DATA SYS

Děláme to chytřeji.cz

Integrovaný bezpečnostní a provozní monitoring Datasys ELISA

Hana Bauerová, MBA
Account manager

Mgr. Pavel Štros, Ph.D.
Certified Information Systems Auditor
Vedoucí týmu „Bezpečnost a monitoring“
bauerova@datasys.cz
stros@datasys.cz

DATASYS s.r.o. - všechna práva vyhrazena
Obsah prezentace je chráněn autorským zákonem a jakékoliv jeho šíření, kopírování, a to celku i jakékoliv jeho části, je bez předchozího souhlasu výslovně zakázáno.

Představení společnosti DATASYS, s.r.o.

- 22 let zkušeností – komplexní implementační a integrační služby v oblasti IT, telekomunikací a vývoje na zakázku

Strategické vize

- Skutečné potřeby zákazníků
- Dlouhodobá spolupráce
- Kvalitní partnerská spolupráce

85

Zaměstnanců

10

Strategických oblastí

750

Obrat 2015: 750 mil. korun

50

V roce 2015 realizováno více jak 50 projektů

4

Pobočky

DATASYS

Strategické kompetence firmy

Bezpečnost a monitoring

Microsoft a virtualizace

Storage a zálohování

Networking

Aplikační vývoj

Dokumenty

Inovace

Unified Messaging System

ServiceDesk/HelpDesk

Infrastruktura

DATA SYS

DATASYS a jeho řešení pro Průmysl 4.0

1. Řízení skladového hospodářství pomoci QR a RFID

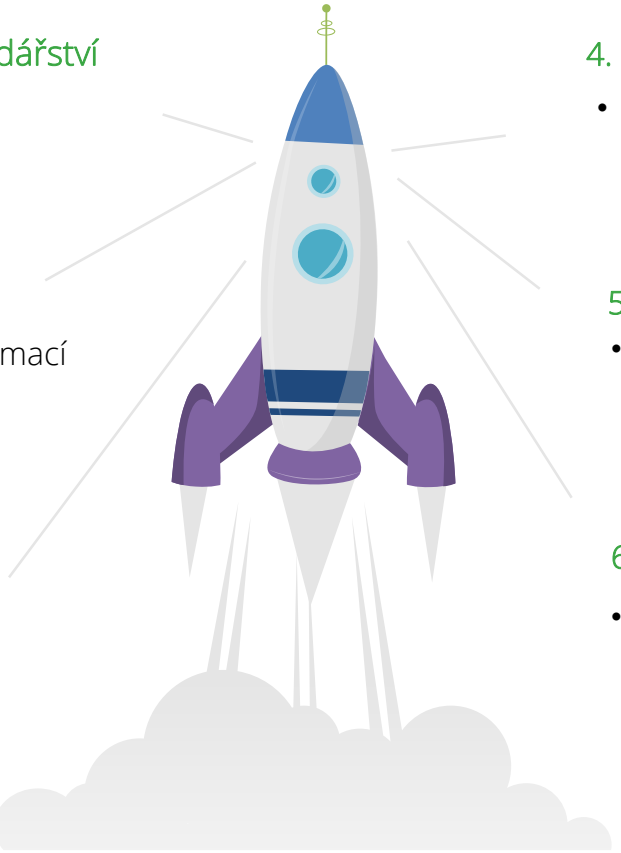
- Řízení skladů

2. Kybernetická bezpečnost

- Zajištění bezpečnosti informací
  Bezpečnostní audity
  Provozně bezpečnostní monitoring

3. Prediktivní údržba

- Využití čidel a senzorů propojených do virtuální sítě
- IoT oblast



4. Bezpapírová kancelář

- Řízení oběhu dokumentů celým výrobním procesem včetně pravidel schvalování

5. BI – business inteligence

- Analýza a využití posbíraných dat

6. Infrastrukturní projekty

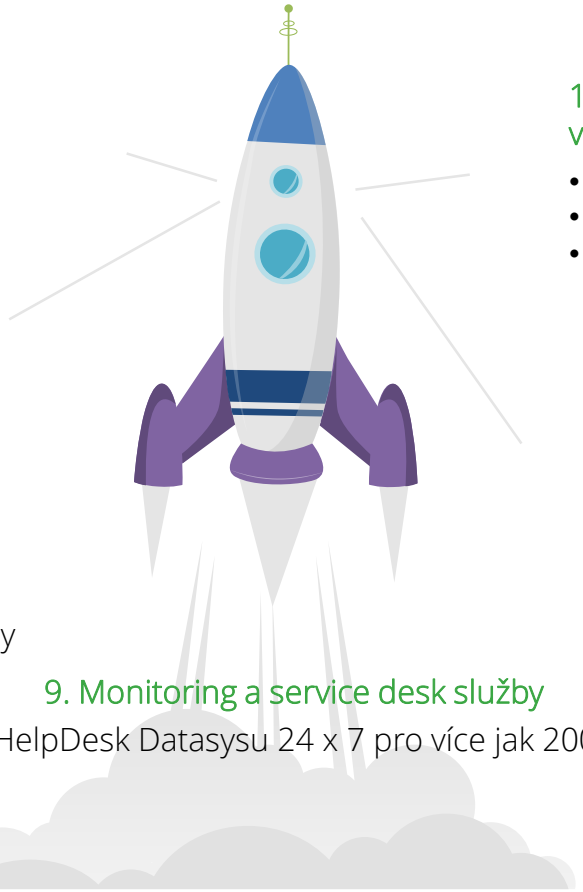
- Obnova stávající infrastruktury, nová architektura

DATASYS

DATASYS a jeho řešení pro Průmysl 4.0

7. Inteligentní budovy

- Využití IT technologií pro správu budov
- Řídící systém pro ovládání např. vytápění, spotřeby, predikce, údržby, alternativních zdrojů energií



8. 3D tisk a technologie

- Rychlé prototypování
- Automotive
- Konstrukční práce všemi systémy

10. UMS – řízení komunikace napříč všemi systémy

- Výstražní systémy
- Mobilní přenos dat
- Datové přenosy – data, video, hlas

11. Smarteam řešení pro řízení

- Pro komplexní sledování a správu informací souvisejících s výrobkovými daty

9. Monitoring a service desk služby

- HelpDesk Datasysu 24 x 7 pro více jak 200 klientů

DATA SYS

Specifika bezpečnosti v Industry 4.0

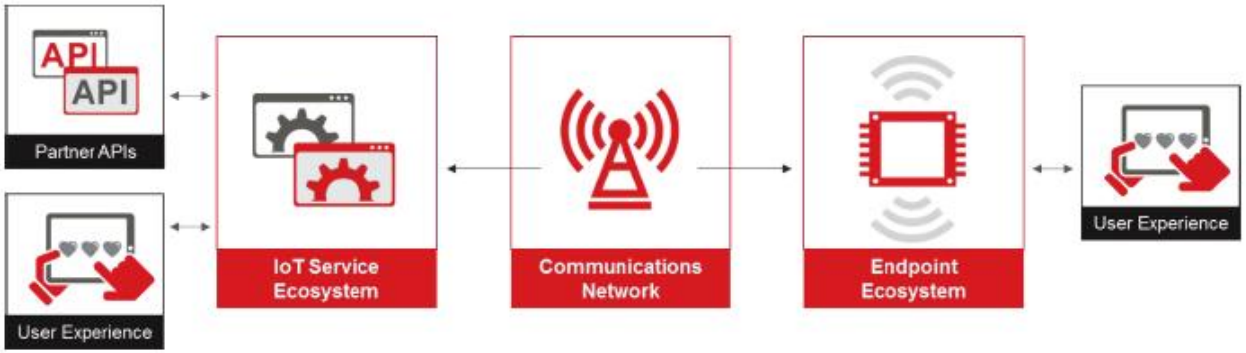
- Je kybernetická bezpečnost v Industry 4.0 hodně jiná?
  - Není to „*jiná kybernetická bezpečnost*“, **principy jsou úplně stejné**

- Ne? Tak co se nám to tu chystáte přednášet? ;-)
  - V podnicích často není dobře ošetřena ani „běžná“ informační bezpečnost
    - Rekapitulace hlavních principů neuškodí
    - Máte např. ve vašem podniku personálně oddělen výkon správy IT od bezpečnostního dohledu? Dodržujete princip separace kompetencí?
  - Pod nálepkou „Industry 4.0“ lze rozvíjet i oblast IoT
    - Internet věcí má svá specifika
    - Existuje opodstatněná obava před rozmělňováním bezpečnosti na úkor ceny
    - Inspiraci lze čerpat zejména ve světě mobilních komunikací

DATA SYS

Internet věcí – bezpečnostní model

- Bezpečnostní model zformulovaný GSM Asociací
  - Bere inspiraci ve světě mobilních komunikací
  - Léty prakticky prověřený model
- GSMA model
  - Endpoint Ecosystem
    - Bezpečnostní architektura specifických zařízení
  - Service Ecosystem
    - Typicky služba v Internetu, v podstatě s běžnými vlastnostmi
  - Network Security
    - Doporučení pro operátory – při komunikaci přes veřejné sítě



DATA SYS

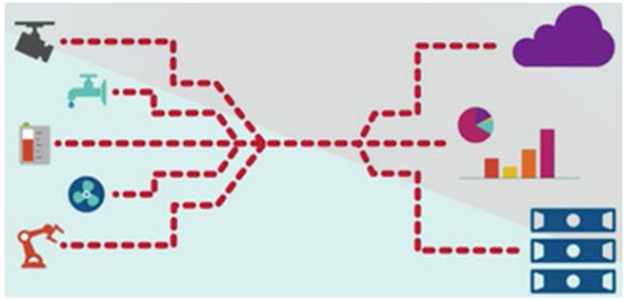
Ekosystém koncových zařízení

- Důraz na vyhodnocování rizik
  - Architektonických i implementačních
    - **Už ve fázi návrhu** architektury
    - **Uvažovat celý životní cyklus** zařízení
  - Typ koncového zařízení
    - Lightweight, např. jednoduchý senzor na měření srdečního tepu
      - ***jednoúčelové zařízení***, napájeno často jen baterií bez možnosti dobíjení
    - Complex, např. dron s množstvím senzorů a pokročilou logikou řízení letu
      - ***výkonnější procesor a HW*** obecně, tj. i vyšší nároky na energii
      - potřeba a podpora vyšší úrovně zabezpečení
        - např. Arduino/Genuino MKR1000 s kryptočipem nebo Raspberry Pi 3
    - Gateway, např. řídící systém auta s podporou pro V2V komunikaci
      - též označováno jako ***HUB***, slouží jako ***komunikační brána*** pro „lightweight“ zařízení
      - potřeba a podpora vyšší úrovně zabezpečení
        - souboj „velkých hráčů“ jako Dell, IBM, Intel, Microsoft
        - často ve spojení s cloudovými službami

DATA SYS

Funkční specifika IoT zařízení

- Specifika funkčních požadavků
  - Dlouhá životnost, nízká spotřeba energie
  - Nízké výrobní i provozní náklady
  - Nelze spoléhat na vnější fyzickou bezpečnost



- Běžné aspekty informační bezpečnosti
  - Zachování důvěrnosti, integrity a dostupnosti dat
  - Někdy též zajištění nepopiratelnosti (průkaznosti) operací

DATA SYS

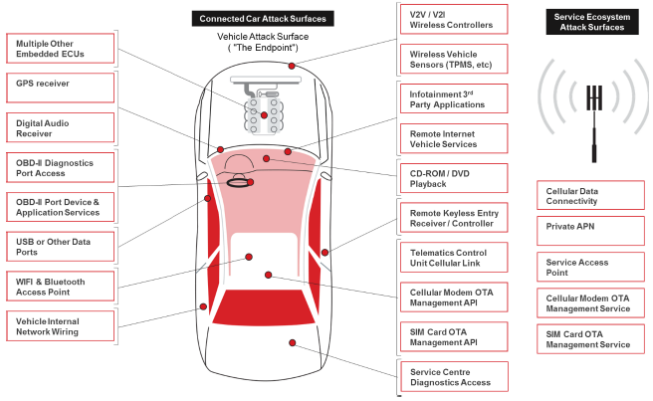
Bezpečnostní specifika IoT zařízení

- Specifika bezpečnostních požadavků
  - Dostupnost
    - Často spíše **s plošným pokrytím a dlouhodobá**, ne nutně okamžitá dostupnost
    - Někdy též vysoká fyzická odolnost
  - Jednoznačná identifikace
    - **Odolnost proti klonování** na fyzické i komunikační úrovni
      - Nabízí se integrace s GSM technologií, identifikací na bázi SIM
      - SIGFOX (Simplecell) to řeší unikátním certifikátem na zařízení už z výroby
  - Ochrana soukromí a zabezpečení dat
    - Sbírat jen „opravdu **nezbytná data**“
    - Vzájemná **autentizace a šifrování** komunikace, „**chip level**“ bezpečnost
      - Opět možnost řešit integrací s GSM včetně Over-The-Air aktualizací
      - SIGFOX řeší integritu dat při komunikaci, šifrování nutno případně řešit v aplikaci
    - Ochrana dat v cloudu už je běžnou IT disciplínou

DATA SYS

Řízení rizik

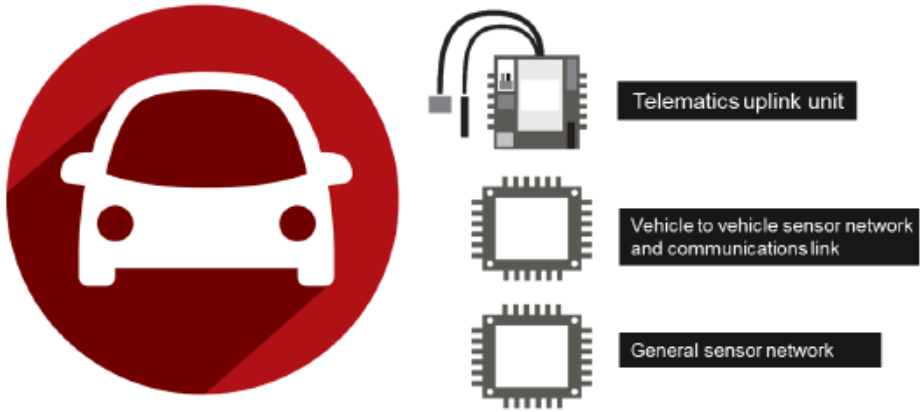
- Doporučené fáze hodnocení rizika
  - Rozbor technického návrhu
    - „Itemizace“ technologií a funkcí, týmově
  - Rozvaha bezpečnostního modelu
    - Identifikace nejpravděpodobnějších **hrozeb**
    - Identifikace **dopadů**
  - Přiřazení odpovědností a řešitelských týmů
    - Nízkoúrovňově, na úrovni atomických technologií
  - Posouzení doporučených praktik
    - Provádět globálně, **napříč technologiemi a řešitelskými týmy**
  - Detailní zhodnocení rizika
    - Identifikace zranitelností na technologické úrovni řešitelským týmem
    - Návrhy **ošetření zranitelností**
  - Řízené zavádění bezpečnostních opatření
  - Řízení bezpečnosti během životního cyklu



DATA SYS

Výsledky procesu řízení rizik

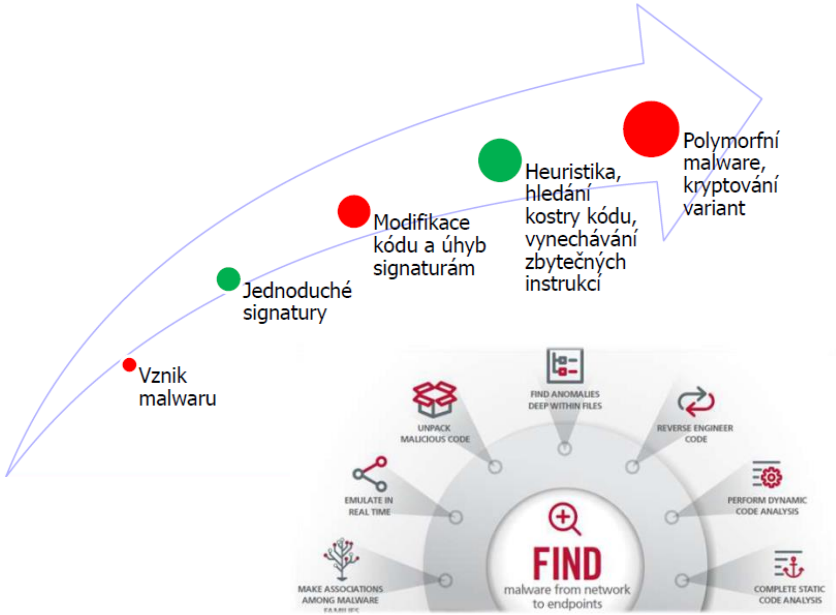
- Příklady bezpečnostních opatření
  - Umístění senzoru do „tamper-resistant“ obalu
  - Zvolen GSM operátor, který podporuje poskytování SIM s aplikačními klíči
  - EEPROM data jsou zašifrována klíčem uloženým na SIM kartě
  - Bootloader zařízení pomocí klíče nově kontroluje integritu firmwaru
  - Klíče a přístupové heslo jsou zpracovávány výhradně v interní paměti CPU
  - Uživatelské rozhraní zařízení validuje kvalitu hesla při jeho změně
  - Uživatelské rozhraní zařízení poskytuje seznam sbíraných dat

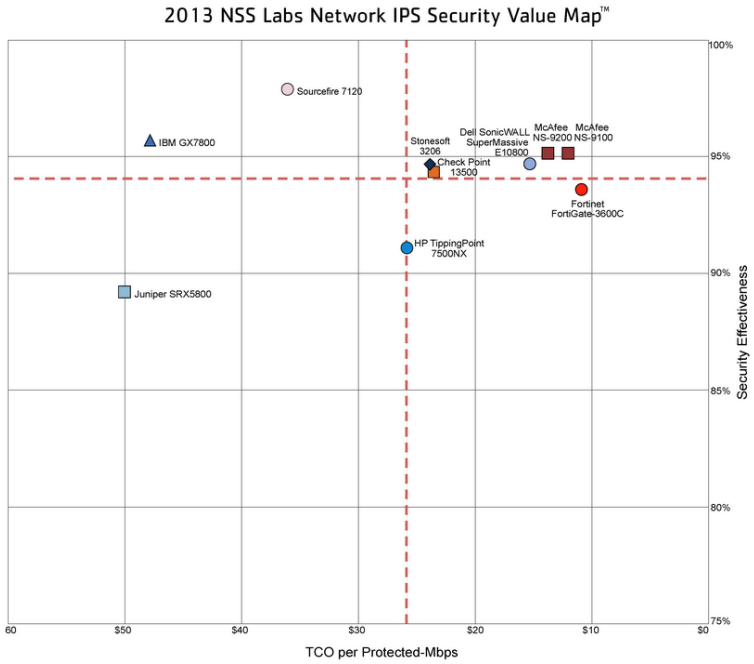


DATA SYS

Detekci nelze kvalitně řešit „levně“ …

- Naše zkušenost:
  - vybírejte špičkové **nástroje pro detekci** , které se hodí do vašeho prostředí
    - je tedy nutné investovat i do procedury jejich výběru,
    - antiviry (next gen), IDS/IPS systémy,
    - UTM firewally, detektory DDoS, apod.

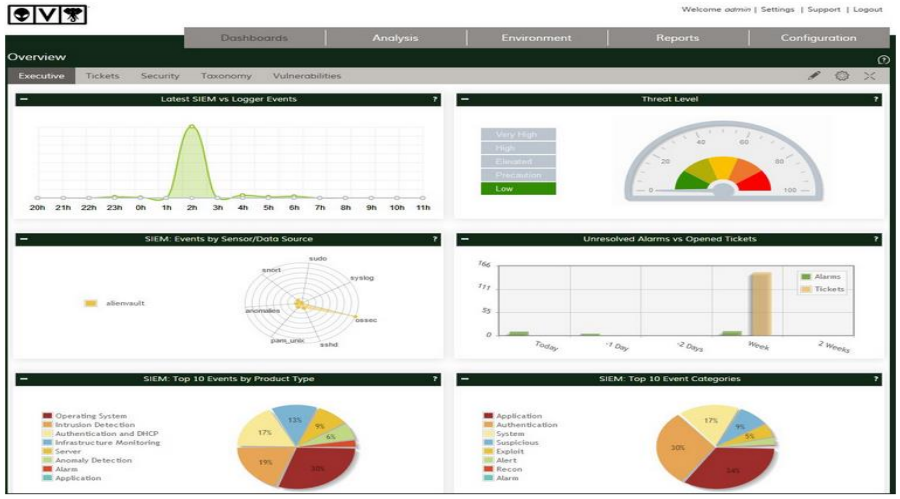




DATA SYS

… sběr a vyhodnocování lze řešit „levně“.

- Naše zkušenost:
  - dnes existují velmi kvalitní „svobodné“ **nástroje pro sběr a vyhodnocení** kybernetických bezp. událostí,
    - stačí vědět, jak je používat,
      - (my jsme do toho investovali),
    - pořizovací náklady jsou nízké,
    - náklady na implementaci a provoz jsou srovnatelné s komerčními produkty.



DATASYS - technologie – strategie

- Nízkonákladové systémy podnikové úrovně
  - Log management systém DATASYS ELISA
    - Máme zvučné reference
    - Užitečný nejen pro bezpečáky, ale i pro správce systémů a aplikací
    - Výkon, stabilita, flexibilita, líbivé webové GUI pro analýzu dat
    - Distribuované sondy, řízení přístupu k datům, pokročilý reporting
  - Monitorovací systém ZABBIX CERTIFIED PARTNER
    - Máme zvučné reference
    - Disponujeme množstvím odladěných monitorovacích šablon
    - Výkon, stabilita, flexibilita, přehledné webové GUI
    - Distribuované sondy, automatizace, vyhodnocování KPI, měření SLA
- Produkty renomovaných výrobců
  - Cisco, Fortinet, IBM, Intel Security, Microsoft

DATASYS

Zvučné reference i k ELISA

- Státní správa
  - **Statutární město Kladno**
    - stovky zařízení, desítky serverů
    - zaměřeno na monitoring síťových prvků
- Soukromá sféra
  - **Lagardere Travel Retail**
    - desítky serverů, více než 1000 stanic, VMware
    - převážně systémová úroveň monitoringu logů
- Finanční sektor
  - **Artesa spořitelní družstvo**
    - desítky windows serverů, desítky zařízení, VMware
    - systémová i aplikační úroveň monitoringu logů

KLADNO
MĚSTO PRO KVALITNÍ ŽIVOT

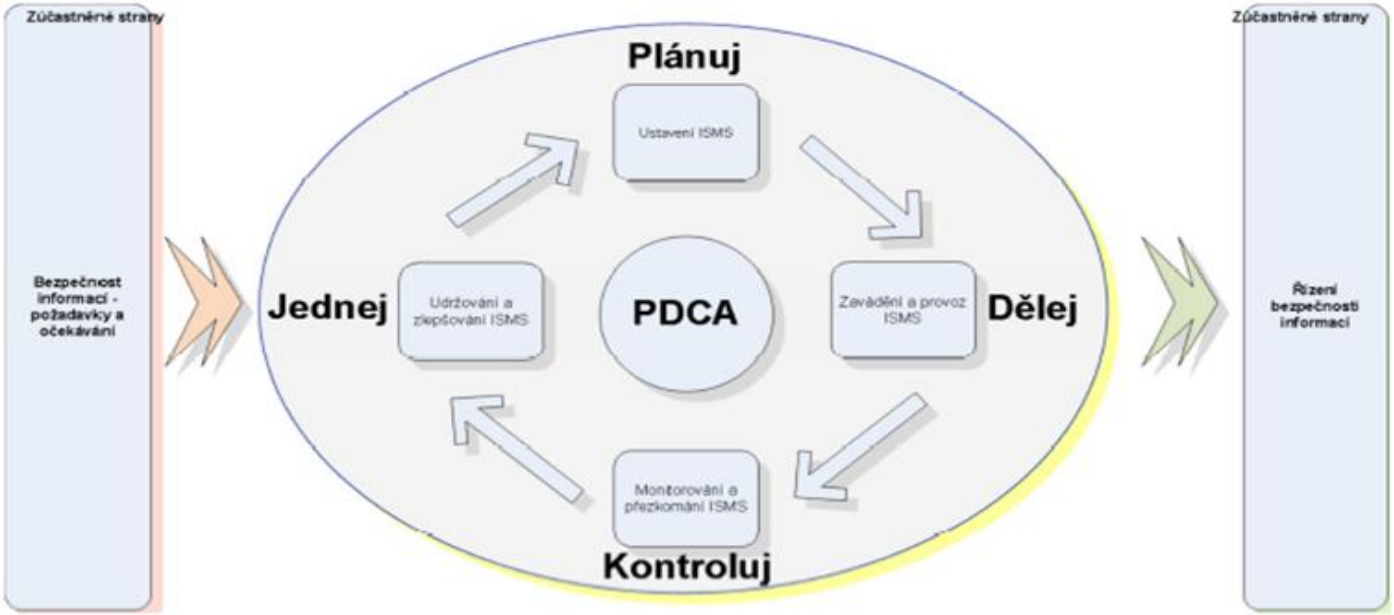
Lagardère
TRAVEL RETAIL

artesa

DATA SYS

Motivační faktory pro „log management“

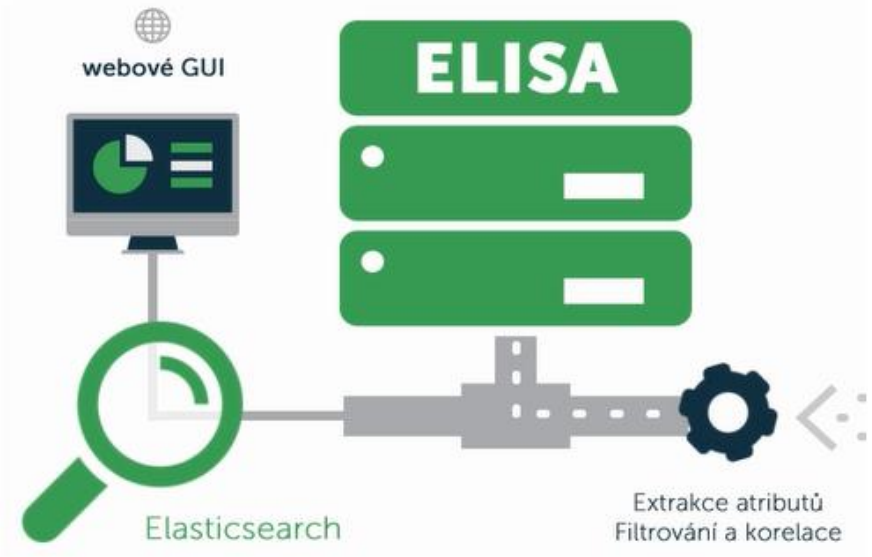
- Jeden z hlavních nástrojů pro **systematické řízení bezpečnosti v organizaci** (ČSN ISO/IEC 27001)
  - i **zákon o kybernetické bezpečnosti** na něj klade důraz



DATA SYS

Motivační faktory pro „log management“

- Stěžují si správci a bezpečnostní správci na nedostatek času?
  - Jak dlouho jim trvá vyhodnocení bezpečnostního nebo provozního incidentu?



- Dokáží správci systémů po sobě zamést stopy?
- Dokážete získat kompletní stopu aktivit uživatele během pár vteřin?
- Odhalíte včas anomálie v chování uživatelů?

DATA SYS

Manažerský přehled k ELISA LM

- Robustní řešení, podnikové vlastnosti
- Líbivé a praktické uživatelské rozhraní
- Široká podpora různých zdrojů logů
  - Množství explicitně podporovaných zařízení
- Nízké pořizovací i provozní náklady
  - svobodný software (s technickou podporou)
  - VMware appliance (kompaktní systém)
  - HW appliance (postaveno na Dell serverech)

DATA SYS

Proč právě log management od Datasysu?

Budete překvapeni, co

všechno dokážete rychle zjistit!

DATASYS

Děkuji
za pozornost

Mgr. Pavel Štros, Ph.D.
Certified Information Systems Auditor
Vedoucí týmu „Bezpečnost a monitoring“
stros@datasys.cz

DATASYS

DATASYS s.r.o. - všechna práva vyhrazena
Obsah prezentace je chráněn autorským zákonem a jakékoliv jeho šíření, kopírování,
a to celku i jakékoliv jeho části, je bez předchozího souhlasu výslovně zakázáno.