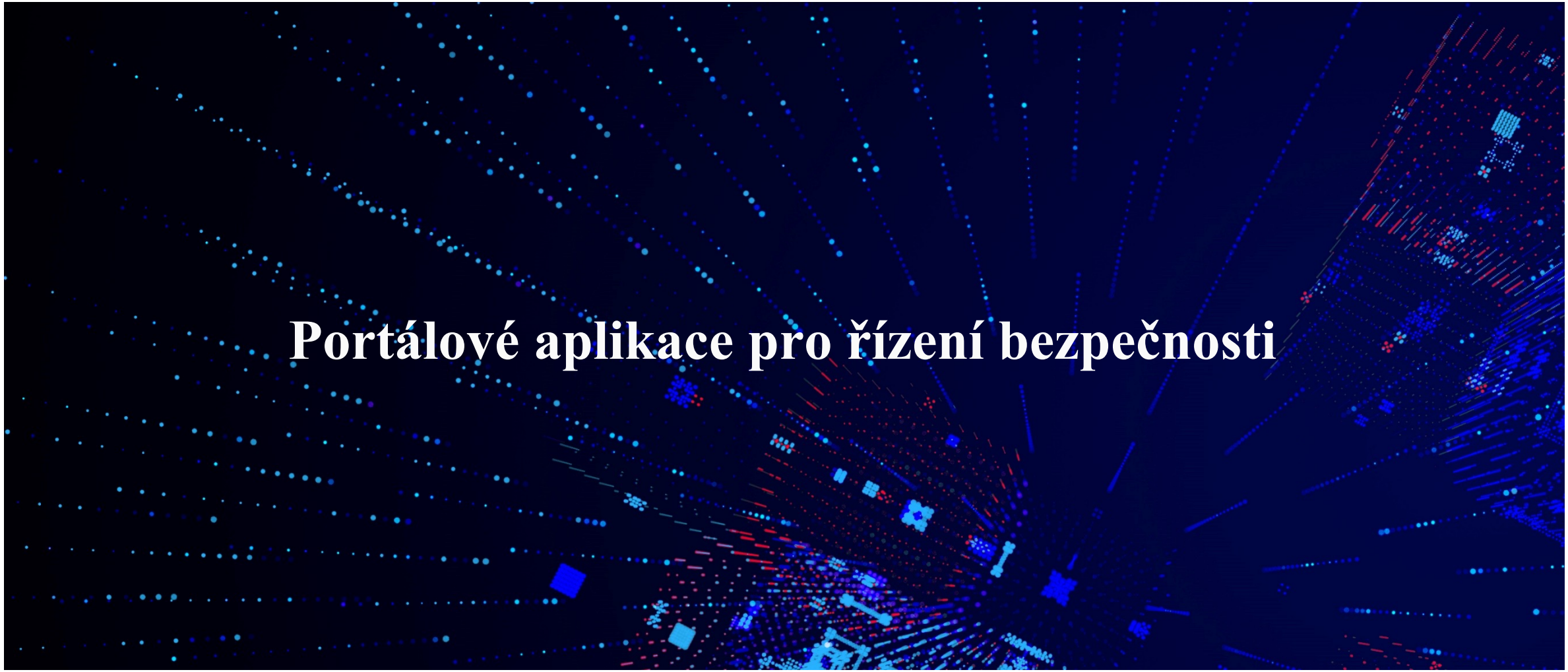
GORDIC

Bezpečnost portálových řešení

Kamil Virág

GORDIC



Portálové aplikace pro řízení bezpečnosti

GDA

řízení ochrany osobních údajů (GDPR)

online dokumentace, datová kostka, zpracování OÚ, auditní log

GDPO

řízení bezpečnostních událostí a incidentů

plnění práv subjektu údajů (GDPR), online evidence žádostí
řízení bezpečnostínch událostí (ZoKb)
řízení vzdělávání a prokazatelné seznámení zaměstnanců

PDIL

audit osobních údajů

obecné (i konkrétní) vyhledání výskytu osobních údajů
anonymizace dokumentů, podpora OCR

CSA

analýza a řízení aktiv v organizaci

kompletní správa kybernetické bezpečnosti, řízení aktiv dle ZoKb

CSA


Evidence aktiv
CSA
Identifikace zranitelností a hrozeb
Bezpečnostní audit
Analýza rizik

GORDIC

Portálové aplikace usnadňující život občanům


Portál
občana
Osobní
portál

GORDIC

Úskalí bezpečného návrhu

Úskalí bezpečného návrhu

- Bezpečně vyvíjená aplikace
  - Vývojový tým má KnowHow jak využívat programovací jazyk
  - Testování aplikace během vývoje
  - Testování aplikace v testovací IT infrastruktuře
  - Pravidelné aktualizace knihoven vývojového jazyka

Úskalí bezpečného návrhu

- Provozní implementace v IT infrastruktuře
  - Cloud – poskytování služby
  - On-premis - Implementace v IT infrastruktuře zákazníka

Úskalí bezpečného návrhu

- Cloud implementace
  - Smluvní vztah s poskytovatelem
    - Výběr služeb (služba, storage, DBs, webový server, reverzní proxy)
    - Specifikace služby (PaaS, IaaS, SaaS, …)
    - Definovaný perimetr zodpovědnosti
    - Rozdělení rolí
  - Aktualizace
  - Penetrační test

Úskalí bezpečného návrhu

- On-premis - Implementace v IT infrastruktuře zákazníka
  - Smluvní vztah se zákazníkem
    - Definovaný perimetr zodpovědnosti
    - Rozdělení rolí
  - Implementace aplikace
    - DMZ – (typy DMZ) FrontEnd aplikace + webový server
    - Intranet – BackEnd aplikace, DBs, souborové úložiště
  - Aktualizace
  - Penetrační test implementace
  - Penetrační retest

Vývoj aplikací GORDIC – kybernetická bezpečnost

Aplikace, které Poskytovatel (Realizátor) vyvíjí, ve většině případů zavádí nové bezpečnostní dopady. Již při vývoji se dbá na bezpečnost procesů v životním cyklu softwaru. Bezpečnost na procesním přístupu k zadávání, navrhování, vývoji, testování, zavádění a udržování bezpečnostních funkcí a kontrol v aplikačních systémech je nezbytná pro tvorbu bezpečných aplikací.

Bezpečně vyvíjená aplikace navíc bere v úvahu bezpečnostní požadavky, které vyplývají z typu dat, cílového prostředí (kontext činnosti organizace, regulatorní a technologické kontexty), aktivních účastníků a specifikací aplikace a poskytuje důkaz prokazující dosažení přijatelné (nebo tolerovatelné) úrovně zbytkového rizika a udržování této úrovně.

Vývoj aplikací GORDIC – kybez, legislativa

Problematika kybernetické bezpečnosti vychází z právních předpisů ZoKB, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27034, GDPR.

Potřeby řízení bezpečnosti informací vychází z ustanovení ZoKB, jeho prováděcích předpisů a dalších zákonů č. 106/1999 v platném znění, č. 365/2000 (ve změně č. 104/2017 Sb.) v platném znění a č. 240/2000 v platném znění.

Poskytovatel, jako tvůrce software vychází z toho, že prováděcí předpisy ZoKB nahrazují celý oddíl bezpečnosti na straně ZoISVS na informační systémy veřejné správy (dále jen „ISVS“). Z hlediska řízení životního cyklu IS dle ISVS pak je nutno respektovat proběhy lhůt a periodicitu úkonů vyplývající z předešlého a zahrnovat výstupy části bezpečnostní.

Vývoj aplikací GORDIC – kybez VIS KIS

Poskytovatel je tvůrcem programového vybavení, který je u Odběratelů v řadě případů klasifikován jako významný informační systém, v některých případech provozován také na kritické informační infrastruktuře. Zajištění shody s požadavky stanovenými zákonem č. 181/2014 Sb. (aktualizovaný zákonem 205/2017 Sb. ve znění zákona 104/2017 Sb.), o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), vše ve znění pozdějších předpisů, je tedy pro tvůrce software samozřejmostí.

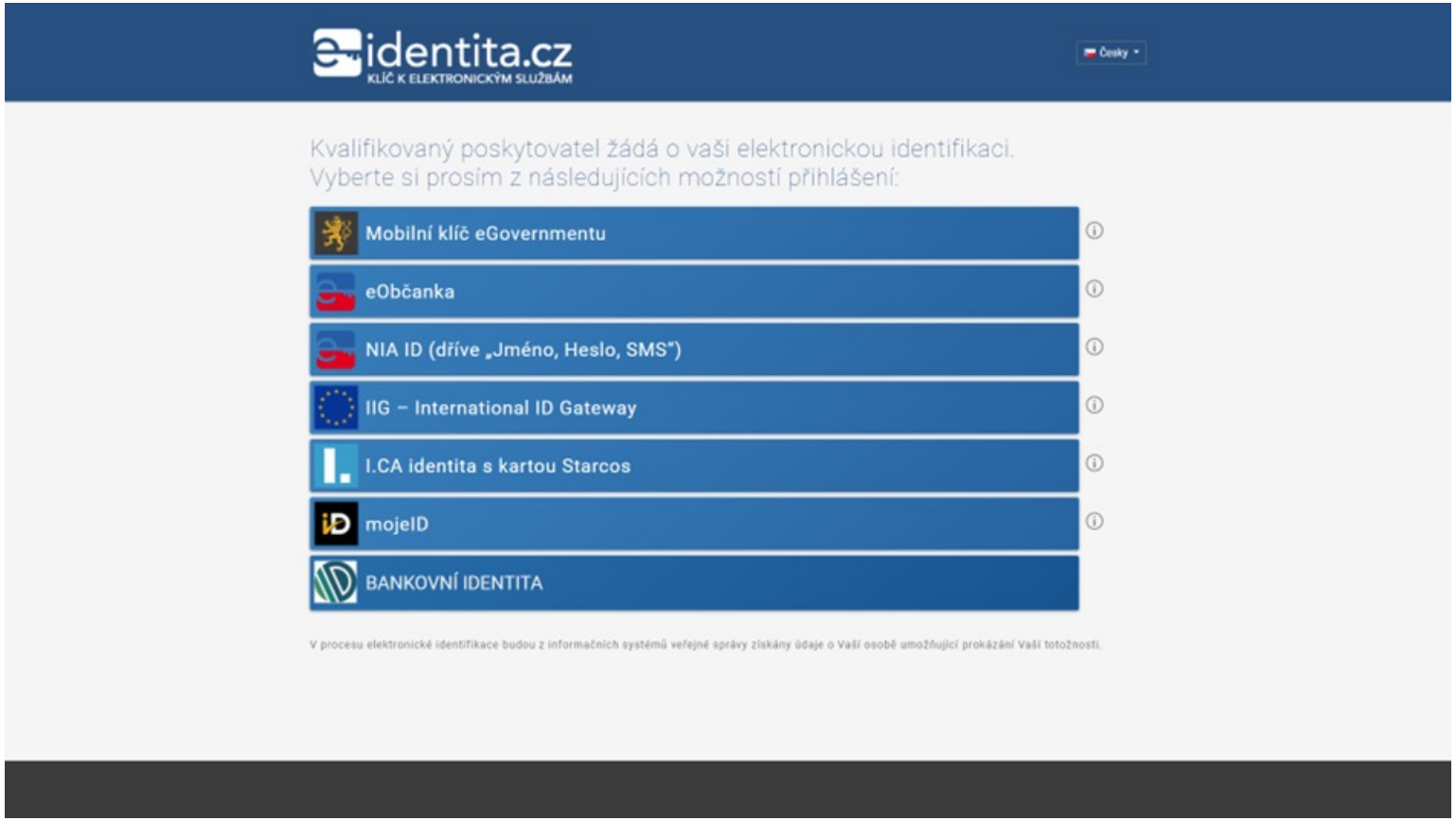
Portálová řešení

Portálové aplikace (veřejná služba) jsou implementovány jako součást aplikačního systému lehkého klienta GINIS Standard, instalovaného na IT infrastruktuře zákazníka.

Kybernetická bezpečnost je v těchto aplikacích řešena v rámci aplikačního systému GINIS. Jsou tedy aplikována veškerá pravidla a bezpečnostní politiky, kterými Ginis disponuje a splňuje tím zákonné povinnosti ve smyslu platné legislativy ČR viz výše.

Portálová řešení – bezpečnostní prvky

- Portál občana - Bezpečné ověření registrovaného uživatele



Portál občana – bezpečnostní prvky

(Zákon č. 181/2014 o kybernetické bezpečnosti, Vyhláška č. 82/2018 Sb.)

- Platební brány
  - GPwebpay, GoPay, PayU, ČSOB
- Informační systém datových schránek (ISDS)
  - odesílání formulářů z DS uživatele
- Přímé propojení do GINIS POD, GINIS VFP, GINIS DDP, GINIS BUC, GINIS SSL
- Gordic.Browser.Extensions (GBE)
  - pro elektronické podepisování odesílaných formulářů

Portál občana – implementace

(Zákon č. 181/2014 o kybernetické bezpečnosti, Vyhláška č. 82/2018 Sb.)

- Portál občana neprovozuje vlastní databázi
- Na webovém serveru a ani v prostředí klienta, se neukládají žádná zpracovávaná data
- Webový server poskytuje klientovi pouze prázdné formulářové šablony
  - po vyplnění klientem jsou data odeslána přímo do centrální databáze aplikačního systému GINIS
- Komunikační prostředí portálu občana
  - webový prohlížeč – webový server (front end) je striktně odděleno od datového úložiště (back end)
- Ochrana relace přihlášeného klienta do Portálu občana
  - zajištěna automatickým uzamčením respektive odhlášením relace od serveru po vypršení nastaveného času v případě nečinnosti klienta

Portál občana – implementace

(Zákon č. 181/2014 o kybernetické bezpečnosti, Vyhláška č. 82/2018 Sb.)

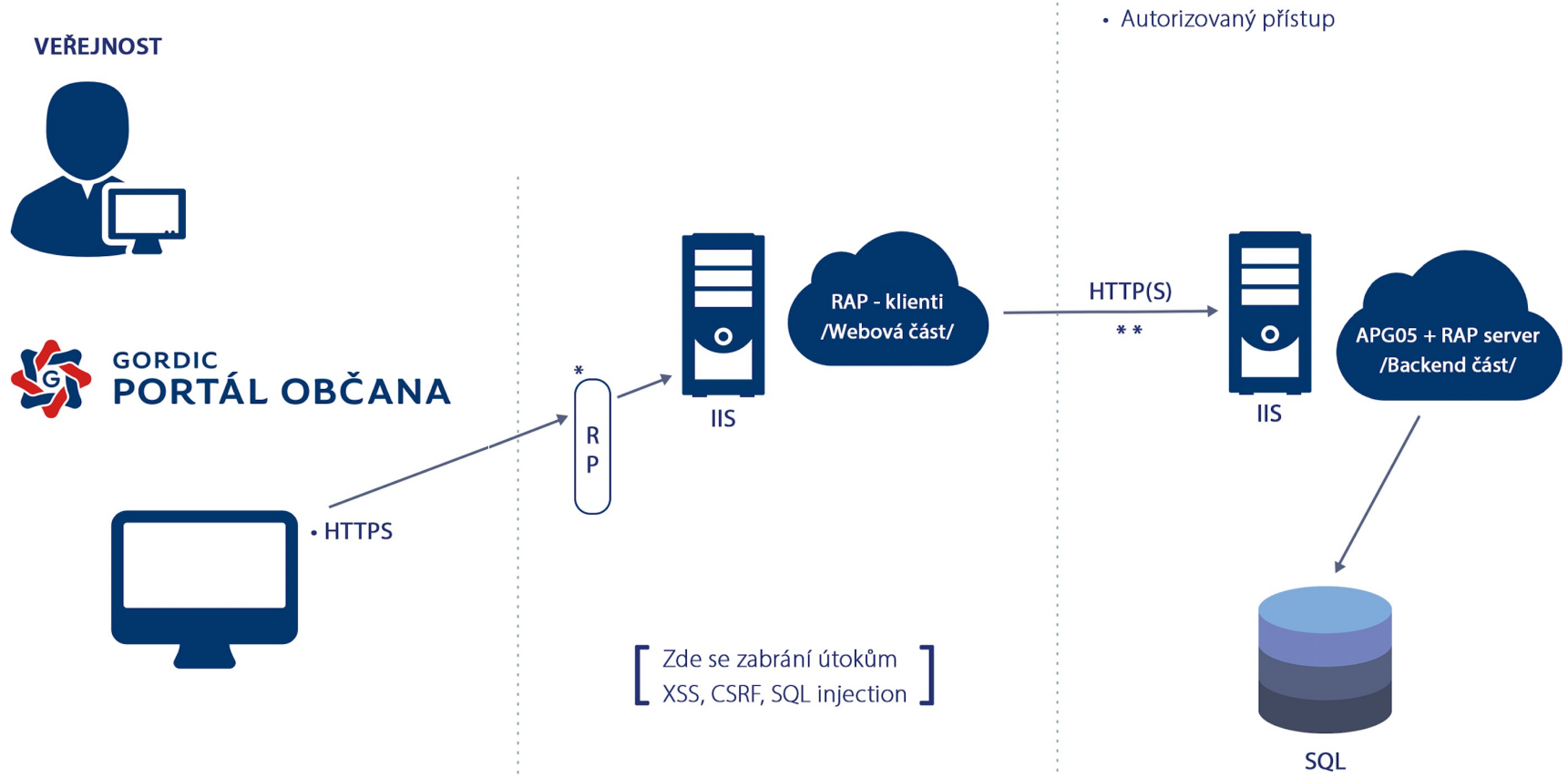
- FrontEnd – DMZ *(reverzní proxy)*
  - Webový server, RAP aplikace, přístup HTTPS, komunikace Identita občana, platební brána – SSL/TLS, timeout relace
- BackEnd – Intranet
  - Databázový systém GINIS, SQL propojení šifrované

Portál občana – implementace APG

(Zákon č. 181/2014 o kybernetické bezpečnosti, Vyhláška č. 82/2018 Sb.)

- FrontEnd – DMZ *(reverzní proxy)*
  - Webový server, RAP klient *(webová část),* přístup HTTPS, komunikace Identita občana, platební brána – SSL/TLS, timeout relace
- BackEnd – Intranet
  - Modul APG je součástí bezpečnostní infrastruktury portfolia GINIS
    - Vstupuje do komunikace mezi modulem RAP a databází. Zamezuje potencionálnímu útočníkovi přímému přístupu do databáze. Funguje na principu webových služeb.
    - Tato úroveň zabezpečení výrazným způsobem znesnadňuje útočníkovi:
      - Převzetí přístupových oprávnění
      - Odcizení databáze
      - Podvrh identity
  - RAP server
  - Databázový systém GINIS

Vyšší stupeň bezpečného návrhu



Portálová řešení

- Bezpečně vyvíjená aplikace
  - Vývojový tým má KnowHow jak využívat programovací jazyk
  - Součástí vývojového týmu je bezpečnostní tým
  - Testování aplikace během vývoje
  - Testování aplikace v testovací IT infrastruktuře
  - Pravidelné aktualizace knihoven vývojového jazyka
- Penetrační testování

Portálová řešení - PenTesty

- Penetrační testování
  - FrontEnd – webové stránky uživatelského rozhraní portálu jsou pravidelně testovány proti známým útokům dle doporučení OWASP TOP 10.
    - Zejména SQL Injection, Cross Site Scripting XSS, Broken Authentication, Broken Access Control, Sensitive Data Exposure, apod.
  - Penetrační test aplikace v testovací IT infrastruktuře
  - Penetrační test implementace v IT infrastructure zákazníka
    - OWASP TOP 10, Buffer overflow, případně zátěžové DoS testování aplikace
  - Penetrační retest implementace v IT infrastructure zákazníka
    - Cílem reTestu je nejen ověření nápravy původních nálezů, ale také kompletní přetestování s případným nalezením co nejvíce nových a aktuálních nálezů a problémů týkajících se bezpečnosti webové aplikace

Úskalí bezpečného návrhu

Vzhled aplikace

Zabezpečení aplikace

Podpora a osvěta kybernetické bezpečnosti

- KYBEZ – Platforma kybernetické bezpečnosti
  - www.kybez.cz
- Iniciativa KYBEZ
  - www.iniciativakybez.cz

Analýza kybernetické bezpečnosti a GDPR ZDARMA a online

Víte…, **www.kybez.cz/bean**

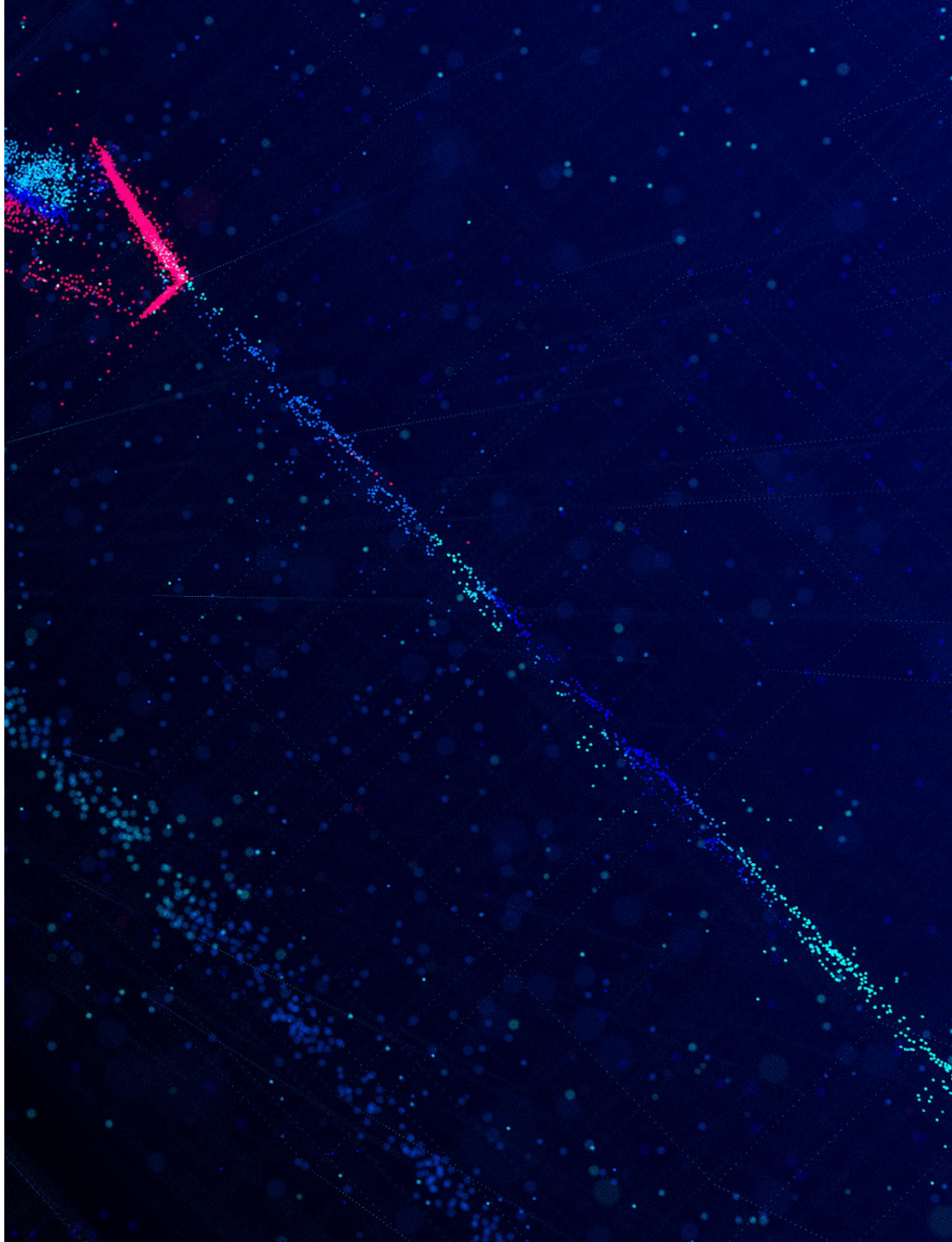
jaké sektory jsou z hlediska KYBEZ nejzranitelnější? Jak jste na tom Vy?

GORDIC

Realizovaný projekt u zákazníka

Děkuji za pozornost.

- Kamil Virág
- kamil_virag@gordic.cz
- +420 724 031 682



GORDIC