Projekt "Cybersecurity in the interconnected industry"

Projektnr.: 2023-1-NL01-KA220-VET-000153812

Indholdsfortegnelse

Indhold

Introduktion til Operationel Teknologi (OT) og Cybersikkerhed

Hvad er Operationel Teknologi (OT)?

Operationel Teknologi (OT) omfatter **hardware- og softwaresystemer, der overvåger, styrer og automatiserer fysiske processer i industrielle omgivelser**. Disse systemer er afgørende for alt fra fabriksgulve til kraftværker, hvor de sikrer, at komplekse processer udføres sikkert, effektivt og uden afbrydelser.

OT's kerneformål:

- **Tilgængelighed**: OT-systemer skal køre kontinuerligt, ofte 24/7, da enhver uplanlagt nedetid kan stoppe produktionen, føre til dyre forsinkelser eller kompromittere sikkerheden.
- **Sikkerhed:** OT skal designmæssigt beskytte både menneskelige operatører og udstyr. Automatiske spærringer, fejlsikker logik og stringent testning forebygger farlige forhold.
- **Realtidskontrol:** OT kræver øjeblikkelig respons. Kontrolløkker opererer med millisekundpræcision for at opretholde stabilitet og præcision, f.eks. ved justering af tryk i en rørledning eller synkronisering af robotter.

Typiske anvendelser og karakteristika for OT-miljøer: OT anvendes i automatiserede produktionslinjer, rørledningsstyring, kemisk forarbejdning og elproduktion og -distribution. Karakteristika inkluderer:

- **Lang levetid for udstyr:** OT-enheder som Programmable Logic Controllers (PLC'er) og Remote Terminal Units (RTU'er) forbliver ofte i drift i årtier, langt ud over typiske IT-hardwareudskiftningscyklusser.
- **Proprietære kommunikationsprotokoller:** Mange OT-systemer bruger specialiserede protokoller (f.eks. Modbus, DNP3, PROFIBUS), der prioriterer deterministisk[1] timing over indbyggede sikkerhedsfunktioner. Disse kommunikerer ofte i klartekst.
- **Minimal nedetidstolerance:** Selv planlagte vedligeholdelsesvinduer er sjældne og skal nøje koordineres for at undgå produktionstab eller sikkerhedshændelser.

Hvorfor OT er vigtig i dag: Forståelse af OT er afgørende for ingeniører, cybersikkerhedsspecialister og beslutningstagere. Disse systemer er **rygraden i moderne industrielle operationer**, og en manglende sikring kan føre til fysisk skade, sikkerhedsrisici og driftsforstyrrelser. Med accelerationen af IT/OT-konvergens[2] bliver sikring af OT-miljøer et **strategisk imperativ for at opretholde modstandsdygtighed**, beskytte mennesker og aktiver og sikre forretningskontinuitet.

OT vs. IT: To forskellige verdener

Operational Technology (OT) og Information Technology (IT) repræsenterer to sammenflettede, men fundamentalt forskellige domæner inden for cybersikkerhed. At forstå deres forskelle er afgørende for at designe forsvarsstrategier.

Mål og prioriteter:

- **OT: Styring af den fysiske verden.** OT-miljøer sikrer, at fysiske processer (f.eks. bevægelse af varer, dosering af kemikalier, regulering af tryk) kører kontinuerligt og sikkert. Forsinkelser eller fejl kan stoppe produktion, beskadige maskineri eller bringe personale i fare.

[1] Præcis og fastlagt
[2] Samkørsel; at IT og OT 'flyder' mod hinanden

- **IT: Håndtering og beskyttelse af information.** IT-infrastrukturer fokuserer på data: lagring, behandling og transmission af information. Prioriteter er fortrolighed, integritet og tilgængelighed af tjenester, typisk med plads til planlagt nedetid via backup og redundans.

Tolerance for forstyrrelser og risikotolerance:

- **OT: Nul nedetid.** Enhver uplanlagt nedlukning i OT er kostbar, både økonomisk og sikkerhedsmæssigt. Vedligeholdelse og opdateringer kræver streng planlægning for at undgå at kompromittere driften.
- **IT: Hyppig vedligeholdelse.** IT-systemer drager fordel af automatiserede patching- og opdateringsmekanismer. Nedetid kan ofte håndteres med backupsystemer.

Arkitektur og kommunikationsprotokoller:

- **OT: Proprietære realtidsprotokoller[3].** Mange OT-applikationer bruger protokoller designet uden sikkerhed for øje (f.eks. Modbus, DNP3, PROFIBUS). De prioriterer stabilitet og hastighed i kontrolløkker. OT-hardware er "robust" til at modstå barske miljøer.
- **IT: Åbne standarder og kryptering.** IT-netværk bruger TCP/IP, HTTPS, SSH og VPN'er, der inkorporerer kryptering og autentificering som standard.

Livscyklus og patchstyring:

- **OT: Lange, komplekse livscykler.** OT-enheder forbliver ofte i drift i årtier, og leverandører udsteder muligvis ikke længere patches[4] til ældre systemer. Dette kræver "virtuel patching" eller streng netværkssegmentering. Engrosudskiftning af kontrolsystemer er typisk omkostningskrævende og forstyrrende.
- **IT: Automatiserede patchcyklusser.** IT-miljøer bruger automatiserede opdateringer, hvilket reducerer eksponeringen for sårbarheder.

Sikkerhedsfokus:

Integritet, Tilgængelighed, Fortrolighed (I-A-C): Traditionel IT-sikkerhed centrerer sig om fortrolighed (Confidentiality), integritet (Integrity) og tilgængelighed (Availability) (CIA-triaden). I OT er prioritetsrækkefølgen ofte **Integritet, Tilgængelighed og derefter Fortrolighed (I-A-C)**.

- **Integritet:** Sikring af, at kontrollogik, konfigurationsfiler og sensordata forbliver uændrede, er altafgørende.
- **Tilgængelighed:** OT-systemer skal køre 24/7 for at undgå produktionstab eller sikkerhedshændelser.

IT/OT-konvergens og brobygning: Med Industry 4.0, IoT-sensorer og smart fremstilling udviskes grænsen mellem OT og IT, hvilket udvider angrebsoverfladen. For at harmonisere de to områder bør organisationer:

1. **Fremme tværfagligt samarbejde:** Del viden, prioriteter og incidenthåndteringsplaner.
2. **Implementere netværkssegmentering og tillidszoner:** Isoler kritiske OT-segmenter med firewalls og DMZ'er.
3. **Vedtage ensartede politikker:** Klare regler for adgangskodeadministration, VPN-brug og patchprocedurer.

[3] Kommunikationsprotokoller, der er udviklet og ejet af en enkelt virksomhed eller organisation. De er ikke standardiserede.
[4] Sikkerhedsopdateringer

Kernekomponenter i et OT-system

OT-miljøer bygger på et lagdelt sæt af specialiserede enheder, grænseflader og kommunikationsprotokoller.

Sensorer og aktuatorer:

- Lukker løkken mellem digitale kommandoer og fysiske handlinger.
- **Sikkerhed:** Kalibreringsverifikation, overvågning af signalintegritet og fysisk adgangskontrol.

Programmable Logic Controllers (PLC'er):

- "Arbejdshestene" i OT, der udfører styrelogik i realtid.
- Fortolker input fra sensorer og sender output til aktuatorer med deterministisk timing.
- Sikkerhedspraksis inkluderer **code whitelisting**[5]**, adgangskontrol** (begrænsning af programmeringsporte, stærke legitimationsoplysninger) og **firmwarevalidering** (verifikation af digitale signaturer).

Remote Terminal Units (RTU'er):

- Designet til **fjerne eller barske steder** (oliebrønde, understationer, vandreservoirer).
- Kan anvende trådløse forbindelser og er ofte robuste.
- **Sikring:** Krypteret kommunikation (f.eks. DTLS), fysisk hærdning (lukkede skabe, manipuleringssikre forseglinger) og fejlsikker logik (standard til en sikker tilstand ved tab af forbindelse).

Human-Machine Interfaces (HMI'er):

- **Oversætter rå OT-data til grafiske dashboards**, der gør det muligt for operatører at træffe informerede beslutninger.
- **Sikkerhedsbehov:** Sessionsstyring (automatiske timeouts, skærmlåsning), inputvalidering (beskyttelse mod injektionsangreb) og patchdisciplin (regelmæssige softwareopdateringer).

Supervisory Control and Data Acquisition (SCADA):

- En arkitektur med flere lag: feltudstyr (PLC'er/RTU'er), kommunikationsnetværk, SCADA-servere (masterstation, datahistoriker) og operatørarbejdsstationer.
- **Sikkerhedsforanstaltninger:** Netværksisolering (DMZ), krypterede tunneler (VPN, TLS) og rollebaseret adgang.

Elektrikerens rolle her: Som elektriker er du afgørende for den fysiske integritet af disse systemer:

- **Installation og vedligeholdelse:** Korrekt installation og kabling af PLC'er, SCADA-komponenter og HMI'er er fundamental for deres funktion og sikkerhed.
- **Fysisk sikring:** Du er ansvarlig for at sikre, at programmeringsporte på PLC'er er utilgængelige for uautoriseret adgang. Det kan inkludere installation af låse, forseglinger eller andre fysiske barrierer.
- **Strømforsyning:** Sikring af stabil og beskyttet strømforsyning til disse kritiske komponenter for at undgå uplanlagte nedlukninger, der kan udnyttes af angribere.

[5] At koden er godkendt

- **Overvågning og rapportering:** At bemærke og rapportere enhver fysisk manipulation, usædvanlig adfærd eller skade på kabinetter, der huser disse enheder.

Integration og kommunikationsprotokoller: OT-netværk anvender både ældre og nye protokoller.

- **Modbus, DNP3, PROFIBUS:** Udbredt, men ukrypteret, kræver netværkssegmentering og trafikinspektion.
- **OPC-UA:** Vinder frem på grund af indbygget sikkerhed (autentificering, kryptering).

Nye tendenser: Edge Computing og Digital Twins:

- **Edge gateways** forbehandler data lokalt, før de sendes videre.
- **Digitale tvillinger** afspejler levende OT-processer i virtuelle modeller, hvilket muliggør proaktiv vedligeholdelse, men også nye API-sikkerhedsudfordringer.

Elektrikerens rolle her: Din ekspertise er afgørende for at beskytte disse komponenter:

- **Fysisk sikring af RTU'er:** Installation af RTU'er i låste, manipuleringssikre kabinetter og anvendelse af forseglinger er en central opgave for at forhindre fysisk manipulation.
- **Sensorintegritet:** Sikring af korrekte installationer af sensorer og aktuatorer, herunder kabelføring, for at forhindre signalmanipulation eller uautoriseret adgang til feltkabling. Regelmæssig kontrol af fysisk tilstand.
- **Kommunikationsinfrastruktur:** Korrekt kabling og installation af netværksudstyr til både ældre og nye protokoller er afgørende. Dette inkluderer forståelse af krav til redundans og Quality of Service (QoS) i netværksopsætningen.
- **Håndtering af nye teknologier:** Viden om, hvordan edge-enheder og andre nye komponenter integreres fysisk i OT-miljøet, og hvilke sikkerhedsaspekter (f.eks. strømforsyning, fysisk placering) der skal overholdes.

Purdue-modellen: En referenceramme for OT-sikkerhed

Purdue-modellen er en udbredt ramme, der definerer en lagdelt tilgang til organisering og sikring af OT- og IT-systemer i industrielle kontrolmiljøer. Den strukturerer kommunikation og beskyttelse af industrielle systemer.

Hvad er Purdue-modellen? Modellen opdeler industrielle operationer i fire niveauer, fra fysiske processer op til forretningssystemer, suppleret med et femte niveau for eksterne tjenester:

- **Niveau 0 – Fysisk proces:** Grundlaget, hvor sensorer og aktuatorer direkte interagerer med det fysiske miljø.
- **Niveau 1 – Grundlæggende kontrol:** PLC'er, RTU'er og andre automatiseringscontrollere behandler data fra Niveau 0 og træffer realtidsbeslutninger.
- **Niveau 2 – Overvågning:** HMI'er og SCADA-systemer giver operatører dashboards, alarmer og kontrol til at overvåge og finjustere industrielle processer.
- **Niveau 3 – Drift:** Fokus på styring af produktionsarbejdsgange, proceshistorikere og vedligeholdelsesapplikationer.
- **Niveau 4 – Forretning:** Omfatter virksomhedens IT-systemer som ERP, forsyningskædestyring og kundeforholdsstyring.

- **Niveau 5 – Eksterne/Cloud-tjenester (Valgfri):** Fjernovervågning, cloud-baseret analyse og tredjepartsintegrationer.

Sikkerhedsimplementering i Purdue-modellen: Modellen fremmer en **"forsvar-i-dybden"** sikkerhedsstrategi ved at isolere niveauer og håndhæve strenge kommunikationsregler.

- **Firewalls og VLAN'er** anvendes til at håndhæve segmentering mellem niveauer.
- **DMZ'er (Demilitarized Zones)** isolerer følsomme systemer og buffer ekstern adgang, ofte placeret mellem Niveau 3 og 4.
- **Overvågnings- og indbrudsdetekteringssystemer (IDS)** ved centrale netværksknudepunkter.
- **Rollebaseret adgangskontrol (RBAC)** sikrer, at brugere og enheder kun har de passende adgangsrettigheder.
- **Datadioder** sikrer ensrettet dataflow, f.eks. fra OT til IT, og blokerer fysisk eller logisk returtrafik.

Hvorfor Purdue-modellen er vigtig: Den gør det muligt for organisationer at **klart definere sikkerhedsparametre**, styre dataflow sikkert, beskytte kritisk infrastruktur og tilpasse OT-systemer med IT-styring.

Elektrikerens rolle her:

- **Fysisk implementering af zoner:** Forståelse af Purdue-modellens niveauer er afgørende for at kunne udføre korrekte installationer og kablinger, der respekterer de definerede sikkerhedszoner. Du skal sikre, at der ikke oprettes "ukontrollerede" forbindelser mellem niveauerne.
- **Firewall- og DMZ-installation:** Som elektriker kan du være involveret i den fysiske installation af firewalls og andre netværksenheder, der opretholder segmenteringen mellem niveauerne, f.eks. mellem Niveau 3 (drift) og Niveau 4 (forretning) via en DMZ.
- **Adgangskontrol for udstyr:** At sikre, at fysiske adgangspunkter til udstyr på de forskellige niveauer er beskyttet i overensstemmelse med sikkerhedspolitikken, f.eks. låse på kabinetter.

Cybersikkerhedsudfordringer i OT og modforanstaltninger

Cybersikkerhed i OT adskiller sig fundamentalt fra IT, da den beskytter systemer, hvis fejl kan have virkelige, sikkerhedskritiske konsekvenser. Digitale sikkerhedsforanstaltninger skal stemme overens med tekniske kontroller for at bevare kontinuerlig og sikker drift.

Dybdegående sårbarheder:

1. Ældre udstyr: Ofte med forældede operativsystemer (OS) og firmware, der ikke længere modtager patches, efterladende kendte sårbarheder åbne.
2. Usikrede protokoller: Klarteksttrafik (f.eks. Modbus/TCP, DNP3) gør aflytning og injektion triviel.
3. Flade, konvergerede[6] netværk: Manglende segmentering tillader, at et brud i et kontornetværk kan sprede sig direkte til kontrolenheder.
4. Svag autentificering: Mange enheder leveres med standardlegitimationsoplysninger eller ingen Multi-Factor Authentication (MFA), hvilket øger risikoen for tyveri af legitimationsoplysninger.

Lagdelte forsvarsstrategier (Defense-in-Depth):

1. **Netværkszonering og segmentering:** Implementer Purdue-modellen med firewalls eller datadioder mellem zoner for at begrænse lateral[7] bevægelse. Anvend mikrosegmentering for at isolere højrisikosenheder.
2. **Forsvar-i-dybden-kontroller:** Brug industrielle firewalls med Dybpakkeinspektion (DPI), applikations-whitelisting og **fysiske sikkerhedslag** som hærdede paneler og låste kabinetter.
3. **Kontinuerlig overvågning og anomali-detektion:** Spejl trafik til Intrusion Detection Systems (IDS) indstillet til ICS-protokoller og opbyg grundlinjer for normal adfærd.
4. **Patch- og ændringsstyring:** Implementer "virtuel patching" for enheder, der ikke kan opdateres direkte, og koordiner firmwareopgraderinger med produktionsnedlukninger.
5. **Stærk adgangskontrol:** Definer granulære roller med skræddersyede tilladelser (Rollebaseret adgangskontrol – RBAC) og håndhæv Multi-Factor Authentication (MFA) på kritiske konsoller.
6. **Menneskecentrerede forsvar:** Målrettet træning for OT-personale i at spotte phishing og usikker USB-praksis.

Styring, standarder og risikostyring:

- Vedtag OT-specifikke rammer som ISA/IEC 62443 og NIST SP 800-82.
- Udfør risikovurderinger og aktivfortegnelser for at prioritere afhjælpning.
- Harmoniser politikker og procedurer på tværs af IT og OT.

Elektrikerens rolle i modforanstaltninger: Som elektriker er dine handlinger afgørende for at styrke forsvaret:

- **Fysiske sikkerhedslag:** Implementering af hærdede paneler, låsning af kabinetter og installation af manipuleringssensorer er direkte din opgave. Disse fysiske foranstaltninger supplerer de digitale forsvarslinjer.

[6] Samløbende
[7] På tværs af lag-segmenteringen

- **Håndtering af ældre udstyr:** Rapportering af ældre, upatchede systemer og deltagelse i implementering af kompenserende kontroller som fysisk isolation og sikker kabling omkring disse enheder.
- **Korrekt kabling og installation:** Sikring af, at alle netværksforbindelser og enheder er korrekt installeret og beskyttet for at understøtte segmentering og forhindre uautoriseret adgang.
- **Bevidsthed og rapportering:** At være opmærksom på usikker adfærd (f.eks. ukendte USB-drev, åbne kabinetter) og rapportere dette, da det kan være indikationer på et cyberangreb.

Reelle OT-cyberangreb og konsekvenser

Del 1 (Angreb)

Gennemgang af faktiske hændelser giver uvurderlig indsigt i, hvordan angribere udnytter OT-sårbarheder, og hvor ødelæggende konsekvenserne kan være.

Landemærke-hændelser:

1. **Stuxnet (2010):**

- **Mål:** Irans Natanz uranberigelsesanlæg.
- **Angrebsvektor:** Inficerede USB-drev introducerede ormen i et luftspærret netværk.
- **Mekanisme:** Ændrede Siemens Step7 PLC-kode til at spinde centrifuger ved skadelige hastigheder, samtidig med at normale aflæsninger blev forfalsket til operatørerne.
- **Betydning:** Første bevis på, at et cybervåben kunne krydse luftspær og forårsage fysisk ødelæggelse gennem PLC-manipulation.

2. **BlackEnergy (2015):**

- **Mål:** Ukraines eldistributionssystem.
- **Angrebsvektor:** Phishing-e-mails leverede malware, der høstede legitimationsoplysninger.
- **Mekanisme:** Angribere brugte stjålne legitimationsoplysninger til at logge ind på SCADA-arbejdsstationer og deaktiverede manuelt afbrydere, backup-systemer og firmware for at forsinke genopretningen.
- **Betydning:** Viste, at relativt usofistikeret social engineering, kombineret med OT-adgang, kan lamme kritisk infrastruktur.

3. **Industroyer / CrashOverride (2016):**

- **Mål:** Kyivs eltransmissionsnetværk.
- **Angrebsvektor:** Brugerdefineret malware, der udnyttede industrielle protokoller (IEC 101/104).
- **Mekanisme:** Malwaren kommunikerede direkte med afbrydere og koblingsudstyr ved hjælp af indbyggede kommandoer og slettede derefter enheds-firmware.
- **Betydning:** Viste en angribers dybe forståelse af IEC-protokoller og transformerstationsarkitektur.

4. **TRITON / HatMan (2017):**

- **Mål:** Petrokemisk anlæg i Mellemøsten.

- **Mekanisme:** Malware manipulerede SIS-logik (Safety Instrumented System) for at deaktivere sikkerhedsfunktioner, hvilket potentielt kunne tillade anlægget at køre usikkert.
- **Betydning:** Første kendte malware designet specifikt til at angribe sikkerhedssystemer, hvilket signalerer et nyt niveau af intention om at forårsage fysisk skade.

Almindelige taktikker, teknikker og procedurer (TTP'er):

- **Initial adgang via IT-vektorer:** Phishing, ondsindede e-mail-vedhæftninger og kompromitterede VPN-legitimationsoplysninger er almindelige indgangspunkter.
- **Lateral bevægelse og privilegeeskalation:** Angribere bruger legitime administrative værktøjer eller protokol-aware malware til at kortlægge netværket og opnå kontrol over PLC/HMI-servere.
- **Protokolmanipulation:** Angribere skaber native Modbus, DNP3 eller IEC-beskeder for at udstede uautoriserede kommandoer direkte til feltudstyr.
- **Forsyningskæde- og USB-spredning:** Malware som Stuxnet udnytter flytbare medier til at infiltrere luftspærrede steder.

Del 2 (Impact og Lektioner)

Impact-kategorier:

- **Fysisk ødelæggelse:** Stuxnets angreb viser, hvordan kode kan føre til kinetisk skade.
- **Servicenedbrud:** BlackEnergy og Industroyer viser den samfundsmæssige og økonomiske skade ved udvidede strømafbrydelser.
- **Sikkerhedskompromittering:** TRITONs mål om at deaktivere nødlukninger understreger potentialet for tab af menneskeliv og miljøkatastrofer.
- **Langvarige genopretningsomkostninger:** Reparation eller udskiftning af specialiseret OT-hardware kan tage måneder eller år og koste millioner.

Konsekvenser forårsaget af OT-angreb:

- **Umiddelbare fysiske og operationelle påvirkninger:** Katastrofale udstyrsfejl, omgåelse af automatiske sikkerhedsspærringer, tab af kontrol og synlighed samt nød-nedlukninger.
- **Sikkerhedsmæssige, miljømæssige og omdømmemæssige følger:** Risici for menneskeliv, miljøskader fra udslip og erosion af interessenternes tillid.
- **Finansielle, juridiske og lovgivningsmæssige konsekvenser:** Direkte omkostninger til reparationer, indirekte omkostninger ved produktionstab, lovgivningsmæssige sanktioner og retssager/ansvar.

Lektioner lært, nye trusler og fremtidsudsigter:

- **Zero Trust** er afgørende; segmentering redder liv.
- **Overvåg OT-specifikke indikatorer**; hærd ældre systemer.
- **Tværfagligt samarbejde** mellem OT-ingeniører og IT-sikkerhedseksperter er nødvendigt.
- **Nye trusler** inkluderer AI-drevne angreb, OT-målrettet ransomware og forsyningskædeindtrængen.

Vigtigheden af elektrikerens bidrag:

- **Forebyggelse af fysisk skade:** Din præcision i installation og vedligeholdelse af udstyr kan forhindre fysisk skade og driftsforstyrrelser. Fejlsikker installation kan modvirke effekten af ondsindede kommandoer.
- **Sikkerhedsbevidsthed:** Forståelse af de alvorlige konsekvenser af et cyberangreb understreger vigtigheden af din rolle i at opretholde fysisk sikkerhed og følge procedurer. For eksempel at være forsigtig med USB-enheder for at undgå at introducere malware som Stuxnet.
- **Rapportering af anomalier:** Din opmærksomhed på uregelmæssigheder i udstyr eller netværk (f.eks. usædvanlig adfærd, forkert kabling) kan være afgørende for tidlig detektion af et angreb.

Incidenthåndtering og Robusthed i OT

Cyberhændelser i OT-miljøer rækker langt ud over tabte data – de kan bringe liv i fare, lamme økonomier og erodere offentlig tillid.

Incidenthåndtering og krisehåndtering: En hurtig og velorkestreret reaktion kan betyde forskellen mellem en inddæmmet forstyrrelse og en langvarig krise.

1. **Hurtig inddæmning:** Forhåndsgodkendte scenariebaserede planer skal give operatører mulighed for at isolere kompromitterede celler, aktivere netværksluftspær eller datadioder og skifte kritiske løkker til manuel eller sikker tilstand.
2. **Integreret IT/OT-retsmedicinsk analyse:** Fælles teams indsamler logs fra både IT-firewalls og OT-controllere, image af PLC-hukommelse og bevarer beviser i henhold til chain-of-custody-protokoller.
3. **Samarbejde med eksterne eksperter:** Tidlig inddragelse af industri-kontrolsystem (ICS)-specialister, nationale eksperter og juridiske rådgivere fremskynder trusselsneutralisering og overholdelse af rapporteringsregler.

Post-incident genopretning, læring og kontinuerlig forbedring: Genopretning handler ikke kun om at komme "online" igen – det er en mulighed for at styrke forsvaret.

- **Årsagsanalyse:** Detaljerede undersøgelser identificerer ikke kun den tekniske del af angrebet, men også proceshuller.
- **Netværks- og systemhærdning:** Opbyg segmenter i henhold til Purdue-modellen, implementer næstegenerations industrielle firewalls med DPI for OT-protokoller, og håndhæv strenge ændringsstyrings-arbejdsgange for PLC-logik.
- **Opdaterede playbooks og runbooks:** Inkorporer de nye erfaringer i håndteringsguider.

Opbygning af en kultur for OT-robusthed: Ægte sikkerhed understøttes af mennesker og processer lige så meget som af teknologi.

- **Tværfaglig styring:** Etabler et OT-sikkerhedsråd med kontrolingeniører, IT-sikkerhedsarkitekter og forretningsledere.
- **Kontinuerlig træning og certificering:** Kræv OT-specifikke cybersikkerhedscertificeringer (f.eks. GIAC GICSP) og årlig træning.
- **Motiverende rapportering:** Implementer "no-blame"-politikker, der opmuntrer operatører til at rapportere nær-ved-ulykker og mistænkelig aktivitet.

Din rolle som elektriker:

- Hurtig inddæmning: I tilfælde af en hændelse kan din evne til hurtigt og sikkert at udføre fysisk isolering af kompromitterede segmenter, afbryde strømmen til kritiske enheder eller skifte til manuel kontrol være afgørende for at inddæmme angrebet.
- Genopretning: Efter en hændelse er din ekspertise nødvendig for at genopbygge eller reparere den fysiske infrastruktur, herunder kabling, PLC'er og andet udstyr, for at sikre, at systemerne fungerer korrekt og sikkert igen.
- Rapportering: Deltag i "no-blame"-politikker og rapporter straks mistænkelig fysisk aktivitet eller nær-ved-ulykker. Din observation kan give værdifuld information til sikkerhedsteamet.
- Deltagelse i øvelser: Deltag i regelmæssige øvelser og simuleringer for at teste responstider og koordination mellem IT og OT-personale.

Netværkssegmentering: Værktøjer og bedste praksis for elektrikere

Netværkssegmentering er en grundlæggende strategi i OT-cybersikkerhed, der involverer logisk eller fysisk opdeling af et netværk i mindre, mere håndterbare enheder. Dette forbedrer sikkerheden, reducerer kompleksiteten og forbedrer evnen til at overvåge og kontrollere dataflows.

Hvorfor segmentering er vigtig i OT: OT-miljøer er sårbare over for cyberangreb, især når de er forbundet til bredere IT-systemer, på grund af lang levetid for enheder, proprietære protokoller og historisk mangel på cybersikkerhedsintegration. Segmentering isolerer følsomme komponenter og sikrer, at sikkerhedsbrud i ét område ikke påvirker hele systemet.

Fordele ved netværkssegmentering:

- **Inddæmning af angreb:** Forhindrer malware, ransomware[8] eller indtrængere i at bevæge sig lateralt i netværket.
- **Forbedret synlighed og overvågning:** Hvert segment kan overvåges uafhængigt.
- **Granulær[9] politikudførelse:** Administratorer kan anvende unikke regler til forskellige typer trafik og systemer.

Værktøjer og teknologier til segmentering:

- **VLAN'er (Virtual Local Area Networks):** Tillader oprettelse af flere logiske netværk på én fysisk infrastruktur. Dette isolerer trafik efter funktion eller sikkerhedsniveau.
- **Firewalls:** Fungerer som kritiske kontrolpunkter mellem netværkssegmenter og håndhæver politikker, der tillader eller blokerer trafik.
    - Pakke filtreringsfirewall: Undersøger individuelle datapakker og blokerer dem baseret på regler som IP-adresser eller porte. Opererer på netværkslaget, er simple og hurtige.
    - Stateful Inspection Firewall: Mere avanceret, sporer aktive forbindelser og sikrer, at kun legitim trafik tillades. Opretholder en tilstandstabel over aktive forbindelser.
    - Proxy Firewall: Fungerer som mellemmand, filtrerer trafik før det når netværket. Kan inspicere hele indholdet af trafikken, men kan forårsage forsinkelser i dataflow'et.

[8] …hvor ens data bliver taget som 'gidsel'
[9] En fin, detaljeret tilgang til adgangskontrol og sikkerhedspolitikker

    - Next-Generation Firewall (NGFW): Den mest avancerede type, kombinerer traditionelle firewallfunktioner med intrusion detection og prevention (IDS/IPS), pakkeinspektion og applikationskontrol. Opererer på flere lag og kan inspicere krypteret trafik.
- **DMZ'er (Demilitarized Zones):** Mellem-netværkszoner, der giver kontrolleret adgang mellem interne OT-systemer og eksterne netværk. Anvendes ofte med dual-firewall-arkitekturer.
- **Datadioder:** Envejs netværksenheder, der håndhæver ensrettet dataflow og fysisk eller logisk blokerer returtrafik. Giver en ekstrem form for segmentering, f.eks. fra OT til IT, og er ideelle til højsikkerhedsmiljøer.

Dine opgaver vedrørende segmentering:

- **Korrekt kabling:** Installation og vedligeholdelse af kabling for VLAN'er og fysiske segmenter er afgørende. Forkert kabling kan kompromittere hele segmenteringsstrategien.
- **Installation af netværksudstyr:** Fysisk installation af firewalls, switche og data diodes skal udføres præcist og i overensstemmelse med de definerede arkitekturer. Dette inkluderer sikring af udstyret i kabinetter.
- **Fysisk adskillelse:** Du har ansvar for at sikre den fysiske adskillelse af kritiske OT-systemer, f.eks. at kontrollere adgang til kabler og udstyr, der forbinder forskellige netværkssegmenter.
- **Dokumentation:** Detaljeret dokumentation af netværkstopologier og kabling er essentiel for at lette fejlfinding og sikre, at segmenteringspolitikker håndhæves korrekt.

Adgangskontrol og Overvågning

Rollebaseret adgangskontrol (RBAC): RBAC tildeler brugere tilladelser baseret på deres rolle, hvilket sikrer, at de kun kan få adgang til de ressourcer, der er nødvendige for deres funktion. Dette involverer:

1. **Definition af roller og ansvar:** Identificer jobfunktioner og kortlæg dem til minimumssættet af nødvendige tilladelser.
2. **Etablering af en tilladelsesmatrix:** Udvikl en matrix, der lister ressourcer (PLC'er, SCADA-konsoller) over for roller og tildeler læse-, skrive-, udførelses- og konfigurationstilladelser.
3. **Implementering af mindste privilegium:** Tildel kun de tilladelser, der er nødvendige for en rolles opgaver.
4. **Adskillelse af opgaver:** Undgå interessekonflikter, f.eks. kan samme bruger ikke både konfigurere PLC-logik og godkende dens implementering.
5. **Integration med identitetsstyring:** Brug centraliserede IAM-systemer for brugerprovisionering, SSO, MFA og LDAP/Active Directory-integration.
6. **Audit og compliance:** Opretholde detaljerede logfiler over rolletildelinger og adgangsanmodninger.

Netværksovervågning og -styring: Effektiv overvågning er afgørende for at opretholde synlighed i segmenterede OT-miljøer.

- Intrusion Detection/Prevention Systems (IDS/IPS):

- **IDS (Intrusion Detection System):** Monitorerer netværkstrafik og systemaktiviteter for at identificere potentielle trusler. IDS opererer passivt, alarmerer om mistænkelig aktivitet, men blokerer ikke direkte.
- **Netværksbaseret IDS (NIDS):** Overvåger trafik til og fra alle enheder i netværket.
- **Host-baseret IDS (HIDS):** Installeres på individuelle enheder og overvåger systemlogs og filintegritet.
- **Detektionsmetoder**: Signatur-baseret (kendte trusler), anomali-baseret (afvigelser fra normal adfærd) og adfærdsbaseret (identificerer usædvanlig adfærd, kan bruge AI).
- **IPS (Intrusion Prevention System):** Designet til aktivt at forhindre trusler. Opererer "in-line" med netværkstrafik og kan blokere pakker, terminere forbindelser, isolere kompromitterede systemer og forhindre skadelige aktiviteter. Moderne IDS har ofte blokeringsfunktioner og er mere en del af IPS.

- **Security Information and Event Management (SIEM):** Samler logs fra firewalls, PLC'er og SCADA-systemer, korrelerer begivenheder og genererer prioriterede alarmer.
- **Deep Packet Inspection (DPI):** Afkoder industrielle protokoller (Modbus, DNP3, OPC-UA) for at identificere fejlformede pakker eller uautoriserede kommandoer.
- **Anomali-detektion og maskinlæring:** Bruger statistiske modeller og AI til at detektere subtile ændringer i enhedens adfærd.

SSL-inspektion og web-/applikationskontrol:

- **SSL-inspektion:** Afgørende for at forbedre netværkssikkerheden ved at tillade sikkerhedsværktøjer at inspicere krypteret trafik. Processen involverer at opfange trafik, dekryptere data, analysere for trusler og genkryptere trafikken.
- **Web- og applikationskontrol:** Kombinerer elementer fra firewalls, IDS og IPS for at styre adgangen til specifikke websteder, applikationer og tjenester baseret på sikkerhedspolitikker.

Hvad betyder det for dig som elektriker?

- **RBAC for fysisk adgang:** Du skal følge de fastsatte RBAC-politikker for fysisk adgang til serverrum, kontrolrum og kabinetter, der indeholder OT-udstyr. Dette betyder, at du kun bør have adgang til de områder og enheder, der er relevante for din rolle.
- **Bevidsthed om overvågning:** Vær opmærksom på, at netværkstrafik og systemaktiviteter overvåges af IDS/IPS og SIEM-systemer. Enhver uautoriseret fysisk handling, såsom at tilslutte ukendte enheder eller ændre kabling uden godkendelse, kan udløse alarmer.
- **Rapportering af usædvanlig adfærd:** Hvis du observerer usædvanlig netværksadfærd (f.eks. ukendte enheder på netværket, uforklarlig aktivitet på udstyr) eller fysiske manipulationer, skal du rapportere det omgående til det relevante sikkerhedsteam.
- **Sikkerhedsforanstaltninger under arbejde:** Forstå, at visse netværkssikkerhedsfunktioner som SSL-inspektion og web-/applikationskontrol er på plads for at beskytte systemerne, selv når du udfører dit arbejde.

Industrielle Protokoller og IT/OT-Samarbejde - Elektrikerens Perspektiv

Overblik over almindelige industrielle protokoller:

- **Modbus:** Ældste og mest udbredte protokol, enkel og effektiv, men mangler kryptering og autentificering.
- **DNP3 (Distributed Network Protocol):** Bruges i el- og vandforsyning. Nyere versioner understøtter autentificering, men kryptering implementeres ofte ikke i ældre installationer.
- **Profinet:** Højhastigheds industriel Ethernet-protokol til automatisering, sårbar uden yderligere sikkerhedslag.
- **OPC-UA (Open Platform Communications Unified Architecture):** Moderne og sikker protokol med indbygget kryptering, autentificering og robust interoperabilitet. Bedste praksis for nye OT-implementeringer.

Typiske protokolsårbarheder: Industrielle protokoller mangler ofte indbyggede sikkerhedsfunktioner.

- **Manglende kryptering:** Data i klartekst (Modbus, klassisk DNP3) tillader aflytning og manipulation.
- **Svag eller ingen autentificering:** Protokoller bygger på standard- eller statiske legitimationsoplysninger, hvilket tillader spoofing af legitime noder og uautoriserede kommandoer.
- **Usikre standardkonfigurationer:** Mange OT-enheder leveres med åbne porte, standardlegitimationsoplysninger og debug-tjenester aktiveret.
- **Sårbarhed over for Denial-of-Service (DoS):** Uden begrænsning af datahastighed eller robust fejlhåndtering kan enheder overvældes, hvilket fører til procesforstyrrelser.
- **Manglende segmenteringsbevidsthed:** Protokoller designet til flade netværk antager direkte tilgængelighed og kan uforvarende eksponere administrationsgrænseflader.
- **Upatchet firmware og ældre software:** Efterlader kendte sårbarheder udbredte.

Modforanstaltninger for protokolsikkerhed:

- **Krypterede protokolimplementeringer:** Implementer sikre versioner (f.eks. TLS-aktiveret OPC-UA) eller brug IPsec-tunneler.
- **Robust netværkssegmentering:** Isoler protokolltrafik i dedikerede VLAN'er eller fysiske segmenter.
- **Dybpakkeinspektion og DPI-IDS-integration:** Brug DPI-firewalls til at afkode industrielle protokoller og detektere ondsindet trafik.
- **Endpoint-hærdning og sikker konfiguration:** Deaktiver ubrugte tjenester og porte, håndhæv stærke legitimationsoplysninger og brug sikker boot.
- **Firmware- og patchstyring:** Oprethold en opdateret fortegnelse over firmware og koordiner regelmæssige opdateringer. Brug virtuel patching for ældre enheder.
- **Adgangskontrol og autentificering:** Håndhæv MFA for al fjernadgang og privilegeret adgang til OT-systemer.

Roller for IT- og OT-personale i segmentering og samarbejde: Effektive segmenterede netværk kræver **koordination mellem IT- og OT-personale**.

- **IT-teams** bidrager med ekspertise inden for cybersikkerhedsstandarder, netværksarkitektur og databeskyttelse.

- **OT-teams** fokuserer på procespålidelighed, udstyrsydelse og fysisk sikkerhed. **Samarbejde** er afgørende for at harmonisere disse verdener, hvilket kræver fælles planlægning, delte KPI'er, politikker udarbejdet i fællesskab og **styringsstrukturer som RACI-modellen**.

Din rolle i protokolsikkerhed og samarbejde:

- **Korrekt tilslutning og kabling:** Du skal sikre, at enheder, der bruger usikre protokoller som Modbus, er korrekt isoleret via fysiske netværkssegmenter, og at kabling understøtter brugen af mere sikre protokoller som OPC-UA.
- **Bevidsthed om sårbarheder:** Forstå, at protokoller som Modbus overfører data i klartekst, hvilket gør fysisk beskyttelse af netværkskabler og enheder endnu vigtigere.
- **Endpoint-hærdning:** Bistå med at sikre, at OT-enheder ikke har unødvendige porte åbne eller kører med standardadgangskoder, hvilket du kan hjælpe med at identificere og rapportere under installation eller vedligeholdelse.
- **Aktivt samarbejde med IT:** Du er en vigtig brik i IT/OT-samarbejdet. Del din viden om de fysiske systemer og protokoller med IT-teamet, og lyt til deres input om cybersikkerhedsbehov. Deltag i fælles træning og øvelser.

Ordliste med forkortelser

Her er en opslagsliste over de forkortelser, der bruges i denne brochure, for at gøre det lettere at forstå terminologien inden for cybersikkerhed i OT-miljøer.

ACL (Access Control List): En liste over regler, der bruges af en router eller firewall til at styre netværkstrafik og begrænse adgang til bestemte ressourcer.

AI (Artificial Intelligence): Kunstig intelligens, der bruges i cybersikkerhed til f.eks. adfærdsanalyse og detektion af anomalier.

API (Application Programming Interface): Et sæt definerede metoder til at kommunikere mellem softwarekomponenter. I OT kan usikre API'er udgøre en angrebsvektor.

CIA-triaden (Confidentiality, Integrity, Availability): En grundlæggende model for informationssikkerhed. I OT ændres prioriteringen ofte til I-A-C (Integritet, Tilgængelighed, Fortrolighed).

CRM (Customer Relationship Management): Systemer til styring af kunderelationer.

CVE (Common Vulnerabilities and Exposures): En liste over offentligt kendte cybersikkerhedssårbarheder.

DCS Et Distribueret Kontrolsystem er et automatiseringssystem, der bruges til at styre og overvåge kontinuerlige eller batch-orienterede processer i store anlæg

DLP (Data Loss Prevention): Værktøjer og processer til at forhindre tab af følsomme data.

DMZ (Demilitarized Zone): En mellemliggende netværkszone, der giver kontrolleret adgang mellem interne systemer og eksterne netværk. Bruges til at isolere følsomme OT-systemer fra virksomhedens IT-netværk.

DNP3 (Distributed Network Protocol 3): En kommunikationsprotokol, der bruges i forsyningssektoren (f.eks. el og vand).

DoS (Denial-of-Service): Et cyberangreb, der sigter mod at gøre en tjeneste utilgængelig for dens tilsigtede brugere.

DPI (Deep Packet Inspection): En avanceret form for netværkspakkeinspektion, der undersøger datadelen af en pakke samt headeren.

ERP (Enterprise Resource Planning): Virksomhedssoftware, der integrerer styring af de vigtigste forretningsprocesser.

HIDS (Host-based Intrusion Detection System): Et IDS, der er installeret på individuelle enheder for at overvåge systemlogs og filintegritet.

HMI (Human-Machine Interface): En grafisk grænseflade, der giver operatører mulighed for at overvåge og styre industrielle processer.

HTTPS (Hypertext Transfer Protocol Secure): En sikker version af HTTP, der bruger SSL/TLS-kryptering.

IAM (Identity and Access Management): Styring af digitale identiteter og adgangsrettigheder.

ICS (Industrial Control Systems): Generel betegnelse for systemer, der styrer industrielle processer.

IEC (International Electrotechnical Commission)

IEC 61131-3 En standard for programmeringssprog til PLC'er.

IEC 62443 (ISA/IEC 62443): En serie af standarder for sikkerhed i industrielle automatiserings- og kontrolsystemer.

IDS (Intrusion Detection System): Et system, der overvåger netværkstrafik og systemaktiviteter for at detektere potentielle trusler.

IoT (Internet of Things): Forbindelse af industrielle enheder og sensorer til internettet.

IPS (Intrusion Prevention System): Et system, der aktivt forhindrer trusler i at forårsage skade på netværket.

ISO 27001 En international standard for informationssikkerhedsstyringssystemer.

IT (Information Technology): Informationsteknologi, systemer til databehandling og kommunikation.

KPI (Key Performance Indicator): Nøgletalsindikatorer, der bruges til at måle ydeevne og effektivitet.

MFA (Multi-Factor Authentication): Multi-faktor autentificering, hvor brugeren skal bevise sin identitet på mere end én måde.

Modbus: En seriel kommunikationsprotokol, der bruges til at forbinde industrielle elektroniske enheder.

NGFW (Next-Generation Firewall): Næstegenerations firewall, der kombinerer traditionelle firewallfunktioner med avancerede sikkerhedsfunktioner.

OPC-UA (Open Platform Communications Unified Architecture): En moderne, sikker og interoperabel standard for dataudveksling i industrielle automatiseringsmiljøer.

OS (Operating System): Operativsystem.

OT (Operational Technology): Operationel teknologi, hardware- og softwaresystemer, der styrer fysiske processer.

PLC (Programmable Logic Controller): En programmerbar logikkontrol, der bruges til at automatisere industrielle processer.

PROFIBUS (Process Field Bus): En standard for feltbuskommunikation i automatisering.

QoS (Quality of Service): Ydeevne-prioritering

RACI-modellen (Responsible, Accountable, Consulted, Informed): En model til at tildele og definere roller og ansvar.

RBAC (Role-Based Access Control): Rollebaseret adgangskontrol, der tildeler brugere tilladelser baseret på deres rolle.

RCA (Root Cause Analysis): Rodårsagsanalyse, en metode til at identificere de grundlæggende årsager til en hændelse.

RTU (Remote Terminal Unit): En fjernterminalenhed, der bruges til at forbinde med fysiske enheder på fjerne steder.

SCADA (Supervisory Control and Data Acquisition): Et system, der overvåger og styrer industrielle processer på et overordnet niveau.

SIEM (Security Information and Event Management): Et system til sikkerhedsinformation og hændelsesstyring, der samler og korrelerer sikkerhedslogs.

SIS (Safety Instrumented System): Sikkerhedsinstrumenteret system, designet til at forhindre farlige SITUATIONER eller mindske konsekvenserne.

SOC (Security Operations Center): Et sikkerhedsoperationscenter, der overvåger, detekterer og reagerer på sikkerhedshændelser.

SSH (Secure Shell): En netværksprotokol, der giver sikker dataoverførsel.

SSL (Secure Sockets Layer): En tidligere version af TLS, der bruges til kryptering af netværkskommunikation.

SSO (Single Sign-On): En autentificeringsordning, der giver en bruger adgang til flere systemer med ét sæt legitimationsoplysninger.

TCP/IP (Transmission Control Protocol/Internet Protocol): En suite af kommunikationsprotokoller, der bruges i internettet.

TLS (Transport Layer Security): En krypteringsprotokol, der bruges til at sikre kommunikation over et computernetværk (afløser for SSL).

USB (Universal Serial Bus): En standard for kablet forbindelse mellem enheder.

VLAN (Virtual Local Area Network): Et virtuelt lokalt netværk, der logisk opdeler et fysisk netværk.

VPN (Virtual Private Network): Et virtuelt privat netværk, der giver en sikker forbindelse over et usikkert netværk.