1. Organizace dokumentu

V tomto dokumentu jsou popsány organizační a technická opatření přijatá Hybrid Company a.s. pro jednotlivé služby a produkty týkající se poskytovaných služeb a produktů

2. Zabezpečení jako priorita

Hybrid Company vyvíjí maximální úsilí k tomu, aby infrastruktura, služby a vlastní produkty, kterou společnost nabízí a provozuje byla maximálně bezpečná. Je to klíčové nejen pro nás a naše zákazníky, ale i pro stát. Bezpečnost našich služeb, a dostupnost, integritu a obnovitelnost zpracovávaných dat považujeme za důležitou prioritu a vysokou a přidanou hodnotu pro naše zákazníky.

Z našeho přístupu k bezpečnosti jako prioritě vychází bezpečnost infrastruktury a úložiště dat. Na to navazují cloudové ekosystémy poskytující výpočetní výkon a specializované služby advertního systému a HbbTV aplikací. Každá z těchto nadstavbových platforem disponuje dalšími úrovněmi ochrany. Z našeho pohledu se jedná o komplexní soubor opatření, kterému věnujeme mimořádnou pozornost. Zahrnuje fyzické, procesní a technologické prostředky.

3. Cloudová infrastruktura Hybrid Ads

Cloudová infrastruktura je využívána pro poskytování služeb s vyšší přidanou hodnotou, kde zákazník čerpá její benefity jen nepřímo, prostřednictvím jiné služby. Cloudová služba poskytuje systém pro reklamně orientovanou platformu Hybrid Ads.

3.1. Hybrid Ads Cloud Infrastructure

3.1.1. Přístup ke Cloudové infrastruktuře

Platforma Hybrid Ads Cloud Infrastructure je spravována interní skupinou poskytovatele a implementuje řadu omezení v přístupu k infrastruktuře. Přístup k infrastruktuře neobsahuje přístup k zákaznickým datům.

Mezi tato bezpečnostní opatření patří:

- Omezení přístupu na zaměstnance poskytovatele
- Přístup je omezen pouze z interních sítí poskytovatele
- Logování veškeré aktivity prováděné v rámci infrastruktury
- Monitoring infrastruktury prostřednictvím dohledových systémů poskytovatele

3.1.2. Přístup k datové struktuře

Přístup k datové struktuře platformy Hybrid Ads Cloud Infrastructure, včetně zákaznických dat, je možný pouze skrze infrastrukturu. Abychom zamezili přístupu k datovým strukturám platformy, implementovali jsme nad rámec výše uvedených omezení tato bezpečnostní opatření:

- Změny v přístupu k infrastruktuře je možné pouze po schválení administrátorem
- Aktivity administrátorů jsou logovány
- Prostředí je monitorováno

3.1.3. Řízení přístupu ke službám platformy

Přístup ke službám platformy slouží uživatelům platformy v jejím efektivním využívání. Pro řízení přístupu jsou implementovány nástroje řízení přístupu izolované pro tuto jedinou platformu.
Pro zajištění bezpečnosti při přístupu ke službám platformy jsou implementována tato opatření:

- Přístup je možný pouze z vyhrazených a schválených sítí
- Změna rozsahu přístupu je možná pouze po autorizaci administrátorem platformy
- Aktivity uživatelů jsou logovány
- Prostředí je monitorováno na virtuální úrovni za účelem bezpečného poskytování služby. Jedná se o monitoring technického stavu infrastruktury.

3.1.4. Kontrola přenosu dat

Platforma Hybrid Ads Cloud Infrastructure má implementováno sledování přenášených dat za účelem řízení kvality a bezpečnosti služby.
Tato opatření jsou:

- Využití šifrování pro přístup k řízení platformy
- Dohled infrastruktury
- Analýza přenosu dat při neočekávaném chování

3.1.5. Řízení dostupnosti

Platforma Hybrd Ads Cloud Infrastructure je vytvořena s cílem zajistit vysokou dostupnost provozovaných aplikací. K zajištění této dostupnosti jsou v rámci platformy implementována tato opatření:

- Redundance na úrovni kritických prvků infrastruktury
- Izolace jednotlivých částí infrastruktury vedoucí k minimalizaci tzv. lavinového afektu
- Využití redundantních prvků s využitím mechanismu Fail-Over mechanismu
- Dohled všech prvků infrastruktury
- Pravidelné vyhodnocování využívaných zdrojů a řízení změn rozsahu za účelem efektivního nakládání s prostředky
- Pravidelné vyhodnocování SLA jednotlivých služeb

3.1.6. Dohled

Platforma Hybrid Ads Cloud Infrastructure je na mnoha úrovních monitorována. Abychom zajistili znalost přesného stavu celé platformy, implementovali jsme tato pravidla pro monitoring:

- Provozní parametry platformy (např. dostupnost, výkonnost, disponibilní prostředky, síťové služby apod.) jsou v režimu 24x7 monitorovány online nástroji poskytovatele s okamžitým zobrazením stavu v rámci dohledového centra
- Monitoring je implementován na úrovních:
- Přenosové infrastruktury – stavu jednotlivých spojení v rámci infrastruktury, jejího využití a přehled o nenadálých situacích v rámci těchto spojení

4. Zabezpečení dat při přenosech v telekomunikační síti

Pro přenos dat, včetně zákaznických dat, využíváme veřejnou síť. Standardně veškerá komunikace v této síti je šifrována end to end řešením. Tento způsob přenosu dat lze, s ohledem na standardy na trhu, považovat za bezpečný . Veškeré zákaznické aplikace pro přenos dat po síti využít standardních šifrovacích end to end prostředků. V těchto případech je přístup generický a řešení probíhá dvěma způsoby. Jednak jsou klíče zpravovány poskytovatelem platformy. V případě end-to-end aplikací jsou případě jsou veškeré klíče spravovány ze strany zákazníka.
Šifrování přenosu je proces, kdy je celý provoz, včetně užitečného obsahu zpráv zašifrován na vstupu a rozšifrován na výstupu. V případě přenosu packetů, které jsou větší než MTU (maximum transmission unit) přenosové cesty dochází k fragmentaci, tj. rozdělení packetů na části, jejich přenosu a následnému spojení.

5. Ochrana před vnějšími vlivy

- Pro ochranu před vnějšími vlivy využíváme specializované nástroje pro ochranu webových aplikací a služeb. Tyto nástroje jsou volitelně rozšiřitelné a obsahují mimo jiné rozšíření pro dohled nad OWASP TOP 10, SOC2 atd. Dále umožňují inspekci, detekci a následnou reakci v případě ohrožení aplikací či služeb, a to vše v reálném čase.
- Pro zajištění dostupnosti služeb je infrastruktura Hybrid vybavena ochranou před DDoS útoky, která snižuje rizika spojená se zahlcením nevalidním provozem.
- Všechny síťové bezpečnostní prvky jsou nepřetržitě monitorovány zaměstnanci Hybrid Company v režimu 24x7..
- Klíčové prvky jsou v režimu vysoké dostupnosti (HA).

6. Detekce a správa incidentů zabezpečení informací

Společnost Hybrid Company a.s. disponuje interním týmem pro řešení bezpečnosti incidentů v rámci IT infrastruktury.

7. Správa účtů

7.1. Řízení a kontrola přístupu/ správa účtů

Přístup k zákaznickým datům je umožněn pouze osobám, které je potřebují k zajištění činností vyplívajících ze smlouvy, a to pouze v nezbytně nutném rozsahu (princip need to know). Přístupy k systémům (účtům) z nezabezpečeného prostředí jsou vždy kontrolovány a případě přenos dat je vždy šifrován. Dle zákona o kybernetické bezpečnosti máme implementovanou politiku hesel. Veškerá hesla pro všechny skupiny uživatelů systémů jsou šifrována použitím hash funkce. Veškeré systémy mají svého administrátora, který přiděluje uživatelské přístupy. Minimální požadavek na přístup do systémů je uživatelské jméno a heslo, některé systémy používají pro přihlášení model dvou faktorové autentifikace. Přihlašování do všech systémů probíhá přes zabezpečený protokol https.

7.2. Skupiny uživatelů:

- Administrátoři

Administrátoři služeb mají přístup pouze k vymezené skupině činností, přičemž je zachován princip oddělení rolí administrátora a auditora.
Přístup do systémů mají pověření pracovníci Hybrid Ads, nebo dodavatele, kterým je vygenerováno pro přístup uživatelské jméno a heslo. Veškeré aktivity těchto uživatelů v systémech jsou logovány a vyhodnocovány v souladu s interními pravidly.

- Zákazníci

Zákazníci obdrží přístup do systémů na základě podepsané smlouvy. Některé systémy umožňují zákazníkovi vytvářet další uživatele/role v systému. Platí stejná pravidla pro kontrolu a správu účtu a aktivit na těchto účtech prováděných.

- Koncoví uživatelé služeb

Účty jsou zřizovaný na základě registrace ve front-end aplikacích. Každý uživatel je autorizován pomocí jména a hesla. Heslo splňuje bezpečnostní standardy pro bezpečná hesla. Hesla jsou ukládána v databázi a zašifrována jednosměrnou šifrou. Používají se pouze šifry, které jsou v daném čase doporučené k používání Uživatelům je umožněna správa účtu, obnova účtu probíhá některou ze standardních autorizačních metod, například zasláním linku na asociovaný e-mail uživatele. Rozsah dat požadovaných pro vytvoření

účtu, je řízen podmínkami služby od zákazníků. Přístup a možnost vytvořit heslo dostane osoba uvedená na smlouvě služby. U vybraných služeb si může, pro zvýšení bezpečnosti přístupů, uživatel aktivovat dvou faktorovou autentizaci.

8. Zabezpečení subdodavatelů

Hybrid může najmout subdodavatele za účelem poskytování služeb jejím jménem. Tito subdodavatelé budou smět zákaznická data získat pouze za účelem poskytování služeb a zákaznické podpory, k jejichž poskytování se zavázali, a nebudou smět tato data používat za jakýmkoli jiným účelem. Hybrid zůstávají odpovědné za dodržování souladu s povinnostmi stanovenými v těchto podmínkách svými subdodavateli. Zákazník již dříve souhlasil s tím, že Hybrid smí přenést zákaznická data a údaje o podpoře k subdodavatelům podle popisu v těchto podmínkách.