ControlTech

Value-Add Distributor
A ROCKWELL AUTOMATION PARTNER

Kybernetická bezpečnost v automatizovaných provozech pivovarů

ControlTech s.r.o.
Ovčáry 297, 280 02 Ovčáry
https://www.controltech.cz

Tomáš Glabazňa
Product Manager Software & IIoT
tglabazna@controltech.cz
+420 775 858 851

Zaměření této prezentace

ControlTech

OT – Operational Technology

V této prezentaci se zaměřujeme na kybernetickou bezpečnost OT sítí. Kybernetická bezpečnost OT provozů je relativně novým tématem. Množství efektivních SW a HW nástrojů pro zajištění kybernetické bezpečnosti v OT je na trhu omezeno.

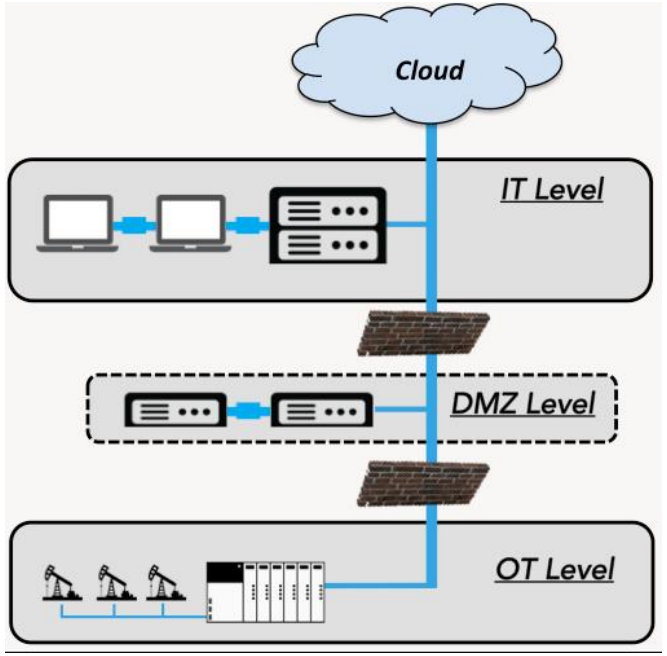
IT – Information Technology

Kybernetická bezpečnost IT prostředí je samozřejmě neméně důležitým tématem při řízení podniku. Technologické nástroje pro zajištění kybernetické bezpečnosti v IT sítích jsou však všeobecně poměrně dobře známé. Na trhu působí mnoho poradenských společností a výrobců HW či SW nástrojů pro řešení této problematiky.

Kybernetická bezpečnost v OT

Historicky byly OT sítě do značné míry izolované, proto byla jejich kybernetická zranitelnost nízká.

S postupující digitální transformací rostou požadavky na propojení OT a IT prostředí a jejich vzájemnou datovou komunikaci. Tím se OT sítě stávají zranitelnější pro kybernetické útoky.



škody způsobené kybernetickými útoky v průmyslu rostou

ControlTech

za poslední 3 roky

$12+B

škody způsobené ramsomware útoky

53%

průmyslových podniků bylo konfrontováno s kybernetickým útokem

Zdroj: *Cybersecurity Ventures. LNS Research Study.*

PROČ JSOU PRŮMYSLOVÉ PODNIKY TERČEM KYBERNETICKÝCH ÚTOKŮ?

Starší neudržovaná infrastruktura a nedostatek kvalifikovaných zdrojů pro řádné řízení kybernetických rizik. Protivníci vědí, že tato prostředí mají mnoho zranitelných míst a pokud jsou napadeni, mohou mít pro infikované vážné následky.

PROČ PIVOVARY?

Pivovary patří v České republice mezi významná a prestižní průmyslová odvětví, Proto mohou být lákavým terčem kybernetického útoku. Podíl automatizovaných zařízení v pivovarech narůstá, podniky se modernizují. Roste i objem datové komunikace mezi OT a IT prostředím, čímž se otvírá větší množství kybernetických rizik a zranitelností.

typy kybernetických útoků

typy kybernetických útoků
hacking
počítačové viry
phishing (získávání citlivých údajů)
neoprávněný monitoring dat
zneužití identity
social ingeneering (podvody)
denial of service (znefunkčnění zařízení zahlcením daty)

Denial of Service

Nejčastější druh kybernetické hrozby v průmyslovém prostředí. Zařízení je zahlceno velkým objemem datové komunikace, kterou nestihne zpracovávat. Tím je vyřazeno z provozu a dojde k přerušení výroby.

nové požadavky na kybernetickou bezpečnost v průmyslu

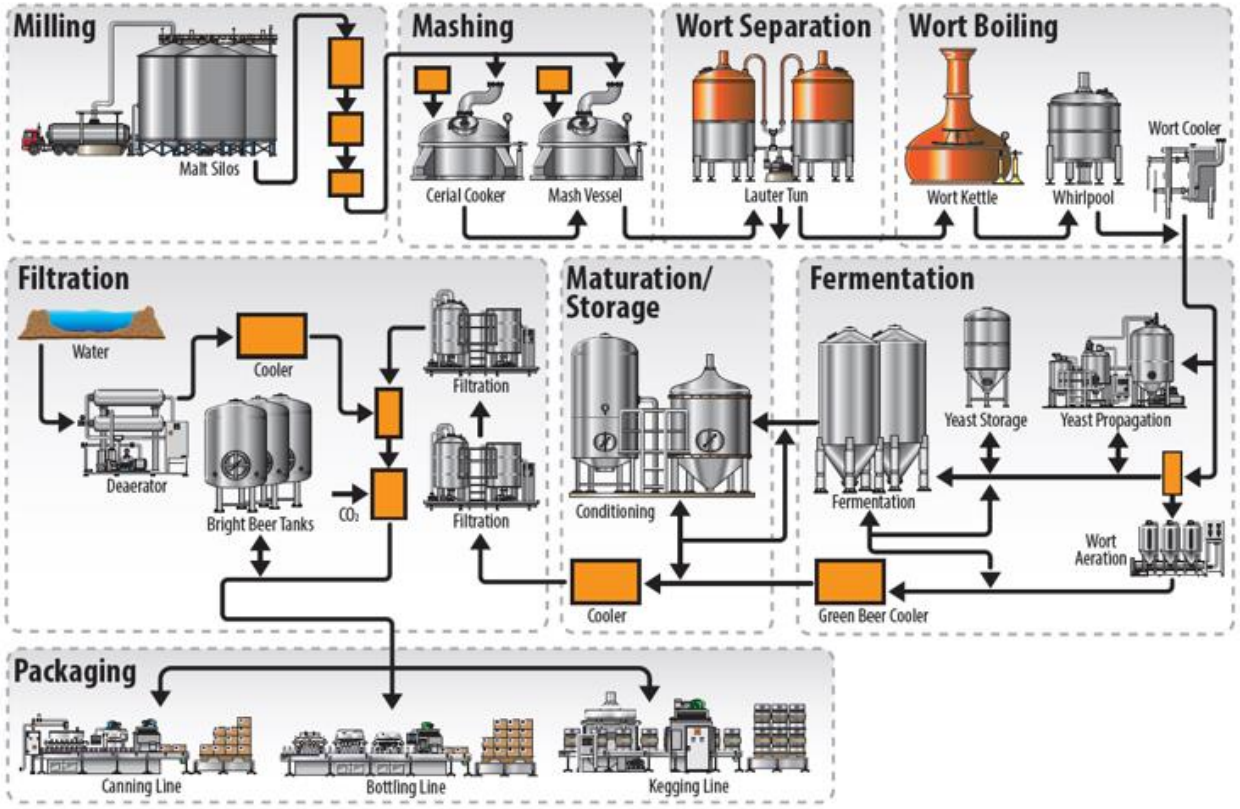
Digitální transformace vytváří kybernetická rizika pro průmyslové provozy, která je třeba zmírnit.

	INSIDERS	TERRORISTS	HACKTIVISTS	CYBERCRIMINALS
situace	• zařízení komunikující vlastními protokoly • Vznikající technologie s novými komunikačními metodami • zánik tradičního izolovaného modelu OT sítí	• Omezené chápání přirozeného rizika OT prostředí • Mezery v porozumění kompenzujících control • Není jasné, jak upřednostňovat zmírňování rizik	• Oportunistické útoky, jako je ransomware, jsou stále aktivní • Cílené útoky kyberzločinců za účelem finančního zisku • Cílené útoky hacktivistů sponzorovaných některými státy	• Nástroje IT Security nemají nativní viditelnost do prostředí OT • Osoby s rozhodovací pravomocí potřebují komplexní pohled na podniková rizika
nové požadavky	• viditelnost všech zařízení, jejich síťové komunikace a procesů • viditelnost OT, IT a IIoT zařízení	• stanovení inherentního rizika OT zařízení • stanovení opatření ke zmírnění rizik • stanovení zbytkového rizika po použití kontrol	• monitorovat zbývající rizika a známky útoků • vytvořit odolný detekční model pro zjištění různých útočných vektorů	• Propojit OT zabezpečení s architekturou zabezpečení IT • Poskytnout osobám s rozhodovací pravomocí komplexní pohled na rizika OT

nekriminální kybernetické hrozby

Cílené útoky sofistikovaných hackerů nejsou zdaleka jedinou hrozbou pro kybernetickou bezpečnost vašeho pivovaru

Nepřátelský vstup útočníka do automatizovaného provozu vašeho podinku je pouze jedním z kybernetických rizik, se kterými se v praxi můžeme setkat. Je třeba si uvědomit, že existují i rizika vyplývající z běžného každodenního provozu v automatizované výrobě.



- patch management
- přístup k periferiím a rozhraním (USB)
- nezodpovědná správa hesel
- nedodržení vnitropodnikových směrnic
- a další

kybernetická bezpečnost – srovnání IT a OT

ControlTech

problematika	IT (ISMS)	OT (IACS)
antivirový SW	široce používaný, snadno aktualizovatelný	komplikovaný, často nelze implementovat
životní cyklus	3-5 let	5-20 let
povědomí	dobré	nízké
správa patchů	častá, pravidelná	není zvykem, mnohdy vyžaduje souhlas výrobce
management změn	pravidelný a plánovaný	není zvykem
vyhodnocování logů	zavedená praxe	nezvyklé
zpoždění	zpoždění jsou akceptovatelná	zpoždění jsou kritická
dostupnost	ne nutně vždy	nutně 24x7
testy zabezpečení	rozšířené	vzácné a problematické
testovací prostředí	k dispozici	většinou není k dispozici

mezinárodní normy
pro kybernetickou bezpečnost

ControlTech

IT Security Policies and Practices
(ISO 2700x Series)

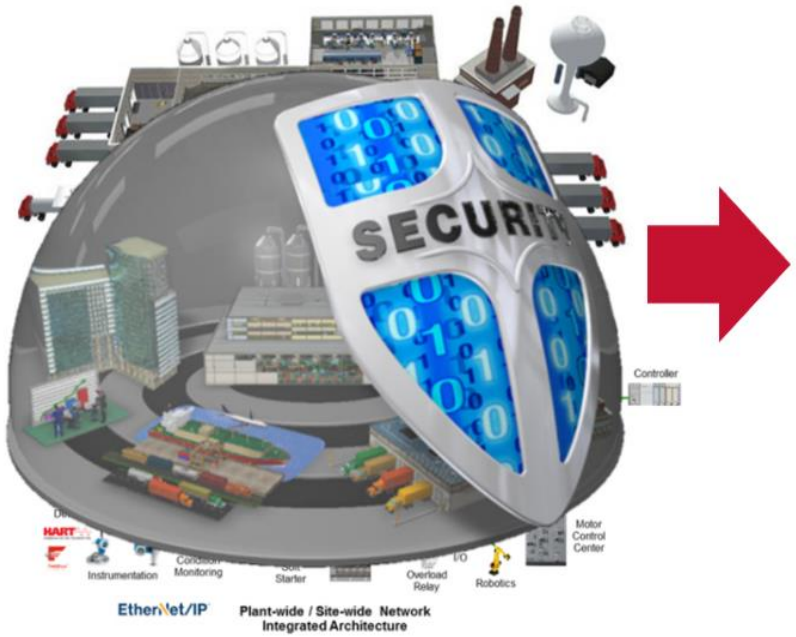
Security for Industrial Automation
and Control Systems
(ISA/IEC62443)

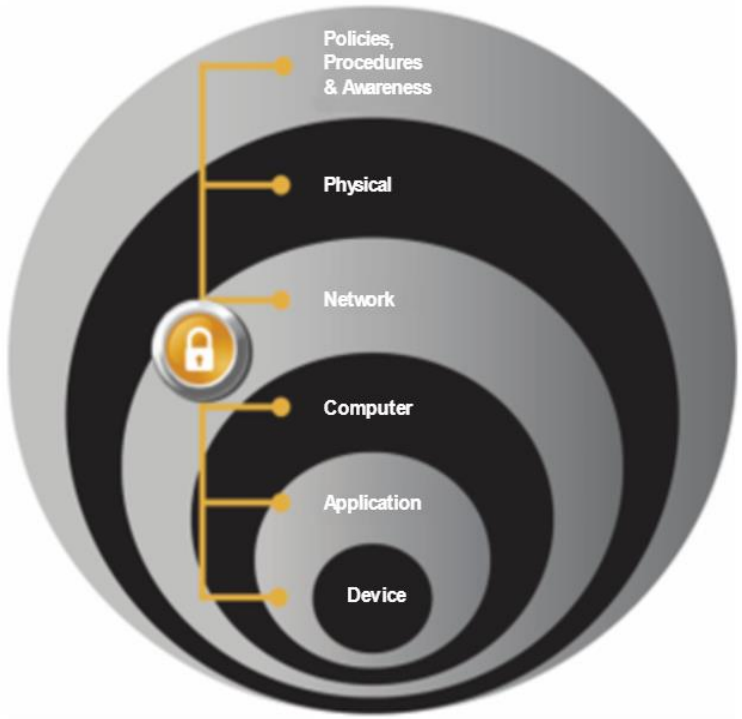
defence-in-depth

ControlTech

KOMPLEXNÍ HLOUBKOVÁ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI

Neexistuje jeden SW nebo HW produkt, jehož zakoupení a instalací by byla kybernetická bezpečnost automatického provozu zcela zajištěna.





KONCEPT DEFENSE-IN-DEPTH

je založen na analýze rizik a zajištění bezpečnosti na několika různých vrstvách:

- **vnitropodnikové předpisy a nařízení**
- **fyzické zabezpečení**
- **zabezpečení sítě**
- **zabezpečení počítačů**
- **zabezpečení aplikací**
- **zabezpečení průmyslových automatizačních zařízení**

ControlTech

Value-Add Distributor

A ROCKWELL AUTOMATION PARTNER

Naše řešení pro kybernetickou bezpečnost

ControlTech s.r.o. jako autorizovaný distributor Rockwell Automation nabízí hardwarová, softwarová a poradenská řešení pro zajištění kybernetické bezpečnosti automatizovaných průmyslových provozů.

ControlTech

Value-Add Distributor

A ROCKWELL AUTOMATION PARTNER

THINMANAGER

A Rockwell Automation Technology

software pro správu tenkých klientů

ControlTech

THINMANAGER
A Rockwell Automation Technology

výhody využití tenkých klientů v průmyslu

Tencí klienti jsou počítače, které pracují v přímé závislosti na centrálním počítači (serveru). Jejich použití v průmyslové automatizaci přináší řadu výhod:

- Tenký klient nemusí obsahovat operační systém. Tím odpadají problémy spojené s aktualizací operačního systému, výkon stroje je navíc plně využit k plnění určených úkolů.
- Tenký klient nemusí obsahovat fyzické datové úložiště (pevný disk). Při výpadku stroje tedy nehrozí riziko ztráty dat, která jsou bezpečně uložena na serveru.
- Při zachování požadovaného výkonu má tenký klient výrazně nižší hardwarové nároky. Využitím tenkých klientů je tedy možné snížit celkovou cenu investice.
- Výměna zařízení při výpadku nebo poruše se v případě tenkých klientů obejde bez obnovování operačního systému a potřebných aplikací. Výrazně se tak snižuje doba prostojů při těchto zásazích údržby.
- V neposlední řadě využití tenkých klientů minimalizuje riziko ohrožení malwarem či jiným nežádoucím SW, který by mohl negativně ovlivnit chod a výkon zařízení.

ControlTech

THINMANAGER
A Rockwell Automation Technology

další bezpečnostní prvky

no local storage	žádná data nejsou uchovávána na jednotlivých koncových zařízeních
Windows Desktop blocked	možnost zablokování přístupu na pracovní plochu operačního systému Windows
no data from USB	v základním nastavení jsou USB porty koncových zařízení blokovány a slouží pouze k připojení klávesnice nebo myši
redundancy	podpora redundantního zapojení tenkých klientů, přechod na záložní zařízení v reálném čase, bez ztráty dat

ControlTech

THINMANAGER
A Rockwell Automation Technology

Správa uživatelského přístupu

ThinManager umožňuje nastavit oprávnění pro přístup k poskytovanému obsahu jednotlivým uživatelům nebo uživatelským skupinám.

- podpora systému Active Directory
- doručování notifikací na jednotlivá koncová zařízení
- doručování emailů na autentifikované emailové adresy
- podpora biometrických údajů – přihlašování uživatelů pomocí otisku prstu či detekce obličeje
- nově ve verzi 12 – podpora zjednodušené autentikace uživatele číselným PIN kódem

ControlTech

Value-Add Distributor
A ROCKWELL AUTOMATION PARTNER

CIP Security

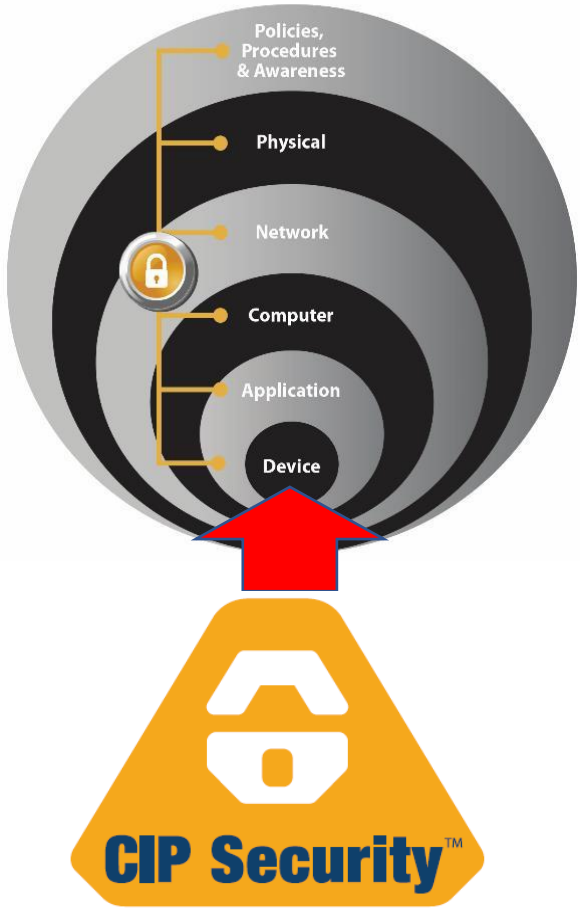
zabezpečení jednotlivých automatizačních zařízení
kryptování síťové komunikace

CIP Security

ControlTech

CIP Security protokol je standardem zabezpečené komunikace mezi zařízeními v OT síti. Zařízení komunikující na bázi CIP Security protokolu musí být schopno:

- odmítnout data, která byla při přenosu pozměněna
- odmítnout datové zprávy od nevěrohodných uživatelů a zařízení
- odmítnout instrukce k provedení akcí, které nejsou povoleny



CIP Security

Tři základní principy:

ověřování koncových bodů – pomocí x.509 certifikátů nebo sdílených klíčů se provádí ověření zdroje i adresáta datové zprávy

integrita dat – pomocí TLS message authentication code se ověřuje, že zpráva nebyla během přenosu pozměněna (ochrana proti útokům Man-in-the-Middle (MitM)

kryptování dat – šifrování dat pomocí TLS a DTLS kryptografických protokolů (ochrana proti monitorování, resp. zneužití dat neoprávněným uživatelem)

CIP Security

Produkty Rockwell Automation s nativní podporou CIP Security:

software

- **FactoryTalk Policy Manager** (verze 6.11 +)
- **FactoryTalk System Services** (verze 6.11 +)
- **FactoryTalk Linx** (verze 6.11 +)
- **Studio 5000 Logix Designer** (verze 31 s využitím 1756-EN4TR komunikačního modulu, verze 32 + i bez tohoto modulu)

CIP Security

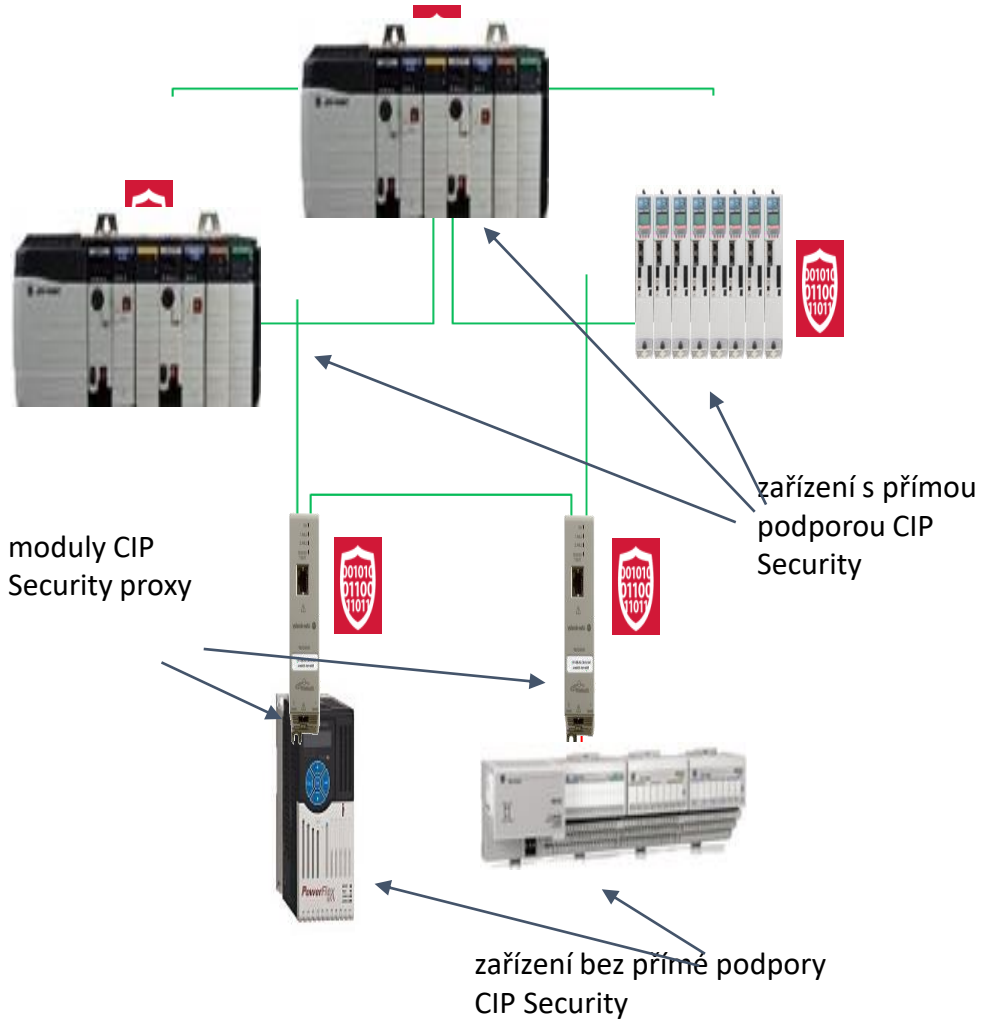
Produkty Rockwell Automation s nativní podporou CIP Security:

hardware

- **ControlLogix 5580 controllers**
- **1756-EN4TR ControlLogix EtherNet/IP Communication Module**
- **Kinetix 5300 drives**
- **Kinetix 5700 drives**
- **PowerFlex 755T drives**
- **1783-CSP CIP Security Proxy**

CIP Security

1783-CSP CIP Security Proxy



1783-CSP CIP Security Proxy představuje samostatné hardwarové řešení kybernetické bezpečnosti pro ta zařízení, která vestavěnou podporou **CIP Security** nedisponují.

ControlTech

Value-Add Distributor

A ROCKWELL AUTOMATION PARTNER

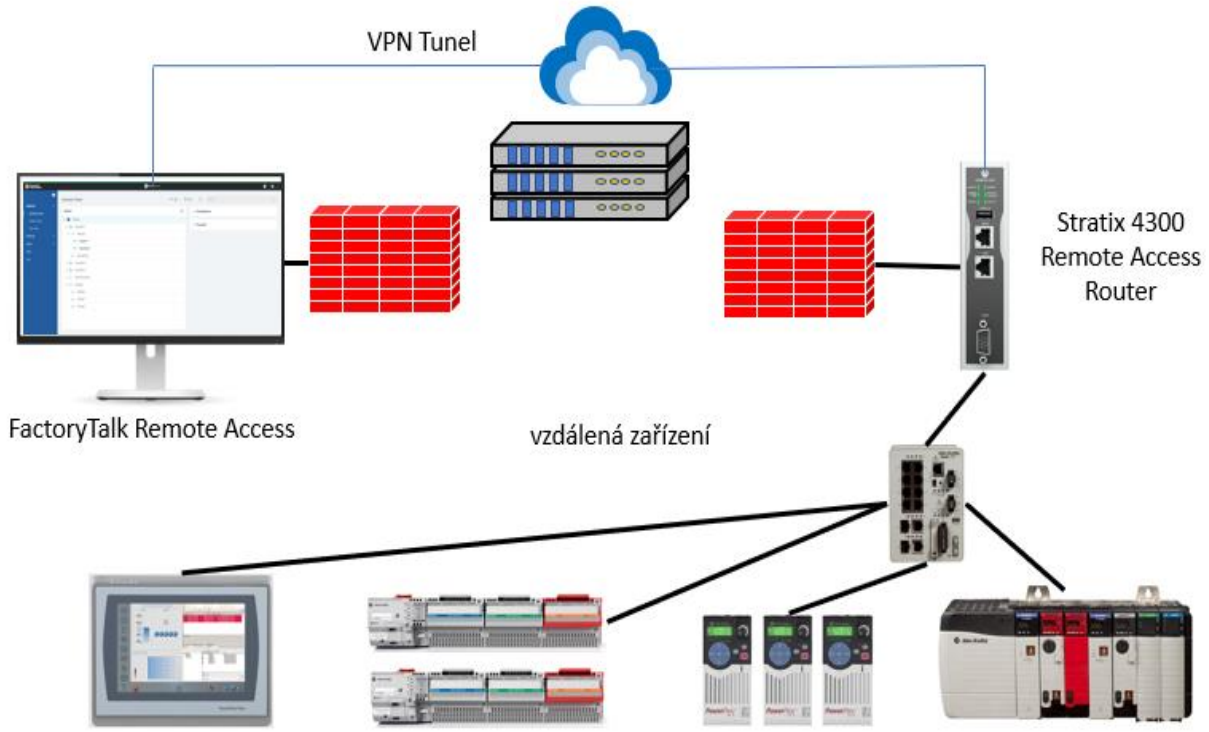
Remote Access for Industrial Equipment

zabezpečený vzdálený přístup k automatizačním zařízením

Remote Access for Industrial Equipment

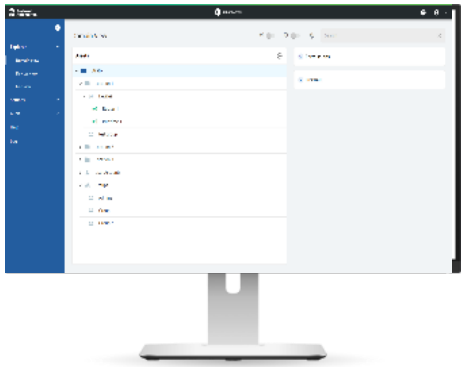
ControlTech

Vzdálené zabezpečené VPN připojení



Remote Access for Industrial Equipment

ControlTech



+

Integrace dvou produktů

HARDWARE: Stratix 4300 Remote Access Router

SOFTWARE: FactoryTalk Remote Access

Remote Access for Industrial Equipment

ControlTech

Stratix 4300 Remote Access Router

Stratix 4300 Remote Access Router	1783-RA2TGB	1783-RA5TGB
Total RJ45 ports	2	5
WAN	1 GE	1 GE
LAN	1 GE	4 GE
USB 2.0	✓	✓
Serial port	✓	✓
Digital input/output	✓	✓

Remote Access for Industrial Equipment

FactoryTalk Remote Access – 9545C-FTRAT1(1,2)

webový klient pro centralizovanou správu vzdáleného přístupu.

- Inicializuje VPN vzdálené připojení a registruje dostupná zařízení
- Nabízí správu uživatelského přístupu – vytváření uživatelů, uživatelských skupin a nastavení jejich přístupu k jednotlivým zařízením
- Umožňuje konfiguraci **Stratix® 4300** routeru a nastavení oprávnění
- Zaznamenává a zobrazuje historii vzdálených připojení a uživatelské aktivity
- Přístup přes FactoryTalk Hub (Operation Hub)

ControlTech

Value-Add Distributor

A ROCKWELL AUTOMATION PARTNER

Poradenství v kybernetické bezpečnosti

poradenské služby poskytované certifikovaným partnerem

Poradenství v kybernetické bezpečnosti

ControlTech

Spolupracujeme s partnerskou společností, která se stala prvním držitelem certifikátu pro normu IEC 62443-2-4 v České republice.

Primárním cílem této normy je zajistit bezpečný provoz průmyslových automatizačních systémů a ochránit tak všechny komponenty systému před nechtěnými zásahy.

Náš partner splňuje požadavky, podmínky a kritéria tohoto mezinárodního standardu pro tvorbu projektů, integraci řídicích systémů a IT sítí.

Zákazníkům tak dokážeme poskytnout systematický a praktický přístup ke kybernetické bezpečnosti jejich průmyslových systémů. Jelikož se jedná o mezinárodní certifikaci, naše navrhovaná řešení jsou uznávaná téměř na celém světě.

Poradenství v kybernetické bezpečnosti

ControlTech

- Analýza rizik
- Analýza zabezpečení OT sítě a komponent
- Návrh zajištění zabezpečení bezdrátových sítí
- SIS – Safety Instrumented Systems – návrh a jejich zabezpečení
- Návrh a poskytování přesné dokumentace logické a fyzické infrastruktury
- Zabezpečení vzdáleného přístupu
- Kybernetické bezpečnostní incidenty (zvládání, vyhodnocení, náprava)
- Dokumentování přístupových účtů
- Ochrana před malware včetně vyhodnocení, schválení a testování
- Instalace a správa patchů a bezpečnostních záplat
- Specifikace a dokumentace ke správě a provádění zálohování dat a konfigurací

ControlTech

Value-Add Distributor

A ROCKWELL AUTOMATION PARTNER

Claroty Continuous Threat Detection

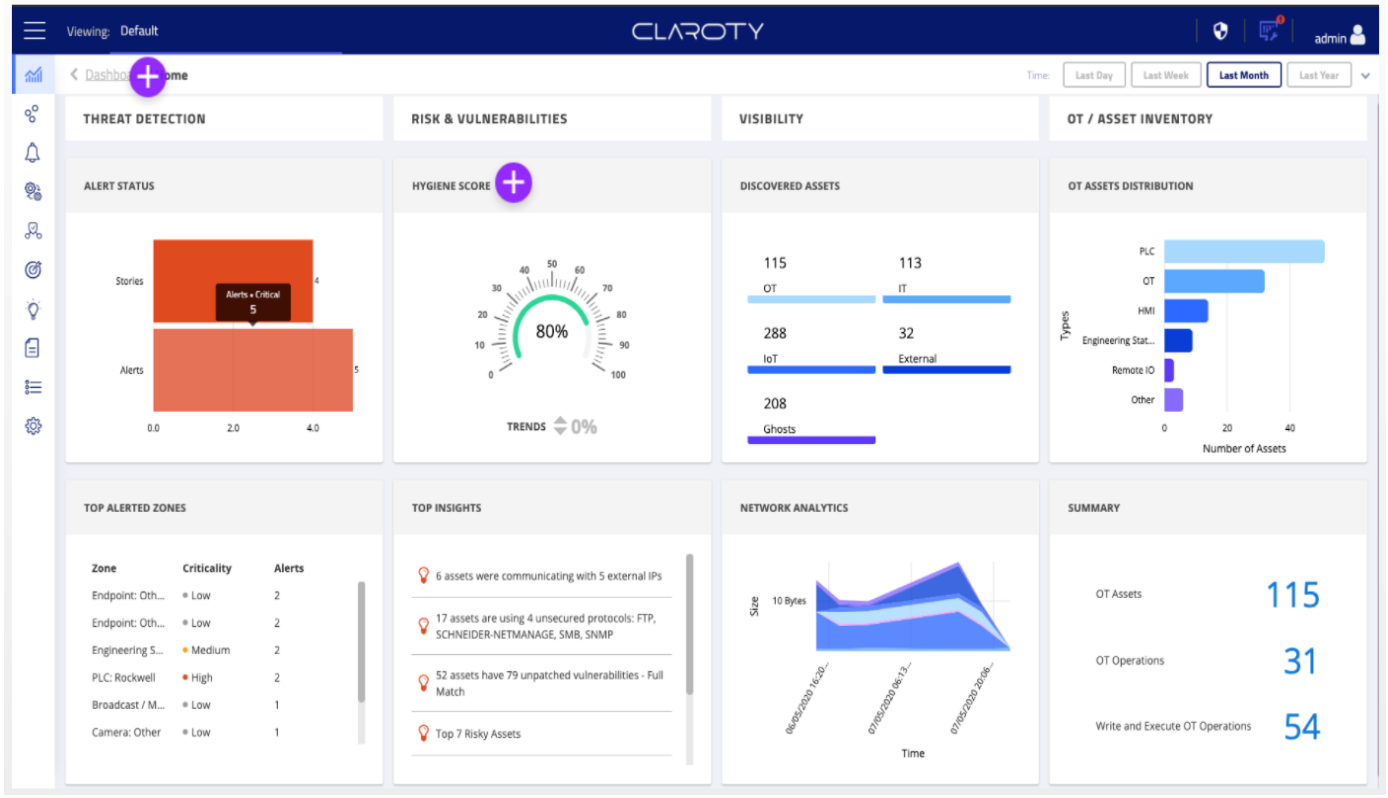
systém pro permanentní kontrolu síťového provozu a detekci hrozeb

ControlTech

CLAROTY

CONTINUOUS THREAT DETECTION

- viditelnost a správa zařízení
- segmentace sítě
- management rizik
- detekce anomálií a hrozeb



CONTINUOUS THREAT DETECTION

Viditelnost a správa zařízení

- Claroty CTD poskytuje detailní viditelnost všech OT, IoT a IIoT zařízení v průmyslové síti, včetně sériových sítí

- rozsáhlá knihovna průmyslových síťových protokolů – univerzální systém pro zařízení jakéhokoliv výrobce

ControlTech

CLAROTY

CONTINUOUS THREAT DETECTION

Viditelnost a správa zařízení

Asset visibility	zobrazení podrobných informací o každém zařízení, mimo jiné včetně čísla modelu, verze firmware, brány firewall, identifikace kartového slotu, apod.
Session visibility	sledování všech relací průmyslové sítě spolu s provedenými akcemi či změnami a s podrobnými údaji o cestě připojení
Process visibility	sledování všech průmyslových operací, programové aplikace a hodnoty tagů všech procesů, které na zařízeních probíhají. Vyhodnocování neobvyklých změn procesních hodnot, které by mohly představovat ohrožení integrity procesu.

CONTINUOUS THREAT DETECTION

Segmentace sítě

- CTD automaticky mapuje a virtuálně segmentuje průmyslové sítě na virtuální zóny - logické skupiny zařízení, která spolu za normálních okolností komunikují

- segmentace sítě výrazně snižuje bezpečnostní rizika

CONTINUOUS THREAT DETECTION

Management rizik a zranitelností

- CTD automaticky porovnává každé zařízení v OT síti s rozsáhlou databází nezabezpečených protokolů, konfigurací, nestandardních bezpečnostní postupů a dalších zranitelností
- pro porovnávání je k dispozici databáze společnosti Claroty, stejně tak i americká „Národní databáze zranitelností“
- pro tuto analýzu využívá systém CTD algoritmy umělé inteligence
- tato aktivní analýza zranitelností přispívá k maximální efektivitě při jejich odstraňování

ControlTech

CLAROTY

CONTINUOUS THREAT DETECTION

Detekce anomálií a hrozeb

- CTD využívá pět různých detekčních technologií k automatickému profilování všech zařízení, komunikací a procesů v průmyslové síti
- na základě monitoringu si automaticky vytváří model běžného provozu sítě
- v reálném čase pak upozorňuje na všechny anomálie, odlišnosti od běžného provozu a potencionální hrozby

Claroty SaaS for AssetCentre Add-on

ControlTech

Claroty SaaS for AssetCentre Add-on je rozšíření softwarového systému Rockwell Automation **FactoryTalk AssetCentre**. S jeho pomocí je možné rozšířit náhled na automatizační zařázení v síti o analýzu jejich rizik a zranitelností z pohledu kybernetické bezpečnosti.

Claroty SaaS for AssetCentre Add-on

- Poskytuje komplexní přehled rizik a zranitelností u aktiv spravovaných systémem **FactoryTalk AssetCentre**, a to včetně obtížně identifikovatelných vnořených zařízení a zařízení umístěných na úrovních 0-2.
- Navrhuje proveditelné kroky ke zmírnění rizik, a to jak jednotlivě, tak pro celé skupiny zranitelností.

ControlLogix Security Compute Module

ControlTech

ControlLogix Security Compute Module je kombinací vysokorychlostního integrovaného compute modulu pro řídicí systémy **ControlLogix** a softwarového produktu **Claroty Edge**. Tento produkt je navržen tak, aby poskytoval rychlou identifikaci připojených zařízení a okamžité údaje o rizicích a zranitelnostech těchto zařízení z hlediska kybernetické bezpečnosti.

ControlLogix Security Compute Module

ControlTech

- poskytuje komplexní přehled OT sítě a centralizovanou, plně automatizovanou inventarizaci všech připojených zařízení, dokonce i o obtížně identifikovatelných vnořených zařízeních a zařízeních umístěných na úrovních 0-2. Inventarizační data zahrnují popis hardwaru, modelové označení, aktuální verzi firmwaru, označení slotu, IP adresu, název výrobce zařízení a další související podrobnosti.

- provádí kontinuální monitoring bezpečnostních rizik a zranitelností na jednotlivých zařízeních a nabízí tak automatické uplatňování kroků sloužících ke zmírnění těchto rizik. Tento management zranitelností v reálném čase přispívá výrazně k redukci prostojů při řešení problémů kybernetické bezpečnosti.

- nabízí velice snadnou Plug and Play instalaci pouhým připojením compute modulu do šasi řídicího systému **ControlLogix.**

ControlTech

Value-Add Distributor
A ROCKWELL AUTOMATION PARTNER

závěrem mi dovolte popřát vašemu pivovaru co nejefektivnější automatizovanou výrobu nijak neohroženou kybernetickými riziky.

děkuji za pozornost

ControlTech s.r.o.
Ovčáry 297, 280 02 Ovčáry
https://www.controltech.cz

Tomáš Glabazňa
Product Manager Software & IIoT
tglabazna@controltech.cz
+420 775 858 851