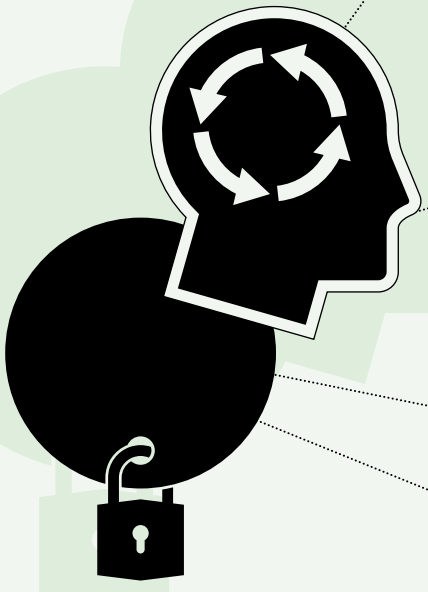
TIPS & TRICKS

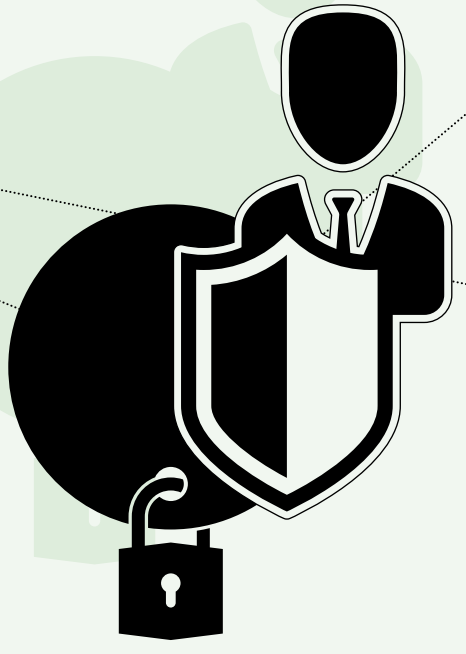
FULLY COVERED

Everyone's talking about digitization, but what about security? Customers are increasingly reporting cyber attacks involving job data losses or even production stoppages. The excuse that "we aren't interesting enough to be attacked" doesn't count – everyone is a potential victim if they don't follow these simple rules.



TEAR DOWN THE FIREWALL IN THE MIND

Small print shops in particular risk lulling themselves into a false sense of security if they think they don't have anything worth taking. Personal data such as bank details and address information is always useful for hackers, and there is no shortage of it at any print shop. Most attacks are also automated and look for the weakest link in the chain. Raising employee awareness is thus the top priority and the first step toward data security.



TAKE RESPONSIBILITY

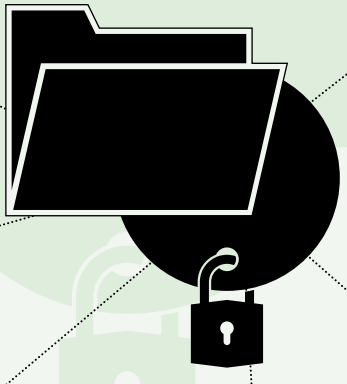
If no one's in charge, any steps taken will come to nothing. So appoint a security officer who documents the devices and software used, the purpose for which they are used and the employees who use them. The officer uses this information to draw up security guidelines and measures for how to eliminate risks. The guidelines also document how to comply with contractual obligations. If management then also demonstrates its commitment to data security, this closes the gaps for hackers.

The Heidelberg white paper on IT security at print shops:

www.heidelberg.com/IT-Security-whitepaper

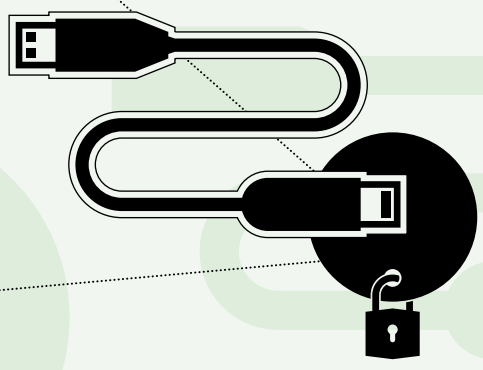
DUAL APPROACH

Sensitive data needs to be encrypted. This simple principle applies both to storing and sending information. And if data is lost and there's no backup, you only have yourself to blame. Daily back-up copies on external storage media protect against data loss in the event of the company network being infected with ransomware, for example.



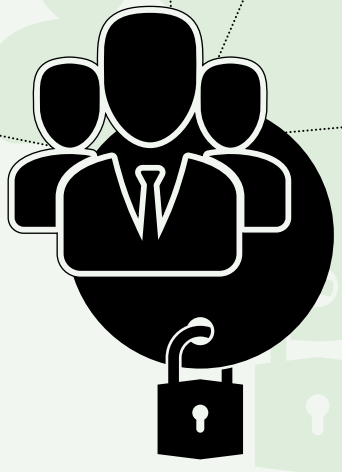
USE THE RIGHT MATERIAL

Outdated software offers hackers numerous opportunities. This is also true of programs that are not used at all, such as applications installed by the manufacturer. Unnecessary software should therefore be removed, and required programs always kept up-to-date. Use different passwords for each application and device. These should be at least eight characters long, consist of numerals, letters and special characters, and be changed at regular intervals. Names, dates of birth and number sequences such as 123456 must not be used. Up-to-date virus protection should be standard for all devices, including mobile computers that may be used in employees' home offices.



RESIST TEMPTATION

As well as security risks, online services such as Dropbox may also present compliance problems. It is rarely clear which data center or jurisdiction files end up in. What's more, many print shops still use the FTP transfer protocol. Yet simplicity has its price, as FTP sends data unencrypted, and hackers may be able to pick up passwords and use them for attacks. Extended versions such as SFTP and FTPS that offer more security when sending data should therefore be used at the very least.



PLAY YOUR PART

In many cases, if employees act carelessly, for example by opening email attachments without knowing the sender, this sets off an avalanche in which they feed viruses, Trojans or so called ransomware – as seen recently with WannaCry – into the company network. To minimize the risk, they should only be given access rights to the data, networks and software they need for their work. Administrator rights are so named for good reason – they are reserved for administrators. This prevents unrestricted access by malware to the entire system.

FACTS AND FIGURES

No fewer than **53 percent** of German companies have fallen victim to sabotage, espionage or data theft. *Source: Survey by the German Federal Intelligence Agency*

In May, **WannaCry ransomware** crippled hundreds of thousands of computer systems in more than 150 countries in just a few hours. The hackers used a security loophole in Microsoft's Windows operating system. Only equipment without the latest updates were hit. *Source: Süddeutsche Zeitung newspaper*

Ransomware **netted criminals** more than 1 billion U.S. dollars (848 million euros) last year and yet the software enabling attacks of this kind is available online for as little as 28 dollars. *Source: Frankfurter Allgemeine Zeitung newspaper*