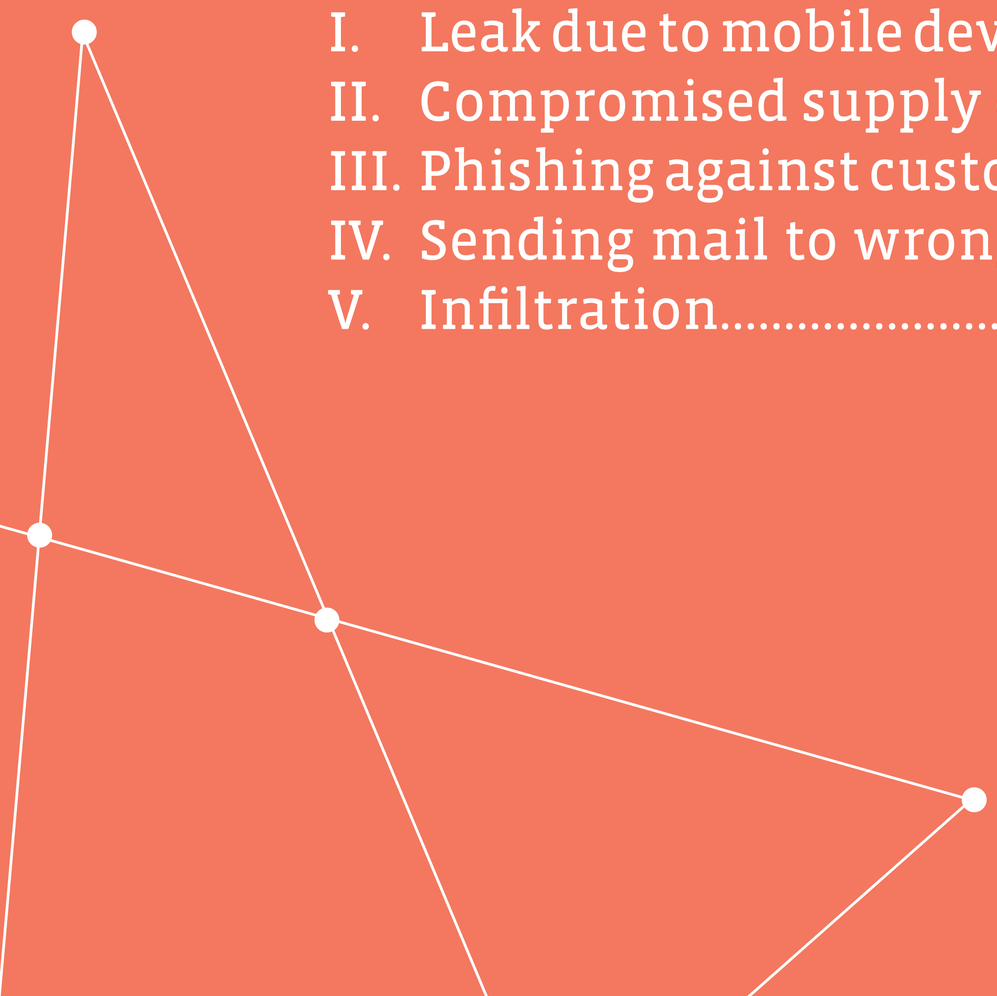
CYBERESPIONAGE FOR THE INDUSTRY SECTOR

FEDIL
The Voice of Luxembourg's Industry

TABLE OF CONTENTS



FOREWORD

FEDIL, The Voice of the Luxembourg's Industry, in collaboration with the **Ministry of the Economy** (Department of the e-commerce and Information Security) launched a **Forum on Cybersecurity** dedicated to the manufacturing industry (IND). This forum follows the principles of an **« Information Sharing and Analysis Center »** (ISAC).
The IND-ISAC mission is to promote the cooperation in terms of cybersecurity within the manufacturing industry sector in Luxembourg and the Greater Region for the benefit of the attractiveness of the ecosystem.

As stated in the political guidelines for the European Commission 2019–2024, « *we need to move from "need to know" to "need to share"* ». The mission is achieved through (1) information and knowledge sharing among trusted representatives of the member organizations, and (2) dissemination of manufacturing industry-related risk information relevant for the public.

The IND-ISAC aims at creating a "taxonomy", common language required, to foster synergies and share common understanding of the risks within the company, the group, and the ecosystem by highlighting :

- the importance of informed governance, meaning cybersecurity governance at a sectorial, group or company level based upon as much factual information as possible (advantages for the CISO), and
- the importance of risk management and most of all the usage of as much objective and factual information as possible, and
- the importance of implementing communication between technical and organizational security by involving companies' top management.

The IND-ISAC is composed of companies' cybersecurity representatives from several industries.

The IND-ISAC will continue its work by enabling companies to share information, experience, knowledge and best practices among peers in a climate of trust. It aims at indentifying sector-specific risk scenarios, vulnerabilities and threats and provides companies with a concrete guidance in conducting a risk management analysis.

Should you wish to join the IND-ISAC and become an active member, we kindly invite you to contact our team.

FEDIL

INTRODUCTION

Espionage should be considered as high priority for companies. Spies can use three levers to steal company information:

- by exploiting human vulnerabilities of the company's staff;
- by fiddling with company processes; and
- by making use of technology, and in particular, technical vulnerabilities

to gain an economic advantage, steal information on patented products, influence business opportunities, or get valuable information for adjusting competitive pricing in the frame of the proposal of contracts.

This document lists and describes the possible espionage scenarios that were established in the specific context of the industrial sector but can also be tailored to any other economic sector.

A. ATTACK PATHS

I-PEOPLE

The sections below explain why people remain one of the first vulnerabilities in need of specific attention.

1. PEOPLE, AS VICTIMS

a) MUGGED WHILE TRAVELLING

KEY FINDINGS

People may carry sensitive documents and count as easy targets when travelling (abroad, in public transport, at conferences, ...). Physical or media containing digital documents can easily be stolen.

KEY MEASURES

- Set-up anti-theft measures (locks, Kensington-like security slots, ...),
- Consider using burner phones and laptops containing only the necessary documents,
- Encrypt storage media and laptops (laptops must be shut down when transported),
- Never leave material unattended (fairs, hotel rooms, public transport, meeting rooms, ...),
- Encrypt phones,
- Organize awareness training for physical security,
- Use tamper-evident envelopes if phones must be left outside a meeting room, switch them off, or even better mandate one delegation member to keep phones outside a meeting room,
- Never leave anything in a hotel room or safe,
- Never use the hotel business lounge to work,
- Never talk about confidential affairs in hotel rooms, bars, restaurants, public transport, taxis, airports or train stations,
- Organize dedicated briefings for high-risk travel destinations.

b) EAVESDROPPING IN PUBLIC NETWORKS

KEY FINDINGS

Criminals may attack employees in public, corporate or hotel Wi-Fi networks and sniff network connections.

KEY MEASURES

- Enforce the use of VPN for the entirety of network connections when travelling (in some countries, hotels, facilities, typical VPN ports might be blocked – be prepared for that),
- Consider using mobile data (such as 4G) instead of Wi-Fi,
- Use end-to-end security communication instead of e-mail,
- Check the connection types of your mobile phone. If it falls back to 2G, your phone is most probably being eavesdropped. The downgrade attack consists in disconnecting a phone from the network by sending malicious data, forcing it to fall back to 2G encryption that is easily cracked.

c) SOCIAL ENGINEERING

KEY FINDINGS

Manipulating people by exploiting human vulnerabilities (such as fear, insecurity, sex or greed - ‘MICE’: Money, Ideology, Constraint, Ego) is simple and effective. Using social engineering techniques, spies are able to bypass security checks or physical barriers.

KEY MEASURES

- Organize awareness training for social engineering,
- Watch out during airport security checks.

d) DECEPTION USING IMPERSONATION VIA E-MAIL

KEY FINDINGS

Criminals use fake e-mail messages (similar to phishing) to impersonate a company department or an employee's superior and try to make employees hand over sensitive information.

KEY MEASURES

- Organize awareness training for social engineering,
- Secure alternatives to e-mail designed in such a way that impersonation is not possible (company-internal messaging or collaboration platforms, but also a digital signature of e-mails),
- Implement the four-eyes principle and segregation of duties for sensitive processes (e.g. accessing or modifying sensitive data).

e) INFILTRATION

KEY FINDINGS

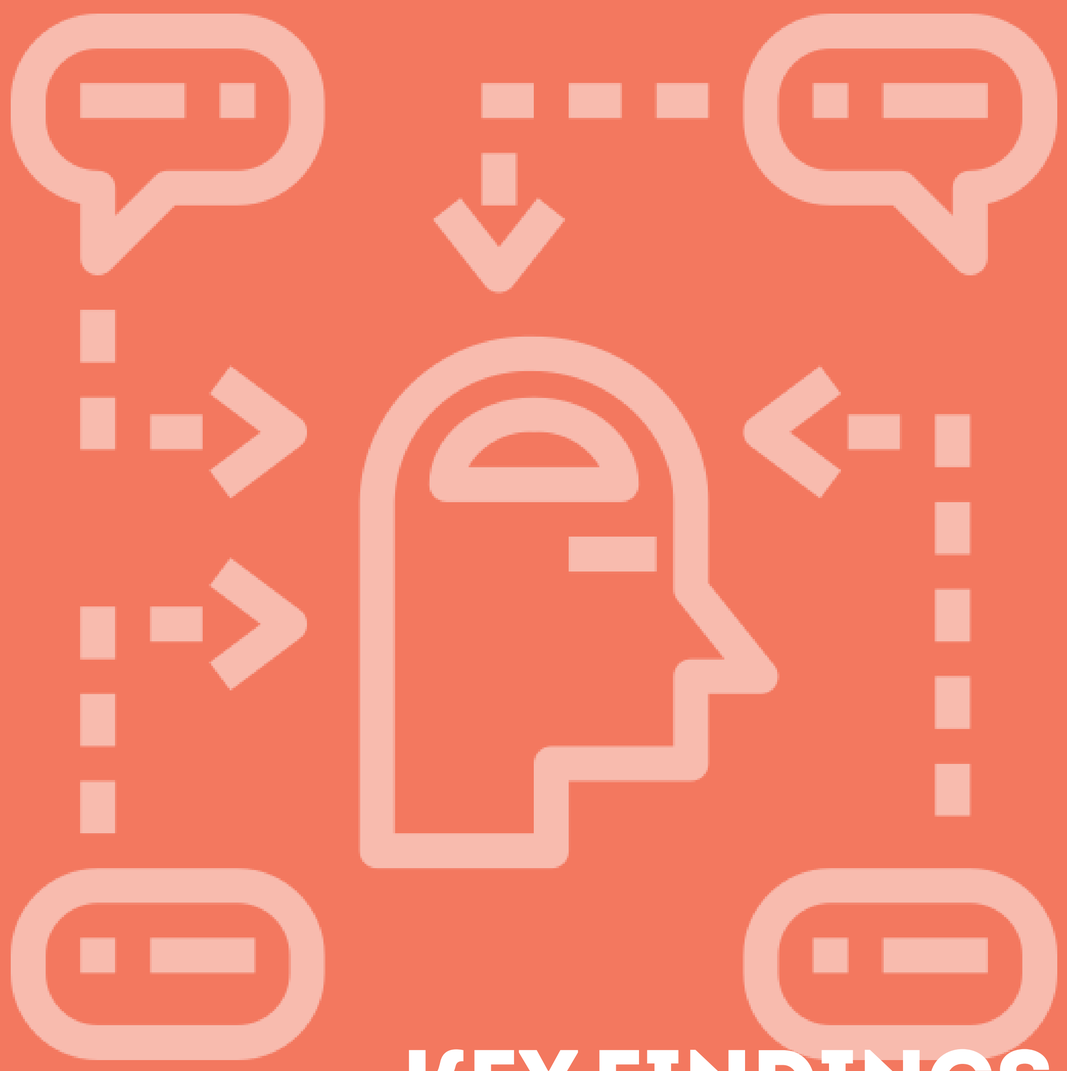
Infiltration starts with spies collecting publicly available information about a potential target from social media, websites, organizational charts, etc. The goal of creating such a profile is to ultimately get in touch with the person. In a second step, spies try to obtain non-public information from the person or their colleagues, either digitally (e.g. phishing) or physically (e.g. by approaching them at an event). Once enough information is gathered, spies try to get in touch (befriending the person or their colleagues, apply for an internship, etc.). When confidence has been built, they start asking for small favours, then larger ones such as leaking sensitive information.

KEY MEASURES

- Organize special awareness training for people who travel a lot or who appear publicly for the company (conferences, events).

2. PEOPLE, AS OFFENDERS

a) INSIDER THREAT



KEY FINDINGS

Employees may wilfully leak information for many reasons. Unsatisfied employees may wish to harm the company. Badly paid employees are susceptible to corruption, since organized criminals may be ready to pay a multiple of their annual salary at once.

KEY MEASURES

- Corruption detection and prevention,
- Contact with law enforcement,
- Prevention through strict ‘Need To Know’ policies, compartmentalization of information, detection of unexpected accesses (volumes, times).

b) BLACKMAIL

KEY FINDINGS

Any employee can be blackmailed to leak sensitive information, especially when they are in difficult financial situations.

KEY MEASURES

- Contact with law enforcement,
- Put in place a ‘Hotline’ with trained people.

3. PEOPLE, ACCIDENTALLY

a) ACCIDENTAL LEAK OF INFORMATION

KEY FINDINGS

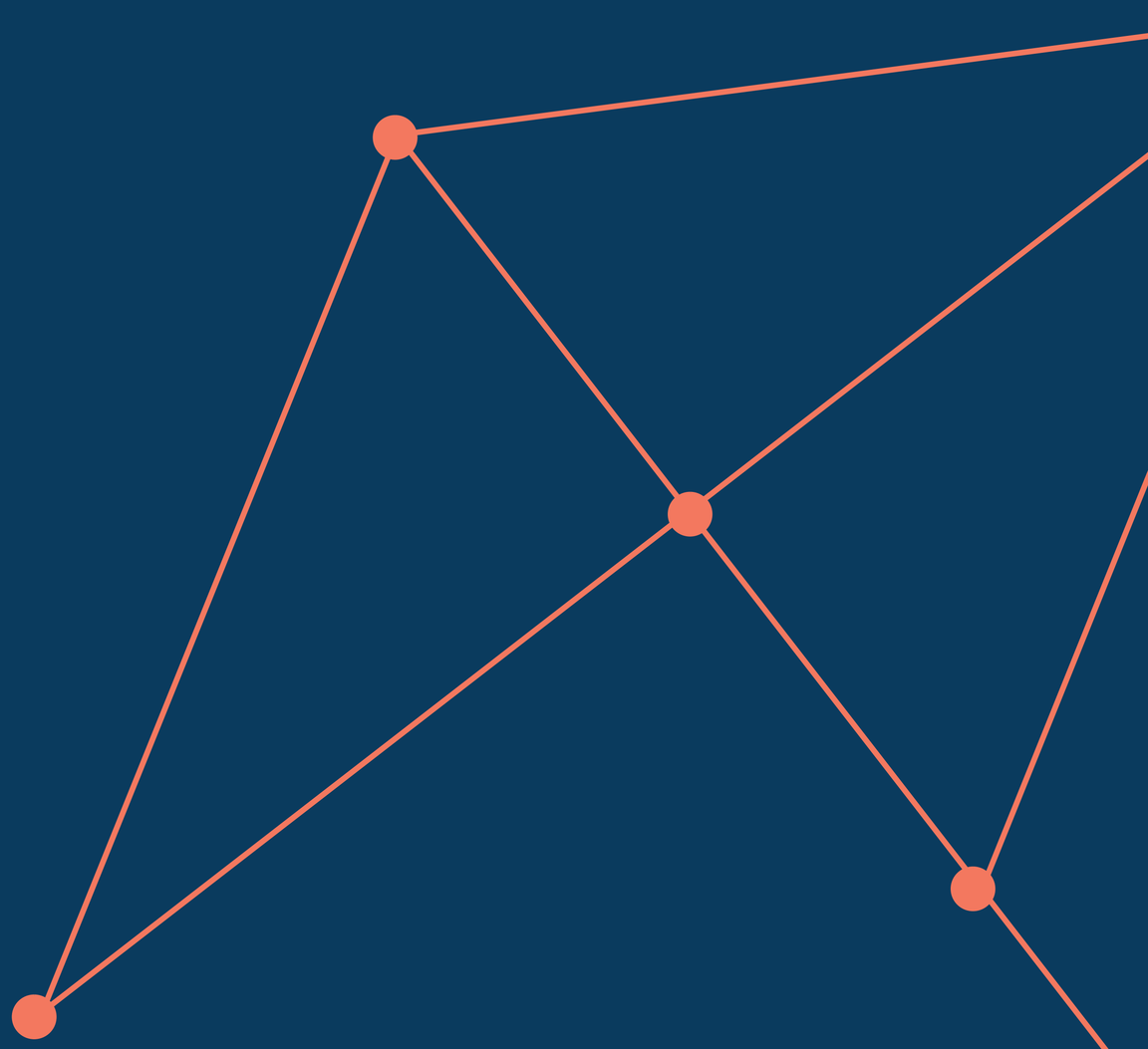
Mistakes happen. For example, employees may send sensitive information to the wrong recipient. Moreover, when people have auto-forwarding set up (e.g. when they are out of office), confidential e-mail potentially leaves the perimeter of the company. The first thing a hacker will do with a compromised mail account is to activate auto-forwarding and/or delegation, which shall thus be monitored.

KEY MEASURES

- Organize awareness training,
- Implement secure sharing platform, enforce and train its use,
- Security incident response,
- Discourage and disable the use of auto-forwarding e-mail,
- Put a policy in place rewarding employees who report security incidents.

II-PROCESSES

1. LOW SUPPLIER SECURITY



KEY FINDINGS

Industrial suppliers often have lower security standards because they have fewer resources available (personnel and financial). Criminals try to compromise suppliers first, and then use them covertly to compromise the contracting company.

KEY MEASURES

- Carry out due diligence,
- Review supplier management process (including audit of suppliers),
- Strengthen incident management preparedness,
- Help/require your suppliers to become better protected (e.g. through certification).

2. HIGH-TECH SPYING USING DRONES

KEY FINDINGS

Modern technology has allowed for miniature but high-resolution cameras and flying drones. Both enable criminals to exfiltrate information (e.g. manufacturing processes, documents lying around) without the need of hacking devices or manipulating people.

KEY MEASURES

- Strengthen physical security to consider the risk of robots and drones,
- Enforce clean desk policy.

3. LOW PHYSICAL SECURITY

KEY FINDINGS

When physical access to sites is poorly secured, spies can enter the premises and steal/copy documents. Moreover, documents can lie around on desks, but also in the printer tray.

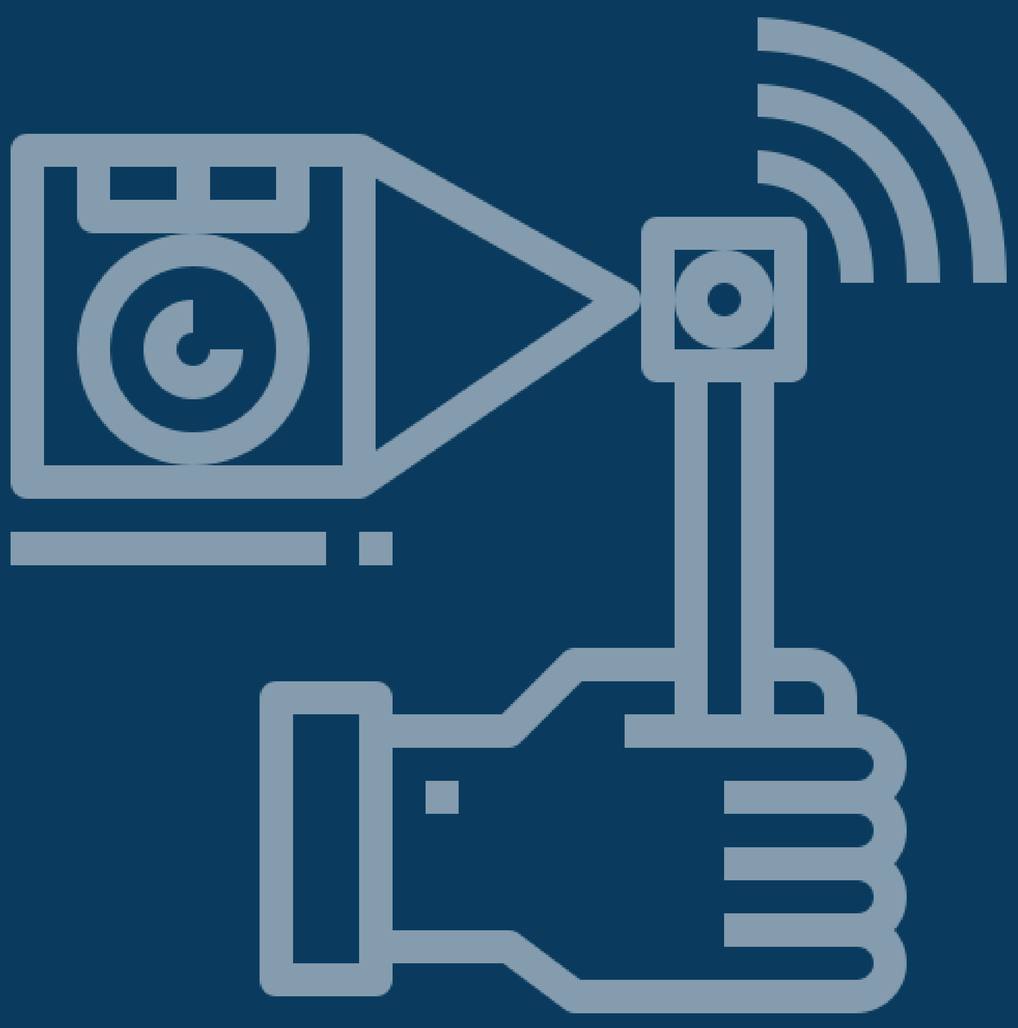
KEY MEASURES

- Reinforce physical access control (e.g. reception desk),
- Define public and private zones. Insist that employees stop seeing respectively will not stay with unknown people in public zones,
- Enforce clean desk policy,
- Require log-in for industrial control systems, even if terminals are on-site and physical access is controlled,
- Enforce the use of screen locking and the need to unlock using credentials,
- Encourage people to pick up printed documents immediately (possibly require badges for printing on printers).

4. SPYING COMPONENTS WITHIN PREMISES

KEY FINDINGS

Once inside the company premises, a criminal can place spying devices, such as microphones, cameras or keyloggers.



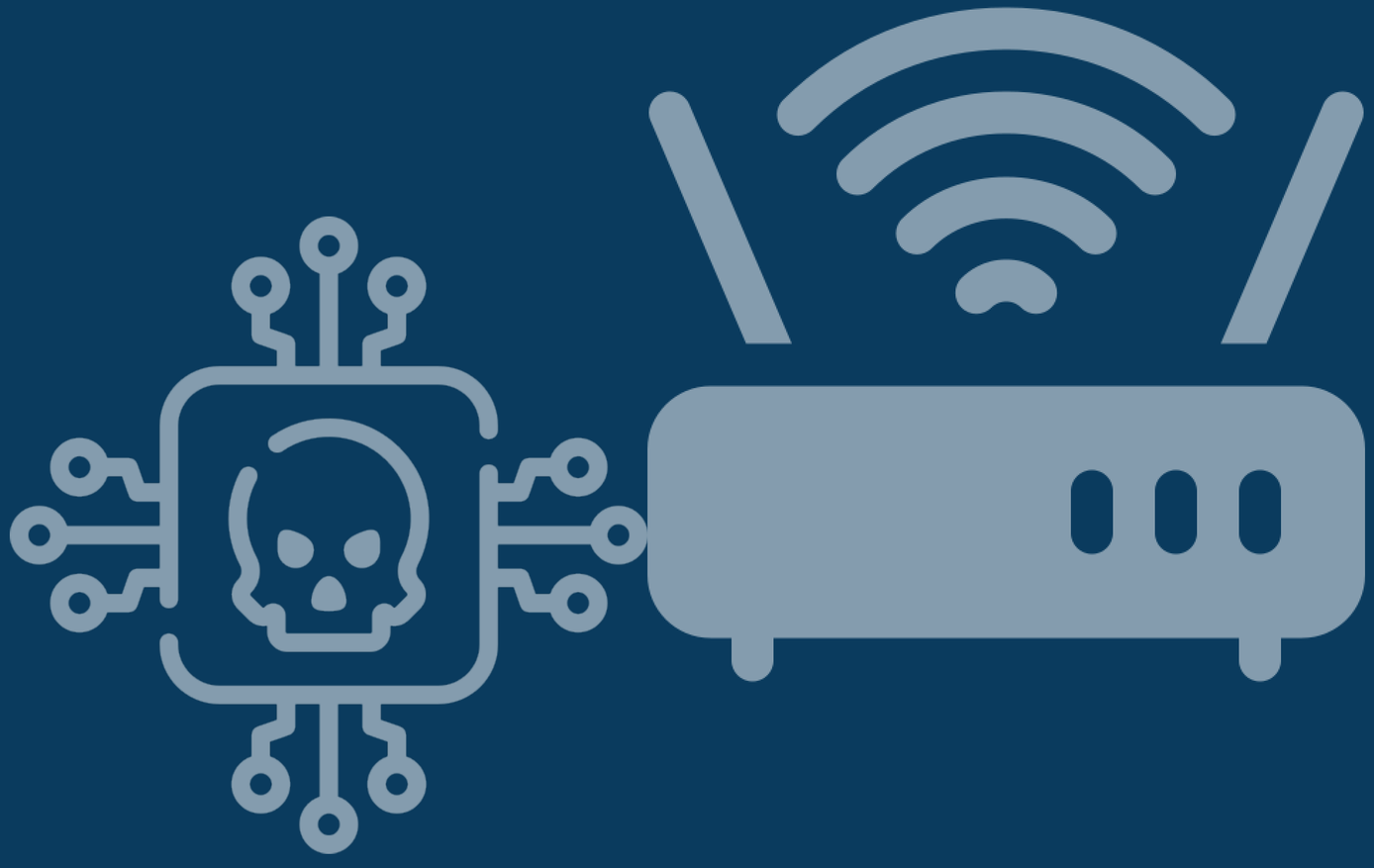
KEY MEASURES

- Deploy and enforce Network Access Control (NAC) capabilities for protecting wired connections,
- Carry-out a Wi-Fi audit to detect rogue access points,
- Organize awareness training for detecting spying devices.

5. ROGUE WI-FI ACCESS POINT

KEY FINDINGS

Once inside the company premises, criminals can plug a Wi-Fi access point into any unprotected network socket to obtain permanent access to the company's internal network.



KEY MEASURES

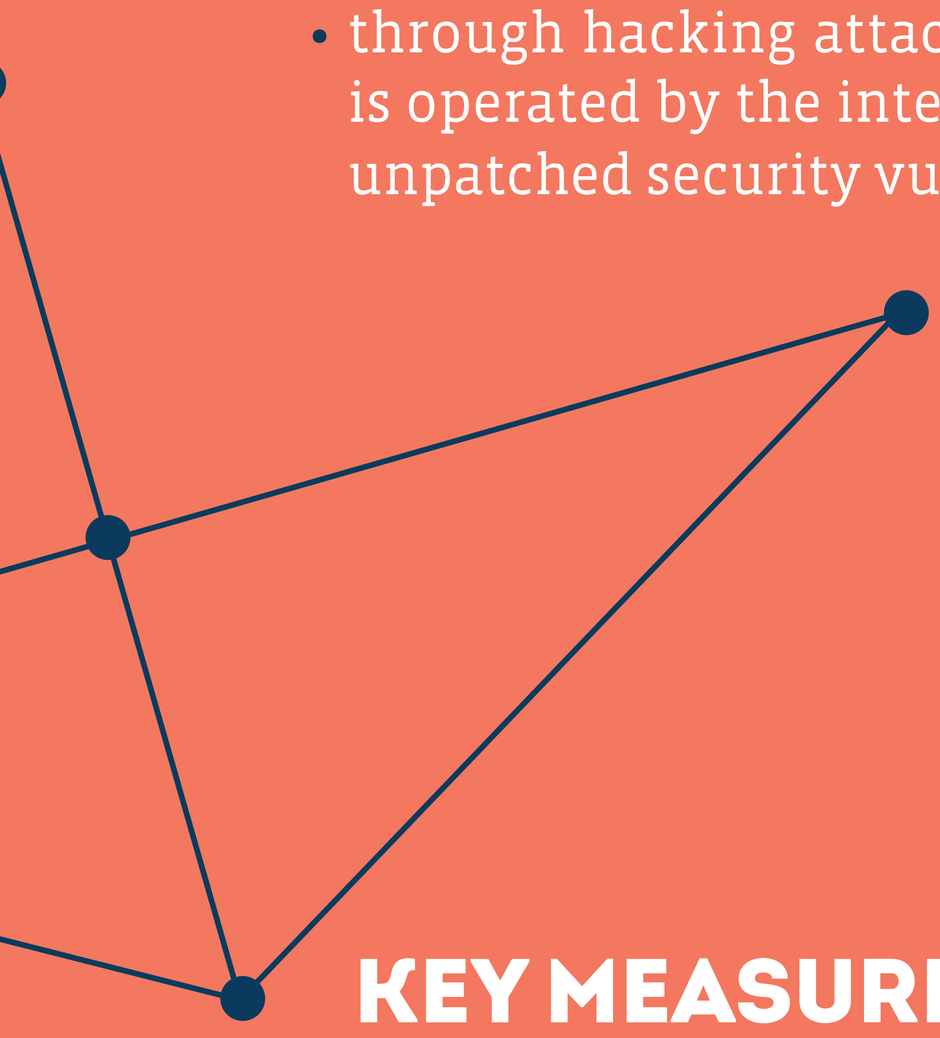
- Implement Network Access Control (NAC),
- Carry-out a Wi-Fi audit to detect rogue access points.

1. ENDPOINT SECURITY

KEY FINDINGS

Especially when working from home on their personal computers, employees are susceptible to malware that they receive via e-mail attachments or download online. In unprotected home networks, personal devices are exposed to a certain risk of being compromised:

- from other devices in the home network,
- via Wi-Fi (when it is not properly protected, e.g. with a weak password),
  or
- DNS protection is not strong enough,
- through hacking attacks onto the internet router (which is operated by the internet service provider and often has unpatched security vulnerabilities).



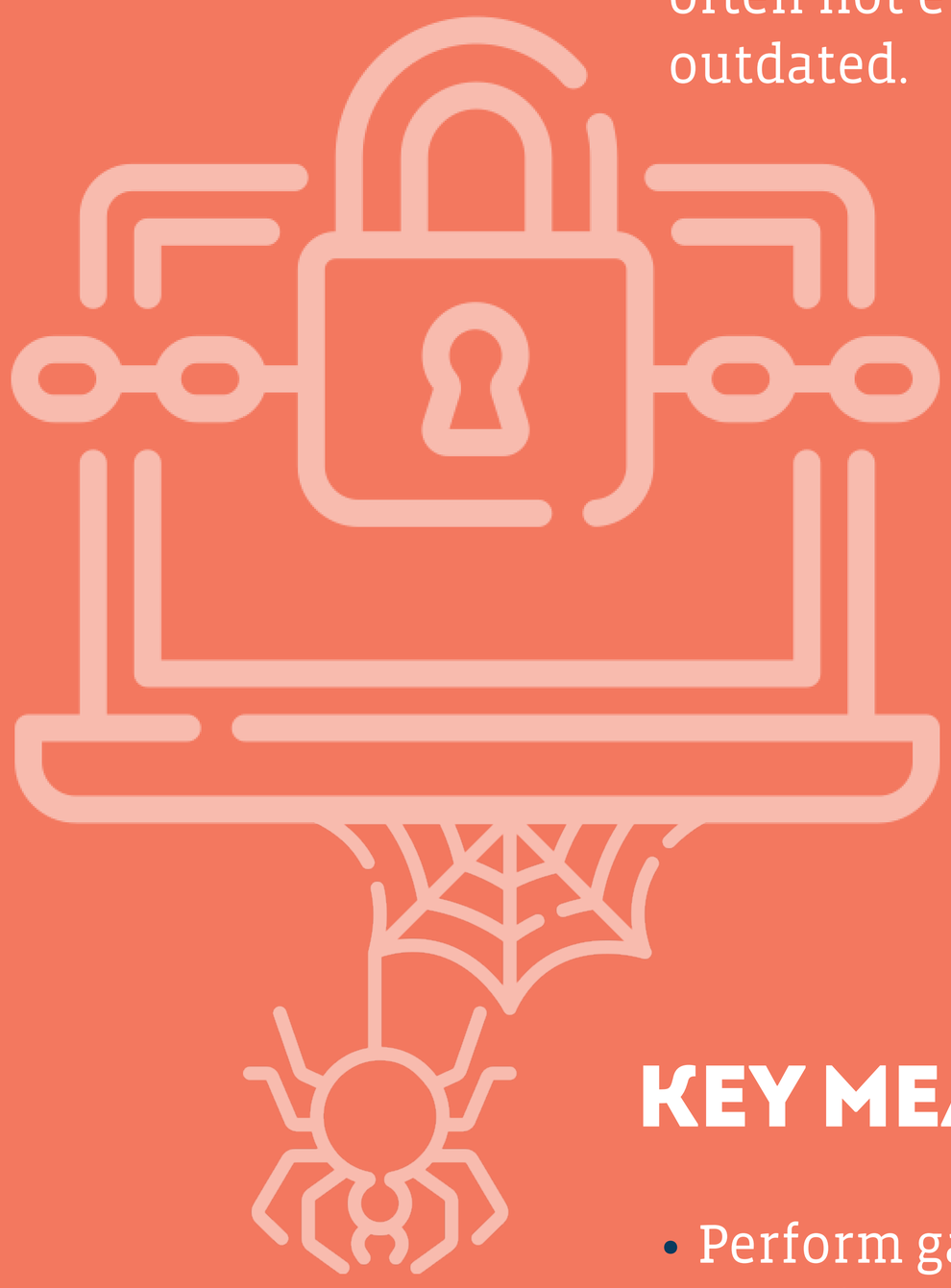
KEY MEASURES

- Provide an additional router to your (critical) employees to ensure the required security level,
- Ensure security on endpoint devices (scanning, monitoring, logging, updates, back-ups, strong authentication),
- Organize awareness training for malware.

2. OUTDATED IT SECURITY CONTROLS

KEY FINDINGS

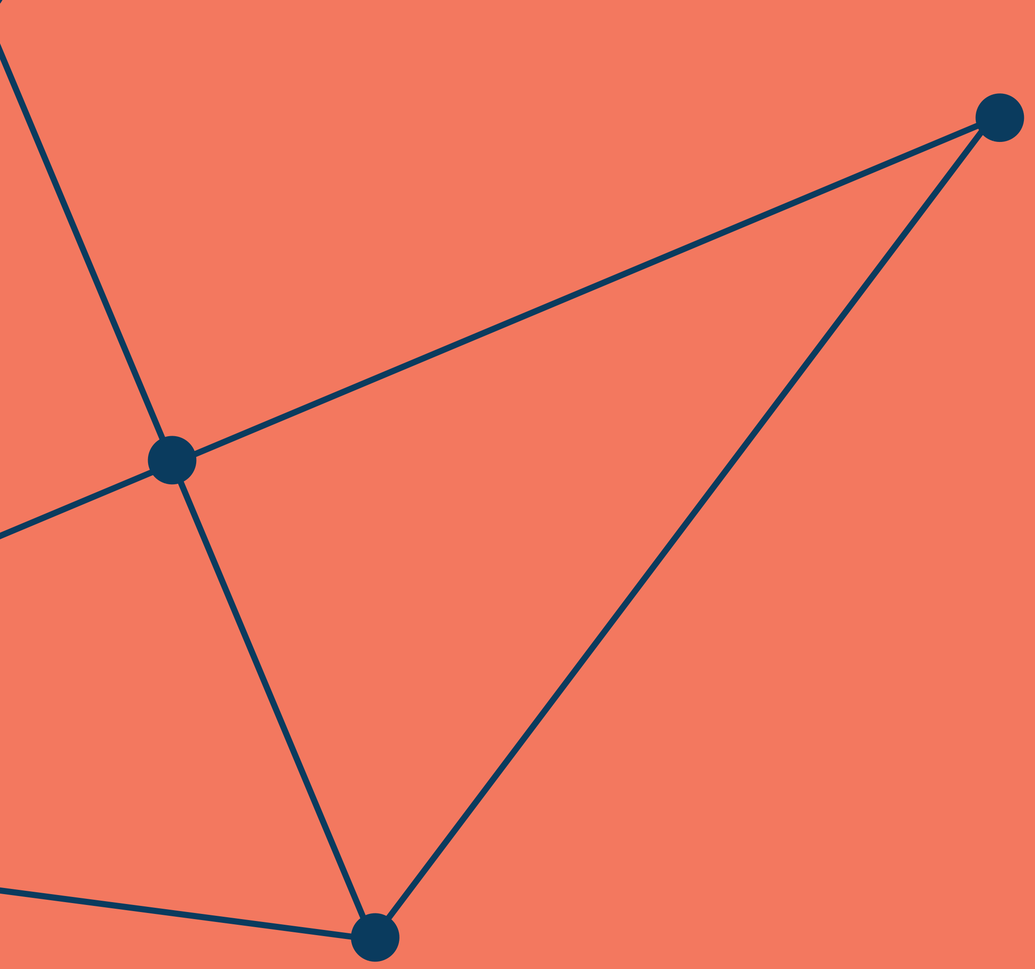
IT and information security is only a supporting process for the manufacturing industry since it is not lucrative. On the contrary, the manufacturing industry is rather reluctant to spend resources on IT or security equipment. However, since security is rapidly evolving, it requires regular modernization. As a result, the IT infrastructure is poorly secured (which becomes critical in an industry 4.0 context). Companies are often not even aware of the fact that their infrastructure is outdated.



KEY MEASURES

- Perform gap/maturity assessment to evaluate the level of security of the infrastructure,
- Convince the management department that security is primordial,
- Modernize IT infrastructure (especially from a security perspective).

3. CLOUD SECURITY



KEY FINDINGS

Cloud solutions usually provide good security opportunities, such as high availability and physical security. However, cloud platforms are often badly configured or poorly managed due to the lack of competence and resources. Moreover, cloud platforms are publicly accessible and thus suffer from phishing problems, especially when strong authentication is rarely implemented.

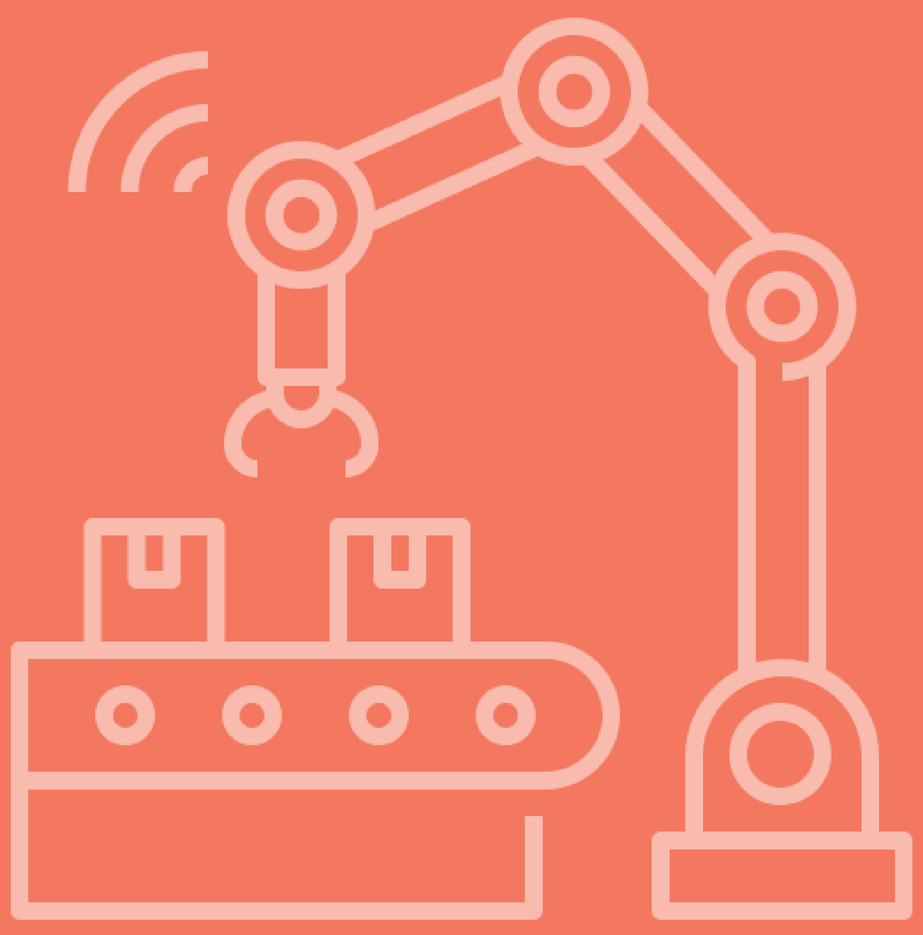
KEY MEASURES

- Extend cloud competences in the company, or subcontract a recognized professional,
- Implement strong/multi-factor authentication,
- Configure back-ups and document versioning,
- Ensure that security patches are applied,
- Implement Cloud Security Posture Control.

4. INDUSTRY 4.0

KEY FINDINGS

Industry 4.0 components collect a lot of sensor data. This data might be sent to the suppliers without sanitization and reveal critical information.



KEY MEASURES

- Implement information governance and decide what sensor data can be sent to a supplier,
- Implement maintenance procedures with vendors (dedicated time, from a specific IP address), limited to the necessary sub-networks. Record and keep proof of these sessions,
- Implement strong authentication for maintenance interfaces,
- Secure VPN endpoint management.

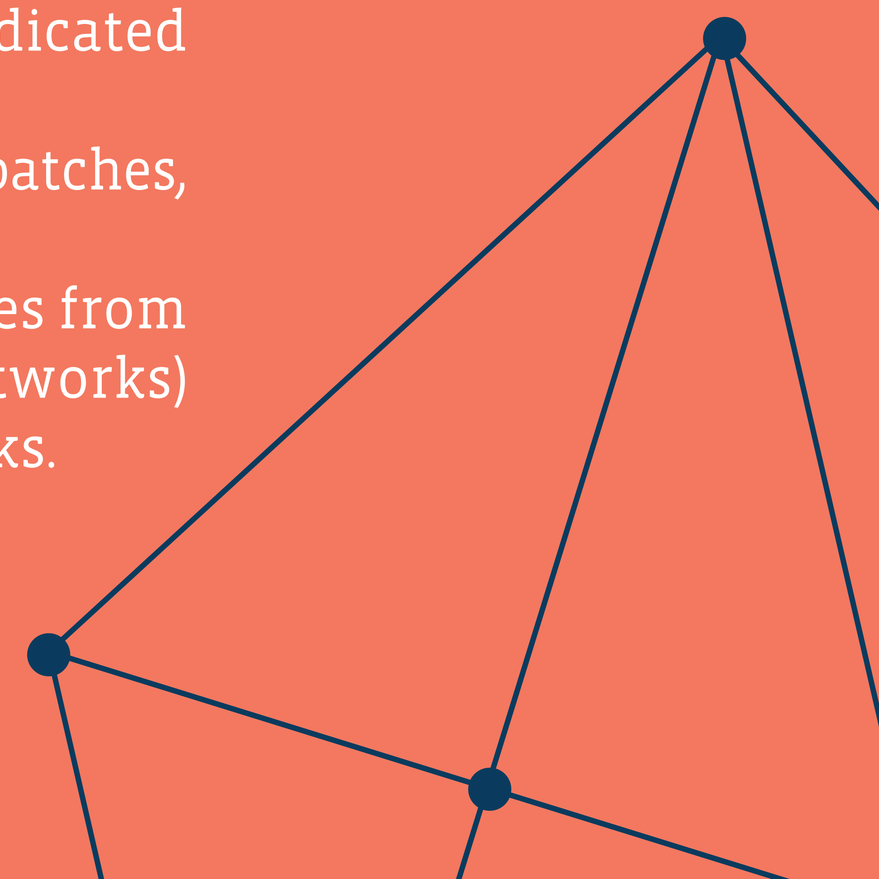
5. INTERNET OF THINGS

KEY FINDINGS

Smart devices (e.g. smart door locks) often have a poor security design or use unmaintained software. If that is the case, they can be remotely controlled or hacked, which allows spies to get insight into the company (e.g. when the guards leave) or even remotely open doors or disable alarms. Moreover, they can be an entry point to the internal network.

KEY MEASURES

- Avoid buying IoT devices that require an (uncontrolled) connection to external cloud or networks,
- Restrict network access of IoT devices through dedicated networks and firewalls (inbound and outbound),
- Regularly check for firmware updates and security patches,
- Use strong passwords for IoT devices,
- As much as possible, isolate networks of IoT devices from other resources of the company (systems and networks) by segregating IoT devices and associated networks.



B. RISK SCENARIOS

I-LEAK DUE TO MOBILE DEVICES HAVING ACCESS TO CONFIDENTIAL INFORMATION

DESCRIPTION

Employees need permanent access to company documents or mail on their mobile devices, especially, when they are travelling or at home. To this end, confidential data that is otherwise well-protected within the company's premises, is exposed and possibly stolen. Moreover, detecting phishing and scam on mobile devices is much harder than on computers. The risk that employees save confidential documents (consciously or not) on their phones, where malicious apps have access to, is high. Furthermore, there is a risk that employees share sensitive information over social networks or third-party service providers (cloud, e-mail) that are out of the control of the company.

Hardening measures:

- Device encryption (e.g. BitLocker) and mandatory screen locks prevent data leaks after a device is stolen,
- Mobile device management (MDM) software allows a company to apply restrictions on what an employee is allowed to access to or do on his or her (professional) smartphone and allows the company to have remote control over the devices (mainly to be capable of performing a remote wipe in case of theft of the device),
- Multi-factor authentication prevents easy stealing of credentials,
- IP address or domain locking hardens unauthorized access,
- Offering secure messenger alternatives (such as company-internal collaboration platforms) to employees limits the risk of sharing via insecure media.

ATTACK PATHS

HUMAN

- [x] Mugged while travelling
- [ ] Eavesdropping in public networks
- [x] Social engineering
- [x] Deception using impersonation via e-mail
- [ ] Infiltration
- [ ] Insider threat
- [ ] Blackmail
- [ ] Accidental leak of information

PROCESSES

- [ ] Low supplier security
- [ ] High-tech spying using drones
- [ ] Low physical security
- [ ] Spying components within premises
- [ ] Rogue Wi-Fi access point

TECHNOLOGY

- [x] Endpoint security
- [ ] Outdated IT security controls
- [x] Cloud security
- [ ] Industry 4.0
- [ ] Internet of Things

II-COMPROMISED SUPPLY CHAIN

DESCRIPTION

Compromises in the supply chain are not necessarily detected, and even if they are, suppliers might not transparently communicate about it for fear of the consequences (financial, legal or repudiation) when such an incident becomes public.

Specific controls:
- Address the ‘right to audit’ with suppliers,
- Establish and maintain contact with suppliers,
- Prepare the scenario of the supply-chain compromission into the incident management process.

ATTACK PATHS

HUMAN

- ☐ Mugged while travelling
- ☐ Eavesdropping in public networks
- ☐ Social engineering
- ☐ Deception using impersonation via e-mail
- ☐ Infiltration
- ☐ Insider threat
- ☐ Blackmail
- ☐ Accidental leak of information

PROCESSES

- ☑ Low supplier security
- ☐ High-tech spying using drones
- ☐ Low physical security
- ☐ Spying components within premises
- ☐ Rogue Wi-Fi access point

TECHNOLOGY

- ☐ Endpoint security
- ☐ Outdated IT security controls
- ☐ Cloud security
- ☐ Industry 4.0
- ☑ Internet of Things

III-PHISHING AGAINST CUSTOMERS

DESCRIPTION

The company's customers may also hold a copy of confidential information (plans, configuration data, pricing, ...). Criminals may apply social engineering techniques (e.g. phishing mail) to customers, impersonating the company and asking for this confidential information.

Hardening measures:

- Secure communication channels with customers,
- Increase staff's awareness,
- Inform customers and partners of the social engineering risk and recommend performing security awareness to their staff.

ATTACK PATHS

HUMAN

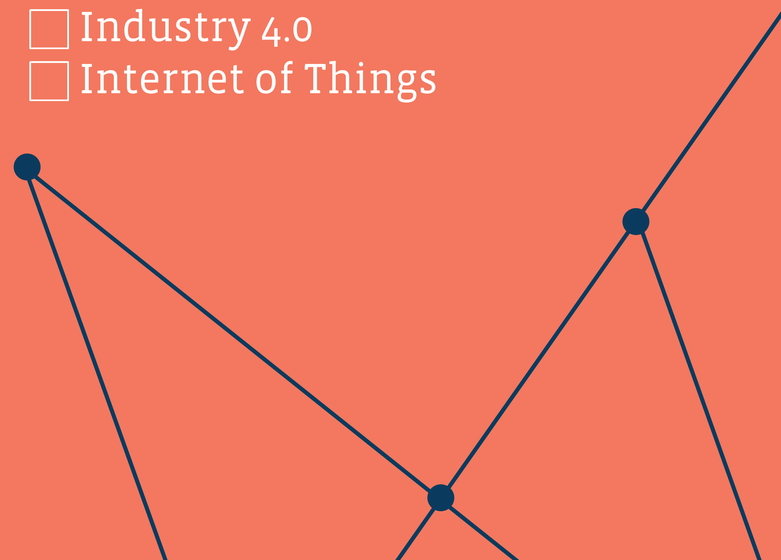
- ☐ Mugged while travelling
- ☐ Eavesdropping in public networks
- ☑ Social engineering
- ☑ Deception using impersonation via e-mail
- ☐ Infiltration
- ☐ Insider threat
- ☐ Blackmail
- ☐ Accidental leak of information

PROCESSES

- ☐ Low supplier security
- ☐ High-tech spying using drones
- ☐ Low physical security
- ☐ Spying components within premises
- ☐ Rogue Wi-Fi access point

TECHNOLOGY

- ☐ Endpoint security
- ☐ Outdated IT security controls
- ☐ Cloud security
- ☐ Industry 4.0
- ☐ Internet of Things



IV-SENDING MAIL TO THE WRONG PEOPLE

DESCRIPTION

Confidential documents leak when the wrong people are put in copy of an e-mail.

Hardening measures:

- Appending the company name of business contacts at the end of each contact's display name makes it easier to spot mistakes,
- Increase staff's awareness,
- Consider removing the auto-completion of the e-mail address,
- Request a formal approval (by clicking on a button) when sending e-mails outside the company (when they contain sensitive material, the latter require to have data classification policy and Data Leakage Prevention (DLP) solution in place).

ATTACK PATHS

HUMAN

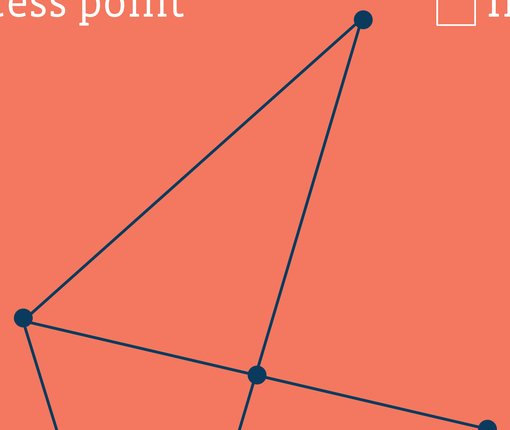
- ☐ Mugged while travelling
- ☐ Eavesdropping in public networks
- ☐ Social engineering
- ☐ Deception using impersonation via e-mail
- ☐ Infiltration
- ☐ Insider threat
- ☐ Blackmail
- ☑ Accidental leak of information

PROCESSES

- ☐ Low supplier security
- ☐ High-tech spying using drones
- ☐ Low physical security
- ☐ Spying components within premises
- ☐ Rogue Wi-Fi access point

TECHNOLOGY

- ☐ Endpoint security
- ☐ Outdated IT security controls
- ☐ Cloud security
- ☐ Industry 4.0
- ☐ Internet of Things



V-INFILTRATION

DESCRIPTION

Spies try to approach or befriend employees with the goal of asking favours, such as giving them sensitive information.

Hardening measures:
- Awareness training for employees who are in touch with the public (travelling, conferences, events, ...).

ATTACK PATHS

HUMAN

- [x] Mugged while travelling
- [x] Eavesdropping in public networks
- [x] Social engineering
- [x] Deception using impersonation via e-mail
- [x] Infiltration
- [x] Insider threat
- [x] Blackmail
- [ ] Accidental leak of information

PROCESSES

- [ ] Low supplier security
- [ ] High-tech spying using drones
- [x] Low physical security
- [ ] Spying components within premises
- [ ] Rogue Wi-Fi access point

TECHNOLOGY

- [x] Endpoint security
- [ ] Outdated IT security controls
- [ ] Cloud security
- [ ] Industry 4.0
- [ ] Internet of Things

Should you wish to join the ISAC, please, contact:

Céline Tarraube
Adviser Digital & Innovation
celine.tarraube@fedil.lu
(+352) 43 53 66 610