Pressemitteilung
SoSafe GmbH I Ehrenfeldguertel 76 I 50823 Köln

Jedes dritte Unternehmen hat im letzten Jahr einen erfolgreichen Cyber-Angriff erlebt

SoSafe veröffentlicht „Human Risk Review 2022“: Studie über die europäische Cyber-Bedrohungslage

Drei Erkenntnisse stechen hervor: (1) Neun von zehn IT-Sicherheitsverantwortlichen sagen, dass sich die Cyber-Bedrohungslage verschärft hat. Insbesondere Supply-Chain-Angriffe und Ransomware werden groß angelegt. Drei von vier Befragten ergänzen, dass sich die Angriffslage durch Homeoffice und hybride Arbeitsmodelle zugespitzt hat. (2) Fast die Hälfte der Nutzenden öffnen Phishing-Mails, fast jede und jeder Dritte klicken auf enthaltene schädliche Inhalte. Damit sind Öffnungs- und Klickraten nochmal gestiegen. Aktuelle politische und gesellschaftliche Geschehnisse werden instrumentalisiert. (3) Potenzielle Angriffsrisiken können durch systematische Awareness-Maßnahmen um bis zu 90 Prozent gesenkt werden.

Köln, 07. April 2022: SoSafe, einer der am schnellsten wachsenden Cyber-Security-Awareness-Anbieter weltweit, hat seinen „Human Risk Review 2022“ veröffentlicht: „Mit dem Human Risk Review wollen wir Einblicke in aktuelle Trends und Entwicklungen in der europäischen Cyber-Bedrohungslage geben. Unser Ziel ist es, die Aufmerksamkeit für dieses Thema weiter zu stärken – insbesondere für den ‚Faktor Mensch' in der Informationssicherheit“, sagt Dr. Niklas Hellemann, Managing Director von SoSafe. Dass diese Aufklärung wichtig ist, zeigen auch andere Quellen: Eine Umfrage der Allianz-Versicherung[1] belegt, dass Cybervorfälle weltweit auf Platz 1 der größten Business-Risiken stehen. Auf der RSA Conference 2021 sprach Cisco CEO Chuck Robbins von 6 Billionen Dollar Schaden pro Jahr.[2] Die Schnittstelle zwischen Mensch und Maschine bleibt dabei weiterhin Einstiegstor Nummer 1 – mehr als 85 Prozent aller Angriffe starten beim Faktor Mensch.[3]

Während sich Cyberkriminelle zunehmend professionalisieren, muss sich auch die Verteidigerseite entsprechend aufstellen: „Mitarbeitende brauchen mehr als Sicherheitsrichtlinien. Sie können als ‚Human Firewall' eingebunden werden, um das Sicherheitsrisiko nachhaltig zu senken. Dafür muss eine Sicherheitskultur in Unternehmen etabliert werden, die Menschen einbezieht und sie darin unterstützt, Cybergefahren zu identifizieren und sich sicher zu verhalten“, sagt der Diplom-Psychologe Hellemann. Der Human Risk Review hilft dabei: Er gibt Sicherheitsverantwortlichen Handlungsempfehlungen, um die Sicherheitskultur in Unternehmen nachhaltig zu stärken. Mit Hilfe des „Behavioral Security Models“ von SoSafe können Organisationen menschliche Risiken auf Basis psychologisch fundierter Ansätze maßgeblich und effektiv minimieren: SoSafes Daten zeigen, dass systematische Awareness-Maßnahmen die Risiken um bis zu 90 Prozent senken können.

Der Human Risk Review basiert auf unterschiedlichen Datenquellen: Neben einer von SoSafe durchgeführten Umfrage mit 251 IT-Sicherheitsverantwortlichen wurde auf exklusive

[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.

Reaktionsdaten aus der SoSafe Awareness-Plattform (4,3 Mio. simulierte Phishing-Angriffe von 1.500 Organisationen) und aus der jährlich von SoSafe und Botfrei durchgeführten Studie „Phish-Test“ zur allgemeinen Phishing-Awareness (1350 User in 2021, die drei Phishing-Simulationen in einer Woche erhalten haben) zurückgegriffen. Darüber hinaus wurden bestehende Inhalte und Studien analysiert sowie Interviews mit anderen Branchenexpertinnen und -experten geführt.

Verschärfung und Professionalisierung von Cyberkriminalität

Die Umfrage von SoSafe zeigt vor allem: Die Cyber-Bedrohungslage hat sich weiter verschärft. Jede dritte Organisation (35 %) hat demnach im letzten Jahr einen erfolgreichen Cyberangriff erlebt. Darüber hinaus haben neun von zehn (90 %) IT-Sicherheitsexperten die Verschärfung der Lage in der Umfrage bestätigt. Cyberkriminelle haben ihre Angriffstaktiken und Geschäftsmodelle professionalisiert: „Organisationen sehen sich einer innovativen Dark Economy gegenübergestellt, in der Cybercrime-as-a-Service das gängige Geschäftsmodell ist. Taktiken werden beinahe im Minutentakt weiterentwickelt“, sagt Hellemann. Es zeigen sich zwei Cybercrime-Trends: Groß angelegte Supply-Chain-Angriffe zielen auf schwache Glieder in Lieferketten und legen ganze Industrien oder Versorgungssysteme lahm. Darüber hinaus spricht die Agentur der Europäischen Union für Cybersicherheit (ENISA) von der „goldenen Ära“ für Ransomware[4]. Komplexe Angriffstaktiken wie Mehrfacherpressungen erhöhen die Gefahr von Datenmissbrauch demnach um 800 Prozent.

Fast jede und jeder Dritte klicken auf schädliche Inhalte in Phishing-Mails

Phishing und Social Engineering bleiben Dauerbrenner. Angriffe werden laufend und anlassbezogen weiterentwickelt, wie beispielsweise im Angriffskrieg auf die Ukraine: „Innerhalb kürzester Zeit kursierten Social Engineering-Angriffe, die die Hilfsbereitschaft der Menschen gegenüber der Ukraine ausgenutzt haben“, sagt Hellemann. SoSafes Daten zeigen, dass diese Taktiken funktionieren: Fast die Hälfte aller Nutzenden (45 %) öffnen Phishing-Mails. Davon klickt fast jede und jeder Dritte (30 %) auf enthaltene Links, Anhänge oder andere schädliche Inhalte. Ein stetiger Trend zeigt sich bei der Unterscheidung nach Personengruppen: Wie schon im Jahr 2021 klicken Männer häufiger auf Phishing-Mails (23 %) als Frauen (20 %) und jüngere häufiger (18-49 Jahre; 29 %) als ältere Menschen (über 50; 19 %). 58 Prozent der Nutzenden, die geklickt haben, interagieren zudem mit den Inhalten und geben beispielsweise persönliche Daten in fingierte Login-Masken ein. Damit sind die Öffnungs-, Klick- und Interaktionsraten bei Phishing-Mails weiterhin auf hohem Niveau. Im Vergleich zum Vorjahr sind sie sogar noch weiter angestiegen.

Hybride Arbeitsmodelle als Herausforderung für Unternehmen

Drei von vier Befragten (75%) sagen, dass sich die Angriffslage durch Homeoffice und hybride Arbeitsmodelle verschärft hat. Das ist nicht überraschend: Hybride Arbeitswege haben neue Kommunikationskanäle mit sich gebracht, die Cyberkriminellen zusätzliche Eintrittswege für Cyber-Angriffe auf Unternehmen eröffnen. Dabei setzen sie weiterhin verstärkt auf Social Engineering, da Menschen sich immer auf ähnliche Art und Weise angreifen lassen: Über emotionale Manipulation. Psychologisch fundierte Ansätze helfen maßgeblich dabei, menschliche Risiken in einer

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

Organisation zu minimieren. 99 Prozent der Befragten wollen im nächsten Jahr daher ihre organisationseigene Sicherheitskultur stärken.

Über SoSafe

SoSafe unterstützt Organisationen mit seiner DSGVO-konformen Awareness-Plattform dabei, ihre Sicherheitskultur aufzubauen und Risiken zu minimieren. 2018 von Dr. Niklas Hellemann, Lukas Schaefer und Felix Schürholz gegründet, hat SoSafe heute mehr als 1.800 Kunden weltweit und ist einer der führenden Anbieter für Security Awareness Training in Europa. Mit verhaltenspsychologischen Elementen und smarten Algorithmen ermöglicht SoSafe personalisierte Lernerfahrungen und Angriffssimulationen, die Mitarbeitende dazu motivieren und ausbilden, sich aktiv vor Online-Bedrohungen zu schützen.

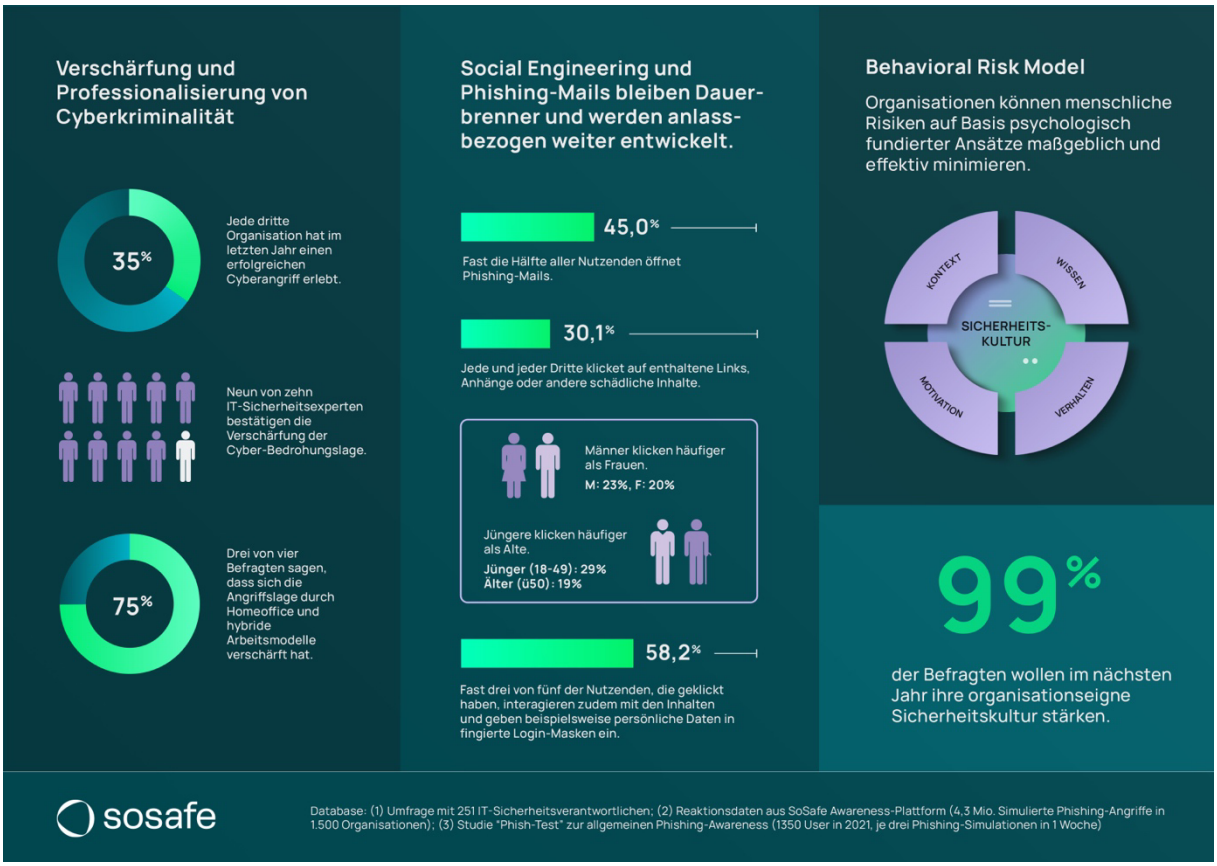
Website: www.sosafe.de/
LinkedIn: www.linkedin.com/company/sosafe-cyber-security/mycompany/

Pressekontakt

Weitere Fragen beantwortet Ihnen gerne Frau Laura Hartmann über presse@sosafe.de

Den vollen Report finden Sie hier: www.sosafe-awareness.com/de/resources/reports/human-risk-review/

Bildmaterial



Beschreibung: Zusammenfassung der wichtigsten Erkenntnisse des „Human Risk Reviews 2022“ von SoSafe. **Credits:** SoSafe GmbH