Gehackte Promi-Konten sorgen für Ausnahmezustand bei Twitter

Viele prominente und sogar verifizierte Twitter-Konten haben gestern Kryptocoin-Scams verbreitet. Es wurden zahlreiche gefälschte Tweets von bekannten Personen und Unternehmen gemeldet, darunter Joe Biden, Elon Musk, Barack Obama, Bill Gates, Apple und viele andere.

Die betrügerischen Tweets enthielten Berichten zufolge scheinbar sehr eingängige, wenn auch höchst unwahrscheinliche Nachrichten wie "Fühlen Sie sich großartig, Verdoppelung aller an meine Bitcoin-Adresse geleisteten Zahlungen". Mit solchen und ähnlichen Tweets wurden Follower aufgefordert, erst 1.000 US-Dollar einzuzahlen, um dann 2.000 US-Dollar zurückzuerhalten. Natürlich ist dieses Angebot völliger Unsinn und Bauernfängerei – und dennoch stammen diese Tweets tatsächlich von verifizierten Konten. Aus diesem Grund könnten Personen trotz der Verrücktheit des Angebots darauf hereinfallen. Es ist schließlich nicht so, als würden sie eine E-Mail erhalten, unter der z.B. "Elon Musk" steht, sondern der Tweet steht wirklich im offiziellen Twitter-Konto des Prominenten.

Aufgrund des Ausmaßes der Scam-Attacke hat Twitter den ungewöhnlichen, aber verständlichen Schritt unternommen, Teile seines Dienstes während der Untersuchung zu schließen. So bestanden u.a. Einschränkungen zu twittern oder das Passwort zurückzusetzen. Bis man genau wisse, wie diese betrügerischen Tweets gesendet wurden, ist es schwierig zu sagen, welche Maßnahmen Nutzer ergreifen könnten, insbesondere angesichts des eingeschränkten Zugriffs auf Dienste wie Kennwortänderungen (und vermutlich auch Änderungen von Details wie Zwei-Faktor-Authentifizierungsnummern). Allgemein lässt sich allerdings sagen, dass diese Betrüger immer nur dann erfolgreich sind, wenn Menschen auf ihre unwahrscheinlichen Nachrichten hereinfallen – deren Erfolg darauf beruht, dass Menschen ihren Verstand abschalten, nur weil der Tweet von einer Berühmtheit oder von einer Quelle stammt, der sie vertrauen möchten.

Man kann sich schützen, indem man die folgenden drei einfachen Tipps beherzigt:

1. Wenn eine Nachricht zu gut klingt, um wahr zu sein, ist sie zu gut, um wahr zu sein. Wenn Musk, Gates, Apple, Biden oder eine bekannte Firma aus einer Laune heraus riesige Geldbeträge verschenken möchten, würden sie nicht verlangen, dass sie zuerst in Vorleistung gehen müssen. Das ist kein Geschenk, es ist ein Trick und es ist ein offensichtliches Zeichen dafür, dass das Konto der Person gehackt wurde. Das aktuelle Beispiel taucht in den verschiedensten Varianten in der Social-Media-Welt auf. Deshalb: Wenn man auch nur leichte Zweifel hat, Finger von der Sache lassen!

2. Transaktionen mit Kryptowährungen bieten nicht den rechtlichen Schutz, den man bei Banken oder Kreditkartenunternehmen erhält. In der Welt der Kryptowährung gibt es keinen Betrugsmeldedienst oder Transaktionsstornierung. Das Senden von Kryptocoins ist wie das Übergeben von Banknoten in einem Umschlag – wenn das Geld an einen Gauner geht, gibt es keine Möglichkeit, es zurückzubekommen. Deshalb auch hier: keine Überweisung von Kryptowährungen, wenn Sie sich nicht ganz sicher sind!

3. Auf Anzeichen achten, dass eine Nachricht möglicherweise nicht echt ist. Gauner müssen keine Rechtschreibfehler machen oder wichtige Details falsch darstellen. Aber oft entlarven sie sich durch eine seltsame Sprachwahl, wie das Wort "großartig" im obigen Beispiel. Wenn die Gauner also einen Fehler machen, z. B. Euro 50 schreiben, obwohl

das Währungszeichen an letzter Stelle stehen sollte, die eigene Telefonnummer nicht standardmäßig dargestellt ist oder eine unnatürliche Sprache verwenden wird, sollte man besonders vorsichtig sein und sich lieber doppelt und dreifach absichern, bevor man aktiv wird.

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