Wirtschaft

Festnetz- und Mobilfunksysteme funktionierten während des Cyberangriffs, aber viele Nutzer konnten sich nicht mit den Netzen verbinden, hält Wirtschaftsminister Lex Delles fest. Foto: Anouk Antony

Post-Cyberattacke traf Server, nicht das Telefonnetz selbst

Telefone funktionierten während des Cyberangriffs auf die Post, aber die Kunden konnten nicht auf das Netz zugreifen

Von Aaron Grunwald

Der massive Ausfall bei Post Luxembourg Ende Juli wurde dadurch verursacht, wie die Systeme der Post auf die Cyberattacke reagierten, und nicht durch die Cyberattacke selbst. Das sagte Wirtschaftsminister Lex Delles (DP) in einer Antwort auf eine parlamentarische Frage des Abgeordneten Sven Clement (Piratepartei).

Die Internet- und Mobilfunkdienste des Telekommunikationsanbieters waren am 23. Juli für etwa vier Stunden nahezu vollständig ausgefallen, sodass Tausende von Nutzern die Telefonnummer 112 nicht erreichen konnten. Die luxemburgischen Festnetz- und Mobilfunksysteme funktionierten während des Cyberangriffs weiter, aber viele Nutzer konnten sich nicht mit den Netzen verbinden, hält Delles fest.

Die Post erklärte zunächst, der Ausfall sei durch ein Softwareproblem verursacht worden. Zwei Tage nach dem Netzausfall erklärte das Unternehmen jedoch, dass der Ausfall durch einen Cyberangriff verursacht wurde.

Internet zum Telefonieren

In seiner Antwort führt Delles weiter aus, dass die VOIP-Infrastruktur (Voice over Internet Protocol) der Post „nicht direkt vom Internet abhängig ist und während des Cyberangriffs von vielen professionellen Kunden mit Festnetzanschlüssen weiter genutzt werden konnte". VOIP bezieht sich auf die Technologie und den Netzwerktyp, der für Sprachtelefonanrufe verwendet wird, und nicht auf die tatsächliche Nutzung des Internets selbst. Viele Kunden nutzen jedoch ihre Internetverbindung, um sich mit dem Telefonsystem zu verbinden.

„Durch den Angriff war der Zugang zu DNS-Servern für einige Post-Kunden nicht mehr möglich, und auch das Festnetztelefon funktionierte in diesem Fall nicht mehr", so Delles. DNS-Server dienen dazu, den Internetverkehr automatisch umzuleiten.

„Das Mobilfunknetz ist ebenfalls nicht direkt vom Internet abhängig, aber der Angriff führte dazu, dass die internen Systeme in den Notfallmodus versetzt wurden, was in diesem Fall zu Konnektivitätsproblemen führte", so Delles. „Die Maßnahmen, die nach dem Angriff ergriffen wurden, um die Auswirkungen auf die VOIP-Dienste zu minimieren, waren nicht auf die Cyberbedrohung selbst zurückzuführen, sondern darauf, wie die internen Systeme der Post, die zur Verwaltung des Telekommunikationsnetzes eingesetzt werden, auf die plötzliche Veränderung des Internetverkehrs reagierten."

In Zukunft vorbereitet

Nach einer Analyse des Vorfalls haben Post und Govcert, das IT-Sicherheitszentrum der Regierung, Informationen vom Technologieanbieter von Post erhalten, „mit den notwendigen technischen Informationen und Empfehlungen, um einem solchen Angriff in Zukunft zu begegnen".

Auf die Frage nach kritischen Infrastrukturen, die auf das Postnetz angewiesen sind, sagte Delles, dass „die potenziellen Auswirkungen dieses Vorfalls von den zuständigen Behörden analysiert wurden und ein Austausch mit allen kritischen Infrastrukturen stattgefunden hat". Er nannte keine Einzelheiten über die betroffenen Infrastrukturen und die potenziellen Risiken.

Delles wies darauf hin, dass die Regierung keine Pläne habe, neue Cybersicherheitsregeln für Telekommunikationsbetreiber in Bezug auf Cybersicherheit und den Einsatz von Technologieanbietern einzuführen.

Dieser Artikel erschien zuerst bei „Luxembourg Times". Er wurde mit KI-Tools übersetzt, die aus Daten von menschlichen Übersetzungen lernen, und von Melanie Ptok redigiert.