IT Security Management

Phishing-Simulation

Cybercriminals do not limit their attacks to a company's IT infrastructure. They also target employees to obtain sensitive information, gain unauthorised access, or trick them into inadvertently executing malicious code. These attacks, commonly referred to as social engineering, are among the leading causes of successful security breaches.

In its report The State of IT Security in Germany, the German Federal Office for Information Security (BSI) continues to classify the threat posed by such attacks as significant. Phishing remains a widespread attack vector, primarily aimed at stealing sensitive information and compromising user accounts.

Our Approach

With phishing.42, we simulate realistic email-based phishing attacks targeting all or selected employees within your organisation. Our goal is to assess and strengthen employees' ability to recognise fraudulent emails, malicious links, and potential malware threats.

The results identify specific security awareness gaps and provide a solid foundation for targeted training and awareness measures. phishing.42 can also be integrated into your organisation's broader information security awareness programme.

Methodology

1. **Planning & Design** – At the beginning of the project, we work with you to define the objectives, scope, and execution of the phishing simulation. Typically, we conduct two different attack scenarios at intervals of four to eight weeks.

   To prepare the simulation, you provide us with the email addresses of the participating employees. Optionally, these can be assigned to specific organisational units to enable a more detailed analysis of the results.

2. **Creation of Simulated Websites** – For the phishing simulation, we set up realistic websites hosted in plan42's data centre. Depending on the attack scenario, these may imitate voucher offers, information portals, or log-in pages for internal and external business applications. This allows us to assess how employees respond to seemingly trustworthy websites.

3. **Sending Simulated Phishing Emails** – Selected employees receive a simulated phishing email that, depending on the scenario, may invite them to claim a voucher or enter their login credentials on a specially prepared website.

   We tailor the difficulty level to your specific requirements. Scenarios range from easily recognisable phishing emails containing typical warning signs to professionally crafted messages with spoofed sender addresses that are difficult to identify as fraudulent.

4. **Final Analysis** – Each simulated phishing email contains a unique tracking link, allowing us to identify which recipients click on links or enter information on the simulated phishing websites. Depending on your requirements, the results can be evaluated anonymously, individually, or by organisational unit.

   We apply strict technical and organisational security measures to protect the data entrusted to us. Upon completion of the project, all personal data is securely deleted in accordance with applicable data protection requirements.

plan42

plan42 is a consulting company specialising in IT Security, IT Service Management, and Business Solutions. From process analysis and consulting to solution design and implementation, plan42 combines technical expertise with proven, practical approaches.