KYBEZ Platforma kybernetické bezpečnosti

Kybernetická bezpečnost

Co je nutné vědět

http://www.gordic.cz

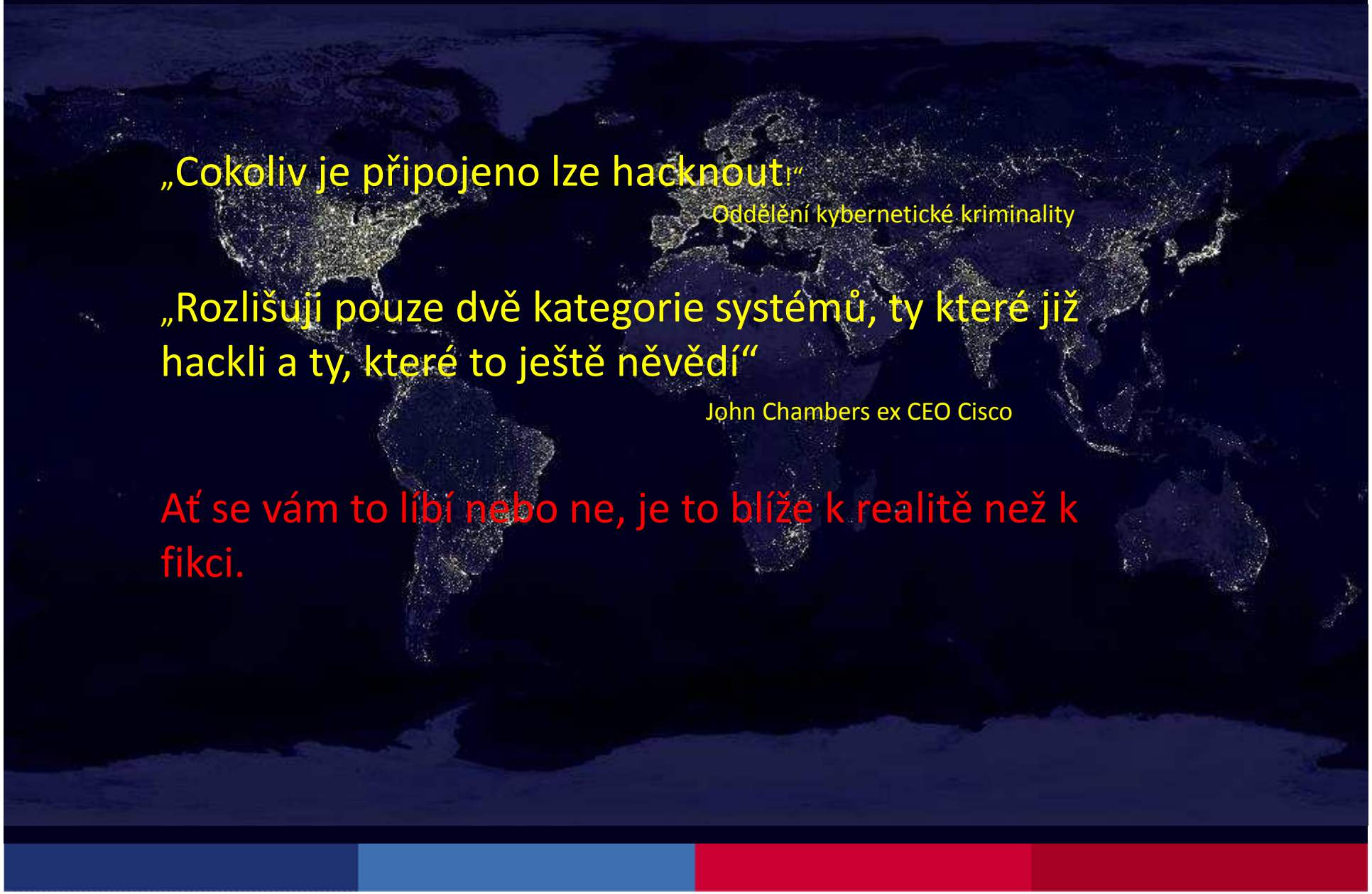
http://www.kybez.cz

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!“

Oddělení kybernetické kriminality

„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

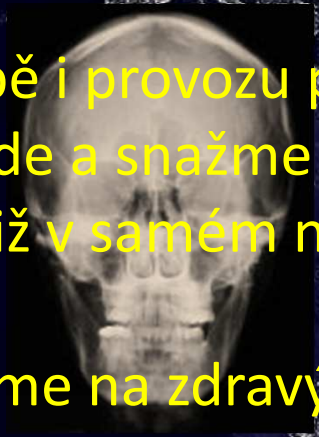
přístupové klíče

společenský vliv

výsledky výzkumu

Co s tím?

Zapomeňme na to, že existuje bezpečný systém

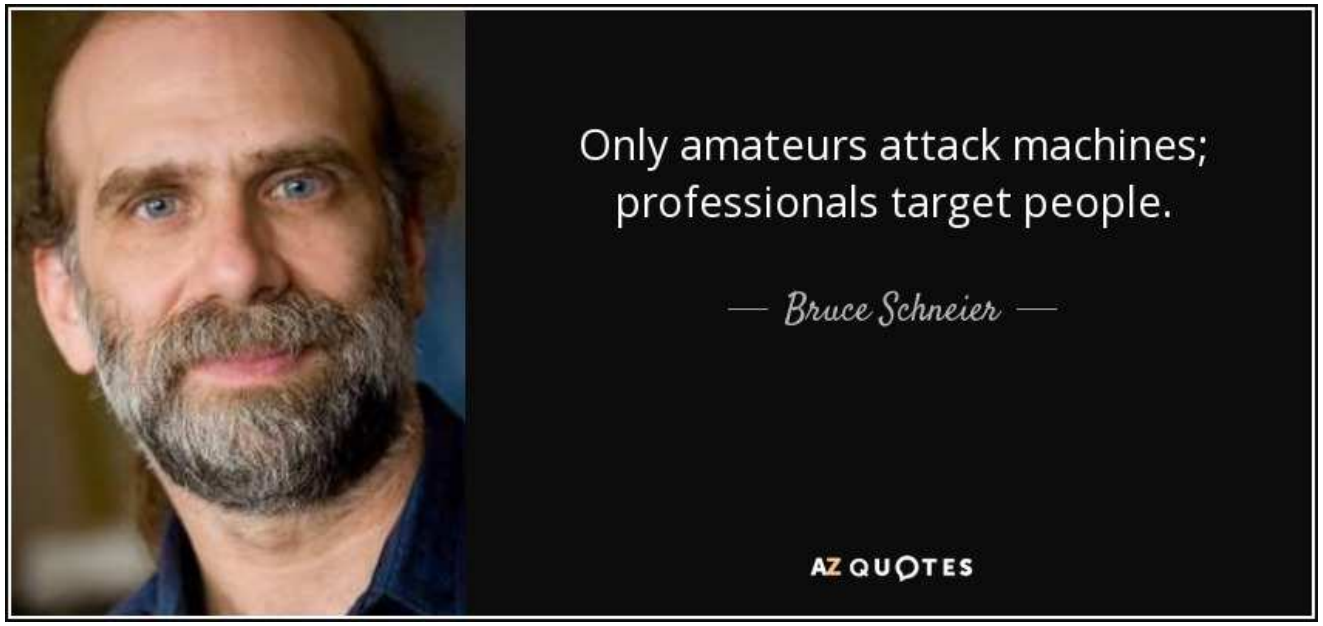


Při návrhu stavbě i provozu počítejme s tím,
že k narušení dojde a snažme se minimalizovat
možné škody již v samém návrhu systému

Nezapomínejme na zdravý selský rozum

Systém je tak bezpečný, jak bezpečný je jeho nejslabší článek

Bezpečnost – nejslabší článek



Pracujete s ním dostatečně?

Přehled jednotlivých oblastí bezpečnosti

- Vše souvisí se vším a pokud se jedno ošidí, tak se to projeví ve všech souvisejících oblastech

JAK? Se implementuje bezpečnost?

- Posouzení stávající úrovně bezpečnosti
  - Z hlediska legislativy (současné i připravované)
  - Z hlediska reálných hrozeb (i bez ohledu na legislativu)
  - Z hlediska aktiv, která je třeba chránit
- Návrh úprav pro zvýšení bezpečnosti
  - Definice reálných potřeb
  - Definice reálných možností (včetně finančních)
  - Strategie bezpečnosti
- Zavedení technických a organizačních bezpečnostních opatření
  - ZKB vhodnou pomůckou

Životní cyklus řízení KB

- Demingův cyklus nebo PDCA Cyklus
  - metoda postupného zlepšování

Organizační bezpečnostní opatření

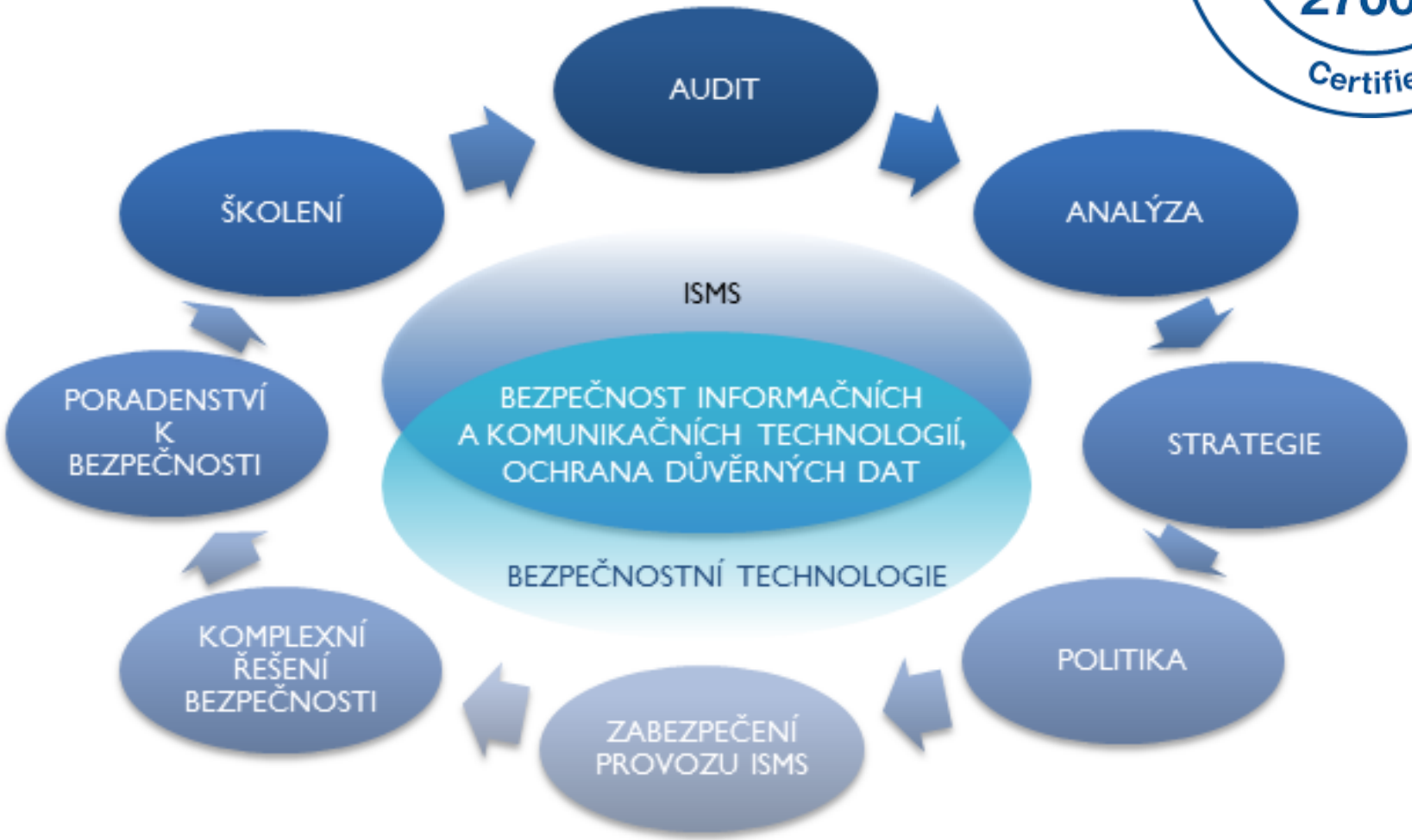
- § 3 Systém řízení bezpečnosti informací
- § 4 Řízení rizik
- § 5 Bezpečnostní politika
- § 6 Organizační bezpečnost
- § 7 Stanovení bezpečnostních požadavků pro dodavatele
- § 8 Řízení aktiv
- § 9 Bezpečnost lidských zdrojů
- § 10 Řízení provozu a komunikací
- § 11 Řízení přístupu a bezpečné chování uživatelů
- § 12 Akvizice, vývoj a údržba
- § 13 Zvládání KB událostí a incidentů
- § 14 Řízení kontinuity činností
- § 15 Kontrola a audit

Technická bezpečnostní opatření

- § 16 Fyzická bezpečnost
- § 17 Nástroj pro ochranu integrity komunikačních sítí
- § 18 Nástroj pro ověřování identity uživatelů
- § 19 Nástroj pro řízení přístupových oprávnění
- § 20 Nástroj pro ochranu před škodlivým kódem
- § 21 Nástroj pro zaznamenávání činností KII a VIS
- § 22 Nástroj pro detekci KBU
- § 23 Nástroj pro sběr a vyhodnocení KBU
- § 24 Aplikační bezpečnost
- § 25 Kryptografické prostředky
- § 26 Nástroje pro zajištění vysoké úrovně dostupnosti
- § 27 Bezpečnost průmyslových a řídicích systémů

KB je nikdy nekončící sled činností

- Systém řízení bezpečnosti informací



Co je tedy to nejdůležitější a čím začít

- Zálohujte vaše data, ať máte z čeho obnovovat.
- Patchujte, ať omezíte známé bezpečnostní mezery.
- Odhalte průnik včas, ať je útočník rychle odhalen.
- Vyzkoušejte si incident, ať se rychle obnoví provoz.
- Školte uživatele, ať znají pravidla bezpečného chování.
- Omlazujte infrastrukturu, ať máte šanci obrany.
- Důvěřujte, ale prověřujte bezpečnost šifrované komunikace.
- Připravte se na prevenci, detekci i reakci.
- Mějte přehled o nejnovějších fintách hackerů.
- Prověřte svého IT manažera, zda tyto zásady dodržuje.

Děkujeme za pozornost

KYBEZ Platforma kybernetické bezpečnosti