popsány základní teoretické pojmy, které jsou potřebné pro pochopení práce, a to v kapitole 2. Budou taktéž popsány způsoby, jak si zprovoznit svůj hybridní cloud, jak nastavit logování, aby bylo následně možné sledovat aktivitu (nejen) „útočníka“, to lze najít v kapitole 3. Budou vytvořeny jednotlivé případy zneužití, na kterých bude ukázáno, jak je možné útoky detekovat, jaké artefakty lze získat, a to v kapitolách 4 a 5 a na závěr budou tyto postupy vyhodnoceny a seskupeny – kapitola 6. Výstupem této práce pak bude metodologická příručka a vhodné virtuální prostředí pro ukázání popsaných příkladů. Tato prostředí i s příručkou budou poskytnuty vybraným jedincům pro vyzkoušení a podle jejich odpovědí na dotazníky bude vyhodnocena její kvalita.

[1] https://explodingtopics.com/blog/corporate-cloud-data

Kapitola 2

Teoretická část

Aby bylo možné hlouběji pochopit cíl této práce, je zapotřebí si hned v úvodu vysvětlit a zadefinovat klíčové pojmy, které se budou prolínat celou prací. Tato kapitola bude rozdělena do několika sekcí, ve kterých budou postupně představeny hlavní klíčové pojmy této práce, které jsou důležité pro jednoznačné pochopení práce, konkrétně toho, co je to digitální forenzní analýza, cloud jako takový a nebo s jakými výzvami je možné se při jeho analýze potkat. Dále budou představeny i nejčastější metody zneužití cloudu a techniky, které jsou pro analýzu cloudů specifické.

2.1 Digitální forenzní analýza

Digitální forenzní analýza je soubor technik a nástrojů používaných pro hledání důkazů na počítači s cílem získat usvědčující digitální důkazy [20] [3]. Hlavním cílem digitální forenzní analýzy je extrahovat a analyzovat data z důkazů, zpracovat je a předložit jako poznatky k dalšímu zkoumání. Všechny procesy využívají vhodné forenzní techniky, aby bylo zajištěno, že nálezy budou u soudu přípustné [8]. Zároveň je možné jej využít pro interní vyšetřování, například při řešení bezpečnostních incidentů.

Díky forenzní analýze lze určit například motiv činu, totožnost pachatele, odhad potencionální škody, zároveň je zde často možnost obnovy smazaných dat a mnoho dalších. Důležité také je získání postupů, které útočník použil, čímž lze do budoucna zabránit jejich opakování [23].

Jde o několika-fázový proces, jehož výsledkem je v případě potřeby předložit výstupy jako důkaz u soudu během soudního řízení. Těmito fázemi jsou [17]:

Identifikace – V první fázi je třeba identifikovat potenciální zdroje relevantních důkazů, informací a zařízení, stejně jako umístění těchto dat.

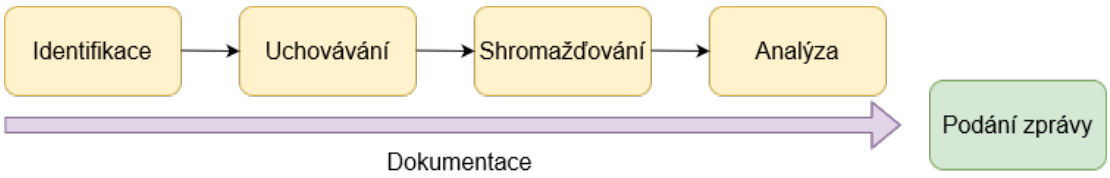
Uchovávání – Proces uchovávání relevantních elektronicky uložených informací se provádí ochranou místa činu zachycením vizuálních obrazů a zdokumentováním všech relevantních informací o důkazech a způsobu jejich získání.

Shromažďování – Shromažďování digitálních informací, které mohou být relevantní pro vyšetřování. Sběr může zahrnovat odstranění elektronického zařízení z místa činu a následné zobrazení, zkopírování nebo vytištění jeho obsahu.

Analýza – Analýzou je myšleno hloubkové systematické vyhledávání důkazů týkajících se vyšetřovaného incidentu. Výstupem vyšetření jsou datové objekty nalezené ve shro-

máždených informacích. Tyto výstupy mohou zahrnovat systémové a uživatelem generované soubory. Cílem analýzy je vyvodit závěry na základě nalezených důkazů.

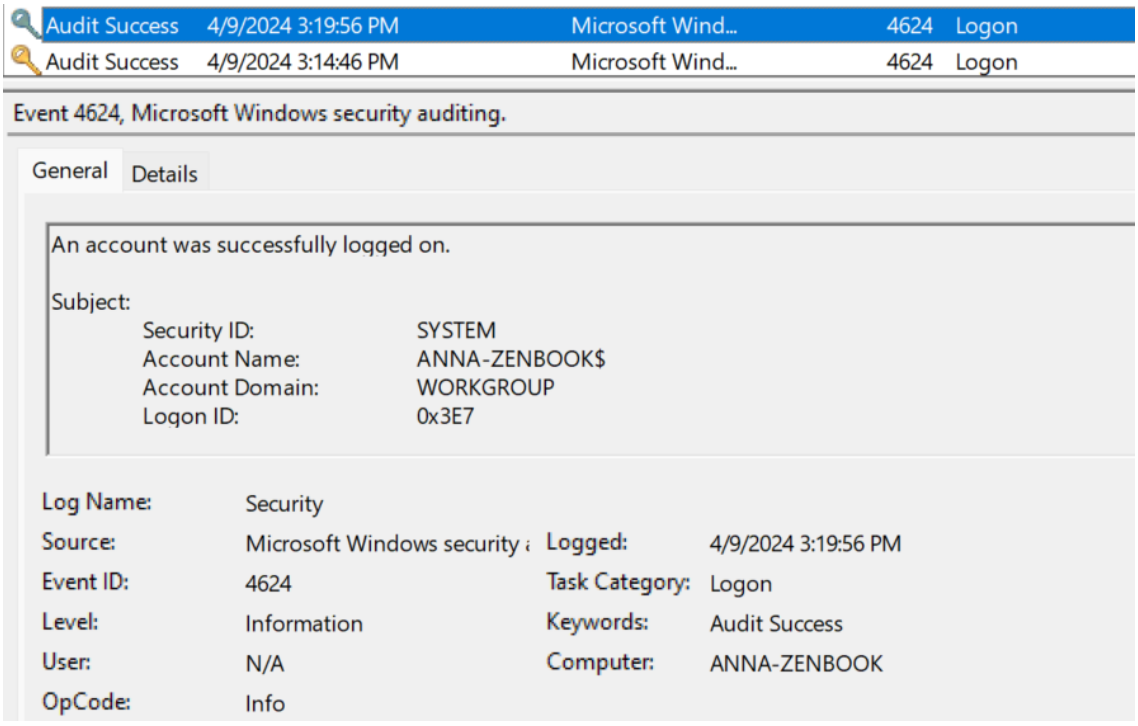
Podání zprávy – Zpráva je založena na osvědčených technikách a metodologii. Je důležité, aby pokud někdo další analyzuje stejný případ, aby zprávy uváděly stejné výsledky.



Obrázek 2.1: Proces digitální forenzní analýzy.

2.1.1 Elektronické důkazy aneb artefakty

Během analýzy dat se objevují indikátory narušení útočníkem, ty se označují jako elektronické důkazy nebo také artefakty. Elektronické důkazy lze shromažďovat z celé řady zdrojů, jako jsou nejen počítače, telefony, vzdálené úložiště (cloudy), chytré hodinky, ale třeba i čipy aut. Jako příklad je možné ukázat artefakt o přihlášení uživatele 2.2 z Prohlížeče událostí (Event Viewer), kde je možné vidět přihlášení účtu `ANNA-ZENBOOK$` na počítači `ANNA-ZENBOOK`. $ v názvu indikuje, že jde o takzvaný „účet počítače“.



Obrázek 2.2: Artefakt o přihlášení účtu ANNA-ZENBOOK$.

2.1.2 Protokolování událostí neboli logování

Protokolování událostí je proces zaznamenávání informací o tom, co se děje v systému, aplikaci nebo jakémkoliv softwarovém nebo hardwarovém zařízení. Jednotlivé záznamy se pak označují jako logy událostí. Běžně se v tomto kontextu používají z angličtiny převzaté pojmy `logování` a `logy`. Jelikož jde o již zaběhnuté termíny a jejich používání usnadní pochopení, budou i nadále v této práci využívány, tedy logování – protokolování událostí a log – protokol.

Logy jsou pravidelným nebo systematickým záznamem akcí, které objekt provedl, nebo stavů, kterými objekt byl. Je to nejběžnější součást, která se používá v digitální forenzní analýze [21]. Tři příklady takových logů jsou logy **auditu, zabezpečení** a logy **aplikací**. Logy auditu jsou záznamy interakcí mezi službami a základním operačním systémem. Logy zabezpečení sledují uživatele k akcím tak, že identifikují konkrétního uživatele, který provedl akci v určité datum a v určitou dobu. Logy aplikací zaznamenávají aktivitu generovanou aplikacemi spolu s chybami a dalšími provozními závadami aplikací [12].

2.2 Forenzní analýza cloudu

Forenzní analýzu cloudu lze definovat jako proces využívání dostupných nástrojů a metodologií ke shromažďování a analýze kompromitovaných dat nebo systému v cloudovém prostředí [2].

Při analýze cloudu je nutné analyzovat datové toky ve třech hlavních fázích – data v klidu na serverech, data v klidu na klientských zařízeních a data v přenosu [27]. Proto je důležité provádět statickou i dynamickou analýzu aplikací nainstalovaných na klientském zařízení, analýzu datové komunikace a exfiltračních kanálů, a další [4].

Cloudové služby je obzvláště obtížné prozkoumat, protože mohou být obtížně přístupné nebo agregovatelné kvůli oddělení povinností mezi aktéry a nedostatečné transparentnosti dat logů pro spotřebitele [12].

2.2.1 Forenzní analýza cloudu vs. Digitální forenzní analýza

Ačkoli se pojmy `Forenzní analýza cloudu` a `Digitální forenzní analýza` používají zaměnitelně, jsou mezi němi rozdíly. Digitální forenzní analýza zahrnuje shromažďování, analýzu a uchovávání dat z **elektronických zařízení**, jako jsou počítače, notebooky, mobilní telefony a další paměťová média. Na druhou stranu cloudová forenzní vyšetřuje data uložená v **cloudovém úložišti** [25]. Kromě rozsahu vyšetřování se liší i v dalších bodech, příkladem mohou být:

Způsob sběru dat – Při analýze cloudu je nezbytné získat povolení od poskytovatele služeb pro přístup k důkazním datům z cloudového serveru.

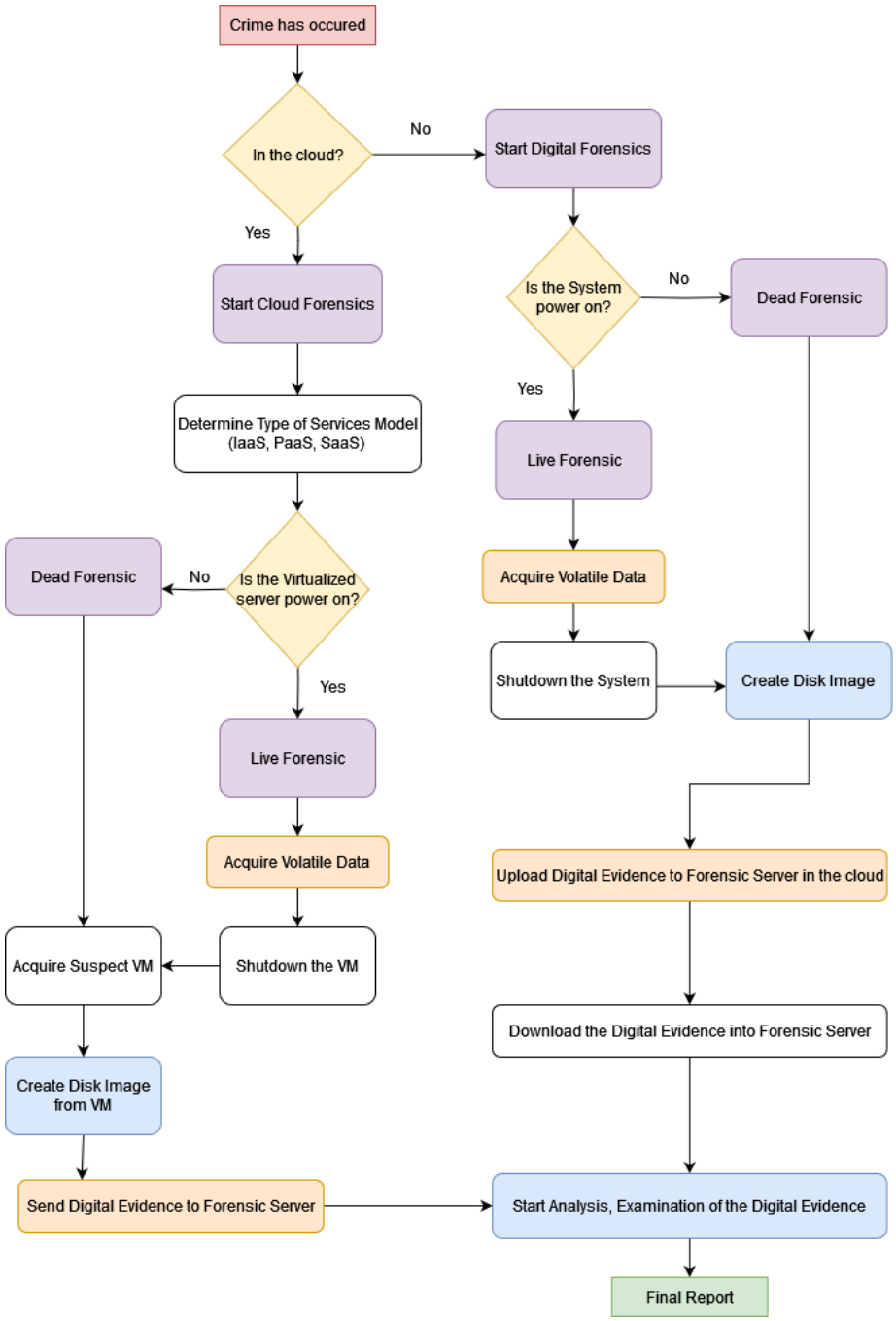
Ochrana dat – U analýzy cloudu musí poskytovatelé služeb udělit přístup k důkazům a společnosti ukládat důkazy na základě právních norem.

Právní důsledky – Cloud má více právních aspektů kvůli složitosti cloudové infrastruktury a získávání souhlasu od poskytovatelů cloudových služeb.

Rozdíl je také u získávání artefaktů. V tradiční digitální forenzní analýze je vyšetřovatelům umožněno mít plnou kontrolu nad forenzními artefakty – ať už logy směrovačů,

procesů, nebo přímo pevné disky. V cloudech se kontrola nad funkčními vrstvami liší u jednotlivých aktérů cloudu v závislosti na modelu cloudové služby. Proto mají vyšetřovatelé nižší úroveň viditelnosti a kontroly nad forenzními artefakty [36].

I když se tedy digitální a cloudová forenzní analýza zabývá vyšetřováním digitální trestné činnosti, jsou v každé oblasti vyžadovány různé dovednosti a odborné znalosti. Na následujícím obrázku 2.3 lze vidět porovnání těchto procesů. Rozdíl mezi nimi teoreticky není velký, jde ale o důležité detaily [25].



Obrázek 2.3: Rozdílné postupy digitální forenzní analýzy a forenzní analýzy cloudu [11].

2.3 Cloud

Cloudy jsou rozsáhlé sítě vzdálených serverů po celém světě, které jsou propojeny a mají fungovat jako jeden ekosystém. Tyto systémy jsou navrženy tak, aby ukládaly a spravovaly data, spouštěly aplikace nebo doručovaly obsah nebo službu, jako je streamování videí, webová pošta nebo sociální média. Místo přistupování k souborům a datům z osobního počítače se k nim přistupuje online z jakéhokoli zařízení, co má připojení k internetu a standardní prohlížeč [31].

2.3.1 Druhy cloudů

Cloudy lze dělit minimálně dvěma způsoby – na základě typu nasazení a na základě služeb.
Je pět způsobů, jak dělit cloudy **na základě nasazení**.

Veřejný cloud – Ve veřejném cloudu jsou veškeré výpočetní zdroje vlastněny a provozovány poskytovatelem cloudových služeb třetí strany a uživatelé k nim mají přístup přes internet. Je to nákladově nejefektivnější cloudový model, protože snižuje náklady společností na vývoj a údržbu. Uživatelé platí pouze za to, co používají.

Soukromý cloud – Soukromý cloud využívá a udržuje výhradně jedna organizace. Může být hostován v místě organizace nebo v datovém centru poskytovatele cloudu. Soukromý cloud poskytuje nejvyšší úroveň zabezpečení a kontroly.

Hybridní cloud – U hybridního cloudu jde o kombinaci veřejných a soukromých cloudů, která usnadňuje využívání výhod obou modelů. Umožňuje bezproblémový přenos dat mezi veřejnými a soukromými cloudovými systémy. Jelikož jde o klíčovou část této práce, bude jí věnováno více prostoru v následující sekci 2.4.

Komunitní cloud – Model nasazení, ve kterém je integrováno několik cloudových infrastruktur, které řeší potřeby konkrétní komunity. Komunitní cloud tedy sdílejí organizace s podobnými potřebami a zájmy.

Multi-cloud – Používá více úložných zařízení v jedné architektuře; sdílí zdroje pouze mezi organizacemi, například s vládními institucemi Je možné využívat kombinaci veřejných a privátních cloudů. Snižuje závislost na jediném dodavateli, což usnadňuje škálovatelnost, flexibilitu a redundanci. [32] [25].

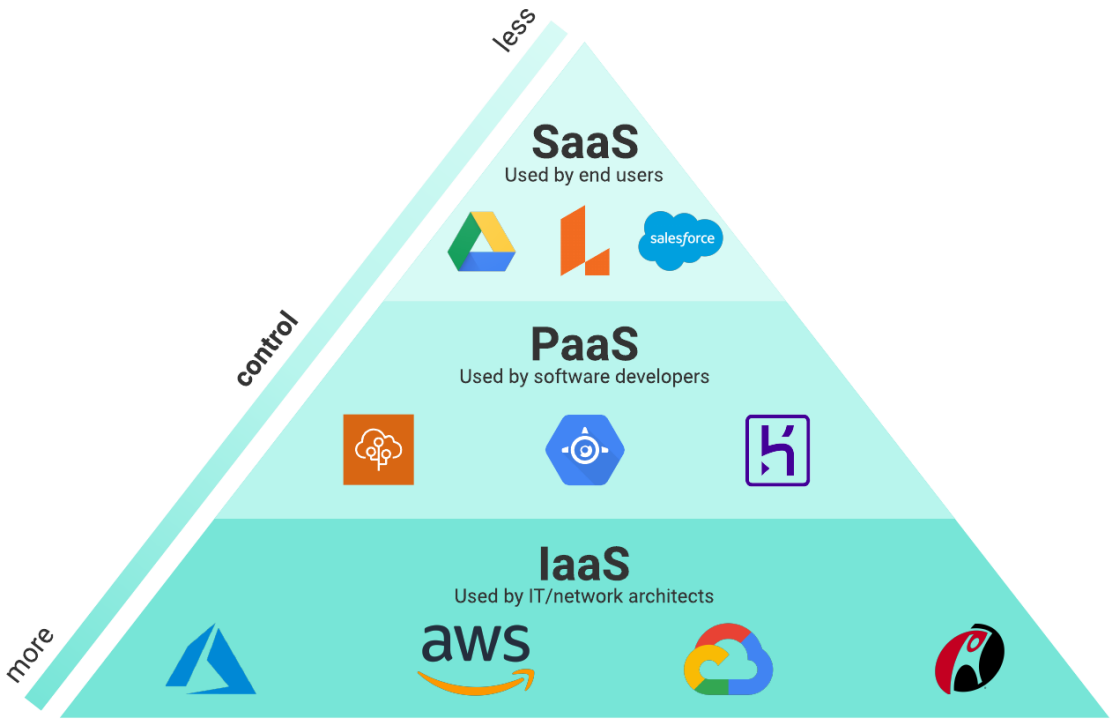
Na základě služeb lze dělit cloudy podle tří hlavních modelů. Každý nabízí různé úrovně abstrakce a kontroly nad základní výpočetní zdroje [25].

IaaS neboli infrastruktura jako služba Uživatel si pronajímá pouze infrastrukturu, tedy server, úložiště a sítě, na nichž vyvíjí vlastní software. Infrastruktura je plně škálovatelná, takže může využívané servery rozšiřovat či snižovat na základě aktuálních potřeb.

PaaS neboli platforma jako služba Poskytuje uživatelům přístup k vývojářským nástrojům, které mu umožní vytváření a správu aplikací, aniž by musel investovat do podpůrné serverové infrastruktury. Narozdíl od SaaS si tedy v tomto případě klient platí i za komponenty infrastruktury. PaaS využívají zejména vývojáři, analytici či profesionální správci IT.

SaaS neboli software jako služba Uživatel si v tomto případě pronajímá koncovou službu, tedy aplikaci či program. V praxi se jedná např. o různé kancelářské balíčky jako Microsoft Office, ale i jiné programy. Veškerou správu hardwaru i softwaru obstarává poskytovatel. Saas se vyplatí hlavně zaměstnancům v netechnologických firmách a koncovým uživatelům. Umožňuje rychlé zprovoznění a poskytuje přístup k novým technologiím [6].

Mnoho organizací využívá infrastrukturu veřejného cloudu jako službu (IaaS) ke zpracování některých úloh, zatímco jiné si ponechávají ve svém soukromém cloudu, ať už z důvodu nákladů, souladu s předpisy nebo z technologických důvodů. Nejběžnějšími veřejnými poskytovateli IaaS jsou Amazon Web Services (AWS), Microsoft Azure a platforma Google Cloud (GCP) [34]. Na obrázku 2.4 je možné vidět porovnání těchto modelů na základě pravomocí, které zde má uživatel. Největší kontrolu mají u IaaS, naopak nejmenší v SaaS. Zároveň jsou zde znázorněny i konkrétní platformy.



Obrázek 2.4: Porovnání toho, jakou kontrolu mají uživatelé v jednotlivých modelech [26].

2.4 Hybridní cloud

Hybridní cloud je kombinace soukromých a veřejných cloudových služeb, které mohou sdílet a migrovat aplikace a data přes připojení k rozsáhlé síti (WAN) [30], a které spolupracují a podporují celou organizaci [16]. Tato konfigurace umožňuje, že se data a aplikační zátěže mohou plynule přesouvat mezi platformami a sdílet data mezi aplikačními zátěžemi. Toho je dosaženo virtualizací dat a pracovních zátěží, virtualizací síťových funkcí (NFV) nebo VPN a konektivitou k jednomu nebo více poskytovatelům cloudu. Hybridní cloud rozšiřuje

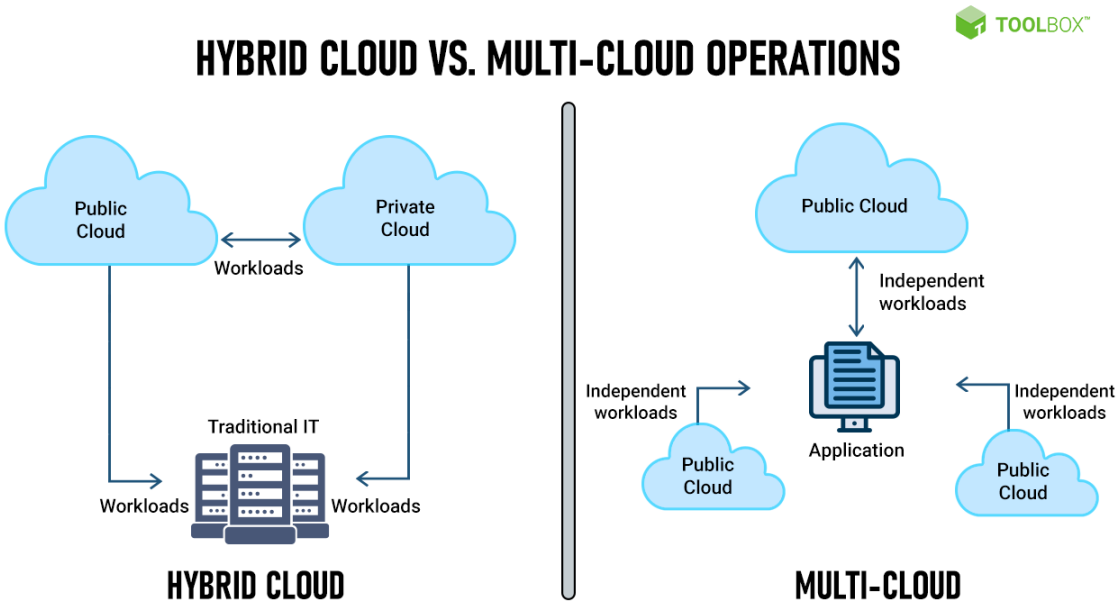
infrastrukturu a provoz konzistentně a poskytuje jednotný operační model, který spravuje aplikační zátěže napříč oběma prostředími, což umožňuje bezproblémovou migraci zátěží ze soukromého do veřejného cloudu nebo z něj [33]. V mnoha případech nabízí hybridní cloudy řešení mezi výhodami moderní cloudové technologie a praktickými omezeními cloudových možností, například když se jedná o vysoce výkonnostně náročné výpočty [16].

Hybridní cloudová řešení umožňují migrovat a spravovat pracovní zátěže mezi různými cloudovými prostředími. Hybridní cloud je dnes jedním z nejběžnějších nastavení infrastruktury. Migrace cloudu často přirozeně vedou k implementacím hybridního cloudu, protože organizace musí často převádět aplikace a data pomalu a systematicky. Hybridní cloudová prostředí umožňují nadále používat místní služby a zároveň využívat flexibilní možnosti ukládání a přístupu k datům a aplikacím, které nabízejí poskytovatelé veřejných cloudů, jako je Google Cloud [28].

2.4.1 Rozdíl mezi hybridním cloudem a multicloudem

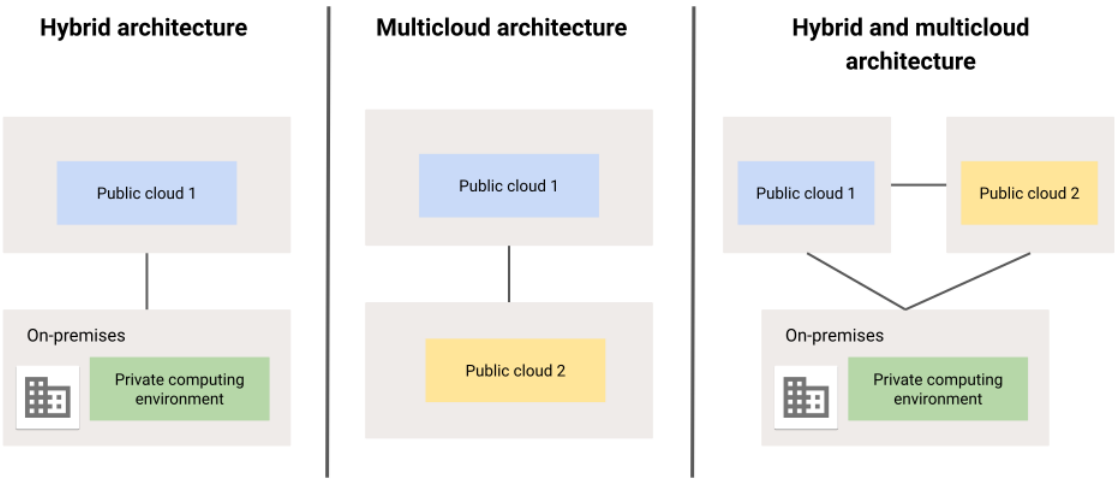
Hybridní cloud – Nabízí různé propojené veřejné a soukromé cloudy, které spolupracují, sdílejí data a procesy za účelem provádění stejného úkolu.

Multicloud – Využívá služeb z **více cloudů stejného typu** k provádění různých úkolů, bez ohledu na to, kde jsou hostovány [28].



Obrázek 2.5: Rozdíl mezi hybridním cloudem a multicloudem, převzato z [13]

Hybridní cloudový přístup lze také považovat za multicloud, pokud zahrnuje zdroje ze soukromého cloudu a zdroje od alespoň dvou poskytovatelů veřejných cloudových služeb viz 2.6. Tedy nastavení multicloudu zahrnují nastavení hybridního cloudu, ale hybridní cloud není automaticky považován za multicloud [28].



Obrázek 2.6: Ukázka hybridního multicloudu; převzato z [22]

2.4.2 Základní komponenty hybridního cloudu

Sjednocující povaha hybridní cloudové infrastruktury znamená, že je složitější než pouhé nastavení veřejného nebo privátního cloudu. Migrace dat přes více vrstev, centralizované přístupy a kontroly, jednotné procesy ověřování a autorizace jsou zde výzvou. Kromě toho se bezpečnostní kontroly musí měřit s větší plochou útoku, kterou hybridní cloud přináší.

S ohledem na toto vše se typická hybridní cloudová infrastruktura skládá z následujících komponent [15]:

Veřejný a soukromý cloud, který není třeba opětovně popisovat, viz 2.3.1.

Integrátory Celý koncept hybridního cloudu závisí na tom, jak dobře jsou stávající komponenty propojeny a nastaveny pro nadcházející rozšíření. Mezi každým prvkem musí být aktivní komunikace. To je obvykle implementováno pomocí aplikačních programovacích rozhraní (`API`), virtuálních privátních sítí (`VPN`) a rozlehlých sítí (`WAN`). Každá z těchto metod musí být bezpečná, aby se zabránilo ztrátě dat, kompromitaci nebo krádeži.

Datová struktura Datová struktura, nebo také datová tkanina, umožňuje organizacím spravovat data, která proudí mezi jednotlivými segmenty. Je podobná vazbě rozprostřené přes každý přístupový a úložný bod v architektuře. Tyto body mohou být kdekoli – veřejný cloud, soukromý cloud nebo tradiční on-premise systémy. Usnadňuje zpracování, přesun, ukládání a údržbu dat na jakémkoli místě uvnitř, to znamená, že existuje více než jedna cesta k získání přístupu v daný okamžik. Pokud je jedno spojení přetíženo, systém najde jiné cesty k dokončení dané akce.

Jednotné nástroje pro správu Správce hybridního cloudu funguje jako centrální přístupový bod ke všem prostředím, ve kterých technologie běží. To zahrnuje propojení

různých přihlašovacích systémů, různých funkcí a různých manipulací s daty. Mezi tyto nástroje patří:

Centralizovaná IAM napříč prostředími – Centrální systém se zásadami jednotného přístupu usnadňuje údržbu uživatelů a audit činnosti uživatelů. To pomáhá identifikovat špatné uživatele, anomálie v chování uživatelů a dodržování předpisů.

Integrovaná síť se segmentací – WAN je síť sítí. Přenáší provoz mezi více nezávislými sítěmi a funguje na základě virtualizace, zásad na úrovni aplikací a překryvných sítí.

Správa zdrojů – Software pro správu je nezbytný pro alokaci zdrojů na základě požadavků aplikace.

Řešení pro monitorování – Umožňuje odhalit redundanci a nevyužité servery. Pomáhá také vyhnout se zbytečným nákladům. Řešení centrálního logování a hlášení také umožňuje bezpečnostním týmům být proaktivní a umožňuje hladší audity dodržování předpisů.

Nástroje pro správu dat – Umožňují vytvářet a udržovat zásady a logy, které nastiňují, jak musí být data organizace uložena, spravována a používána.

2.4.3 Výhody a nevýhody hybridních cloudů

Kromě běžných výhod cloudových platforem přináší hybridní zapojení nové, důležité výhody. Zároveň však i nějaké nevýhody hybridního cloudu.

Výhody

Většina organizací přijala hybridní cloudovou infrastrukturu, aby snížila rizika, minimalizovala celkové náklady na IT a cloud, aby měla větší kontrolu nad správou zdrojů, a aby splnila sezónní špičky v poptávce po výpočetních a úložných zdrojích (takzvaný „Cloud bursting"[1]) [33] [15].

Mezi hlavní **výhody** hybridních cloudů patří i možnost modernizace vlastním tempem, tedy to, že s hybridním cloudem je možné migrovat aplikace postupně. Jeho architektura umožňuje nejprve přesunout front-endové a bezstavové aplikace do cloudu a poté přenést další aplikace, jako virtuální počítače, kontejnery, a podobně [34]. Hybridní cloudy také urychlují nový vývoj tím, že umožňují nasazení vznikajících aplikací s nevyzkoušenou zátěží. To umožňuje předpovídat zdroje potřebné k provozování jejich operací s minimální počáteční investicí.

Nevýhody

Vzhledem k tomu, že modely hybridního cloudu zahrnují použití soukromého cloudu a místní infrastruktury, stále jsou zde určité **nevýhody**, které je potřeba vzít v úvahu. Jde zejména o [29]:

Náklady – Počáteční nasazení síťové architektury stojí více než pouhé použití veřejného cloudu. K nasazení v prostorách je zapotřebí investice do hardwaru, jako jsou soukromé servery. S přibývajícím výkonem se také zvýší hodinové poplatky.

[1] **„Cloud bursting"** je schopnost správce hybridního cloudu expandovat a půjčovat si z veřejných cloudových zdrojů, když soukromé cloudy dosáhnou své kapacity [15].

Kompatibilita – Kompatibilita cloudu může být problémem, proto je důležitý pečlivý výběr kombinace cloudu. IT týmy musí rozumět tomu, jak jejich platformy a aplikace spolupracují, aby dosáhly optimálního výkonu. Rychle výkonná místní infrastruktura nemusí být schopna úspěšně fungovat v kombinaci s pomaleji výkonnou architekturou veřejného cloudu, což vede k pomalé hybridní cloudové síti.

Management – Je podstatné mít přehled o dostupných zdrojích a pravidelně kontrolovat dostupné nástroje, které mohou pomoci se správou hybridního cloudu.

Přijetí hybridního cloudu často vyžaduje nové technické znalosti jak od IT týmů, tak od podnikových uživatelů. Nastavení a údržba prostředí vyžaduje technické znalosti a pečlivou konfiguraci, aby byla zajištěna bezproblémová integrace a zabezpečení. Prostředí hybridního cloudu může být také složité. Může být obtížné získat přehled o všech systémech, aplikacích, platformách a procesech v hybridním cloudu, což může způsobit promeškání kritických problémů nebo příležitostí [28].

2.5 Výzvy spojené s forenzní analýzou cloudu

Forenzní analýza cloudů je relativně novou oblastí forenzní vědy a jako taková čelí při vyšetřování v cloudových prostředích spoustě výzvám. Je třeba zmínit, že většina prezentovaných výzev se týká zejména veřejných cloudů.

Výzvou pro organizace sledující hybridní cloud je hledání provozního model, který zjednodušuje operace, snižuje složitost správy, zvyšuje flexibilitu a zároveň řeší požadavky aplikačních architektur [33];

Jednotlivé výzvy lze rozřadit do různých kategorií, mezi které patří [12]:

Výzvy spojené s architekturou – Zde se řadí například vypořádání se s variabilitou cloudových architektur mezi poskytovateli nebo přesný a bezpečný původ dat pro zachování spotřebitelského řetězce.

Výzvy při sběru dat – Lokalizace forenzních artefaktů ve velkých, distribuovaných a dynamických systémech, lokalizace a sběr nestálých dat, sběr dat z virtuálních strojů, integrita dat v prostředí s více nájemci, kde jsou data sdílena mezi více počítači na více místech (a přístupná více stranám), neschopnost zobrazit všechny forenzní artefakty v cloudu nebo přístup k údajům jednoho nájemce bez porušení důvěrnosti ostatních nájemců. To vše a mnohem více může být forenzní výzvou při sběru dat.

Výzvy v průběhu analýzy – Zde může jít o korelaci forenzních artefaktů napříč cloudovými poskytovately, rekonstrukci událostí z virtuálních obrazů nebo úložiště, problémy s integritou metadat nebo časová analýza dat logů, včetně synchronizace časových razítek.

Výzvy spojené s první reakcí na incidenty – Zde jde o potíže při provádění počátečního třídění, či zpracování velkého objemu shromážděných forenzních artefaktů. Řadí se sem ale i nutná důvěra v poskytovatele – třeba důvěra v to, že bude udržovat důvěryhodné logy o cloudové aktivitě a na požádání – například na soudní příkaz – bude poskytovat zprávy o aktivitách uživatelů, kteří jsou důležití v průběhu vyšetřování [4].

Výzvy při správě rolí – Mezi tyto výzvy se řadí správa identit, vlastnictví dat, autentizace a řízení přístupu a nebo problém se snadnou anonymitou a vytváření fiktivních identit online.

Technické výzvy Technických výzev je spousta. Jsou to takové výzvy, které mohou nastat například v důsledku chyby technického rázu [25].

Nedostatek fyzického přístupu – Jedna z největších výzev cloudových forenzních vyšetřovatelů je nedostatek fyzického přístupu k základnímu hardwaru a infrastruktuře. Poskytovatelé cloudových služeb mají často bezpečnostní kontroly a postupy – vyšetřovatelé musí pracovat v rámci těchto omezení. Může to ztížit sběr a analýzu digitálních důkazů, protože vyšetřovatelé nemusí mít přístup ke všem relevantním údajům.

Dynamické prostředí – Cloudová prostředí jsou vysoce dynamická, zdroje a data se neustále pohybují a mění. Je proto náročné zachytit snímek prostředí v konkrétním čase. Navíc mohou virtuální stroje a kontejnery ztížit určení umístění dat a prostředků v cloudovém prostředí.

Šifrování dat – K ochraně dat při přenosu a v klidu se šifrování, což ztěžuje přístup a analýzu digitálních důkazů. Použití šifrování může také zkomplikovat proces získávání dat, protože před analýzou je třeba získat přístup k datům a dešifrovat je.

Migrace bez refaktoringu – Pokud jsou aplikace migrovány z odlišných prostředí, potřebují aplikace během migrace časově náročné a nákladné refaktorování. Konzistentní infrastruktura umožňuje rychlou a nízkonákladovou migraci do cloudu, a v případě potřeby i snadnou migraci zpět [33].

Zabezpečení a zásady konzistence – U hybridního cloudu je důležité umět propojit zásady zabezpečení a dodržování předpisů s pracovní zátěží, aby bylo možné zásady konzistentně vynucovat [33].

Udržování spotřebitelského řetězce – Známé jako `Chain of Custody`, může být pro digitální důkazy v cloudových prostředích náročné. Je nutné prokázat, že důkazy nebyly nijak zmanipulovány ani pozměněny, což při práci v dynamickém a distribuovaném cloudovém prostředí může být obtížné [25].

Právní výzvy – V neposlední řadě jsou zde také výzvy právní. Stejně jako u každého digitálního forenzního vyšetřování musí cloudové forenzní řešení splňovat příslušné zákonné požadavky [25]. A to ať už jde o otázky jurisdikce, různým předpisům o ochraně osobních údajů, určování vlastnictví dat v cloudových prostředí nebo problémy s důkazními standardy.

Aby se právním problémům předešlo, tak musí organizace úzce spolupracovat s právními experty, aby bylo zajištěno, že vyšetřování bude v souladu se všemi platnými zákony a předpisy [25].

Další příklady i s jejich popisy a možným výsledkem po překonání výzvy lze vidět v dokumentu od NIST, v příloze A s názvem `Cloud Forensic Challenges` [12].

2.6 Forenzní techniky specifické pro vyšetřování cloudů

V prostředí, kde mohou být data rozptýlena napříč různými cloudovými službami a geografickými lokacemi, poskytují tyto techniky možnost sledovat a dokumentovat stopy digitální

aktivity. Jsou důležitou částí forenzního vyšetřování, jelikož umožňují shromažďovat, analyzovat a uchovávat digitální důkazy při vyšetřování bezpečnostních incidentů, narušení dat a dalších digitálních zločinů v cloudovém prostředí [25].

Akvizice paměti virtuálního stroje Cloudové systémy často běží na virtuálních strojích. Ke shromažďování důkazů z virtuálního stroje používají forenzní vyšetřovatelé speciální techniky k získávání paměti z virtuálního stroje. To zahrnuje vytvoření snímku paměti virtuálního stroje, který lze analyzovat, identifikaci procesů, otevřených souborů a síťových připojení.

Analýza síťových paketů Při analýze síťových paketů se zachycuje a analyzuje síťový provoz v cloudovém prostředí. Tato technika umožňuje identifikovat síťové útoky, podezřelé vzorce provozu a neoprávněné přenosy dat.

Analýza logů specifických pro cloud Poskytovatelé cloudu obvykle generují logy, které zaznamenávají systémové události, aktivity uživatelů a další aktivity v prostředí cloudu. Nástroje pro analýzu logů specifické pro cloud shromažďují a analyzují tyto logy, aby identifikovaly podezřelé aktivity, bezpečnostní incidenty a neoprávněný přístup. Vybrané nástroje budou později popsány v kapitole 2.7.

Analýza logů řízení přístupu Logy řízení přístupu zaznamenávají aktivity uživatelů související s řízením přístupu v cloudovém prostředí. Pomocí těchto logů je možné určit, kdo měl přístup ke konkrétním zdrojům, kdy k nim přistupoval, a jaké akce provedl.

2.7 Forenzní nástroje k analýze cloudů

Forenzní analýza cloudů může být obtížná bez specifických nástrojů vyvinutých pro usnadnění procesu shromažďování důkazů. Data totiž nemusí být zpočátku ve formátu vhodném pro shromažďování jako digitální důkaz, a proto je nutné „dekódovat“ log používaný aplikací nebo operačním systémem pro ukládání anebo přenos dat [25].

Konkrétně v této práci však nebude potřebné používat speciální nástroje, jelikož důkazní materiály, které budou k analýzám připojeny, budou logy v `.log` a `.json`, případně `.eml` formátu, které není nutné dekódovat – jsou uloženy v čisté formě. Jediným potřebným nástrojem zde bude 2.7.1. Logy budou následně ručně zpracovávány.

2.7.1 Google Cloud Audit Logs

Logy Google Cloud, často označované jako `Cloud Audit Logs`, jsou nástrojem pro monitorování a analýzu logů, který poskytuje podrobné logy o aktivitě uživatelů a systémových událostí v prostředí Google Cloud. Tyto logy zachycují informace související s různými službami, zdroji a akcemi uživatelů a pomáhají monitorovat a analyzovat aktivity v rámci cloudové infrastruktury. Umožňují tak forenzním vyšetřovatelům identifikovat anomálie a řešit bezpečnostní incidenty.

Cloud Audit Audit Logs poskytuje několik typů logů auditu, z nichž každý slouží specifickému účelu při monitorování a sledování aktivit v cloudovém prostředí [5]. Jde o:

Administrátorská činnost – Administrativní akce provedené v rámci projektu GCP, jako je vytváření, úprava nebo mazání zdrojů. Tyto logy například zaznamenávají, vytváření instance virtuálních počítačů nebo změny oprávnění správy identit a přístupu.

Přístup k datům – Zaznamenává akce související s přístupem nebo úpravou dat v rámci konkrétních služeb GCP. Jde o čtení nebo zápis dat do cloudového úložiště, přístup k záznamům v databázi nebo aktualizace nastavení konfigurace. Logy přístupů k datům jsou uloženy v segmentu logů `\Default`.

Systémové události – Záznamy související s událostmi na úrovni systému a změnami v prostředí GCP. Jde zde o změny v konfiguraci sítě, úpravy pravidel brány firewall nebo o aktualizace nastavení projektu.

Události odepřené zásadami – Zachycuje události, ke kterým byl přístup odepřen na základě zásad IAM.

Mezi další, stále velice důležité logy patří události autentizace nebo logy z kontejnerových akcí. Logy jsou primárně generovány dvěma různými mechanismy.

Nativní logy auditu platformy – Zachycují události a aktivity na úrovni systému.

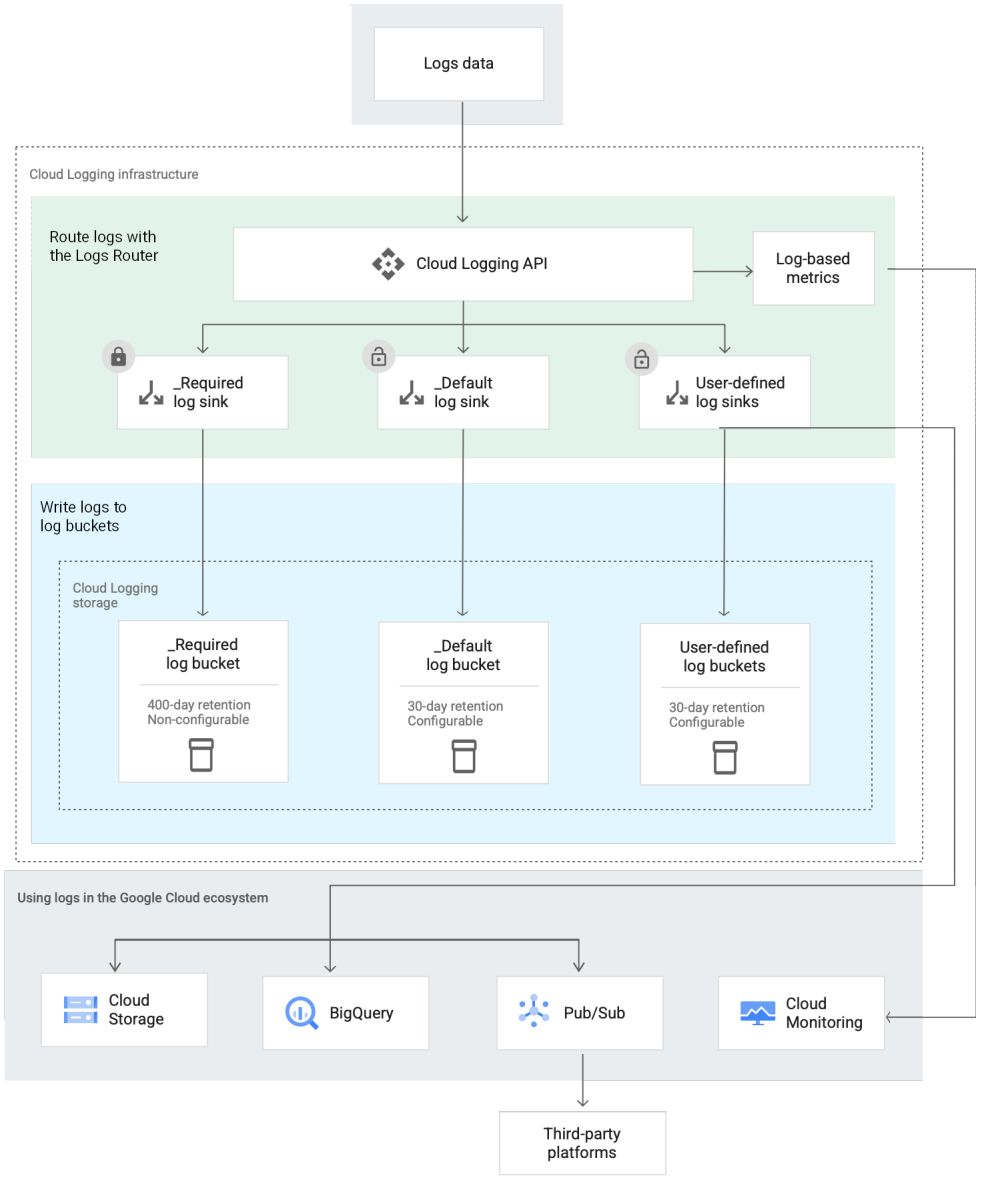
Logy generované aplikacemi (službami) ve virtuálních strojích – Zahrnují širokou škálu logů, od logů vytvářených webovými službami provozovanými na virtuálních počítačích až po logy provozu a další.

Google Cloud automaticky zaznamenává sadu akcí a konkrétní kategorie těchto akcí spadá do segmentu `\Required` logů. Tyto logy jsou trvale povoleny a jejich uložení není zpoplatněno. Jsou klíčové pro zachycování událostí s vysokou prioritou, které jsou nezbytné pro zachování bezpečnosti, to zahrnuje události, jako jsou přihlášení uživatelů a administrativní změny provedené v rámci platformy.

V rámci Google Cloud existuje další skupina logů, které se ukládají do segmentu `\Default` logů. Tyto logy jsou ve výchozím nastavení povoleny a primárně se zaměřují na zachycení odepřených akcí. Tyto logy je možné uchovávat až po dobu až 30 dnů bez dalších nákladů [5]. Více lze vidět na obrázku 2.7.

2.8 Zneužití cloudu

Vznik cloudů přinesl významný posun ve způsobu, jakým organizace spravují svá data a IT infrastrukturu. Přestože nabízejí spousty výhod, čelí také řadě kybernetických hrozeb, které přináší nová rizika a hrozby. Ty mohou ohrozit integritu, dostupnost, ale i důvěrnost dat. Pro implementaci účinných bezpečnostních opatření je zapotřebí tyto hrozby prvně znát. V této sekci budou představeny nejběžnější kybernetické hrozby, kterým cloudové infrastruktury čelí [25].



Obrázek 2.7: Rozdělení zaznamenávaných logů v GCP [19].

Únik dat – K porušení dat dochází, když neoprávněné osoby získají přístup k citlivým nebo důvěrným údajům. K narušení dat může dojít, když útočníci zneužijí zranitelnosti cloudové infrastruktury nebo aplikací. Pokud systém poskytovatele cloudových služeb není řádně zabezpečen, může útočník získat přístup k datům uloženým v cloudu.

Vnitřní hrozby – Vnitřní hrozby, známé též jako `insiders`, představují významné riziko pro bezpečnost cloudu. Zasvěcení lidé mohou záměrně nebo náhodně zneužít svůj přístup do cloudu ke krádeži nebo úniku citlivých dat. Mohou také smazat, upravit nebo poškodit data. Zasvěcenci mohou zahrnovat zaměstnance, dodavatele nebo partnery s legitimním cloudovým přístupem.

DoS útoky – DoS neboli `Denial of Service`, doslovně přeloženo jako „odmítnutí služby“, je útok, který může být spuštěn proti cloudové infrastruktuře, čímž se stane

nedostupnou pro legitimní uživatele. Tyto útoky jsou obvykle prováděny zahlcením systému provozem, což způsobí jeho zhroucení. DoS útoky mohou spustit jednotlivci, hacktivisté nebo aktéři národního státu.

Malwarové nebo ransomwarové útoky – Malware a ransomwarové útoky mohou být použity k infikování cloudů. Malware lze použít ke krádeži dat, logování stisknutých kláves nebo k získání přístupu do cloudového systému. Ransomware dokáže zašifrovat data tak, že budou nepoužitelná, dokud nebude zaplaceno výkupné.

Cryptojacking – Cryptojacking zahrnuje použití počítače oběti nebo cloudových zdrojů k těžbě kryptoměny. Útočníci mohou získat přístup ke cloudové infrastruktuře a nainstalovat software pro těžbu kryptoměn bez vědomí nebo souhlasu vlastníka. Může to mít za následek výrazné zvýšení využití procesoru a zpomalení cloudových aplikací.

Phishing – Phishingové útoky a útoky sociálního inženýrství mohou uživatele přimět k odhalení jejich přihlašovacích údajů nebo jiných citlivých informací. Tyto útoky mohou být e-maily, rychlé zprávy nebo příspěvky na sociálních sítích, které vypadají, že pocházejí z důvěryhodného zdroje. Jakmile útočníci získají přístup ke cloudovému systému, mohou ukrást data, přesměrovat provoz na škodlivé stránky, zahájit další útoky nebo způsobit poškození systému.

APTs – APTs [2] jsou dlouhodobé a cílené kybernetické útoky, při kterých útočník proniká do sítě, aby časem ukradl data. Cloudové infrastruktury lze zacílit tak, aby získaly přístup k velkému množství dat.

2.8.1 Lidské faktory

Je třeba brát v potaz, že i přes kvalitní bezpečnostní zabezpečení může dojít k nesprávné konfiguraci, nedostatku řádného řízení přístupu či dalším lidským chybám, které mohou potenciálně vést ke zneužití. Může jít například o:

- Nedostatečnou kontrolu přístupu.
- Nesprávné umístění dat.
- Nezabezpečené konfigurace sítě.
- Otevřené porty a nezabezpečené koncové body API.
- Nedostatek monitorování a logování.
- Chybějící postupy zálohování a obnovy.

2.8.2 Sám útočník používající cloud

Je potřeba myslet i na to, že cloud může zneužít i sám zločinec, který by jej mohl využívat k ukládání a skrývání inkriminovaných a nelegálních materiálů nebo k distribuci materiálů chráněných autorským právem. Dalším běžně se vyskytujícím kriminálním zneužíváním cloudu je podpora provádění rozsáhlých a distribuovaných útoků, například kompromitováním některých instancí virtuálních strojů v cloudové infrastruktuře za účelem spuštění útoků Distributed Denial-of-Service (DDoS) proti třetím stranám [4].

[2] APT, neboli Advanced Persistent Threat, lze do češtiny přeložit jako „Pokročilá trvalá hrozba“. Jde o sofistikovaný a dlouhodobý kybernetický útok zaměřený na proniknutí do specifických cílů s cílem krást data nebo provádět špionáž, zatímco zůstává nedetekován.

Kapitola 3

Návrh řešení práce

Prvním krokem při řešení této práce je výběr a konfigurace vhodných platforem a jejich následné propojení za účelem vytvoření hybridního cloudu. Další fází práce je nastavení logovacích mechanismů na těchto platformách. Následuje výběr relevantních use-case scénářů, které demonstrují možnosti forenzní analýzy hybridních cloudů. Tento výběr umožňuje praktickou aplikaci a evaluaci forenzních metodik. Výstupem práce je realizace vybraných scénářů, provedení detailní analýzy a formulace metodiky, která bude dokumentovat zjištěné postupy a výsledky.

3.1 Nastavení hybridního cloudu

Základem této práce je nastavení hybridního cloudu, tedy propojení privátního a veřejného cloudu. Dlouho jsem se rozhodovala, zda použít již funkční hybridní cloudovou platformu, jako je `Google Anthos`, nebo se pokusit vytvořit vlastní prostředí. Nakonec jsem zvolila cestu, kdy se sama pokusím vytvořit vlastní hybridní cloud, a to s vědomím, že to bude obtížnější cesta. Při hledání požadovaných informací jsem totiž nenarazila na žádné relevantní články o tom, jak se takový hybridní cloud dá vytvořit za domácích podmínek, což mě zaujalo a chtěla jsem to prozkoumat. Mojí motivací tedy bylo hlavně zdokumentovat postup a zjistit, jak obtížné je takový cloud nastavit. Pro toto řešení jsem tedy vybrala Nextcloud, jako řešení privátního cloudu, a Google Cloud, jako cloud veřejný. Hlavním důvodem výběru těchto platforem bylo to, že díky své rozšířenosti jsou tyto dvě platformy známé většině uživatelům, používání Nextcloudu je velice jednoduché a přímočaré a na obou platformách se pracuje dosti efektivně. U Google Cloudu navíc vyhrála i cena za užívání.

Obě použité platformy budou následně krátce představeny, a to jak fungují jednotlivě, dohromady, potom jak je propojit a jak správně nastavit logování. V této části bude čerpáno zejména z dokumentace Google Cloudu[1] a dokumentace Nextcloudu[2]. Části, které nebudou ozdrojovány jinak, jsou přebraty právě z těchto dokumentů.

3.1.1 Nextcloud

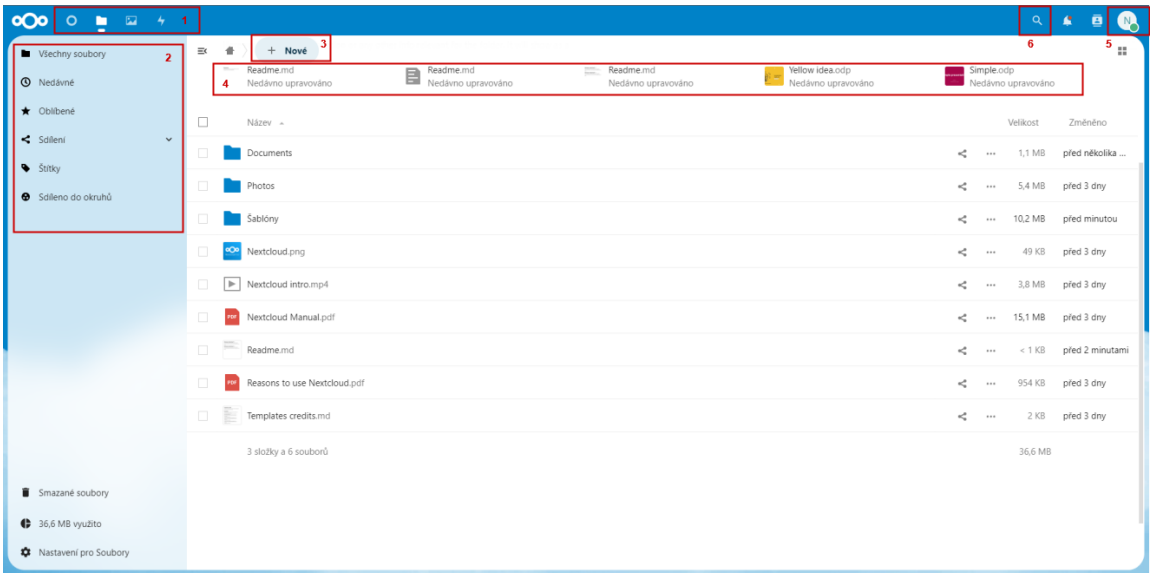
Nextcloud byl vybrán jako řešení soukromého cloudu. Je to odnož předcházejícího projektu Owncloud. Jedná se o bezplatný open-source software, který také nabízí hostování služeb. Kdokoli si jej může nainstalovat a používat na soukromém serveru. Nextcloud upřednostňuje bezpečnost a soukromí a má několik externích penetračních testerů a odborníků. Mají také

[1] https://cloud.google.com/docs
[2] https://docs.nextcloud.com/

program, ve kterém lidem platí za to, že najdou a nahlásí zranitelnost, takzvané „bug bounty“. Je vhodný jak pro organizace, tak i pro jednotlivce [9]. Nextcloud je možné nasadit například na Docker nebo do virtuálního prostředí.

Mezi výhody Nextcloudu patří zejména to, že jde o open-source projekt, tedy na opravě chyb se může podílet několik lidí najednou, dále je to cena – sám o sobě je Nextcloud zdarma a je možné jej hostovat i na levných, jednoprocesorových počítačích, jako je Raspberry Pi (pak jde o NextcloudPi). Další výhodou je vysoká bezpečnost, jelikož data můžou být teoreticky doma s uživatelem a tedy uživatel má plnou moc nad svými daty. Zároveň Nextcloud podporuje dvoufaktorovou autentizaci, šifrování a podobně [1]. Obsahuje také funkce pro řízení a monitorování dat a komunikace, včetně funkcí Řízení přístupu k souborům a pracovních postupů nebo rozsáhlých logů auditu. Právě ty budou využity v této práci.

Webové rozhraní Nextcloudu je jednoduché pro pochopení, lze jej vidět na obrázku 3.1. Skládá se z několika základních komponent, kterými jsou: (1) – Nabídka aplikací; (2) – Pole s informacemi o aplikaci; (3) – Tlačítko pro přidání nebo nahrání nových souborů; (4) – Poslední otevřené soubory; (5) – Profil a nastavení; (6) – Vyhledávací pole.



Obrázek 3.1: Přehled základních komponent Nextcloudu.

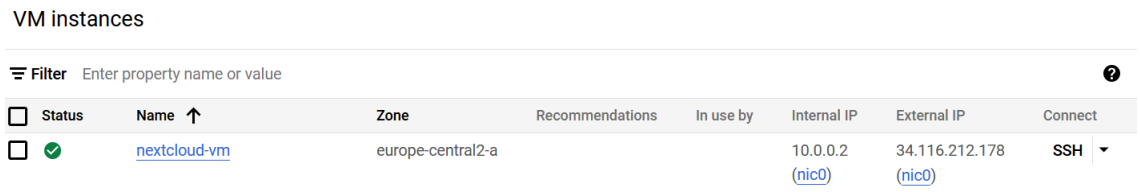
Nastavení Nextcloudu

Mnou navrhnuté řešení mělo původně využívat NextcloudPi, které by běželo na Raspberry Pi 5. NextcloudPi však nepodporuje nejnovější verzi Raspberry Pi, což jsem zjistila až když bylo pozdě. Samotný Nextcloud použitý pro tuto práci tedy běží ve virtuálním stroji na Ubuntu přímo v Google Compute Engine (viz 3.1.2) a je v tomto případě je dostupný na IP `34.116.212.178`.

Nastavení Nextcloudu ve virtuálním stroji může postrádat výhody běžného privátního cloudu, jelikož je i tak zapojen vzdáleně. Každopádně kdyby neběžel v Compute Engine, ale na jakémkoli jiném stroji například doma na Linuxu, fungoval by stejně, a pro demonstraci této práce toto zapojení nepřináší žádná změny.

Kdyby však někdo měl takto zapojený cloud v reálném životě, přineslo by to snížení bezpečnosti dat na privátním cloudu. Pokud by došlo ke krádeži přihlašovacích údajů do Google Cloudu, mohl by být privátní cloud v něm nasazený v ohrožení – mohl by být

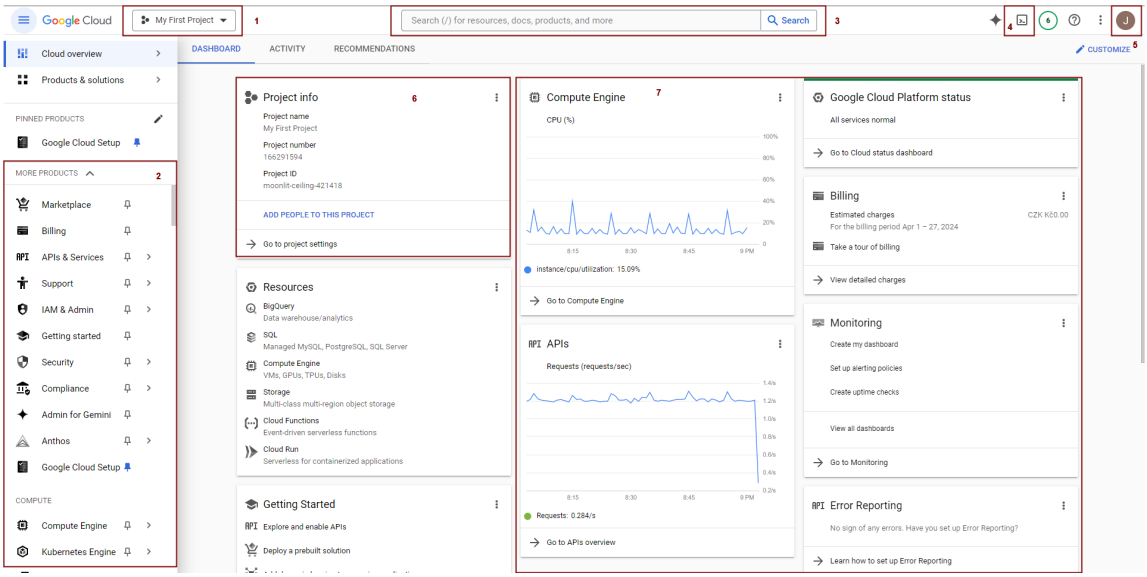
kompromitován, zároveň by však mohl být celý virtuální stroj, na kterém privátní cloud běží, smazán a smazání virtuálního stroje v GCP je nezvratné. Do běžné praxe je tedy vhodnější nasadit cloud buď na vlastní server nebo právě na Raspberry Pi.



Obrázek 3.2: Virtuální stroj, na kterém běží Nextcloud v Google Compute Engine.

3.1.2 Google Cloud

Google Cloud, často také jako **Google Cloud Platform** (zkráceně GCP), je primární poskytovatel cloudových služeb od společnosti Google. Poskytuje různé výpočetní služby a služby zpracování dat, které umožňují analýzy a optimalizaci procesů. Funguje na stejné infrastruktuře, kterou Google interně používá pro své produkty, jako je vyhledávač Google, Gmail, úložiště souborů a YouTube. Přístup k serverům je udržován nepřetržitě [14]. GCP byla pro tuto práci vybrána hlavně z důvodu její potenciální rozšiřitelnosti v budoucnu. GCP lze považovat za velmi efektivní nástroj pro ukládání a zpracování obrovského množství dat, který umožňuje výrazné úspory nákladů a zdrojů. Mezi jeho další výhody patří zejména vysoká bezpečnost nebo jeden z největších přístupů ke globální síti [14]. Na obrazku 3.3 je možné vidět základní komponenty GCP, kterými jsou: (1) – Přehled projektů; (2) – Rozcestník produktů; (3) – Vyhledávací pole (produktů, dokumentace,...); (4) – Cloud Shell; (5) – Profil a jeho nastavení; (6) – Základní info o prohlíženém projektu; (7) – Přehledové tabulky.



Obrázek 3.3: Základní přehled v GCP.

Hierarchie Google cloudu

Hierarchie Google Cloud popisuje, jak jsou zdroje, řízení přístupu a zásady strukturovány. Díky pochopení hierarchie mohou zasahující rychle posoudit rozsah incidentu, určit postižené oblasti a zaměřit své úsilí na omezení, vyšetřování a nápravu.

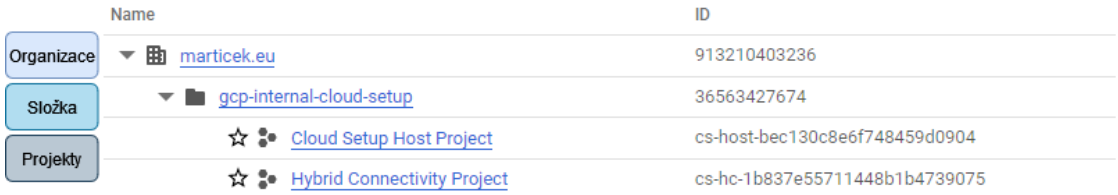
Nejdůležitějšími prvky hierarchie GCP jsou:

Organizace Entita nejvyšší úrovně, organizace, poskytuje široký pohled na všechny zdroje a projekty v prostředí GCP. Organizace je životně důležitá pro komplexní pohled na zdroje a projekty. Během incidentu umožňuje bezpečnostním týmům rychle identifikovat rozsah problému ve všech projektech a zdrojích. Centralizovaná správa identit a přístupu je zásadní pro zajištění toho, aby se do procesu reakce na incidenty mohli zapojit pouze oprávnění pracovníci.

Složka Složky nabízejí způsob, jak strukturovat vaše zdroje do logických skupin, jako jsou oddělení, týmy nebo projekty, což umožňuje lepší organizaci a alokaci zdrojů. Složky pomáhají logicky strukturovat zdroje a často odrážejí hierarchii oddělení nebo projektu organizace. V případě incidentu je toto logické seskupení neocenitelné pro izolaci a správu zdrojů ovlivněných incidentem. Umožňuje také aplikaci konkrétních zásad k účinnému omezení a zmírnění problému.

Projekt V projektech se vytvářejí a spravují vaše zdroje, jako jsou virtuální stroje a databáze. Jsou to pracovní prostory pro jednotlivé iniciativy ve vaší organizaci. Každý projekt je nezávislým pracovním prostorem pro zdroje. Týmy pro reakci na incidenty mohou tuto nezávislost využít k izolaci postižených zdrojů a provádění forenzních vyšetřování, aniž by to mělo dopad na jiné projekty. Bezpečnostní ovládací prvky jedinečné pro každý projekt lze upravit tak, aby reagovaly na konkrétní hrozby.

Zdroje Zdroje jsou skutečné cloudové služby a infrastruktura, jako jsou virtuální stroje, databáze a úložiště, které vytváříte v rámci projektů. Zdroje představují cloudové služby a infrastrukturu, kde jsou umístěny aplikace a data. Během incidentu je důležité rychle identifikovat, které zdroje jsou ohroženy nebo ohroženy.



Obrázek 3.4: Ukázka hierarchie Google cloudu tak, jak ji je možno vidět přímo v GCP.

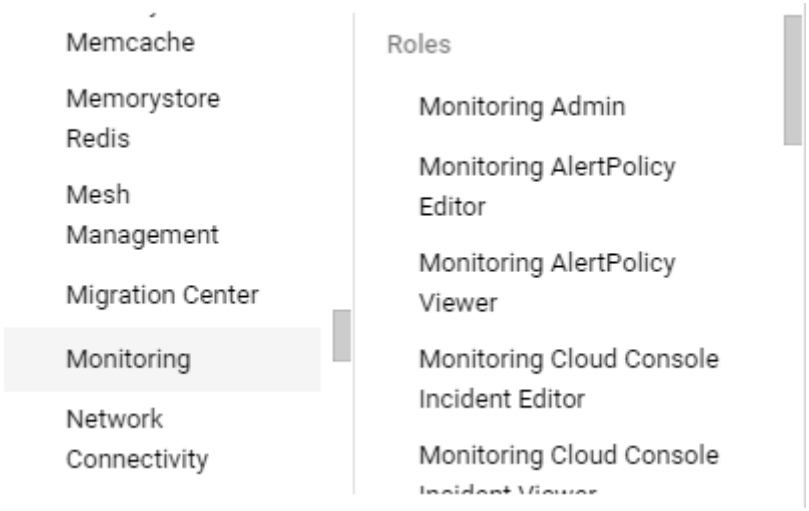
Hierarchie se vztahuje i na politiky, tedy je možné nastavit stejné politiky na celou organizaci nebo jen na projekt a podobně.

GCP obsahuje několik různých produktů. Ty, které budou stěžejní pro tuto práci, budou v rychlosti představeny. Konkrétně se jedná o **Správu identit a přístupů (IAM)**, **Cloud Storage** a **Compute Engine**.

Správa identit a přístupů – IAM

Primární úlohou IAMu je definovat a regulovat, kdo může přistupovat ke zdrojům a co s těmito zdroji může dělat. Rozšiřuje však svou roli do reakce na incidenty a hraje důležitou

roli při zajišťování bezpečnosti a integrity cloudových prostředí. Jakmile je totiž incident detekován, IAM hraje ústřední roli při analýze a zmírňování incidentů. Pomocí konfigurace IAM lze posoudit, jak mohl útočník získat neoprávněný přístup – je možné identifikovat mezery v řízení přístupu nebo kompromitované přihlašovací údaje, které vedly k incidentu. Příklad rolí, které lze nabýt pomocí IAM lze vidět na obrázku 3.5.



Obrázek 3.5: Možné příklady rolí, které lze přidělit v IAM.

IAM se v Google Cloudu skládá z několika základních komponent, které spolupracují na řízení přístupu a oprávnění v prostředí Google Cloud. Jsou jimi **Uživatelé** – to jsou jednotlivci nebo subjekty s účty Google nebo doménovými účty, **Skupiny**, anebo kolekce uživatelů, **Servisní účty**, to jsou účty používané aplikacemi nebo službami k interakci se zdroji, **Role**, to jsou předdefinované sady oprávnění a **Oprávnění**, podrobné akce, které lze provádět se zdroji.

Google Cloud Storage

Cloud Storage je služba pro ukládání objektů v Google Cloudu. Objekt je neměnný kus dat sestávající ze souboru libovolného formátu. Předměty se ukládají do kontejnerů zvaných „kbelíky“ (`buckets`). Segmenty mohou také obsahovat spravované složky, které lze použít k poskytnutí rozšířeného přístupu ke skupinám objektů se sdílenou předponou názvu.

Po nahrání objektů do cloudového úložiště, přichází kontrola nad tím, jak jsou data zabezpečená a sdílená. Otevírá se tu prostor pro zlepšení zabezpečení dat.

Správa identity a přístupu – Pomocí IAM lze určit, kdo má přístup ke zdrojům v projektu. Je možné udělit určité typy přístupu, jako je aktualizace, vytváření nebo odstraňování objektů.

Šifrování dat – Cloud Storage používá k šifrování dat ve výchozím nastavení šifrování na straně serveru.

Autentizace – Každý, kdo přistupuje k datům, musí mít správné přihlašovací údaje.

„Soft Delete“ – Trvalé ztrátě dat (např. náhodným nebo úmyslným smazáním) se dá zabránit tak, že se budou uchovávat nedávno odstraněné objekty.

Verzování – Když je živá verze objektu nahrazena nebo odstraněna, může být zachována jako neaktuální verze, pokud je to povoleno přes správu verzí objektů.

Compute Engine

Jelikož bude během této práce využit i tento modul Google Cloudu, v rychlosti a skromnosti bude též popsán. Compute Engine je IaaS produkt, který nabízí flexibilní, samoobslužné virtuální stroje (`VM`) hostované v infrastruktuře Google. Zahrnuje virtuální počítače se systémem Linux a Windows běžící na KVM (`Kernel-based VM`), možnosti místního a odolného úložiště a jednoduché rozhraní API pro konfiguraci a ovládání. Každý virtuální CPU (`vCPU`) je zde implementován jako jediné hardwarové hypervlákno na jedné z dostupných CPU platforem.

I Google Compute Engine může být zneužit útočníkem, a to když si hostují škodlivý obsah na App Engine a využívají službu jako distribuční platformu pro phishing, malware nebo jiné škodlivé aktivity. Hostováním škodlivých dat v Google infrastruktuře mohou obejít bezpečnostní řešení, která důvěřuje Google doméně. Engine zároveň umožňuje šifrovat provoz pomocí TLS (`Transport Layer Security`), je ve většině případů výhodou, v případě využití útočníky nikoli – ztěžuje to kontrolu obsahu komunikace. Stejně tak i poskytování široké škály IP adres v tomto případě výhodou není, jelikož útočníkům umožňuje se schovat v tomto IP prostoru, a je pak náročné efektivně identifikovat a blokovat škodlivé aktivity.

3.1.3 Kombinace Nextcloud a Google Cloudu

Kombinace těchto dvou platforem přináší veškeré výhody hybridní cloudů, které již byly popsány v části 2.4.3. Pro toto konkrétní řešení lze brát jako dvě hlavní výhody následující;

Úložiště – Pro ukládání dat může být využito jak lokální úložiště virtuálního stroje, tak cloudové úložiště GCP, v tomto případě `Google Cloud Storage`. Nextcloud již přímo nepodporuje externí úložiště (od verze 16), ale je možné to vyřešit manuálně viz 3.1.4.

Bezpečnost – GCP nabízí silné bezpečnostní funkce včetně šifrování dat ve stavu klidu i při přenosu, správy identit a přístupu, síťové bezpečnosti a další. Tyto funkce doplňují bezpečnostní opatření Nextcloud, jako je šifrování na straně serveru, dvoufaktorová autentizace a firewally aplikací.

Krom nevýhod hybridních cloudů popsaných v části 2.4.3 může být konkrétně v této kombinaci problémem například závislost na síti, aby mohly cloudy komunikovat. Navíc je potřeba zajistit bezpečný přenos mezi úložišti. Taktéž celková správa cloudu se ztíží, jelikož jde o dvě odlišné platformy.

3.1.4 Propojení cloudů

Nejsložitějším krokem při vytváření hybridního cloudu je zajistit jejich bezpečné propojení. Jejich propojení se stalo jednou z nejtěžších částí práce. Proces propojení cloudů se skládá ze dvou hlavních kroků – Síťování a Propojení služeb.

Síťování

Přenos dat mezi soukromým a veřejným cloudem by měl být zabezpečený a spolehlivý. Z toho důvodu je nejčastějším řešením propojení pomocí zabezpečených VPN sítí. Při těchto

připojeních se řeší i takzvané SLA[3]. V Google Cloud Platform je možné vytvořit dva druhy VPN, jedna je `High Availibility VPN (HA VPN)`, neboli VPN s vysokou dostupností, zde se zavazují až k 99.99% dostupnosti, a pak klasickou, kde se jde o 99.9%.

V této jsem zkusila tři cesty, kde až poslední z nich byla úspěšná.

1. **HA VPN** – Při mém prvním pokusu pro propojení cloudů jsem se mezi nimi snažila vytvořit HA VPN tunel. Zde jsem prošla od nastavování tunelů, šifrování (vpn) až k nastavování směrování. Směrování je v Googlu Cloudu řešeno pomocí BGP (`Border Gateway Protocol`). Pro manuální nasazení konfigurace VPN se používá externí aplikace Terraform[4]. VPN a tunel se pomocí něj dá nakonfigurovat, ale BGP pomocí něj nastavit nemůžu, jelikož konfiguraci BGP nejde upravovat v Compute Engine – na to je potřeba automatické nasazení od Googlu. K tomu je ale zapotřebí navýšit účtování, což dělá Google na žádost a trvá dlouho, než to schválí. Proto jsem se po několika dnech čekání na schválení posunula k jinému řešení.

Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status	BGP session status
nextcloud-vpn-tun0	nextcloud-vpn 34.124.52.203	nextcloud-vpn 34.118.37.254	169.254.17.117	169.254.17.118	No incoming packets	Waiting for peer
nextcloud-vpn-tun2	nextcloud-vpn 34.104.118.81	nextcloud-vpn 34.118.37.254	169.254.143.5	169.254.143.6	No incoming packets	Waiting for peer

Obrázek 3.6: Takto vypadá nefunkční nastavení VPN tunelů v GCP.

2. **Klasická VPN** – Tato možnost oproti předcházející zaručovala stále skoro stoprocentní SLA (`Service Level Agreement`), a nebylo potřebné konfigurovat BGP. Nepodařilo se mi nastavit ani tuto variantu. Při konfiguraci jsem pravděpodobně někde udělala chybu, kterou jsem však nemohla objevit, a tak propojení nebylo funkční.

3. **TLS přes internet** – Potom, co jsem strávila několik desítek hodin neúspěšným nastavováním VPN spojení mezi cloudy jsem se rozhodla z velké části změnit mojí ideu o finálním řešení. Jako finální možnost jsem zvolila komunikaci přes otevřený internet s pomocí requestů na API Google služeb s použitím TLS zabezpečení.

Propojení služeb

Pro propojení služeb jsem zvolila `rclone`[5], který implementuje rozhraní pro komunikaci s Google Cloud Storage. Postup propojení služeb byl následují:

1. Instalace `rclone` na virtuální stroj, na které se nachází i Nextcloud.

2. Vytvoření servisního účtu v GCP – Kromě samotného vytvoření účtu tu bylo potřebné upravit politiky pro vytvoření klíče, konkrétně `constraints/iam.disableServiceAccountKeyCreation` nastavit na `Not enforced` (česky „nevynucováno“) a vygenerovat klíč pro servisní účet.

3. Konfigurace `rclone` pomocí interaktivního průvodce příkazem `rclone config`.

[3] SLA, z anglického Service Level Agreement, je označení pro vzájemně vyjednané smluvní podmínky mezi poskytovatelem a firmou. Obsahem je ujasnění o stupni, rozsahu a kvalitě poskytované služby [24].

[4] https://cloud.google.com/docs/terraform

[5] https://rclone.org/googlecloudstorage/

4. Vytvoření `bucketu`[6] – při jeho vytváření je třeba mu dát globálně jedinečný název a geografickou polohu, kde bude jeho obsah uložen. V tomto případě je název `krcalova-bucket` a lokace je ve střední Evropě viz 3.7.

	Name ↑	Created	Location type	Location	Default storage class
☐	krcalova-bucket	May 7, 2024, 5:00:14 PM	Region	europe-central2	Standard

Obrázek 3.7: Vytvořený bucket pro uchování dat.

5. Nastavení synchronizace dat – Pro synchronizaci jsem vytvořila naplánovanou úlohu pomocí `cron` úlohy, která spouští příkaz `rclone sync`. Ten zálohuje všechna data z „Public“ složek každého uživatele z Nextcloudu do Google Cloud Storage, a to každou pátou minutu.

```
*/5 * * * * rclone sync /var/snap/nextcloud/common/nextcloud/data --include "**files/Public/**"
gcp:krcalova-bucket
```

Obrázek 3.8: Nastavení synchronizace Public složky z Nextcloudu na Cloud Storage.

Hybridní cloud tedy vypadá tak, že se každých pět minut synchronizují data z „veřejné složky“ `Public` na Google Cloud Storage a data z jiných složek zůstávají výhradně na Nextcloudu. Hybridní cloud je takto připraven na další akce a možné pokračovat dál v nastavení logování událostí.

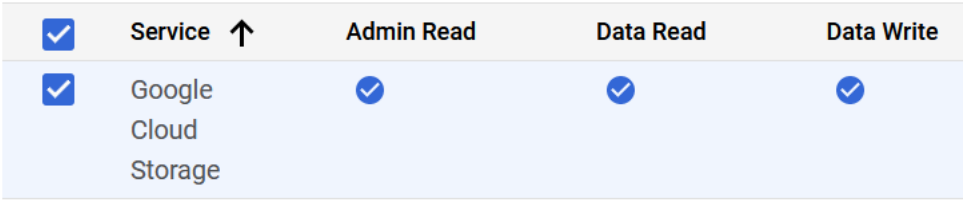
3.2 Nastavení logování událostí

Správné nastavení logování událostí bylo pro tuto práci klíčové, a to jak pro Google Cloud, tak i pro Nextcloud. Je potřeba spoustu věcí nastavit, přenastavit, zapnout, a informace o tom, jak na to, nejsou snad nikde jednotně zapsané. Tato část slouží čistě jenom pro **nastavení** logování událostí, jak tyto logy exportovat bude představeno až později, v kapitole 5, před samotným auditem.

Google Cloud

V samotném GCP jsou dvě hlavní možnosti, jak generovat logy – pomocí vestavěné platformy `Audit Logs` a pomocí aplikací nebo služeb, které v cloudu běží, to zahrnuje logy z webových služeb spuštěných na virtuálním počítači nebo to mohou být síťové logy, jako je Flow nebo PCAP, a to z provozu generovaného virtuálním počítačem a službami, které jsou na nich spuštěné. Spustit logování v Audit Logs je poměrně jednoduché, stačí k tomu administrátorská práva. V IAM je sekce `Audit logs` a zde je potřeba nastavit logování pro užívané aplikace, v tomto případě pro Google Cloud Storage, což jde vidět v obrázku 3.9.

[6] Buckety jsou v podstatě kontejnery, které uchovávají data. Vše, co se uloží do cloudového úložiště musí být obsaženo v bucketu [10].



Obrázek 3.9: Nastavení logování událostí Google Cloud Storage v IAM.

V Google Cloud Storage je možné monitorovat jak jednotlivé „buckety“, tak i celé projekty. Záleží, co je pro mě, jako analytika důležitější – logy jednotlivých bucketů nebudou tak objemné a bude jednodušší v nich hledat zlo, každopádně tyto logy mnohdy nemusí stačit.

Ukázka struktury logu události z GCP jde vidět v příloze A.

Nextcloud

Pro nastavení logování v Nextcloudu bylo potřeba zjistit, kde se nachází konfigurační soubor `config.php`, k tomu stačil příkaz `find` s admin právy. Soubor se v tomto případě nachází na cestě `/var/snap/nextcloud/41512/nextcloud/config/config.php`. Nastavení lze vidět na obrázku 3.10.

log_type – Určuje, kam se budou zapisovat logy. V tomto případě se logy budou zapisovat do souboru. Jinou možností je například `Syslog`, kde by se logy zapisovaly do systémových logů.

logfile – Určuje umístění souboru obsahujícího logy, pro potřeby této práce nebylo potřeba měnit.

loglevel – Určuje, od jaké úrovně se bude logovat. Zde jsem nastavila logování od `Info` úrovně, tedy se nebudou logovat věci z `Debug` úrovně.

logdateformat – Podle tohoto se určí formát data a času zapsaných v lozích. Formát je nastaven tak, aby byl stejný jako logy z GCP.

```
'log_type' => 'file',
'logfile' => '/var/snap/nextcloud/current/logs/nextcloud.log',
'loglevel' => 1,
'logdateformat' => 'Y-m-d H:i:s',
```

Obrázek 3.10: Logy se budou zapisovat do souboru nextcloud.log, a to od Info úrovně.

Dále bylo potřeba zapnout aplikaci pro logování aktivit uživatelů. Po přihlášení do administrátorského účtu je nutné přejít do nastavení aplikací a zde zapnout aplikaci „Auditing/Logging“. Následně se logy o aktivitách uživatelů začnou zapisovat do složky `audit.log`, kterou lze najít na cestě `/var/snap/nextcloud/common/nextcloud/data/audit.log`. Na obrázku 3.11 lze vidět, že se uživatel „Ignác Kuřátko“ přihlásil do Nextcloudu v 19:15:44 UTC z IP 62.44.6.147 z prohlížeče od Mozilly.

```
{
    "reqId":"P9Vj8gNNokz8CphcN2rz",
    "level":1,
    "time":"2024-05-10 19:15:44",
    "remoteAddr":"62.44.6.147",
    "user":"Ignac Kuratko",
    "app":"admin_audit",
    "method":"GET",
    "url":"/",
    "message":"Login successful: \"Ignac Kuratko\"",
    "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0",
    "version":"27.1.8.1",
    "data":{"app":"admin_audit"}
}
```


Obrázek 3.11: Ukázka struktury logu z Nextcloudu.

Nextcloud loguje samozřejmě mnohem více věcí sám o sobě, ale tyto dva soubory s logy budou stěžejní pro další řešení práce.

- `/var/snap/nextcloud/common/nextcloud/data/audit.log`
- `/var/snap/nextcloud/nextcloud/current/logs/nextcloud.log`

Kapitola 4

Návrh zneužití hybridního cloudu a jeho realizace

V této kapitole budou navrženy a realizovány možné způsoby, jak lze zneužít hybridní cloud. Případy mají různou variabilitu obtížnosti. Ta bude ohodnocena na škále od 1 po 10 sestupně od nejsložitějšího útoku podle **realizace**. Bude se zde čerpat poznatků z kapitoly 2. Cílem je vytvoření vhodných příkladů, které budou následně zanalyzovány, podrobně popsány a vyhodnoceny v závěru této práce a zároveň i v metodologické příručce, která tuto práci doplňuje, a postup znázorňuje více graficky. Příručka je elektronicky přiložena k práci, a byla distribuovaná mezi respondenty, kterých zpětná vazba bude shrnuta ve vyhodnocení.

Nyní budou představeny jednotlivé příklady, vždy bude na začátku smyšlený úvod o tom, co se stalo, následovat bude popis útoku a jak proběhla jeho realizace.

4.1 Příklad 1 – Insider

Insider, česky nejlepší překlad „Vnitřní pracovník“, označuje jedince s legitimním přístupem do systému, který tento přístup zneužívá k provádění škodlivých akcí.

Úvod: V naší firmě bylo zjištěno, že naši největší konkurenti dávají do základních desek, které prodávají, úmyslně vadné konektory. Chtěli jste s touto informací jít do médií, ale den předtím tato firma na tiskové konferenci „objevila“ tento problém a zavázala se k lepší kontrole. Nyní se domníváme, že došlo k exfiltraci TLP:RED[1] dokumentu z Vaší firmy. K dokumentu měli mít přístup dohromady tři zaměstnanci – Alfréd Znamenitý, Jana Zelenkatá a Jonáš Nebožácký.

Popis útoku: Jeden z legitimních uživatelů chybou nastavení soukromí nabyl práv pro zobrazení tajného dokumentu v soukromé části cloudu. Přečetl si obsah tohoto dokumentu a i přes označení `TLP:RED` si jej nahrál do své složky ve veřejném cloudu. Následně ho nasdílel i svému kolegovi. Ten si však ale dokument nenechal pro sebe a přeposlal jej subjektu, o kterém se ve zmiňovaném dokumentu psalo. Jedinec, který se dopustil původní exfiltrace dokumentu, tento incident zamlčel, jelikož se bál ztráty své pozice.

[1] Informace označené jako TLP:RED jsou určeny pouze pro určené uživatele. Ti tyto informace nesmí sdílet s nikým jiným. Toto označení se používá pro velmi citlivé informace, kde by neoprávněné šíření mohlo mít vážné důsledky.

Realizace: K realizaci tohoto scénáře je potřeba vytvořit několik různých účtů. Je potřeba povolit přístup k danému dokumentu minimálně jednomu z vybraných účtů, následně tímto účtem stáhnout konkrétní dokument a nahrát ho na veřejnou část cloudu. Poté je potřeba vytvořit emailovou komunikaci mezi jedinci. V neposlední řadě je potřeba odstranit soubor z cloudu od pachatele.

Předpokládaná obtížnost realizace: 4

4.2 Příklad 2 – Smazání nezálohovaného dokumentu

Úvod: Teta Marta se rozhodla psát vlastní kuchařku, a protože neměla vlastní počítač, poprosila vnuka, aby problém vyřešil. Ten jí vytvořil hybridní cloud, se synchronizací na externí úložiště, na který mohla přistoupit i z knihovny. Teta tak pracovala na kuchařce na počítači v knihovně, a to tak, že se přihlásila na Nextcloud, kam si nahrála novou verzi, a při odchodu z knihovny roztrhala svoje poznámky, co měla na papíru, a vyhodila je do tříděného odpadu před knihovnou. Mohla ji tak bez problému ukázat všem kamarádům z telefonu a nemusela kvůli tomu kupovat nový počítač. Když ale teta ukazovala poslední verzi před tiskem své sestře, omylem klikla na tlačítko pro smazání a soubor se odstranil. Smutná teta teď žádá o pomoc s obnovením dokumentu.

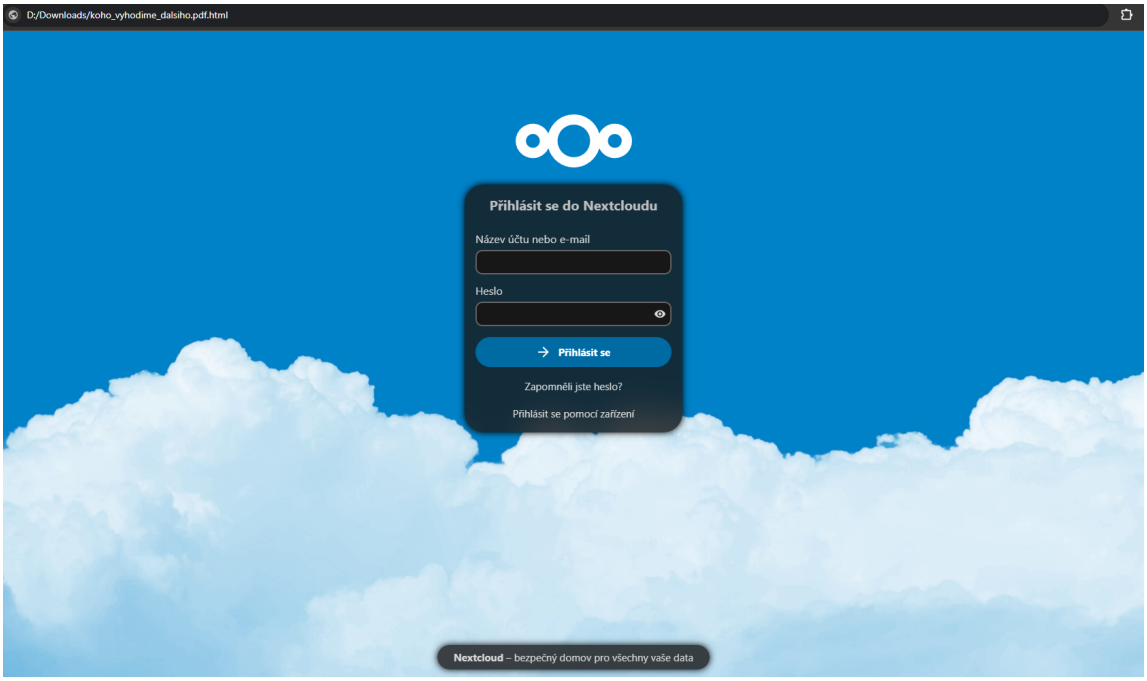
Popis útoku: Útočníkem zde je samotná teta Marta, která omylem smazala soubor. Je potřeba zjistit, zda je soubor někde na cloudu zálohovaný a případně jej obnovit.

Předpokládaná obtížnost realizace: 1

Realizace: Realizace tohoto „útoku“ je velice snadná, jelikož útočníkem je jediný účet, který má přístup do cloudu. Je potřeba opakovaně nahrát soubor a poté ho smazat.

4.3 Příklad 3 – Škodlivý soubor

Úvod: Jeden ze zaměstnanců nahlásil, že na cloudu měl uložené soubory a nyní je nemůže nikde najít. Přiznal, že během posledních uplynulých dní otevřel jeden ze souborů s pochybným názvem, co mu nasdílela kolegyně. Po jeho stažení jej otevřel a dostal se na přihlašovací obrazovku Nextcloudu, kam zadal svoje přihlašovací údaje, každopádně k souboru se již nedostal. Domněnkou je, že šlo o škodlivý soubor, který obsahoval odkaz na phishingovou stránku. Po analýze tohoto souboru byly domněnky potvrzeny, po rozkliknutí souboru vyskočila phishingová stránka tvářící se jako přihlašování do Nextcloudu.



Obrázek 4.1: Zobrazení phishingové stránky po otevření škodlivého souboru.

Popis útoku: Do Nextcloudu byl nahrán škodlivý soubor s úmyslně lákavým názvem `koho_vyhodime_dalsiho.pdf.html`, po jehož stáhnutí a otevření došlo k přesměrování na phishingovou stránku, která vypadala jako přihlašování na Nextcloud. Tento soubor byl zpřístupněn všem uživatelům. Minimálně jeden z uživatelů se nechal oklamat a údaje vyplnil, na čež přišel o data, co měl uložená v cloudu. Otázkou pro analýzu cloudu je zjistit rozsah kompromitace, zjistit, zda byl tento uživatel jediný, co si soubor stáhnul, a zda nebyly napáchány další škody.

Zápletka: Uživatelka, která soubor nahrála a následně nasdílela všem svým kolegům byla v době kompromitace na dovolené. Po jejím návratu nahlásila, že se nemůže přihlásit ke svému účtu.

Předpokládaná obtížnost realizace: 7

Realizace: K realizaci tohoto příkladu bylo zapotřebí vytvořit několik různých účtů, vytvořit a nahrát na ně obsah, který se byl částečně nasdílen mezi uživatele. Ke kompromitaci byl vybrán účet uživatelky `Amálie Široké`. Byl proveden jednoduchý `slovníkový útok`[2], kde byla použita hesla jako „AmaliePatalie, Amalka1234, vilaamalka“ a další (reálné heslo k účtu je „VilaAmalka“). Pod tímto účtem pak byl vytvořen soubor s názvem `koho_vyhodime_dalsiho.pdf.html`, aby upoutal pozornost uživatelů a následně byl všem jednotlivě nasdílen. Kód tohoto .html souboru byl extrahován z oficiální přihlašovací obrazovky Nextcloudu a byl upraven. Formulář neukládá/neposílá nikam zadané údaje, slouží čistě pro demonstraci. Pro akci je zde byla naznačena exfiltrace do Telegram skupiny viz 4.2.

[2]Při slovníkovém útoku si útočník předem připraví vlastní databázi slov, z které následně zkouší použít různé varianty pro prolomení ochrany uživatelského systému či účtu [7].

```
<form data-v-57e9d1c0="" method="post" name="login" action="telegram.app/sxs2432DAC/" class="login-form">
```

Obrázek 4.2: Naznačení posílání dat z formuláře do Telegram skupiny.

Poté bylo potřeba přistoupit jednotlivými účty, tři byly vyčleněné pro stažení souboru, jeden z nich byl administrátorský účet.

Nakonec bylo potřeba znovu přistoupit nyní již kompromitovanými účty, postahovat k sobě dokumenty a některé z nich odstranit.

4.4 Příklad 4 – Ilegální obsah v cloudu

Úvod: Policie zadržela notebook jednoho ze státních zaměstnanců. Ten byl zadržen poté, co jim anonymní zdroj nahlásil, že by se mohl podílet na nelegální aktivitě, konkrétně na distribuci dětské pornografie na internetu. Pro zatím nebylo dodáno dostatek důkazů.

Při domovní prohlídce policie zajistila nejenom dvě nelegálně držené fotky, ale i laptop potenciálního pachatele. Pod samotným laptopem se nacházel sešit se zapsaným heslem. Na počítači jako takovém inkriminovaná data nebyla, ale v historii prohlížení byly záznamy o užívání cloudu. Při forenzní analýze disku byla zajištěna hesla ke cloudu. Analýza cloudu je zde poslední možností k usvědčení možného kriminálníka.

Popis útoku: Jde zde o ukázku případu, kdy je cloud zneužit přímo útočníkem. Pravděpodobně jej využil pro uchování nelegálně držených souborů. Otázkou zůstává, zda bude nalezeno dostatek důkazů, aby bylo prokazatelně jasné, že se tato aktivita děla a že ji prováděl přímo zadržený.

Realizace: Pro realizaci je potřeba nahrát několik fotek a videí ideálně na soukromou část cloudu. Soubory, které by měly znázorňovat nelegální činnost z pochopitelných důvodů nejsou explicitní, jsou ale nahrazeny fotkami koťátek.

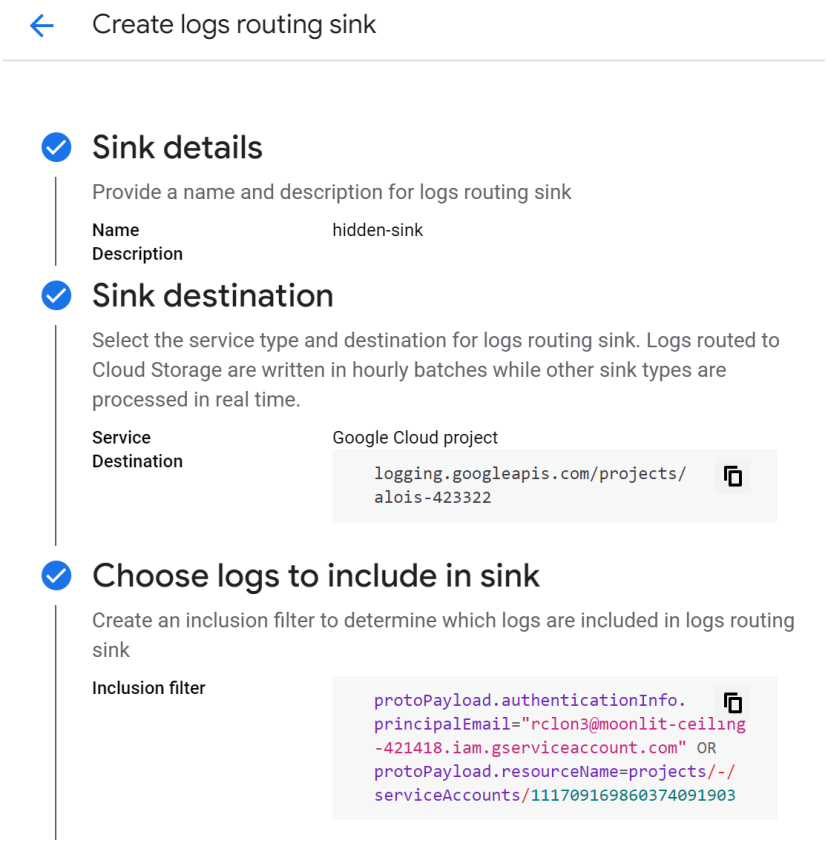
Předpokládaná obtížnost realizace: 4

4.5 Příklad 5 – APT

Úvod: Po kompromitaci přihlašovacích údajů administrátora v příkladu 4.3 bylo potřebné zkontrolovat, zda se útočník nepřistoupil k účtu, případně zda zde neprovedl nějakou škodlivou aktivitu.

Popis útoku: Po odcizení hesel k administrátorskému účtu mohlo dojít ke kompromitaci systému.

Realizace: K realizaci tohoto příkladu bylo zapotřebí přihlásit se k účtu kompromitovaného uživatele pomocí hesla ze souboru `hesla.txt`. Po přihlášení byl vytvořen nový servisní účet s názvem `rclon3`, kterému byla nastavena nejvyšší možná práva. Poté byl vytvořen privátní klíč pro tento servisní účet, který slouží na přihlášení se z `rclone`. Následně byl vytvořen nový projekt s názvem `alois` a také „sink“ s názvem `hidden-sink`, který bude všechny logy z nově vytvořeného servisního účtu přesouvat do úložiště logů nově vytvořeného projektu.



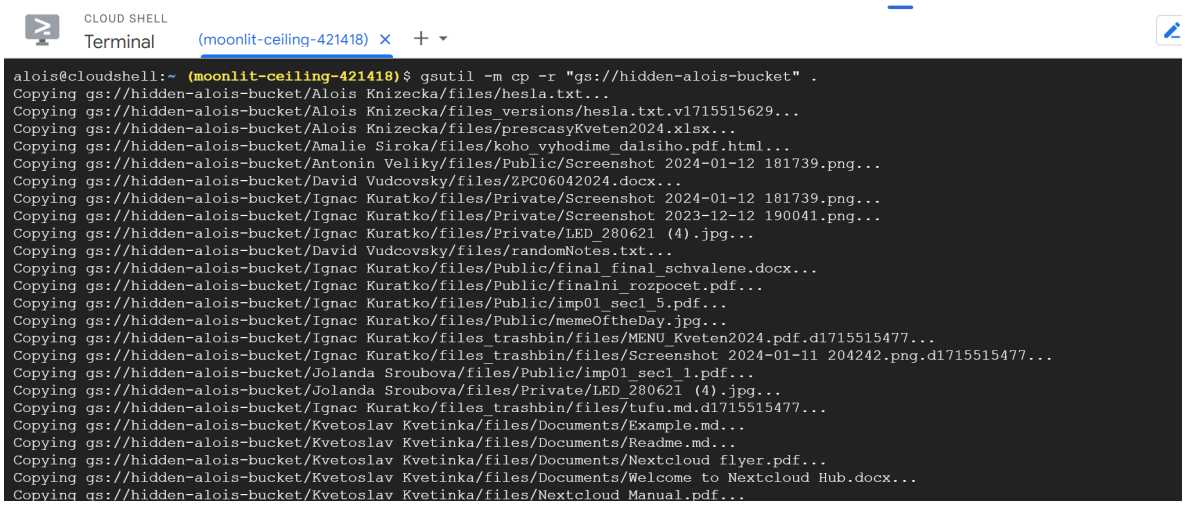
Obrázek 4.3: Nastavení směrovacího „sinku“ a jeho filtrování na aktivity servisního účtu.

Dále došlo na napojení se do virtuálního stroje, kde běží Nextcloud, a nastavení nové synchronizace dat pomocí `rclone`. Dále došlo k vytvoření bucketu `hidden-alois-bucket`, kam si následně pomocí příkazu 4.4 zazálohoval data z Nextcloudu, tentokrát však ne jenom veřejnou složku, ale všechna data.

```
rclone sync /var/snap/nextcloud/common/nextcloud/data --include "**files**" gcs:hidden-alois-bucket
```

Obrázek 4.4: Příkaz, pomocí kterého byly zazálohované všechny data z Nextcloudu.

Pomocí příkazu `gsutil -m cp -r "gs://hidden-alois-bucket"` byly tato data na závěr staženy do Cloud Shellu , odkud byly dále exfiltrovány 4.5.



Obrázek 4.5: Exfiltrace dat z Nextcloudu do Cloud Shellu.

Předpokládaná obtížnost realizace: 9

4.6 Virtualizace

Veškeré podklady pro forenzní analýzu cloudu jsou v této chvíli připraveny. Je vytvořen virtuální stroj pro zkoušení analýzy jednotlivých příkladů, ten je možné najít na SD kartě přiložené k této práci spolu s metodologickou příručkou. Ve virtuální stroji se nachází složku obsahující důkazní materiály (logy, emaily), VsCode, který je jediný potřebný k analýze logů, a v neposlední řadě předpřipravená šablona pro zprávu z analýzy, kterou lze vidět v příloze B.

Konkrétně jsou příklady k analýze vloženy do jednoho virtuálního stroje, kde je pro každý příklad vytvořena vlastní složka a ta obsahuje:

Insider – ve složce `insider` je podsložka `logy`, kde se nachází soubory:

- audit.log
- nextcloud.log
- krcalova_bucket.json
- jonas_nebojacny.json

Dále složka s emailovou komunikací, kde se nachází emaily k analýze s názvem `emaily`:

- email1.eml
- email2.eml
- email3.eml

Škodlivý soubor – ve složce `malware` je podsložka `logy`, kde se nachází soubory:

- audit.log
- nextcloud.log
- gcp-logs.json

Dále v podsložce `malware` se nachází škodlivý soubor:

- koho_vyhodime_dalsiho.pdf.html

APT – ve složce `apt` se nachází podsložka `logy`, kde se nachází soubory:

- gcp-all.json
- alois-knizecka.json
- krcalova_bucket.json
- vpc-flows.json

SHA1 hashe jednotlivých souborů jsou uvedeny vždy u konkrétní analýzy.

Analýza těchto dat rozdělena podle jednotlivých příkladů je znázorněna v následující kapitole. Analýza příkladů 2 a 4 je založena na práci s živým cloudem, tyto analýzy tedy budou pouze názorně předvedeny, nebude možnost si je vyzkoušet.

4.6.1 Přihlašovací údaje do virtuálního stroje

Přihlašovací údaje do virtuálního stroje jsou následující:

Uživatel: forensics

Heslo: dummypassword

Kapitola 5

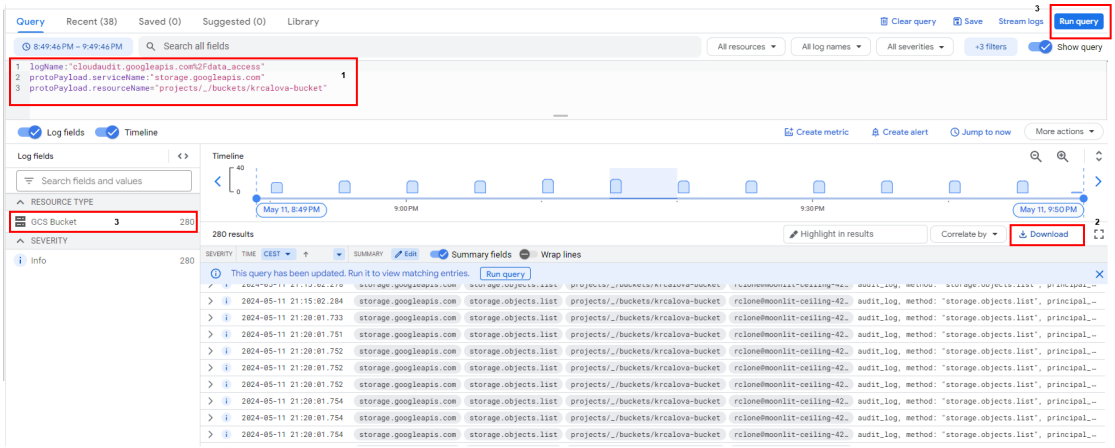
Audit aktivit

V této kapitole bude názorně ukázán podrobný postup, jakým lze provést audit jednotlivých příkladů z kapitoly 4. Případy mají různou variabilitu obtížnosti. Ta bude ohodnocena na škále od 1 po 10 sestupně od nejsložitějšího útoku pro **audit**. Ke každému příkladu bude připraven i smyšlený scénář pro snadnější vcítění se do příkladu. Úvod je zvolen tak, že by teoreticky mohl vést k analýze, která zde bude prováděna.

Export logů pro analýzu

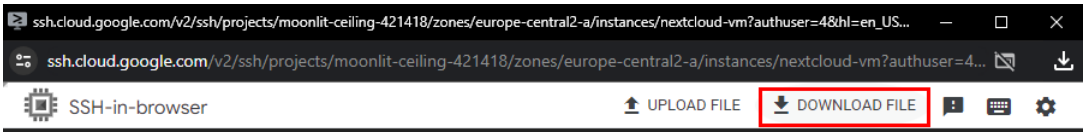
Jelikož se v příkladech nebude pracovat s živým systémem, je zapotřebí vyexportovat všechny podstatné logy. Tento krok se bude opakovat pro všechny příklady, proto je ideální vědět jak na to dříve, než začnou samotné audity.

Export logů z GCP Exportovat logy událostí je možné pomocí Log Exploreru. Pro filtrování logů zde slouží `query`. Na obrázku 5.1 je možné vidět vyfiltrované logy z konkrétního „bucketu“ `krcalova-bucket`. Pomocí query (1) se vyfiltrují události pouze pro `krcalova-bucket`. Tuto query je možné spustit tlačítkem napravo, `Run Query` (4). Tím se vyfiltruje 280 událostí (3) a ty je možná stáhnout pomocí tlačítka `Download` (2).



Obrázek 5.1: Filtrování a stahování logů z Log Exploreru.

Export logů z Nextcloudu Soubory obsahující logy je potřeba extrahovat z virtuálního stroje. Konkrétně je potřeba vytáhnout auditní logy, ty se zaznamenávají do `/var/snap/nextcloud/common/nextcloud/data/audit.log`. Systémové logy se zaznamenávají do `/var/snap/nextcloud/nextcloud/current/logs/nextcloud.log`. Pro extrahování těchto souborů bylo zapotřebí se připojit na virtuální stroj přes SSH. Dále bylo potřeba zkopírovat soubory do domovského adresáře uživatele a následně je možné je pomocí tlačítka 5.2 stáhnout k sobě do počítače.



Obrázek 5.2: Tlačítko pro stahování souborů z virtuálního stroje do lokálního počítače.

Logy událostí z Nextcloudu jsou uchovávány v .log souboru, logy událostí z GCP jsou uchovány v `.json` formátu. Oboje logy jsou v UTC čase.

Jelikož se zde kromě posledního příkladu neobjevuje velký počet zalogovaných událostí, beru pro tuto práci využití SIEM nástrojů, jako je Splunk [1] za zbytečné. V případě však, že bych měla stovky záznamů, tak bych určitě šla touto cestou. Takto stačí analyzovat logy „ručně“.

5.1 Audit příkladu 1 – Insider (4.1)

Shrnutí: Dne 11. 05. 2024 mělo dojít k exfiltraci interního TLP:RED dokumentu s názvem `TLPRED_finalni_verze_zpravy.pdf`. Pravděpodobně tak učinil jeden z legitimních uživatelů, jde tedy o případ vnitřního pracovníka.

Úkol: Cílem je potvrdit nebo vyvrátit, že došlo k exfiltraci souboru. Najít usvědčující materiály k poskytnutí souboru třetí straně.

Audit :

Identifikace: Pro audit budou podstatné auditní logy z Nextcloudu, dále budou potřeba i obecné Nextcloud logy. Logy z Google Cloud Storage budou taktéž potřeba, protože mohlo dojít k exfiltraci na veřejný cloud. V neposlední řadě bude potřeba zajistit emailové schránky uživatelů, co měli přístup k dokumentu.

Uchování a shromažďování: Byly zajištěny soubory `audit.log` a `nextcloud.log` z Nextcloudu a logy z „bucketu“ `krcalova-bucket`. Později byly zajištěny konkrétní emailové schránky. Kopie těchto souborů byly nahrané do složky **Case1**.

[1] Splunk je platforma pro „velká data“, která zjednodušuje shromažďování a spravování velkého objemu strojově generovaných dat a vyhledávání v nich [35].

Názvy souborů s důkaznými materiály	SHA1
audit.log	D7741518E8F4623CFD2008B213469B40E906216E
nextcloud.log	56F82573F7D272D115C1952324AAB2FC0E27608B
krcalova_bucket.json	54F2899D28204B2F662216AD084CBD4DDC4F6A10
jonas_nebojacny.json	F7D5892A7443716B594957EAA9F93DE3F60CA572
email1.eml	70F6101AA9236139496E218A3D8CEC95489E1A13
email2.eml	7E8C3AC8841B49F991C65571BEBDBF5DD8A49378
email3.eml	069996C46D85B5F9BBECEE3827F6D44C8AC6DAAD

Tabulka 5.1: Tabulka obsahující hashe SHA1 souborů obsahujících důkazní materiály k příkladu 1.

Analýza: Již úvod této analýzy měl dobrý začátek, jelikož bylo známo jak datum, kdy se incident stal, tak i název souboru, který je nutné sledovat. Jako jsem začala s analýzou souboru `audit.log`, protože jsem zde předpokládala největší úspěšnost najití potřebných artefaktů. Hned jako první záznam bylo nahrání souboru uživatelem Alfrédem Znamenitým na Nextcloud. Ten následně tento soubor nasdílel dvěma zaměstnancům: Janě Zelenkaté a Jonáši Nebojácnému. Již toto nesedělo s původními informacemi, podle nich neměl mít přístup Jonáš Nebojácný, ale Jonáš Nebožácký. K souboru tedy měli přístup tito tři uživatelé, bylo tedy potřeba sledovat jejich aktivitu.

Dle logů se jako první přihlásila právě paní Jana, která si soubor otevřela. Dále s ním však nic nedělala. V 19:00:51 UTC se přihlásil uživatel Jonáš Nebojácný. Ten si taktéž zobrazil tento soubor, pár minut na to vytvořil stejnojmenný soubor ve své `Public` složce. Lze se domnívat, že v tuto chvíli došlo k exfiltraci dokumentu do Google Cloud Storage. Následně se znovu přihlásil, tentokrát z jiné IP adresy, pravděpodobně tedy z jiného zařízení. Soubor ve své `Public` složce si opět zobrazil. Po pár minutách soubor smazal a odhlásil se.

Byl dožádán obsah jeho emailové schránky za den 11. 05. 2024. Zde byla mimo jiné nalezena zpráva, ve které byl poslán stejnojmenný soubor v příloze na emailovou adresu mimo doménu firmy, konkrétně na adresu `tondaMycka@email.cz`.

Exfiltrace souboru tedy byla jednoznačně potvrzena a byla provedena dne 11. 05. 2024 v 19:06:42 uživatelem Jonášem Nebojácným.

Časová osa :

Datum, čas (UTC)	Původ artefaktu	Artefakt
2024-05-11 17:12:24	Audit.log	Přihlášení uživatele Alfréd Znamenitý z IP 62.44.6.140.
2024-05-11 18:48:40	Audit.log	Uživatel Alfréd Znamenitý nahrál soubor do Nextcloudu.
2024-05-11 18:58:23	Audit.log	Nasdílení dokumentu Janě Zelenkaté a Jonáši Nebojácnému.
2024-05-11 18:59:25	Nextcloud.log	Poslání notifikace mailem oběma uživatelům.
2024-05-11 19:00:51	Audit.log	Přihlášení uživatele Jonáš Nebojácný.
2024-05-11 19:01:31	Audit.log	Vytvoření složky Public.
2024-05-11 19:03:03	Audit.log	Zobrazení obsahu TLP:RED dokumentu.
2024-05-11 19:04:46	Audit.log	Vytvoření stejnojmeného souboru v složce Public.
2024-05-11 19:05:02	GCP logy	Nahrání souboru na Google Cloud Storage.
2024-05-11 19:05:07	Audit.log	Odhlášení uživatele Jonáš Nebojácný.
2024-05-11 19:05:52	Audit.log	Přihlášení uživatele Jonáš Nebojácný z IP 66.44.6.148.
2024-05-11 19:06:16	Audit.log	Přístup k dokumentu TLPRED... ve složce Public.
2024-05-11 19:08:42	Email 1	Dokument zaslán v příloze emailu externímu uživateli.
2024-05-11 19:13:06	Audit.log	Smazání souboru z Public složky.
2024-05-11 19:14:24	Audit.log	Odhlášení uživatele Jonáš Nebojácný.
2024-05-11 19:15:02	GCP logy	Odstranění souboru z Google Cloud Storage.

Tabulka 5.2: Časová osa analýzy prvního příkladu.

Složitost: 5

Závěr: Zaměstnanec Jonáš Nebojácný porušil podmínky při práci s dokumenty, při čemž došlo k **exfiltraci** TLP:RED dokumentu. K exfiltraci interního dokumentu s názvem `TLPRED_finalni_verze_zpravy.pdf` došlo nejdříve na Google Cloud Storage uživatele Jonáše Nebojácného do složky Public a následně došlo i k exfiltraci dokumentu emailovou komunikací na adresu "tondaMycka@email.cz".

Zároveň se však dopustil chyby i uživatel Alfréd Znamenitý, který dokument nasdílel zaměstnanci, který k dokumentu dle jeho slov vůbec neměl mít přístup. Kdo je hlavním viníkem incidentu je tedy nejednoznačné a rozhodnutí zůstává na posouzení vedení.

Jde tedy jak o případ vnitřního pracovníka, tak i o případ pochybení lidských zdrojů, které mu dokument zpřístupnily.

Doporučení: Je důležité znovu proškolit své zaměstnance se zaměřením na TLP a PAP protokoly, poučit je o tom, co s dokumenty dělat můžou, co ne, a jaké budou následky v případě porušení těchto pravidel. Dále je potřeba zajistit, aby se již neopakovalo chybné zpřístupnění důvěrného dokumentu uživatelům, kteří by k němu přístup mít neměli a při jejich sdílení vypnout možnost stahování souboru k sobě. Bylo by také dobré zvážit, zda v Google Cloud Storage nezapnout kontrolu důvěrných dokumentů, která by v případě detekce takového souboru automaticky přesunula soubor do karantény.

5.2 Audit příkladu 2 – Smazání nezálohovaného dokumentu (4.2)

Shrnutí: Paní Marta omylem smazala pro ni důležitý dokument ze svého cloudu a potřebovala by pomoct s jeho obnovením.

Úkol: Úkolem je zjistit, zda dokument byl či nebyl zálohovaný, případně jej obnovit.

Místa k hledání důkazů: Cloudové úložiště jako takové – k dispozici jsou přihlašovací údaje.

Audit : Jelikož nejde o běžný audit, ale o obnovu dokumentu, bude využit živý cloud pro demonstraci. Tento příklad není možné prakticky zkoušet analyzovat na virtuálním stroji.

Identifikace: Veškeré potřebné informace se nachazí v živém cloudu. Byl však extrahován soubor `audit.log` pro potvrzení příčiny události.

Uchování a shromažďování: Byly zajištěny přihlašovací údaje k GCP a Nextcloud účtům. Byl však zajištěn i soubor `audit.log`.

Názvy souborů s důkazními materiály	**SHA1**
audit.log	FA32F4B0A34529CAD518EE412EF4E83523AE52DC
přihlašovací údaje	–

Tabulka 5.3: Tabulka obsahující hashe SHA1 souborů obsahujících důkazní materiály k příkladu 2.

Analýza a obnovení souboru: V tomto případě slouží logy pouze pro potvrzení toho, že info, které poškozený subjekt uvedl bylo správné. To se při analýze potvrdilo, došlo k přihlášení účtu, smazání již existujícího souboru s názvem `kucharka_tety_marty.docx` a odhlášení uživatelky.

Časová osa :

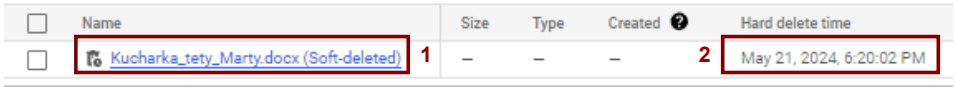
Datum, čas (UTC)	**Původ artefaktu**	**Artefakt**
2024-05-14 18:00:11	Audit.log	Přihlášení uživatelky Marty z IP 80.23.76.12
2024-05-14 18:30:19	Audit.log	Smazání souboru kucharka_tety_marty.docx
2024-05-14 18:50:28	Audit.log	Odhlášení uživatelky Marty z IP 80.23.76.12.

Tabulka 5.4: Časová osa analýzy druhého příkladu.

Pro obnovení souboru bylo důležité zjistit, zda je bucket, do kterého se synchronizují data, opatřen některou z zálohovacích schopností, jako je verzování nebo takzvaný „Soft Delete“. To bylo potvrzeno, bucket `krcalova-bucket` byl nastaven s možností „Soft Delete“ a smazané soubory tak byly zálohovány na dalších sedm dní. Jelikož uživatelka nahlásila tento problém okamžitě, byla zde možnost data obnovit.

Obnovení dat probíhalo následovně:

1. Data byla synchronizována do Google Storage bucketu `krcalova-bucket`, takže bylo potřeba se přihlásit do GCP a najet do sekce Cloud Storage.
2. Zde po rozkliknutí nebyla implicitně vidět složka uživatelky Marty, jelikož po synchronizaci byl obsah její `Public` složky prázdný, a tak se smazala. V implicitní nastavení se ukazují `Live objects only` (česky „Pouze živé objekty“). Toto nastavení bylo potřeba změnit na `Soft-deleted objects only` (česky „Pouze soft-deleted objekty“). Poté již byla vidět složka uživatelky Marty. Obsah této složky je vidět na obrázku 5.3.

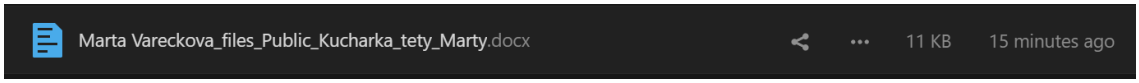


Obrázek 5.3: Smazaný soubor (1) a datum, kdy by byl soubor nezvratně smazán (2).

3. Po rozkliknutí smazaného souboru se konečně otevře možnost obnovit dokument 5.4. Na tomto obrázku je možné vidět následující: Cesta k dokumentu; (2) – Datum poslední nahrané verze dokumentu; (3) – Zde je potřeba nastavit, aby se ukázaly již smazané dokumenty; (4) – Možnost pro obnovení dokumentu. K obnovení slouží tlačítko `Restore`.

Obrázek 5.4: Pokud je nastaven „Soft Delete“, zde je možné smazaný dokument obnovit.

4. Jelikož je na cloudu pro synchronizaci nastavena pouze jednosměrná synchronizace. Bylo tak nutné obnovený soubor stáhnout z Cloud Storage a opětovně jej nahrát na Nextcloud, jinak by se po synchronizaci soubor opět smazal. Na obrázku 5.5 lze vidět, jak se změní název souboru po obnovení – nově bude ukazovat cestu, ze které byl po obnovení stažen.



Obrázek 5.5: Opětovně nahraný obnovený soubor na Nextcloud.

Složitost: 2

Závěr: Tento incident se stal na základě lidského faktoru, při kterém byl neúmyslně smazán konkrétní soubor. Jelikož byl zálohován, povedlo se jej obnovit. Aby se díky synchronizaci soubor opětovně nesmazal z Cloud Storage, byl opětovně nahrán na Nextcloud.

5.3 Audit příkladu 3 – Škodlivý soubor (4.3)

Shrnutí: Dne 11. 05. 2024 nahlásil uživatel `Ignác Kuřátko` ztrátu několika souborů z cloudu. V cloudu byl nalezen škodlivý soubor, který místo otevření .pdf souboru přesměruje na falešnou přihlašovací obrazovku Nextcloudu – jde totiž o .pdf.html soubor, konkrétně soubor `koho_vyhodime_dalsiho.pdf.html`.

Úkol: Cílem je najít tento škodlivý soubor, zjistit, co soubor dělá, kdo jej nahrál, jak a kdy. Jaká je možná ztráta a zda byl uživatel jediný, co byl kompromitován.

Audit :

Identifikace: V tomto konkrétním případě nejsou podstatné logy událostí z Google Cloud Storage, byly však i tak staženy pro případné dohledávání událostí. Budou zde podstatné hlavně auditní logy Nextcloudu a systémové Nextcloud logy.

Uchování a shromažďování: Byly zajištěny soubory audit.log a nextcloud.log z Nextcloudu a logy z GCP v souboru gcp-logs.json. Kopie těchto souborů byly nahrané do složky **Case3** a jejich SHA1 hashe jsou následující:

Názvy souborů s důkazními materiály	**SHA1**
audit.log	B68A1C9758D2F4459BA9E967935054C4BF714063
nextcloud.log	3C7EEFA7E8467192D5C83D802A49458FA3DBDFF1
gcp-logs.json	AEABAFB47BA7978759C63B5C14D6881B35646CD4

Tabulka 5.5: Tabulka obsahující hashe SHA1 souborů obsahujících důkazní materiály k příkladu 3.

Zároveň byl zajištěn i jeden škodlivý soubor, ten byl vložen do složky na cestě `/Case3/Quarantine`.

Název škodlivého souboru	**SHA1**
koho_vyhodime_dalsiho.pdf.html	FB1AFA99E1EAF0A968169DF1675CDABB81A4EFE1

Analýza: Incident byl nahlášen 03. 05. 2024, tedy první předpoklad byl, že akce byla provedena před tímto datem včetně. Bylo zjištěno, že dne 01. 05. 2024 v 10:40:29 byl škodlivý soubor `koho_vyhodime_dalsiho.pdf.html` nahrán uživatelkou Amélií Širokou z IP `84.55.18.29`. Přihlášení k jejímu účtu předcházelo šest (6) neúspěšných přihlašování, lze se domnívat, že se stala terčem slovníkového nebo brute-force útoku. Během tohoto přihlášení bylo **změněno heslo k tomuto účtu**.

Útočník dále pod tímto účtem přistoupil k souboru `doplnit_dopravu.docx`. Následně došlo k jeho odhlášení. Jako pravděpodobně první byly zcizeny přihlašovací údaje uživatele Květoslava Květinky, jemuž útočník následně odcizil celkem šest souborů. Následně byly zcizeny i přihlašovací údaje uživatele Ignáce Kuřátka, jemuž byly odcizeny a následně i smazány čtyři soubory. V neposlední řade byly odcizeny přihlašovací údaje i uživateli Aloisy Knížečkovi, které mu byly odcizeny celkem čtyři soubory, jeden z kompromitovaných souborů byl i textový soubor s názvem `hesla.txt`.

Po analýze škodlivého souboru bylo potvrzeno, že jde o phishingový formulář, který odesílal data do telegramové skupiny `telegram[.]app/sxs2432DAC`. Identitu vlastníka této skupiny nebylo možné zjistit.

Časová osa :

Datum, čas (UTC)	Původ artefaktu	Artefakt
2024-05-01 10:36:00	Nextcloud.log	Šest neúspěšných přihlášení uživatelky Amálie.
2024-05-01 10:37:17	Audit.log	Přihlášení uživatelky Amálie z IP 84.55.18.29.
2024-05-01 10:40:29	Audit.log	Vytvoření souboru .html v Nextcloudu uživatelkou.
2024-05-01 10:40:54	Audit.log	Nasdílení souboru 8 uživatelům.
2024-05-01 10:42:25	Audit.log	Přístup k souboru doplnit_dopravu.docx
2024-05-01 10:47:55	Audit.log	Změna hesla k účtu Amálie Široké.
2024-05-01 10:48:11	Audit.log	Odhlášení uživatele.
2024-05-01 10:48:57	Audit.log	Přihlášení uživatele Květoslav Květinka.
2024-05-01 10:49:30	Audit.log	Přistoupení ke kompromitovanému .html souboru.
2024-05-01 10:50:01	Audit.log	Stažení škodlivého souboru .html.
2024-05-01 10:54:31	Audit.log	Odhlášení uživatele Květoslava.
2024-05-01 10:54:37	Audit.log	Neúspěsné přihlašování kompromitovaného účtu Amálie.
2024-05-01 11:58:03	Audit.log	Přihlášení uživatele Ignáce Kuřátka.
2024-05-01 11:59:07	Audit.log	Stažení škodlivého souboru .html.
2024-05-01 12:00:09	Audit.log	Odhlášení uživatele Ignáce Kuřátka.
2024-05-02 03:03:02	Audit.log	Přihlášení uživatele Květoslav Květinka z IP 84.55.18.29.
2024-05-02 03:03:06	Audit.log	Přístup k dokumentu Readme.md.
2024-05-02 03:03:30	Audit.log	Exfiltrace celkem šesti souborů.
2024-05-02 03:03:57	Audit.log	Odhlášení uživatele.
2024-05-02 03:04:04	Audit.log	Přihlášení uživatele Ignác Kuřátko z IP 84.55.18.29.
2024-05-02 03:04:31	Audit.log	Exfiltrace celkem čtyř souborů.
2024-05-02 03:04:37	Audit.log	Smazání exfiltrovaných souborů z cloudu.
2024-05-02 03:04:44	Audit.log	Odhlášení uživatele.
2024-05-02 12:06:06	Audit.log	Přihlášení uživatele Aloise Knížečky.
2024-05-02 12:10:04	Audit.log	Stažení škodlivého souboru .html.
2024-05-02 12:10:31	Audit.log	Odhlášení uživatele Aloise.
2024-05-02 23:10:37	Audit.log	Přihlášení uživatele Aloise z IP 84.55.18.29.
2024-05-02 23:10:57	Audit.log	Exfiltrace souboru hesla.txt a dalších tří souborů.
2024-05-02 23:11:05	Audit.log	Odhlášení uživatele.

Tabulka 5.6: Časová osa analýzy třetího příkladu.

Složitost: 7

Poznámka: Jedním z nekompromitovaných účtů jsem při realizaci okomentovala dokument přímo v Nextcloudu jako rádoby „naznačení“ nahlášení, k mému překvapení tato akce není zalogovaná.

Závěr: Během tohoto útoku došlo ke kompromitaci celkem **tří** účtů, konkrétně účtů uživatelů: Ignác Kuřátko, Květoslav Květinka a Alois Knížečka. Poslední účet, Alois Knížečka, je **adminem** Nextcloudu i Google Cloudu. 02. 05. 2024 došlo k exfiltraci celkově **třinácti** (13) souborů, některých z nich opakovaně. Jejich seznam lze vidět dále. Po exfiltraci souborů z cloudu uživatele Ignáce Kuřátka došlo následně i ke **smazání** těchto souborů. Jeden z těchto souborů, `data_cest.xlsx`, byl zálohovaný v Google Storage, ten se podařilo obnovit. Další tři soubory se však obnovit nepodařilo.

Dne 02. 05. 2024 došlo taktéž k exfiltraci souboru s názvem `hesla.txt` uživatele Aloise Knížečky – administrátora.

Kompromitované účty byly dočasně zablokovány.

Seznam exfiltrovaných dokumentů :

Květoslav Květinka –

- 13102023.txt,
- 7.pdf
- dailyMeeting.pptx
- data_cest.xlsx
- doplnit_dopravu.docx
- final_final.docx

Ignác Kuřátko –

- tufu.md (odstraněn – nezálohován)
- Screenshot 2024-01-11 104242.png (odstraněn – nezálohován)
- data_cest.xlsx (odstraněn – **zálohován**)
- MENU_Kveten2024.pdf (odstraněn – nezálohován)

Alois Knížečka –

- final_final_schvalene.docx
- planOprav2025.pptx
- prescasyKveten2024.xlsx
- **hesla.txt**

Doporučení: Je potřeba změnit hesla kompromitovaným účtům, ideálně využít dvoufaktorové ověřování. Dále je potřeba zálohovat dokumenty, aby již nedošlo k nezvratné ztrátě dokumentů. U uživatele Aloise Knížečky je potřeba změnit hesla na všech platformách, ke kterým měl napsaná hesla v textovém souboru na cloudu a to urychleně. Také je potřeba zjistit, zda v mezidobě do změny hesel nedošlo např. k další kompromitaci mimo tento cloud. Je důležité vyjasnit, že ani soukromý cloud organizace není místo pro uchovávání hesel a jako uchovávač hesel je vhodné užít aplikaci k tomu určenou (např. keypass). V neposlední řadě je potřeba proškolit zaměstnance o existenci phishingových a jiných útoků, aby byli schopni tyto útoky odhalit a nahlásit, čímž by se jim do budoucna zabránilo.

5.4 Audit příkladu 4 – Ilegální obsah v cloudu (4.4)

Shrnutí: Nejmenovaný muž je obviněn z držení nelegálních fotek a nahrávek nezletilých, je ale potřeba doplnit více důkazů soudu. Soubory by se mohly nacházet v cloudu.

Úkol: Úkolem je objevit usvědčující materiály a potvrdit, že je zde opravdu nahrál obžalovaný.

Místa k hledání důkazů: Živý cloud.

Audit :

Identifikace: Pro audit tohoto případu je možné využít celý cloud, jeho obsah i s možností vygenerovat logy.

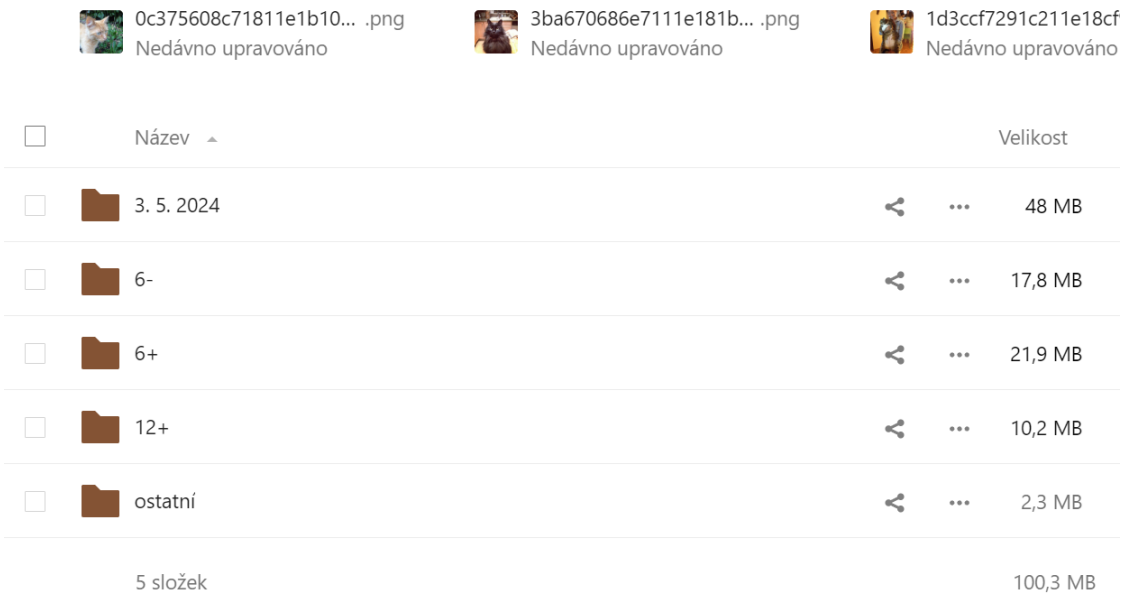
Uchování a shromažďování: Přihlašovací údaje k účtům byly zajištěny společně s pachatelem. Jsou tedy uchovány v místnosti s důkazy a analytik dostal jejich kopii.

Názvy souborů s důkazními materiály	SHA1
email1.eml	29F20F7FFE3E48A03A4DAACA5A90040D3B1B2486
email2.eml	0BBC373E61D7A6C9CF0ACC1C44F893AA307BCED5
email3.eml	2EF7F1E871BEEE05DEE079949B2F5040FE49DCDE
email4.eml	0AA4CDD73CE2AD6C362ECA8BAE602039466C76DB
faktura1.docx	2E879C704B1530103236281B05D4F9D5D62C36FD
přihlašovací údaje	–

Tabulka 5.7: Tabulka obsahující hashe SHA1 souborů obsahujících důkazní materiály k příkladu 4.

Analýza: Po přihlášení do cloudu bylo zjištěno, že má pachatel spojený Nextcloud s e-mailem, byla tedy možnost zajistit obsah této schránky.

Již při prvním vstupu do cloudu bylo jasné, o co zde půjde. Cloud obsahoval stovky fotek zobrazující malá koťátka. Fotky byly rozděleny do složek podle věkové kategorie. Konkrétně zde byly složky – 6-, 6+, 12+, ostatní a „03. 05. 2024“. Dohromady došlo k zajištění 10.2MB nelegálně držených fotek 5.6.



Obrázek 5.6: Zobrazení obsahu zadrženého cloudu.

V Cloud Storage byl nalezen jeden nedávno smazaný soubor díky funkci „Soft Delete“. Tento soubor byl obnoven a přidán do složky s důkazními materiály. Jednalo se o soubor s názvem `faktura1.docx`. Po obnovení souboru bylo zjištěno, že vystavovatelem této faktury byl skutečně pachatel – `Jaroslav Štrůdl`. Fakturovaný byl muž jménem `Jiří Mrázek`. Jednou z fakturovaných položek bylo „Focení 03. 05. 2024“ – v cloudu byla nalezena složka s názvem „03. 05. 2024“ a obsahovala taktéž fotky koťátek. Jde tedy o usvědčující fakturu.

Ve schránce byly nalezeny dvě zprávy právě od `Jiřího Mrázka`, ve kterých se domlouvali na předání obálky. Byly tu ale i další dva znepokojivé e-maily, od `Marie Stránské`, která napsala: „4000 ti za 2 fotky nedám, jedině v případě, že by byly mladší.“. Poslední zpráva byla od `Radima Olejníka`, zde došlo opět k domlouvání místa předání obálky, tentokrát bylo jasně řečeno, že jde o obálku s penězi.

Složitost: 5

Závěr: Po analýze cloudu bylo zajištěno dostatek důkazů pro obvinění z držení a distribuce fotek malých koťat. Bylo zadrženo celkem 303 nelegálně držených fotek. Důkazní materiály byly staženy z cloudu. Taktéž byla zanalyzovaná komunikace s třemi lidmi, kteří by mohli být terčem dalšího vyšetřování.

5.5 Audit příkladu 5 – APT (4.5)

Shrnutí: Po kompromitaci přihlašovacích údajů bylo zapotřebí zauditovat akce konané pod tímto účtem.

Úkol: Cílem je zanalyzovat aktivitu kompromitovaného účtu.

Místa k hledání důkazů: Jelikož útočníkova aktivita na privátním cloudu již byla zanalyzována, tak je zapotřebí zanalyzovat veškerou aktivitu kompromitovaného uživatele na veřejné části cloudu.

Audit :

Identifikace: Analýze je potřebné podrobit veškerou aktivitu kompromitovaného účtu v Google Cloudu.

Uchování a shromažďování: Pro analýzu budou staženy logy zvlášť do jednotlivých souborů z „bucketu“ projektu (`krcalova-bucket.json`) , zvlášť logy vyfiltrované o aktivitu kompromitovaným účtem (`alois-knizecka.json`), logy toků ve virtuální síti (`vpc-flows.json`) a celkově všechny logy z projektu GCP (`gcp-all.json`). Důležité jsou v tomto případě i logy celé organizace marticek.eu (`organization-logs.json`).

Názvy souborů s důkazními materiály	**SHA1**
krcalova-bucket.json	1641C2817D3E7AB8CAD9B49C9356145306B56A76
gcp-all.json	F87A101FD25EFB84286ADD59F4F344DCF34876F4
alois-knizecka.json	A947BB903C70A788DF07DF5D9C3651C6C37001AD
vpc-flows.json	DDA4799DFB6BFB520E9EC38FD89DA6EEF0898661
organization-logs.json	FFAFCA4DDFCE7B9CF8DEFFB02D345498B35C072F

Tabulka 5.8: Tabulka obsahující hashe SHA1 souborů obsahujících důkazní materiály k příkladu 5.

Analýza: Složitost této analýzy je vysoká hlavně z důvodu velkého množství logů, které je potřeba procházet a zároveň kontrolovat, zda nejde o legitimní aktivitu uživatele. Nebylo jasné, zda útočník účet použil, kdy, ani jak. Nakonec však bylo potvrzeno, že byl účet skutečně využit útočníkem:

Po přihlášení ke kompromitovanému účtu došlo k vytvoření servisního účtu s názvem `rclon3`. Tomuto účtu byla následně přidána role `owner`. Pro tento servisní účet byl vytvořen nový klíč. Dále byl také účtem vytvořen nový projekt a také „sink“. Následně došlo k nahrání klíče do virtuálního stroje a byl nastaven `rclone config`. V neposlední řadě došlo k vytvoření nového bucketu a pomocí gsutil došlo k exfiltraci dat uživatelů z Nextcloudu.

Během tohoto případu tedy opravdu došlo ke zneužití uživatelského účtu a následně i k exfiltraci velkého množství dat.

Časová osa :

Datum, čas (UTC)	Původ artefaktu	Artefakt
2024-05-14 22:07:28	gcp-all.json	Přihlášení účtu Aloise Knížečky z IP a přistoupení k projektu moonlite-celiling..
2024-05-14 22:08:56	gcp-all.json	Vytvoření servisního účtu „rclon3“.
2024-05-14 22:09:11	gcp-all.json	Přidání owner práv servisnímu účtu.
2024-05-14 22:09:50	gcp-all.json	Vytvoření klíče pro servisní účet.
2024-05-14 22:12:26	organization-logs.json	Vytvoření nového projektu.
2024-05-14 22:14:49	gcp-all.json	Vytvoření nového „sinku“.
2024-05-14 22:17:09	gcp-all.json	Nahrání klíče do virtuálního stroje.
2024-05-14 22:20:50	gcp-all.json	Nastavení rclone config.
2024-05-14 22:23:31	gcp-all.json	Vytvoření nového bucketu.
2024-05-14 22:29:55	gcp-all.json	Pomocí gsutil exfiltrace velkého počtu souborů.

Tabulka 5.9: Časová osa analýzy pátého příkladu.

Složitost: 9.5

Závěr: Byla potvrzena kompromitace Google Cloud účtu uživatele Aloise Knížečky. Jeho účet byl zneužit pro vytvoření servisního účtu, pomocí kterého došlo k exfiltraci velkého počtu souborů všech uživatelů z Nextcloudu. K tomu došlo za využití `rclone`. Pomocí OSINTu[2] bylo zjištěno, že tyto techniky využívá jediná APT skupina, a to Brněnské APT29810.

Analýza všech příkladů je tímto ukončená. Obtížnost jednotlivých analýz byla rozmanitá, stejně tak i rozsah jejich působnosti. Úvod byl vždy vymyšlen tak, aby analytika vtáhl do děje. Snažila jsem se, aby byly příklady blízké situaci, která může v realitě nastat. Pro podrobnější postup při analýze je vhodné se podívat do příručky, která doplňuje tuto práci. Tato příručka je dodána v elektronické formě.

Všechny jména, emaily i úvody k příkladům použité v realizaci byly smyšlené a neodkazují na žádné reálné lidi ani situace.

[2]OSINT, neboli Open-Source Intelligence, je definována jako zpravodajská informace vytvářená sběrem, vyhodnocováním a analýzou veřejně dostupných informací za účelem zodpovězení konkrétní zpravodajské otázky [18].

Kapitola 6

Vyhodnocení

Vybraným způsobem pro vyhodnocení této práce bylo nechat příklady zanalyzovat dalšími lidmi. Tito jedinci dostali krátké uvedení do problému, metodickou příručku s postupy a virtuální stroj. Všechny analýzy probíhaly za mé přítomnosti.

Jedinci byli vybráni jak z řad odborníků na digitální forenzní analýzu, tak i z řad forenzních laiků. Všichni respondenti však měli minimálně bakalářský titul z IT a byli ve věku 23-28 let.

Každý dostal za úkol zkusit zanalyzovat příklady 4.1, 4.3 a příklad 4.5, a to pouze s pomocí příručky – bez možnosti dohledávat informace na internetu. Následně pak měli za úkol vyplnit formulář, ve kterém byly otázky týkající se jak případu samotného, tak i zpracování příručky. Přehled celkových odpovědí z formulářů lze vidět v příloze C.

Následující tabulka 6.1 zobrazuje výsledky, ke kterým jsem došla po vyhodnocení dotazníků. Písmena A – E zde označují jednotlivé respondenty, mezi nimiž respondenti A a B jsou odborníky na forenzní analýzu koncových stanic a serverů.

U většiny otázek byla škála od 1 po 5, kde 1 znamená „Naprosto souhlasím“ a 5 znamená „Naprosto nesouhlasím“. Pouze u otázek na obtížnost analýzy byla škála jiná, a to od 1 po 10, kde 1 znamená „Příliš jednoduchá obtížnost“ a 10 znamená „Obtížnost pro forenzního veterána“.

Otázka	**A**	**B**	**C**	**D**	**E**	**Průměr**
Mám zkušenost s forenzní analýzou.	Ano	Ano	Ne	Ne	Ne	2/5
Spustit virtuální stroj mi nedělalo problém.	1	1	1	1	1	1
Ve virtuálním stroji jsem vždy věděl, kde co je.	1	1	1	1	1	1
S pomocí příručky jsem neměl problém příklad 1 (Insider) zanalyzovat.	1	1	1	1	1	1
Zanalyzovat příklad 1 (Insider) bych zvládl i bez příručky.	1	1	1	2	1	1,2
Na škále od 1 po 10 mi obtížnost analýzy příkladu 1 (Insider) přišla:	3	2	3	4	3	3
S pomocí příručky jsem neměl problém příklad 2 (Škodlivý kód) zanalyzovat.	1	1	1	1	1	1
Zanalyzovat příklad 2 (Škodlivý kód) bych zvládl i bez příručky.	1	1	3	2	2	1,8
Na škále od 1 po 10 mi obtížnost analýzy příkladu 2 (Škodlivý kód) přišla:	4	5	5	5	6	5
S pomocí příručky jsem neměl problém příklad 3 (APT) zanalyzovat.	1	1	2	1	1	1,2
Zanalyzovat příklad 3 (APT) bych zvládl i bez příručky	3	3	4	5	5	4
Na škále od 1 po 10 mi obtížnost analýzy příkladu 3 (APT) přišla:	8	8	9	10	9	8,8
Neměl jsem problém s pochopením jednotlivých kroků v příručce.	1	1	1	1	1	1
Příručka mi přišla intuitivní.	1	1	1	1	1	1
Postupy mi přišly zbytečně podrobné.	2	3	4	5	5	3,8
Úvody příkladů mě snadno vtáhly do analýzy.	1	1	1	1	1	1
Scenáře jednotlivých příkladů mi přijdou reálné.	1	1	2	1	1	1,2

Tabulka 6.1: Odpovědi respondentů z dotazníku.

Všichni respondenti se shodli na následujícím:

- Virtuální stroj byl nastaven v pořádku. Jeho spuštění ani orientace v něm nebyla problémem.
- Příklady 1 a 2 byly s pomocí příručky jednoduché k analýze.
- Příručka byla intuitivní a jednotlivé kroky byly napsané pochopitelně.
- Úvody k příkladů byly vymyšlené tak, aby člověka snadno vtáhly do analýzy.

Odpovědi respondentů při posuzování obtížnosti analýz se taktéž nijak výrazně nelišily, ačkoliv jsem zde čekala, větší rozptyly odpovědí. Kde se naopak odpovědi lišily bylo v otázce ohledně podrobnosti postupů v příručce. Jelikož byli mezi respondenty jak odborníci, tak forenzní amatéři, tak můj předpoklad, že pro odborníky budou postupy moc jednoduché, byly potvrzeny.

Obtížnosti jednotlivých příkladů byly rozmanité – nejjednodušší příklad pro analýzu byl příklad Insidera a naopak nejtěžší pro analýzu byl příklad spojený s APT. Na tom se respondenti taktéž shodli.

Zároveň jsem si potvrdila, že příručka je funkční a splňuje to, co jsem chtěla – můžou podle ní analyzovat nejenom znalí analytici, ale i nezkušení IT nadšenci. To, zda jsou postupy v ní moc podrobné nebo ne je již čistě na schopnosti jednotlivců.

Kapitola 7

Závěr

Cílem práce bylo vytvořit metodologii pro digitální forenzní analýzu hybridního cloudu. Tento cíl byl splněn, stejně tak všechny body zadání. Byly nastudovány metody forenzní analýzy hybridních cloudů, pro experimentální prostředí byla vytvořena vlastní hybridní platforma ve spojení Google Cloudu a Nextcloudu. Možnosti auditu aktivit uživatelů byly nastudovány i popsány v této práci, stejně tak i způsob získávání důkazních materiálů. Zároveň bylo navrženo a realizováno pět příkladových situací, které jsem se snažila vybrat tak, aby nešlo o pět stejných analýz, ale aby byla analýza různorodá. Některé příklady tak byly zaměřeny více na soukromou část cloudu, další naopak na část veřejnou. Postup analýzy těchto příkladů byl popsán v této práci, podrobnější postup byl pak popsán v příručce, která slouží k doplnění této práce. Na závěr bylo vytvořeno virtuální prostředí, ve kterém jsem dala prostor vybraným jedincům k ozkoušení příručky a podle jejich zpětné vazby jsem práci vyhodnotila. Respondenti se shodli na tom, že je příručka funkční a vybrané příklady k analýze působily reálně a byly dostatečně podrobně popsány.

Myslím si, že tato práce rozvíjí spoustu možností pro její rozšíření, jako je porovnání s jiným, „samo-složeným“ hybridním cloudem, porovnání s již vytvořenou hybridní platformou, jako je například Google Anthos. Zajímavé by také bylo zpracování s využitím SIEM platforem, kde by byly logy jednotně analyzovatelné.

Práce mi dala nový rozhled do oblasti forenzní analýzy nejen cloudu a otevřela mi nové prostory, ve kterých se můžu zlepšovat. Sama práci hodnotím pozitivně, a to nejen podle vyhodnocení. Kdybych mohla na práci něco změnit, tak bych se nesnažila sama vytvářet hybridní cloudovou platformu, jelikož jsem na jeho nastavování strávila až moc času, a šla bych cestou již vytvořeného hybridního řešení.

Literatura

[1] *About us* [online]. Nextcloud [cit. 2024-01-13]. Dostupné z: https://nextcloud.com/about/.

[2] Agbedanu, P. R., Wang, P., Nortey, R. N. a Odartey, L. K. Forensics in the Cloud: A Literature Analysis and Classification. In: *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*. 2019, s. 124–132. DOI: 10.1109/BIGCOM.2019.00027.

[3] Caloyannides, M. *Computer Forensics and Privacy*. Artech House, 2001. ISBN 9781580532839.

[4] Choo, K.-K. R., Esposito, C. a Castiglione, A. Evidence and Forensics in the Cloud: Challenges and Future Research Directions. *IEEE Cloud Computing*. 2017, sv. 4, č. 3, s. 14–19.

[5] *Cloud Audit Logs overview* [online]. Google Cloud [cit. 2024-03-20]. Dostupné z: https://cloud.google.com/logging/docs/audit.

[6] *Cloud vs. on-premise: Jaká je budoucnost?* [online]. TotalService [cit. 2024-03-10]. Dostupné z: https://www.totalservice.cz/novinky/cloud-vs-on-premise-jaka-je-budoucnost-2021-04-14.

[7] *Co je to slovníkový útok* [online]. Správa sítě [cit. 2024-04-30]. Dostupné z: https://www.sprava-site.eu/slovnikovy-utok/.

[8] *Digital forensics* [online]. Interpol [cit. 2023-10-02]. Dostupné z: https://www.interpol.int/How-we-work/Innovation/Digital-forensics.

[9] Dissanayaka, A., Mengel, S., Shetty, R., Gittner, L., Kothari, S. et al. A review of MongoDB and singularity container security in regards to HIPAA regulations. In:. Association for Computing Machinery, Inc, Prosinec 2017, s. 91–97.

[10] *Google Cloud Documentation* [online]. Google Cloud [cit. 2024-03-27]. Dostupné z: https://cloud.google.com/docs.

[11] Hemdan, E. E.-D. a Manjaiah, D. H. A cloud forensic strategy for investigation of cybercrime. In: *2016 International Conference on Emerging Technological Trends (ICETT)*. 2016, s. 1–5. DOI: 10.1109/ICETT.2016.7873667.

[12] Herman, M., Iorga, M. et al. *NIST Cloud Computing Forensic Science Challenges*. NIST Interagency/Internal Report (IR) 8006. National Institute of Standards and Technology, srpen 2020.

[13] Kanade, V. Multi-Cloud vs. Hybrid Cloud: 10 Key Comparisons. *Spiceworks*. Březen 2022.

[14] Maksymovych, O. *Google Cloud for Data Scientists: Harnessing Cloud Resources for Data Analysis* [online]. 2023 [cit. 2024-01-14]. Dostupné z: https://www.datacamp.com/blog/google-cloud-for-data-scientists.

[15] Mohanakrishnan, R. *What Is Hybrid Cloud? Definition, Architecture, and Management Best Practices for 2021* [online]. Spiceworks [cit. 2024-04-01]. Dostupné z: https://www.spiceworks.com/tech/cloud/articles/what-is-hybrid-cloud/.

[16] Murphy, C. *What is a Hybrid Cloud?* [online]. Oracle, 2024 [cit. 2024-10-05]. Dostupné z: https://www.oracle.com/cz/cloud/hybrid-cloud/what-is-hybrid-cloud/.

[17] Quick, D., Martini, B. a Choo, K.-K. R. Chapter 2 – Cloud Storage Forensic Framework. In: *Cloud Storage Forensics*. Boston: Syngress, 2014, s. 13–21. ISBN 978-0-12-419970-5.

[18] Ritu, G. *What is Open-Source Intelligence?* [online]. Sans, 2023 [cit. 2024-05-14]. Dostupné z: https://www.sans.org/blog/what-is-open-source-intelligence/.

[19] *Routing and storage overview* [online]. Google Cloud, 2024 [cit. 2024-04-30]. Dostupné z: https://cloud.google.com/logging/docs/routing/overview.

[20] Sammons, J. Chapter 1 – Introduction. In: *The Basics of Digital Forensics*. Boston: Syngress, 2012, s. 1–12. DOI: https://doi.org/10.1016/B978-1-59749-661-2.00001-2. ISBN 978-1-59749-661-2.

[21] Sang, T. A Log Based Approach to Make Digital Forensics Easier on Cloud Computing. In: *2013 Third International Conference on Intelligent System Design and Engineering Applications*. 2013, s. 91–94. DOI: 10.1109/ISDEA.2012.29.

[22] Shawi, M. A. *Build hybrid and multicloud architectures using Google Cloud* [online]. Google [cit. 2024-04-09]. Dostupné z: https://cloud.google.com/architecture/hybrid-multicloud-patterns.

[23] Simplilearn. *What Is Digital Forensics?* [online]. Simplilearn, srpen 2023 [cit. 2023-10-02]. Dostupné z: https://www.simplilearn.com/what-is-digital-forensics-article.

[24] *SLA* [online]. Správa sítě [cit. 2024-05-03]. Dostupné z: https://www.sprava-site.eu/sla/.

[25] *Uncovering Digital Evidence: Navigating the Complexities of Cloud Computing Forensic Science* [online]. Cyber Security Journal, duben 2023 [cit. 2024-01-14]. Dostupné z: https://www.ssl2buy.com/cybersecurity/cloud-computing-forensic-science.

[26] *Understanding the basics of cloud computing* [online]. Lucidchart [cit. 2024-04-16]. Dostupné z: https://www.lucidchart.com/blog/cloud-computing-basics.

[27] Wang, Y., Uehara, T. a Sasaki, R. Fog Computing: Issues and Challenges in Security and Forensics. In: *2015 IEEE 39th Annual Computer Software and Applications Conference*. 2015, sv. 3, s. 53–59. DOI: 10.1109/COMPSAC.2015.173.

[28] *What is a Hybrid Cloud?* [online]. Google [cit. 2024-10-05]. Dostupné z: https://cloud.google.com/learn/what-is-hybrid-cloud.

[29] *What is a hybrid cloud network?* [online]. Vmware [cit. 2024-03-25]. Dostupné z: https://www.vmware.com/topics/glossary/content/hybrid-cloud-networking.html.

[30] *What is a Hybrid Cloud Strategy?* [online]. Vmware [cit. 2024-03-25]. Dostupné z: https://www.vmware.com/topics/glossary/content/hybrid-cloud-strategy.html.

[31] *What is cloud?* [online]. Windows Azure [cit. 2023-10-02]. Dostupné z: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud.

[32] *What is cloud computing?* [online]. Oracle. Dostupné z: https://www.oracle.com/cz/cloud/what-is-cloud-computing/.

[33] *What is Hybrid Cloud?* [online]. Vmware [cit. 2024-03-21]. Dostupné z: https://www.vmware.com/topics/glossary/content/hybrid-cloud.html.

[34] *What is Hybrid Cloud Architecture?* [online]. Vmware [cit. 2024-03-25]. Dostupné z: https://www.vmware.com/topics/glossary/content/hybrid-cloud-architecture.html.

[35] *What is Splunk?* [online]. Fortinet [cit. 2024-05-02]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-splunk.

[36] Zawoad, S. a Hasan, R. Digital Forensics in the Cloud. *The Journal of Defense Software Engineering*. Září 2013, sv. 26.

Příloha A

Ukázka struktury logu z GCP

Ukázka, jak vypadá struktura logu události v GCP. Zaznamenává událost synchronizaci dat pomocí rclone do „bucketu“ `krcalova-bucket`, ke kterému došlo v 21:05 UTC.


```
{
  "protoPayload": {
    "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
    "status": {},
    "authenticationInfo": {
      "principalEmail": "rclone@moonlit-ceiling-421418.iam.gserviceaccount.com",
      "serviceAccountKeyName": "//iam.googleapis.com/projects/moonlit-ceiling-421418/serviceAccounts/
rclone@moonlit-ceiling-421418.iam.gserviceaccount.com/keys/94ab08937caf2fe81d9c23d8ee86fd9499ead943"
    },
    "requestMetadata": {
      "callerIp": "34.116.212.178",
      "callerSuppliedUserAgent": "rclone/v1.66.0,gzip(gfe)",
      "callerNetwork": "//compute.googleapis.com/projects/moonlit-ceiling-421418/global/networks/
__unknown__",
      "requestAttributes": {
        "time": "2024-05-10T21:05:02.375669914Z",
        "auth": {}
      },
      "destinationAttributes": {}
    },
    "serviceName": "storage.googleapis.com",
    "methodName": "storage.objects.list",
    "authorizationInfo": [
      {
        "resource": "projects/_/buckets/krcalova-bucket",
        "permission": "storage.objects.list",
        "granted": true,
        "resourceAttributes": {}
      }
    ],
    "resourceName": "projects/_/buckets/krcalova-bucket",
    "resourceLocation": {
      "currentLocations": [
        "europe-central2"
      ]
    }
  },
  "insertId": "c7z501dalsn",
  "resource": {
    "type": "gcs_bucket",
    "labels": {
      "project_id": "moonlit-ceiling-421418",
      "bucket_name": "krcalova-bucket",
      "location": "europe-central2"
    }
  },
  "timestamp": "2024-05-10T21:05:02.367575185Z",
  "severity": "INFO",
  "logName": "projects/moonlit-ceiling-421418/logs/cloudaudit.googleapis.com%2Fdata_access",
  "receiveTimestamp": "2024-05-10T21:05:03.111126874Z"
}
```


Obrázek A.1: Struktura logu události z GCP.

Příloha B

Šablona pro vytváření zprávy z analýzy

Jde o jednoduchou šablonu pro vytvoření zprávy z analýzy, která je uložená v textovém souboru zprava.txt.

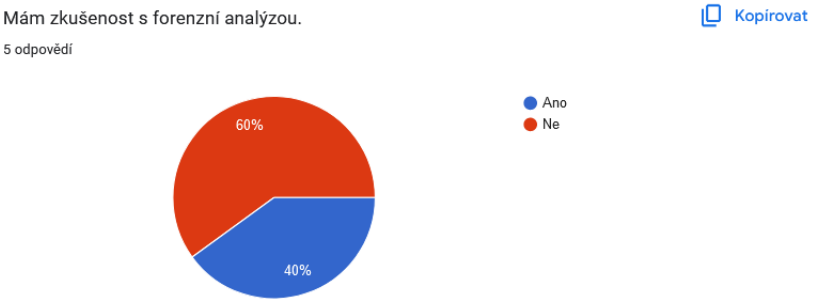
```
_____________________________________________________________________________

Zpráva z analýzy:
_____________________________________________________________________________

Základní informace:

        - Datum nahlášení incidentu:
        - Nahlásil/a:
        - Důvod analýzy:
        - Předpokládaný datum a čas nahlášeného incidentu:
        - Cíl analýzy:
-----------------------------------------------------------------------------
        - Datum vytvoření zprávy:
        - Analýzu vykonal/a a zprávu sepsal/a:
-----------------------------------------------------------------------------

Časová osa:
_____________________________________________________________________________
|  <datum, čas> |     původ artefaktu   |       artefakt        |    Poznámka   |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|               |                       |                       |               |
-----------------------------------------------------------------------------
|_______________|_______________________|_______________________|_______________|

Nalezené indikátory kompromitace (IOC`s)
_____________________________________________________________________________
|     Název     |        Umístění               |        Hash (MD5, SHA1)       |
-----------------------------------------------------------------------------
|               |                               |                               |
-----------------------------------------------------------------------------
|               |                               |                               |
-----------------------------------------------------------------------------
|               |                               |                               |
-----------------------------------------------------------------------------
|_______________|_______________________________|_______________________________|

Závěr:
```

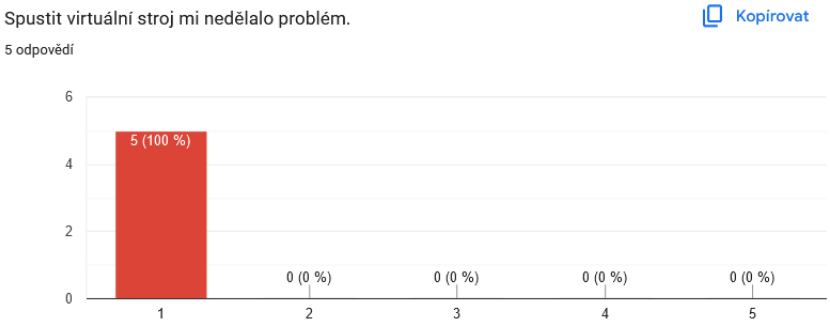
Obrázek B.1: Šablona pro vytvoření zprávy z analýzy.

Příloha C

Dotazník k příručccce a analýzám

Odkaz na formulář je následující: https://forms.gle/JBLB8y31atVVCc536. Dotazník se skládal celkem z 18 otázek, kde jedna konečná byla otázka otevřená. Na dalších obrázcích jsou vidět celkové odpovědi od všech respondentů.

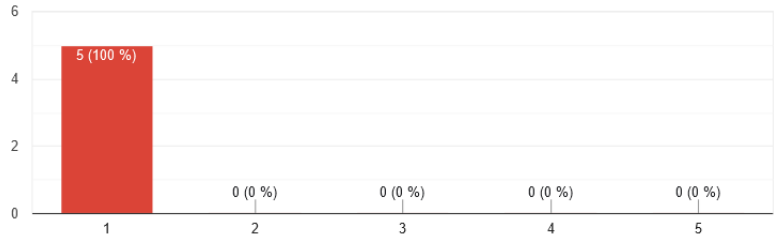




Ve virtuálním stroji jsem vždy věděl, kde co je.

Kopírovat

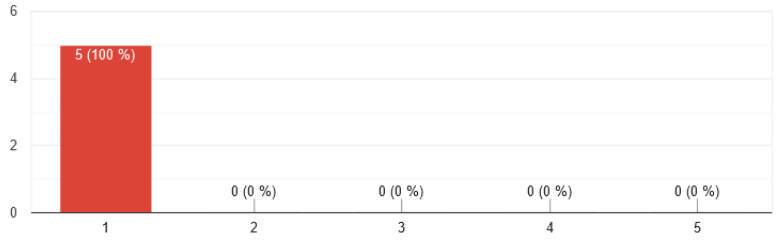
5 odpovědí



S pomocí příručky jsem neměl problém příklad 1 (Insider) zanalyzovat.

Kopírovat

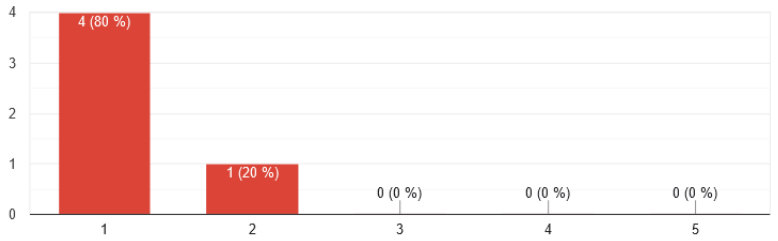
5 odpovědí



Zanalyzovat příklad 1 (Insider) bych zvládl i bez příručky.

Kopírovat

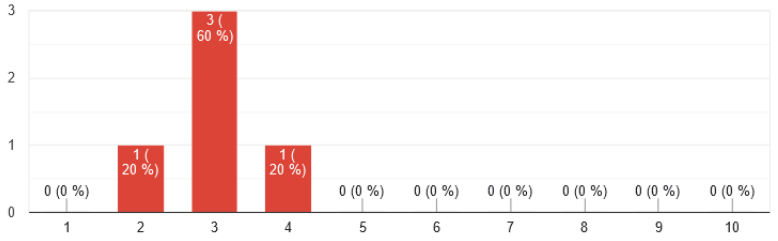
5 odpovědí



Na škále od 1 po 10 mi obtížnost analýzy příkladu 1 (Insider) přišla:

Kopírovat

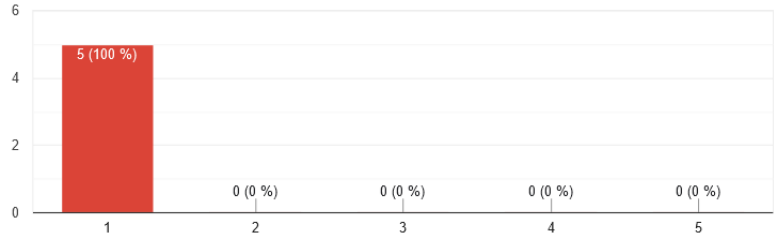
5 odpovědí



S pomocí příručky jsem neměl problém příklad 2 (Škodlivý kód) zanalyzovat.

Kopírovat

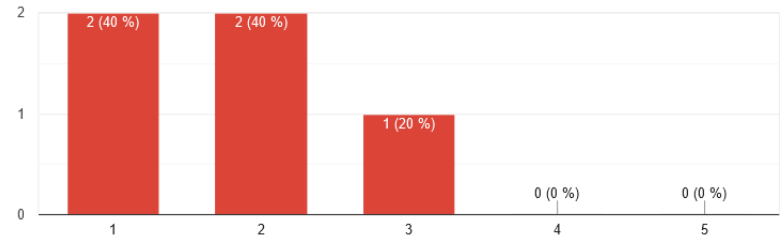
5 odpovědí



Zanalyzovat příklad 2 (Škodlivý kód) bych zvládl i bez příručky.

Kopírovat

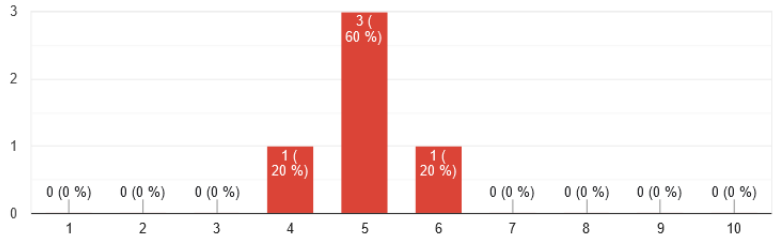
5 odpovědí



Na škále od 1 po 10 mi obtížnost analýzy příkladu 2 (Škodlivý kód) přišla:

Kopírovat

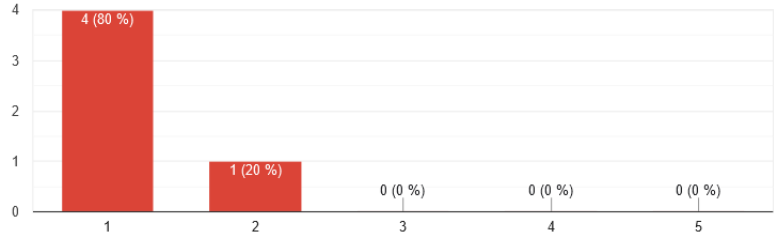
5 odpovědí



S pomocí příručky jsem neměl problém příklad 3 (APT) zanalyzovat.

Kopírovat

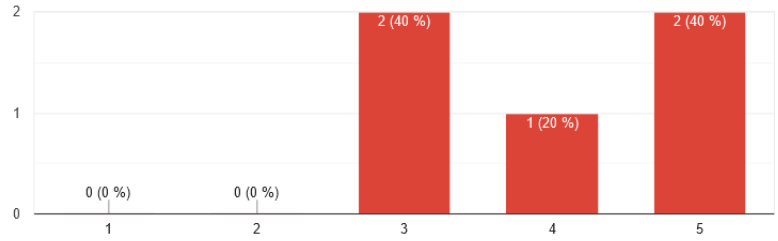
5 odpovědí



Zanalyzovat příklad 3 (APT) bych zvládl i bez příručky

Kopírovat

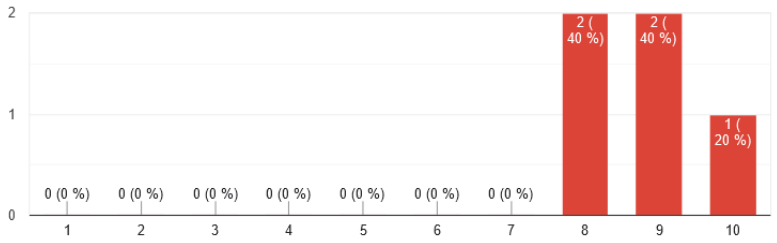
5 odpovědí



Na škále od 1 po 10 mi obtížnost analýzy příkladu 3 (APT) přišla:

Kopírovat

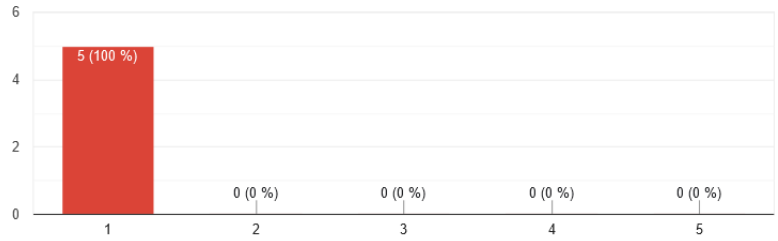
5 odpovědí



Neměl jsem problém s pochopením jednotlivých kroků v příručce.

Kopírovat

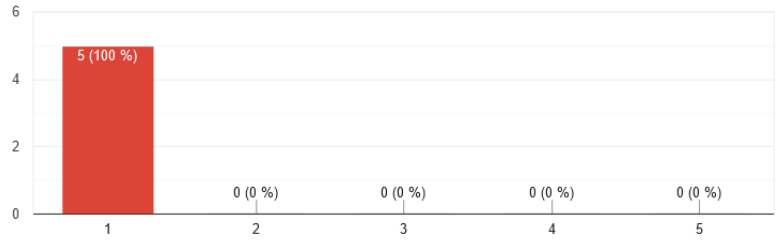
5 odpovědí



Příručka mi přišla intuitivní.

Kopírovat

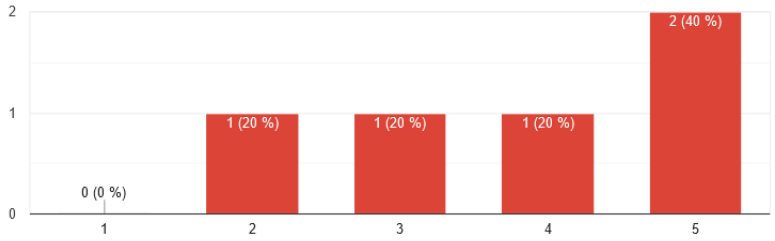
5 odpovědí



Postupy mi přišly zbytečně podrobné.

Kopírovat

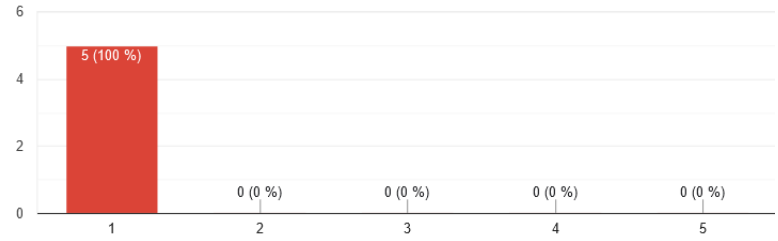
5 odpovědí



Úvody příkladů mě snadno vtáhly do analýzy.

Kopírovat

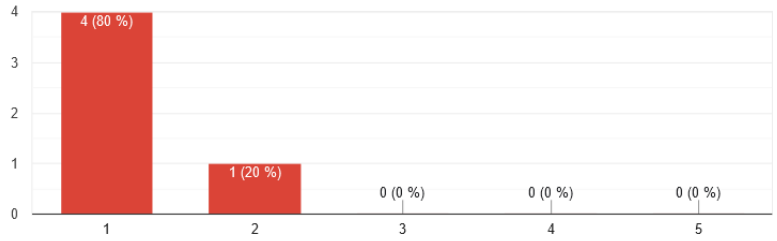
5 odpovědí



Scenáře jednotlivých příkladů mi přijdou reálné.

Kopírovat

5 odpovědí



Otevřená odpověď: Prostor pro vlastní komentář; Bylo zde něco, co se ti líbilo a chceš to zmínit? Doplnil bys příručku o další informace? Něco zde chybělo nebo přebývalo?

4 odpovědi

mam zkusenost s forenzkou, ale ne s forenzkou cloudu. u posledniho prikladu toho bylo dost co hledat a spousta logu, hodil by se tu siem nejakej... v prirucce mi nic podstatneho nechybelo. libilo se mi, ze byli popsany i use-cases z zivyho cloudu, skoda ze to neslo zkouset ve virtualce.

Dobrá příručka. Příklad s apt bych dost složitej.

Bolo to izi, izi, až to izi nakonec nebolo. Príručka sa hodila, neviem ako by som bez nej analyzoval trojku. A tie logy z googlu sú otrasné, fakt.

Jednička byla dost izi, dvojka byla dobře zvolená a trojka byla... Zajímavé zpestření. Jestli bych ji dal bez příručky, to nevim. Asi kdyby tam bylo víc k tomu, co útočník udělal, ale když to nevim a hledám vlastně jestli vůbec něco najdu, tak to je složitý no. :D hlavně když tam bylo tolik záznamů. Jinak super, příklady pobavili.