Jak na digitalizaci

Několik zkušeností a tipů z praxe pro efektivní a bezpečná řešení

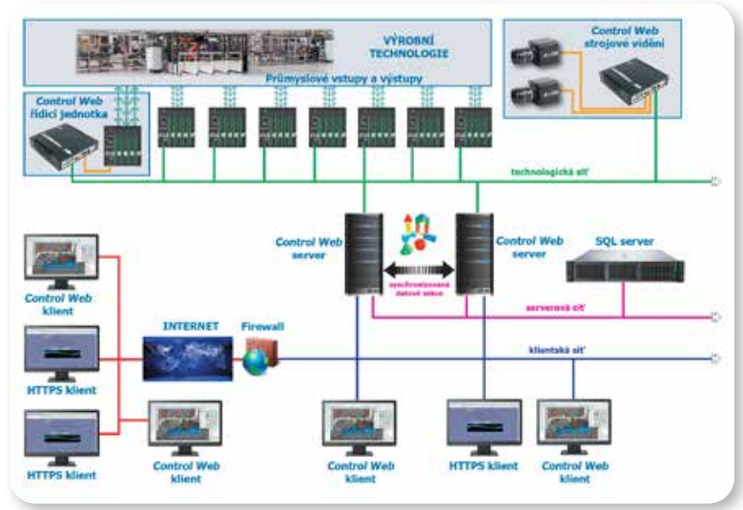
Roman Cagaš
Moravské přístroje, a. s.

I když to největší rušno kolem marketingové kampaně označované jako Průmysl 4.0 se již pomalu, ale jistě uklidňuje, stále se občas v souvislosti s ní objevují informace, které stojí za povšimnutí. Některá hojně publikovaná moudra jsou spíše k pousmání, jiná jsou ale z hlediska odolnosti digitalizovaných systémů a jejich kybernetické bezpečnosti na pováženou.

Nedávno byl často publikován nový trend ve strategii Průmyslu 4.0, kterým je tzv. edge computing. Není přeci nutno, aby veškerá data byla vždy přenášena někam do cloudu. To je tedy objev! Znamená to, že je opět moderní dělat věci tak, jak se obvykle vždy dělávaly.

Ale vážně, největším rizikem je propagovaný princip, kde jsou všechna zařízení připojena do ploché struktury průmyslového internetu věcí. To je z hlediska kybernetické bezpečnosti docela riskantní, protože napadení kteréhokoli prvku může mít dopad na celou digitalizovanou výrobu. Zde můžeme doporučit právě opačný přístup, a to vybudovat strukturu komunikujících zařízení jako hierarchickou stavbu, kde k žádnému zařízení nebude možný přímý přístup z veřejného internetu ani z jakéhokoli koncového zařízení ve vyšší vrstvě.

Vzhledem k obrovskému a neustále rostoucímu počtu nikterak nezabezpečených zařízení v internetu věcí si zadělváme na docela velké potíže. I v průmyslu hodně lidí rizika podceňuje. Říkají nám, že jim nevadí, mají-li ve své vnitřní síti např. chytrý elektroměr posílající data někam do veřejné sítě. Každé zařízení, které je chytré, je také zranitelné. Obvyklý argument interních odpůrců zabezpečení, který zní „k čemu by někomu byla naše data“, je natolik hloupý, že ani nestojí za polemiku. Jestliže se vám rizika a hrozby nezdají příliš důležité, vyhledejte si na webu seznamy nezabezpečených IoT zařízení, podívejte se na záznam z volně přístupných kamer a možná na problematiku kybernetické bezpečnosti změníte názor.



Obrázek 1: Možnosti systému Control Web při řízení průmyslového provozu v síti, která je segmentována s ohledem na maximální zabezpečení proti kybernetickým útokům

Rizikem při napadení některého vašeho zařízení může být:

- zneužití zařízení s cílem poškodit uživatele, v průmyslu to může být cokoli, od krádeže dat přes narušení až po zastavení výroby;
- zneužití zařízení jako přístupového bodu, přes který se lze dostat do dalších komunikačních struktur;
- zneužití výpočetní a komunikační kapacity zařízení k prospěchu útočníka.

Tipy pro bezpečnost

- Do vnitřní sítě nesmí být připojeno žádné zařízení bez schválení zodpovědného pracovníka.
- Zvažme, jestli opravdu potřebujeme internetové připojení daného zařízení, jak budeme využívat produkovaná data a jak budeme k zařízení z vnějšku přistupovat.
- Pokud již nějaké zařízení potřebujeme připojit, zvažme důvěryhodnost výrobce i dodavatele, zabezpečení komunikace i možnosti aktualizací softwaru a záplatování bezpečnostních děr.
- Měli bychom mít trvalý přehled o všech chytrých zařízeních ve své síti. Musíme vědět, jaká data odesílají do vnějšího prostředí a také kdo má z vnějšího prostředí k našim zařízením přístup.
- Zablokujme veškerou funkčnost, která není pro používání zařízení nezbytná.
- Neotevírejme server RDP (Remote Desktop Protocol) do veřejné sítě (tato služba bude rychle identifikována hledacími roboty, které to na nás začnou přinejmenším masivně zkoušet).
- Omezme rozsah přístupu z vnějšího prostředí prostřednictvím bezpečných webových portálů, jako je např. HTTPS server systému Control Web.
- Bezpečný vzdálený přístup s neomezenou funkčností zajistí rovněž klientská aplikace systému Control Web s autorizací a šifrovanou komunikací. V aplikaci lze použít i vícefaktorovou autorizaci.
- Sledujme, co zařízení dělají, zdali se nechovají divně, a buďme připraveni je případně odpojit a nahradit.

Tipy pro výkon a efektivitu

Efektivitu řešení digitalizace můžeme významně zvýšit decentralizací zpracování dat, tedy tím, čemu se v moderní terminologii říká edge computing. Opravdu není nutno vše posílat do cloudu nebo do vzdáleného datového centra. Tím nechceme říci, že cloudové služby v mnoha případech mohou přinášet i úsporu peněz. I tak ale většina cloudových služeb vznikla na základě snahy poskytovatelů získat pravidelné plátce prodejem „čehokoli jako služby“.

Distribuované systémy současně přinášejí i významné bezpečnostní výhody. Centralizovaná síťová a datová architektura cloudu je velmi zranitelná, co se výpadků napájení a útoků týče, včetně nejjednodušího DDoS. Distribuovaná struktura na druhou stranu rozptyluje ukládání a zpracování dat do více zařízení. Jednotlivé poruchy už nemohou zastavit celou síť. V řadě případů, jako jsou např. systémy strojového vidění a vizuální inspekce, výrobní automaty či robotizovaná pracoviště atd., ani jiné než decentralizované řešení není na segmentované síti technicky rozumné.

Současná situace zvyšuje důležitost automatizace a digitalizace a zrychluje rozvoj nástrojů pro tuto oblast. Budujme digitalizační systémy jako hierarchicky strukturované a decentralizované na segmentovaných sítích. Získáme vyšší efektivitu a výkon, lepší kybernetickou bezpečnost i snadnější přehlednost a možnosti dalšího rozvoje.

Obrázek 2: Na vysoké efektivitě řešení má podíl i skutečnost, že celé rozváděče se stovkami průmyslových vstupních a výstupních signálů jsou připojeny vždy jen jedním ethernetovým kabelem