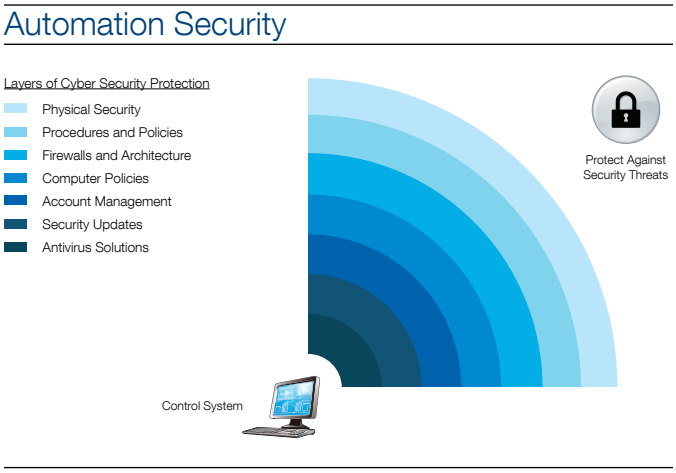
Divize Procesní automatizace

Cyber Security Fingerprint
Chrání řídicí systémy před potenciálními bezpečnostními hrozbami

ABB Cyber Security Fingerprint odkrývá silné a slabé stránky ve struktuře procesního řídicího systému pro ochranu před kybernetickým útokem. Nejprve jsou shromážděna data všech kritických systémových konfigurací a s pomocí analytických softwarových nástrojů ABB porovnána s osvědčenými postupy a nejlepšími řešeními ověřenými praxí. Součástí shromažďování dat je také analýza operačních procesů. Výsledná zpráva poskytuje detailní doporučení pro omezení zranitelnosti kybernetickými útoky a zároveň pomáhá rozvíjet udržitelnou bezpečnostní strategii se zaměřením na procesní řídicí systémy.



Současné procesní řídicí systémy jsou více než kdykoli předtím propojeny do rozsáhlejších sítí, vzrůstá mobilita zařízení a s tím souvisí nová rizika ohrožující jejich dostupnost a bezpečnost. Ať už to byl nebezpečný útok, např. typu počítačového červa Stuxnet* nebo neúmyslné narušení bezpečnosti, jako například otevření infikovaného souboru zaměstnancem, potenciální dopad takové události může vést k veřejnému ohrožení nebo ohrožení bezpečnosti zaměstnanců, výrobním ztrátám, nedodržení zákonných požadavků, poškození životního prostředí či samotného zařízení.

*Stuxnet je počítačový červ zachycený v červnu 2010, který se šířil v prostředí Microsoft Windows a cílem útoku byl průmyslový software a řídicí systémy. Šlo o první objevený malware, který vyhledával a poškozoval funkčnost průmyslových řídicích systémů.

Užitek

– zvýšení bezpečnosti výrobního podniku, lidí a dat
– omezení možnosti pro narušení systému a zastavení výroby
– komplexní pohled na stav kybernetické bezpečnosti v provozu
– vylepšení procesu zmírňování rizik kybernetických útoků
– porovnání se zavedenými standardy a osvědčenými postupy, takzvaná „the best practice“
– pevný základ pro vybudování udržitelné strategie pro kybernetickou bezpečnost

Vlastnosti

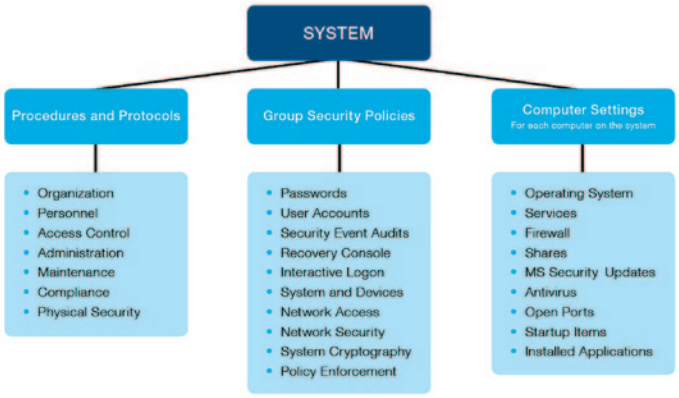
– přístup k bezpečnostním expertům ABB
– detailní zpráva o stavu včetně doporučení pro uzavření bezpečnostních děr
- softwarový nástroj pro srovnávání stavu zabezpečení provozu s nejzabezpečenějšími řešeními v daném segmentu (jeden z nejlepších ve své třídě)
– standardní opakovatelný postup, který zajistí konzistentní analýzu napříč systémy a výrobními provozy
– možnost rozšíření služby „Cyber Security Fingerprint“ na pravidelnou plánovanou kontrolu zabezpečení a sledování potenciálních událostí s vlivem na kybernetickou bezpečnost. Nejefektivnější cestou je pak zavedení průběžného sledování bezpečnosti prostřednictvím služby **ABB ServicePort**.

Cyber Security Fingerprint odhaluje nedostatky a tím snižuje bezpečnostní rizika, která by mohla ohrozit zaměstnance, majetek, provozuschopnost zařízení nebo kompromitovat cenná data. Přístup ABB je založen na porovnání Vaší bezpečnostní politiky s průmyslovými standardy, stanovuje hranice a zajistí, že Vaše procesní řídicí systémy budou zabezpečeny několika vrstvami ochrany.

Popis služby

ABB Cyber Security Fingerprint je neinvazivní služba aplikovatelná na jakýkoliv procesní řídicí systém a sestává z třístupňového sběru dat. Rychlý SW nástroj ABB, Security Logger (SEL100), shromáždí informace a systémová nastavení z řídicího systému a počítačů podnikové sítě.

Tyto informace jsou spolu s údaji získanými ze strukturovaných interview s klíčovými pracovníky provozu použity pro porovnání systému a stavu podnikového zabezpečení s nejlepší



3 klíčové komponenty systému pro stanovení ukazatelů výkonnosti

průmyslovou praxí a standardy, jako je ISO/IEC27000 a ISA99. Následně spuštěný ABB Security Analyzer (SEA100) vypočítá klíčové ukazatele výkonnosti (KPI), které zdůrazňují silné a slabé stránky kybernetické bezpečnosti procesního řídicího systému.

Indikátory klíčových ukazatelů výkonnosti (KPI)

Po kontrole a sběru dat ABB určí KPI pro následující oblasti:
– **Procedures and Protocols:** kvalitativní analýza, která indikuje, jak je organizace zabezpečena s pomocí písemných pokynů a nařízení
– **Group Security Policies:** omezení uplatněná v systému, vyžadovaná centrálním serverem nebo implementovaná na jednotlivých počítačích
– **Computer Settings:** nastavení a aplikace na jednotlivých počítačích které jsou součástí systému

Reportování

Po vyhodnocení je učiněn závěr a připraven report. Na základě zmíněných tří posuzovaných oblastí je vygenerován diagram, který ukazuje bezpečnostní rizika.

I když malý diagram indikuje prostředí s nízkým rizikem, neznamená to, že je systém v bezpečí před útokem. Vyjadřuje dobrou základní bezpečnost systému, která omezuje rizika útoku.

Zpráva rovněž obsahuje podrobná zjištění pro každou sekci a doporučení pro omezení oblastí zranitelnosti. ABB může zajistit implementaci doporučených zjištění.

Typický harmonogram dodávky

(uzpůsoben na míru dle místních podmínek).

Den 1

Uvedení projektu - jednání se zákazníkem

Den 2

Nastavení softwaru pro sběr dat
Zahájení sběru bezpečnostních dat
Rozhovory s klíčovým personálem
Kontrola dat a konfigurace

Den 3

Ukončení sběru procesních dat
Zahájení analýzy dat

Den 4 - 5 (mimo podnik)

Kompletace analýzy dat
Příprava vyhodnocení poznatků a příprava reportu
Prezentace získaných informací

Implementace a podpora.

ABB Cyber Security Fingerprint slouží jako první krok k rozpoznání slabých stránek zabezpečení Vašich procesních řídicích systémů. Přestože výsledná zpráva zachycuje stav zabezpečení v daném čase, doporučení nezaručují pro procesní řídicí systém stoprocentní bezpečnost. Jakýkoliv systém může být ohrožen, bez ohledu na to, jaká opatření budou přijata.

Pro dosažení nejlepších výsledků a optimální udržování úrovně zabezpečení je potřeba aplikovat pravidelně určitá opatření, jako je např. management záplat či aktualizace antivirového SW. Další možností jsou plánované pravidelné kontroly zabezpečení nebo lze zavést průběžné sledování bezpečnosti prostřednictvím služby ABB ServicePort.

Za účelem získání dalších informaci, nebo naplánovaní služby ABB Cyber Security Fingerprint pro Váš podnik, prosím kontaktujte zástupce oblastního servisu ABB.

ABB s.r.o.
divize Procesní automatizace
28. října 3348/65
Nová Karolina Park
702 00 Ostrava
Tel.: +420 597 468 801
Fax: +420 597 468 802
Email: kontakt@cz.abb.com
Kontaktní centrum: 800 312 222
(ze zahraničí: +420 597 468 940)

www.abb.cz/controlsystems

7/2013