Social Hacking

07.11.2006, 17:18 | Politik, Recht & Gesellschaft

Pressemitteilung von: *Zorn Reich Wypchol, Rechtsanwälte in Sozietät*

Zeigen Sie Ihrem Problem die rote Karte!

Unsichere Freemail-Konten

Untersuchungen ergab, dass eine Vielzahl von Geschäftsleuten Freemail -Anbieter für ihre geschäftliche E-Mail-Korrepondenz nutzen. In Feldversuchen stellten Sicherheitsberater anschließend unter Beweis, dass zahlreiche Freemail-Konten innerhalb weniger Minuten mit einfachen Mitteln zu knacken sind.
Diese Tests wurden ausschließlich auf Methoden beschränkt, die keinerlei Spezialwissen erfordern und praktisch von jedem durchführbar sind. Die Ergebnisse dieser Tests sind alarmierend: E-Mail-Konten bei namhaften Anbietern konnten in weniger als zehn Minuten gehackt werden. Sind zu dem Konteninhaber nur einige wenige Informationen bekannt, reduzierte sich der Zeitaufwand oft auf weniger als fünf Minuten.

Die Folgen eines erfolgreichen Einbruchs sind für den Betroffenen in den allermeisten Fällen gravierend. Der Eindringling kann alle eingegangenen Mails lesen. Es ist ihm möglich, in die Privatsphäre des Konteninhabers einzudringen und beispielsweise firmeninterne Informationen zu erhalten, die mit Mails auf oder über dieses Konto gesendet wurden. Der Eindringling kann alle Funktionen des Mail-Kontos uneingeschränkt nutzen und so auch eingegangene Mails löschen oder verändern, ehe der Konteninhaber sie gelesen hat. Das bedeuten, dass der Konteninhaber wichtige Mails entweder gar nicht erhält oder die Mails einen falschen, veränderten Inhalt haben.

Ein unbefugter Eindringling in ein Mail-Konto kann im Namen und mit der Absenderadresse des Konteninhabers Mails versenden, die nicht als Fälschung zu erkennen sind. Der Eindringling kann sogar das Passwort ändern und so dem Konteninhaber am Abholen seiner E-Mails beziehungsweise am Senden von E-Mails hindern. Ist man beruflich auf E-Mails angewiesen, kann damit ein empfindlicher Schaden zugefügt werden.

Missbräuchliche Handlungen lassen sich sogar automatisieren. Der Einbrecher kann beispielsweise hinterlegen, dass von jeder ein- und ausgehenden Mail eine Kopie an ein anderes E-Mail-Konto - nämlich das des Eindringlings - zu senden ist. Der Effekt ist, dass sich der Eindringling nie wieder in das betreffende Konto einhacken muss, da er jede Mail, die über dieses Konto geht, zugleich auch automatisch auf sein eigenes E-Mail-Konto geschickt bekommt. Das funktioniert so lange, bis der Inhaber des betreffenden Kontos den Weiterleitungseintrag in den Grundeinstellungen bemerkt und löscht.

Das Diensteangebot einiger E-Mail-Anbieter, die auch Funktionen wie Telefon- und Adressbuchverwaltung, einen persönlichen Kalender und anderes mehr zur Verfügung stellen, birg zusätzliche Gefahr. Die Schäden, die einem Nutzer solcher Funktionen durch ein unbefugtes Eindringen in sein Account entstehen können, sind kaum absehbar.

Neben technischen Sicherheitslücken in Freemail-Systemen, die es Angreifern ermöglichen, ohne Authentisierung auf das System zuzugreifen, ist die Methode des sogenannten „Social Hacking“, des Erratens der Zugangsdaten, durchaus vielversprechend. Um auf diesem Weg unbefugten Zugang zu einem Mail-Konto zu erlangen, benötigt ein Eindringling entweder den Account-Namen oder die komplette E-Mail-Adresse des Opfers. Daten, die leicht zu besorgen sind. Aus nachvollziehbaren Gründen wird auf eine detaillierte Darstellung der Verfahrensmodalitäten wie man sich sodann in ein Email-Konto unbefugterweise einhackt wegen der offensichtlichen Gefahr der Nachahmung verzichtet.
Nur soviel – schwer ist es nicht!

Als Gegenmaßnahmen empfiehlt es sich einen Freemail-Anbieter zu wählen, der keine beliebig vielen Fehl-Log-ins zulässt, ohne das E-Mail-Konto zu sperren. Eine andere Möglichkeit für Anbieter, solche Attacken zu verhindern, besteht darin, dass zwischen jedem Fehl-Log-in eine immer längere Wartezeit notwendig ist, bis der nächste Log-in erfolgen kann. Wegen der immer größeren Wartezeiten würde eine sogenannte Brute-Force-Attacke so lange dauern, dass sie praktisch undurchführbar ist. Und eine dritte, ebenfalls einfache Möglichkeit für den Freemail-Anbieter besteht darin, dem Konteninhaber nach dem Log-in anzuzeigen, ob Fehl-Log-ins erfolgten. Werden einem Konteninhaber solche Fehl-Log-ins angezeigt, dann weiß er zumindest, dass jemand (erfolgreich oder erfolglos) versucht hat, in sein Konto einzudringen.

Ein Passwort ist umso schwerer zu erraten, je länger es ist.
Für Passwörter bis zu einer Länge von vier bis fünf Zeichen braucht ein Angreifer kaum themenbezogene Wortlisten, sondern kann ein leistungsfähiges Brute-Force-Programm einfach alle möglichen Worte dieser Länge durchprobieren lassen. Passworte mit einer Länge von acht und mehr Zeichen sind auf diese Weise auch mit sehr leistungsfähigen Computern nicht mehr zu ermitteln. Sicherer ist ein Freemail-Anbieter, der eine Passwortlänge von mindestens acht Zeichen zwingend festlegen. Gleiches gilt für die möglichen Zeichen. Je mehr Zeichen für ein Passwort verwendet werden können, umso mehr mögliche Passworte einer bestimmten Länge gibt es. Während ein Hacker beispielsweise ein sechsstelliges Passwort, in dem nur Kleinbuchstaben vorkommen dürfen, noch relativ einfach ermitteln kann, ist das Hacken eines Passworts, in dem Klein- und Großbuchstaben, Ziffern und 20 Sonderzeichen vorkommen können, praktisch unmöglich.

Kritisch sind Anbieter zu bewerten, die beim vergessen des Passwortes eine „geheime Frage“ stellen, bei deren Beantwortung das Passwort freigegeben wird.

Auch hier wird auf eine detaillierte Darstellung der Verfahrensmodalitäten wie man sich sodann in ein Email-Konto unbefugterweise einhackt wegen der offensichtlichen Gefahr der Nachahmung verzichtet.

Nutzern von Freemail-Diensten sowie sollte es bewusst sein, dass diese Konten oft leicht zu knacken sind. Es empfiehlt es sich, bei der Auswahl eines Freemail-Dienstes neben den dort angebotenen Features auch die Sicherheitsvorkehrungen mit in die Auswahl einzubeziehen.

Der firmeninterne Zugriff auf diese Dienste sollte in jedem Fall verboten werden.
Hiezu sollte das Verbot mit den Mitarbeiter erörtert werden und diese sollten schriftlich bestätigen das Verbot zur Kenntnis genommen zu haben.

Technisch sind alle bekannten URLs für den Zugriff aus dem Firmennetz zu sperren.

Eine Maßnahme, die insbesondere unter dem Gesichtspunkt, dass über das gehackte E-Mail-Konto Straftaten begangen werden können, besonderes Augenmerk verdient.

Zorn Reich Wypchol, Rechtsanwaelte in Sozietät
Wetzlarer Straße 95
35398 Gießen

Tel:0641/202121
Fax:0641/28730
reich@anwaelte-giessen.de
http://www.anwaelte-giessen.de

Portrait

Rechtsanwalt Jörg Reich berät zusätzlich im Bereich Kapitalanlagerecht, Anlegerschutz, Bankenrecht und Börsenrecht.
Er vertritt erfolgreich die Rechte geprellter Anleger (Schrottimmobilie, Immobilienfonds, Grauer Kapitalmarkt).
Er verfügt über internationale Erfahrung (Asien: China, Korea, Vietnam, Afrika: Namibia, Süd Afrika, Amerika: USA (Ostküste)) und ist, unter anderem, Ihr Ansprechpartner für unsere Kooperation in Athen, Griechenland.
Herr Rechtsanwalt Edgar Zorn bildet neben seinem weitreichendem lokalen Netzwerk (Frankfurt, Gießen, Limburg, Marburg, Wetzlar) das feste Bindeglied zu unserer Kooperation in Palma de Mallorca.
Hier werden Kunden insbesondere in Bezug auf Immobilienerwerb und Anlageinvestitionen auf Mallorca sowie in Spanien insgesamt beraten.
Neben weiteren Sprachen beraten wir durch Frau Rechtsanwältin Beate Wypchol in polnischer Sprache. Frau Rechtsanwältin Beate Wypchol, die in Polen aufgewachsen ist, betreut im Team mit Herrn Rechtsanwalt Jörg Reich, im Rahmen unserer Kompetenzen, das Gebiet Osteuropa.
Rechtsberatung in Deutschland und vor Ort aus einer Hand!
Wir verstehen unsere Tätigkeit als moderne Dienstleistung auf höchstem Niveau und bemühen uns fortwährend, unsere Kompetenz und unser Know-how für unsere Mandanten auszubauen. Wir arbeiten eng mit weiteren Experten bundesweit und international zusammen.
Durch den intensiven Austausch unter den Anwälten unserer Kanzlei profitieren unsere Kunden zum einen von der Erfahrung von über 25 Jahren rechtsanwaltschaftlicher Tätigkeit und zum zweiten von der Aufgeschlossenheit gegenüber modernen online-gestützter Daten- und Recherchemethoden zu aktuellen Entscheidungen
Wir nehmen uns Zeit, sind für unsere Kunden direkt ansprechbar und bearbeiten die uns übertragenen Mandate forciert.

News-ID: 107115 • Views: 2643 (Stand: 03.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/107115/Social-Hacking.html