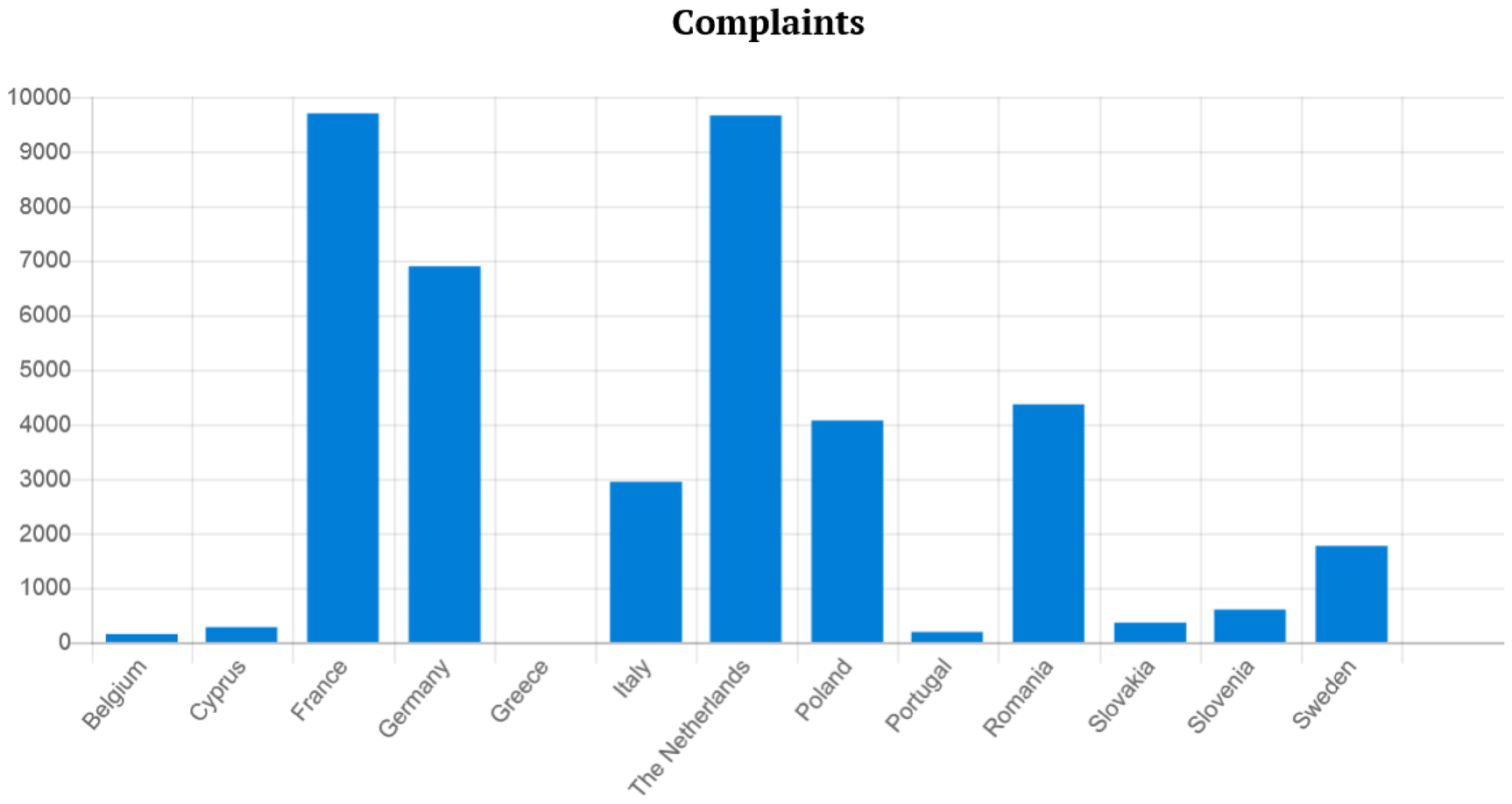
DATALAN

Bezpečnosť citlivých dát

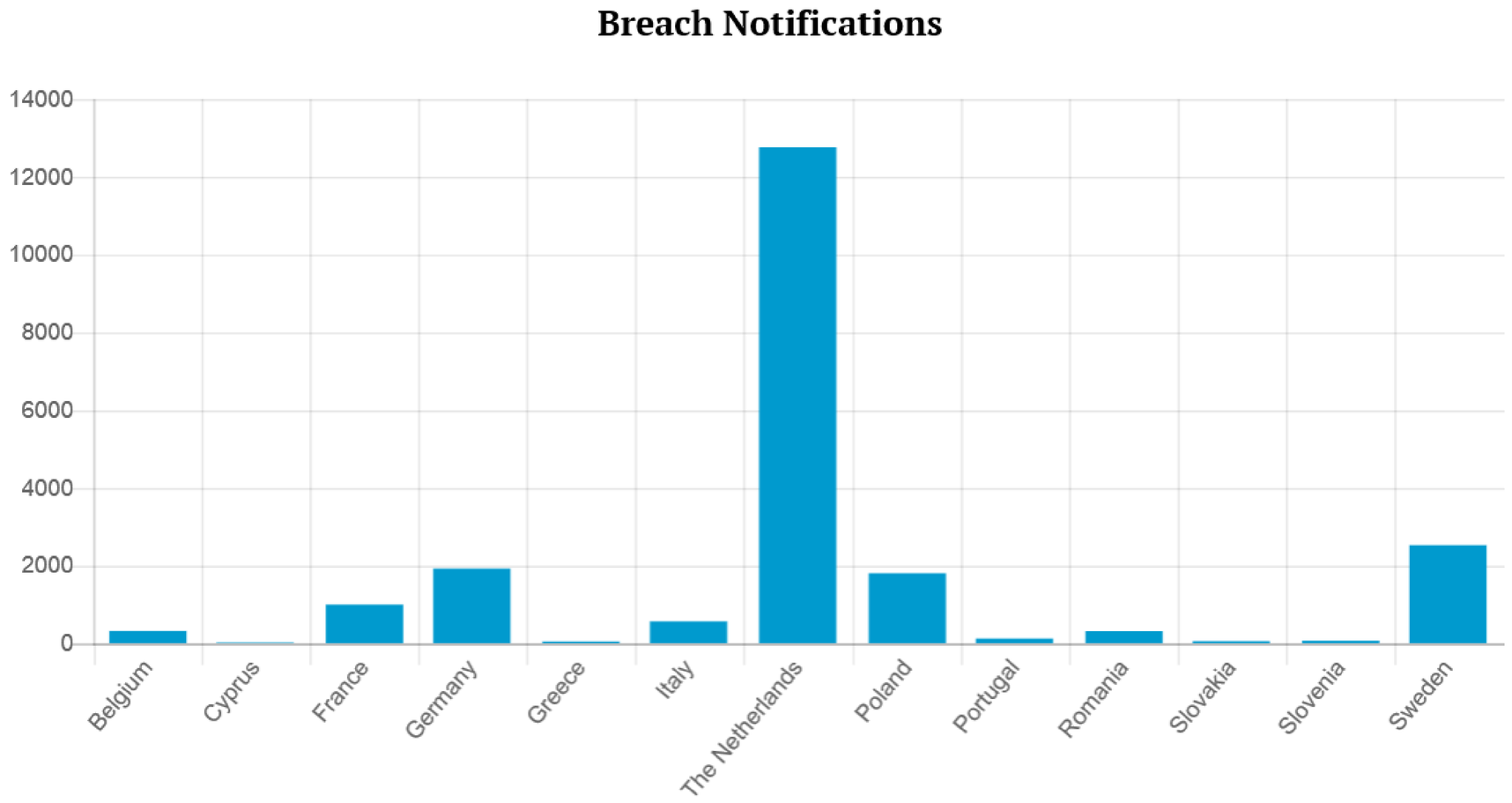
GDPR v číslach

- Celkový počet sťažností na ochranu osobných údajov v EU za 8 mesiacov - **95 180**



GDPR v číslach

- Celkový počet nahlásených únikov osobných údajov v EU za 8 mesiacov - **41 502**



DATALAN

GDPR v číslach

- Najvyššia pokuta – Francúzsky úrad pre ochranu údajov udelil firme Google kvôli nedostatočne a nejasne informuje používateľov o spracovaní ich osobných údajov a nezískal pritom ani ich súhlas s personalizovanými reklamami.

50 000 000 EUR

https://www.gdprtoday.org/gdpr-in-numbers/

- V Čechách pokuta (58 000 eur) pre Internet Mall, a.s.

https://www.finance.sk/182771-padli-prve-pokuty-za-gdpr/

- Pokuty pre nemocnicu v Portugalsku – 400 000EUR - 985 registrovaných profilov v rámci IT systému, pričom iba 296 z nich boli profily lekárov

https://www.semancin.sk/novinky/portugalska-nemocnica-dostala-hned-dve-pokuty-za-vazne-porusenie-gdpr-400-000-eur/

Kde sú naše údaje?

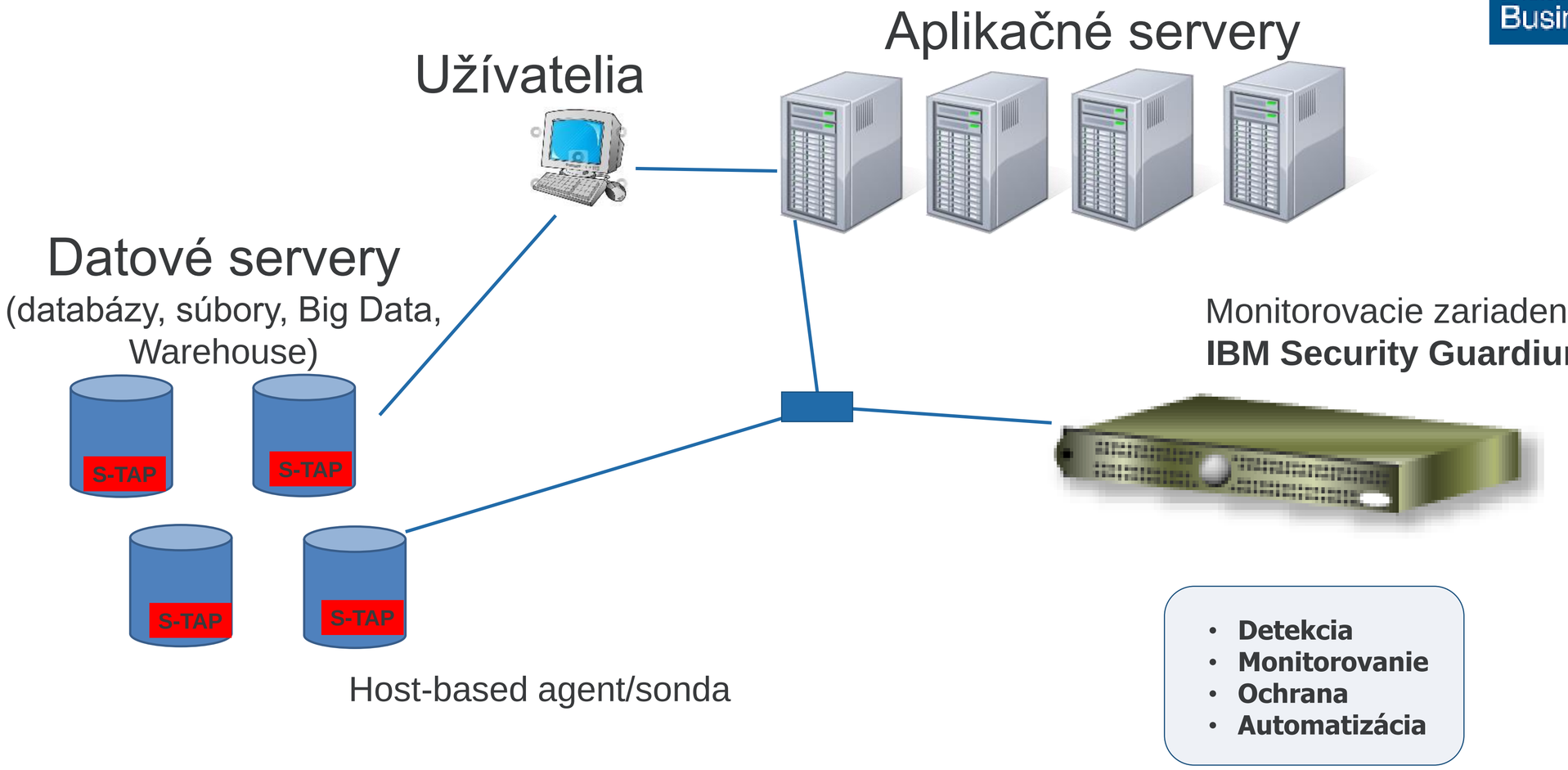
- Databázy
- BigData
- Súborové servery, NAS, Sharepoint ...
- Cloud

Kto pristupuje k našim údajom?

- štandardní užívatelia: zamestnanci
- 3-tie strany (dodávatelia)
- Privilegovaní užívatelia
- ???

RIEŠENIE = IBM Security Guardium

Architektúra riešenia



- **Detekcia**
- **Monitorovanie**
- **Ochrana**
- **Automatizácia**

RIEŠENIE = IBM Security GUARDIUM

1. Klasifikácia citlivých dát a užívateľov
2. Skenovanie zraniteľností databáz
3. Monitorovanie prístupu k údajom
4. Obmedzenie prístupu
5. Analýza aktivity nad údajmi
6. Integrácia s už existujúcimi bezpečnostnými riešeniami v prostredí zákazníka
   - SIEM (Security Information and Event Management)
   - F5 – aplikačný firewall
   - ...

Výhody

Požiadavky na cieľový stav

- Súlad so štandardmi (GDPR, SOX, PCI, NIST, STIG…)
- Minimálny zásah do konfigurácie databázových serverov
- Minimálny vplyv na výkonnosť databázavých serverov
- Integrácie s existujúcimi bezpečnostnými riešeniami
- Škálovateľnosť

PRÍNOSY

Prínosy riešenia

- Výrazné zvýšenie bezpečnosti firemných dát.
- Centralizované monitorovanie a auditovanie prístupu k dátam uložených v databázach alebo v súboroch
- Automatizovanú klasifikáciu citlivých dát
- Definovanie pravidiel a politík prístupu k citlivým dátam
- Blokovanie neautorizovaného i podozrivého prístupu k dátam
- Nezávislosť ochrany dát od administrátorov a privilegovaných užívateľov
- Monitorovanie a audit 100% dátových operácií
- Detekciu zraniteľností dátových zdrojov ako sú databázy
- Súčasť zabezpečenia súladu s legislatívou na ochranu osobných údajov, ktorý vyžaduje monitorovanie aktivít nad osobnými údajmi ako napr. GDPR,

ĎAKUJEM