Manage an adequate operational framework to meet cyber security challenges in process, product and service design and implementation

- responsibilities, roles, experience, capacities: manage a well balanced approach
- quality assurance of processes, services, and products: capable and competent provisions in structures, responsibilities, authorities and procedures

Statements – Security is everybody‘s business

- Security has to involve everybody (product chain, employees, partners, leadership)
- Security has to be started with product development
- Security only works Top down
- Implement Security in business model

Statements – Key facts

- Advantages if IT Security is not part of IT
- 80% of companies only invest in IT security once they got breached
- Minimize impact of attack → resilience
- Risk Management instead of 100% Security
- Different security levels depending on data sensitivity
- Perimeter is not visible anymore
- Enduser security education is not the answer

National differences

- Difference in countries, e.g. Israel is more educated on cyber security (starting in school)
- Germany is (10 years?) behind Israel and US developing security systems (i.e. in Israel security companies get startup funding)
- Strong cooperation between public/private

Open Questions

- How do you implement Security (updates/patches) into low cost mass systems (i.e. IoT)
- Security expiration for products ?
- Is the manufacturer allowed to update i.e. a car in case of security updates ?
    - Who is liable ?
    - Warranty lost if security updates are not implemented ?
- Wouldn´t it make more sense to support non security startups with processes for secure development instead of patching issues afterwards ?

Baseline

GLOBAL INDUSTRY CLUB

We don´t need more security –
we need the right security

… but what is right ?