MARKET SNAPSHOT: AUSTRIA

CYBERSECURITY INCIDENTS – DO'S AND DON'TS IN PRACTICE

By Axel Anderl, Managing Partner, and Nino Tlapak, Partner, Dorda

Over the last years and especially during the high peak of the COVID-19 pandemic, the risk of being subject to harmful and systematic cyberattacks has massively increased. Although the aim of cybercriminals – to extort money – is still unchanged, their methods and targets have been developed in line with the overall increase of digitalization. In contrast to industries with a focus on sensitive data and trade secrets, such as pharmaceuticals, banks, or insurance companies, industrial companies have not focused on preventive measures against potential cyberattacks in the past. Nowadays, however, production machines are linked to each other via a network and are therefore threatened to the same extent.

Worst-Case Scenario: Standstill Overnight

As regards methods, the risk exposure has changed due to the increase of ransomware attacks. In such a scenario, the attacker successfully penetrates the system and encrypts and/or deletes all data. In return for a ransom, which is usually paid in Bitcoin, the attacker offers to decrypt and release the data. During the refurbishment by IT professionals, it often turns out that the attackers were already in the system for a long period of time without being discovered. Triggers are often minor negligence, such as missing updates or patches that would cover already known vulnerabilities and thus allow access, or even an employee clicking on a compromised link.

Upon that, attackers continuously work their way through the system in search of information and admin access rights. The shutdown then regularly occurs at night or the beginning of the weekend to further increase the pressure on the target. This regularly involves shutting down all production and communication systems, encrypting and deleting all data in the company, and then demanding a ransom. Whether, up to what amount, and under which legal conditions this can and should be paid then needs to be decided on a case by case basis. Sometimes data can be restored via a backup or significant parts of production can be restarted autonomously. This mainly depends on which crisis and recovery method takes effect in the event of an incident.

How To Prepare for Such a Crisis Situation?

In the event of an incident, very tight deadlines apply due to the pressure of the attackers and legal obligations. In order to be able to react promptly, adequate preventive measures have to be in place. Therefore, it is necessary to clarify responsibilities and processes in advance in a defined crisis plan. In practice, preparation is also primarily about procedural, strategic, and legal details: who must be contacted and when to ensure coverage by cyber insurances as well as compliance with legally required notification duties (e.g., data breach notification according to GDPR)? What are the setup, awareness, and status quo of training of the responsible crisis team? What should and may be communicated to customers, colleagues, or even the press in the case of inquiries and when? What information is the target allowed to provide and what should be withheld? Answers to those questions shall make sure to set the course at the right time, both internally via legal, compliance, and IT departments, as well as via external experts – from IT forensic professionals to crisis PR assistance.

Successful defense and prevention measures start with simple things like the correct handling of private and professional passwords and end with the implementation of complex IT security and warning systems by the company.

What To Do in a Worst-Case Scenario?

In addition to evaluating the extent of the damage and refurbishing IT systems, complying with the applicable legal requirements and deadlines is of utmost importance in order to prevent claims for damages, penalties, and damages to reputation. First and foremost, the data protection authority must be informed within 72 hours – but depending on the industry, other authorities may also need to be involved in due time. In addition, communication with the insurance company and law enforcement authorities is also important. Ultimately, preventive measures must also cover an overall strategic decision whether a ransom can be paid at all (or whether this may be punishable by law) and what considerations and evidence are required.

For all areas, and especially the question of (personal) liability, the following applies: clean documentation and ongoing coordination with experts are the keys to success. ■