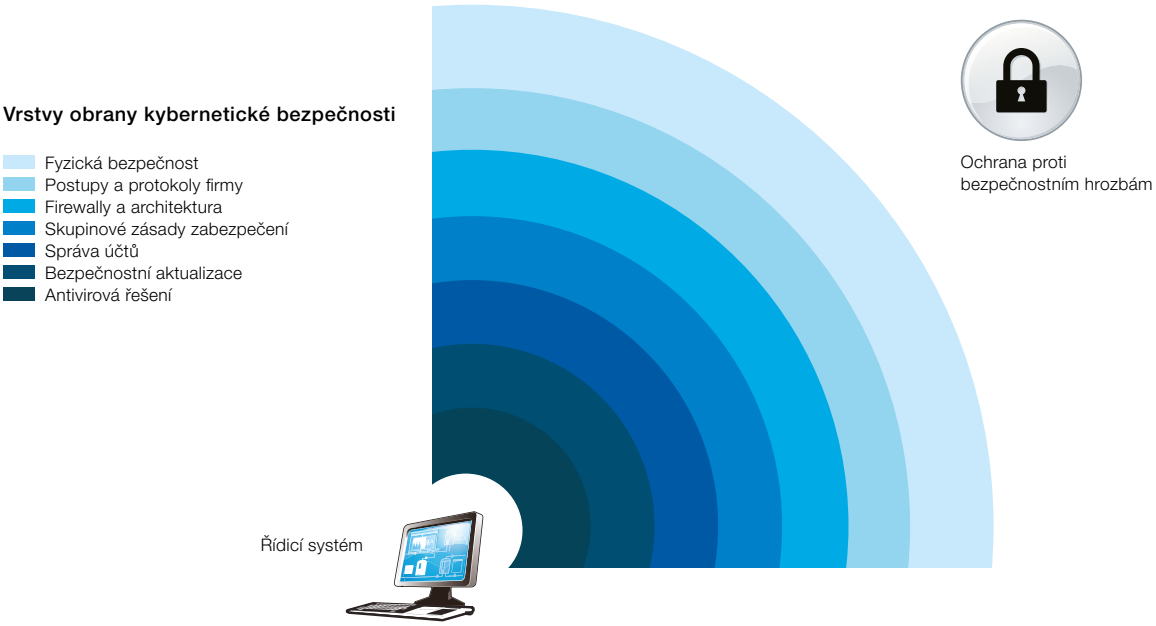
ABB Cyber Security Fingerprint
Vyhodnocení potenciálních bezpečnostních hrozeb pro řídicí systémy



Současné 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 nebo poškození samotného zařízení.

ABB Cyber Security Fingerprint

Odkrývá silné a slabé stránky ve struktuře řídicího systému z hlediska ochrany 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.

Přínosy

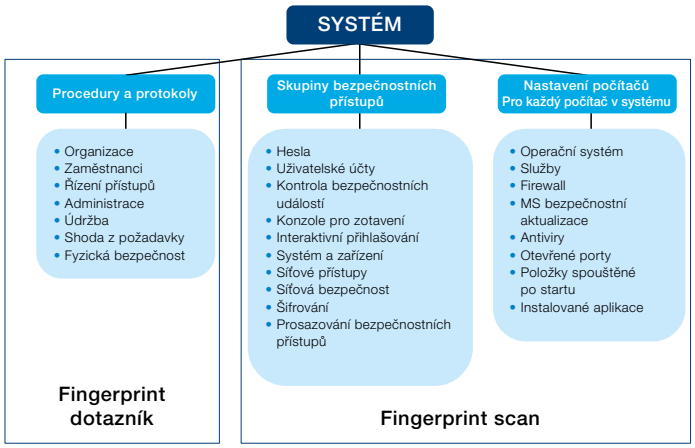
– zvýšení bezpečnosti podniku, lidí a dat,
– omezení možnosti pro narušení systému,
– komplexní pohled na stav kybernetické bezpečnosti v provozu,
– vylepšení procesu zmírňování rizik kybernetických útoků,
– porovnání se zavedenými standardy a osvědčenými postupy,
– pevný základ pro vybudování udržitelné strategie pro kybernetickou bezpečnost.

Vlastnosti

– zpracováno bezpečnostními experty ABB,
– detailní zpráva o stavu včetně doporučení pro omezení bezpečnostních rizik,
– 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 ABB Cyber Security Fingerprint na pravidelnou plánovanou kontrolu zabezpečení a sledování potenciálních událostí s vlivem na kybernetickou bezpečnost. Nejefektivnější cestou je zavedení průběžného sledování bezpečnosti prostřednictvím služby **ABB ServicePort**.

Dobře definovaná strategie kybernetické bezpečnosti může zmírnit bezpečnostní rizika. **ABB Cyber Security Fingerprint** je snižuje tím, že odhalí slabiny, které by mohly ohrozit zaměstnance, majetek nebo provozuschopnost systému.



Přístup ABB uplatňuje strategii obrany do hloubky. Porovnává vaše zásady zabezpečení a nastavení s průmyslovými standardy pro zabezpečení několika vrstev ochrany vašich systémů.

Popis služby

ABB Cyber Security Fingerprint je neinvazivní služba aplikovatelná na jakýkoliv řídicí systém používající operační systém Microsoft Windows® 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 průmyslovou praxí a standardy, jako je ISO/IEC27001 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 (KPI)

Po kontrole a sběru dat ABB určí KPI pro následující oblasti:

– **Procesy a protokoly:** kvalitativní analýza, která indikuje, jak je organizace zabezpečena s pomocí písemných pokynů a nařízení.
– **Skupiny bezpečnostních zásad:** omezení uplatněná v systému, vyžadovaná centrálním serverem nebo implementovaná na jednotlivých počítačích.
– **Nastavení počítačů:** nastavení a aplikace na jednotlivých počítačích, které jsou součástí systému.

Závěrečný výkaz

Po vyhodnocení je učiněn závěr a připraven výkaz. Na základě zmíněných tří posuzovaných oblastí je vygenerován diagram, který ukazuje bezpečnostní rizika.
I pokud 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
Nastavení softwaru pro sběr dat a provedení sběru bezp. dat
Rozhovory s klíčovým personálem
Kontrola dat a konfigurace

Den 2 (mimo podnik)

Kompletace analýzy dat
Příprava vyhodnocení poznatků a příprava výkazu a prezentace získaných informací

Den 3

Předání výsledků a výkazů analýzy
Prezentace a vysvětlení výsledků analýzy
Návrh dalších kroků k zajištění zvýšení bezpečnosti

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 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.

Za účelem získání dalších informací, nebo naplánování služby ABB Cyber Security Fingerprint pro Váš podnik, prosím, kontaktujte:

ABB s.r.o.
Divize Energetika
Centrum pro automatizaci energetických soustav
Průmyslová 137
541 01 Trutnov
Kontaktní centrum: 800 312 222
(ze zahraničí: + 420 597 468 940)

www.abb.cz