BSI bietet Sicherheitstest für E-Mail-Adressen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat angesichts eines Falles von großflächigem Identitätsdiebstahl unter *https://www.sicherheitstest.bsi.de* am 21.01.2014 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*, 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 Befall 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*

IT-Sicherheit im Arbeitsrecht/TeleTrusT – Bundesverband IT-Sicherheit e.V. informiert am 15.04.2014 in Berlin

Der Einsatz von Informationstechnologie und IT-Sicherheitsanforderungen haben für Arbeitsgeber und Beschäftigte zahlreiche arbeitsrechtliche Implikationen. Rechtsetzung und Rechtsprechung folgen dabei mit Mühe der dynamischen technischen Entwicklung. In der Praxis verbleiben Fallstricke, deren Kenntnis hilft, Probleme bereits in Vorfeld zu vermeiden. Bei Arbeitgebern und Mitarbeitern besteht oftmals Unklarheit über wechselseitige Rechte und Pflichten. TeleTrusT informiert im Rahmen einer Veranstaltung über aktuelle arbeitsrechtliche Probleme und praktische Lösungsansätze. Spezialisierte und praxiserfahrene IT-Rechtsanwälte widmen sich aus arbeitsrechtlicher Sicht ausgewählten Themen:

- RA Matthias Hartmann, HK2 Rechtsanwälte:
  "Bring your own device & Derivate"
- RA Prof. Dr. Lambert Grosskopf, Kanzlei Grosskopf:
  „Biometrie in der Arbeitswelt"
- RA Dr. Carsten Ulbricht, Diem & Partner:
  „Social Media im Arbeitsverhältnis"
- RA Dr. Jan K. Köcher, DFN-CERT:
  „Rechtliche Absicherung von Administratoren"
- RA Karsten U. Bartels, LL.M., HK2 Rechtsanwälte :
  „Sicherheit in Cloud-Diensten"
- RA Dr. Axel von dem Bussche, Taylor Wessing:
  „Mitarbeiter-Datenschutz nach EU-Datenschutz-Grundverordnung"

Die Veranstaltung richtet sich an Interessierte, die mit einschlägigen Rechtsfragen befasst sind, an klein- und mittelständische Unternehmen und Organisationen – insbesondere ohne eigene Rechtsabteilung – sowie an Arbeitnehmervertreter.

Programm und Anmeldung unter: *https://www.teletrust.de/veranstaltungen/arbeitsrecht/*

D-TRUST schließt sich der FIDO-Allianz an

D-TRUST, das akkreditierte Trustcenter der Bundesdruckerei GmbH, ist seit dem 21.01.2014 das 50. Mitglied der Vereinigung FIDO (Fast IDentity Online, *http://www.fidoalliance.org/*). Die von Google und PayPal gegründete Initiative hat das Ziel, das übliche Anmeldeverfahren mit Benutzername und Passwort durch neue Sicherheitskonzepte abzulösen. Auf dem Branchenkongress Omnicard 2014 hat D-TRUST das neue Authentifizierungsverfahren, das die Sicherheit bei der Anmeldung im Netz erhöht und um sichere Identitäten ergänzt, vorgestellt.

Sichere Identitäten sind das Schlüsselthema im 21. Jahrhundert. Im Zeitalter des Internets und der weltweiten Mobilität ist es zu einer anspruchsvollen Aufgabe geworden, persönliche Daten, E-Mail-Accounts und Identitäten zu schützen. Die Bundesdruckerei ist führend bei innovativen Lösungen rund um die „Sichere Identität". D-TRUST, das Trustcenter der Bundesdruckerei, ist der branchen- und technologieübergreifenden FIDO-Allianz beigetreten und arbeitet gemeinsam mit Mitgliedern wie Google, PayPal und Microsoft an der Weiterentwicklung von Passwort-Verfahren. Millionenfach gestohlene Passwörter und gehackte E-Mail- und Nutzer-Accounts machen deutlich, dass das Verwenden eines Passworts längst nicht mehr genügt, um persönliche Daten ausreichend zu schützen. Die FIDO-Allianz hat das Ziel, einen neuen Standard zu etablieren, der das Sicherheitslevel des üblichen Benutzername-Passwort-Verfahrens deutlich erhöht, dabei aber genauso einfach und benutzerfreundlich anzuwenden ist. Bei der sogenannten „Universal Second Factor" (U2F) Authentifizierung kommt zusätzlich zum Passwort ein Token zum Einsatz, beispielweise ein USB-Sicherheitsstick für den Computer oder die kontaktlose NFC-Smartcard für die mobile Nutzung via Handy und Tablet. Der Nutzer gibt wie gewohnt sein Passwort ein, weist sich aber zudem durch den Besitz des Tokens aus, den er per USB anschließt oder via NFC überträgt.