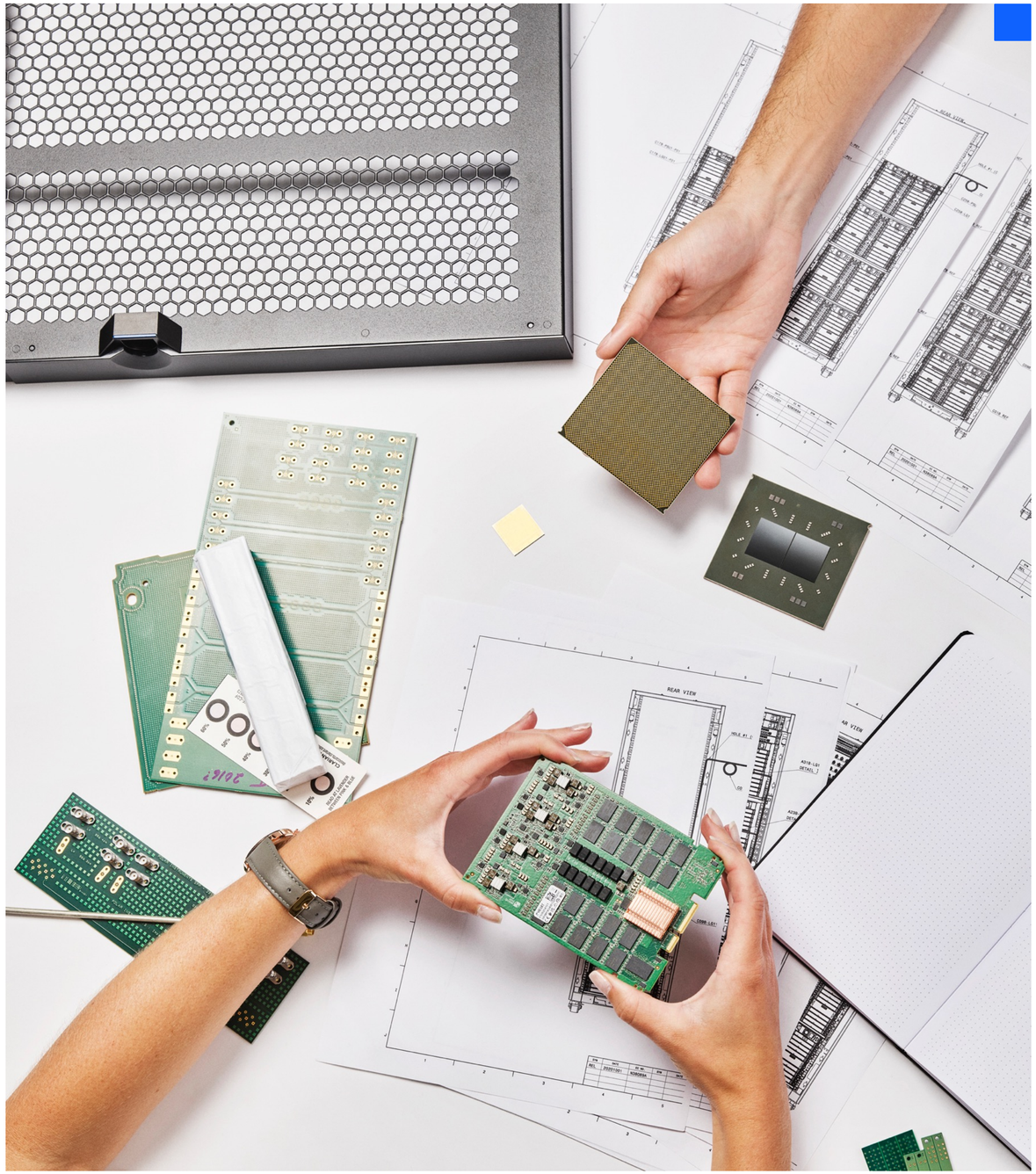
PROČ JE BEZPEČNOST V SYSTÉMECH SAP TAK DŮLEŽITÁ?

A jak na ni pohledem IBM



Karim Ifrah
Senior Security Consultant,
Cybersecurity Services

kifrah@cz.ibm.com
+420 721 361 472

Proč je zabezpečení systémů SAP tak důležité?

Boření mýtů o SAP…

- SAP je komerční produkt a přináší Security by default
- Při implementaci standardních funkcí bez vlastního vývoje je SAP secure by default (v základu)

Bohužel to není tak jednoduché…

SAP přináší bezpečnostní funkce… ale to neznamená, že je bezpečný. Tyto funkce musí být správně implementovány / nakonfigurovány…

- **Access Management:** Rozsáhlé možnosti Otevřené vstupy
- **Custom Code: SAP** běží nad vývojovým frameworkem
- **Konfigurace:** Stovky bezpečnostních parametrů
- **Interfaces:** On-premise, privátní a veřejné cloudové systémy
- **Integrace:** s jinými systémy mimo SAP. Jak?
- Zařazení SAP do **bezpečnostního prostředí organizace**
- **Pokuty:** Jaká je cena za "nesoulad" s předpisy?

Trh začíná chápat rizikovou expozici Obavy Forbes-500 CIO’s & CISO’s

92%

naznačilo, že narušení systému SAP by bylo závažné, **velmi závažné nebo katastrofické**

65%

Případech došlo k narušení systému SAP v posledních **24 měsících**

47%

"nejistých" nebo "nemělo důvěru", že by dokázali **odhalit narušení SAP do 12 měsíců**

4.5M

Průměrné náklady výpadku SAP do režimu offline z důvodu bezpečnostního incidentu

59%

věří, že Cloud, HANA, Fiori, IOT **zvyšují pravděpodobnost útoku**

Source: Forbes-500 CIO’s & CISO’s

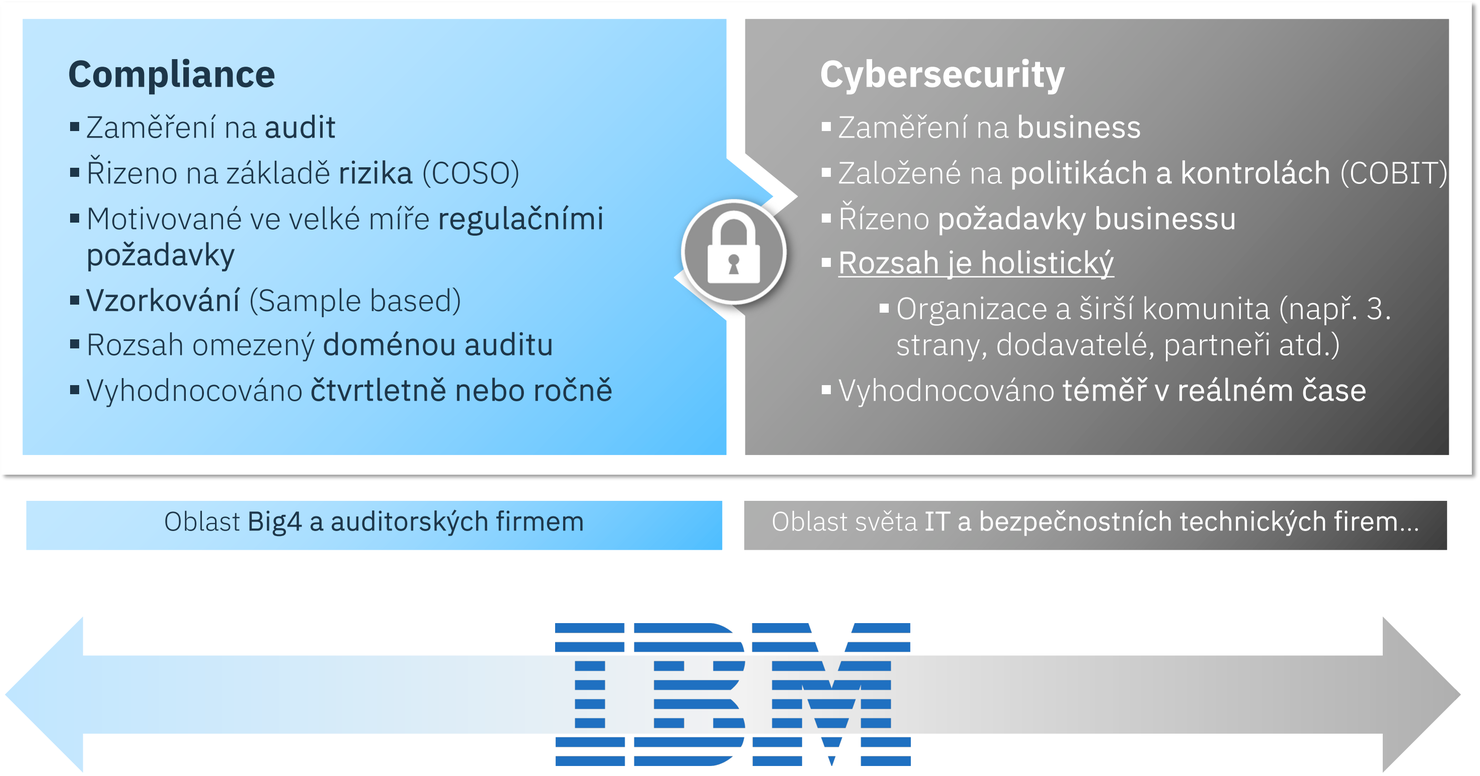
IBM se snaží být vůči našim klientů vždy v roli **Důvěryhodného partnera** v otázce Bezpečnosti pro SAP systémy

Pohled IBM na bezpečnost SAP

Pohled IBM na potřeby zabezpečení SAP je výsledkem dlouhých let poskytování služeb v této oblasti našim klientům. Výsledná iniciativa pak nese název.

“13 vrstev zabezpečení SAP”

Tento rámec je komplexní a zahrnuje všechny bezpečnostní aspekty, které mohou ohrozit zabezpečení systémů SAP.



IBM Cybersecurity Pohled na bezpečnost SAP – 13 vrstev zabezpečení SAP

Compliance

Cyber security

1. Governance & Regulatory
2. Access Management
3. Data Privacy
4. CCM & Automation
5. Authentication
6. Application Security
7. Application Server (AS) Security
8. SAP HANA Security
9. Data Encryption
10. Network & Communications
11. Vulnerability & Threat Mgmt.
12. Infrastructure Security
13. Cloud Security & Hosting

Aplikační bezpečnost

- **GRC řešení** pro Interní kontrolu, Interní Audit a Regulace
- **Access Management** řešení (IAM, IAG a PAM)
- Compliance SAP prostředí s požadavky na **Data Privacy** a implementace technických a organizačních opatření
- **Kontinuální monitoring kontrol** Compliance, IT, a Security kontroly
- Definice a automatizace ad-hoc **Security Baseline pro SAP**
- Design a implementace strategie **Zabezpečení dat**
- Adopce **DevSecOps** a implementace odpovídajících technických a organizačních opatření
- Security **interních / externích připojení a rozhraní** (hybridní landscapes)

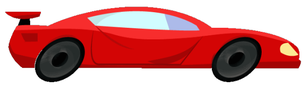
Aplikační i platformní pokrytí

- **Data encryption** (at-rest / in-motion)
- **Vulnerability Management** (Aplikace a Platforma)
- **Threat Management** (Applikace a Platforma) a **Integrace na SIEM** (např., IBM QRadar, Splunk, ArcSight, atd.)
- **Penetrační testování** (Applikace a Platforma)

Bezpečnost platformy

- **Infrastruktura**: Network, Firewall, Gateways, Operating Systems
- **Security vzory a blueprinty pro všechny Hyperscalery**
- **RISE with SAP** // **Security in SAP Cloud**

Jak se vyrovnat s bezpečností v kontextu SAP transformace...?



Poradenský rámec

Typické poradenské služby se zaměřují na...

- Access Management
  - SAP Role a Autorizace
  - IAM a Provisioning platforma
  - SSO a poskytovatelé Identit

Doporučený rozsah zahrnuje i...

- Security Maturity Review
  - Posouzení AS-IS (slabé oblasti)
  - Nastavení plánu a stanovení priorit
  - Zamýšlený TO-BE stav a možnosti automatizace
- Segregation of Duties
- Data Privacy a Data Protection
- Vulnerability Assessment
- DevSecOps

Doporučené

Implementační rámec

Typické implementační služby se zaměřují na...

- Access Management
  - SAP Role a Autorizace
  - IAM a Provisioning platforma
  - SSO a poskytovatelé Identit
- Segregation of Duties
- Základní SAP Security hardening (RSPARAM, atd.)
- Custom Code na základě SAP standardů
- Data Privacy compliance standard

Doporučený rozsah zahrnuje, ale není omezen na...

- **Security Baseline pro SAP systémy**
- **Design, Implementace a Automatizace kontrol**
- **Data Privacy Discovery**
- **Bezpečnost rozhraní**: Interní / Externí
- **Šifrování**: Data “at-rest” a “in-motion”
- **DevSecOps**: Security kontroly + TOMs
- **Vulnerability Assessment** (před Go-Live)
- **Penetrační testování** (před Go-Live)

Doporučené

AMS rámec

Typické služby AMS se zaměřují na...

- Access Management
  - L1, L2, L3 tickety
- Základní SAP Security hardening (Maintenance)
- Custom Code na základě SAP standardů
  - Evoluční / Korektivní vývoj

Doporučený rozsah zahrnuje, ale není omezen na...

- **Security Baseline pro SAP systémy** (Maintenance)
- **Vulnerability a Threat Management**
  - Periodické kontroly + remediační akce
  - Zlepšování baselines a kontrol
- **DevSecOps:**
  - Periodické kontroly + remediační akce
  - Vylepšování AppSec procedur
- **Penetrační testování**

Doporučené

Nedávné úspěšné zabezpečení SAPu ze strany IBM Consulting

Rakousko (Energetika – ropa/plyn)

SAP Enterprise Threat Detection (ETD)

Konfigurace a vyladění SAP ETD pro automatizovanou analýzu hrozeb / útoků v lozích SAP ve více než 65 systémech SAP.
Podpora provozu a monitorování 24x7 (on call) + integrace s IBM Qradar.

Švýcarsko (Farmaceutický průmysl)

Onapsis Platform (Moduly ASSESS, COMPLY a DEFEND)

Instalace, konfigurace a vyladění platformy Onapsis.
SAP security office pro provádění VM & TM a návrh akčního plánu / nápravných opatření pro 57 produktivních systémů SAP.

Švédsko / USA (reatail / těžba kovů)

Zabezpečení SAP S/4HANA Cloud

Strategie SAP GRC
Implementace SAP Cloud IAG pro správu přístupu a SoD v cloudových systémech SAP (S/4, Ariba a SSFF)
Soulad s ochranou osobních údajů pro SAP Cloud (správce dat, protokolování uživatelského rozhraní a maskování uživatelského rozhraní)

USA (Elektrotechnický průmysl)

Připravenost na dodržování předpisů a due-diligence pro fúze a akvizice

Zahraniční akvizice. Získaná společnost byla první společnosti ve skupině s technologie SAP. Klient potřeboval ověřit, zda nová akvizice splňuje požadavky předpisů v oblasti IT a kritických podnikových aplikací.

Děkuji Vám za pozornost

.