FIS-ASP®

REPORT

CARELESSNESS FACILITATES CYBER ATTACKS

PHISHING ATTACKS ARE AMONG THE MAJOR THREATS TO IT SECURITY. HOW SMALL AND MEDIUM-SIZED ENTERPRISES CAN FACE THIS PROBLEM.

Large-scale attacks on corporate groups, authorities and institutions are no longer a rarity, but have almost become an everyday occurrence. The corona crisis has even increased this effect. According to a report published by the European Union Agency for Cybersecurity on October 20, 2020, attacks via mailboxes already caused losses amounting to approximately 26.2 billion Euro in 2019. 42.8 percent of all malicious attachments could be attributed to widely used Microsoft Office documents. According to ENISA, phishing attacks increased by 667 percent within a single month at the beginning of the pandemic (between the end of February 2020 and the end of March 2020).

Surveys support these assertions: According to Capterra, a rating platform for business software, decision-makers from small and medium-sized enterprises consider e-mail phishing as the greatest threat. Due to partially insufficient safety measures and their roles as suppliers or vendors for large companies, small and medium-sized enterprises have become interesting targets for attackers. As a consequence, they face the challenge of reaching a high safety level with limited financial resources (compared to large corporations).

LOW INHIBITION THRESHOLDS FOR INTERACTION

Phishing attacks are particularly popular among cybercriminals. By tricking, deceiving or misleading their victims, they try to obtain confidential and sensitive data. This type of attack is classified by the term “social engineering”. In addition to attacks via e-mail, it also comprises so-called USB drop attacks, fake text messages via SMS or fake telephone calls.

In e-mail correspondence, mails contain malicious attachments or links to “fake” sites. Winnings or inheritances are promised, but such attacks may also appear as serious offers placed by known vendors or customers, so that the inhibition threshold for interaction is as low as possible for potential victims. Sometimes, specific user groups or business positions are targeted systematically to obtain particular authorizations or identities.

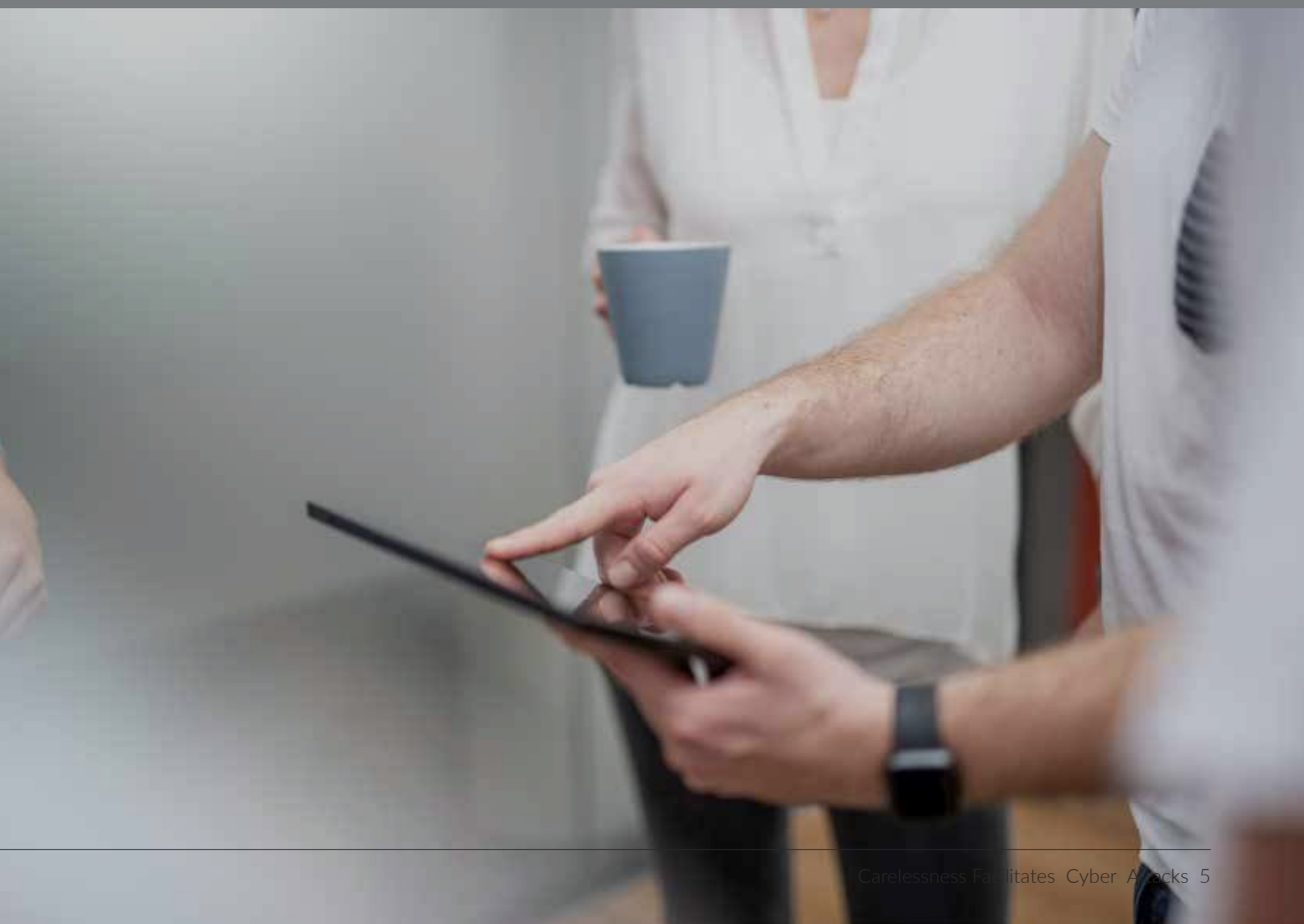
After all, the human factor is the decisive point. If employees do not scrutinize e-mail addressees or contents as a supposedly “last line of defense”, but interact with them, the attack has already been successful. The data obtained by so-called “sniffing” can now be read by the attacker and used for other criminal activities. In worst cases, logon data is captured, which enables the attacker to access other company data and subsequently even delete, encrypt or offer it in the darknet.

FINANCIAL AND REPUTATIONAL DAMAGES

In case of encryptions, the used encryption technique usually cannot be decoded easily to regain access to the data. Enterprises that have not secured their data by regularly carried out backups should nonetheless pay the demanded ransom by no means, but instead seek advise from experts on how to handle this situation. The reason is that it is questionable whether the systems are decoded at all after the ransom has been paid.

Eventually, such attacks may involve enormous financial and reputational damages for enterprises. Loss of customer confidence, costs for know-how loss and elimination of consequential damages, production losses or order cancelations represent only a small overview of possible consequences that may arise from successful cyber attacks. Furthermore, such data mishaps must immediately be reported to the responsible supervisory authority.

Cyber criminals will continue to rely on phishing attacks in the future since the technical security of numerous systems that is already available reduces their attacking possibilities and, as a consequence, human beings can meanwhile be considered as the weakest links in the chain. Moreover, such attacks can be carried out with considerably less know-how and on a larger scale than classic hacker attacks. In the end, the rate of success is decisive as well: Irrespective of the company size, one distracted or careless employee is enough to cause serious impacts for their enterprise. Out of 1,000 employees, only one person (0.01%) needs to interact with the phishing mail to be “at the mercy” of the attackers. There is hardly any other attack scenario with such probability of success that is underestimated to such an extent - particularly in the area of small and medium-sized enterprises, where means and resources for IT security are frequently limited and no sufficient know-how is available.



SIMPLE COUNTERACTIVE MEASURES DO NOT NEED TO BE EXPENSIVE

The decisive keyword is “awareness”. Repetitive and well-coordinated sensibility measures of employees are the key to “steal the thunder” from these phishing attackers, because without human interaction with the compromised mails, there is usually no increased danger - provided that the enterprise’s technical measures correspond to a specific safety level. Furthermore, awareness training courses are extremely cost-effective compared to the recovery costs after a cyber attack. However, this type of sensitization must take place regularly and always has to be adjusted to the current security situation.

FAKE HYGIENE INSTRUCTIONS AGAINST THE CORONAVIRUS

Internal phishing tests should also be an essential component for reviewing the measures. Here, fake phishing mails can be sent to employees in order to test and assess their reactions. Cyber criminals rapidly find new ways and possibilities of modifying their attacks and adjusting them to current circumstances. A good example of such an adjustment to current conditions is the sudden increase of such mails at the beginning of the pandemic with contents such as “corona rules of conduct”. These mails were sent under the guise of authorities and organizations to draw attention to the current hygiene rules in the working world. They alone were responsible for two percent of all phishing attacks in February/March 2020 (see report published by the European Union Agency for Cybersecurity). The technical term for such attacks under a pretext is called “e-mail spoofing”. If corporate communications are transparent and employees trained and forewarned, the risk of not recognizing such attacks as criminal acts will significantly decrease.

FIS-ASP Application Service Providing
und IT-Outsourcing GmbH
Röthleiner Weg 4
D-97506 Grafenrheinfeld
www.fis-asp.de