Ewon Cosy+ posouvá kybernetickou bezpečnost IIoT na vyšší úroveň

S Ewon Cosy+ uvádí společnost HMS Networks na trh novou generaci routerů pro vzdálenou údržbu, která zvyšuje úroveň kybernetické bezpečnosti IIoT. Díky bezpečnostním mechanismům integrovaným v hardwaru mohou uživatelé bezpečně přistupovat k průmyslovým zařízením odkudkoliv, uvádět je do provozu, odstraňovat jejich problémy a programovat je online.

Již dvacet let stojí značka Ewon za spolehlivými řešeními vzdálené údržby v průmyslu, s nimiž mohou výrobci strojů a provozovatelé zařízení přistupovat k průmyslovým systémům kdykoliv a odkudkoliv. Řešení vzdálené údržby Ewon jsou snadno použitelná, cenově výhodná a důkladně zabezpečená.

Prostřednictvím Ewon Talk2M – zabezpečené cloudové platformy pro průmyslovou vzdálenou údržbu – je připojeno více než 300 000 strojů a zařízení. Díky tomu je HMS Networks se značkou Ewon přední firmou v oboru připojování průmyslových zařízení na dálku.

Nová generace routerů pro vzdálenou údržbu Cosy+

Na základě velkého úspěchu průmyslového routeru (směrovače) Ewon Cosy nyní společnost HMS Networks představuje Ewon Cosy+ (*obr. 1*) jako výsledek nejnovějšího vývoje systémů pro přístup na dálku v kontextu průmyslového internetu věcí (IIoT). Zákazníci na novém routeru Cosy+ ocení moderní hardwarové zabezpečení, vylepšený výkon a komfortní obsluhu. Cosy+ tak nastavuje nový standard v oboru.

Umožňuje např. automatické aktualizace digitálně podepsaného firmwaru prostřednictvím platformy Talk2M. Tím je zajištěno, že routery vždy splňují nejnovější bezpečnostní standardy a uživatel se již nemusí starat o jejich aktualizaci. Pro datovou komunikaci se používají vylepšené šifrovací algoritmy s vynikající ochranou před kybernetickými útoky. Kromě toho se ještě více zjednodušila použitelnost a uvedení routeru do provozu. Díky Talk2M nabízí routery Ewon uživatelům globálně dostupnou centrální platformu vzdálené údržby pro jednoduchou správu routeru a přístupů na dálku, včetně smlouvy o servisu (SLA). Směrovač byl vyvinut v souladu s požadavky normy ISO 27001 (*Certifikace systémů managementu bezpečnosti informací*) a celé řešení vzdálené údržby včetně Talk2M je podle této normy certifikováno.

Hardwarové zabezpečení a řetězec důvěryhodnosti

V internetu věcí (IoT) jsou propojeny miliardy zařízení mezi sebou a s cloudem. S tím je spojena výměna velkého množství dat.

Obr. 1. Router Ewon Cosy+ ETH pro kabelové ethernetové sítě

Co dělají zařízení IoT? Sbírají data, zpracovávají je a výsledky poskytují dalším zařízením. A je známo, že data jsou velmi cenná. Proto přitahují nežádoucí pozornost osob, které je chtějí zneužít.

Typická infrastruktura IoT má několik vrstev: síťovou, aplikační nebo cloudovou, a každá z nich nabízí příležitosti pro útočníky. Nejsou-li zařízení zabezpečena, útočníci z nich mohou data zkopírovat, změnit je, prostřednictvím nich proniknout hlouběji do sítě nebo je využít k rozsáhlým útokům DDOS.

K ochraně zařízení se používají metody autentizace, opatřování dat digitálními podpisy a šifrování komunikace asymetrickou kryptografií. Tyto mechanismy také chrání vestavný firmware a software před nežádoucími modifikacemi.

V současné době se stává potřebným, nejen aby tyto mechanismy byly využívány mezi propojenými objekty, ale aby se autentizace, šifrování a mechanismy digitálních podpisů uplatnily i mezi jejich elektronickými komponentami. Sítě IoT, a zvláště sítě průmyslového internetu věcí, tedy IIoT, musí být zabezpečené už od návrhu – není dostačující zabezpečit je až dodatečně. Vytváří se tak řetězec důvěryhodnosti od jednotlivých zařízení až do cloudu.

Asymetrická kryptografie ovšem vyžaduje, aby přijímající zařízení disponovalo tajným dešifrovacím klíčem. Ten musí být uložen v zařízení. Základním prvkem pro jeho bezpečné uložení a provádění kryptografických operací je hardwarový kořen důvěry (HRoT, *Hardware Root of Trust*). Ten zaručuje vysokou míru odolnosti: zatímco řádky programu, operačního systému nebo uživatelského rozhraní mohou být přepsány, data vypálená v polovodičové součástce změnit nelze. A na HRoT stojí celý řetězec důvěryhodnosti, kde se vyšší úroveň vždy spoléhá na důvěryhodnost té nižší: hardware důvěřuje HRoT, firmware se spoléhá na důvěryhodný hardware, firmwaru zase věří operační systém, na němž běží uživatelské rozhraní, jež důvěřuje svému operačnímu systému.

Pro realizaci služby HRoT se používá speciální čip nazývaný Secure Element, který nedovoluje, aby v něm uložená data bylo možné modifikovat, a vykonává kryptografické operace (generuje náhodná čísla, šifruje a dešifruje data, obsahuje mechanismus digitálního podpisu atd.). Komunikaci mezi čipem Secure Element a hlavním procesorem zajišťuje šifrovaný kanál.

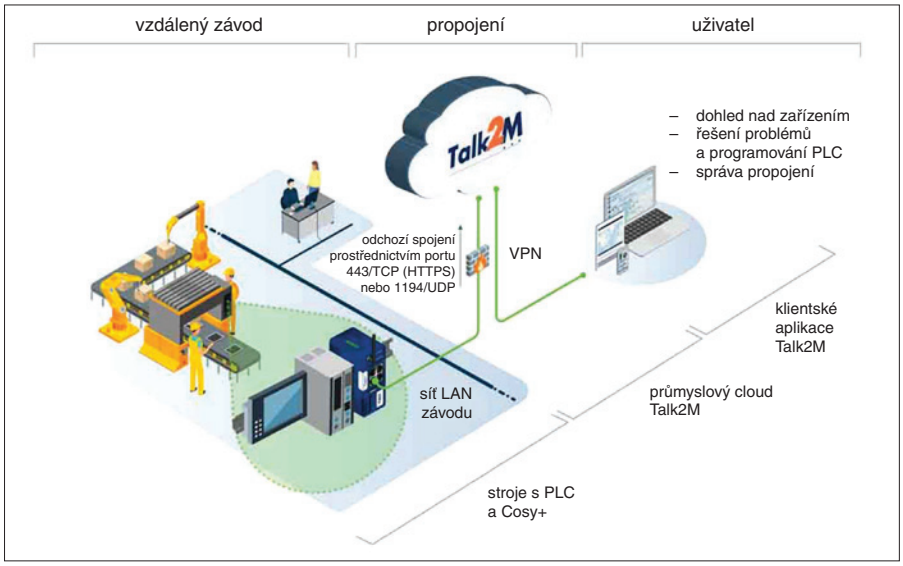
Právě tímto způsobem, pomocí čipu Secure Element, je realizováno zabezpečení routerů Cosy+. Jejich konstruktéři se spolehli na zkušenosti firmy NXP, dodavatele elektronických součástek, v oblasti zabezpečených procesorů a jako operační systém vybrali nezávisle certifikovaný OS s hodnocením podle standardu CC (*Common Criteria*) Evaluation Assistance Level EAL6+.

Řetězec důvěryhodnosti routeru Cosy+ zahrnuje:

- vestavěný čip Secure Element,
- certifikaci softwaru digitálním podpisem, který znemožňuje klonování a dodatečné změny,
- zabezpečenou sekvenci bootování, která zaručuje, že v routeru lze spustit jen software podepsaný firmou Ewon,
- silné šifrování veškeré komunikace s cloudem Talk2M.

Partnerství s NVISO: routery jsou testovány podle nejpřísnějších bezpečnostních standardů

Podle zprávy společnosti Palo Alto Networks, která se zabývá kybernetickou bezpečností, je 98 % provozu IoT nezašifrováno a téměř 60 % zařízení je zranitelných středně závažnými nebo závažnými kybernetickými útoky. „Dnes je důležitější než kdy jindy chránit továrny a řídicí systémy před kybernetickými útoky. Nový router Ewon Cosy+ implementoval nový bezpečnostní koncept, kterým společnost HMS Networks posouvá trh řešení pro přístup na dálku v průmyslu na novou úroveň," říká Thilo Döring, výkonný ředitel společnosti HMS Industrial Networks GmbH.



Obr. 2. Schéma přístupu na dálku prostřednictvím routeru Cosy+

Díky exkluzivnímu partnerství se společností NVISO může společnost HMS Networks se svou značkou Ewon nabídnout systém vzdálené údržby, který byl testován podle nejvyšších standardů a splňuje nejnovější bezpečnostní požadavky.

NVISO je nezávislá společnost, která se ve své činnosti soustředí zejména na zabezpečení informačních a komunikačních systémů a specializuje se na zabezpečení kriticky důležitých průmyslových podniků a finančních institucí. Všichni zaměstnanci NVISO mají prověrku NATO (na stupeň tajné). Firma se zabývá jak poskytováním poradenství v oboru kybernetické bezpečnosti, tak hodnocením zabezpečení produktů, aplikací a infrastruktury. Je spoluautorem standardů pro verifikaci zabezpečení webových aplikací (OWASP – *Open Web Application Security Project*) a mobilních aplikací a podílí se i na tvorbě standardů zabezpečení pro IoT a IIoT.

Součástí zabezpečení sítí využívajících routery Cosy+ je mj. důsledná segregace sítě, takže vzdálený účastník má přístup jen k cílovému zařízení a nikam jinam. Všechny vzdálené aktivity jsou navíc podrobně zaznamenávány. Vzdálené připojení k zařízení je místně indikováno digitálním výstupem a koncový uživatel má možnost je kdykoliv ukončit.

Shrnutí výhod Cosy+

Hlavní rolí routerů Cosy+ je vytvořit zabezpečené připojení prostřednictvím VPN mezi strojem a jeho uživatelem, a to na dálku, kdykoliv a odkudkoliv. K propojení se využívá Talk2M, vysoce zabezpečená cloudová služba vzdáleného přístupu určená pro použití v průmyslu (*obr. 2*).

Díky Talk2M mohou technici získat přístup ke svým PLC, HMI nebo podobným zařízením a zajistit dohled nad nimi a údržbu z jakéhokoliv zařízení připojeného do internetu, dokonce i z chytrého telefonu. To velmi spoří čas a náklady a poskytuje významné konkurenční výhody.

(*HMS Industrial Networks GmbH*)

krátké zprávy

Jednání v Jižní Koreji o spolupráci na dostavbě jaderných bloků v ČR

Zástupci Aliance české energetiky CPIA, sdružující významné české dodavatele do energetiky, se koncem května setkali s vedením jihokorejské společnosti KHNP. Jednali o spolupráci při výstavbě nového jaderného zdroje v České republice.

Cílem aliance je dojednat účast českých firem na výstavbě nového jaderného zdroje v Dukovanech a tím zajistit budoucnost jaderněenergetického dodavatelského oboru v České republice, stejně jako energetickou bezpečnost a nezávislost při provozu nových bloků a jejich servisu. Pro splnění tohoto cíle aliance usiluje o dohody o předběžné spolupráci se všemi uchazeči o tendr.

Setkání v Jižní Koreji se za českou stranu zúčastnili zástupci firem Škoda JS a. s., Doosan Škoda Power s. r. o., Sigma Group a. s., I&C Energo a. s. a ZAT a. s., které tvoří Alianci české energetiky.

Čeští odborníci měli také příležitost navštívit jihokorejskou jadernou elektrárnu Shin Kori a prohlédnout si bloky 5 a 6 ve výstavbě a rovněž část technologie již provozovaného bloku 4. Jde o technologická zařízení APR 1400, která Jihokorejci v současné době instalují např. ve Spojených arabských emirátech na čtyřech blocích JE Barakah.

Jihokorejská společnosti KHNP patří mezi vážné zájemce o dostavbu jaderných bloků v ČR. V současné době koncern provozuje 24 jaderných elektráren a dalších osm buduje ve Spojených arabských emirátech a v Koreji. Společnost KHNP dodává reaktory generace III+ EU-APR a APR1000, opatřené nejmodernějšími prvky pasivní bezpečnosti a chráněné též pro případ havárie velkého letadla i kybernetických útoků. (*ev*)

TAL 2021
Trends in Automotive Logistics
Going Digital: Where's the Right Balance?
21. 9. 2021, Plzeň
Registrace na talconference.com