TAB OFFICE OF TECHNOLOGY ASSESSMENT AT THE GERMAN BUNDESTAG

Cybersecurity in the food supply

TAB-Fokus no. 47 regarding report no. 213 October 2024

Summary

- The digitisation and integration of technical systems increases the vulnerability of companies in the food chain to threats from cyberspace.
- In the agricultural sector, supply chain attacks on manufacturers of operating equipment or external service providers in particular might have an impact on the production and delivery of food.
- Compared to this, processing, logistics and retail have achieved a comparatively higher degree of digitisation and show a higher concentration. Without access to central IT systems, necessary services can often no longer be provided.
- With the transposition of the NIS 2 Directive into German law, external service providers, providers of critical IT technology and suppliers will be held accountable to a greater degree, the scope of application of cyber security obligations will be extended to medium-sized companies and the focus on supply chains will be strengthened. These measures should minimise the identified risks.
- In order to reduce the risk of cyber attacks on a large number of smaller companies and their service providers, measures should be implemented that enable them to better protect themselves against cyber attacks without unnecessarily increasing administrative burdens.
- Overall, the gaps in knowledge about the state of cyber security are large. The data situation with regard to the spread of digital technologies, incidents and protection levels needs to be improved.

What is involved

The digitisation and integration of technical systems increases the vulnerability of companies in the food chain to threats from cyberspace. In 2023, the threat to IT security was higher than ever before. The food sector (food production, processing and trade) is one of the critical infrastructures that require particular protection. With regard to information security, this is ensured by the BSI Act, which obliges large companies in the food sector to secure their IT systems according to the state of the art. However, the agriculture and food sector are heavily characterised by small and medium-sized enterprises (SMEs), to which the obligations of the German BSI Act have not been applied so far. With the implementation of Directive (EU) 2022/2555 (NIS 2 Directive), the food sector is also recognised as an important sector at the European level. Secondly, this directive no longer only obliges large operators of critical infrastructures, but also medium-sized companies to secure their systems against IT security incidents. The TAB working report examines the vulnerabilities of food supply in Germany with regard to potential threats from cyberspace and outlines options for action to strengthen the sector's cyber resilience.

Agricultural systems

Even if agriculture has not yet been the main target of sophisticated attacks on operating equipment, this might change due to the rapid digitisation of farms. Due to the high number of small and medium-sized farms in the agricultural sector, it can be virtually ruled out that attacks on individual farms would have an impact on the food supply as a whole. It would be much more likely that an attack on the manufacturers of the operating equipment used or on external service providers with high market penetration would impair the supply of agricultural products.

In livestock farming, this applies to IT service providers such as cloud hosting platforms that provide storage space, computing power and databases, as well as to providers of cloud-based systems. The failure of Internet or laboratory services

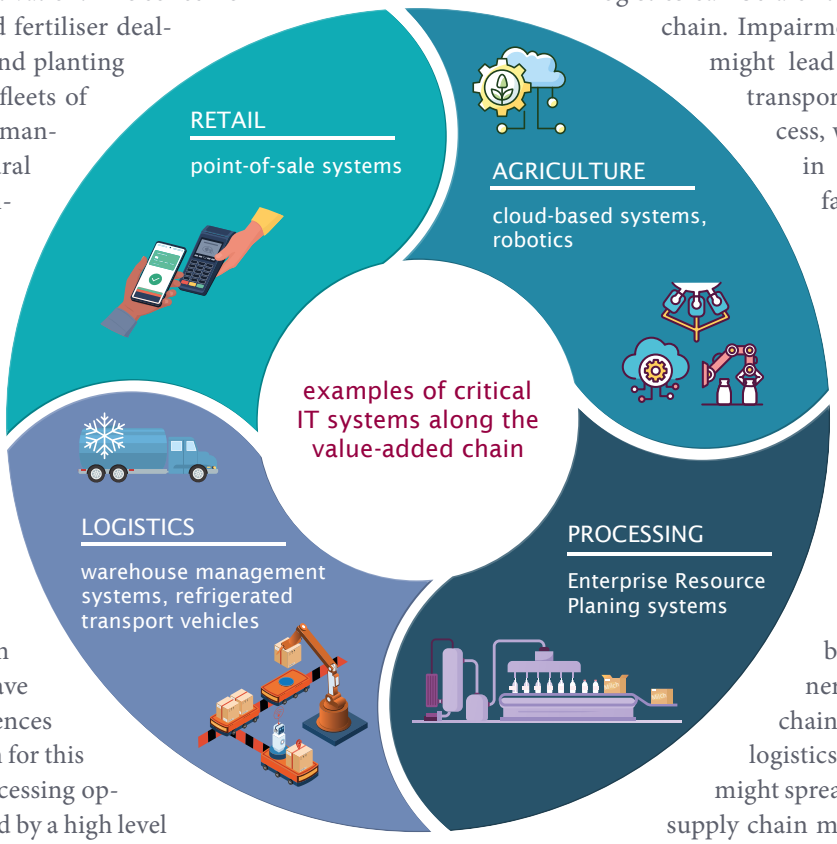
Client
Committee on Education, Research and Technology Assessment
+49 30 227-32861
bildungundforschung@bundestag.de

might have similar problematic implications. In addition to indirect attacks on service providers with a high market share, IT systems that are used as standard in livestock farming and have a high criticality can also be attacked directly. These include, for instance, barn ventilation and automatic milking systems in dairy farms.

Due to the lower perishability of the products, crop cultivation is generally characterised by a lower criticality. Nevertheless, attacks on the supply chain also bear a relevant risk potential in crop cultivation. This concerns e. g. attacks on seed and fertiliser dealers during the sowing and planting season. Attacks on the fleets of agricultural machinery manufacturers and agricultural machinery are also considered to be likely. If harvesting machines are not available in time, this might lead to a total loss for farms.

Food processing

Compared to a technical failure in agriculture, a technical failure in food processing can have far-reaching consequences more quickly. The reason for this is that many critical processing operations are characterised by a high level of dependency on IT systems – and increasingly also on Internet access. Without access to central systems, particularly to the Enterprise Resource Planning (ERP) system, the necessary services can often no longer be provided. The impact of production losses on food security depends in particular on the perishability of the products affected and the number of people to be supplied. Attacks on companies that act as central points of contact for products (e. g. a dairy that collects milk from many milk producers) pose a particular threat to security of supply. A high market concentration is an indicator for potential weak links.



Logistics

Attacks on IT systems that support logistic processes are categorised as particularly serious. This is due to the fact that logistics can be a critical point in the supply chain. Impairments to logistic systems might lead to disruptions in the transport and management process, which in turn can result in supply shortages. The failure of central control systems – such as Enterprise Resource Planning systems or warehouse management systems – is particularly critical, as a result of which orders in the logistics warehouse (fig.), for example, can no longer be processed. The networking of systems between trading partners along the value-added chain also bears new risks for logistics companies, as incidents might spread to partners within the supply chain more quickly than in the past due to one supplier having taken weak cyber security measures. In this respect, increasing access to cloud services for the storage of data between trading partners is seen as particularly problematic. The issue that disruptions might have far-reaching consequences is also due to the fact that many logistic processes are coordinated to ensure that goods are available with the exact quantity and

Typical gateways for large-scale cyber attacks

The most common and most dangerous types of attack include ransomware, phishing and (D)DoS attacks.

- Ransomware: Ransomware is understood to be the manipulation, destruction or encryption of data – combined with a request to pay a ransom. To do this, malware is infiltrated into an IT system. Infection can occur via an e-mail, a website, a storage medium or a mobile device which is integrated into the company network. As soon as access to data and systems is blocked – for example via cryptographic encryption – the user is asked to pay the ransom, usually using cryptocurrency payment methods that are difficult to trace.
- Phishing: Phishing involves faking a person‹s identity with the aim of obtaining confidential information (e. g. passwords, credit card numbers) or persuading a person to

Illustration: morepiixel, bsd studio, Sergii Pavlovskyi, Sarawut, Siberian Art, elenabsl (all Adobe Stock)

at the right place at the right time in order to maintain the production process without any delays or overstocking. This is why disruptions are difficult to mitigate. Attacks on refrigeration systems (refrigerated transport vehicles and warehouses) also have a high probability of occurrence and a potentially major impact, as the products would perish quickly. Potential gateways might be, for example, telemetry (telematics systems) in refrigerated vehicles or remote maintenance of refrigerated warehouses.

Fig. Warehouse system of the Ocado Group for e-commerce

Food retail

Besides logistics, the retail sector is an attractive target for cybercriminals due to the extensive processing of sensitive customer and business data. Ransomware represents the greatest threat in food retail as well – particularly via the phishing attack vector, which can result in breaches of data protection. As a rule, the availability of core services remains unaffected even in the event of data protection breaches. Among the attacks that can take place against IT systems in the retail sector, those against central management systems and digital point-of-sale (POS) systems currently pose the greatest threat to the retail sector. In principle, such incidents can make access to food more difficult. So far, the consequences of individual disruptions have been mitigated by the dense supermarket network in Germany. But due to the high concentration of food retailers in Germany, there is a risk of homogenisation of the systems used – which might make scaled attacks via software updates dangerous. An indirect attack on an external IT service provider can prove even more problematic if the majority of retail outlets access the same service. Besides services for monitoring and controlling IT networks or software for card payment terminals, the growing use of cloud-based applications – which present a new potential target for hackers thanks to their connection to the Internet – might also entail an increased vulnerability.

Attacks by cybercriminals pose a particularly great threat to businesses involved in e-commerce, as their activities rely on web servers and logistics automation. A failure of these systems represents a threat to the availability of the core services they deliver. Yet, despite the devastating impact on individual companies, a failure of their online business is generally not a serious problem for the security of food supply as a whole, as e-commerce only has a relatively small market share so far and is not the primary sales channel for most food retailers.

Options for action

Critical services are crucial for the functioning of our society and should therefore be protected to a high degree. However, security measures may entail high costs. It is therefore necessary to identify the greatest threats against which appropriate protection measures should be taken. In order to secure the food supply, it is important to guarantee the supply of energy

transfer money. This is done, for example, by enticing the victim to click a fake link. If the sender's IP, name or address are falsified in such a way that a recipient believes them to be trustworthy, this is known as spoofing. Company services can also be faked (e. g. Amazon, DHL) and even your own superiors (CEO fraud).

› Denial-of-service (DoS) attacks: A DoS attack is the sending of mass requests to a system, which then comes to a standstill due to overload. This blocks access to the company‹s internal or external systems (e. g. customer platform). If mass requests are sent from various distributed, compromised computers, they are referred to as distributed DoS (DDoS) attacks. Prevention and containment of (D)DoS attacks represent a major challenge for companies.

Fig.: Rodríguez García, M.; Agmoni, E. (2024): The Warehouse of the Future: Toward Highly Automated, Interconnected, Sustainable Warehouses. MIT Center for Transportation & Logistics

or electricity, water for crop cultivation and livestock farming as well as a functioning information and communication technology (ICT) infrastructure. Moreover, an attack on IT systems might have far-reaching consequences, in particular if:

- the IT system is used as standard in a large number of companies or to provide an externally commissioned service;
- the IT system or service has a high criticality, i. e. it fulfils a central and almost irreplaceable function in the operations of the company;
- the system is only offered by few manufacturers;
- the system influences the perishability of goods.

The high diversity of products and companies in the food sector ensured that the failure of a supplier or company did not have any serious consequences for the supply of the population in most cases. This is why operators of large critical systems above a legally defined threshold have so far been obliged to protect their IT systems and networks against cyber attacks. Against the background of increasing risks due to the networking and integration of systems and data both within individual companies and along the value-added chain, as well as of having opportunities to carry out attacks on a large number of smaller companies or through supply chain attacks more easily using Artificial Intelligence (AI), it makes sense to lower the thresholds and focus more strongly on supply chains. In 2022, the NIS 2 Directive was published. Its implementation in Germany (currently going through the legislative procedure) will increase the sector's cyber security. Overall, a higher level of cyber security in the food supply sector requires external service providers and suppliers of critical IT technology to be made more aware of their responsibilities. Smaller companies need to be motivated to improve their cyber security and knowledge about the prevalence of IT systems, incidents and protection levels in the industry sector as well as the risks due to new technologies needs to be improved. Measures to reduce the shortage of IT specialists and to raise awareness of cyber risks also appear to be of particular importance.

TAB report no. 213
Cybersicherheit in der Nahrungsmittelversorgung
Pauline Riousset

Website of the project
www.tab-beim-bundestag.de/en/cybersecurity-food

Project manager and contact
Dr. Pauline Riousset
+49 30 28491-105
riousset@tab-beim-bundestag.de

The Office of Technology Assessment at the German Bundestag (TAB) advises the German Bundestag and its committees on questions of scientific and technological change. TAB has been operated by the Institute for Technology Assessment and Systems Analysis (ITAS) of the Karlsruhe Institute of Technology (KIT) since 1990. It has been cooperating with the IZT – Institute for Futures Studies and Technology Assessment and VDI/VDE Innovation + Technik GmbH since September 2013. The Committee for Education, Research and Technology Assessment decides on TAB's work programme, which also includes subjects proposed by other parliamentary committees. The standing »TA Rapporteur Group« consists of the Chairman of the Committee Kai Gehring (Bündnis 90/Die Grünen), and one member from each of the parliamentary parties: Dr. Holger Becker (SPD), Lars Rohwer (CDU/CSU), Laura Kraft (Bündnis 90/Die Grünen), Prof. Dr. Stephan Seiter (FDP), Prof. Dr. Michael Kaufmann (AfD).