Expert interview

Cybersecurity is an important issue for the pharmaceutical industry

In an increasingly interconnected world, the pharmaceutical and biotechnology sectors need to be aware of cybersecurity threats in manufacturing. We talked about these threats with Holger Mettler (54) who is in charge of computer system validation and cybersecurity at Exyte (formerly M + W), a global enterprise that designs, engineers and constructs complex manufacturing facilities and buildings for the life sciences industry. The Exyte Group has a global workforce of 5,000 people. Mettler has studied communications technology, bionics and computer science.

Holger Mettler, cybersecurity expert. © exyte

Has the increased networking of machines and people now arrived in the pharmaceutical industry?

Yes, it has. Many companies, especially those that need to invest in their existing facilities and machinery, know that their suppliers rely heavily on digitized and IT-based systems. The industry increasingly favours the concept of paperless production but unfortunately, some manufacturers still rely heavily on paper. In my opinion, digitized and IT-based systems have not yet really entered pharmaceutical manufacturing.

Do IT networks in pharmaceutical manufacturing facilities make cybersecurity more important?

Definitely. Pharmaceutical companies' manufacturing plants play an absolutely critical role in the manufacturing process as a whole. First and foremost, the plants must be safe operationally, something that is achieved by traditional mechatronics, which is a combination of mechanics, electronics and computing. IT and cybersecurity are not just about a single plant, but encompass an entire cyberspace in which packaging, filling or media supply systems are interconnected and share data with each other. Nowadays, pharmaceutical data are stored in distributed data centres, i.e. cloud data centres, rather than on a single computer. If internet or intranet are connected in some way with the manufacturing process, then IT and cybersecurity threats will also affect the manufacturing processes.

Pharmaceutical manufacturing is highly regulated. Is that also true for IT security or are there gaps?

Data integrity has become a very important regulatory issue, alongside patient safety and product quality, especially as analog processes are increasingly being replaced with digital ones. The manipulation of operational and IT systems has had unwanted outcomes. Products have even had to be removed from the market. Analysis and manufacturing results have been electronically falsified, which is why inspectors tend to put the emphasis on data integrity, especially as far as analytics is concerned, where cyberthreats can lead to the greatest problems. Similar threats have since started to affect drug manufacturing companies where access to computer systems is sometimes easy due to frequent lack of protection against cyberattacks. Some computer systems are outdated and can easily become infected with viruses or Trojans.

Is the pharmaceutical industry the target of cyberattacks?

Yes, cyberattacks on the pharmaceutical industry have been common for some time. If cybercriminals are able to access R&D and manufacturing data, companies whose data have been stolen or compromised risk becoming the target of blackmail. It came as quite a surprise that the WannaCry virus spread not only to the office computers of pharmaceutical companies but also rapidly across their manufacturing computers. Some

of the affected companies experienced disruptions and even manufacturing downtimes lasting several days.

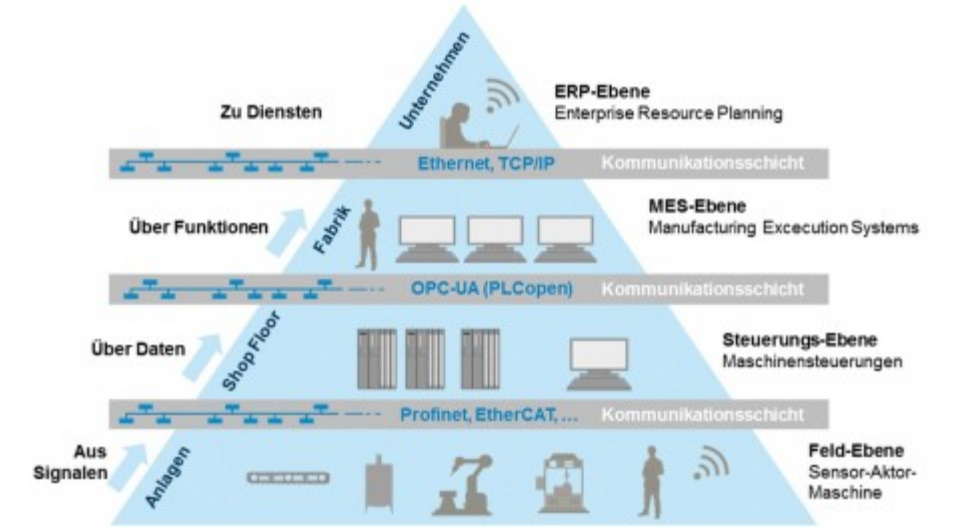
In order to understand why cyberattacks pose such a major threat, it is important to know that so-called industrial control systems (ICS) which manage GMP-based drug manufacturing processes lie at the heart of pharmaceutical manufacturing facilities. While old systems are often still autonomous, modern systems increasingly consist of automated systems that communicate with each other.

The remote monitoring and maintenance of IT systems services used by drug manufacturing companies can also represent a security loophole. When maintenance service providers install remote IT tools on a company's computers, they gain direct access to a network which, although it may be well secured, is nevertheless exposed to potential attacks as the person carrying out the maintenance is anonymous. Remote monitoring and maintenance providers use cloud solutions from IT service providers that operate computing centres. As far as GMP (good manufacturing practice) is concerned, relying on external service providers can be fatal as GMP requires any critical activity to be traceable. Data are, however, shared with somebody outside the company when a system is monitored externally. The example of Stuxnet, a computer worm that targets ICS, has shown that it is possible to destroy an industrial control system through infection with a shared printer.

Does an IT security system have to involve all systems or can it be limited to parts of a plant?

There are different IT and cybersecurity approaches, which, when combined, come close to a holistic approach. Technically, this can be measures such as virus protection or a firewall, organizationally, it may be an identity management system that severely restricts access to certain equipment, as required by GMP, procedurally, it could be through a holistic information security management system, for which certain norms and standards exist. ISO 27001 is one of the most widely used standards, and the BSI (ed. note: German Federal Office for Information Security) has its own standard called IT-Grundschutz that helps companies achieve an appropriate security level for all types of information by assessing the security status of a particular infrastructure. This is a complex process and can be certified.

How can existing pharmaceutical facilities be protected against cyberattacks? What do new plants need to be equipped with?



The graphic shows the different processes of automated pharmaceutical manufacturing and how the different levels and nodes of the drug manufacturing process need to be protected against cyberattacks. © exyte

From the perspective of good manufacturing practice and IT security, manufacturing parameters are critical process steps that can impact drug quality. Protective shells have to be built around them. Traditional facilities that are not yet connected to the internet are built on trust. However, this is very dangerous as hierarchies that regulate data access are needed. Critical data such as those related to drug formulas should only be modified by trained personnel and in compliance with quality assurance and control. It is a similar situation as far as IT is concerned where it is always necessary to find out which security standards need to be applied at which level.

The industry has developed a new standard for ICS security (ICE 62443), which aims to protect the cyberenvironment and encrypted data of an organization. Another standard is the ISO 27001 concept for information security management. It can also be transferred to pharmaceutical manufacturing. Unfortunately, this has not yet been fullyimplemented in the industry.

It is important to understand that technical tools such as virus protection software are unsuitable for manufacturing systems, because machines operate over long periods and anti-virus software that runs in the background could cause the manufacturing process to shut down. It is therefore necessary to restrict access to the manufacturing systems as much as possible.

Is there any official monitoring of IT security standards in pharmaceutical manufacturing?

In 2017, the provision of pharmaceuticals, and thus parts of the pharmaceutical industry, became part of what is regarded as a critical infrastructure. This concerns between 120 and 150 companies in Germany. The Act to Strengthen the Security of Federal Information

Technology (BSIG) states that critical infrastructure operators must protect their critical IT systems against availability, confidentiality, authenticity and integrity disruptions. In addition, they must provide the BSI with a contact point and report significant IT disruptions. Pharmaceutical manufacturers with a critical infrastructure are currently also developing an industry-specific standard in cooperation with the BSI.

Actually, data integrity is an old concept and part of GMP regulations. But what is new is that lawmakers require companies to take action and demonstrate what they are doing to implement IT security. This is a certified process. While the provision of an ISO 27001 certificate is not yet mandatory, organizations still have to prove that they have established an analog information security management model ensuring a product's quality and public safety.

Does this mean that pharmaceutical companies at which the new legislation is aimed will be facing even greater challenges than at present?

Yes, the number of challenges companies will have to deal with will increase with the growing number of inspections, where data integrity is always a major concern. The FDA has repeatedly noted data integrity infringements, and has also sent warning letters to German companies that have failed to appropriately document the safety of new drugs. Data and information security are in principle nearly the same as data integrity in the sense that companies must be able to demonstrate at certain points in the manufacturing process that data have not been manipulated. The future goal must be to merge IT security and GMP requirements, as this would also help as far as costs are concerned.

References:

Regulation on the amendment of the BSI Kritis regulation, 21st June 2017, amended by KRITIS health: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1903.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1903.pdf%27%5D__1543301401959

Initiative on the comprehensive interconnection with pharmaceutical manufacturing: https://ispe.org/initiatives/pharma-4.0#