



SPEAR-PHISHING ATTACKEN FÜHREN HÄUFIG ZUM ERFOLG

Unternehmen immer häufiger Ziel von gezielten Phishing Angriffen

Unter Phishing (engl. für „Angeln“) versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

Eine Sonderform des Phishings ist das „Spear-Phishing“. Bei dieser Attacke stehen einzelne Personen im besonderen Fokus der Betrüger. Durch gezielte Recherche nach Informationen zu Mitarbeitern in den sozialen Medien oder auch auf der Seite des Unternehmens, gelingt es Betrügern durch personalisierte Anschreiben in fingierten E-Mails einen vertrauenswürdigen Eindruck beim Empfänger zu erwecken. Häufig wird dabei von den Angreifern ein langfristiges Ziel verfolgt, nämlich so möglichst weit in das befallene Netzwerk vorzudringen, um an geschäftskritische Daten und Ressourcen zu gelangen. Dabei versuchen die Cyber-Kriminellen möglichst lange unbemerkt zu bleiben, um an eine große Menge an Daten zu gelangen. Herkömmliche IT-Sicherheitsvorkehrungen, die diese Vermögensgüter normalerweise vor unbefugten Zugriffen schützen, werden beim Spear-Phishing umgangen.

Die Erfolgsquote spricht für sich. Im Schnitt werden 70 % aller Spear-Phishing E-Mails geöffnet und von 50 % werden ebenfalls die angehängten Dateien heruntergeladen.

Sensibilisierung als Erfolgsfaktor

Aufklärung ist eine der Schlüsselfunktionen zur effektiven Abwehr von Cyber-Kriminalität. Als leistungsstarker Partner bietet RSM seinen Mandanten u. a.

Schulungen für Mitarbeiter und Sensibilisierungsveranstaltungen auf jeder Unternehmensebene an.

RSM verfügt über weitreichende Expertise in der IT-Beratung und Optimierung von IT-Sicherheitssystemen. Die umfangreiche Analyse und Optimierung Ihres eingesetzten IT-Systems sowie die angepasste Verwendung von Anti-Viren- und Spammail-Systemen, kann dazu beitragen, dass gezielte Angriffe frühzeitig erkannt und abgewendet werden können.

Im Zeitalter der Digitalisierung stellt Phishing eine ebenso einfach anzuwendende wie wirkungsvolle Bedrohung dar. Obwohl die Tricks der Betrüger bekannt sind, haben Unternehmen und Behörden bisher keine wirkungsvollen Gegenmaßnahmen entwickelt. Internet-Nutzer sind daher weiterhin sowohl in ihrem privaten Bereich als auch im Arbeitsumfeld davon betroffen. Es bleibt dem Verbraucher also erstmal nur die eigene Auskunftsfreudigkeit sowohl auf sozialen Plattformen als auch beim Erhalt fragwürdiger Emails kritisch zu hinterfragen.

Lassen Sie sich gerne von unseren RSM Experten zum Thema „Sensibilisierung im Bereich IT-Sicherheit“ beraten.

RSM Risk Consulting Germany GmbH & Co.KG

Jungfernstieg 30, D-20354 Hamburg

ras@rsm.de

Telefon: +49 40 35006 225, www.rsm.de