Press release
SoSafe GmbH I Ehrenfeldguertel 76 I 50823 Cologne I Germany

One in three companies has experienced a successful cyberattack in the last year

SoSafe publishes “Human Risk Review 2022“: study about the European cyberthreat situation

Three findings stand out: (1) Nine out of ten cyber security executives say the cyberthreat environment has worsened. Supply chain attacks and ransomware in particular are becoming large-scale. Three out of four respondents add that remote work and hybrid work models have made the attack situation more acute. (2) Almost half of all users open phishing emails, and one in three click on malicious content contained therein. This means that opening and click rates have risen once again. Current political and social events are instrumentalized. (3) Risks can be reduced by up to 90 percent through systematic awareness measures.

Cologne, April 7, 2022: SoSafe, one of the fastest growing cyber security awareness providers worldwide, has published its "Human Risk Review 2022": "With the Human Risk Review we want to provide insights into current trends and developments in the European cyber threat landscape. Our goal is to further raise awareness of this topic – especially for the 'human factor' in information security," says Dr. Niklas Hellemann, Managing Director of SoSafe. Other sources also verify that this is important: A survey by Allianz Insurance[1] shows that cyber incidents are the number one business risk worldwide. At the RSA Conference 2021, Cisco CEO Chuck Robbins spoke of $6 trillion in damages per year[2]. The interface between man and machine remains the number one entry point – more than 85 percent of all attacks start with the human factor.[3]

While cybercriminals are becoming increasingly professionalized, the defending side must also position itself accordingly: "Employees need more than security guidelines. Employees can be activated as a 'human firewall' to sustainably reduce the security risk. To achieve this, a security culture must be established in companies that involves people and supports them in identifying cyberthreats and behaving safely," says Hellemann, a qualified psychologist. The Human Risk Review helps with this: It gives security managers recommendations for action to strengthen the security culture in companies holistically and sustainably. With the help of SoSafe's "Behavioral Security Model", organizations can significantly and effectively minimize human risks based on psychological approaches. SoSafe's data shows that systematic awareness measures reduce risks by up to 90 percent.

The Human Risk Review is based on various data sources: In addition to a survey conducted by SoSafe with 251 cyber security managers, exclusive response data from the SoSafe Awareness Platform (4.3 million simulated phishing attacks from 1500 organizations) and from the annual "Phish Test" study conducted by SoSafe and Botfrei on general phishing awareness (1350 users in

[1] Allianz (2022). Allianz Risk Barometer 2022: Cyber perils outrank Covid-19 and broken supply chains as top global business risk. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html
[2] SDX Central (2021). Cisco CEO: Cybercrime Damages Hit $6 Trillion. https://www.sdxcentral.com/articles/news/cisco-ceo-cybercrime-damages-hit-6-trillion/2021/05/
[3] Gartner Report (2021). Market Guide for Security Awareness Computer-Based Training.

2021 who received three phishing simulations in one week) were used. In addition, existing content and studies were analyzed, and interviews were conducted with other industry experts.

Aggravation and professionalization of cybercrime

Above all, the SoSafe survey shows that the cyberthreat situation has worsened. According to the survey, one in three organizations (35%) has experienced a successful cyberattack in the past year. Furthermore, nine out of ten (90%) cyber security experts confirmed the worsening situation in the survey. Cybercriminals have professionalized their attack tactics and business models. "Organizations face an innovative dark economy where cybercrime-as-a-service is the common business model. Tactics are evolving almost by the minute," Hellemann says. Two cybercrime trends are emerging: Large-scale supply chain attacks target weak links in supply chains and bring entire industries or utility systems to a standstill. In addition, the European Union Agency for Cybersecurity (ENISA) refers to the "golden era" for ransomware[4]. According to the report, complex attack tactics such as multiple extortions increase the risk of data misuse by 800 percent.

Nearly every third person clicks on malicious content in phishing emails

Phishing and social engineering remain perennial issues. Attacks evolve continuously and are adapted based on current political or social situations, such as in the war of aggression in Ukraine: "Within a very short time, social engineering attacks were circulating, exploiting people's willingness to help Ukraine," says Hellemann. SoSafe's data shows that these tactics work: Almost half of all users (45%) open phishing emails. Of those, nearly one in three (30%) click on links, attachments, or other malicious content contained therein. A steady trend can be seen when differentiating between groups of people: As in 2021, men click on phishing emails more often (29%) than women (20%) and younger people more often (18-49 years; 29%) than older people (over 50; 19%). 58 percent of users who clicked also interact with the content and, for example, enter personal data in fake login screens. This means that the opening, click, and interaction rates for phishing emails remain at a high level. Compared to the previous year, they have risen even further.

Hybrid work models still pose a challenge for companies

Three out of four respondents (75%) say that remote work and hybrid work models have exacerbated the attack situation. This is not surprising, as hybrid working models have brought with them new communication channels that open up additional entry routes for cyberattacks on companies by cybercriminals. They continue to rely increasingly on social engineering, because people can always be attacked with one common tactic: emotional manipulation. Psychologically based approaches therefore significantly and effectively help to minimize human risks in an organization. Therefore, 99 percent of respondents want to strengthen their organization's own security culture in the coming year.

[4] ENISA (2021). ENISA Threat Landscape 2021.

Press release
SoSafe GmbH I Ehrenfeldguertel 76 I 50823 Cologne I Germany

About SoSafe

SoSafe empowers organizations to build a security culture and mitigate risk with its GDPR-compliant awareness programs. The company was founded in Cologne, Germany, in 2018 by psychologist and former BCG consultant Dr. Niklas Hellemann, Digitalization Expert and previous McKinsey consultant Lukas Schaefer, and seasoned software engineer Felix Schuerholz. Today, it serves more than 1800 customers worldwide and is the market leader in security awareness and training in the DACH region. As one of the leading second-generation awareness platforms, they are powered by behavioral science and smart algorithms and focus on user engagement and the needs of the customer. In doing so, SoSafe delivers engaging, personalized learning experiences and smart attack simulations that turn employees into active assets against online threats.

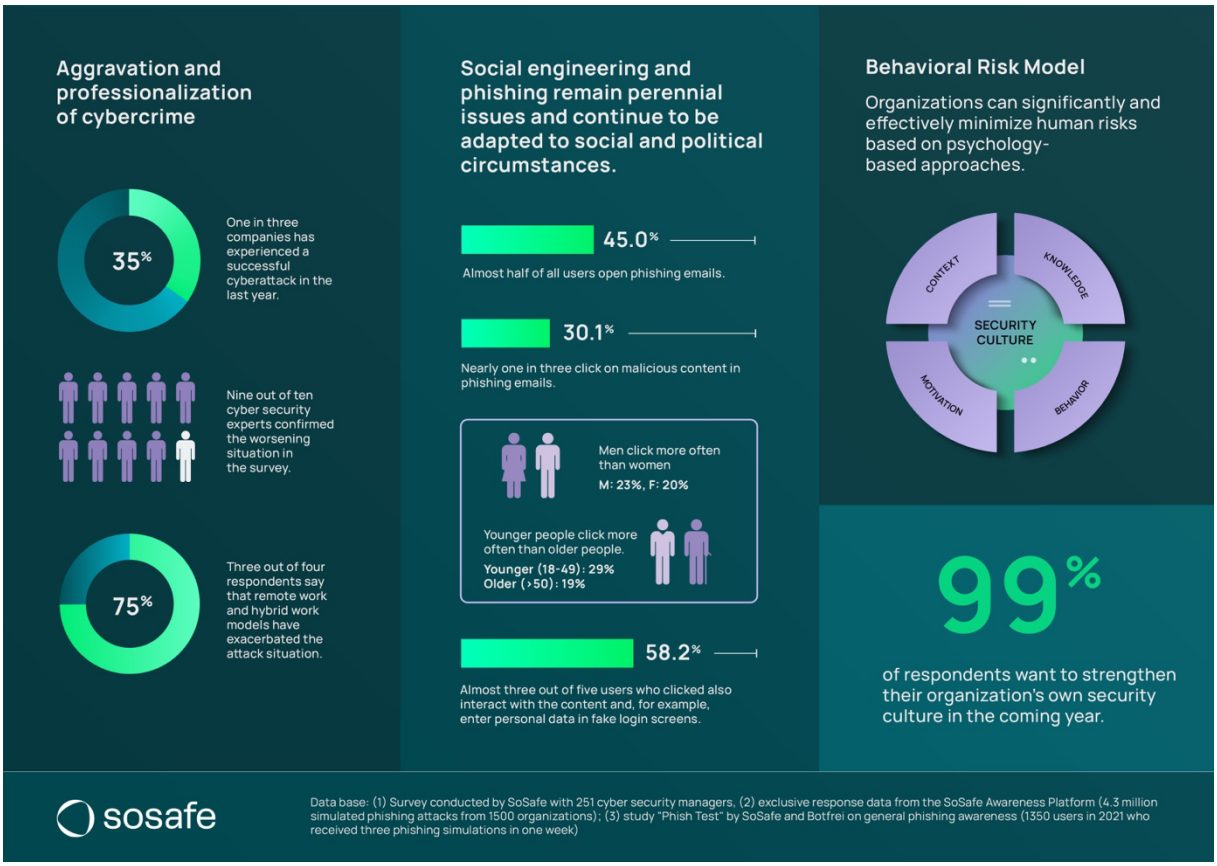
Website: www.sosafe-awareness.com/
LinkedIn: www.linkedin.com/company/sosafe-cyber-security/mycompany/

Press contact

For further questions please contact Mrs. Laura Hartmann via press@sosafe-awareness.com

Please find the full report here: www.sosafe-awareness.com/resources/white-papers/human-risk-review/

Pictures



Description: Summary of the main insights from the "Human Risk Review 2022" from SoSafe.
Credits: SoSafe GmbH