„Železnice je kritická infrastruktura. Bez bezpečné konektivity a nepřetržitého dohledu se neobejde.“

Rozhovor s Ing. Marcelem Ouřadou, předsedou představenstva a generálním ředitelem společnosti COM PLUS CZ a.s.

Ing. Marcel Ouřada

Vysokorychlostní tratě přivedou do železniční infrastruktury nové technologie i přísnější nároky na dostupnost. Kde z vašeho pohledu začíná kybernetická odolnost železnice?
Začíná u architektury. Jakmile se řízení dopravy, zabezpečovače a provozní technologie opírají o datové sítě, je nutné je navrhovat jako mission-critical systém: oddělení IT/OT, vícevrstvé zabezpečení, řízení identit a přístupů, dohled v reálném čase a jasně popsané provozní postupy. Kyberbezpečnost není produkt, ale nepřetržitý proces napříč životním cyklem tratě.

Jaké specifické hrozby a rizika v drážním prostředí vnímáte nejvíce?
Jednak cílené útoky na provozní technologie, jednak lidské a procesní chyby — obojí může mít srovnatelný dopad. Klíčová je proto mikrosegmentace, princip minimálních oprávnění a kontinuální monitoring anomálií. Velkou pozornost věnujeme i prověřování třetích stran a řízení dodavatelského řetězce. Dráha je komplexní ekosystém.

Řada evropských správ zavádí IP/MPLS jako páteř pro provozní komunikace. Proč právě tato technologie?
IP/MPLS je dnes standardní páteř pro spolehlivý přenos více služeb v jedné síti – od dat ETCS/ERTMS přes hlas a video až po telemetrii a dohled. Poskytuje deterministickou kvalitu služeb, oddělené virtuální sítě a přenos starších technologií. Díky rychlým přepnutím při poruše a řízení toků udržuje parametry i při výpadcích. Výsledek v praxi: nižší latence, vyšší dostupnost a jednodušší provoz napříč rozmanitou infrastrukturou v terénu.

Máte praktické zkušenosti s nasazením technologií na dráze?
Ano. Dodávali jsme přenosové systémy Nokia pro GSM-R a v rámci projektů jsme zajišťovali technickou součinnost při jejich nasazení v transportní vrstvě. Díky tomu dobře známe nároky drážního prostředí: vysokou dostupnost, deterministické chování sítě a důsledné oddělení provozních částí.

Na jaké standardy a regulace se v železničním sektoru díváte?
Vycházíme především ze směrnice NIS2 a navazujícího českého zákona o kybernetické bezpečnosti včetně vyhlášek NÚKIB. S ohledem na povahu železnice zohledňujeme rámec kritické infrastruktury — krizový zákon a související nařízení vlády — a evropskou směrnici

CER o odolnosti kritických subjektů. V drážních technologiích respektujeme požadavky interoperability a příslušné evropské normy, bezpečnou komunikaci a kybernetickou bezpečnost železničních aplikací; na síťové a provozní vrstvě se opíráme o mezinárodně uznávané rámce pro OT/ICS a o standardy ISMS, zejména ISO 27001. U klientů vycházíme také ze specifikací FRMCS (UIC/3GPP/ETSI). Důraz klademe na řízení identit a přístupů a na auditovatelnost; to vše stavíme na penetračních testech, red-team cvičeních, školení, provozních runboocích a nepřetržitém (24/7) dohledu.

Pracujete i pro energetiku. Jak se zkušenosti z ČEPS a ČEZ promítají do železnice?
Energetika i dráha jsou kritická infrastruktura s důrazem na dostupnost, odolnost a bezpečnost. Z energetiky přenášíme disciplínu v řízení změn, segmentovaný design, disaster recovery a cvičení krizových scénářů. Zároveň umíme koexistenci starších technologií s moderní IP/MPLS sítí. Tato zkušenost se do železničního prostředí promítá velmi přirozeně.

Kde vidíte roli COM PLUS u vysokorychlostních tratí konkrétně?
Ve třech krocích, v prvé řadě návrh a dodávka páteřní konektivity — optické DWDM a IP/MPLS transport pro provozní komunikace a dispečerské systémy; dále pak kybernetická bezpečnost a dohled — bezpečnostní architektura, SIEM/SOAR, náš SMART MONITORING, testy a školení; a v neposlední řadě provoz a rozvoj — 24/7 dohled, incident a problem management, SLA a life-cycle management. Naším cílem je, aby se správa a provoz sítí nestal úzkým hrdlem při zavádění a rozšiřování VRT.

Zmínil jste SMART MONITORING. Co je to za systém, co umí?
Jde o náš vlastní dohled nad servery, sítěmi a aplikacemi. Monitorujeme síť napříč technologiemi – vidíme do všech vrstev, chápeme souvislosti mezi prvky v různých vrstvách a hlavně sledujeme služby napříč vrstvami. Otevřená architektura integruje telemetrii z aktivních prvků, bezpečnostní události, logy i environmentální senzory. V železničním prostředí je klíčová korelace provozního a bezpečnostního pohledu – například propojení anomálie v latenci s neobvyklými přístupy. SMART MONITORING dodáváme zákazníkům kritické infrastruktury a přizpůsobujeme jej provozním i regulačním požadavkům.

Jak vypadá vaše 24/7/365 servisní podpora?
Provozujeme nepřetržité dohledové pracoviště s podporou L1–L3. L1 provádí rychlou diagnostiku a korelaci událostí, L2/L3 řeší eskalace a zásahy. Máme on-call týmy a field techniky s pokrytím celé České republiky, vlastní zásobu náhradních dílů a jasně nastavené SLA včetně měření KPI. Důraz klademe na proaktivitu — chyby chceme zachytit dřív, než se promění v incident. Procesy pravidelně prověřujeme interními i externími audity.

Zmiňme i personální a procesní stránku – jak řešíte prověřenost a práci s citlivými informacemi?
Tato otázka je velmi aktuální vzhledem k účinnosti nového zákona o kritické infrastruktuře (266 /2025 sb.). Klade vyšší nároky na lidský faktor, což je patrné i ve stávající mezinárodní normě ISO 27001:2022 a jejího dopadu na dodavatelský řetězec. Tuto skutečnost jsme vnímali jako příležitost.
Naše společnost absolvovala prověrku NBÚ na stupeň „Tajné“ a nastavení procesů pro práci s citlivými daty byla jejím východiskem. Prověření společnosti a samotných zaměstnanců vnímáme jako součást firemní kultury a důkazu kompetence a jasné sdělení našim zákazníkům a partnerům. V praxi se projevuje zvýšenými požadavky na řízení Identit, oddělení rolí, důsledný audit a pravidelné prověřování aktuálního stavu. Samotné normy nám umožňují systematicky řešit požadavky pro dodavatele v kritické infrastruktuře.

Jak se díváte na přechod z GSM-R k FRMCS?
Je to evoluce s velkým důrazem na kvalitní transportní síť. FRMCS přinese vyšší kapacitu a flexibilitu služeb, ale jen pokud stojí na spolehlivé IP/MPLS páteři a dobře navrženém zabezpečení. Důležitá je konvergence IT/OT a jednotný provozní dohled.

Když se zeptám úplně prakticky – čím umí COM PLUS pomoci hned?
Auditem a architektonickým návrhem transportní sítě (DWDM, IP/MPLS), kybernetickým posouzením dle NIS2, zavedením centrálního dohledu a 24/7 podpory. Kde je to účelné, nasazujeme SMART MONITORING jako centrální dohled nad infrastrukturou.

Dráhu označujete jako strategického zákazníka. Proč?
Protože železnice je páteř mobility a současně kritická infrastruktura. Právě zde se potkává naše technologická odbornost s provozní disciplínou — a můžeme přinést měřitelnou hodnotu: bezpečnou konektivitu a nepřetržitý, stabilní provoz.