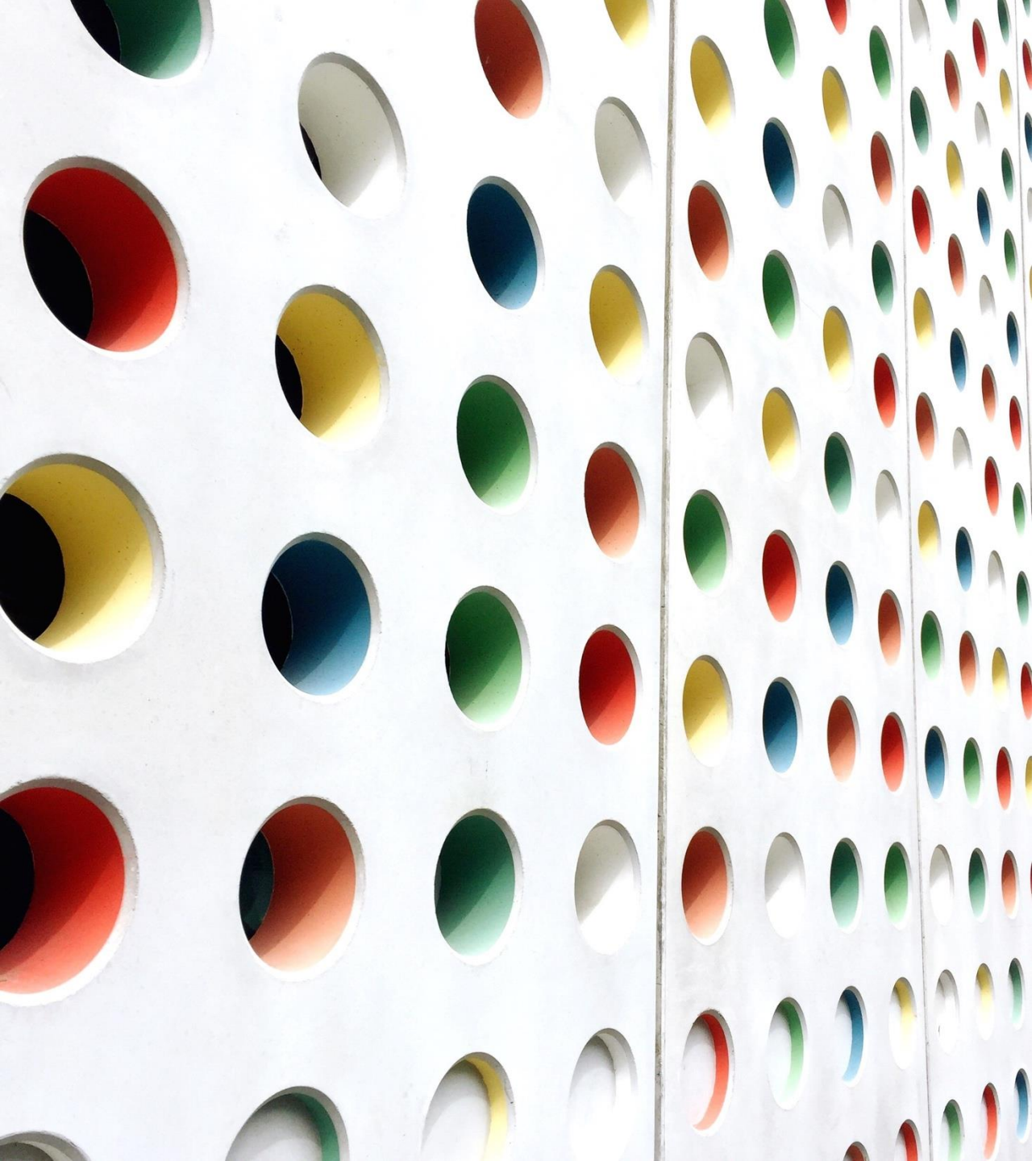


Lantech®

Pioneering Industrial and IP Networks

AACII

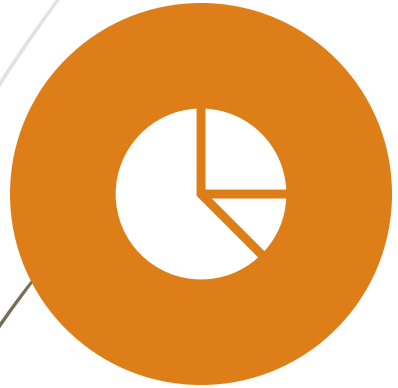
Cyber Security

The Challenge of the future in a growing business

Günter Meixner, CEO Europe

The Three Pillars

Lantech®
Pioneering Industrial and IP Networks



HANDLING

TECHNOLOGY

SOCIAL CHALLENGE

Günter Meixner, CEO Lantech Communications Europe GmbH

Feeling

- What is SECURITY? ….. possible descriptions

1. You can‘t put your hands on Cyber Security
2. Cyber Security is a feeling
3. Cyber Security is a need
4. Cyber Security is based on experiences
5. Cyber Security is based on education
6. Cyber Security is based on infrastructure
7. Cyber Security is based on technology

Cyber Security

If you do not know what is going on in your area of responsibilty

- You will always have a bad feeling
- You do not know how to act
- You do not know how to protect

You need a reliable team to communicate and to build up a team with dedicated responsibilities.

You need external consultants with an outside view of the internal structure to find weak points.

Günter Meixner, CEO Lantech Communications Europe GmbH

Handling

What has been considered so far?

- Data centers
- Enterprise environment
- Home offices
- Critical infrastructure

but not (apparently) closed networks… mainly industrial used equipment

-> Most of them are meanwhile connected to the internet and attackable

Technology

Technology is very good in enterprise environments

- Firewalls
- Software
- Processes
- Monitoring
- Updates
- Segmentation (minimize the attackable area)

Technology

Lantech®
Pioneering Industrial and IP Networks

Did you consider the industrial used parts of your organization?

- Infrastructure
- Reliability
- Cyber security feature built-in?
- Monitoring
- Updates
- Segmentation (minimize the attackable area)

Social Challenge

What percentage of attacks are social engineering?

Social engineering accounts for approximately **70-90%** of cyber attacks, with phishing being the most prevalent method. (12/31/2024)

Conclusion

Besides the infrastructural, technological and procedural challenges, the social component is by far the greatest challenge.

It is highly recommended to train all employees to sensitize them to recognize attacks.

What to do?

Consider the entire existing infrastructure and all associated technologies.

Devices and connections must also be secured in industrial networks. In future, manufacturers will have to implement cyber security mechanisms in the devices to ensure secure data transfer.

Lantech®
Pioneering Industrial and IP Networks

THANK YOU

Günter Meixner, CEO Lantech Communications Europe GmbH