4.2.2 Vulnerable railway infrastructure	
Security Goal(s):	Integrity: Control signals could be abused to manipulate railway switches and therefore provoke accidents.
Motivation:	Malefactors interested in creating chaos.
Mistake(s) / Vulnerabilite(s):	Standard passwords of network switches are circulated online.
Solution:	Raise the awareness among the suppliers to not use standard passwords.

4.3.1 Advertising networks **4.3.1.1 Website infections on daily newspaper**	
Security Goal(s):	Integrity: Installed the e-banking Trojan Gozi IFSB in an advertising network. The infected advertising content is sent out to a wide range of clients, e.g. online newspapers. This attack vector is called drive-by infection. The malware scans the browsers for vulnerabilities in the browser itself or in installed plugins (Java, Flash).
Motivation:	Gain access to bank accounts and execute illegitimate financial transactions.
Mistake(s) / Vulnerabilitie(s):	Online newspaper websites have no control over the content delivered to them from third-parties.
Solution:	Website admins should be able to suppress third-party content in case of an emergency. Contact with ICT security officers of third-parties should be established quickly. Always use the latest version of your browser. Don't install/use insecure browser plugins, such as Adobe Flash Player.

4.3.4 DDoS extortion: first DD4BC, now Armada Collective **4.3.4.1 ProtonMail attack**	
Security Goal(s):	Availability: Perpetrators execute DDoS attacks on companies, whose business model relies heavily on website availability, and in the process disrupt normal service. The web server is unable to service other legitimate clients. Example: ProtonMail attack
Motivation:	Perpetrators execute DDoS attacks on website and extort money from the victims.
Mistake(s) / Vulnerabilitie(s):	DDoS attacks can hit every organisation. Some are unprepared, other are more or less prepared. The biggest mistake is to be completely unprepared. After suffering from daily attacks, ProtonMail assumed there was only one attacker and paid the ransom. However the attacks didn't stop. One should never pay the ransom, there is absolutely no guarantee the attack will stop.
Solution:	Measures to counter DDoS attacks include: - Knowing the "normal status" of your networks and systems. - The firewall should filter all unrequired protocols. - Having a firewall with big enough system resources that is able to cope with large amounts of packets in the event of a DDoS attack.

	- Using an IDS can detect abnormalities in the network traffic. - Consider IP geo-blocking, if your customer base is mainly from a given country or continental region.

5.2.1 Data leaks – Talk Talk	
Security Goal(s):	Confidentiality: Personal data of over 150'000 customers was stolen from a company that provides telephone, internet and television services.
Motivation:	The captured data is sold on underground markets. This data is especially used to design tailor-made scams for Talk Talk customers.
Mistake(s) / Vulnerabilitie(s):	Information systems of the company Talk Talk were compromised twice, in relative short interval. Personal data of customers wasn't stored securely (unencrypted). According to security experts the attack started with a SQL injection, but a DDoS attack was used in parallel as a smoke screen which allowed the attackers to compromise the system. The executives of the company didn't learn any lessons from the first attack.
Solution:	Personal data of customers should be encrypted.

5.3.1 Power cut in the Ukraine (industrial control systems)	
Security Goal(s):	Availability of utilities (energy provider and power grid). The goal was to disrupt the power grid in the Ukrainian region of Ivano-Frankivsk Oblast. A sophisticated attack was used to achieve this.
Motivation:	Create chaos (probably politically motivated)
Mistake(s) / Vulnerabilitie(s):	The attack on the power company occurred on several levels. The malware was identified as BlackEnergy (BE). However, BE could not be determined as the primary cause of the power cut. The computers were infected via e-mail attachments. The attackers scouted out the network with the help of BlackEnergy malware. Security experts assume that circuit breakers were being triggered from SCADA consoles.
Solution:	Think twice before opening an e-mail attachment. SCADA consoles and interfaces should never be reachable directly from the internet → place the SCADA systems in a segregated network zone. Only specific internal IP addresses should be granted access to the network. Use multi-staged malware protection.

5.3. The intelligent car – the responsibility of the car industry	
Security Goal(s):	Integrity: connect to the Uconnect system of a car from Fiat-Chrysler and taking over the control electronics.
Motivation:	Security researchers conducted this experiment to raise the awareness of car manufacturers. The researchers presented their findings at a Black hat conference.
Mistake(s) / Vulnerabilitie(s):	A vulnerability in the Uconnect system allowed the attackers to connect to it by only knowing the IP address of the system. Since Uconnect is connected to other control electronics of the car by CAN bus, the attackers were able to take control of these electronics.
Solution:	Entertainment and control electronics of cars must be strictly separated.