Ressort: Technik

Bericht: Deutsche Parteien erneut Ziel eines Hackerangriffs

Berlin, 20.09.2016, 17:22 Uhr

GDN - Deutsche Parteien sind im Sommer offenbar abermals zum Ziel eines breit angelegten Hackerangriffs geworden. Sicherheitsexperten der Bundesregierung nehmen den Vorfall sehr ernst und befürchten, dass eine ausländische Macht Geheimnisse aus dem Berliner Politikbetrieb ausspähe, um die Bundestagswahl im kommenden Jahr zu beeinflussen, berichten die "Süddeutsche Zeitung", NDR und WDR. Politiker und Mitarbeiter mehrerer Parteien erhielten am 15. und 24. August E-Mails, die vermeintlich aus dem Hauptquartier der Nato stammten, berichten die drei Medien.

Darin befand sich ein Link, über den Spähsoftware auf den betroffenen Rechner gelangen konnte. Anders als bei einem früheren Angriff auf das Parlament waren diesmal nicht nur Fraktionen im Bundestag betroffen, wie etwa die Linken-Fraktionschefin Sahra Wagenknecht, sondern auch Teile der Parteien wie die Junge Union, die Bundesgeschäftsstelle der Linken oder die CDU im Saarland, wo im März ein neuer Landtag gewählt wird. Die E-Mails stammten von einem Account mit der Adresse "hq.nato.int", was auf das Hauptquartier des Militärbündnisses Nato hindeutete. In den Schreiben wurden Informationen über das Erdbeben in Italien oder den Militärputsch in der Türkei angeboten. Tatsächlich aber führte der entsprechende Link zu einem Server, der Schad- oder Spähsoftware auf den Computer des Empfängers überspielen sollte. Der Cyber-Angriff fiel der Nato und dem Bundesnachrichtendienst auf, sie warnten am 7. September das Abwehrzentrum des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dort nahm man die Sache nach Informationen von SZ, NDR und WDR so ernst, dass BSI-Präsident Arne Schönbohm am 9. September persönlich die Fraktionen im Bundestag informierte. Der Bundestag war bereits 2015 Ziel eines Cyberangriffs. Damals wurden Mails mit einem Absender verschickt, der auf die Vereinten Nationen hindeutete und Informationen zur Ukraine anbot. Den Hackern gelang es, Administratorenpasswörter abzufangen und auf das gesamte Netz im Parlament zuzugreifen. Experten vermuten, dass die Urheber des damaligen Angriffs aus Russland stammen. Auch der neue Fall deutet nach Ansicht von Regierungsexperten auf russische Hacker hin. Sie sollen wie schon 2015 der Gruppe apt28 oder der Sofacy Group angehören. Das BSI befürchtet nun, dass die Täter die öffentliche Meinung vor der Bundestagswahl im Herbst 2017 manipulieren wollen. Sie könnten bei ihren Angriffen vertrauliche Informationen aus dem Inneren der deutschen Parteien abgreifen und dann kurz vor der Wahl veröffentlichen, um gezielt die öffentliche Stimmung zu beeinflussen. Ein ähnliches Szenario hat sich jüngst in den USA abgespielt: Die Enthüllungsplattform Wikileaks veröffentlichte Tausende E-Mails aus der Demokratischen Partei, die ihr offenbar von einem Hacker zugespielt worden waren. Aus der Korrespondenz ergab sich, dass die Parteispitze im Vorwahlkampf die Präsidentschaftskandidatin Hillary Clinton bevorzugt hatte. Die Parteichefin Debbie Wasserman Schultz musste zurücktreten. BSI-Chef Schönbohm bestätigte auf Anfrage von SZ, NDR und WDR, die Parteien über den neuen Hacker-Angriff informiert zu haben. "Vor dem Hintergrund der amerikanischen Ereignisse war es mir wichtig, dass sich die Parteien vor Ausspähung schützen", sagte er.

Bericht online:
https://www.germandailynews.com/bericht-78304/bericht-deutsche-parteien-erneut-ziel-eines-hackerangriffs.html

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

Haftungsausschluss:
Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.

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