COMGUARD

air/bank
ČLEN SKUPINY PPF

PŘÍPADOVÁ STUDIE

> Air Bank a.s. má díky ThreatGuard jednoduše přístupné informace o aktuálních hrozbách.

- jasné, ucelené informace a možné dopady hrozeb
- upozornění na hrozby dle aktiv nasazených v infrastruktuře
- úspora kapacit o cca 2 – 3 MD měsíčně

Air Bank a.s. má díky **ThreatGuard** jednoduše přístupné informace o aktuálních hrozbách.

Společnost **COMGUARD, a.s.** má z pohledu **specialisty IT bezpečnosti** detailní přehled o dlouhodobých problémech v dané oblasti, kterým čelí společnosti napříč všemi sektory.

K nejvýznamnějším z těchto problémů můžeme zařadit těžkou **dohledatelnost** a nestrukturovanost informací o aktuálních **IT hrozbách** relevantních pro zákazníkovu **IT infrastrukturu**.

Jedna z **předních** společností z bankovního sektoru, **Air Bank a.s.**, tuto problematiku dlouhodobě řešila, protože potřebovala předejít **incidentům v IT infrastruktuře**, které mohou zapříčinit neplánované odstávky služeb.

Vznikla zde potřeba mít k dispozici co nejdetailnější informace o **aktuálních IT hrozbách**, a tak splnit nastavené **bezpečnostní standardy**.

Ověření konceptu

Naše společnost **COMGUARD a.s.** představila zákazníkovi službu **ThreatGuard**. Zákazníka služba **zaujala** a měl zájem o její testování.

Společnost **Air Bank** službu **ThreaGuard** testovala v časovém úseku **dvou týdnů**, kdy tuto expertní službu zhodnotila jako **přínosnou**. Díky ní získala k dispozici **tým analytiků**, který **vyhledával a vyhodnocoval aktuální a relevantní IT hrozby**, jež evidoval na jednom místě.

Výchozí situace

Společnost **Air Bank a.s.** využívala aktuální informace z interních systémů a veřejně dostupných zdrojů, mezi nimiž byly **sociální sítě, webové stránky** zabývající se touto problematikou, **CSIRT týmy, weby** výrobců z oblasti IT security apod.

Na kontrolu těchto zdrojů byly dedikovány interní kapacity **Air Bank**.

Pravidelně byly procházeny jednotlivé zdroje a probíhala kontrola, zdali jsou relevantní pro infrastrukturu společnosti.

Následně byly **nalezené hrozby vyhodnoceny** a s ohledem na jejich závažnost byla dohledána opatření nebo řešení, jak **hrozbám předejít či jak snížit riziko**.

Takto sumarizované hrozby byly postoupeny do procesu **patch managementu**.

ThreatGuard

V rámci testování zákazník ocenil především **funkce portálu ThreatGuard:**

- Aktivní **filtry** umožňují zobrazit pouze hrozby týkající **se aktiv nasazených v IT infrastruktuře** zákazníka.
- **Customizované notifikace** informují **jednoduchým a efektivním způsobem** prostřednictvím **e-mailu o IT hrozbách** vycházejících z nastavení **aktivního filtru**.

COMGUARD

air/bank
ČLEN SKUPINY PPF

PŘÍPADOVÁ STUDIE

> **Díky ThreadGuard má bezpečnostní tým přesné informace o relevantních hrozbách.**

> **Tým analytiků ThreatGuard zachytil důležité informace o IT hrozbách.**

Implementace a aktuální stav

Implementace celého řešení byla **jednoduchá**, jelikož se jedná pouze o **zřízení přístupu pro vybrané** pracovníky společnosti k **webovému portálu**.

V něm mají tito pracovníci k dispozici všechny informace o **IT hrozbách, které zachytil tým analytiků ThreatGuard.**

Portál byl **přizpůsoben** potřebám zákazníka tak, aby zobrazoval pouze informace, které jsou pro něj **relevantní**.

Díky **ThreatGuard** má zákazník k dispozici **preventivní nástroj**, který ho informuje o aktuálních **IT hrozbách** a pomáhá mu předejít případným incidentům a tím usnadňuje **analýzu dopadů** a **zrychluje proces rozhodování**.

Tato služba zákazníkovi pomohla **zpřesnit a zrychlit** proces **vyhodnocování** dopadů **konkrétních hrozeb.**

Současně **ThreatGuard** poskytuje **návrh preventivních opatření** pro dané **hrozby**.

> **Díky ThreatGuard má náš bezpečnostní tým přesnější informace o relevantních hrozbách a je na ně schopen efektivněji reagovat.**
>
> **V důsledku se nám také uvolnily kapacity pro další aktivity v oblasti IT bezpečnosti.**
>
> **Josef Mačica, manažer informačních technologií**