Ressort: Technik

Zeitung: Hacker plünderten Konten von Bankkunden

Berlin, 03.05.2017, 00:00 Uhr

GDN - Hackern ist es in den vergangenen Monaten offenbar in einem zweistufigen Angriff gelungen, Konten von Bankkunden zu plündern. Laut eines Bericht der "Süddeutschen Zeitung" (Mittwochsausgabe) verschafften sich die Kriminellen erst Login-Daten und Mobilfunknummer, um anschließend SMS umzuleiten.

Auf diese Weise konnten die Angreifer Geld auf eigene Konten überweisen. Auch deutsche Kunden waren betroffen. International besteht die Schwachstelle dem Bericht zufolge weiterhin. Der Telekommunikationskonzern O2/Telefonica bestätigte der Zeitung, dass es Anfang des Jahres entsprechende Vorfälle gegeben habe: "Ein krimineller Angriff aus dem Netz eines ausländischen Providers hat Mitte Januar dazu geführt, dass eingehende SMS für vereinzelte Rufnummern in Deutschland unbefugt umgeleitet wurden." Der entsprechende Provider sei gesperrt worden, die Kunden informiert, mittlerweile habe die Polizei Ermittlungen aufgenommen. Der Hacker-Angriff bringt vor allem Telekommunikationsanbieter in Erklärungsnot, da die ausgenutzte Schwachstelle seit Ende 2014 öffentlich bekannt ist, schreibt die SZ. Bereits damals wurde gewarnt, dass es für motivierte Kriminelle ein Leichtes sei, auf diese Weise Geld zu klauen. Zuerst müssen die Hacker an sämtliche Daten kommen, die für eine Überweisung nötig sind: Kontonummer, dazugehöriges Passwort und die Handynummer. Dafür verschicken sie zum Beispiel Phishing-Mails. Diese Mails täuschen vor, von einer Bank zu kommen. Tatsächlich kommen sie von Webseiten, die die Angreifer kontrollieren. Jede dort eingegebene Information landet bei ihnen. Doch Überweisungen per Einmalkennwort abgesichert werden - dem sogenannten mTan-Verfahren - reicht dieser Schritt nicht aus: Deshalb nutzen die Hacker eine Schwachstelle im SS7-Netzwerk aus. Über dieses Verfahren tauschen sich Mobilfunkunternehmen weltweit aus. In SS7 enthalten ist eine Datenbank mit dem Namen Home Location Register. Darüber könne man das Handy sowohl orten als auch Rufnummern umleiten. Diese Umleitung können Provider einfach anfordern. Über diesen Zugang ist es den Kriminellen möglich, eine Rufnummer-Umleitung einzurichten. Erst mit diesem zweiten Schritt ist der Angriff komplett. Sie können sich nun zu einem in das Konto des Opfers einloggen, die Überweisung tätigen, die SMS über den Provider auf eine Rufnummer ihrer Wahl umleiten lassen und damit die Überweisung bestätigen. Die Änderung der Rufumleitung durch Dritte kann blockiert werden, erklärt Hendrik Schmidt von IT-Sicherheitsfirma ERNW. "Wenn man Kunde bei Vodafone, O2 oder Telekom ist, sollte es auch nur Vodafone, Telekom oder O2 gestattet sein, Rufnummern umzuleiten - und nicht jeder Organisation, die Zugang zu diesem Netzwerk besitzt." Karsten Nohl ist einer der Sicherheitsforscher, die Ende 2014 auf die Schwachstelle in SS7 aufmerksam gemacht haben. Er zeigte, wie es zum Beispiel für Geheimdienste möglich wäre, Nachrichten mitzulesen. Entsprechend vernichtend fällt sein Urteil nun aus: "Die ganze Industrie will dieses Problem lösen. Aber es ist enttäuschend, dass es so viele Jahre gedauert hat und erst ein finanzieller Schaden entstehen musste, bevor etwas unternommen wurde. Die Privatsphäre der Kunden alleine war wohl nicht ausschlaggebend genug."

Bericht online:
https://www.germandailynews.com/bericht-88829/zeitung-hacker-pluenderten-konten-von-bankkunden.html

Redaktion und Veranwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV:

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com