



Sie sind hier: [Startseite](#) [Presse](#) **Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen**

Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen

16 Millionen Digitale Identitäten betroffen

Bonn, 21.01.2014.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat angesichts eines Falles von großflächigem Identitätsdiebstahl unter <https://www.sicherheitstest.bsi.de> [<https://www.sicherheitstest.bsi.de>] eine Webseite eingerichtet, auf der Bürgerinnen und Bürger überprüfen können, ob sie von diesem Identitätsdiebstahl betroffen sind. Im Rahmen der Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden wurden rund 16 Millionen kompromittierte Benutzerkonten entdeckt. Diese bestehen in der Regel aus einem Benutzernamen in Form einer E-Mail-Adresse und einem Passwort. Viele Internetnutzer verwenden diese Login-Daten nicht nur für das eigene Mail-Account, sondern auch für Benutzerkonten bei Internetdiensten, Online-Shops oder Sozialen Netzwerken. Die E-Mail-Adressen wurden dem BSI übergeben, damit Betroffene informiert werden und erforderliche Schutzmaßnahmen treffen können.

Auf der Webseite <https://www.sicherheitstest.bsi.de> [<https://www.sicherheitstest.bsi.de>], die das BSI mit Unterstützung der Deutschen Telekom eingerichtet hat, können Internetnutzer ihre E-Mail-Adresse eingeben, um zu überprüfen, ob sie von dem Identitätsdiebstahl betroffen sind. Die eingegebene Adresse wird dann in einem technischen Verfahren vom BSI mit den Daten aus den Botnetzen abgeglichen. Ist die Adresse und damit auch die Digitale Identität des Nutzers betroffen, so erhält dieser eine entsprechende Information per E-Mail an die angegebene Adresse. Diese Antwort-Mail enthält auch Empfehlungen zu erforderlichen Schutzmaßnahmen. Ist die eingegebene E-Mail-Adresse nicht betroffen, so erhält der Nutzer keine Benachrichtigung.

Betroffene sollten Rechner säubern und Passwörter ändern

Betroffene Internetnutzer sollten in jedem Falle zwei Maßnahmen ergreifen:

1. Der eigene Rechner ebenso wie andere genutzte Rechner sollten auf Befehl mit Schadsoftware überprüft werden. In den Empfehlungen des BSI zur sicheren Konfiguration von Windows-PCs ist eine Auswahl an geeigneten Virenschutzprogrammen aufgeführt, die hierfür genutzt werden können.
2. Anwender sollten alle Passwörter ändern, die sie zur Anmeldung bei Sozialen Netzwerken, Online-Shops, E-Mail-Accounts und anderen Online-Diensten nutzen. Es sollten auch diejenigen Passwörter geändert werden, die nicht zusammen mit der betroffenen E-Mail-Adresse als Login genutzt werden. Dies ist deshalb empfehlenswert, weil im Falle einer Betroffenheit die Möglichkeit besteht, dass ein benutzter Rechner mit einer Schadsoftware infiziert ist. Diese kann neben den in den Botnetzen aufgetauchten Benutzerkennungen auch andere Zugangsdaten, Passwörter oder sonstige Informationen des Nutzers ausgespäht haben. Hinweise zur Nutzung sicherer Passwörter erhalten Anwender unter <https://www.bsi-fuer-buerger.de/Passwoerter> [https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html]

Identitätsdiebstahl gehört zu den Top-Gefährdungen im Internet

Identitätsdiebstahl ist eines der größten Risiken bei der Internetnutzung. Online-Kriminelle stehlen die digitalen Identitäten von Internetnutzern, um in deren Namen aufzutreten, E-Mails zu versenden, auf fremde Kosten in einem Online-Shop einzukaufen oder sich auf andere Weise zu bereichern oder den Betroffenen zu schaden. Personenbezogene Anwendungen wie E-Mail- oder Messenger-Dienste, Online-Shops oder Soziale Netzwerke bieten personalisierte Services, für die man sich anmelden muss, um seine Daten zu erhalten oder die Dienstleistung in Anspruch nehmen zu können. Zur Authentisierung wird in den meisten Fällen immer noch die Kombination aus

Benutzername und Passwort genutzt. Geraten diese Authentisierungsmerkmale in die falschen Hände, können sie für Identitätsmissbrauch verwendet werden.

Meist geschieht dies durch eine Schadsoftware-Infektion des genutzten Internet-Rechners. Die Schadprogramme werden unbemerkt auf den Rechnern der Anwender platziert, um beispielsweise Tastatureingaben und Anmeldevorgänge zu protokollieren oder Transaktionen direkt zu manipulieren. Die protokollierten Daten werden dann vom Nutzer unbemerkt an speziell vom Angreifer dafür präparierte Rechner im Internet ("Dropzones") gesendet, von wo sie von den Tätern heruntergeladen und missbraucht werden können.

Pressekontakt:

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200363

53133 Bonn

Telefon: 0228 99 9582-5777

+49 228 99 9582-5777

Telefax: 0228 99 9582-5455

+49 228 99 9582-5455

E-Mail: presse@bsi.bund.de

© Bundesamt für Sicherheit in der Informationstechnik. All rights reserved