
# Kybernetická bezpečnost
## Zákonná povinnost nebo existenční nutnost?

Ing. Jan Dienstbier

22. 3. 2016

# Proč kybernetická bezpečnost?

*„… zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.“*

ZoKB 181/2014 Sb. § 4, odst. 1

# Nebo protože je to nutnost?

„Cokoliv je připojeno lze hacknout!“

„Rozlišuji pouze dvě kategorie systémů, ty které již hackli a ty, které to ještě nevědí“ John Chambers ex CEO Cisco

Ať se vám to líbí nebo ne, je to blíže k realitě než k fikci.

# Co vše je připojeno?

osobní údaje

vztahy a vazby

obchodní tajemství

kontakty

regulace a dohled

peníze

chytrá města

rozvodné sítě a řídící systémy

důvěryhodnost

akcie

strategické plány

**MOC**

duševní vlastnictví

**technické prostředky internet of things**

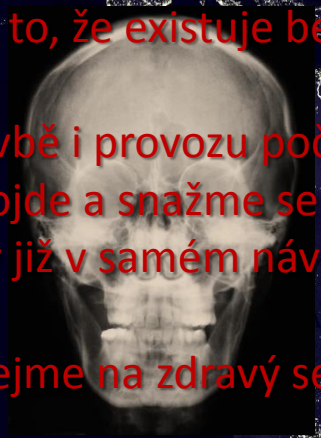
krizové řízení

přístupové klíče

výsledky výzkumu

společenský vliv

# Co s tím?



Zapomeňme na to, že existuje bezpečný systém

Při návrhu stavbě i provozu počítejme s tím,
že k narušení dojde a snažme se minimalizovat
možné škody již v samém návrhu systému

Nezapomínejme na zdravý selský rozum

Systém je tak bezpečný, jak bezpečný je jeho nejslabší článek

# Co to tedy znamená?

- Pohlížejme na bezpečnost jako na celek
- Neoddělujme bezpečnost fyzickou od kybernetické
- Soustřeďme se na nejslabší články
- Nezaštiťujme se zákonem
- Učme se z chyb (raději z chyb druhých než z těch vlastních)
- Komunikujme (vysvětlujeme) raději více než méně
- Buďme vždy připraveni
- Cvičení dělá pokroky
- Důvěřujme, ale prověřujme

29.3.2016

# Co to znamená v praxi?

- Vůli vedení k budování bezpečnostní kultury instituce.
- Zhodnotit aktiva a analyzovat rizika - co chránit, s jakou hodnotou a proti čemu
  - ❑ Průtok peněz
  - ❑ Systémy
  - ❑ Know-how,
  - ❑ Prestiž,
  - ❑ Značku apod.
- Řízení dodavatelů
  - ❑ Bezpečnostní díra zabezpečeného systému.
  - ❑ Bezpečnost informačního systému jako služba, zodpovědnost stejně nese vlastník
- Řízení celého životního cyklu všech prvků informačního systému (od pořízení po likvidaci – bezpečnou)
- Personální bezpečnost (osvěta, vzdělání)
- Nastavení procesů pro zvládání incidentů a sdílení a rozvíjení znalostí o hrozbách a zranitelnostech
- Zavedení monitorovacího systému (dohledová centra)
- Zajištění kontinuity činnosti
- Fyzická bezpečnost všech rozhodujících technologií informačního systému
- Mít jasně definovány parametry bezpečnosti informačního systému
  - ❑ Ochrana identit,
  - ❑ Pravidla pro přístupy do informačního systému,
  - ❑ Pravidla pro používání mobilních zařízení,
  - ❑ Pravidla pro BYOD (Bring Your Own Device) apod.
- Síťovou bezpečnost

# Nebo slovy zákona

- Bezpečnostní pravidla
- Organizace informační bezpečnosti
- Klasifikace a inventarizace informačních aktiv
- Zabezpečení vůči zaměstnancům
- Fyzické zabezpečení výpočetního centra
- Bezpečnost komunikací a provozu IT
- Přístupová práva k sítím, systémům, aplikacím, funkcím a datům
- Implementace zabezpečení do aplikací
- Předvídání a řešení incidentů
- Zabezpečení kontinuity chodu kritických systémů
- Zabezpečení konformity s nastavenými požadavky, audit

# Kybernetická bezpečnost – nekonečný příběh


# Jak vám může pomoci

# Projektové služby kybernetické bezpečnosti

- Studie řízení bezpečnosti informačního systému
- Analýzy a konzultace:
  - Identifikace, klasifikace a ocenění aktiv
  - Bezpečnostní politika informačních systémů
  - Business continuity management
  - Metodiky procesů průběžné analýzy rizik
  - Procesy řízení incidentů
  - Politiky hesel, autentizace a autorizace
  - Bezpečnostní role
  - Řízení bezpečnosti lidských zdrojů
  - Fyzické zabezpečení výpočetního centra
  - Metodiky skartace el. médií a výpočetní techniky

- Confidentiality – důvěrnost
- Integrity – integrita
- Accessibility - dostupnost

# Projektové služby kybernetické bezpečnosti

- Služby ve spolupráci s partnery :
  - Analýza a konzultace řešení technických zranitelností systémů
  - Návrh a realizace penetračních testů
  - Implementace a konfigurace bezpečnostních nástrojů
    - (např. log management, SIEM, IDS/IPS, antiviry,...)
  - Mobile Device Management (MDM), BYOD
  - Podpora provozu bezpečnostního systému
  - Dohledové centrum
  - ...


KYBEZ
Portál Kybernetické Bezpečnosti
HOME
O NÁS
BEZPEČNOST
POSTUP
ZPRÁVY
KONTAKT
PŘIHLÁŠENÍ
KYBERNETICKÁ BEZPEČNOST
ZÁKONNÁ POVINNOST NEBO EXISTENČNÍ NUTNOST?
NEJNOVĚJŠÍ ZPRÁVY
6
ŘÍJ 2014
Jak zajistit svou bezpečnost
Vladimír Přech
Se schválením zákona o kybernetické bezpečnosti se objevuje mnoho otazníků kolem praktické realizace bezpečnostní politiky povinných institucí tak, aby odpovídala nové...
Zobrazit více...
3
ZÁŘ 2014
Zákon vstoupil v platnost
Vladimír Přech
V pátek 29. 8. 2014 byl ve Sbírce zákonů pod č. 181/2014 Sb. publikován zákon o kybernetické bezpečnosti. Přijetím této normy Česká republika reaguje na rizika zneužití...
Zobrazit více...
NEPŘEHLÉDNĚTE
Proč řešit kybernetickou bezpečnost?
Žijeme ve společnosti, která se spoléhá na informační systémy a začíná být na nich závislá. Ohrožení jejich funkčnosti může způsobit ohrožení fungování základní infrastruktury potřebné pro život.
Prosazení připravovaného zákona o kybernetické bezpečnosti je zásadním počinem pro řešení bezpečnosti informačních systémů, a to nejen v oblasti organizací veřejné správy (veřejné moci).
Obchodní korporace a organizace, které budou podle tohoto zákona osobami povinnými, se musí včas seznámit, důsledně prostudovat a včasně realizovat požadavky v tomto zákoně uvedené, jež lze chápat i jako srozumitelné a efektivní kroky pro zavedení Systému řízení bezpečnosti informací (ISMS) ve smyslu požadavků definovaných v normě ISO/IEC 27001. Velmi si ceníme důrazů na přínosy a náklady, hlavní principy, přiměřenost a efektivitu,

www.kybez.cz

# Partneři













www.kybez.cz

# Služby GORDIC pro řešení požadavků 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

Partneři

# Co znamená KB pro zákazníky GORDIC?

- 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

29.3.2016

# GINIS® splňuje požadavky ZoKB

- GINIS® v roli významného informačního systému
  - Instalace u orgánů veřejné moci (a krajů v přenesené působnosti)
  - Subsystémy spisová služba, správní řízení, ekonomika, personalistika,...
- Soulad GINIS® a ZoKB
  - Od počátku je navržen s ohledem na aktuální bezpečnostní normy
  - Je koncipován pro nasazení v silových rezortech (MO, MV)
  - Obsahuje mechanismy pro zajištění **důvěrnosti**, **integrity** a **dostupnosti**
  - Podpora rozšířených požadavků dle ZoKB: GINIS 3.76 – podzim 2015
  - Již dnes obsahuje volitelné komponenty **Cyber Security GINIS®**
- GORDIC je držitelem certifikátů:
  - ISO 9000 (řízení jakosti)
  - ISO 20000 (poskytování ICT služeb)
  - ISO 27001 (řízení bezpečnosti informací)

29.3.2016

# Cyber Security GINIS®

## Komplexní zabezpečení primárních aktiv v aplikačních systémech

| Modul GINIS® | | Podporuje IS | | Potenciální přínos pro zabezpečení aktiv* | | |
|---|---|---|---|---|---|---|
| | | GINIS® | ostatní | Důvěrnost | Integrita | Dostupnost |
| **IDM** | Identity Management | ANO | ANO | ●●● | | |
| **GDU** | Garantované dlouhodobé úložiště | ANO | ANO | ●● | ●● | ●● |
| **GDA** | Důvěryhodný archiv | ANO | ANO | ●● | ●●● | ●●● |
| **AIB** | Aplikační internetová brána | ANO | ANO | ●●● | | |
| **DKS** | Dokumentový konverzní server | ANO | ANO | | ●● | |
| **WSDMS** | Úložiště dokumentů | ANO | ANO | ●● | ●● | ●●● |
| **GSP** | GORDIC Support Portál | ANO | ANO | ● | ● | ● |
| **ZUD** | Zpracování událostí | ANO | | ●● | ● | ●● |
| **RAK** | Registr autorizovaných konverzí | ANO | | ●● | ●● | |
| **EPK** | Elektronická podpisová kniha | ANO | | | ●●● | |
| **DAA** | DRMS Administrativní audit | ANO | | ● | ●● | ● |
| **SEM** | Security Monitor GINIG | ANO | | ●● | ● | ●● |
| **DSG** | Dohledový systém GINIS | ANO | | | ● | ●● |
| **eConnector** | Konektory na bezpečná úložiště | ANO | | ●●● | ●● | ●●● |
| **SSL** | Individuální přístup k dokumentům | ANO | | ●●● | ● | |
| **ADM** | Záznam činností administrátora | ANO | | ●●● | ● | ● |

*) Potenciální přínos pro zabezpečení aktiv: ●●● kritický / ●● podstatný / ● podpůrný

# Moduly CSG: Cyber Security GINIS®

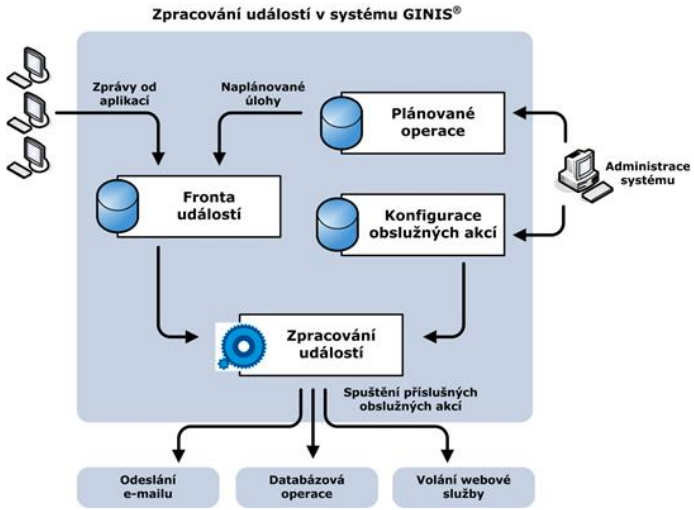
- IDM - Identity management
- ZUD - Zpracování událostí
- AIB - Aplikační internetová brána
- IPA - Informační panel
- EPK - Elektronická podpisová kniha
- WSDMS - Bezpečné úložiště GINIS
- GDU - Garantované dlouhodobé úložiště digitálních dokumentů

# GORDIC Lightweight IDM

- Správa rolí
  - Historizace rolí a jejich přidělení v čase
  - Přehledy uživatelů nákladových středisek
  - Sestavy s aktivními a neaktivními uživateli
  - Automatizovaný systém odebírání rolí
- Zpracování žádostí o přístupy do systému GINIS
  - Rozdělení zodpovědností žadatel-schvalovatel-realizátor
  - Řízený proces přijetí, schválování a zpracování
  - Poloautomatické nastavení přístupů v GINIS
  - Distribuce prvotních údajů potřebných pro přístup - např. heslo
- Zvýšení bezpečnosti celého informačního systému

# Zpracování událostí

- Abyste nic nepřehlédli!
  - Automatické plánované provádění rutinních nebo často opakovaných činností
  - Cílená informovanost o důležitých událostech v rámci systému
  - Rozsáhlé portfolio kategorizovaných událostí a obslužných akcí
- Optimalizace zpracování
  - Účinný dohled nad klíčovými provozními parametry systému
  - Možnost posunu zpracování náročných úloh do doby nízkého vytížení systému
- Podpora napopojení událostního systému na externí SIEM řešení



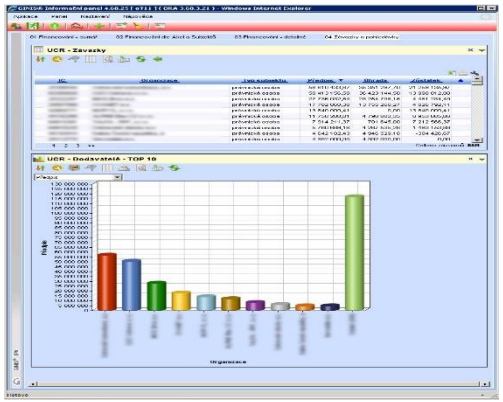

**SIEM**
security information and event management

# Aplikační internetová brána

- Zvýšení bezpečnosti úřadu
- Podrobný log komunikace s externími systémy
- Jedno místo pro správu a instalaci certifikátů
- Centrální přístupový bod pro:
  - ISDS - datové schránky
  - ISZR - základní registry
  - IISSP - státní pokladna
  - ISIR - insolvenční rejstřík
  - ADIS - Registr plátců DPH
  - ČNB - ABOKWS
- Centrální funkce:
  - RAK - autorizovaná konverze
  - TS - tvorba časových razítek
  - SIGN - Podepisování a CLR listy
- Optimalizováno pro GINIS, podporuje i aplikace jiných výrobců

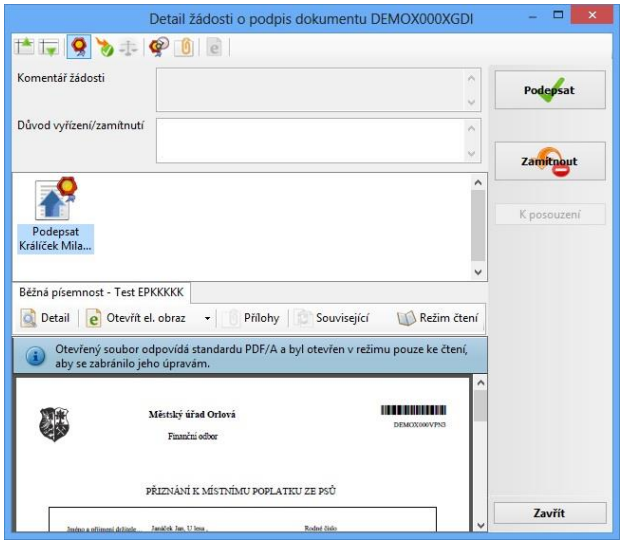
# Informační panel

- Integrace heterogenních informací
- Podpora rozhodovacího procesu
- Drilování – interaktivní detail
- Různé formy výstupů –
  grafy, zvuková upozornění,
  grafické alerty apod.
- Využití jako univerzálního bezpečnostního dashboardu (nejen pro aplikace GINIS)



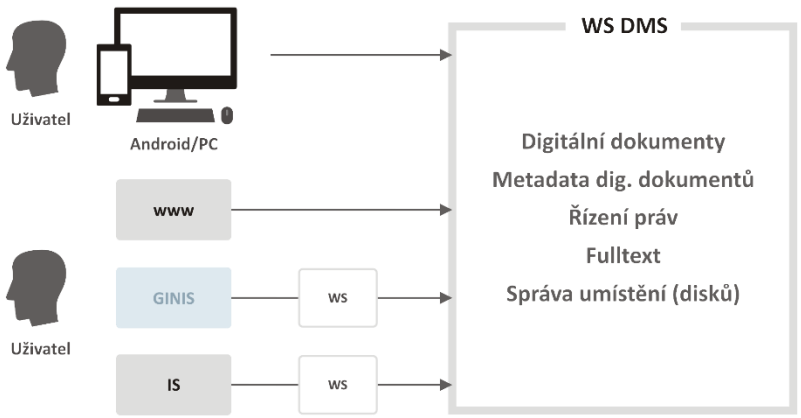
# Elektronická podpisová kniha

- Obdoba procesu schvalování listinných dokumentů
- Žádosti o posouzení/schválení
- Finalizace dokumentu
- Schválení jedním tlačítkem
- Dohledatelné poznámky, komentáře a kroky procesu
- Logování veškerých činností
- Hromadné činnosti



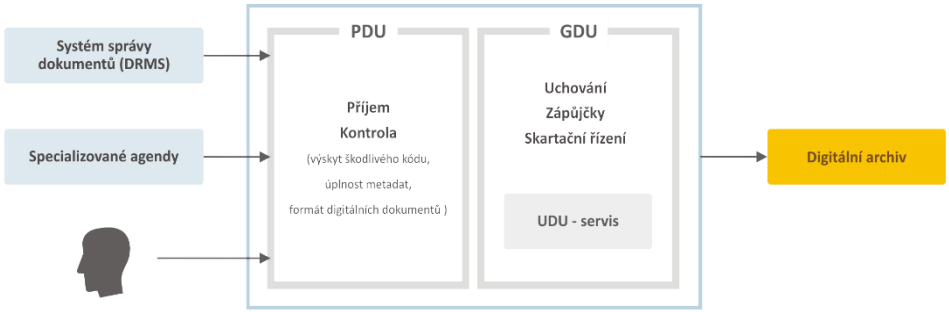
# Úložiště dokumentů WSDMS

- Bezpečná náhrada úložišť typu FTP serveru
- Klientský přístup z mnoha platforem
- Konektivita po internetu pomocí standardních protokolů.
- Bezpečná autorizace.
- Šifrování dat.
- Fulltext.



# Garantované dlouhodobé úložiště

- Důvěryhodné uložení a správa správa digitálních, analogových i hybridních dokumentů a spisů.
- Kontrola metadat, formátů i výskytu škodlivého kódu
- Skartační řízení včetně přenosu archiválií do příslušných archivů či NDA
- Plný soulad s platnou legislativou (vč. Národního standardu pro el. systémy spisové služby) a OAIS





**Fakulta podnikatelská, VUT Brno**
**gestor**


**GORDIC spol. s r. o.**
**provozovatel**

**+ partneři**


# Děkuji za pozornost

Jan Dienstbier

jan_dienstbier@gordic.cz

jan.dienstbier@cimib.cz

www.kybez.cz

www.gordic.cz