Pressemitteilung
SoSafe GmbH • Ehrenfeldgürtel 76 • 50823 Köln
Köln, 2. Februar 2021

Human Risk Review 2021: COVID-19 und Homeoffice führen zu höherem Erfolg bei Cyberangriffen

SoSafe-Report gibt Aufschluss über die erfolgreichsten Einfallstore für Cyberkriminelle in europäischen Organisationen im Coronajahr 2020

Die SoSafe GmbH, Anbieter einer interaktiven Schulungsplattform für IT-Sicherheit und einer der Marktführer im Bereich Awareness-Building in der DACH-Region, veröffentlicht heute die Ergebnisse seines „Human Risk Reviews 2021". Die Ergebnisse des jährlichen Reports zeigen: Mitarbeitende europäischer Organisationen stehen gerade während der COVID-19-Pandemie im Fokus von Cyberangriffen und spielen demnach auch eine maßgebliche Rolle dabei, Organisationen vor den Gefahren zu schützen. Neben einer allgemeinen Betrachtung der Cyber-Bedrohungslage beleuchtet der Bericht insbesondere den Faktor Mensch und die technischen und psychologischen Taktiken, die Cyberkriminelle nutzen, um Klicks auf Phishing-Mails zu provozieren. Zum ersten Mal belegt der Report so eindrücklich, dass sich auch die Erfolgswahrscheinlichkeit von Cyberangriffen in Zeiten der Pandemie und dezentraler Arbeitsmodelle erhöht hat. Als Datengrundlage dienen mehr als 1,4 Millionen Reaktionsdatenpunkte aus der SoSafe Awareness-Plattform, Malware-Analysen durch AV-TEST, eine Awareness-Studie mit mehr als 5.000 Teilnehmenden sowie eine Befragung unter mehr als 100 IT-Sicherheitsexpertinnen und -experten.

Cyberangriffe sind in der Coronakrise nicht nur zahlreicher, sondern auch erfolgreicher

Mit dem Human Risk Review 2021 veranschaulicht SoSafe auf Basis exklusiver Reaktionsdaten eindrücklich, was verschiedenste Berichte in den letzten Monaten bereits andeuteten: Die Bedrohungslage hat sich durch die COVID-19-Pandemie weiter verschärft. Insbesondere Social Hacking, das über das Manipulieren menschlicher Emotionen beispielsweise Klicks auf Phishing-Mails provozieren soll, gewinnt in dieser von Unsicherheit geprägten Zeit weiter an Bedeutung. So geht auch ein Großteil der befragten IT-Sicherheitsexpertinnen und –experten davon aus, dass sich die Erfolgswahrscheinlichkeit von Angriffen in der Krise erhöht hat. Mehr als 4 von 10 nehmen zeitgleich eine Zunahme von Cyberangriffen wahr. Die Analyse der Reaktionsdaten festigt diese Vermutungen: Sowohl der zeitliche als auch der inhaltliche Bezug zum Coronavirus machen erfolgreiche Phishing-Angriffe wahrscheinlicher. SoSafe liefert mit dem Human Risk Review außerdem noch nicht bekannte Einsichten in die technischen und psychologischen Mechanismen, die Cyberangriffen zugrunde liegen, etwa mit welchen Vektoren Kriminelle im letzten Jahr agiert haben und mit welchen sie besonders erfolgreich waren.

Die wichtigsten Erkenntnisse auf einen Blick:

- **COVID-19-Pandemie macht Social-Engineering-Angriffe erfolgreicher – bis zu 4 von 5 Empfängerinnen und Empfängern klicken auf Phishing-Mails mit Coronabezug:** Während des ersten Lockdowns war ein rapider Anstieg an Ransomware-Typen zu beobachten. Die SoSafe-Analysen zeigen zudem, dass gleichzeitig auch die Erfolgswahrscheinlichkeit solcher Angriffe stieg – in den Lockdown-Phasen war die Klickrate auf Phishing-Mails stark erhöht. Vor allem Phishing-Mails mit Bezug auf die COVID-19-Pandemie sind für Cyberkriminelle erfolgversprechend. Liegt die durchschnittliche Klickrate bei 29%, provozieren Phishing-Mails mit dem Wort "Corona" in der Betreffzeile Klickraten von bis zu 78,8%.
- **Die Einführung neuer Kollaborationstools macht Arbeitnehmerinnen und Arbeitnehmer anfälliger für Phishing-Angriffe:** Auch der Wechsel ins Homeoffice bietet ein erhöhtes Angriffspotenzial. Die Hälfte aller Mitarbeitenden klickt auf Phishing-Mails, die im Kontext der Einführung von Remote Tools wie Microsoft Teams oder Slack versendet werden.
- **Der Flurfunkt schützt - das Erkennen von Phishing-Mails ist in dezentralen Organisationen erschwert:** Wie die SoSafe-Analysen ergeben, ist die Klickrate auf Phishing-Mails bei Remote Work auch allgemein signifikant höher als bei Präsenzarbeit – in dezentralen Organisationen sogar um ein Dreifaches im Vergleich zu zentralisierten Organisationen.
- **Digital Natives klicken am häufigsten auf Phishing-Mails:** Entgegen der Vermutung, dass jüngere User eine höhere Digitalkompetenz besäßen, zeigt SoSafe in einer separaten Studie mit über 5.000 Bürgerinnen und Bürgern genau das Gegenteil. 18- bis 29-Jährige liegen mit einer durchschnittlichen Klickrate von 38% deutlich vor anderen Altersgruppen, die nur auf jede vierte Phishing-Mail klickten.

Faktor Mensch und IT-Sicherheit wachsen noch enger zusammen

Die Auswertungen lassen auch einen Ausblick auf zukünftige Entwicklungen zu. Die wichtigste Hypothese: Social Engineering und Cyberangriffe, die sich neue Arbeitsmodelle wie das Homeoffice zunutze machen, werden auch weiterhin einen entscheidenden Einfluss auf die IT-Sicherheit in europäischen Organisationen haben und sollten gerade deshalb im Mittelpunkt entsprechender Sicherheits- und Schulungsmaßnahmen stehen. Ein positiver Ausblick: Immerhin 6 von 10 befragten IT-Sicherheitsexpertinnen und –experten möchten in Zukunft ihre Awareness-Maßnahmen erweitern. Mitarbeitenden kommt im Bereich Cyber Security also eine entscheidende Rolle zu. Mit dem Human Risk Review 2021 gibt SoSafe einen umfassenden Überblick über die aktuelle Bedrohungslage rund um den Faktor Mensch und gibt Organisationen erste Handlungsansätze für eine Minimierung ihres Human Risks an die Hand.

Den vollständigen Bericht lesen Sie hier: Human Risk Review 2021

***

Über SoSafe

Die Awareness-Plattform von SoSafe sensibilisiert und schult Mitarbeitende kontinuierlich im Umgang mit dem Thema IT-Sicherheit. Phishing-Simulationen und interaktive E-Learnings bringen den Mitarbeitenden auf effektive und nachhaltige Art und Weise bei, worauf etwa bei der Nutzung von E-Mails, Passwörtern oder sozialen Medien besonders zu achten ist. Das Unternehmen erhält ein anonymes, aber differenziertes Reporting und kann Awareness-Building so messbar machen – vollkommen DSGVO-konform.

Rückfragen beantwortet Ihnen gerne Herr Florestan Peters via presse@sosafe.de