frische FISCHE
Agentur für Text & PR

Linux-Magazin findet Daten-Leck bei DHL-Paketverfolgung

- *Unbefugtes Auslesen von Kundendaten in Sekundenschnelle möglich*
- *DHL gelobt Besserung und schaltet die Paketverfolgung für den betroffenen Bereich vorerst ab*

München, 03.11.2008 – Die Fachzeitschrift Linux-Magazin deckt in Ausgabe 12/2008 auf: Namen, Adressen und Lieferzeiten sind beim "Track & Trace Standard-Paket" von DHL praktisch schutzlos. Das Unternehmen will Kunden mit schwachen Passwörtern ermahnen und die fehlerhafte Funktion kurzfristig abschalten.

Linux-Magazin-Autor Tobias Eggendorfer staunte nicht schlecht, als er den Link zur Sendungsverfolgung in der E-Mail eines Onlineshops anklickte: Sein Internetbrowser zeigte nicht nur die Lieferadresse seines eigenen Pakets, sondern auch noch die Adressen zweier weiterer DHL-Kunden. Auch bekam er zu sehen, wann die Personen genau ihr Paket entgegengenommen haben, also zu Hause waren.

Der promovierte Computerexperte schrieb ein kleines Programm, ein so genanntes Shellskript, und extrahierte mit zufälligen Paketnummern in Sekunden Hunderte weitere Adressen. Das war so leicht, weil der Link in der Mail das unverschlüsselte Passwort "PUBLIC" enthielt. Für jeden Sicherheitsexperten sind Klartextpasswörter ein überflüssiges Risiko, diese in eine Internetadresse zu packen gilt als fahrlässig.

Privatadressen ungeschützt

Alle so gefundenen Adressen gehörten Kunden eines Versenders - dem, von dem auch Linux-Magazin-Autor Eggendorfer sein Paket empfangen hatte. Mit einem weiteren Linux-Skript konnte er sogar die Zugangsdaten mehrerer hundert weiterer Versender identifizieren und deren Kunden ermitteln, denn auch diese Firmen benutzen das identische Passwort, offenbar ein von DHL vergebenes Standardpasswort. DHL fragt an dieser Stelle keine Daten ab, die nur Absender und Empfänger kennen, beispielsweise die Postleitzahl.

Die Folge: Jeder technisch halbwegs versierte PC-Nutzer kann nach dem Erhalt einer E-Mail auf die im Linux-Magazin 12/2008 geschilderte Weise die Daten anderer Kunden ausspionieren, sofern sein Shopbetreiber das DHL-Passwort nicht geändert hat - was offenbar Gang und Gäbe ist. Das wäre zum Beispiel bei Erotikartikel-Versendern oder Internet-Apotheken für die Betroffenen nicht nur unangenehm, sondern könnte Halunken eine profitable Datenbasis für erpresserische Aktivitäten bilden. Auch Adresshändler könnten sich so aus dem DHL-Adressbestand Listen erzeugen, die in der Vergangenheit bei Versendern bestimmter Produktsegmente eingekauft haben.

Die Reaktion von DHL

Das Linux-Magazin informierte DHL vor Veröffentlichung des Artikels in Ausgabe 12/2008. In einer Stellungnahme bestreitet das Unternehmen zunächst das Vorhandensein einer Sicherheitslücke. Viel mehr liege "ein 'Versehen' des Shopbetreibers vor, indem er seinem Käufer einen Zugriff auf seine interne Sendungsverwaltung zur Verfügung gestellt hat."

Dass solche "Versehen" keine Einzelfälle sind und seine Systeme die eigentliche Ursache des Problems bilden, scheint der Logistikkonzern jedoch zu ahnen. Denn die Stellungnahme schließt mit: "Zum Schutz unserer Kunden ist zur Drucklegung [des Linux-Magazins] eine Benachrichtigung erfolgt [...]. Weiterhin wird diese Funktion zur internen Sendungsverwaltung deaktiviert sein." Die Details zu dem Vorfall veröffentlicht das Linux-Magazin aus dem Linux New Media Verlag in Ausgabe 12/2008, die am 6. November erscheint.

Über Linux New Media AG

Linux New Media AG, gegründet 1999, ist heute der weltweit größte Content Provider rund um Linux und Open-Source-Software. Der Verlag gibt mehr als 30 Print- und Online-Publikationen heraus und betreibt Niederlassungen in sechs Ländern. Neben deutschen Titeln wie Linux-Magazin, Technical Review, LinuxUser und EasyLinux produziert die Linux New Media AG eigenständige Ausgaben in Spanien, Großbritannien, USA, Polen und Brasilien. Die Linux New Media AG organisiert Veranstaltungen und Messeplattformen wie z.B. „CeBIT Open Source“ oder die „Veranstaltungsreihe „LinuxPark“ in Brasilien. Weitere Informationen finden Sie unter http://www.linuxnewmedia.de.

Kontakt:

Linux New Media AG

Jan Kleinert

jkleinert@linux-magazin.de

Phone: +49 89 9934 1166

Putzbrunner Straße 71
81739 München