FUTURE FORCES FORUM
International Platform for Trends & Technologies in Defence & Security
www.future-forces-forum.org

Bezpečnostní konference

SCADA SECURITY

Součástí Future Forces Forum

18. dubna 2024

České Budějovice, VŠTE

Hlavní partner konference

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

Coffee break partner

AUXILIUM Cyber Security

Partneři konference

ALEFNULA

GREYCORTEX

IRON OT Secure The Industry Future

COMGUARD cyber security masters

FUTURE FORCES FORUM

Partneři FFF pro vědu a výzkum

ČVUT České vysoké učení technické v Praze

Univerzita obrany

Generální partner Future Forces Forum

LOCKHEED MARTIN

Partner Future Forces Forum

RESCUE TRAILER

COLSYS
AUTOMATIK

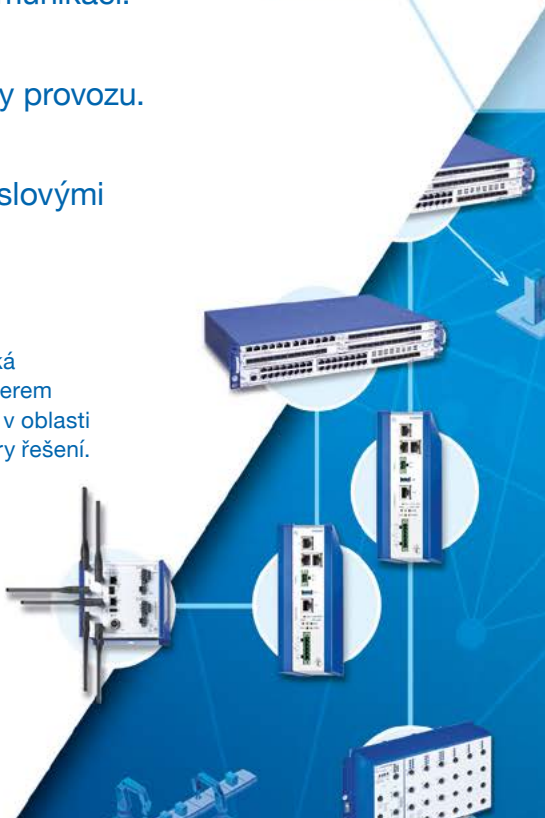
HIRSCHMANN
A BELDEN BRAND

Průmyslové komunikační systémy pro kritickou infrastrukturu

- Analýzy rizik, analýzy zadání.
- Konzultace.
- Inženýring.
- Řešení pro průmyslovou bezpečnost.
- Dokumentace a projekty.
- Dodávky kompletních řešení komunikací.
- Zprovoznění a oživení.
- Analýzy síťového provozu, audity provozu.
- Technická podpora.
- Další služby související s průmyslovými komunikačními systémy.

Společnost COLSYS – AUTOMATIK, a.s., je česká inženýrská společnost. Od roku 1998 jsme partnerem HIRSCHMANN Automation And Control, GmbH, v oblasti kompletních řešení, dodávek a technické podpory řešení.

Podívejte se na náš YouTube kanál
COLSYS – AUTOMATIK, a.s.



www.colaut.cz
obchod@colaut.cz

4. ročník bezpečnostní konference zaměřený na kybernetickou bezpečnost průmyslových řídících systémů, aktuální kyber bezpečnostní trendy a praktické zkušenosti

Kritická informační infrastruktura tvoří páteř moderní společnosti. Díky současné mezinárodní situaci, zejména válce na Ukrajině a konfliktu v pásmu Gazy jakož i rostoucímu počtu a závažnosti kybernetických bezpečnostních incidentů rostou i nároky na ochranu informací. Průmyslové řídicí systémy (ICS) jsou důležitou součástí kritické infrastruktury, bohužel na ně zatím nebyl kladen patřičný důraz, a to i přesto, že v posledních letech byla řada kyberútoků vedena právě proti ICS. Změnit by to měl připravovaný nový Zákon o kybernetické bezpečnosti, jehož přijetí se bohužel čím dál tím více komplikuje.

Kybernetická bezpečnost hraje významnou roli i v oblasti Internetu věcí (IoT), tedy v síti fyzických zařízení, vozidel, domácích spotřebičů a dalších zařízeními, která jsou vybavena elektronikou, softwarem, senzory, pohyblivými částmi a síťovou konektivitou, která umožňuje těmto zařízením se propojit a vyměňovat si data. I tento fakt nově zohledňuje evropská legislativa.

Půldenní odborná konference se zaměří hlavně na aktuální témata v oblasti bezpečnosti ICS v kyberprostoru, vazeb mezi IT a OT, metody kybernetické bezpečnosti v kritické infrastruktuře, průmyslu a energetice, a na další související témata. Konference naváže na předchozí bezpečnostní akce organizované v rámci projektu FFF a vytvoří jedinečné fórum pro partnery a účastníky k diskusi a k výměně informací a zkušeností z oblasti ICS a kybernetické bezpečnosti, bude hledat alternativní řešení nastolených problémů, a to zejména prostřednictvím zapojení světově uznávaných odborníků v oblasti bezpečnosti a ICS systémů.

Zabezpečení informačních systémů, nastavení procesů pro ochranu dat, předcházení kybernetickým incidentům a událostem. A rychlé řešení těch incidentů, kterým se organizace přeci jenom nevyhne.

Počet organizací, které budou muset informační bezpečnost řešit komplexně, jako systém, výrazně vzroste po přijetí nového Zákona o kybernetické bezpečnosti, který bude současně i implementací EU směrnice o kybernetické bezpečnosti, tzv. NIS2 do české legislativy.

František Janů
Moderátor

Vážené dámy, vážení pánové,

opět se setkáváme na konferenci „SCADA Security 2024“, tentokrát v prostorách Vysoké školy technické a ekonomické v Českých Budějovicích.

Je dobře, že tato konference spojuje svět průmyslu a vzdělávání v technických oborech. Toto spojení je velmi důležité pro všechny, kteří se profesně zabývají otázkami (nejen kybernetické) bezpečnosti.

Oblast kybernetické bezpečnosti, ať už v klasickém IT nebo ve světě průmyslovém, je v současné době jednou z oblastí, kde zásadním způsobem chybí odborníci, a právě univerzitní prostředí by mělo být inkubátorem pro tyto lidi a příslušné profese.

Věřím, že do budoucna budou i nové studijní programy zaměřené na bezpečnostní otázky nejen na poli kybernetické bezpečnosti, ale i bezpečnosti jako celku. Ono oddělování jedné bezpečnosti od druhé se historicky ukazuje jako chybný krok, který bezpečnosti rozhodně nepřidává.

Pohledem do programu konference je jasné, že téma je hodně široké a obsáhlé. Proto všem účastníkům přeji, aby se v tématice co nejvíce viděli a co nejvíce dokázali zde získané informace aplikovat ve svých konkrétních případech. Samozřejmě s cílem zvýšení bezpečnostních parametrů svých vlastních aplikací a svých vlastních znalostí a odbornosti.

Věřím, že program bude pro všechny přínosný a těším se na setkání v průběhu konference.

Petr Kolouch
Místopředseda představenstva
COLSYS – AUTOMATIK, a.s.

Ani v roce 2024 nelze zabezpečení technologických a řídicích systémů považovat za dostatečné

Informační a komunikační technologie a různé formy počítačů jsou v současnosti užívány snad ve všech oblastech lidského snažení. Není divu – použití moderních výpočetních systémů s sebou obecně přináší řadu výhod, mj. v oblasti citelného zvýšení efektivity procesů nebo jednodušší standardizace vybraných aktivit. Nese s sebou však i řadu významných rizik a málokde jsou tato rizika citelnější, než v oblasti průmyslových, technologických a specifických systémů.

V době, kdy je převážná většina energetiky, produktovodů, dopravy nebo i komplexnějších zdravotnických vyšetření řízena plně či z části s pomocí k tomu uzpůsobených počítačů, může výpadek těchto systémů, nebo jejich nekorektní funkce způsobit významné finanční ztráty, ale i ztráty na zdraví či na životech. Zajištění bezchybné, bezpečné a zabezpečené funkce těchto systémů tak lze bezpochyby považovat za zcela zásadní.

Problematice zajištění bezpečného fungování řídicích systémů – tzv. „safety", resp. takovému fungování systémů, které neohrozí lidské zdraví či životy a současně umožní bezchybně řídit související procesy – se již od počátků existence těchto systémů věnuje významná pozornost. Problematika efektivního zabezpečení těchto systémů (tzv. „security") však byla až do nedávné doby relativně často citelně opomíjena, resp. řešena pouze na úrovni fyzické vrstvy. Dopady úspěšného kybernetického útoku na technologické či jiné řídicí systémy přitom mohou být extrémně závažné.

V současnosti se situace v této oblasti pomalu zlepšuje, stále však nelze říci, že by všechny řídicí systémy, které ovládají významné procesy – ať už v oblasti zdravotnictví, energetiky, výroby nebo jakéhokoli jiného oboru – byly korektně zabezpečeny. Jak v globálním tak v českém prostředí je dokonce i v roce 2024 stále možné narazit na významné řídicí systémy, s nimiž může kdokoli na světě volně komunikovat přes internet a potenciálně tak ovlivňovat jejich fungování.

Určité budoucí zlepšení v této oblasti lze předpokládat mj. s příchodem aktuálně připravované legislativy. Reálnou odolnost řídicích a specifických systémů proti kybernetickým útokům však bude vždy schopný zajistit pouze vhodně nastavený bezpečnostní program zahrnující efektivní procesy, funkční technologie, ale zejména znalé a dobře vyškolené odborníky.

Tomu, jak efektivně přistoupit právě ke vzdělávání a školení těchto pracovníků, se věnuje náš článek obsažený v tomto katalogu.

Jan Kopřiva
Senior Security Consultant
ALEF NULA, a.s.

Vážení účastníci SCADA Security,

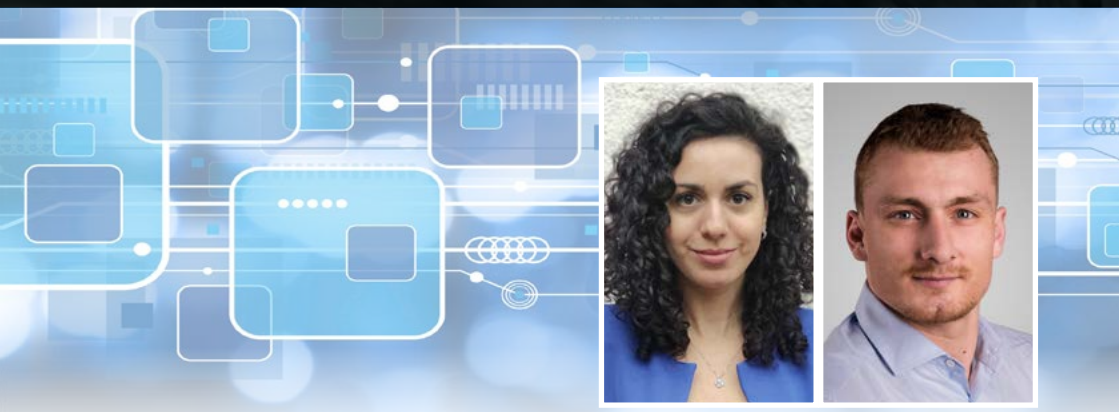
je mi velkou ctí uvítat vás na letošním ročníku této prestižní události, která je zasvěcená nejnovějším trendům a inovacím v oblasti kybernetické bezpečnosti průmyslových řídících systémů. Jako ředitel společnosti zaměřené na vývoj kybernetických bezpečnostních produktů pro síťový monitoring v IT i OT sítích, jsem rád, že se o kybernetické bezpečnosti v průmyslu mluví čím dál tím víc.

V oblasti ochrany průmyslových sítí se neustále vyvíjejí nové technologické postupy, které reagují na nárůst počtu i sofistikovanosti kybernetických hrozeb. Tradiční dělení na IT a OT technologie se stírá, a tak je potřeba chránit organizaci jako celek. Pevně stojíme za naším nástrojem, který vyvíjíme pro monitoring IT sítě i průmyslového prostředí. Zároveň ale víme, že mít dobrý nástroj není zdaleka všechno. K bezpečnosti by organizace měla přistupovat jako ke komplexní úloze – za využití technologií by měl stát personál dedikovaný bezpečnosti, kvalitně nastavené firemní procesy, jejich kontrola a vzdělávání zaměstnanců v oblasti bezpečnostních základů.

Naše společnost se zavázala k poskytování nejlepších řešení pro ochranu průmyslových sítí a věříme, že účast na této konferenci nám umožní lépe porozumět potřebám našich zákazníků a lépe reagovat na aktuální výzvy v oblasti kybernetické bezpečnosti.

Doufám, že vás program konference osloví a přinese vám inspiraci a nové poznatky, které vám pomohou posílit bezpečnost vašich průmyslových systémů.

Petr Chaloupka
CEO
GreyCortex s.r.o.



Vážení kolegové a nadšenci kybernetické bezpečnosti,

jako zástupci společností Comguard a Iron OT bychom vás chtěli srdečně pozvat na nadcházející konferenci SCADA Security, místo setkání předních myslitelů a inovátorů v oblasti ochrany průmyslových systémů. Spojili jsme naše síly a zkušenosti, abychom vám představili něco, co považujeme za klíčové pro každého, kdo se pohybuje v této dynamické a náročné oblasti.

Připravili jsme pro vás prezentaci s názvem „Jak ovládnout IEC 62443: Pokročilé metody kybernetické bezpečnosti pro průmysl a kritickou infrastrukturu". V dnešní době, kdy jsou kybernetické útoky čím dál tím sofistikovanější a destruktivnější, je nezbytné, aby naše průmyslová a infrastrukturní zařízení byla chráněna nejmodernějšími a nejefektivnějšími metodami. Naše společná prezentace vám nabídne pohled na to, jak důležité je porozumění a správné používání standardů IEC 62443 pro zabezpečení operačních technologií (OT).

Nechceme se však omezit pouze na teorii. Ukážeme vám, jak můžete své procesy a architekturu nastavit tak, abyste maximalizovali ochranu vašich systémů před kybernetickými hrozbami. Pomocí příkladů z praxe vám předvedeme, jak využití správných technologií pro detekci zranitelností, monitorování síťových anomálií a dalších pokročilých nástrojů může významně zvýšit vaši obranyschopnost.

Věříme, že sdílení našich znalostí a zkušeností může pomoci posílit celou komunitu kybernetické bezpečnosti a připravit ji na výzvy, které nás v budoucnu čekají. Těšíme se na vaši účast a na možnost společně diskutovat o tom, jak můžeme společně čelit hrozbám a chránit naše nejcennější průmyslová aktiva.

Helena Hrašková
Account & Vendor Manage
Comguard

Ilja David
OT/IT Security
Iron OT

Vážení účastníci konference SCADA Security,

velkou radostí mi je uvést několik úvodních slov k této konferenci a jsem vděčný, že naše společnost může být součástí této události.

V dnešní době, kdy se stále více spoléháme na digitální technologie, je kybernetická bezpečnost bezpochyby jedním z nejvýznamnějších aspektů našeho společenství. V této digitální éře, kde technologický pokrok urychluje neuvěřitelnou rychlostí, je kybernetická bezpečnost nezbytným pilířem pro ochranu dat, infrastruktury a soukromí. Neustále se vyvíjející hrozby vyžadují trvalou pozornost a inovativní přístupy k zajištění integrity, dostupnosti a ochrany našich dat. Zejména v neustále se měnícím prostředí kybernetické ochrany je nevyhnutelné neustále se informovat o aktuálních a budoucích kybernetických hrozbách, jejich prevenci a řešení. Stejně důležité je zaměřit naši pozornost na SCADA systémy, které se postupně vyvíjejí a disponují propracovanější infrastrukturou, čímž se stávají terčem o to více sofistikovanějších kybernetických útoků. Zabezpečení těchto infrastruktur je klíčové pro prevenci jak virtuálních hrozeb, tak fyzických, které mohou mít dopad na celou naši společnost.

Během naší práce se SCADA systémy jsme v rámci testování identifikovali klíčová bezpečnostní rizika a hrozby, které mohou v realitě ohrozit stabilitu a integritu daného systému. Například jsme zaznamenali možnost zneužití, která by umožňovala získat kontrolu nad jeřáby v přístavu. Dalším významným objevem byla možnost zastavit vlak z pozice pasažéra, což vyplývá z našeho hlubšího porozumění bezpečnostním výzvám v oblasti železniční dopravy. Tato identifikovaná zranitelnost může ohrozit jak bezpečnost cestujících, tak stabilitu celého železničního systému. Kromě toho jsme rozpoznali potenciální riziko pro armádní vozidla, spočívající v možnosti odcizení utajených informací ze systému. Tato odhalení poukazují na skutečnost, že existuje stále mnoho práce při zabezpečování rozsáhlejších systémů a infrastruktur, aby byla zajištěna jejich bezpečnost a spolehlivost.

Věřím, že tato konference přinese mnoho nových poznatků a zajímavých informací, které nás povedou dále ve snaze předcházet těmto rizikům, učit se z nich a neustále posilovat bezpečnost našich systémů a infrastruktur. Těším se na inspirativní diskuse a sdílení poznatků.

Přeji vám všem podnětná setkání a osobně se těším na setkání s vámi.

Martin Pozděna
Jednatel společnosti
Auxilium Cyber Security s.r.o.

Program konference

18. DUBNA 2024 — České Budějovice, VŠTE

12.30 – 12.35 Úvodní slovo
František JANŮ – moderátor

12.35 – 13.05 Bezpečné vazby mezi IT a OT v dnešní kyber éře
Petr KOLOUCH, Místopředseda představenstva, **COLSYS – AUTOMATIK, a.s.**
Každé z komunikačních prostředí má svá pravidla a svůj styl myšlení. Prostředí informačních technologií (IT) se od výrobního prostředí (OT) vždy lišilo, zejména pak v tématech bezpečnosti a spolehlivosti. V poslední době se nám ovšem tato dvě prostředí výrazně prolínají…

13.05 – 13.30 Polygon operačních technologií verze 0.2
Jan ZDRHA, Referent bezpečnosti státu, Oddělení bezpečnosti operačních technologií, **NÚKIB**
Seznámení s možnostmi, projekty a ukázkami OT polygonu NÚKIB

13.30 – 13.55 3 velké výzvy OT bezpečnosti a jak se s nimi vypořádat
Jan KOPŘIVA, Security Architect, **ALEF**
V rámci této prezentace se zaměříme na tři z velkých výzev kybernetické bezpečnosti v oblasti průmyslových a specifických systémů – na bezpečné řízení přístupu, smysluplné řízení zranitelností a efektivní zvládání bezpečnostních incidentů – a představíme bezpečnostní opatření, která jsou v jejich kontextu relevantní.

13.55 – 14.20 Efektivní využití nástroje GREYCORTEX Mendel pro ochranu OT sítí
Ondřej HUBÁLEK, GREYCORTEX s.r.o.
Opravdu víte, co se děje ve vašich OT sítích. Víte, kdo reálně pracuje a komunikuje s vaší kritickou OT infrastrukturou?
Pojďme si ukázat, jak mít detailní přehled o OT infrastruktuře. Jak mít pod kontrolou jaká jednotlivá zařízení reálně v OT síti komunikují, jaké jsou vazby mezi nimi, jaké obsahují zranitelnosti, jak jsou dodržovány bezpečnostní politiky v rámci segmentace a oddělení OT sítí atd. Stejně tak, si vysvětlíme jak je neoddělitelná bezpečnost IT světa od toho OT světa a jak je tato vazba zásadně důležitá v rámci ochrany OT infrastruktury

---

14.20 – 14.45 přestávka

14.45 – 15.10 Kyberbezpečnost v jaderné energetice
Dušan MAREČEK, Expert IKB Jaderná elektrárna Temelín, **ČEZ, a.s.**
Výzvy a specifika řešení problematiky zajištění kybernetické bezpečnosti nejen technologických systémů v prostředí jaderné elektrárny

Hlavní partner konference

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

Coffee break partner

AUXILIUM
Cyber Security

Partneři konference

ALEFNULA

GREYCORTEX

IRON OT
Secure The Industry Future

COMGUARD
cyber security masters

Pod záštitou a za podpory

Národní úřad pro kybernetickou a informační bezpečnost

Hospodářská komora České republiky

Ministerstvo průmyslu a obchodu

Jhk.cz

Univerzita obrany

Centrum kybernetické bezpečnosti

ictunie

ČIMIB

Cyber Security Competition Czech

Mediální partneři

CZDEFENCE
CZECH ARMY AND DEFENCE MAGAZINE

Cyber Security Review

NETWORK NEWS

ICT NETWORK NEWS

IT Systems
www.SystemOnLine.cz

katalogakci.cz

AUTOMA

15.10 – 15.50 Jak ovládnout IEC 62443: Pokročilé metody kybernetické bezpečnosti pro průmysl a kritickou infrastrukturu

Helena HRAŠKOVÁ, Account & Vendor Manager, **COMGUARD**
Ilja DAVID, OT/IT Security, **IRON OT**
S kybernetickými útoky v průmyslovém prostředí se setkáváme stále častěji, přičemž bezpečnostní incidenty jsou postupně stále větší a destruktivnější. Náš příspěvek se věnuje pochopení a významu provozních technologií (OT) a správnému použití standardů IEC 62443 pro zabezpečení OT systémů. Současně zdůrazňuje modulární přístup IEC62443 pro zajištění bezpečnosti a porovnává jej s ISO27001. Ukážeme Vám, jak lze mít pomocí kvalitně nastavených procesů a architektury, za využití správných technologií pro detekci zranitelností, síťových anomálií a monitoringu, zajištěnou kybernetickou bezpečnost pro jakékoliv průmyslové sektory a kritickou infrastrukturu.

15.50 – 16.10 Bezpečnostní hrozby v kyberprostoru

Bohuslav ZŮBEK, Ministerstvo vnitra ČR
Umíme se v současné době bránit a vnímat nebezpečí, které na nás svým způsobem číhá na každém bitu kyberprostoru. AI nám může pomoci, ale zároveň je i zdrojem velkého množství dezinformací a manipulací. Jak se orientovat a nebýt slepý k současným hrozbám, když trend jejich dokonalosti se zrychluje.

16.10 – 16.30 Fortinet Security Fabric: Vaše OT sítě pod neprůstřelným štítem

Jan NGUYEN, Cyber Security Consultant, **Seyfor a.s.**
V éře rostoucí digitalizace a sofistikovaných kybernetických hrozeb je nezbytné, aby organizace věnovaly zvýšenou pozornost ochraně svých operačních technologií (OT) a průmyslových sítí. V tomto dynamickém prostředí se Fortinet Security Fabric jeví jako klíčový prvek v arsenálu pro zabezpečení OT infrastruktur, poskytující nejen komplexní ochranu, ale také strategickou výhodu v boji proti kybernetickým útokům.

16.30 – 16.40 Q & A a závěrečné slovo

František JANŮ – moderátor

Změny v programu vyhrazeny.

Efektivní bezpečnostní vzdělávání
v oblasti technologických a řídicích systémů

Problematice kybernetické bezpečnosti průmyslových, dopravních, zdravotnických i dalších specifických prostředí a efektivnímu zabezpečení v nich užívaných zařízení a systémů se věnuje řada generických odborných standardů a norem, z nichž zřejmě nejznámější jsou NIST SP 800-82 a normy patřící do řady ISA/IEC 62443. Pro vybrané oblasti, jako je energetika či doprava, jsou navíc k dispozici i oborové standardy, které hlouběji zohledňují bezpečnostní specifika těchto oborů a v nich užívaných systémů.

Materiálů reprezentujících dobrou odbornou praxi v oblasti kybernetické bezpečnosti technologických a řídicích systémů je tedy v současnosti k dispozici relativně velké množství. Jejich znalost – a mnohdy i povědomí o jejich samotné existenci – na straně specialistů zodpovědných za provoz technologických a řídicích systémů i jejich zabezpečení je však často omezená. Omezená pak v souvislosti s tím bohužel často bývá i efektivita samotného zabezpečení.

Důvod pro tuto skutečnost je prostý – organizace často očekávají, že provozní specialisté automaticky rozumí tomu, jak svěřené systémy zabezpečit, nebo věří, že jejich IT bezpečnostní oddělení jsou schopna zabezpečit technologická prostředí stejně efektivně, jako prostředí organizační IT sítě.

Kompetence v oblasti „OT bezpečnosti" jsou však nejen u provozních specialistů, ale i u bezpečnostních rolí z oblasti IT relativně řídké. Případné dobře míněné, ale neodborné snahy o zavádění bezpečnostních opatření ze strany specialistů na IT bezpečnost v průmyslových a dalších specifických prostředích tak zpravidla provozní specialisté nevítají s nadšením, neb běžné přístupy k zabezpečení užívané v IT nelze v oblasti technologických a řídicích systémů často principiálně aplikovat, neb by měla citelný negativní dopad na zajišťované procesy.

Cestou z aktuálního nepříznivého stavu je bezpochyby mj. nastavení efektivního bezpečnostního systému pro řídicí a průmyslové systémy. Pro jakýkoli systém tohoto typu jsou však nezbytné odpovídající technologie, procesy i personál.

Právě kompetentní personál je v této oblasti klíčový, neb je to on, kdo by měl být schopen relevantní procesy vhodně nastavit a také stanovit smysluplné požadavky na nezbytné technologie. Vzhledem k tomu, že vybudovat samostatné, nové oddělení s personálem zaměřeným výhradně na problematiku bezpečnosti řídicích a specifických systémů a prostředí není v reálných možnostech většiny organizací, jeví se jako jediná možná cesta pro zajištění dostatečných kompetencí doplnění odborného vzdělání u stávajících zaměstnanců – jak těch zodpovědných za provoz řídicích systémů, tak těch zodpovědných v rámci organizace za kybernetickou bezpečnost.

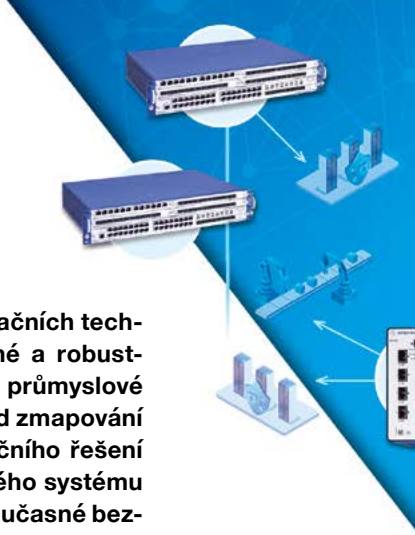
Vzhledem k tomu, že jsme na trhu dlouhodobě vnímali absenci odborného školení, které by výše zmíněným rolím dokázalo předat znalosti nezbytné pro efektivní zabezpečení specifických prostředí a řídicích systémů, rozhodli jsme se začít ve spolupráci se společností Nettles Consulting nabízet specializovaný kurz zaměřený na tuto problematiku nazvaný Bezpečnost průmyslových a specifických systémů a prostředí.

Jedná se o jednodenní školení poskytující úvod do problematiky kybernetické bezpečnosti průmyslových, řídicích a specifických systémů provozovaných v různých prostředích. A účastníci se v rámci něj seznámí se základními principy kybernetické bezpečnosti ve vztahu k OT/ICS systémům a sítím, poznají relevantní bezpečnostní standardy užívané v této oblasti a naučí se aplikovat zásady dobré odborné praxe při zabezpečování nově implementovaných i stávajících systémů.

Bližší informace o školení naleznete v případě zájmu na https://**training.alef.com**/cz/

www.colaut.cz obchod@colaut.cz

Podívejte se na náš YouTube kanál COLSYS – AUTOMATIK, a.s.



Průmysl je v současné době zcela závislý na komunikačních technologiích. Pro spolehlivý chod je zapotřebí bezpečné a robustní prostředí. Společnost COLSYS – AUTOMATIK pro průmyslové podniky zajišťuje kompletní rozsah této oblasti, a to od zmapování aktuálního stavu včetně analýzy rizik, návrhu projekčního řešení až po kompletní konfigurační parametry a dodání celého systému včetně servisu. „Staré technologie často nezvládají současné bezpečnostní požadavky, proto je potřeba najít jiný způsob ochrany," vysvětluje Jiří Kasner ze společnosti COLSYS – AUTOMATIK, která se průmyslové komunikaci věnuje už dvacet let.

Provoz průmyslových podniků je závislý na bezpečných komunikačních systémech

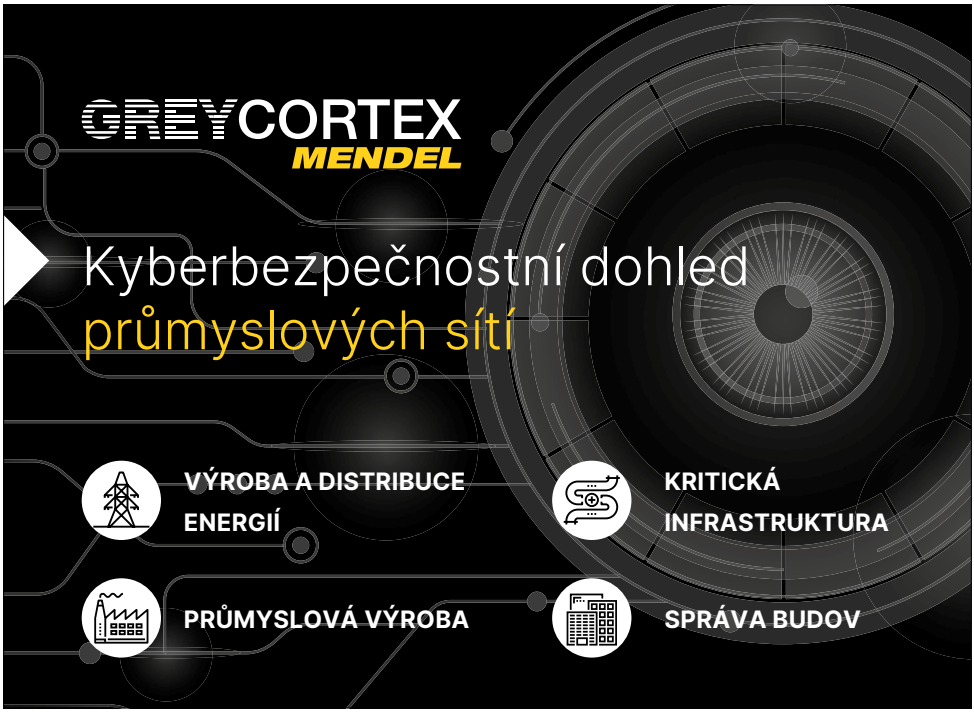
Podcenění rizik stojí peníze

Spousta firem podceňuje zabezpečení průmyslové komunikace včetně kritické infrastruktury. Často si možná rizika ani neuvědomují. Výpadky a narušení pak ale značně komplikují provoz a stojí nemalé peníze. Je zásadní finanční rozdíl v tom, jestli vám nefunguje hodinu poštovní klient nebo turbína. Nechte zkušené odborníky nahlédnout do vašich průmyslových komunikačních systémů. Analýza rizik a návrhy řešení, která budou kombinovat robustnost ve smyslu záložních systémů a bezpečnost, povedou ke spolehlivému zajištění provozu. Kdo je připraven, není překvapen. Zde to platí dvojnásob.

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

HiSecOS
Hirschmann™ Security Operating System



Kybernetická bezpečnost OT prostředí

Ochrana průmyslového prostředí je klíčová pro zachování bezpečnosti a integrity výrobních procesů.

Jedním z hlavních aspektů ochrany je **zajištění komplexního a aktuálního přehledu o všech aktivech** v síti. To umožňuje identifikovat potenciální zranitelnosti a odhalovat kybernetické útoky včas. Těm předejdete sledováním chování zařízení a detekcí anomálií či neobvyklých aktivit.

Dalším klíčovým prvkem je **integrace bezpečnostních řešení**, která umožňuje sledovat a analyzovat kybernetické hrozby napříč různými úrovněmi sítě. Můžete tak efektivněji reagovat na potenciální incidenty a minimalizovat jejich dopady.

GREYCORTEX Mendel monitoruje jak průmyslové i IT sítě. Díky tomu budete mít skvělý přehled o všech svých síťových aktivitech. Prostředí aplikace si navíc každý uživatel může přizpůsobit v závislosti na tom, zda je jeho zaměřením IT nebo OT. Pro klasifikaci bezpečnostních událostí využívá mimo jiné framework MITRE ATT&CK®. Mendel zpracovává nejpoužívanější OT protocoly jako je Siemens S7, Modbus a mnoho dalších.

Zajistěte si komplexní audit vašeho IT i OT prostředí pomocí GREYCORTEX Mendel.

www.greycortex.com

Programový výbor konference

Jan DIENSTBIER, ex-Prezident, Český institut manažerů informační bezpečnosti, Předseda

Doc. **Josef POŽÁR**, CSc., dr. h. c., Katedra zdravotnických oborů a ochrany obyvatelstva, Fakulta biomedicínského inženýrství, České vysoké učení technické v Praze, Čestný předseda

Členové

plk. doc. Ing. **Petr HRŮZA** Ph.D.**,** Prorektor, Univerzita obrany

Petr JIRÁSEK, Místopředseda Výkonného výboru ENISA European Cyber Security Challenge

Jiří KASNER, Předseda představenstva, COLSYS – AUTOMATIK a.s.

Ing. **Luděk KEIST**, Ředitel úřadu, Jihočeská hospodářská komora

Ladislav KOLLÁRIK, Viceprezident, AFCEA Slovakia

pplk. **Radim KOZÁK**, Velitelství informačních a kybernetických sil, Armáda České republiky

Jaroslav PEJČOCH, Člen představenstva, ICT Unie

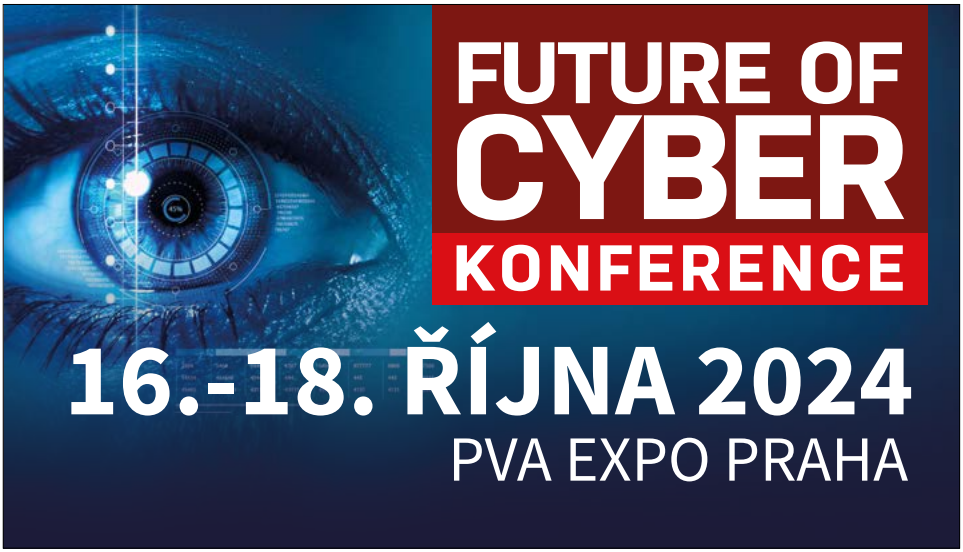
Tomáš PŘIBYL, CEO, Corpus Solutions a.s.

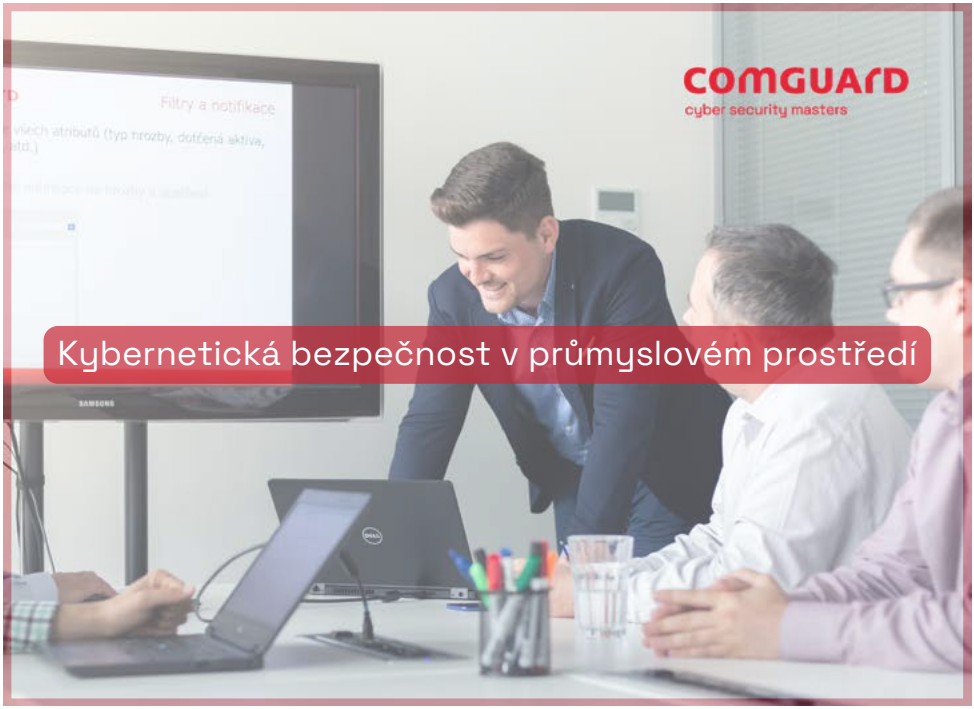
prof. **Boris ŠIMÁK**, Katedra telekomunikační techniky, Fakulta elektrotechnická, ČVUT v Praze

Jakub VESELÝ, Ředitel odboru vládní CERT, Národní úřad pro kybernetickou a informační bezpečnost

Michal ZEDNÍČEK, Cyber Expert, Alef Security

Bohuslav ZŮBEK, Oddělení kybernetické bezpečnosti, Ministerstvo vnitra ČR





Kybernetická bezpečnost v průmyslovém prostředí

COMGUARD je Value Added Distributor (B2B) se specializací na **IT bezpečnost**. Působíme v České republice a na Slovensku. Naše komplexní řešení plně odpovídají potřebám velkých firem, včetně datových center, ale i menších a středních podniků. Zaměřujeme se na bezpečnost koncových stanic, ochranu perimetru, ochranu citlivých dat, vyhodnocování potencionálních rizik, kybernetické bezpečnosti v průmyslovém prostředí a dalších oblastí. Navíc poskytujeme expertní služby jako je například penetrační testování a Security Operation Center (SOC).

Jsme hrdými partnery značek jako Trellix, Sophos, Barracuda, Skyhigh Security, Rapid7, Wallix, Honeywell Scadafence, Gytpol, LogRhythm, Ekran, SecurEnvoy, Whalebone a Labyrinth.

Kybernetická bezpečnost v průmyslovém prostředí

S kybernetickými útoky v průmyslovém prostředí se setkáváme stále častěji. Provozní technologie jsou mnohem zranitelnější než informační technologie a bezpečnostní incidenty jsou destruktivnější a většího rozsahu.

Často mají OT zařízení nedostatečný výkon pro implementaci bezpečnostních mechanismů, jako je šifrování a pokročilé autentizační protokoly. Mnoho těchto zařízení bylo navrženo před desítkami let, aniž by se počítalo s provázaností do IT světa, a většina z nich nemá bezpečnost integrovanou „by design“. Také je důležité porozumět a správně používat standard IEC 62443 pro zabezpečení operačních technologií.

Abychom předešli kybernetickým útokům, potřebujeme detekovat zranitelnosti, anomálie v síti, monitorovat všechna zařízení a včas indikovat náznaky útoku. Správně zvolené technologie nám pomohou zajistit kybernetickou bezpečnost i v průmyslovém prostředí.

COMGUARD pro ochranu operačních technologií nabízí **OT Guard**, který spojuje několik technologií, které působí synergicky a dokážou pokrýt nejdůležitější oblasti v OT bezpečnosti.

Honeywell SCADAfence monitoruje síťový provoz a dává nám přehled o OT sítích, komunikačních vzorcích a potencionálních útocích. Proaktivně upozorňuje na zranitelnosti a rizika v OT síti.

Barracuda Next Generation Firewall se postará o ochranu proti různým kybernetickým hrozbám, zajistí segmentaci sítě a umožňuje nám sledovat a analyzovat veškerý síťový provoz v OT síti. Pomocí firewallu můžeme striktně kontrolovat přístup k OT zařízením a systémům.
Wallix PAM4OT je platforma pro správu přístupů a hesel (PAM), která je speciálně přizpůsobena pro operační technologie. Umožňuje organizacím centralizovaně spravovat a řídit přístup k OT zařízením a systémům, což je klíčové pro zajištění bezpečnosti v průmyslovém prostředí. Navíc poskytuje nástroje pro audit všech aktivit a přístupů k OT zařízením.

Řečníci

Ilja David
OT/IT Security, IRON OT

Ilja David spoluzaložil společnost Iron OT, která se specializuje na průmyslovou kybernetickou bezpečnost a kritickou infrastrukturu. Své hlavní pracovní zkušenosti nabral v Německu, kde pracoval mmj. jako vedoucí bezpečnostní architekt ve společnosti Airbus Defence and Space. Zde vedl mmj. část výzkumného projektu Evropské unie CyberSEAS zaměřeného na kybernetickou bezpečnost energetické kritické infrastruktury a bezpečnostní projekty pro Airbus Hellicopters a Airbus Commercial.

Dříve také pracoval v DNV jako Senior Cyber Security Expert pro ropný, plynárenský a námořní průmysl a ve společnosti Nestlé jako Factory IS/IT Security Officer, kde řídil kybernetickou bezpečnost současně pro 130 továren v Evropě, střední Asii a Africe.

V současné době pokračuje v doktorandském studiu na Univerzitě Tomáše Bati ve Zlíně, kde dále rozvíjí předchozí evropský výzkum. Je držitelem certifikace CISSP, certifikátů Marshall Centre for European Security Studies a IEC 62443 Expert. Zároveň je zároveň členem ISA 99 jenž vytváří standardy řady IEC 62443. Současně je autorem mnoha publikací v oblasti OT kybernetické bezpečnosti.

Jak ovládnout IEC 62443: Pokročilé metody kybernetické bezpečnosti pro průmysl a kritickou infrastrukturu

Helena Hrašková
Account & Vendor Manager, COMGUARD a.s.

Helena Hrašková působí v roli obchodní konzultantky a produktové manažerky u distributora COMGUARD a.s., který působí jako Value Added Distributor v oblasti kybernetické bezpečnosti. Úzce spolupracuje s výrobci a obchodními partnery a ve své obchodní profesi se zaměřuje výhradně na kybernetickou bezpečnost. V Comguardu je zodpovědná za oblast kybernetické bezpečnosti v průmyslovém prostředí.

Jak ovládnout IEC 62443: Pokročilé metody kybernetické bezpečnosti pro průmysl a kritickou infrastrukturu

Ondřej Hubálek
Cyber Security Presales Engineer, GREYCORTEX

IT profesionál se osmnáctiletou praxí v oblastí síťové infrastruktury a kybernetické bezpečnosti. Srdcem je síťař, ale uvědomuje si klíčovou roli kybernetické bezpečnosti. V rámci řešení GREYCORTEX Mendel obě tyto oblasti znalostí propojuje a nadále rozvíjí.

Z pohledu komplexního přístupu k problematice kybernetické bezpečnosti je zastáncem nových trendů v oblasti budování cyber security ecosystémů a robustních XDR platforem, zvláště pak pokud obsahují potřebný kamínek skládačky, NDR systém GREYCORTEX Mendel.

Efektivní využití nástroje GREYCORTEX Mendel pro ochranu OT sítí

IRON OT - PRŮMYSLOVÁ KYBERNETICKÁ BEZPEČNOST

Iron OT je evropská společnost nové generace, specializující se na řízení kybernetické bezpečnosti, ochranu provozních technologií (OT) a informačních technologií (IT).

Dohromady přes 30 let zkušeností s průmyslovými systémy a kybernetickou bezpečností týmu Iron OT zajistí Vaší organizaci efektivní zvýšení kybernetické bezpečnosti, a to primárně prostřednictvím zavedení Systému řízení kybernetické bezpečnosti podle normy IEC 62443 a jeho propojením s informační IT bezpečností založené na normě ISO 27001 (ISMS).

Iron OT nabízí moderní přístup ke kybernetické bezpečnosti a specializovaná řešení vytvořená přesně na míru pro konkrétní organizace, berouc v potaz specifika průmyslových prostředí různých velikostí a složitosti.

NAŠE SPECIALIZACE

- Kritická infrastruktura
- Chemický, farmaceutický, energetický, ropný, dopravní, výrobní průmysl a další
- Zabezpečení SCADA, DCS, PLC, MES, robotů a další
- Konvergence IT/OT prostředí
- Systémy Řízení Kybernetické a Informační Bezpečnosti
- Posouzení a kompletní návrh řešení bezpečnosti
- Kompletní design bezpečnosti technologických celků

Follow us:

ŠPIČKOVÁ KVALITA ŘEŠENÍ

- Implementace Systému řízení kybernetické bezpečnosti (IEC 62443) pro průmyslové technologie i Systému řízení bezpečnosti informací (ISO 27001) pro informační technologie (IT)
- Bezpečnostní analýza organizace dle IEC 62443, ISO 27001, NIS 2 a dalších frameworků
- Analýza rizik kybernetické bezpečnosti pro průmyslové technologie (OT) nebo informační technologie (IT)
- Informační servis o hrozbách a zranitelnostech průmyslových technologií (OT)
- Školení kybernetické bezpečnosti (OT i IT) pro management, zaměstnance a dodavatele
- Cvičení reakce na kybernetické bezpečnostní incidenty pro průmyslové systémy (OT)
- Tvorba inventáře průmyslových technologií (OT)
- Zpracování nákresů architektury průmyslových technologií (OT)
- Program technické vizuální kontroly průmyslového prostředí
- Filosofie návrhu kybernetické bezpečnosti pro konkrétní technologický celek (nový řídicí systém, výrobní linka, továrna, atd.) dle IEC 62443-3-3 a dalších standardů
- Tvorba specifických dokumentů souvisejících s kybernetickou bezpečností (politky, procedury, plány kontinuity provozu, plány obnovy po incidentu atd.)
- Hodnocení bezpečnosti dodavatelského řetězce
- Robustifikace průmyslového řídicího systému
- Posouzení bezpečnosti PLC, segmentace IT/OT sítí, nastavení IDMZ, forenzní analýza a mnoho dalších specializovaných řešení

The European Union Security Company

Petr Kolouch
Místopředseda představenstva, COLSYS – AUTOMATIK, a.s.

Petr Kolouch se ve své praxi již více než 15 let specializuje na oblast průmyslových komunikací.

K oboru ho přivedl zájem o řízení technologických procesů a o dění v průmyslu obecně.

Absolvoval FEL ČVUT v Praze, obor elektrické stroje, přístroje a pohony.

Odborně se zaměřuje na spolehlivé a bezpečné komunikace výrobních systémů. Zajišťuje rovněž technickou a produktovou podporu pro průmyslové komunikační komponenty HIRSCHMANN.

Pracuje též jako projektant komunikačních systémů a je autorizovaným inženýrem ČKAIT.

Bezpečné vazby mezi IT a OT v dnešní kyber éře

Jan Kopřiva
Senior Security Consultant, ALEF NULA

Jan Kopřiva je specialistou na kybernetickou bezpečnost s dlouhou praxí a širokými zkušenostmi.

V současnosti působí mimo jiné jako konzultant ve společnostech Alef Nula a Nettles Consulting a také jako jeden z bezpečnostních odborníků ve světoznámém sdružení SANS Internet Storm Center. Profesně se zaměřuje mj. na bezpečnostní analytiku, reakci na incidenty, analýzu malware a další aspekty tzv. „modré“ bezpečnosti, ale také oblasti penetračních testů, red teamingu a ofenzivní bezpečnosti obecně. Je autorem řady bezpečnostních kurzů, odborných výzkumů a článků zaměřených na různé aspekty kybernetické bezpečnosti a pravidelně přednáší na domácích i zahraničních odborných konferencích.

3 velké výzvy OT bezpečnosti a jak se s nimi vypořádat

Dušan Mareček
Expert IKB JE, ČEZ

Dušan Mareček od roku 1995 spojil svoji kariéru se skupinou ČEZ, a.s.

Účastnil se spouštění bloků v Temelíně, spolupracoval při tvorbě SKŘ v ETE. Následně prošel výrobními úseky na funkcích operátor sekundárního okruhu, operátor primárního okruhu a vedoucí blokové dozorny – kde řídil složité technologické celky jaderné elektrárny. Od roku 2017 se věnuje informační a kybernetické bezpečnosti v Divizi JE, nejprve na pozici Vedoucí útvaru IKB v DJE a následně od roku 2020 pracuje na pozici Expert IKB JE v centrálním útvaru SKČ.

Kyberbezpečnost v jaderné energetice

AUXILIUM
Pentest Labs

EMPOWERING
SAFER STREETS

- 2015 – Founded in Germany as security consultancy
- 2018 – First automotive cyber security project
- 2019 – Established Auxilium Pentest Labs in Prague
- 2021 – First full vehicle penetration test
- 2023 – Established Auxilium Pentest Labs in Detroit

20 pentest engineers on the team

100+ years of cybersecurity experience

Clients from Europe, North America, Asia

OUR TEAM

- 100+ successful projects in Automotive pentesting
- Clients in Europe, North America and East Asia
- 20 experts in automotive penetration testing
- Conference talk at CCC, TROOPERS and DeepSec
- 4 0-day vulnerabilities responsibly disclosed
- 4 university theses defended
- Automotive cyber security subject at CTU Prague

WHY OUR PARTNERS CHOOSE US?

- References: Long-list of satisfied global customers
- Flexibility: Always able to start project within 1 week
- Scalability: 50% growth sustained over 5 years
- Quality: OSCP, OSCE, OSWE, CREST, CISSP certified team members
- Diversity: International team (13 nationalities)
- Research: Academic research, teaching, 0-day research
- Cost-efficiency: Higher than in-house team

Visit us at: auxilium-labs.com

Jan Nguyen
Cyber Security Consultant, Seyfor a.s.

Jan Nguyen je absolventem FEL ČVUT Praha se zaměření na síťovou bezpečnost. Začínal jako síťový a systémový administrátor a v současné době vede tým technických konzultantů se zaměřením na kybernetickou bezpečnost. V oblasti kybernetické bezpečnosti se pohybuje prakticky od dob studia a dále se věnuje také oblasti etického hackingu.

Fortinet Security Fabric: Vaše OT sítě pod neprůstřelným štítem

---

Jan Zdrha
Oddělení bezpečnosti operačních technologií, NÚKIB

Referent bezpečnosti státu. Specialista na zabezpečeni OT a ICS systémů a bezpečnost IT systémů postavených na platformě Microsoft Windows.

Polygon operačních technologií verze 0.2

Bohuslav Zůbek
Ministerstvo vnitra ČR

Bohuslav Zůbek působil jako předseda pracovní skupiny SIS-TECH v Bruselu během předsednictví ČR v Radě Evropy (11/08 - 03/09). Pracoval jako člen akceptačního týmu při schvalování vstupu ČR do Evropské unie, připravoval Schengenský informační systém I. generace a II. generace, byl zástupcem v komisích EU a výborech projektových manažerů za ČR v oblasti Schengenu. Působil jako vedoucí projektových týmů při realizaci projektů informačních systémů a databázových center v oblastech policie ČR. Od dubna 2021 vykovává funkci vedoucího samostatného oddělení kybernetické bezpečnosti na MV.

Bezpečnostní hrozby v kyberprostoru

Partneři konference

ALEF NULA, a.s.

Pernerova 691/42
186 00 Praha 8
+420 225 090 111
cz-sales@alef.com
www.alef.com

ALEF působí na trhu již od roku 1994, letos na podzim oslavíme 30. narozeniny. Cítíme hodnoty jako dlouhodobá spolupráce, prozákaznický přístup a odborné kompetence. Poskytujeme dodávky a služby moderního a funkčního ICT řešení, založeného na elitních značkách v oboru, profesionálním přístupu a bohatých zkušenostech. Naše služby pokrývají celý životní cyklus ICT projektů – od předběžné analýzy, přes navržení a implementaci řešení, školení a certifikaci, až po údržbu, podporu a financování. Tyto služby jsou dostupné pro široké spektrum klientů, od malých a středních podniků až po velké mezinárodní korporace.

V oblasti technologií se zaměřujeme především na produkty a služby od společností jako Cisco, NetApp, Splunk, Flowmon, Microsoft a AWS. Naše odborné znalosti zahrnují nejen teoretické aspekty těchto technologií, ale i praktické zkušenosti z reálných zákaznických projektů, což nám umožňuje efektivně minimalizovat rizika spojená s řízením ICT. Velmi si zakládáme na expertní úrovni technických znalostí, což z nás činí důvěryhodného partnera v oblasti ICT řešení.

PARTNER KONFERENCE

Auxilium Cyber Security s.r.o

Jankovcova 1627/16a
170 00 Praha 7
30100 Telegraph Rd, Ste 481
Bingham Farms, MI 48025
+420739467470
martin.pozdena@auxilium-labs.com
auxilium-labs.com

“Empowering Safer Streets: Your Automotive Cybersecurity Partner“

At Auxilium Pentest Labs, our passionate team specializes in automotive cybersecurity. With our stateof-the-art penetration testing laboratories, we possess the capability to comprehensively assess complete vehicles or Electronic Control Units (ECUs) across various automotive systems, including infotainment, gateway, ADAS, and OBC, as well as ICE and EV powertrains. Since our establishment, we‘ve successfully conducted dozens automotive penetration tests for leading OEMs and Tier-1 suppliers across Europe, Asia, and the Americas. Beyond our practical expertise, we actively engage in automotive security research, collaborating with academic institutions and presenting at conferences. Partner with us to fortify your automotive cybersecurity defenses and drive innovation in this dynamic industry.

COFFEE BREAK PARTNER

COLSYS – AUTOMATIK, a.s.

Huťská 1294
272 01 Kladno
+420 312 285 312
obchod@colaut.cz
www.colaut.cz

Jsme od založení v roce 1998 ryze česká inženýrská společnost, která poskytuje služby a dodávky v oblasti kritické komunikační infrastruktury (KKI) v průmyslu, dále v oblasti systémů pro řízení a dohled nad energetickými celky a konečně v oblasti automatizovaných systémů pro řízení technologií.

V oblasti průmyslové KKI se zabýváme analýzou a hodnocením rizik, analýzou provozu, návrhy a doporučeními (nejen) pro povinné subjekty a celkovým návrhem koncepce, konfigurace i provozu celé KKI až k realizaci a servisu.

HLAVNÍ PARTNER KONFERENCE

COMGUARD, a.s.

Sochorova 38
616 00 Brno
+ 420 770 161 073
helena.hraskova@comguard.cz
www.comguard.cz

COMGUARD je Value Added Distributor (B2B) se specializací na IT bezpečnost. Působíme v České republice a na Slovensku. Naše komplexní řešení plně odpovídají potřebám velkých firem, včetně datových center, ale i menších a středních podniků. Zaměřujeme se na bezpečnost koncových stanic, ochranu perimetru, ochranu citlivých dat, vyhodnocování potencionálních rizik, kybernetické bezpečnosti v průmyslovém prostředí a dalších oblastí. Navíc poskytujeme expertní služby jako je například penetrační testování a Security Operation Center (SOC).

PARTNER KONFERENCE

GREYCORTEX, spol. s r.o.

Purkyňova 649/127
612 00 Brno
+420 733 601 442
info@greycortex.com
www.greycortex.com

GREYCORTEX je jedním z hlavních poskytovatelů bezpečnostního řešení NDR (Network Detection and Response) pro IT i OT (průmyslové) sítě. Zajišťuje jejich bezpečnost a spolehlivost. Produkt GREYCORTEX Mendel je řešení pro monitorování síťové bezpečnosti v IT i průmyslových (OT) sítích. Kombinací pokročilých metod detekce analyzuje síťový provoz a upozorňuje na škodlivé aktivity, běžné i neznámé moderní hrozby a provozní problémy sítě. Dokonale vizualizuje síťovou komunikaci na úrovních uživatelů, zařízení i aplikací a umožňuje systémovým analytikům a správcům sítě rychle a efektivně řešit bezpečnostní i provozní incidenty.

PARTNER KONFERENCE

Iron OT s.r.o.

Sokolovská 111/129
360 05 Karlovy Vary
+420 604 421 371
info@ironot.io
www.ironot.io

Iron OT je evropská společnost nové generace, specializující se na kvalitní řízení průmyslové kybernetické bezpečnosti a související ochranu provozních technologií (OT).

PARTNER KONFERENCE

FUTURE FORCES FORUM

Future Forces®
INTERNATIONAL EXHIBITION
www.natoexhibition.org

OBRANA A BEZPEČNOST

- ▸ VÝSTAVA
- ▸ ODBORNÉ PANELY
- ▸ NETWORKING

16.–18. 10. 2024

www.fff.global