KYBEZ Platforma kybernetické bezpečnosti

Kybernetická bezpečnost
Kam jsme se posunuli po přijetí zákona?

Jan Dienstbier, Ladislav Mazač

6. 9. 2016

Kybernetická bezpečnost: aktuální stav

- bezpečnostní strategie 2015-2020 a akční plán
- rozšiřujeme počty prvků KII i VIS
- novela zákona ZoKB – důvody, očekávání
  - směrnice NIS
  - základní služby
  - digitální služby

Výroční zpráva BIS za rok 2015

„K významnému poškození zájmů státu často vedl únik interních informací, které byly využity k získání výhod pro protistranu. Příčinou byl nejen úmysl konkrétních osob získat vlastní prospěch, ale také nedostatečné povědomí o ***nutnosti ochraňovat i takové citlivé informace, které nejsou chráněné žádným speciálním zákonem****."*

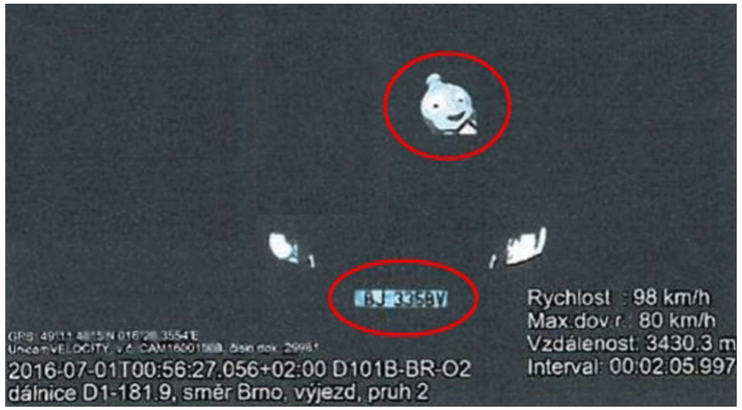
„Kyberšpionážní útoky však necílí pouze na data jako taková nebo na utajované informace, ale zaměřují se spíše na krádeže osobních údajů a přihlašovacích údajů do informačních a komunikačních systémů a krádeže obsahu elektronické komunikace politicky či jinak významných osob. ***Tyto údaje a informace pak dále slouží k sofistikovaným útokům****, které využívají metody sociálního inženýrství."*

„BIS v této oblasti získala v roce 2015 informace o možných tuzemských obětech nové vlny ruské kyberšpionážní kampaně. Na seznamu možných terčů byla i ***dvě česká ministerstva****. Útočníci se v této kyberšpionážní kampani zaměřovali především na kompromitaci routerů, které zřejmě následně využívali k tomu, aby zájmový síťový provoz neautorizovaně přesměrovávali do počítačové infrastruktury, již kontrolovali."*

Za únik informací 1,5 milionu zákazníků přišla pokuta 3,5 milionu korun.

Zpráva NBU o stavu kybernetické bezpečnosti

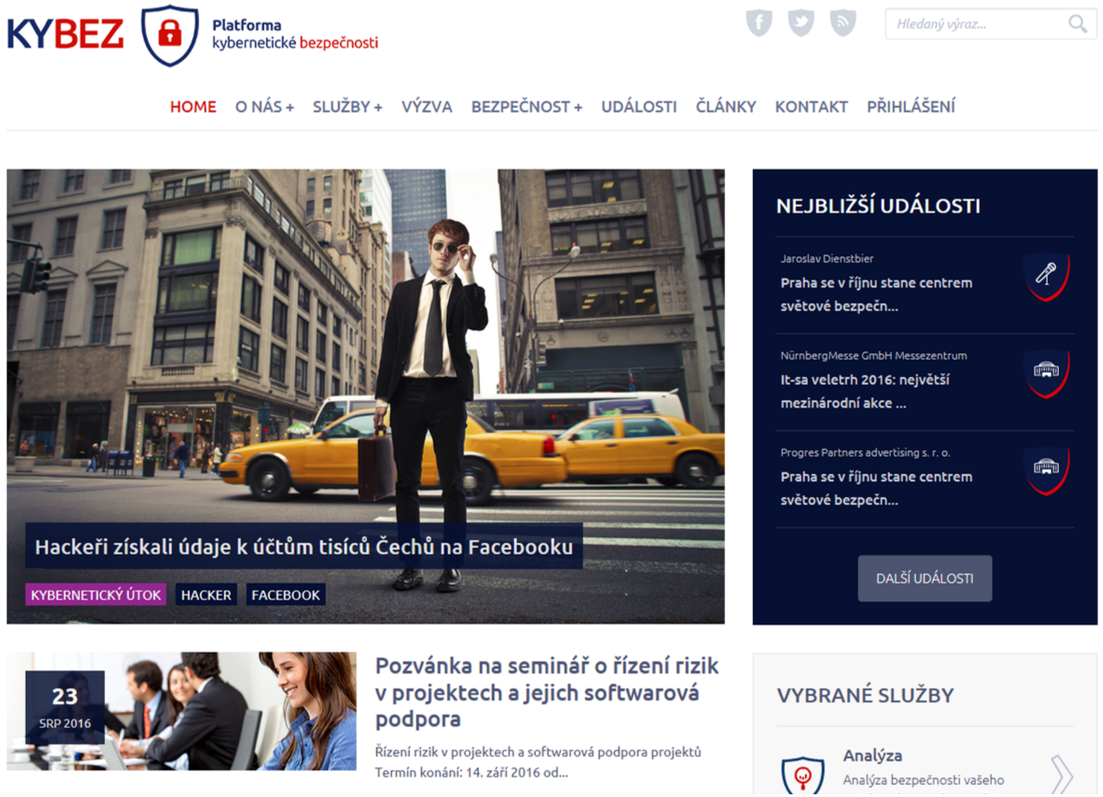
„Podle předběžných informací lze obecně říci, že jednotliví správci KII a VIS k plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti přistupují s odpovědností. Existují však rozdíly mezi úrovní zabezpečení informačních a komunikačních systémů u jednotlivých správců. Nejvýraznější odlišnosti byly evidovány mezi správci v soukromé a veřejné sféře, ***kdy ve veřejné sféře bývá kybernetická bezpečnost a informační bezpečnost podceňována nebo strádá, kromě nedostatku expertů, také nedostatkem financí*** *či administrativními a regulatorními bariérami, byť toto hodnocení samozřejmě nelze na veřejnou sféru uplatnit paušálně.„*



Jak chceme být vnímáni?

- Jsme na dobré cestě:
  - markantnější posun je na straně privátních subjektů
  - nutné zlepšení ve veřejném sektoru
  - sklon k formálnímu plnění (VIS)
- Z hrozby příležitostí: šance pro ekonomiku
- Bude záležet na spolupráci státu, firem a školství (finance, lidské zdroje)

Platforma KYBEZ



KYBEZ

| www.kybez.cz/

Cíle platformy KYBEZ

- Zvyšovat informovanost o problematice ochrany informací včetně kybernetické bezpečnosti
- Upozorňovat na nebezpečí z jejího podceňovaní
- Poskytovat konzultace, řešení a podporu pro veřejný i soukromý sektor a to včetně podpory organizací a úřadů, jež jsou povinné systematicky řešit KB ve smyslu ZoKB kybernetické bezpečnosti
- Dodržovat a prosazovat Compliance program a Etický kodex platformy KYBEZ

Filosofie platformy KYBEZ

› Založená na bezplatné, dobrovolné a efektivní spolupráci odborných akademických, veřejných a mediálních institucí a nezávislých specializovaných komerčních společností z oblasti informačních a telekomunikačních technologií.

Vedení KYBEZ

Rada pro vědu, výzkum a vzdělávání KYBEZ

doc. RNDr. Bedřich Půža, CSc.
Vedoucí ústavu informatiky VUT

Ing. Viktor Ondrák, Ph.D.
Útvar informačních systémů VUT

doc. Mgr. Roman Jašek, Ph.D.
Vedoucí ústavu informatiky UTB

Kdo stojí za KYBEZ

Ing. Michal Řezáč, MSc.
Výkonný ředitel

Ing. Jan Heisler, MBA
Aliančí manažer

Ing. Jan Dienstbier
Technický garant

Partneři KYBEZ

Jak to vidíme?

› Bezpečnost chápeme jako celek
› Neopomíjejme lidský faktor: zaměstnance a uživatele
› Koncept systematického a dlouhodobého vzdělávání (s vysokými školami (VUT, UTB, izraelskými partnery, ale nejen s nimi)
› Služby (studie, analýzy, …)

Služby GORDIC pro řešení ZoKB

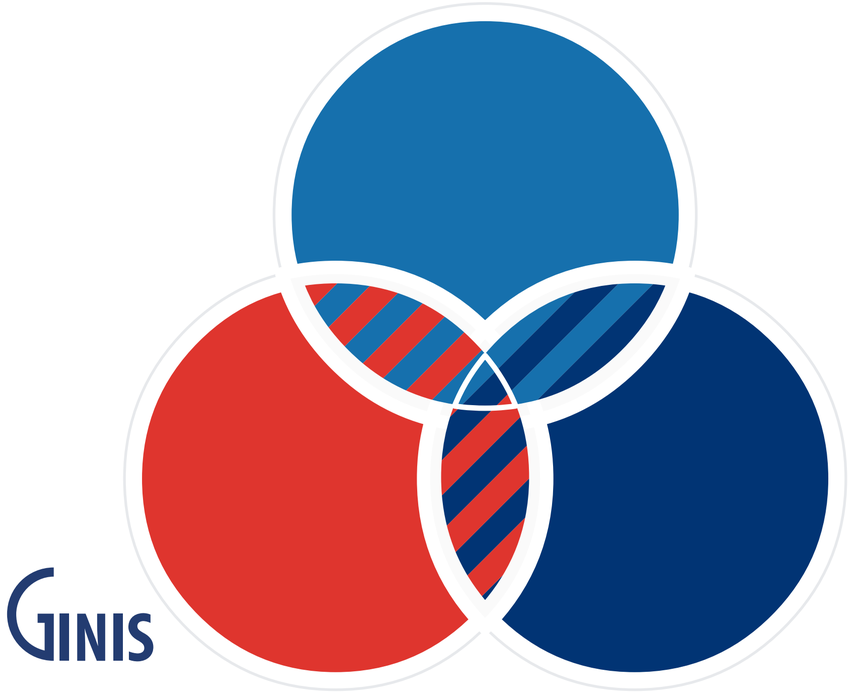
- **Bezpečnostní audit** dle metodiky CISA
- Optimalizace bezpečnostních opatření
- Implementace modulů Cyber Security GINIS®
- Semináře a školení ke kybernetické bezpečnosti
- Příprava komplexního řešení kybernetické bezpečnosti
  - Studie
  - Analýzy
  - Projekty
- Realizace
- Provoz
- Dohled

KYBEZ

Co znamená KB pro zákazníky?

- Aplikace od počátku vyvíjeny s důrazem na bezpečnost provozu (instalace v silových rezortech)
  - Moduly Cyber Security GINIS®
- Standardy – GORDIC je držitelem certifikátů:
  - ISO 9000 (řízení jakosti)
  - ISO 20000 (poskytování ICT služeb)
  - ISO 27001 (řízení bezpečnosti informací)
- Podpora zákazníků v zavádění ISMS
  - Odborné poradenství
  - Inovace v produktech
  - Řešení se specializovanými partnery

Co znamená KB pro zákazníky?



GORDIC spol. s r.o.

Platformy **IS GINIS** **KYBEZ** **IoT**

ZoKB a role systému GINIS

› GINIS jako bezpečný informační systém
› GINIS jako prostředek k sofistikovanému zálohování agendových dat
› GINIS® DRMS jako nástroj řízení kybernetické bezpečnosti

GINIS jako bezpečný informační systém?

› Systém konfigurovatelný tak, aby splňoval požadavky zákona

Certifikát

č. IC-20160501

I 4042

Produkt: Informační systém GINIS®, verze 3.76
ověření shody produktu vůči požadavkům zákona č. 181/2014 Sb.,
o kybernetické bezpečnosti

Objednatel:
GORDIC spol. s r.o., Erbenova 4, 586 01 Jihlava

Inspekce IT/IS v rozsahu zákazníkem definované funkcionality a etalonu
provedená dle schváleného metodického pokynu IO-F-CLIETA.
Posuzovaná kritéria jsou uvedena v Inspekčním protokolu.

Hodnocení: Splňuje kritéria inspekce
Platný od 6. 5. 2016

ID projektu: 120160401
A-TEST je inspekční orgán č. I-4042, zřízený RELSIE spol. s r.o.,
akreditovaný Českým institutem pro akreditaci, o. p. s. podle ČSN EN ISO/IEC 17020:2012.

podpis
hlavní metodik

datum 6. 5. 2016

KYBEZ

GINIS

| www.kybez.cz/

GINIS a automatické a bezpečné zálohování agendových dat

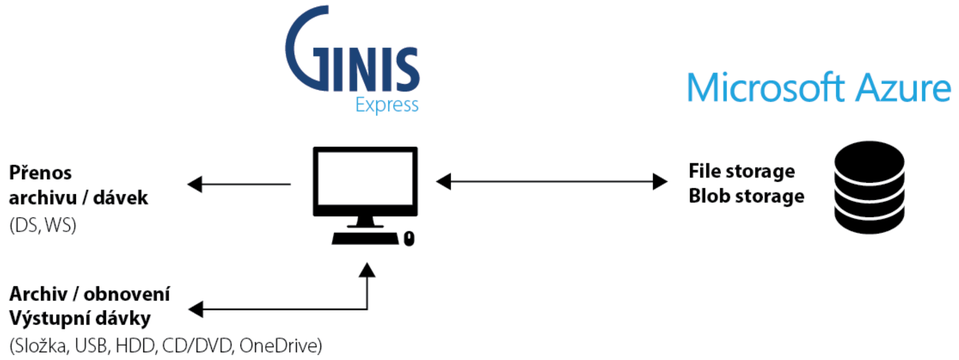
- Nutná součást systému bezpečnosti informací každého úřadu
- Automatické zálohování dat z GINIS v MS Azure
- Neomezená kapacita záložního prostoru Vysoká dostupnost 99,9 až 99,95
- Zabezpečený přístup
- Integrace zálohování v rámci produktů IS GINIS
- Konec problémů se ztracenými daty
- Uživatelé nemusí myslet na vytvoření záloh a jejich uschovávání!

KYBEZ

GINIS

| www.kybez.cz/

GINIS a automatické a bezpečné zálohování agendových dat



KYBEZ

GINIS

| www.kybez.cz/

GINIS jako součást systému řízení kybernetické bezpečnosti organizace

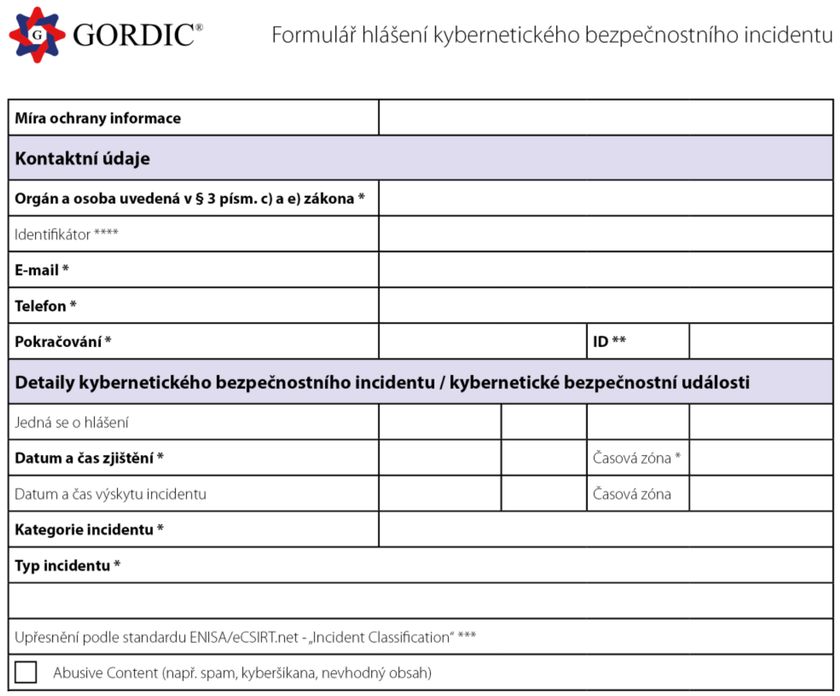
› Software – DRMS ZoKB
› Metodika – Speciální metodika
› Služby – Služby řízení KB

Nástroj DRMS ZoKB

› Dohledatelnost, dostupnost, čitelnost a věrohodnost
› Avizace událostí
› Role a jednoznačná odpovědnost
› Řízení oprávnění, stanovení workflow dokumentů
› Úkoly a termíny, schvalování
› Digitalizace, změna formátu
› Příprava digitálních dokumentů a jejich dlouhodobé důvěryhodné uložení

Speciální metodika

› Šablony dokumentů
› Šablony záznamů (ve formě „prázdných“ formulářů)
› Řízená dokumentace a formuláře zakomponovány do DRMS



GORDIC®

Formulář hlášení kybernetického bezpečnostního incidentu

Míra ochrany informace				
Kontaktní údaje				
Orgán a osoba uvedená v § 3 písm. c) a e) zákona *				
Identifikátor ****				
E-mail *				
Telefon *				
Pokračování *			**ID ****	
Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události				
Jedná se o hlášení				
Datum a čas zjištění *			Časová zóna *	
Datum a čas výskytu incidentu			Časová zóna	
Kategorie incidentu *				
Typ incidentu *				
Upřesnění podle standardu ENISA/eCSIRT.net - „Incident Classification“ ***				
☐ Abusive Content (např. spam, kyberšikana, nevhodný obsah)				

KYBEZ

GINIS

| www.kybez.cz/

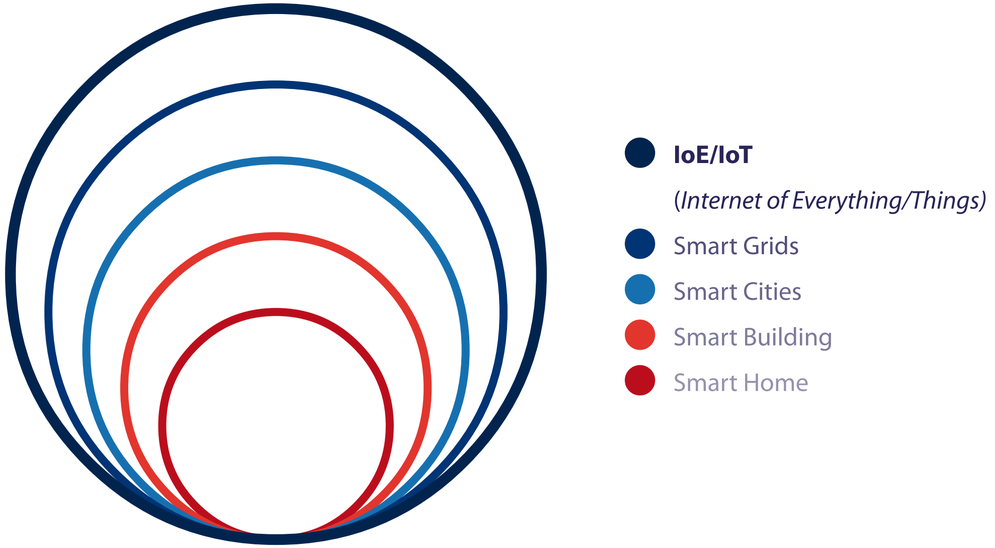
Služby

- Služba „PŘED“:
  - identifikace a zdokumentování stavu řízení bezpečnosti
  - vypracování doporučení pro nasazení nástroje, získání podpory vedení organizace

- Služba „PŘI“:
  - politika bezpečnosti informací, analýza rizik, klasifikace a hodnocení aktiv
  - přiřadit osoby rolím a nastavit jejich oprávnění, školení, výstupní audit, návrh bezpečnostních opatření

- Služba „PO“
  - pravidelné interní auditů, posouzení rizik, přezkoumání systému, adaptace na novou legislativu

IoT Integrační platforma



INTEGRATION PLATFORMS

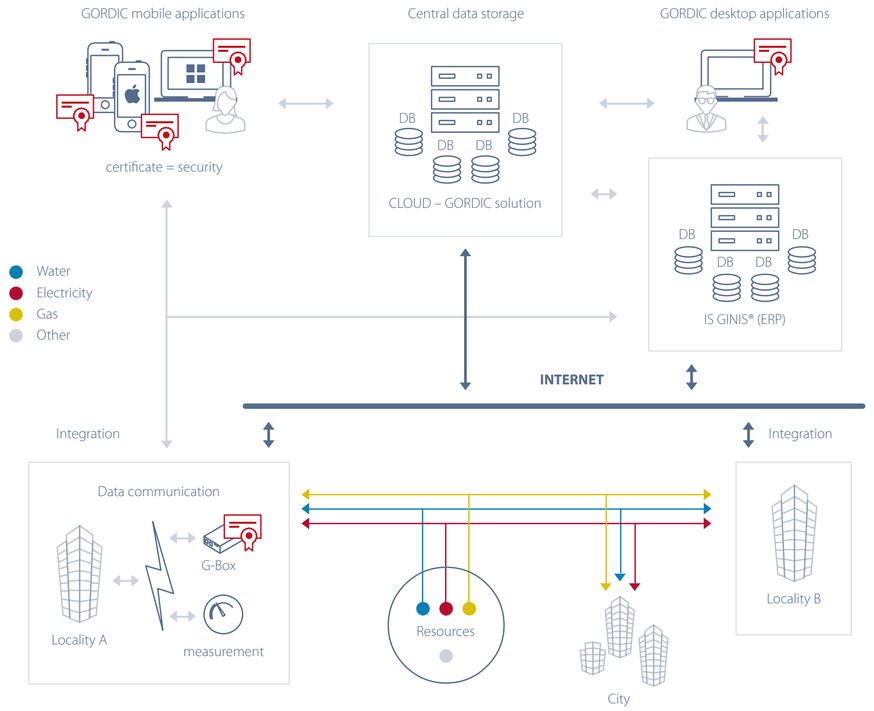
Internet věcí bezpečně

- Studie kybernetické bezpečnosti
- Prvky pro bezpečnost infrastruktury (firewall, atd.),
- Omezení přístupu osob k serverům a jednotlivým částem sítě (prostory s vysokou mírou zabezpečení),
- Využití vysoce bezpečných cloudových platforem
- Centralizovaná správa uživatelů
- Šifrovaná komunikace
- Autentizace přístupů na úrovni certifikátů,
- Zabezpečené bezdrátové sítě postavené mimo hlavní infrastrukturu

Technologie pro chytré budovy – Internet věcí

› GORDIC koncept SDI: Security, Design, Integration

Internet věcí bezpečně: integrace smart meteringu



KYBEZ

Děkujeme za pozornost

www.kybez.cz
www.gordic.cz

Ladislav Mazač
ladislav_mazac@gordic.cz

Jan Dienstbier
jan_dienstbier@gordic.cz
jan.dienstbier@cimib.cz