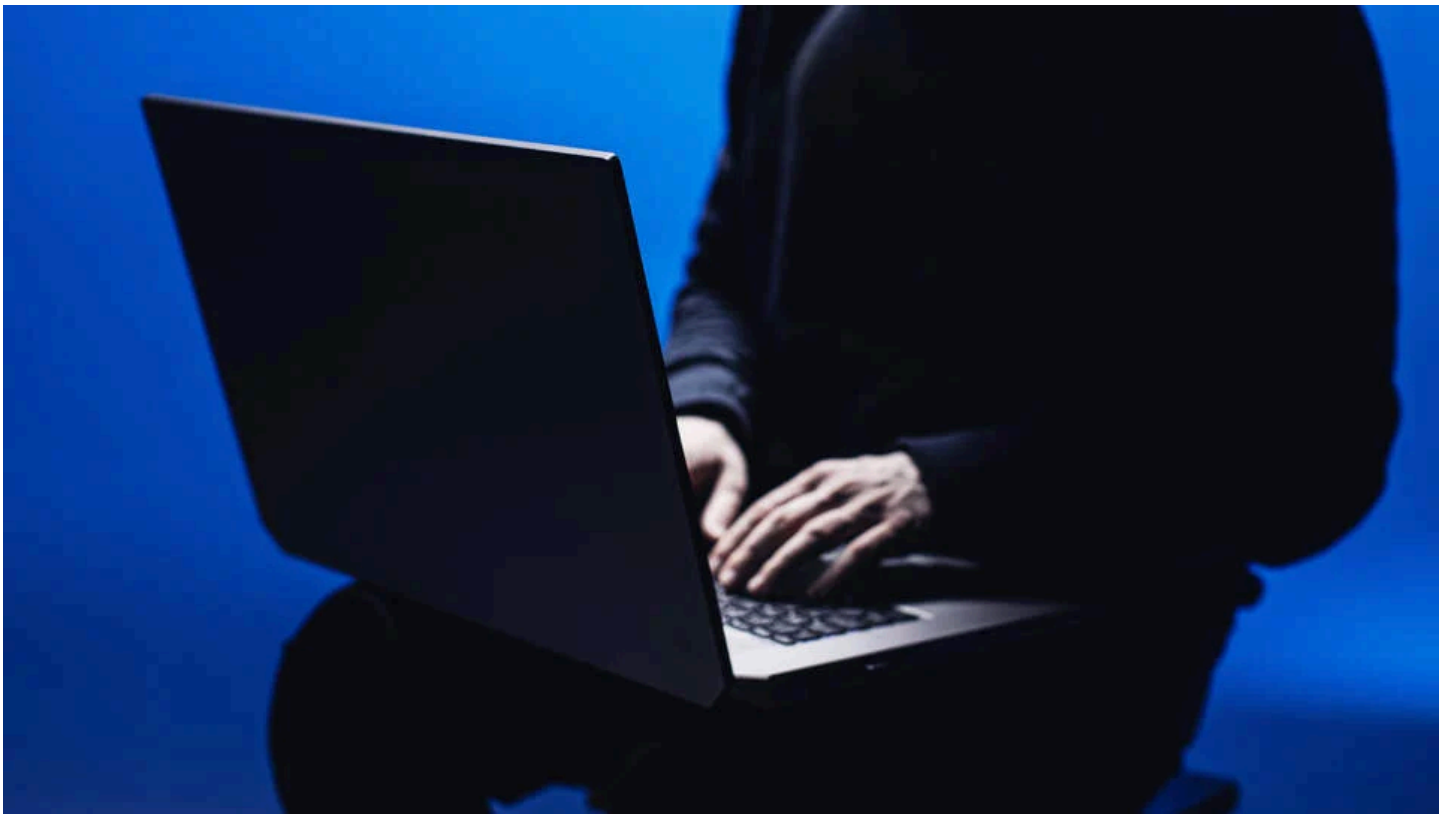
Schwächen offengelegt

Cyberangriff auf die Post: „Schockierend, wie fragil das Netz in Luxemburg ist“

Sam Grüneisen vom Chaos Computer Club Luxemburg über die möglichen Hintermänner der Cyberattacke auf das Netz der Post vom vergangenen Mittwoch.



Es gibt Hinweise, dass der Angriff von einem staatlichen Akteur getätigt wurde. Beweise gibt es derzeit jedoch keine. Foto: Getty Images (Symbolfoto)

Jean-Philippe Schmit
Redakteur

28.07.2025

Teilen

„Wir wissen nicht viel mehr, als das, was öffentlich kommuniziert wurde“, sagt Sam Grüneisen vom Chaos Computer Club Luxemburg (C3L) über den Internet- und Telefonausfall der Post vom vergangenen Mittwoch. Er kann sich jedoch noch sehr gut daran erinnern: „Ich hatte gerade Feierabend, als ich feststellte, dass das Internet ausgefallen war.“ Was an sich erstmal nichts Ungewöhnliches sei.

Lesen Sie auch:
Post: „Es war doch ein Cyberangriff“

Zunächst dachte er an eine lokale Störung, beispielsweise dass ein Bagger ein Kabel beschädigt hat oder eine Trafostation ausgefallen ist. Er fuhr nach Hause. Unterwegs stellte er fest, dass auch sein Handy nicht

mehr funktionierte. Auch das 4G- und das 5G-Netz waren ausgefallen und Sam Grüneisen wurde sich bewusst, dass es sich um „etwas Größeres“ handeln müsse.


H
M

Sam Grüneisen vom Chaos Computer Club Luxemburg glaubt, dass ein staatlicher Akteur hinter dem Angriff stecken könnte. Foto: LW-Archiv

Direkte Probleme bereitete der Ausfall jedoch nicht. „Ich habe nicht den gleichen Internet- und Handyprovider“, sagt er. Das Internet zu Hause funktionierte. Dies sei auch ein Ratschlag an all jene, die auf das Internet angewiesen sind. Wer das fixe Internet bei einem anderen Provider hat als das mobile Internet, ist gegen solche Ausfälle resilienter.

Wer für den Ausfall verantwortlich ist, kann er nicht sagen. „Solange sich keine Gruppe für den Angriff bekennt, ist es auch sehr schwer, den Täter ausfindig zu machen“, sagt er. Es könnten viele Akteure gewesen sein: „Vom jugendlichen Hacker, der auf eine Sicherheitslücke gestoßen ist und diese ausprobieren wollte, bis hin zu staatlichen Hackergruppen.“

Vom jugendlichen Hacker bis zur staatlichen Organisation

In Russland gibt es solche Gruppierungen, doch sicher ist er sich nicht, ob es sich in diesem Fall um eine solche handelte. „Selbst wenn sich herausstellen sollte, dass die Angriffe von Russland aus stattfanden, ist dies kein Beweis“, sagt er. Die Angreifer hätten ihren Angriff auch über Server in Russland laufen lassen können, ohne sich in dem Land zu befinden.

„Das Problem ist, dass wir nicht genau wissen, wie der Angriff vonstattenging“, sagt er. Eine DDoS-Attacke, bei der Server mit Anfragen bombardiert werden, bis sie zusammenbrechen, sei keine „ausgeklügelte, raffinierte Attacke“, wie die Post behauptete. „Wir wissen zudem auch nicht, was genau angegriffen wurde.“

Lesen Sie auch:

Nach Post-Ausfall: Verbraucherschutz erhält Beschwerden über LU-Alert

„Es könnte sein, dass die Software, die laut Post angegriffen wurde, eine bisher unbekannte Sicherheitslücke hatte“, sagt Grüneisen. Ein einzelner Hacker könnte darauf gestoßen sein und die Lücke sofort ausgenutzt haben. Vorstellbar sei aber auch, dass sich eine Person von der Post schlecht behandelt fühlte und jemanden bezahlte, der die Post dann „aus dem Netz warf“.

Auf jeden Fall sei es ein größerer Angriff gewesen. „Ich war schockiert festzustellen, wie fragil das Netz in Luxemburg ist“, sagt er. Er sei erstaunt gewesen, dass sogar die Notrufe nicht mehr funktioniert hätten. „Auch die Dauer des Ausfalls hat mich überrascht.“

Im digitalen Zeitalter ist es durchaus möglich, dass einzelne Personen ein solches Chaos anrichten können. Vorstellbar ist, dass ein Jugendlicher auf einen solchen Bug stieß und sich „ausgetobt hat“. Er wollte der Allgemeinheit zeigen, was möglich ist.

„Solange sich niemand öffentlich zu dem Angriff bekennt, ist es schwierig, den Täter zu ermitteln.“

Sam Grüneisen
Chaos Computer Club

In diesem Fall würden die bekannten Informationen jedoch eher auf einen staatlichen Akteur hinweisen. Jede größere Nation verfügt über ein „Cybercommand“, erklärt er. Hinter dem Angriff könnte eine solche Organisation stecken. In der Vergangenheit hat es bereits ähnliche Fälle gegeben. Es kann sich aber auch um eine nichtstaatliche Untergrundgruppierung handeln. Oder eine speziell für diesen Angriff zusammengestellte Gruppe.

Das Ziel des Angriffs war es, das Netz lahmzulegen. Bisher ist nicht bekannt, dass die Post erpresst wurde. Die Angreifer hätten mit dem Angriff auch kein Geld erbeuten können. „Europa befindet sich im Krieg“, sagt er. Was eher für einen staatlichen Akteur spricht und er wiederholt: „Solange sich niemand öffentlich zu dem Angriff bekennt, ist es schwierig, den Täter zu ermitteln.“

Die kritische Infrastruktur des Kontinents müsse besser geschützt werden. Auch die Bürger sollten sich auf solche Ausfälle einstellen. „Es hat mich überrascht, dass es beim Notruf kein redundantes Backupsystem gab – oder dass der Angriff so ausgeklügelt war, dass dieses umgangen werden konnte.“ Nun sei es an der Post, den Angriff zu analysieren. Sam Grüneisen schließt einen weiteren Angriff nicht aus. „Die Mitarbeiter der Post haben aktuell viel zu tun“, sagt er.

Wirtschaft | Digitalisierung