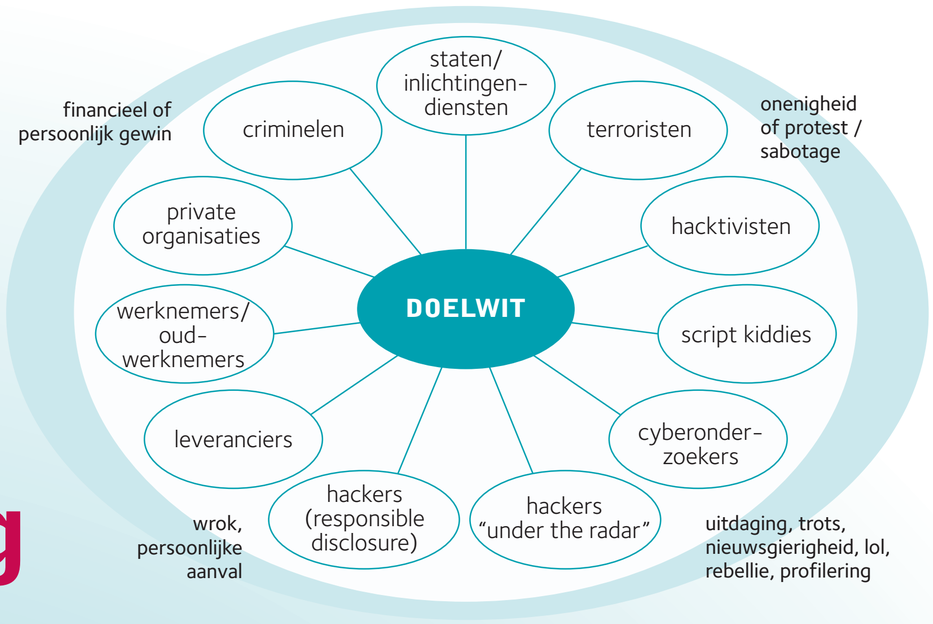
BELANG VAN DE BESTUURDER

- SAFETY: Voorkomen levensbedreigende situaties
- CONTINUITEIT: Geen verstoringen productieproces
- Voldoen aan wetgeving
- Geen ongewenste modificaties
- Geen herstel- of terugroepacties
- Geen schadeclaims
- Voorkomen reputatieschade
- Aandacht voor ketenafhankelijkheid (Supply Chain)

MAATSCHAPPELIJKE WAARDEN

- Geen risico's voor mensen
- Veilige productie en productieprocessen
- Geen ongewenste modificaties in producten: voorkomen gezondheidsrisico's
- Voorkomen grootschalige economische schade
- Voorkomen maatschappelijk ontwrichting als gevolg van uitval vitale sectoren

DREIGINGEN



bron: Nationaal Cyber Security Centrum

Cybersecurity voor Industriële Automatisering

waar de fysieke en digitale wereld samenkomen

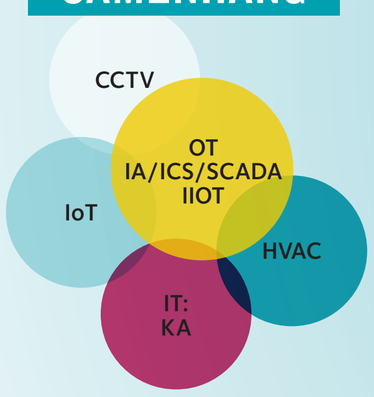
VISIE OP BEVEILIGING VAN INDUSTRIËLE SYSTEMEN

- Risico gebaseerde aanpak
- Focus op Assets: beveiliging van objecten
- Focus op informatie: bij integratie van OT met andere omgevingen
- Zorg voor een integrale aanpak van fysieke beveiliging en logische toegangsbeveiliging
- Scherm industriële systemen af:
  - Zonering en Segmentatie
  - Unidirectional Security Gateways
  - Defence in Depth
- Richt life-cycle management in: vervang zo mogelijk oude en kwetsbare systemen/applicaties
- Pas best practices uit ICT beveiliging toe waar dit mogelijk is:
  - Ken de beperkingen van OT-systemen
  - Richt beheerprocessen, verantwoordelijkheden en governance in
- Voer 'threat intelligence' in
- Zorg voor regulering van de verkeersstromen tussen de domeinen IT, OT en IIOT: werk een datamanagement strategie uit

CYBERSECURITY FOCUS

- In procesautomatisering van oudsher veel nadruk op fysieke (toegangs)beveiliging. (Toegangscontrole is ook digitaal)
- Koppeling OT - IT (kantooromgeving) geeft verhoogde kans op cybersecurity risico's
- Groeiend aantal verbindingen / connecties doet complexiteit toenemen
- Risico procesautomatisering is risico IT plus risico OT (optelsom risico's)
- Menselijke factor is ook in OT omgevingen het grootste risico
- Verschuiving Safety naar Security (kan ook safety mee gemoeid zijn)

SAMENHANG



- **OT** = Operational Technology
- **IA** = Industriële Automatisering
- **ICS** = Industrial Control Systems
- **SCADA** = Supervisory Control and Data Acquisition
- **IIoT** = Industrial Internet of Things
- **HVAC** = Heating, Ventilation and AirConditioning
- **IoT** = Internet of Things
- **CCTV** = Closed Circuit Television (bewakingscamera's)
- **IT** = Informatie Technologie
- **KA** = Kantoorautomatisering

Actieplan

1. Bepaal risico's op Assets en Informatie (prioritering, Quick Wins)
2. Zorg voor draagvlak bij het management (sponsorship)
3. Zorg voor Cybersecurity Awareness bij alle medewerkers
4. Stel een toetskader op met cybersecurity eisen waaraan de OT omgeving moet voldoen
5. Check de OT omgeving op het toetskader en verwerk tekortkomingen in een implementatieplan
6. Denk vanuit een architectuur gedachte aan de mens, processen en technologie
7. Scherm OT omgevingen zo goed mogelijk af (Zonering en Segmentatie, Defence in Depth)
8. Voer Patchmanagement waar mogelijk uit
9. Vervang zonodig 'oude' systemen/applicaties waarmee een hoog risico gelopen wordt
10. Maak offline backups en richt restore in
11. Implementeer actieve monitoring
12. Zorg voor een goed ingeregeld storingsmeldings- en respons proces
13. Richt crisismanagement in
14. Leg relatie met business continuity management
15. Oefen het storingsmeldings- en respons proces (en crisismanagement)

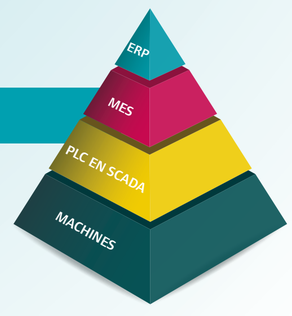
NORMEN, STANDAARDEN EN HANDREIKINGEN

- **NIST SP 800-82** - Guide to Industrial Control Systems (ICS) Security
- **ISO27019** - Information Security for the Energy Utility Industry
- **ISA99** - Industrial Automation and Control Systems Security
- **IEC 62351** - Security Standards for the Power System Information Infrastructure
- **IEC 62443** - Cybersecurity for Industrial Automation and Control Systems (IACS)
- **NCSC** - Checklist beveiliging van ICS / SCADA systemen
- **NCSC** - Uw ICS/SCADA- en gebouwbeheersystemen online
- **ENISA** - Communication network dependencies for ICS/SCADA Systems

VERSCHILLEN IT EN OT OMGEVINGEN

IT		OT
1,5 tot 4 jaar	levensduur	10 tot 30 jaar
informatieverwerking	focus op	fysieke industriële systemen
kantoorwerktijden	in bedrijf	real time, 7x24 uur
generiek en vaak	hackaanvallen	specifiek/doelgericht
dataverlies	gevolgen hackaanval	fysieke schade / kans op slacht-offers / economische schade
persoonlijk	gebruikersaccount	geen of gemeenschappelijk
wordt sneller ontdekt	malware	blijft lang(er) onontdekt
vaak	updates en patches	bijna geen updates of patches
afzonderlijke OTAP	ontwikkel en testomgeving (OTAP)	zelden afzonderlijke OTAP
hoge mate	standaardisatie	veel maatwerk
veel	leveranciers	weinig
veel	beschikbare kennis	beperkt
veel	internetconnectiviteit	neemt toe
datacenter / cloud	dataverwerking	op locatie

TOEKOMST



Ontwikkelingen die impact hebben op cybersecurity:

- Toename genetwerkte omgevingen:
  - 'always connected': anywhere, anytime, anything
  - Industry 4.0: OT, IIOT en Cloud Computing
  - Nieuwe toepassingen
- **IoT**: contactloze sloten, (bewakings)camera's, temperatuuropnemers etc. gekoppeld aan de kantooromgeving en/of internet
- **IIoT**: sensoren en connecties van de fysieke productieomgevingen (OT) naar de informatieverwerkende (IT) omgevingen
- Integratie van bediening en besturingsketens (van ERP t/m machine niveau)
- Toename ketenleveranciers en security risico's in de keten
- **Commodity**: nieuwe technologieën worden steeds meer gemeengoed, bijv. in de medische wereld
- **In-control zijn/governance**: voldoen aan (nieuwe) wetgeving en dit zowel in beleid als in de praktijk laten zien
- IT - OT Big Data analytics, GIS, Forecasting, bijv. ook: weersvoorspelling

Verdonck, Klooster & Associates (VKA) zet zich in om ICT voor mensen te laten werken. We zijn een strategisch ICT-adviesbureau en we houden van complexe vraagstukken. Omdat het uiteindelijk allemaal om mensen draait, hebben we bij VKA niet alleen technische specialisten in huis, maar ook mensen die een organisatie kunnen lezen. Wij realiseren succesvolle projecten die ervoor zorgen dat ICT doet waarvoor het bedoeld is: het leven makkelijker maken met slimmere, efficiëntere en snellere oplossingen. VKA heeft ruim 30 manjaar ervaring in het beveiligen van Industriële Automatiseringssystemen.

Verdonck, Klooster & Associates | Baron de Coubertinlaan 1 | 2719 EN Zoetermeer | T 079 368 1000 | E info@vka.nl | **www.vka.nl**

VERDONCK KLOOSTER & ASSOCIATES