PLNĚ ŠIFROVANÝ SMARTPHONE KAYMERA

ŠIFROVANÝ SMARTPHONE

ZAŘÍZENÍ PRO KONCOVÉHO UŽIVATELE JE ZALOŽENO NA SYSTÉMU KAYMERA OS, VYSOCE ZABEZPEČENÉM OPERAČNÍM SYSTÉMU, KTERÝ BYL VYTVOŘEN OD ZÁKLADU TAK, ABY MAXIMALIZOVAL OCHRANU ZAŘÍZENÍ PŘI ZACHOVÁNÍ POUŽITELNOSTI, JAKÉ POSKYTUJE PLATFORMA ANDROID.

[OCHRANA ZAŘÍZENÍ]

Zařízení je chráněno proti všem bezpečnostním hrozbám:

- Síťová intercepce - veškerá hlasová, SMS a internetová komunikace
- WiFi: před odposlechem, manipulací s daty a infekcí
- SS#7 útoky – před taktickými a signalizačními manipulacemi operátora
- Stažení dat – před extrakcí dat při fyzickém přístupu k zařízení

Trojské koně (APT) a malware útoky: politika plné kontroly oprávnění zabezpečeným OS. Poskytuje ochranu před následujícími hrozbami:

- Man-in-the middle: útoky třetích strann
- Phishing a sociální inženýrství
- Ransomware
- Ochrana před monitoringem kamery a mikrofonu

Detekce nebezpečí:

Pokud je na zařízení veden útok nebo se nachází v rizikovém prostředí, systém okamžitě na hrozbu upozorní uživatele a navrhne obranné opatření. Možnost integrace se systémy SOC a SIEM prostřednictvím Kaymera API.

VLASTNOSTI A VÝHODY

- Oboustranně šifrované hovory
- Šifrované hovory na ostatní volaná čísla
- Šifrované konferenční hovory (maximálně 12)
- Šifrovaný skupinový chat
- Šifrovaný přenos souborů
- Autodestruktivní zprávy

Použitelnost:

Operační systém Kaymera je dostupný pro celou řadu high-end telefonů Google Pixel.
Prostředím je operační systém Kaymera pro uživatele použitelný stejně jako jiné telefony na platformě Android OS.
Hlavními přednostmi Kaymera OS jsou:

- Prostředí shodné s Android včetně aplikací z PlayStore
- Bez předinstalovaného reklamního Bloatware
- Update na nejnovější verzi Over-the-Air (OTA) od společnosti Kaymera Technologies
- Bezpečnostní aplikace Kaymera – telefon, zprávy, detektor bezpečnostních rizik

[KONZOLE CENTRALIZOVANÉ SPRÁVY ZABEZPEČENÍ KAYMERA]

Centralizované řídicí centrum společnosti Kaymera umožňuje manažerům IT a bezpečnostním manažerům mít úplnou kontrolu nad mobilním prostředím koncových uživatelů pro účely mobilního zabezpečení.

Mezi hlavní funkce patří:

- Konzole pro správu systému s podporou více oprávnění
- Úplné monitorování sítě a správa zařízení
- Prosazování zásad rizik organizace na úrovni zařízení, skupiny a organizace
- Sledování úrovně rizika v reálném čase
- Centralizovaný dohled a řízení
- Pokročilý systém generování reportů
- Bezpečná správa aktualizací operačního systému (OTA)
- Monitoring rizikových činností zařízení a stav u jejich zabezpečení
- Možnost dálkového vymazání zařízení
- VPN – blacklist aplikací
- Výstrahy na bezpečnostní rizika zařízení a nouzová hlášení

[TECHNICKÁ SPECIFIKACE]

PŘEDMĚT ZABEZPEČENÍ	POPIS
ZABEZPEČENÉ ZAŘÍZENÍ	• High-endový Android smartphone, vylepšený na vysoký bezpečnostní standard Systému Kaymera. • Veškerá data jsou uložena v šifrovaném úložišti. • Ochrana před stažením dat při fyzickém přístup k zařízení. • Bezpečné vymazání zařízení na dálku. • Uzamčení zařízení na dálku.
ZABEZPEČENÁ KOMUNIKACE	• Silně šifrované hovory ve vysoké kvalitě. • Integrovaná šifrovaná komunikace: textové zprávy, posílání souborových příloh a časově omezené autodestruktivní zprávy. • Permanentně zapnutá VPN. • Systém šifrovacích klíčů v hardwarově chráněné klíčence. • Robustní šifrovací prostředí na úrovni 2048-bit RSA a AES 256-bitovými symetrickými klíči PKI.
ZABEZPEČENÝ OPERAČNÍ SYSTÉM	• Robustní jádro Kaymera o čtyřech vrstvách: šifrování, ochrana, prevence, detekce. • Kontrola všech systémových procesů umožňuje prevenci úniku a zneužití dat. • Odolnost vůči pokročilým hrozbám a malwaru.
SYSTÉM PRO SPRÁVU ZAŘÍZENÍ	• Systém centralizované správy zabezpečení zařízení. • Správa a vynucení oprávnění aplikací, bezpečnostních protokolů a politik na úrovni podniku, skupin i jednotlivých zařízení. • Monitoring hrozeb a aktivit zařízení prostřednictvím centralizovaného rozhraní. • Vyhodnocování úrovně rizik v reálném čase a nasazení protiopatření.
OSOBNÍ BEZPEČNOST	• Senzory monitorující a varující v reálném čase pokusy o průnik a útoky typu Man-in the-middle. • Systém tísňového hlášení při fyzickém ohrožení.

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10, Praha
TEL: + 420 222 271 111
FAX: + 420 222 271 112
E-MAIL: marketing@i.cz