Pandemische Ausmaße: Weltweit 70 Prozent mehr Phishing-Attacken im Homeoffice

Während der Pandemie musste die Arbeit oft überhastet nach Hause verlegt werden – das haben Cyberkriminelle schamlos ausgenutzt: der Sophos Phishing Insights Report 2021 belegt, dass die globalen Phishing-Angriffe auf Unternehmen um 70 Prozent gestiegen sind. In Deutschland liegt die Quote bei 68 Prozent, in Österreich bei 88 Prozent, in der Schweiz bei 87 Prozent.

Sophos veröffentlicht seinen aktuellen Phishing Insights 2021 Report, der auf die Erfahrungen und die Prozesse hinter Phishing-Angriffen auf Organisationen während des Jahres 2020 zurückblickt. Befragt wurden 5.400 IT-Entscheider:innen in 30 Ländern in Europa, Nord- und Süd-Amerika, dem Asia-Pazifik-Raum, Zentralasien, dem Mittleren Osten und Afrika.

Die Ergebnisse zeigen: Phishing-Attacken auf Organisationen haben während der Pandemie erheblich zugenommen. Millionen von Arbeitnehmer:innen mussten ihre Tätigkeiten ins Home-Office verlagern und wurden zur beliebten Zielscheibe für Cyberkriminelle. Aus globaler Perspektive bestätigte die Mehrheit der IT-Teams (70 Prozent), dass die Anzahl der Phishing-E-Mails, die ihre Belegschaft traf, während 2020 zunahm. Aus länderspezifischer Sicht sind die Ergebnisse ähnlich ernüchternd: In Deutschland sind es 68 Prozent, in Österreich sogar 88 Prozent (der zweithöchste Wert nach Israel) und in der Schweiz 87 Prozent der IT-Teams, die einen Anstieg Phishing-E-Mails verzeichneten. Ein Resultat daraus ist, dass global 82 Prozent der IT-Teams im Jahr 2020 Opfer von Ransomware-Attacken wurden.

Weitere Erkenntnisse des Reports:

- IT-Profis haben keine einheitliche Definition von Phishing. Das am weitesten verbreitete Verständnis von Phishing global mit 57 Prozent (Deutschland: 54 Prozent, Österreich: 55 Prozent, Schweiz: 54 Prozent) lautet „E-Mails, die fälschlicherweise behaupten, von einer legitimen Organisation zu stammen, normalerweise in Kombination mit einer Bedrohung oder Anfrage nach Informationen." 46 Prozent (Deutschland: 30 Prozent, Österreich: 37 Prozent, Schweiz: 45 Prozent) halten Business-E-Mail-Compromise-Angriffe für Phishing, und 36 Prozent (Deutschland: 24 Prozent, Österreich: 53 Prozent, Schweiz: 54 Prozent) denken, dass Threadjacking (wenn sich Angreifer als Teil eines Angriffs in einen legitimen E-Mail-Thread einfügen) Phishing ist.
- Die meisten Organisationen – weltweit 90 Prozent – verwenden Cybersecurity-Sensibilitätsprogramme, um gegen Phishing vorzugehen. In Deutschland und der Schweiz tun dies mit 86 bzw. 89 Prozent etwas weniger, österreichische Unternehmen setzen zu 98 Prozent Programme ein.

Chester Wisniewski, Principal Research Scientist bei Sophos, ordnet die Ergebnisse des Phishing Insights 2021 Reports so ein: „Phishing gibt es seit über 25 Jahren und es bleibt eine effektive Technik für Cyberangriffe. Ein Grund für den Erfolg ist seine Fähigkeit, sich ständig weiterzuentwickeln und zu diversifizieren, Angriffe an aktuelle Themen oder Sorgen anzupassen – wie zum Beispiel die Pandemie – und mit menschlichen Emotionen und Vertrauen zu spielen."

Die Versuchung für Unternehmen, Phishing-Angriffe als eine ziemlich niedrige Bedrohung anzusehen, sei groß, so Wisniewski weiter, würde aber das Potential von Phishing unterschätzen. „Denn dieses ist oft der erste Schritt in einer komplexen, mehrstufigen

Attacke.“ Nach Beobachtungen des Sophos Rapid Response Teams nutzen Cyberkriminelle häufig Phishing-E-Mails, um die Nutzer dazu zu verleiten, Malware zu installieren oder sensible Daten zu teilen, die Zugang zum gemeinsamen Netzwerk ermöglichen. „Das Rapid Response Team hat hautnah miterlebt, wie eine scheinbar harmlose E-Mail zu einer Millionen-Dollar Ransomware-Attacke führte. Cryptojacking, Daten- sowie Vermögensdiebstahl sind mögliche Resultate, wenn ein Phishing-Vorfall die Tür für Cyberkriminelle geöffnet hat.“

Am besten wäre es, so der Experte, Phishing-E-Mails daran zu hindern, überhaupt beim vorgesehenen Empfänger zu landen. „Effektive E-Mail-Sicherheitslösungen können hierbei einen großen Beitrag leisten, aber das sollte begleitet sein von aufmerksamen und qualifizierten Mitarbeiter:innen, die in der Lage sind, verdächtige Nachrichten zu erkennen und zu melden und zwar bevor diese im Unternehmen weiterkommen.“

Zahlreiche Details, Zahlen und Grafiken finden Sie hier im aktuellen Phishing Insights 2021 Report.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de