International Working Group
on Data Protection
In Telecommunications

675.39.21

Arbeitspapier zu Risiken für die Privatsphäre im Zusammenhang mit der Wiederverwendung von Email-Accounts und ähnlichen Diensten der Informationsgesellschaft

-Übersetzung-

46. Sitzung, 7.-8. September 2009, Berlin (überarbeitet und aktualisiert auf der 47. Sitzung, 15.-16. April 2010, Granada (Spanien))

Einleitung

Für viele Menschen sind Emails das primäre Kommunikationsmittel geworden, das traditionelle Briefe sowohl für private als auch für geschäftliche Zwecke ersetzt. Bei einem Email-Account, der eine Person identifizieren und für private Kommunikation genutzt werden kann, handelt es sich nach allgemeiner Auffassung der Datenschutzbehörden um personenbezogene Daten.

Eine Person kann einen oder mehrere Email-Accounts haben, die über einen kostenlosen oder kostenpflichtigen Dienst angeboten werden; einem Angestellten kann es auch von seinem Arbeitgeber gestattet sein, eine geschäftliche Email-Adresse für private Zwecke zu nutzen. Email-Accounts, die scheinbar umsonst zu haben sind, können mit anderen Informationsdiensten, wie Breitbanddiensten und Kabelfernsehen gebündelt sein.

Was also geschieht, wenn eine Person ihren Email-Anbieter wechseln muss?

Die Analogie in der realen Welt besteht darin, aus einem Haus in ein anderes umzuziehen. Gewöhnlicherweise schicken Personen, die umziehen, Briefe an alle ihre geschäftlichen und privaten Kontakte, um diese über den Umzug zu informieren. Darüber hinaus wird die Person in der Regel mit dem Post-Zusteller vereinbaren, dass alle Briefe an die neue Adresse weitergeleitet werden – heutzutage keine einfache Angelegenheit, da viele Postzustellungsunternehmen eingebunden sein können. Die Lösung kann darin bestehen, den neuen Bewohnern für die verbleibende Post Etiketten mit der neuen Anschrift zu geben.

Wenn wir diese Analogie aus der echten Welt in die virtuelle Welt übertragen, müssen wir alle Dienste der Informationsgesellschaft in Betracht ziehen, die es mit sich bringen, eine

Person anhand des Namens zu identifizieren. Dies kann die zunehmend beliebten sozialen Netzwerke umfassen und auch Accounts bei virtuellen Marktplätzen, die eine Email-Adresse zu Zwecken der Validierung nutzen und an die elektronische Güter und Belege etc. gesendet werden können. Dasselbe Problem könnte sich auch im Fall des Verschickens von SMS im Zusammenhang mit Mobiltelefonen ergeben.

Wechsel einer Email-Adresse oder eines Accounts bei Diensten der Informationsgesellschaft

Wenn eine Email-Adresse oder ein virtueller Account geschlossen wird, besteht die Möglichkeit, dass ein neuer Nutzer den Benutzernamen wieder benutzen und dessen „Vergangenheit erben" könnte. Diese Möglichkeit ist im Fall von kostenlosen „email-for-life"-Diensten (sowie bei gmail oder hotmail) ziemlich abwegig, da solche Anbieter kaum abgelaufene Accounts neu verteilen würden.

Außer wenn der Nutzer für eine Domain gezahlt hat, wird der Domain-Name aller Wahrscheinlichkeit nach mit dem Service-Provider verbunden und nicht von einem auf den anderen Anbieter übertragbar sein.

Beispielhaft muss man sich jemanden vorstellen, der einen sehr gebräuchlichen Namen hat, wie „Joe Doe", der in Portugal lebt, gmail benutzt, sich bei einem Kabelfernsehkanal anmeldet und für eine Firma namens Xpto arbeitet; Joe könnte mehrere Email-Accounts haben, wie z.B. **joedoe99@gmail.com**, **joedoe@cabletv.pt**, **joedoe@xpto.pt**. Zusätzlich könnte er eine persönliche Domain für seine Familie gekauft haben oder nutzen wie **doe.pt** und die Email-Adresse **joe@doe.pt** benutzen.

Wenn er seinen gmail-Account aufgeben möchte, kann er ziemlich sicher sein, dass sein Account **joe.doe99@gmail.com** nicht wieder vergeben wird, aber wenn er das Abonnement für das Kabelfernsehen beendet oder seinen Arbeitsplatz wechselt, dann wird er vielleicht entdecken, dass er nicht mehr in der Lage ist, auf seine Emails über die Accounts **joedoe@cabletv.pt** oder **joedoe@xpto.pt** zuzugreifen.

Auf der anderen Seite sollte die Domain **doe.pt** nicht ohne Weiteres auf einen anderen übertragbar sein, vorausgesetzt, seine Familie zahlt weiter dafür.

Wenn dagegen sein früherer Kabelfernsehanbieter einen neuen Kunden hat und sein früherer Arbeitgeber einen neuen Angestellten, der auch Joe Doe heißt, könnten sie

entscheiden, seine alte Email-Adresse an diese neue Person zu vergeben. In diesem Fall wird der neue „Inhaber“ wohl Email-Nachrichten und persönliche Information „erhalten“, die an den ursprünglichen Inhaber gerichtet waren.

In gleicher Weise kann jeder neue Besitzer einer wieder vergebenen Domain, bei der die Bezahlung ausgelaufen ist, Email-Verkehr erhalten, der an den früheren Besitzer gerichtet ist.

Mögliche negative Folgen

Dies kann zahlreiche negative Folgen haben:

- Wenn der Nutzer Abonnements für Email-Newsletter nicht kündigt oder nicht alle Kontakte über den Wechsel seiner Adresse informiert hat, wird der neue Besitzer Informationen erhalten, die für den früheren Besitzer bestimmt sind, was zur Preisgabe personenbezogener Daten führt;
- Wenn ein Nutzer die „Passwort-vergessen“-Option eines Dritten nutzt, bei dem er sich unter der alten e-mail-Adresse registriert hat, würde der neue Besitzer seinen Nutzernamen und das Passwort für diese website erhalten;
- Wenn ein Beschäftigter seine Arbeitsstelle verlässt, könnte der neue Beschäftigte persönliche Nachrichten erhalten, die für den ehemaligen Beschäftigten bestimmt sind, sowie auch geschäftliche Emails für denjenigen, der den ehemaligen Beschäftigten ersetzt hat;
- Wenn der Vertrag mit einem Internet-Service-Provider beendet wird, könnte sich der neue Kunde versehentlich oder absichtlich als der ehemalige Inhaber der Email-Adresse ausgeben.

Ähnliche Erwägungen sind auf andere Dienste der Informationsgesellschaft anwendbar, wie z. B. Instant Messaging, VoIP/Internettelefonie und soziale Netzwerke, besonders wenn die Email-Adresse zur Authentifizierung genutzt wird. Wenn ein Benutzer einen Dienst beenden möchte, kann der neue Benutzer Nachrichten empfangen, die für den ehemaligen Nutzer bestimmt sind, oder – was schwerwiegender ist – versuchen, als der alte Benutzer aufzutreten.

Während die mobile Rufnummernmitnahme (mobile number portability – MNP), die Möglichkeit des Auftretens dieses Problems im Zusammenhang mit Mobiltelefonen reduzieren kann, mag die Möglichkeit zur Rufnummernmitnahme nicht immer verfügbar sein

(z.B. im Fall von mangelndem Bewusstsein, Umzug in ein anderes Land, Tod des Nutzers oder bei manchen Formen von „pay-as-you-go“-Diensten). Dann besteht wieder die Möglichkeit, dass jemand anders eine kürzlich verwendete Rufnummer und das damit verbundene Erbe an SMS-Nachrichten übernimmt.

Dies ist deshalb besonders problematisch, weil SMS in der Regel in besonders vertraulichen Bereichen wie Online-Banking und E-Ticketing verwendet werden.

Obwohl die Portabiliät von Mobilfunknummern geholfen hat, diese Probleme zu behandeln, könnte der Benutzer das Gefühl haben, dass er seine Email-Adresse oder die Nummer seines Mobiltelefons, einen bestimmten Internet-Service-Provider oder Mobilfunkanbieter für immer behalten muss, um seine Privatsphäre und persönliche Sicherheit zu wahren.

Empfehlungen

Die Arbeitsgruppe hat sich schon früher mit Aspekten des Schutzes der Privatsphäre und der Sicherheit im Zusammenhang mit Telekommunikationsdiensten[1], Internetdiensten[2] und sozialen Netzwerken[3] beschäftigt.

Die Arbeitsgruppe ist der Auffassung, dass ein Anbieter von Diensten der Informationsgesellschaft (im Folgenden als „ISP“ bezeichnet) Dienste anbieten sollte, die es dem Nutzer ermöglichen, jede schädigende Konsequenz, die aus der Kündigung des Vertrages resultieren könnte, zu minimieren, und gibt folgende Empfehlungen:

1. Der ISP sollte eine Übergangsphase von mindestens drei Monaten vorsehen, bevor irgendjemand die Email-Adresse, persönliche Domain oder Telefonnummer eines vormaligen Nutzers übernehmen kann.
2. Der ISP sollte dem Nutzer eine Möglichkeit bieten, dass für die Dauer der Übergangsphase Nachrichten, die an die ausgesetzte Email-Adresse oder Nummer geschickt werden, zusammen mit einer passenden automatisierten Nachricht zurückgesandt werden.
3. Der ISP sollte einen Warnhinweis anbieten, der den Nutzer über das mit dem Ende des Vertrags verbundene Risiko, seine Email-Adresse zu verlieren, informiert sowie über die mögliche Preisgabe von Daten.
4. Der ISP könnte eine Funktion wie einen „wandernden“ Ordner anbieten, in dem der Nutzer die Login-Daten speichern könnte, die für Web-Dienste verwendet werden, bei denen er sich unter Nutzung seiner e-mail-Adresse oder Mobilfunknummer registriert

hat. Wenn der Account geschlossen oder der Vertrag beendet wird, könnte er den Ordner zu einem anderen Dienst mitnehmen, oder er hätte wenigstens eine Liste aller Dienste Dritter, mit denen seine e-mail-Adresse oder Mobilfunknummer verbunden ist, und könnte die e-mail-Adresse oder Mobilfunknummer dort ändern. Dies würde erfordern, dass der Nutzer solche Informationen stets aktualisiert.

5. Dienste, die eine SMS-Authentifizierung verwenden (z.B. Online-Banking), sollten die Mobiltelefonnummer anzeigen, an die die Nachricht verschickt wurde. Wenn der Dienst innerhalb eines gewissen Zeitraumes keine Rückmeldung von dem Nutzer erhält, dass die Transaktion fortgeführt werden soll, sollte die betreffende Nummer als gefährdet eingestuft und so lange ausgesetzt werden, bis der Inhaber der Accounts erneut die Nummer des zu verwendenden Mobiltelefons bestätigt.
6. Im Falle von SMS-Premium- oder ähnlichen Diensten sollte von dem Diensteanbieter von Zeit zu Zeit eine kostenlose Nachricht versandt werden, um festzustellen, ob der Nutzer diesen Dienst weiter in Anspruch nehmen will. Im Falle eines Bankkontos kann dies zum Beispiel durch die Einführung eines Berechtigungsmerkmals bestätigt werden, das nur der wirkliche Nutzer kennt und auf das nur er Zugriff hat.
7. Einzelpersonen (Arbeitnehmer) sollten für das Abonnement oder die Registrierung von Diensten privater Natur, wie mailing-Listen, e-shops, soziale Netzwerke, etc. keine e-mail-Adressen verwenden, die Anderen zugewiesen werden könnten (z.B. geschäftliche e-mail-Adressen).
8. Eine Person, die eine permanente Email-Adresse haben möchte, sollte einen persönlichen Domain-Namen registrieren, der auch als Homepage, Weblog etc. genutzt werden kann. Allerdings erfordert eine persönliche Domain in der Regel eine jährliche Erneuerung, anderenfalls kann sie verloren gehen und an eine andere Person vergeben werden.
9. Arbeitgeber und andere Organisationen, die geschäftliche Email-Adressen verteilen, sollten den Mechanismus festlegen, der eingreift, wenn ein Mitarbeiter geht oder seine Funktion innerhalb des Unternehmens wechselt. Nachrichten an eine solche Adresse sollten zurückgesandt werden, oder es sollte eine automatisierte Nachricht verschickt werden, sodass der Absender weiß, dass die Adresse des Angestellten sich geändert hat oder nicht mehr besteht. Es wird empfohlen, Bezeichnungen für persönliche e-mail-Adressen nicht wiederzuverwenden, wenn diese bereits ehemaligen Beschäftigten zugewiesen waren.

[1] Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz (Berlin 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

[2] Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP) (Berlin 5/6.09.2006); http://www.datenschutz-berlin.de/attachments/101/WP_VoIP_de.pdf?1201702122

[3] Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten - Rom Memorandum - (Rom 3/4.03.2008); http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf?1234867489