Specialist Article

Phishing as a gateway for cyber attacks

How companies can raise awareness among their teams

Companies, authorities and institutions are increasingly confronted with cyber attacks. One gateway is phishing e-mails that pretend to have a relationship of trust with the recipient. A link is quickly clicked on, ransomware or other malware is downloaded unknowingly - the damage can be immense. Ransomware acts like an "encryption Trojan" by encoding data indissolubly for the user and only releasing it again against payment of a ransom. Since phishing exploits human weaknesses, it is very difficult to prevent with technical solutions. The key is education and training to sensitise employees to the attacks, raise scepticism and create awareness.

The number of cyber attacks is increasing: Companies, public authorities and municipalities are affected, but also healthcare facilities such as hospitals. In October 2021, the President of the Federal Office for Information Security (BSI), Arne Schönbohm, spoke of a "red alert" in some areas of information security. And the reports of successful attacks are increasing: In November 2021, the MediaMarkt electronics retail chain was affected by an extortion attempt with ransomware; servers and systems were compromised, which considerably disrupted operations in branches. According to a company spokesperson, the attack was targeted. In 2020, the Uniklinik Düsseldorf and the Funke Mediengruppe were victims: In the latter case, a phishing email served as a gateway for a ransomware attack.

Phishing is a so-called social engineering attack: it exploits the weaknesses and suspiciousness of humans. Phishing e-mails make the recipient believe that he or she is trustworthy or put him or her under pressure. This entices them to click on a link, initiate a process or disclose confidential information. Three types of phishing can be distinguished:

- In the case of so-called CEO fraud, the attackers pretend to have a high position within the attacked company in order to inspire trust on the one hand, and on the other hand to use the authority of the hierarchy gap and threatened consequences to entice their victim to transfer a large sum of money, for example. The attackers often take a targeted approach and invest a great deal of time in selecting the company and the appropriate recipients. They often have a foot in the door and know how communication works in the target company.

- The same applies to the spear phishing variant: these mails are specifically tailored to the victim or to a certain victim group. The individualisation makes it very difficult to recognise such a mail as phishing. Spear phishing is often the initial attack vector to infiltrate malware into a company.
- Classic phishing often aims to obtain victims' access data to systems and services. However, these emails are not tailored to individuals or groups of people, but are sent to a broad mass. It can also happen that a recipient does not use the service addressed in the e-mail.

Phishing is a constant danger

The danger should not be underestimated, as phishing e-mails are written with sophistication. They no longer have per se strange and dubious email addresses of the sender or spelling and grammatical errors. In addition, the range of addressees is extremely broad: All employees who communicate with external parties via email are potential victims. Companies are usually affected by CEO fraud or spear phishing and thus by targeted campaigns. It has been shown that phishing attempts are particularly frequent among those addressees whose names and email addresses are publicly listed, for example on the company's website - usually they have less pronounced know-how on the subject of malware compared to members of IT departments. This means that it is often precisely those employees who are less sensitive to malware who are targeted by attackers. This makes it more likely that they will click on a link or download a contaminated attachment.

The danger for private individuals is that personal and sensitive data may be tapped. Malware can also be smuggled in via phishing e-mails, so that the attacker secures permanent system access unnoticed. He moves invisibly in the network and thus gains access to the sensitive data.

In companies, phishing e-mails are a frequent gateway for malware such as ransomware. The attackers can gain control of computers, steal victims' identities and thus carry out further attacks. The victim can also be extorted for a ransom with sensitive data. These attacks are very costly for companies: they result in long IT downtimes, hinder or prevent business and damage reputation. If malware is smuggled in, industrial espionage can also take place via phishing.

Prevent phishing with simulations

Since phishing is a psychological weapon and targets human behaviour, it is difficult to ward it off on a technological level: Spam filters only recognise the e-mails inadequately and thus they usually reach the intended recipient. Using the example of a human resources department, it

is possible for them to receive applications via a portal and thus bypass the gateway via e-mail.

Therefore, one effective method of phishing defence consists of training and sensitising employees. Simulations and regular campaigns can be used to raise awareness, e.g. with regard to possible entry points, and thus minimise the risk of an attack.

Employees are specifically confronted with the danger of phishing under real but controlled conditions. Simulations of spear phishing, for example, familiarise them with the tricks of the attackers without causing any damage. In such a campaign, phishing e-mails are sent out in a company over several hours or days, to all or to individual persons, groups of persons or departments. The company decides whether or not the employees are informed of this or of the duration.

If a recipient now opens one of the campaign mails or even clicks on the link, his or her behaviour is stored anonymously in a database. This is made possible by user-specific links in the mails. Over the agreed period of the campaign, a perma-nent evaluation is carried out, and at the end, the results are summarised and processed. This makes it possible to see which areas or departments are particularly susceptible to phishing e-mails. Countermeasures can then be taken with training and education.

Communication is of central importance here: it is not about assigning blame, but it must be clear that the simulations are used to build up know-how and that it is a learning scenario. It is also possible to educate employees about the phishing simulation directly after they have clicked on a link or to keep them in the dark at first. The latter is a good idea, as otherwise it is easy for word to get around in companies that a simulation is underway, which can falsify the results.

Promote scepticism and awareness with trainings

In follow-up trainings, processes can be established to promote awareness and maintain scepticism. Sometimes the name of the boss in an email is enough to prompt immediate action - even without thinking. Employees are therefore provided with features to make it easier to recognise whether an email is valid, for example whether the sender's name and provider match. But it is also important to establish a culture of scepticism, i.e. to ask questions, even if an e-mail from a supposed superior is accompanied by an immediate request for action.

It makes sense for employees to take part in a phishing simulation at regular intervals, e.g. once a quarter or once every six months, depending on the company, in order to achieve the greatest effect, to keep the training level high and to develop a gut feeling for phishing emails.

In doing so, the width of the spread can vary and gateways can be trained again directly with customised campaigns.

Conclusion

Threat scenarios through cyber attacks are expanding, more and more companies are affected by ransomware attacks that hinder operations and cause immense costs. The gateway is often phishing emails, through which the attackers gain access to systems and sensitive data and can thus blackmail companies. This worst-case scenario can be prevented by sensitising employees through targeted phishing simulations and training.

Authors:

Leon Hormel, Cyber Defense Consultant

SECUINFRA Falcon Team

Tobias Messinger, Senior Cyber Defense Consultant

SECUINFRA Falcon Team

Further information: https://www.secuinfra.com/de/news/digitale-bedrohung-phishing/

Press Contact:

SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Mobile: +49 160 921 633 44

marketing@secuinfra.com