



Michal Andrejčák, Automatizace rozvoden, Ampér 2013

Kybernetická bezpečnost Ochrana proti sílící hrozbě

Kybernetická bezpečnost

Co to je?

Cyber Security

The need for safeguarding against cyber crime and cyber terrorism has never been greater.

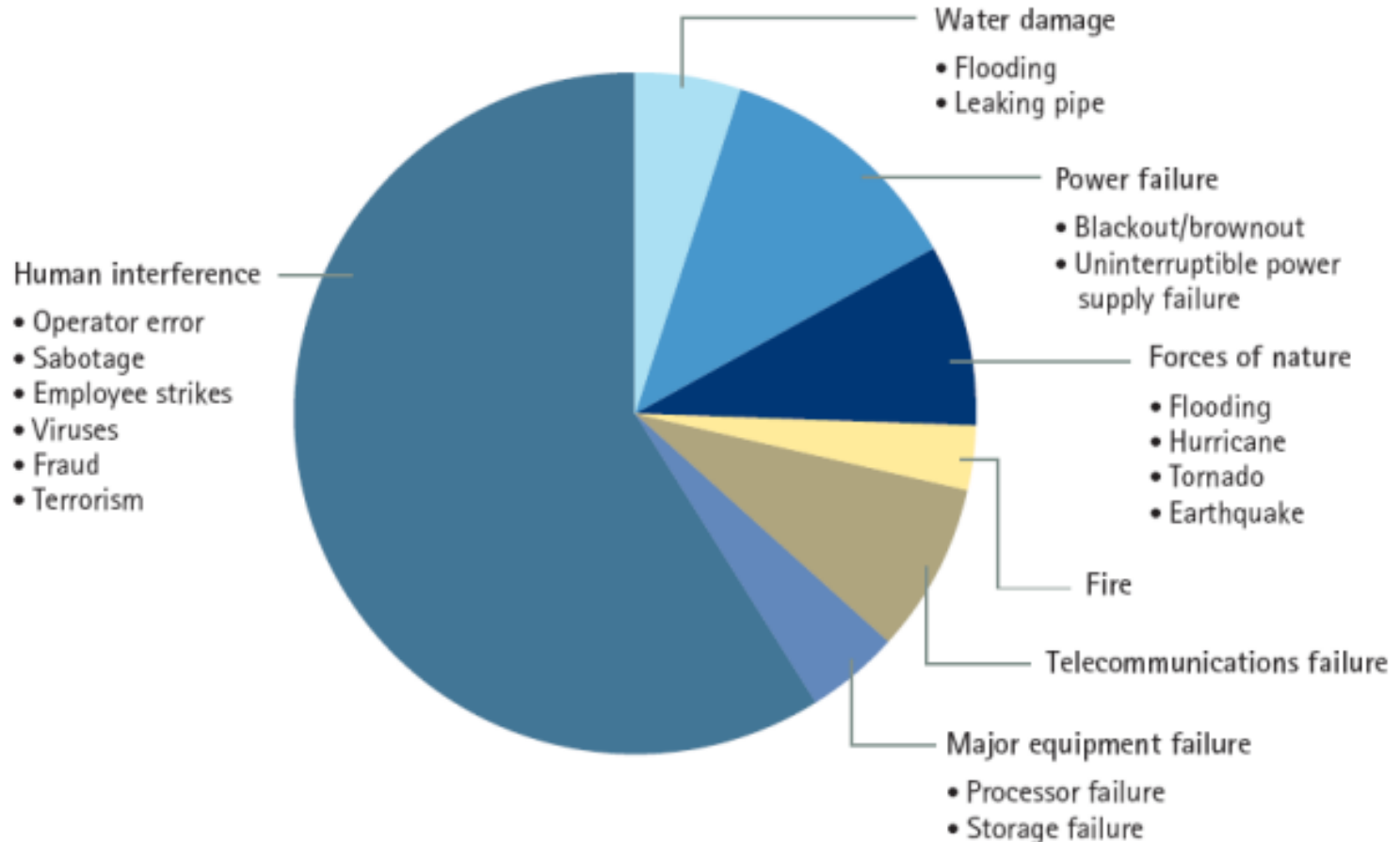


V kontextu informačních technologií, pojem bezpečnost znamená **Kybernetická bezpečnost (Cyber Security)**.

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 vyslání 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



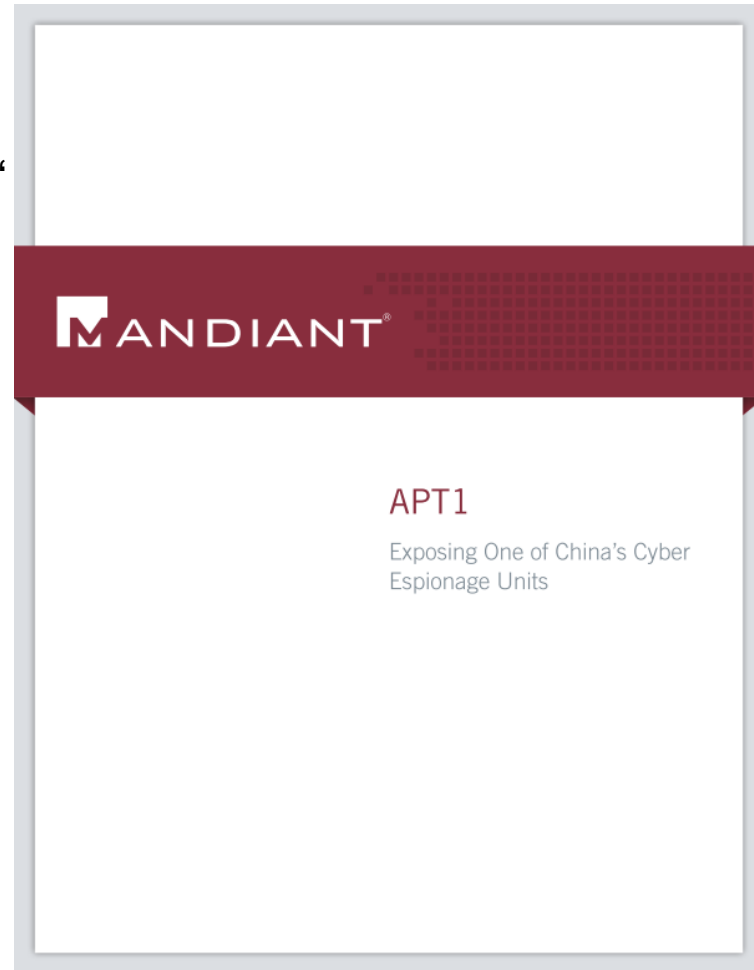
Rajendrasinh Makwana, který byl dočasným smluvním pracovníkem, byl na podzim 2008 obviněn z vložení škodlivého skriptu „serverové bomby“ na servery Fannie Mae.

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 šířící
- 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 rozvodů

Strategie ABB

Vrstvy obrany kybernetické bezpečnosti

- Fyzická bezpečnost
- Postupy a protokoly
- Firewally a architektura
- Skupinové zásady zabezpečení
- Správa účtů
- Bezpečnostní aktualizace
- Antivirová řešení



Ochrana proti
bezpečnostním
hrozbám

Řídicí systém



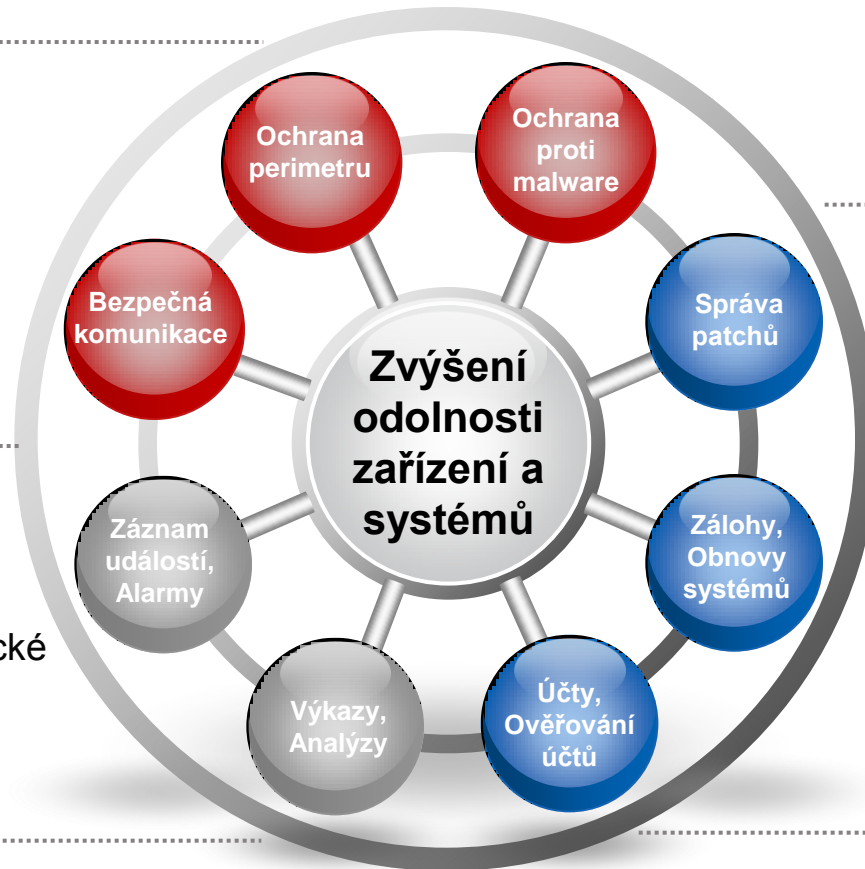
ABB používá strategii „obranu do hloubky“, která zajišťuje různé vrstvy ochrany

Kybernetická bezpečnost pro automatizaci rozvodů

Zvýšení odolnosti zařízení a systémů

Ochrana

Proti hrozbám systémům automatizace rozvodů



Monitoring

Bezpečnostní a diagnostické informace v reálném čase

Správa

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

Kybernetická bezpečnost pro automatizaci rozvodů

Modulární řešení

Integrované Firewally
Samostatné Firewally

VPN a IPSec

Zaznamenávání
bezpečnostních událostí,
mapování do alarmů
Správa událostí

Analýza stop

Nabízené řešení

Základ

Rozšířené

Pokročilé



Antivirová ochrana

Ověřování záplat (patchů)
Centralizované nasazování
záplat (patchů)

Ruční zálohování souborů
Manuální /automatické
zálohování obrazů disků

Správa uživatelů, silná hesla

● Monitoring

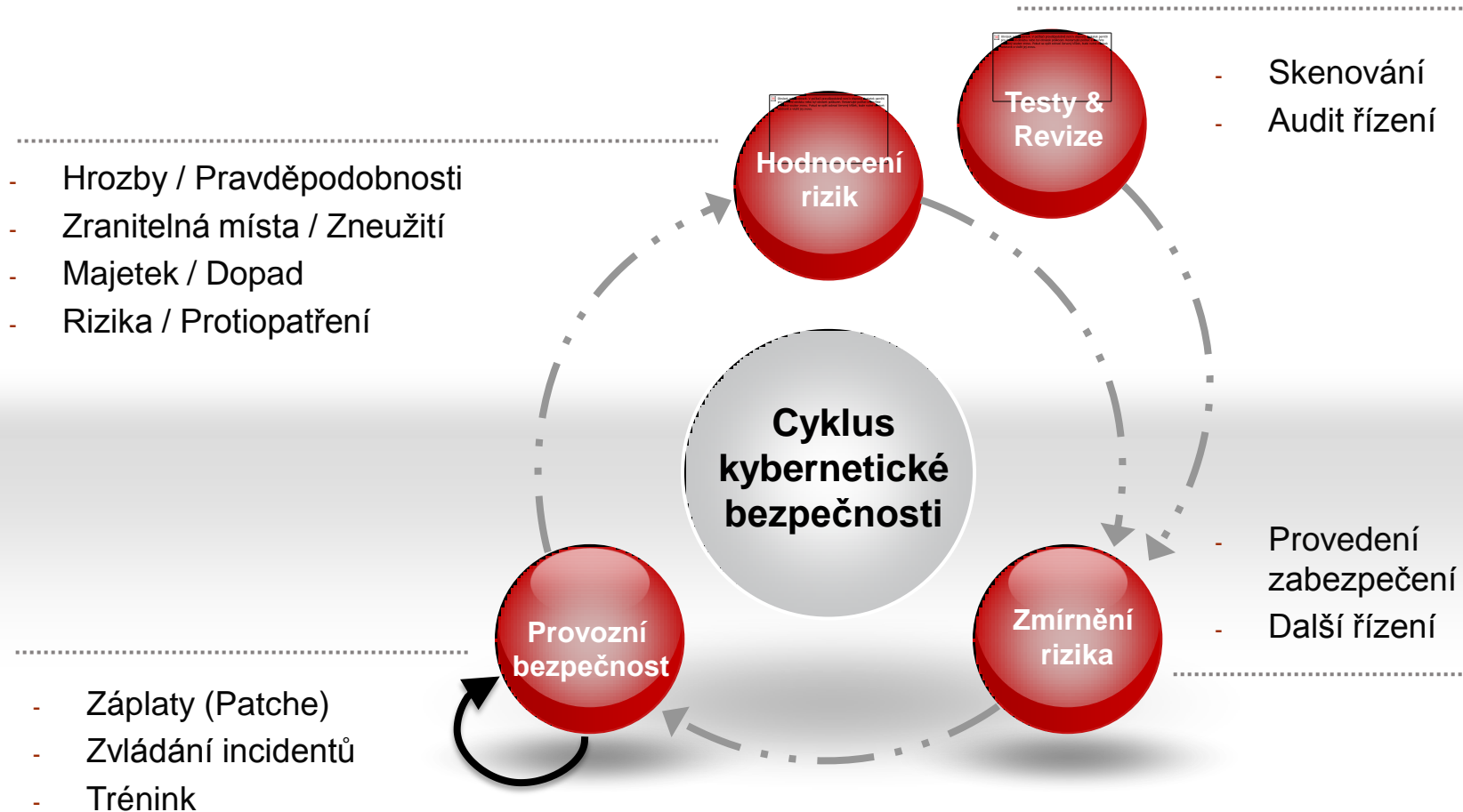
● Správa

● Ochrana



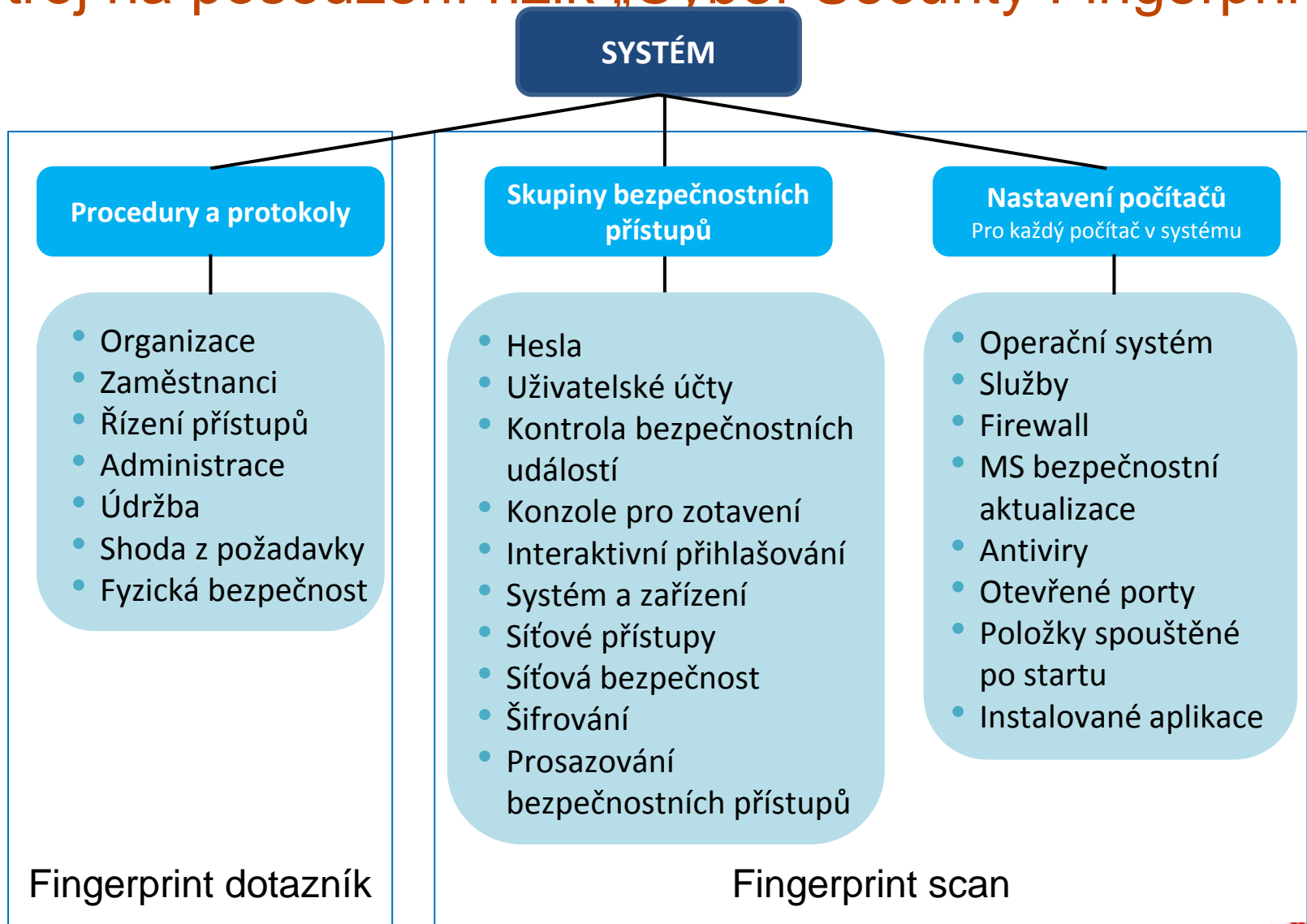
Kybernetická bezpečnost pro automatizaci rozvodů

Zachování / zvýšení úrovně kybernetické bezpečnosti



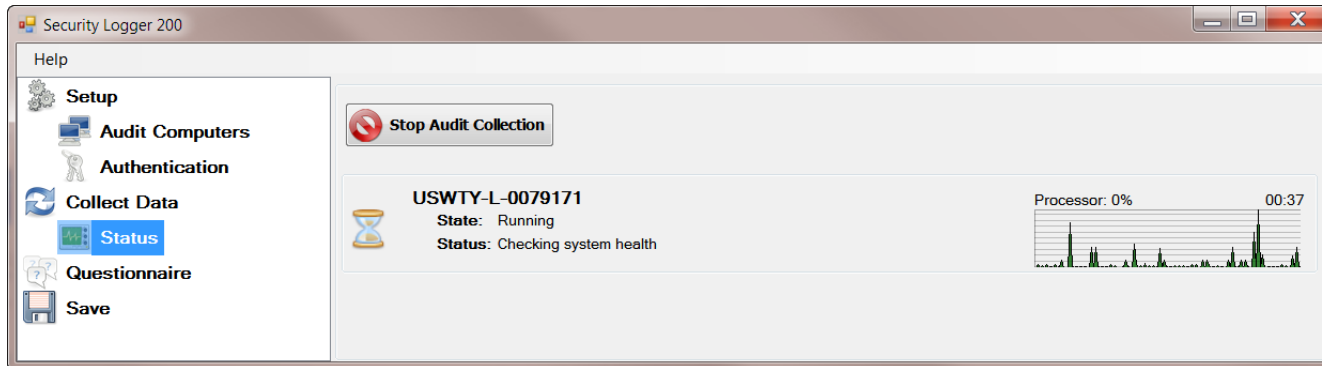
Kybernetická bezpečnost pro automatizaci rozvodů

Nástroj na posouzení rizik „Cyber Security Fingerprint“



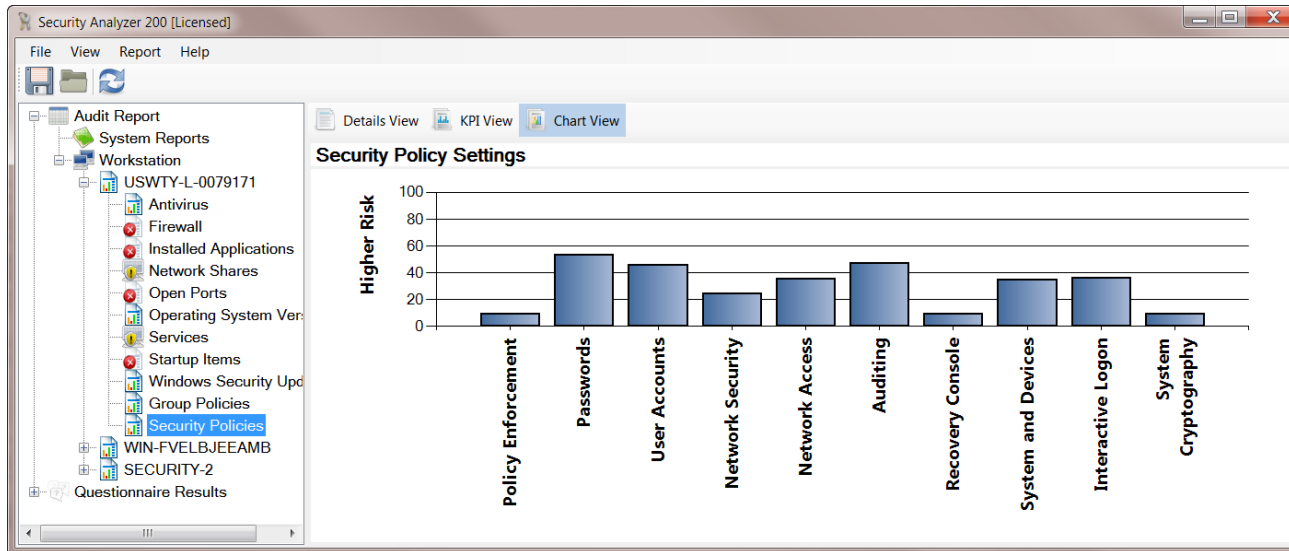
Cyber Security Fingerprint

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
- Analyzátor porovnává shromážděná data s profilem specifickým pro danou oblast

Cyber Security Fingerprint

Výkaz s doporučeními a akčním plánem

Cyber Security Fingerprint

Revision
2012/04/30



Prepared by:
Patrik Boo

Submitted by:
Patrik Boo



2.2.2.2 Passwords

Password settings are checked to verify adequate system password strength and age is enforced. Age and strength are both important to system security because they prevent some of the most common attacks: password brute force type attacks.

Complete list of settings are included in chapter 3.1.2

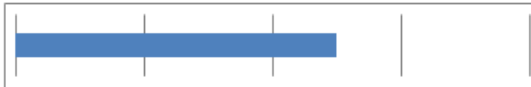


Figure 13 - Combined relative risk based on the password policies enforced by the domain.

Subject	Analysis	Recommendation
Minimum password age	There should be a predetermined amount of days a password must be used before the user is allowed to change it. The number of days can vary between 1 and 999 days, or the user can input 0 to change the password immediately. If a user does not set a minimum password age, he or she can use passwords repeatedly.	Set the minimum password age value greater than or equal to one day.
Maximum password age	There should be a predetermined amount of days a password can be used before the system requires the user to change it. The number of days can vary between 1 and 999 days. In order to limit the amount of time an attack has to hack a user's password, it is recommended to have passwords expire within 30 to 90 days.	Set the maximum password age value to less than or equal to 45 days.
Minimum password length	There should be a requirement for the least number of characters a password must contain. The user can set it between 0 and 14 characters with 0 characters meaning no password is required.	Set the minimum password length value greater than or equal to eight characters.
Password complexity	Complex passwords include various letters, punctuation, numbers and symbols. These passwords force the user to use the whole keyboard, not just commonly used letters and characters. The more complex the password is, the more secure it is. NOTE: Password-hacking software is advanced and automatically checks for commonly used letter-to-symbol conversions including "and" to "4" and "to" to "7".	Set the password complexity value equal to 1.
Password history size	By setting a password history size, users can choose how often old passwords can be reused. Users are discouraged from cycling through a common set of passwords.	Set the password history size value greater than or equal to 13 passwords.

Confidential

Page 24

5/8/2012

2.3.2.2 Services

Services are programs that start up without user intervention and are running in the background on the computer. They generally support the operation of user programs. ABB applications install and start many services. Microsoft Windows also utilizes many services, some of which are essential to the operation of the ABB applications. Services that are not required add to the potential vulnerabilities for malicious behavior or software. Any non-essential services should be disabled. When doing so, it is important to take into account any third-party applications requiring one or several of these services to be enabled. The complete findings from all computers are covered in chapter 3.2.2

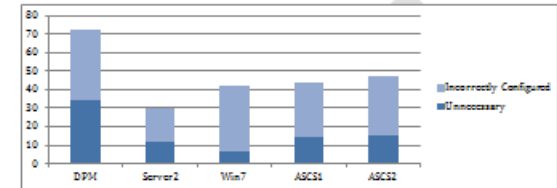


Figure 23 - Number of unnecessary and incorrectly configured services of each computer.

Computer	Analysis	Recommendation
A	There are 30 incorrectly configured and 7 unnecessary services on the computer.	Analyze the need for these services and remove those not necessary. Services that are necessary and incorrectly configured need to be fixed.

References

MeiNG-011 (CI)-001-4 R2
ISA 9000 (20.03.03-SRT.7)
CULP 104 (SAR.2.6)
SANS 20 Critical Controls (Critical control 2, 2, 12)
ISO/IEC 27002 (Chapter 7.1.1, 7.1.2, 7.1.3, 12.4.1, 15.1.5)

Confidential

Page 41

5/8/2012

Kybernetická bezpečnost pro automatizaci rozvodů

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 rozvodů

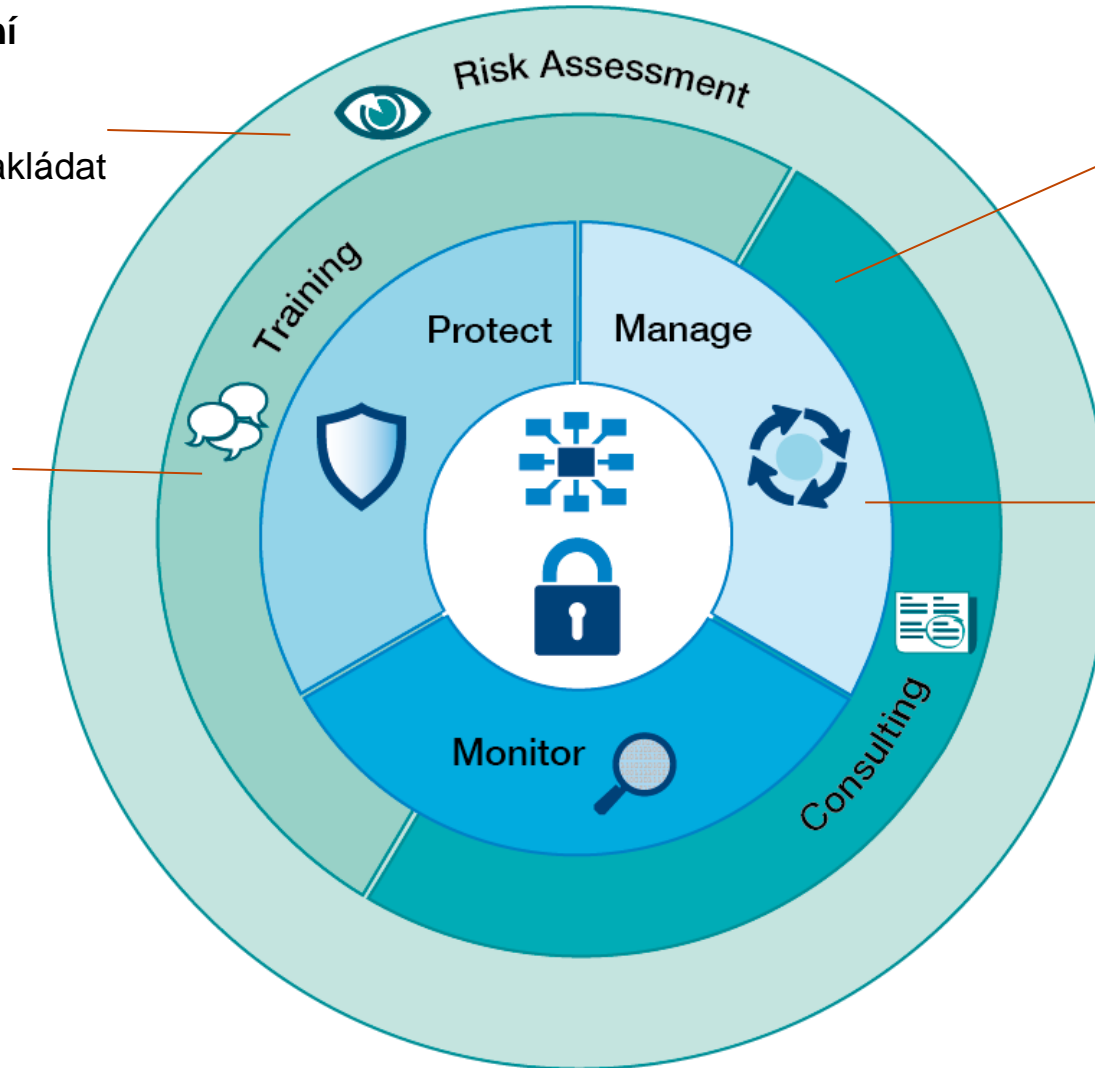
Technická řešení ve spojení se službami

- **(Znovu-)Posouzení rizik:**

Znám rizika v mém systému a umím nakládat s mým systémem?

- **Školení:**

Může systémový uživatel používat kybernetickou bezpečnostní technologii?



- **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™

