Michal Andrejčák, Automatizace rozvoden, Ampér 2013

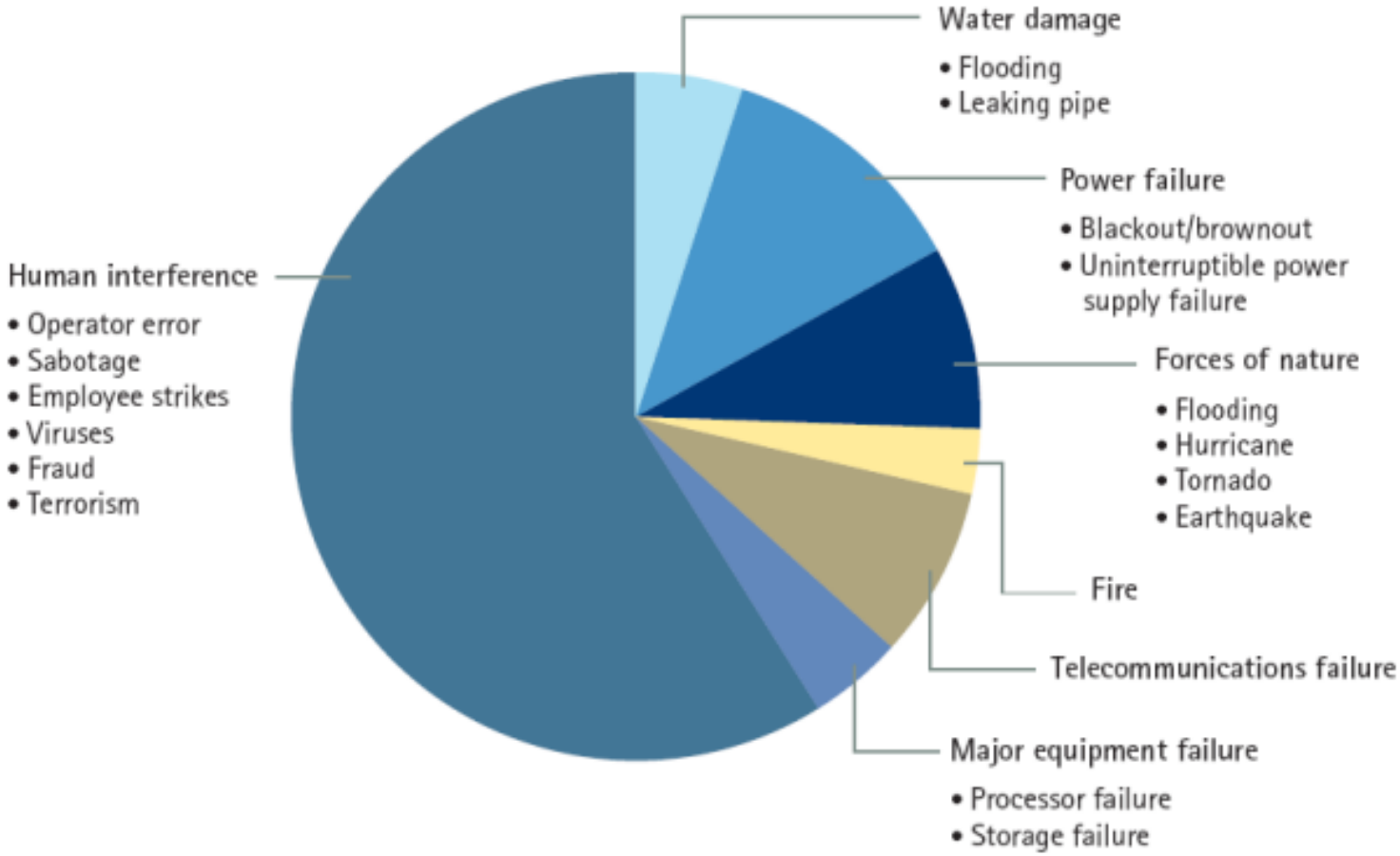
Kybernetická bezpečnost
Ochrana proti sílící hrozbě

Kybernetická bezpečnost
Co to je?

V kontextu informačních technologií, pojem bezpečnost znamená Kybernetická bezpečnost (Cyber Security).

Kybernetická bezpečnost je skupina technologií, procesů a postupů určených na ochranu sítí, počítačů, programů a dat před útoky, poškozením anebo neoprávněným přístupům.

Kybernetická bezpečnost
Nejčastější příčiny výpadků



Source: Accenture survey

Svět se mění
Hacktivismus

„Tito lidé jsou vysoce talentovaní a neuvěřitelně ambiciózní. V mnoha případech nejsou jejich činy motivované ziskem. Je to spíše otázka: Podívejte co dokážu“

- Patrick Peterson, Cisco senior security analyst

„Hacktivismus je přeměnou tradičního hackingu.”

„Nejdříve, vnikali hackeři do systémů pro zábavu. Potom, to bylo pro odměnu anebo finanční zisk. Dnes je to často o vyslaní zprávy a nikdy nemůžete vědět co z vás udělá cíl. V současnosti bráníme novou doménu.”

- John N. Stewart, Cisco chief security officer

Svět se mění
Hrozba zevnitř

Jérôme Kerviel - obchodník největší francouzské banky Societe General využil svoje IT znalosti k oklamání bezpečnostních opatření a kontrol což vedlo ke škodám ve výšce $7.2 miliard dolarů.

Kerviel předtím pracoval v IT oddělení banky a měl tak podrobné znalosti o jejich systémech a procedurách. Mezi triky, které na základě interní zprávy banky používal na zakrytí svých aktivit byli falešné e-mailové správy na doložení chybějících transakcí a „vypůjčování si“ přihlašovacích údajů kolegů pro provedení obchodů v jejich měnách.

Svět se mění
Hrozba zevnitř

Rajendrasinh Makwana, který byl dočasným smluvním pracovníkem, byl na podzim 2008 obviněný z vložení škodlivého skriptu „serverové bomby“ na servery Fannie Mae.

Skript se měl spustit 31. ledna 2009 a měl způsobit vyřazení zpráv z monitorování a záznamů, smazat administrátorská hesla na přibližně 4 000 serverech Fannie, následně vymazat všechny údaje a zálohy údajů a nahradit tyto údaje nulami čímž měl společnosti způsobit miliónové škody. Před spuštěním byl skript náhodně odhalený zaměstnancem Fannie Mae.

Svět se mění
Mezinárodní průmyslová špionáž

- Útvar 61398 armády ČLR v Šanghaji
- K budově v níž sídlí vede mnoho „digitálních“ stop zanechaných po různých hackerských útocích
- Různé cíle
  - Technologické plány
  - Popisy výrobních procesů
  - Výsledky klientských testů
  - Uživatelská jména a hesla
- Více ve zprávě firmy Mandiant

  (http://intelreport.mandiant.com/)

Svět se mění
I podniky v ČR mohou být cílem útoků

4.3. 2013

- DDoS útok proti velkým českým zpravodajským serverům

5.3. 2013

- Seznam.cz a další

6.3. 2013

- Banky včetně ČNB

7.3. 2013

- Mobilní operátoři

11.3. 2013

- UniCredit banka (včetně e-bankingu)

Svět se mění
I technologické systémy jsou v ohrožení

STUXNET

- Počítačový červ zpočátku se skrytě šíří
- Specializovaný kód navržený pro zasáhnutí systémů řídících specifické průmyslové procesy

DUQU

- Sbírá informace použitelné pro útoky na průmyslové řídicí systémy

FLAME

- Slouží ke kybernetické špionáži
- Šíří se sítí nebo pomocí USB disků
- Zaznamenává aktivitu uživatele, komunikaci, obrazovky atd.

Svět se mění
Vzájemné propojení systémů

- Historicky byly systémy a sítě fyzicky a logicky nezávislé a oddělené
- Existovalo málo interakcí a spojení mezi systémy a jinými částmi infrastruktury
- Díky technologickému pokroku se systémy stávají propojenými a automatizovanými
- Propojení systémů je realizováno pomocí sítí, komunikačních zařízení a počítačů
- Vazby stírají tradiční bezpečnostní hranice

Svět se mění
Legislativní požadavky

- V různých zemích existují různé zákonné normy zavazující i soukromé firmy působící v oblastech „kritických“ pro chod státu ke spolupráci se státními orgány a k zajištění určité úrovně kybernetické bezpečnosti
- Je otázkou času, kdy se podobné zákonné požadavky objeví v ČR
- Národní Bezpečnostní Úřad má do roku 2015 vybudovat „ Národní centrum kybernetické bezpečnosti“. Mezi cíle m.j. patří:
  - Systém sdílení informací a včasného varování
  - Koordinaci mezi státními a soukromými subjekty k prevenci útoků a opatření k nápravě škod
  - Pravidla pro řešení mimořádných stavů (stav kybernetického nebezpečí)
- Další podrobnosti: „Věcný záměr zákona o kybernetické bezpečnosti“ (http://www.vlada.cz)

Svět se mění
Požadavky zákazníků ABB (a jiných)

- Požadavky na bezpečnost vzrůstají
  - Zvýšení odolnosti systémů
  - Uzavření nepoužívaných rozhraní
  - Správa opravných balíčků
  - Ochrana proti škodlivému SW (Malware)
  - Bezpečná komunikace
  - Bezpečnostní audity
  - Implementace mezinárodních standardů (IEC 62351, ISO 27000, NERC CIP)

Kybernetická bezpečnost pro automatizaci rozvoden
Strategie ABB

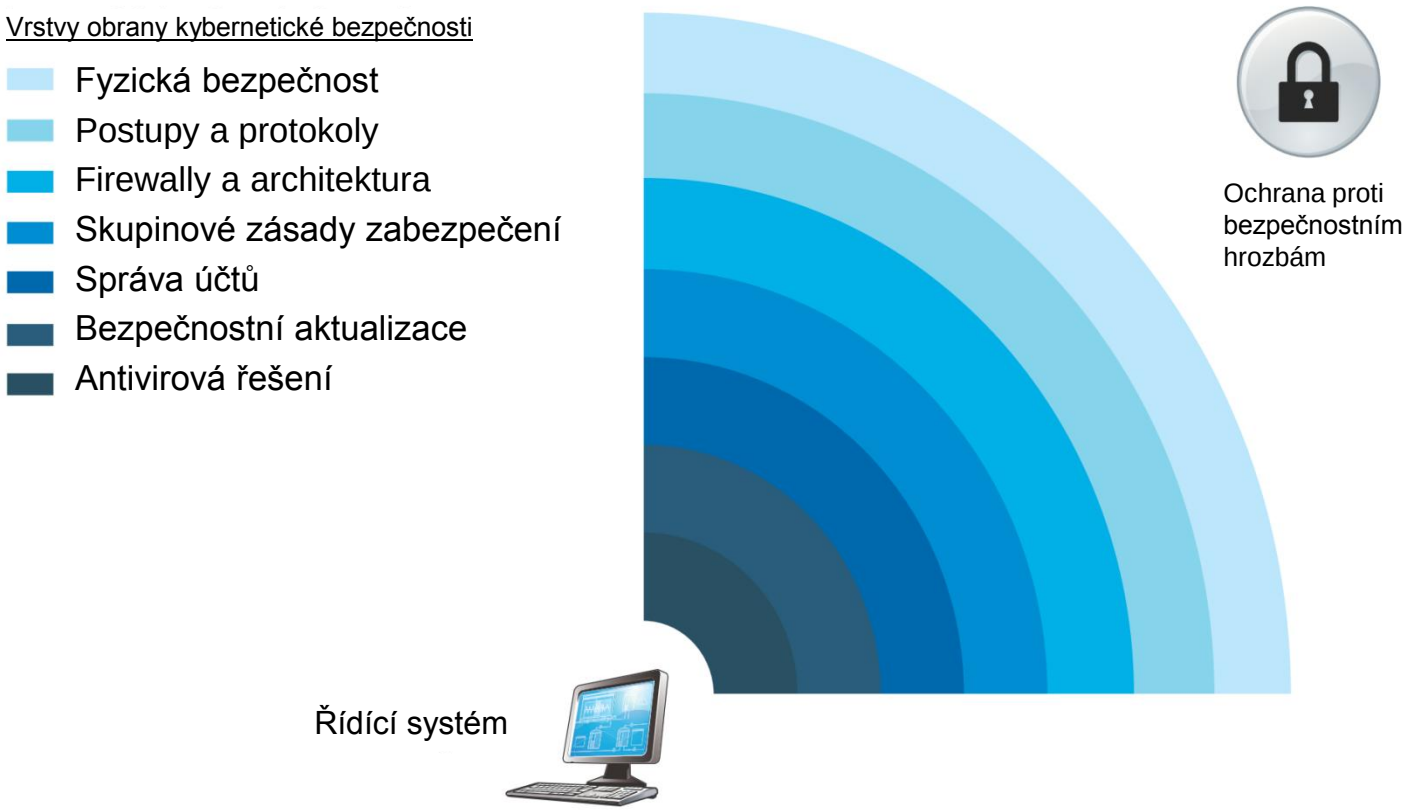


ABB používá strategii „obrany do hloubky“, která zajišťuje různé vrstvy ochrany

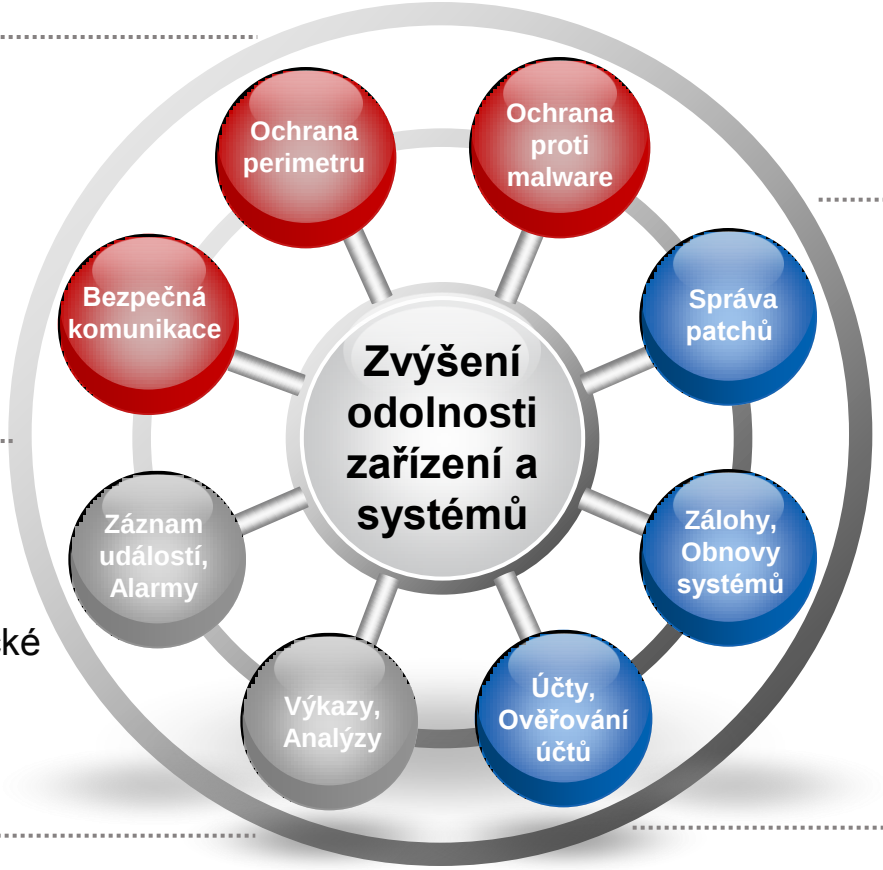
Kybernetická bezpečnost pro automatizaci rozvoden
Zvýšení odolnosti zařízení a systémů

Ochrana

Proti hrozbám systémům automatizace rozvoden

Monitoring

Bezpečnostní a diagnostické informace v reálném čase



Správa

Kritické aktivity jako konfigurování, změny a aplikace záplat (patchů)

Kybernetická bezpečnost pro automatizaci rozvoden
Modulární řešení

Integrované Firewally
Samostatné Firewally

VPN a IPSec

Zaznamenávání bezpečnostních událostí , mapování do alarmů
Správa událostí

Analýza stop

Antivirová ochrana

Ověřování záplat (patchů)
Centralizované nasazování záplat (patchů)

Ruční zálohování souborů
Manuální /automatické zálohování obrazů disků

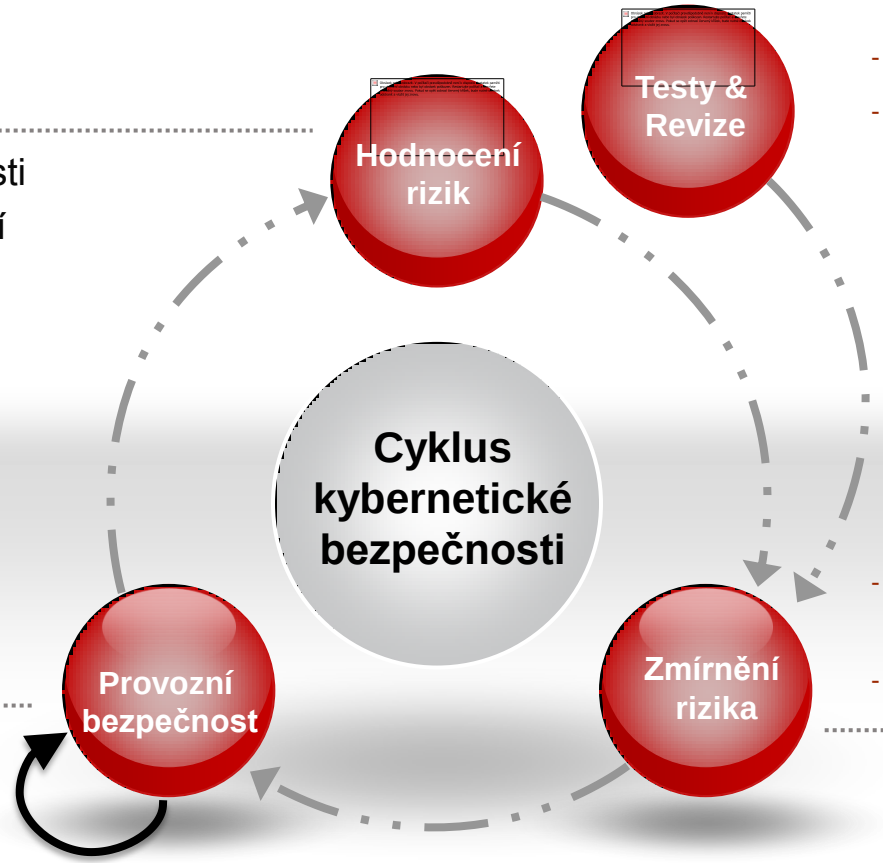
Správa uživatelů, silná hesla

Nabízené řešení
Základ **Rozšířené** **Pokročilé**

Monitoring Správa Ochrana

Kybernetická bezpečnost pro automatizaci rozvoden
Zachování / zvýšení úrovně kybernetické bezpečnosti

- Hrozby / Pravděpodobnosti
- Zranitelná místa / Zneužití
- Majetek / Dopad
- Rizika / Protiopatření

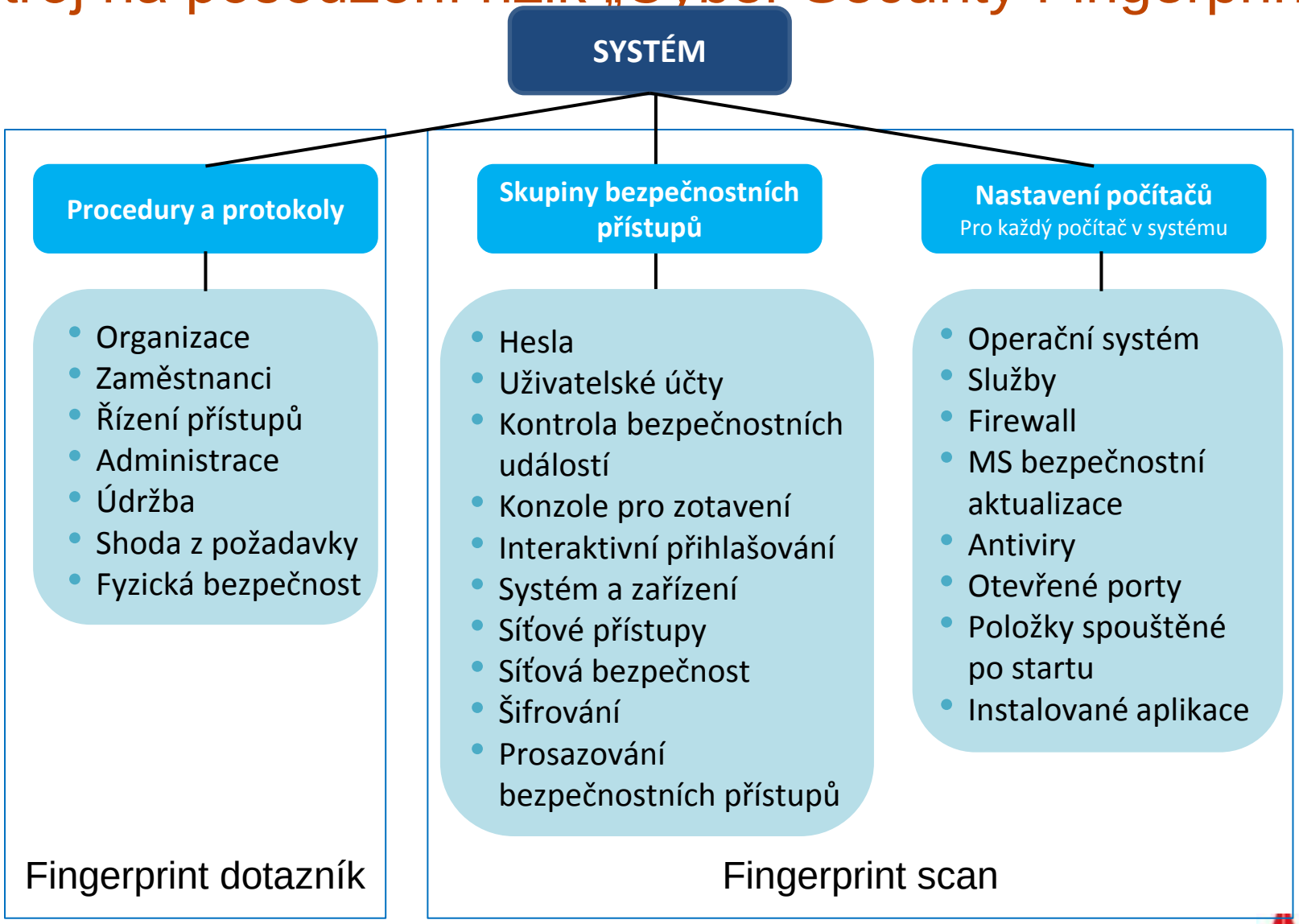


- Skenování
- Audit řízení

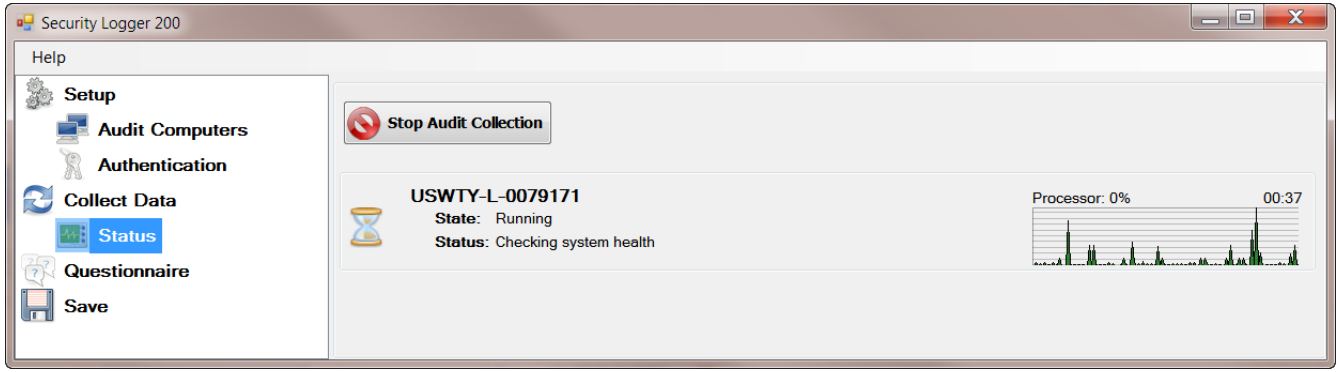
- Provedení zabezpečení
- Další řízení

- Záplaty (Patche)
- Zvládání incidentů
- Trénink

Kybernetická bezpečnost pro automatizaci rozvoden
Nástroj na posouzení rizik „Cyber Security Fingerprint“

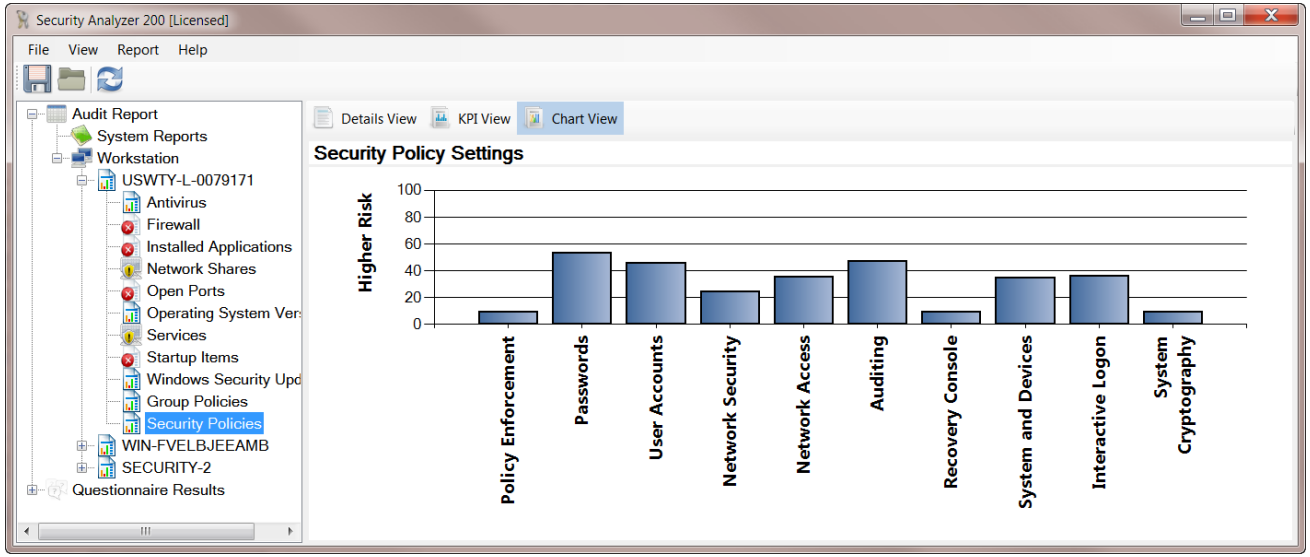


Cyber Security Fingerprint
Nástroj „Security Logger Data Collection“



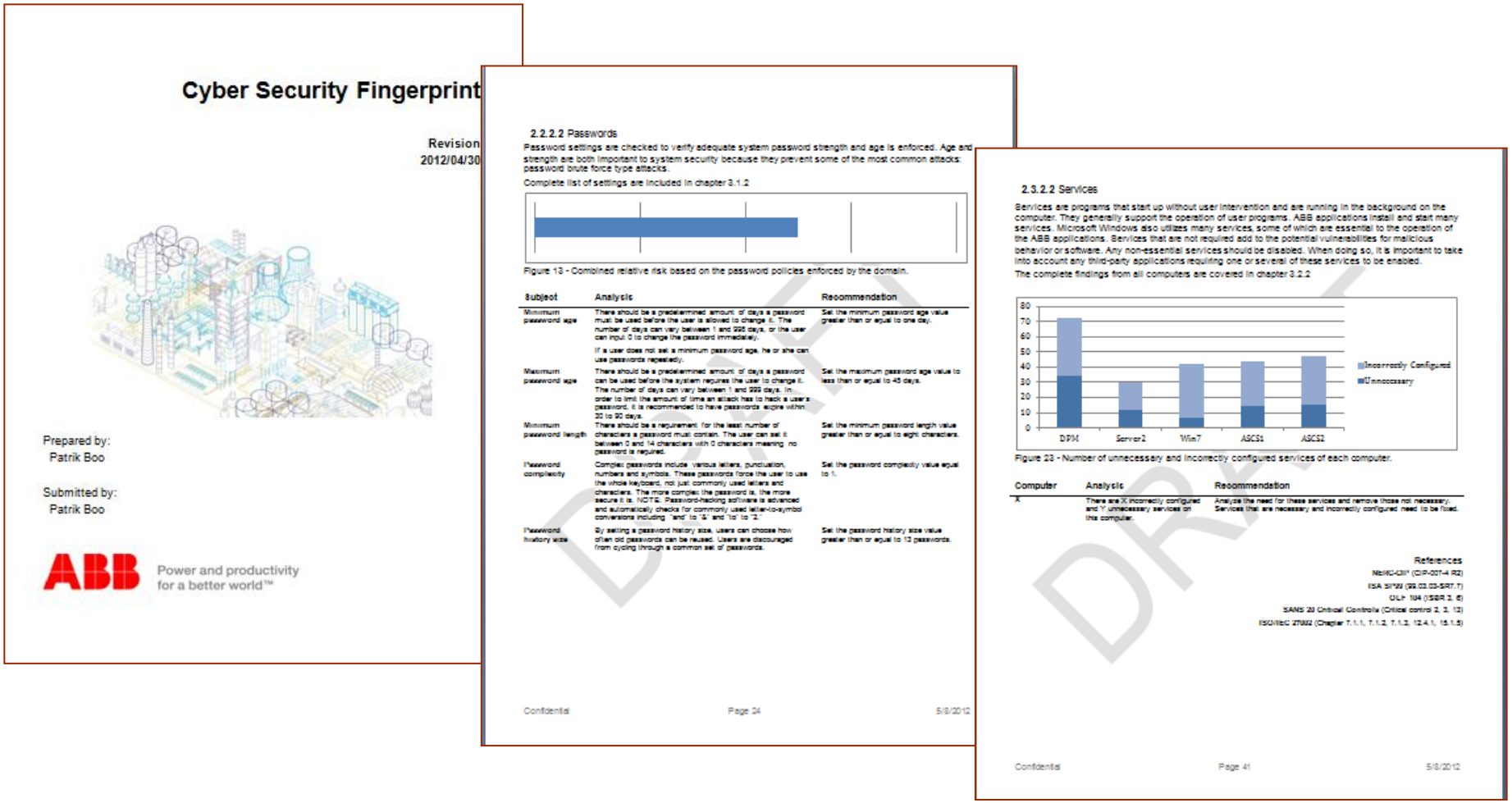
- Shromažďuje data bez omezení provozu
- Není třeba instalace
- Shromážděná data jsou uložena v šifrovaných souborech
- Slouží jako podpora při konzultacích s klíčovými uživateli systému
- Více než 90% úspora času v porovnání s ručním shromažďováním dat

Cyber Security Fingerprint
Nástroj „Security Analyzer“



- Analyzuje shromážděná data
- Jediný nástroj schopný číst šifrované soubory
- Analyzér porovnává shromážděná data s profilem specifickým pro danou oblast

Cyber Security Fingerprint
Výkaz s doporučeními a akčním plánem



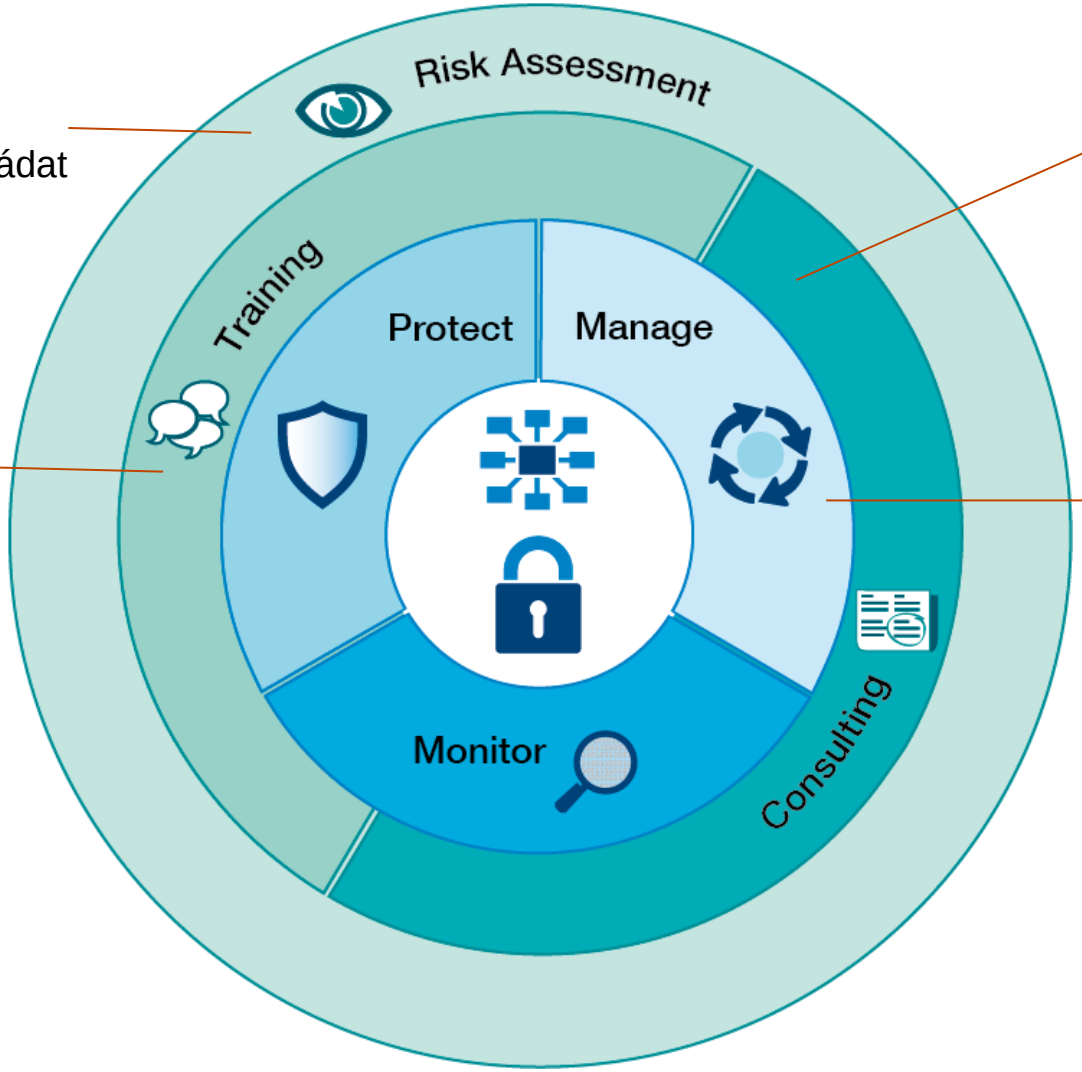
Kybernetická bezpečnost pro automatizaci rozvoden
Nabídka služeb

- Ochrana systémů proti potenciální kybernetické bezpečnostní hrozbě
- Analýza stávajícího stavu s využitím nástroje Cyber Security Fingerprint
  - Identifikace potenciálních rizik
  - Hodnocení rizik
  - Návrh řešení
    - Základní řešení
    - Rozšířené řešení
    - Pokročilé řešení

Kybernetická bezpečnost pro automatizaci rozvoden
Technická řešení ve spojení se službami

- **(Znovu-)Posouzení rizik**:
  Znám rizika v mém systému a umím nakládat s mým systémem?

- **Školení**:
  Může systémový uživatel používat kyberneticko bezpečnostní technologie?



- **Konzultace:**
  Jsou zásady a postupy v souladu s předpisy a proveditelné?

- **Další funkce pro instalovanou základnu**:
  Nabídka dalších technických řešení pro kybernetickou bezpečnost

Power and productivity
for a better world™