Hackerangriffe in Australien

Der Elefant im Cyberraum

Australiens Regierung veröffentlicht bemerkenswerte technische Details zu den jüngsten massiven Hackerangriffen auf das Land. Warum ausgerechnet jetzt - und was ist die eigentliche Botschaft?

Von **Patrick Beuth**
19.06.2020, 14.20 Uhr

Die Botschaft des australischen Premierministers Scott Morrison: Ein staatlicher Cyber-Akteur hackt gerade alles, was geht Lukas Coch/ dpa

Australiens Premierminister Scott Morrison informierte seine Landsleute am Freitag über "Angriffe auf australische Organisationen durch einen hochentwickelten staatsbasierten Cyber-Akteur". Diese seien nicht neu, aber ihre Frequenz steige. Was er nicht sagte: Wer dieser Akteur ist und was er

erreichen will. Warum also warnt Morrison die Australier vor diesem Cyber-Butzemann, ausgerechnet jetzt?

Offiziell will er ein "Bewusstsein schaffen" für die Bedrohungslage. Angegriffen würden schließlich nicht nur "alle Ebenen der Regierung", sondern auch "Wirtschaft, politische Organisationen, Bildungs- und Gesundheitseinrichtungen, Grundversorgungsanbieter und andere Betreiber Kritischer Infrastrukturen".

Dass es solche Angriffe gibt, sollte eigentlich für niemanden neu sein. Die australischen Medien sind voll davon, seit Monaten. "Es klang ein wenig so, als hätte Morrison gesagt 'Wer zum Strand geht, wird Sand finden'", sagt auch der in Australien lebende Chief Technology Officer (CTO) der IT-Sicherheitsfirma Crowdstrike, Michael Sentonas , im Gespräch mit dem SPIEGEL. Aber anders als der Premierminister es darstelle, seien australische Unternehmen und Einrichtungen keineswegs gut darauf vorbereitet, "sonst würden wir nicht jede Woche einen neuen großen Namen wegen eines erfolgreichen Hackerangriffs in den Nachrichten sehen".

Wer nicht schnell patcht, wird gehackt

Um jetzt konkrete Hilfestellung zu geben, veröffentlichte Australiens Cyber Security Centre (ACSC) seine Erkenntnisse über die Techniken und Taktiken der ungenannten Täter . Zusammengefasst lauten sie:

- Vieles von dem, was Sicherheitsforscher in letzter Zeit an Schwachstellen entdeckt und demonstriert haben, wandeln die Täter in kürzester Zeit in Angriffswerkzeuge um, beispielsweise die Ende 2019 bekannt gewordenen Citrix-Sicherheitslücken. Sprich: Gehackt wird, wer nicht schnell patcht, also Schwachstellen schließt.

- Außerdem prüfen die Täter regelmäßig, welche Netzwerke prinzipiell vom Internet aus erreichbar sind, um nach Bekanntwerden neuer Sicherheitslücken sofort passende Ziele zur Hand zu haben.
- Wenn das nicht klappt, versuchen sie es mit verschiedenen Phishing-Ansätzen.
- Ziel ist es immer, gültige Zugangsdaten abzufangen und sich fortan damit Zugang zu verschaffen - vermutlich, weil das weniger auffällig ist, als Software im gekaperten Netzwerk zu platzieren, die Daten ausleitet.
- Werden doch solche Werkzeuge im gehackten Netzwerk installiert, werden diese über ebenfalls gehackte Server in Australien gesteuert. Der dabei entstehende Datenverkehr ist weniger verdächtig als eine neue Verbindung in ein anderes Land. Zudem ist Geoblocking dadurch keine geeignete Schutzmaßnahme: Wer den Zugriff auf Websites im eigenen Land sperrt, behindert sich im Alltagsbetrieb selbst.

Doch weder Morrison, noch das ACSC sagen etwas zum Ziel der Angriffe. Das ACSC schreibt nur, was *nicht* das Ziel sei: "Wir haben keine Absicht des Akteurs erkannt, innerhalb der Netzwerke der Opfer irgendwelche disruptiven oder zerstörerischen Aktivitäten durchzuführen."

"Ein politisches Signal der Stärke"?

Warum also ausgerechnet jetzt dieser Schritt an die Öffentlichkeit, dieser große Auftritt von Morrison mit so wenig Informationsgehalt?

Vielleicht, weil derzeit ein besonders schwerer Angriff läuft, der noch nicht öffentlich bekannt ist? "Man würde nicht, wie

Scholtens. Er geht davon aus, "dass wir darüber in den kommenden Tagen mehr erfahren werden".

Thomas Reinhold vom Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg hält es für möglich, dass sowohl der nicht genannte staatliche Akteur, als auch die australische Regierung vor allem politische Botschaften senden wollen: Die Täter hätten sich "mit der Wahl öffentlich bereits bekannter Sicherheitslücken und fertiger, im Netz verfügbarer Angriffsmethoden einem hohen Risiko ausgesetzt und mussten mit der Entdeckung ihrer Aktivitäten rechnen", sagt Reinhold. Zudem scheine die Auswahl der Ziele "wenig spezifisch", es gehe wohl eher darum, "mitnehmen was zu finden ist". Das sei für Spionage-Aktivitäten eher unüblich. Die Frage sei daher, "ob mit den Angriffen ein politisches Signal der Stärke, der Kapazitäten und Möglichkeiten gesendet werden soll". Sprich: Wollte hier jemand zeigen, dass er Australien großen Schaden zufügen könnte, wenn er wollte?

Und wollte Morrison seinerseits zunächst nur eine rote Linie ziehen, wie Reinhold vermutet? Australien sei schließlich Mitglied der Five Eyes, also einer Allianz mit den Geheimdiensten der USA, Großbritanniens, Neuseelands und Kanadas. Man könne daher auf Unterstützung unter anderem der NSA und des britischen GCHQ zählen, zwei der fähigsten Nachrichtendienste der Welt. "Mit Blick auf die Summe der geballten Fähigkeiten dieser Organisationen im Cyberspace dürfte der Umstand, dass die Regierung Australiens bewusst noch keinen Finger auf einen Staat gerichtet hat, als politisches Warnsignal gewertet werden", sagt Reinhold.

Der Elefant im Cyberraum ist China. Schon kurz nach Morrisons Pressekonferenz berichteten australische Medien unter Berufung auf "senior sources", dass der nicht genannte staatliche Akteur China sei. Solche Vorwürfe gibt es schon lange, zudem sind die Beziehungen der beiden Länder so angespannt wie nie. Es macht aber einen diplomatischen

Unterschied, ob anonyme Quellen die chinesische Regierung beschuldigen, oder die Regierung ganz offiziell.

Das wäre eine der nächsten denkbaren Eskalationsstufen.

Diskutieren Sie mit

Feedback

Mehr lesen über

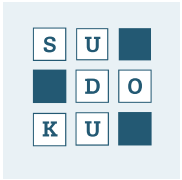
Australien | Scott Morrison | Computersicherheit | Ha

Spiele

mehr Spiele

Trivial Pursuit

Solitaire



Sudoku

M

Serviceangebote von SPIEGEL-Partnern

Gutscheine

Top Gutscheine Alle Shops

Auto

Job

Finanzen

Freizeit

Alle Magazine des SPIEGEL

Dein SPIEGEL

SPIEGEL EDITION

SPIEGEL LESEZEIC

SPIEGEL Gruppe

Abo Shop bento manager magazin Harvard Business Manager

buchreport Werbung Jobs SPIEGEL Akademie SPIEGEL Ed

Impressum Datenschutz Nutzungsbedingungen Kontakt Hilfe

Facebook Twitter Wo Sie uns noch folgen können