ISMS z pohledu technika

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Jakub Onderka

Bezpečnostní analytik, Vládní CERT, NÚKIB

E-mail: j.onderka@nukib.cz
Telefon: +420 720 966 958
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD

Jakub Onderka

- Vládní CERT (GovCERT.CZ)
- Národní centrum kybernetické bezpečnosti
- NÚKIB

- Bezpečnostní analytik
- Řešení incidentů (když je třeba)
- Vývojař
- Kontroly KII/VIS/ISZS (techická část)
- Příprava bezpečnostních regulací (techická část)

„Ajťáci” vs. „Bezpečáci”

The Tower of Babel, Pieter Bruegel the Elder

TLP: WHITE

Společný „jazyk”

Společný „jazyk”

- **„Ajťáci” většinou nebudou rozumět procesům ISMS**
- **„Bezpečáci” většinou nebudou rozumět technickým detailům**

- **Před započetím procesu je potřeba najít společný „jazyk“ mezi těmito skupinami**
  - Společné školení na ISMS i pro „ajťáky” a technická školení pro „bezpečáky”
  - Interní krátké prezentace mezi těmito skupinami
  - Hlavně ze začátku problematiku mezi sebou diskutovat
  - Vyzkoušet si procesy na menším projektu

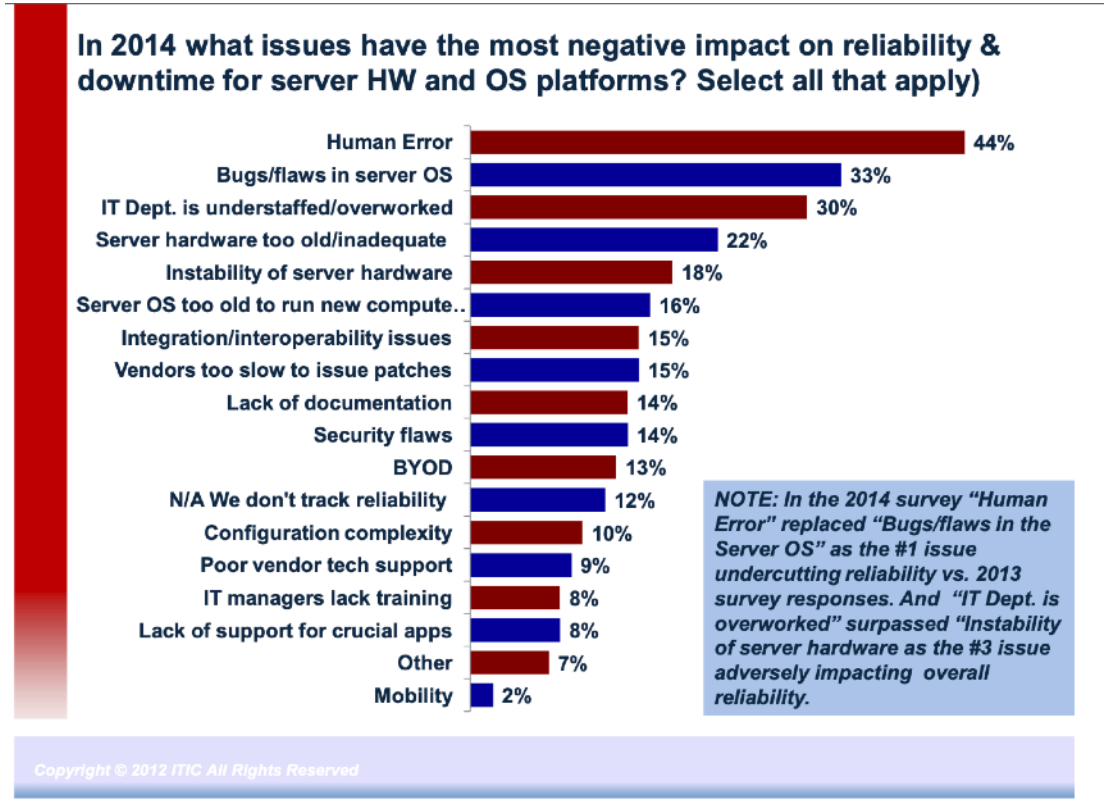
Společný cíl

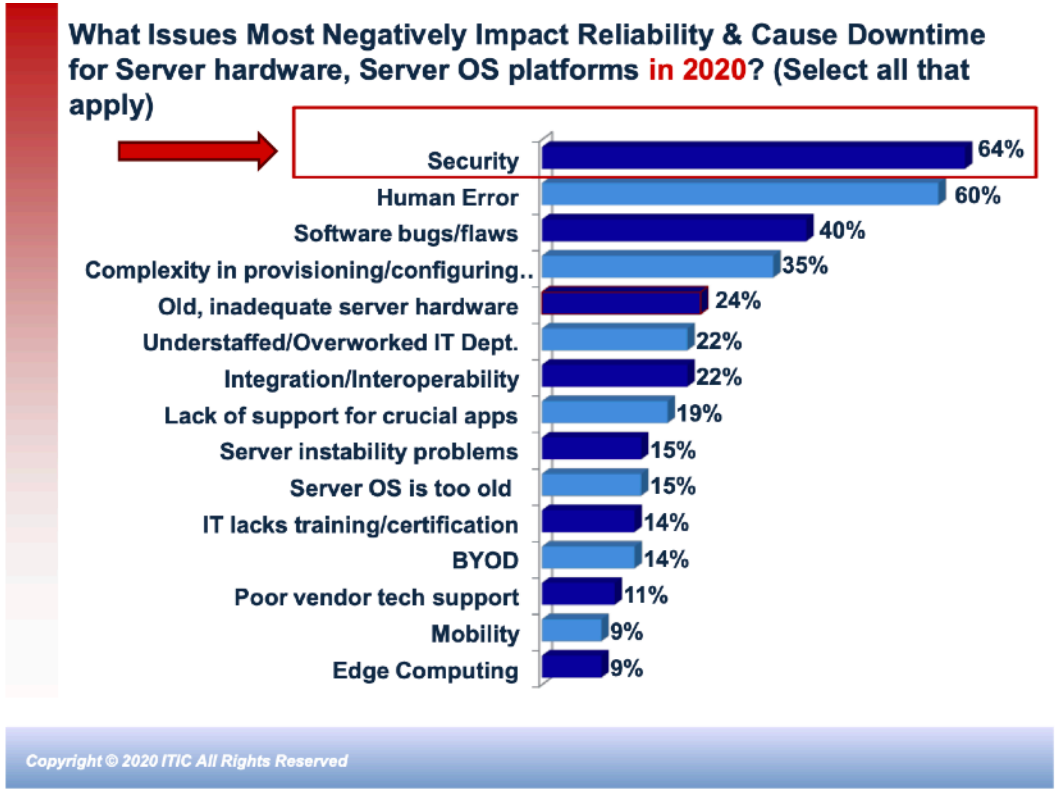
Společný cíl

- **Hlavním cílem není:**
  - Vytvářet politiky a směrnice
  - Zajistit soulad s zákonem a vyhláškou
  - Úspěšně projít kontrolou nebo auditem

- **Hlavním cílem je:**
  - **Zajištění bezpečnosti (včetně provozní) systémů**

Společný cíl





Zdroj: ITIC Global Server Hardware, Server OS Reliability Report

Společné nástroje

Excel a e-mail: ne

- Excel a e-mail jsou skvělé univerzální nástroje, ale nehodí se na všechno

Ticketovací systém

- **Snažte se co nejvíc používat ticketovací systém, kteří už používají „ajťáci”**

- Výhody oproti e-mailu nebo Excelu:
  - Všechny úkoly na jednom místě
  - Minimalizace kopírování informace mezi jednotlivými pracovníky
  - Sdílení informací v rámci celého oddělení
  - Hlídání termínů
  - Auditovatelnost, historie změn
  - Jednoznačný indentifikátor každého úkolu
  - Provazby, návaznosti

Ticketovací systém: příklady použití

- **Nálezy z penetračního testování**
  - Jeden nález => jeden ticket s přiřazenou prioritou
- **Řízení firewallových pravidel**
  - Schvalování nového prostupu v rámci tiketu
  - Unikátní ID do komentáře pravidla
- **Plán zvládání rizik**
  - Jednotlivé úkoly do ticketů, z plánu jen odkazovat
- **Evidence incidentů a zranitelností**
- **Evidence změn**
- **Automatické generování ticketů z monitoringu nebo SIEM**

Ticketovací systém

- **Vhodný už od týmu pěti lidí**
- **Existuje množství bezplatných nástrojů, které naprosto dostačují**
  - Nasazení max dva-tři dny
- **Dodavatelé by měli mít přístup do vašeho systému**
  - Snažit se vyhnout situaci, kdy se požadavky musí dávat do ticketovacího systému dodavatele
  - Jedná se o informace o vašem systému, které je potřeba zachovat i po ukončení smluvního vztahu
  - Zabrání možným podvodům ze strany dodavatele

Audit a pentest

Audit

- **Primárně neslouží k tomu, aby se odhalilo, kdo dělá špatnou práci**
  - Hlavní cíl: odhalil systémové problémy
  - Respondenti musí být co nejotevřenější, aby se zjistil reálný stav
  - Jak motivovat „ajťáky”: konečně se začnou řešit dlouho neřešené problémy

Penetrační testování

- **Opět:** Primárně neslouží k tomu, aby se odhalilo, kdo dělá špatnou práci
- Jak motivovat „ajťáky”: profesní motivace, možnost poučit se, jak dělat věci lépe
- Nemá smysl pentestovat systémy, které jsou zranitelné
  - Jediný důvod: upozornění na problém, který nemá prioritu
  - Je možné začít s menšími celky nebo jen provést test zranitelností
- Sociální pentest: Netrestat pracovníky, kteří udělají chybu, ale nahlásí ji

Co si zapamatovat

- „Ajťáci" a „bezpečáci" by měli…
  - mluvit společným jazykem
  - mít společný cíl
  - používat společné nástroje
  - vědět, že audit a pentest slouží k odhalení systémových problémů

- Každá organizace je rozdílná, doporučené postupy nemusí vždy fungovat