Cybergefahr: Handelsware Nutzerkonten

Die Sozialstiftung der Sparda-Bank Baden-Württemberg, ist gemeinsam mit dem Kultusministerium Baden-Württemberg, dem Verein Sicherheit im Internet e. V. und dem Landesmedienzentrum Baden-Württemberg, Veranstalter und Träger von SpardaSurfSafe. In Kooperation mit den IT-Sicherheitsexperten der 8com GmbH & Co. KG wurde ein Konzept entwickelt, das Schüler im Rahmen des Unterrichts im Umgang mit den Neuen Medien aufklärt. Aktuelle Geschehnisse im Cyberspace - Informationen, die nicht nur für Schüler nützlich sind.

Seit einiger Zeit taucht die E-Mail-Adresse tessa88@exploit.im regelmäßig im Zusammenhang mit größeren Datenpaketen auf, die im Darknet zum Kauf angeboten werden. Rund 360 Millionen MySpace-Konten, 100 Millionen Datensätze des russischen Social Networks VK.com und zuletzt 33 Millionen Twitter-Accounts hat der Hacker offenbar bereits zu barer Münze machen wollen. Enthalten sind im Fall von Twitter mindestens eine E-Mail-Adresse, der Benutzername und das Kennwort im Klartext. Darüber hinaus wird Tessa88 auch im Zusammenhang mit 100 Millionen erbeuteten LinkedIn-Datensätzen, die zum Verkauf stehen, genannt.

Doch wie konnten die Hacker an die Daten gelangen? Zumindest im aktuellen Fall von Twitter scheinen die Zugangsdaten nicht direkt bei dem Nachrichtendienst erbeutet worden zu sein. Besonders die Tatsache, dass die Kennwörter im Klartext verkauft wurden spricht dafür, dass in diesem Fall eine Malware der Übeltäter war, denn Twitter selbst verschlüsselt alle Kennwörter. Es wird vermutet, dass Millionen PCs infiziert sind und die Software jedes gespeicherte Kennwort aus Browsern wie Firefox oder Chrome abfischt und an den Hacker weiterleitet.

Wer wissen will, ob er selbst betroffen ist, kann sich auf der Seite Leaked Source informieren. Deren Betreiber suchen seit einigen Monaten nach Datenpaketen im Darknet und übertragen diese in eine durchsuchbare Datenbank. Jetzt ergab eine Auswertung der häufigsten Kennwörter, dass viele Nutzer immer noch viel zu einfache Kennwörter nutzen – und bei derzeit fast 2 Milliarden Datensätzen lässt sich daran durchaus eine Tendenz ablesen.

Götz Schartner vom Verein Sicherheit im Internet e. V., einem der Mitveranstalter von SpardaSurfSafe, zeigt sich besorgt:

> Wenn selbst vermeintliche Internetprofis wie Facebook-Gründer Mark Zuckerberg sich nicht an die Regeln der Kennwortsicherheit halten und einen offenbar eher laxen Umgang mit ihren Zugangsdaten pflegen – sein Twitter-Kennwort ist kürzlich gehackt worden und lautete angeblich schlicht ‚dadada' – scheint das Thema in den Köpfen noch nicht den gebührenden Stellenwert

einzunehmen. In unseren Vorträgen während der Kampagne SpardaSurfSafe stellen wir das auch leider immer wieder fest.“

Kennwörter stellen praktisch die vorderste Verteidigungslinie aller Online-Konten dar, angefangen von E-Mail-Accounts über die sozialen Netze bis hin zum Shopping im Netz oder sicherem Online-Banking. Wer hier schludert, gefährdet seine digitale Identität, seine Reputation und sein Bankkonto. Umso wichtiger ist die Einhaltung der wichtigsten Kennwortregeln:

1. Verwenden Sie für jeden Account ein eigenes Kennwort.Datenbanken können gehackt werden. Darüber hinaus verbreitet sich Spionage-Software immer weiter, die Kennwörter direkt aus dem Browser abfischt. Mit diesen gestohlenen Zugangsdaten versuchen die Kriminellen dann, sich auch bei anderen Internetanbietern einzuloggen. Wurde ein Kennwort mehrfach verwendet, führt diese Strategie zum Erfolg.

2. Verwenden Sie möglichst komplexe Kennwörter.Ein sicheres Kennwort ist niemals eine fortlaufende Zahlen- oder Buchstabenfolge, egal ob vorwärts oder rückwärts. Auch Wörter, Namen und Kfz-Kennzeichen sind nicht geeignet. Es sollte mindestens 10 Zeichen lang sein, große und kleine Buchstaben sowie Zahlen und Sonderzeichen enthalten.

3. Ändern Sie Ihr Kennwort regelmäßig oder wenn der Verdacht besteht, dass jemand außer Ihnen es kennt.

4. Behalten Sie niemals die voreingestellten Kennwörter, die Dienstanbieter Ihnen zuschicken.

„Natürlich sollte man sich die Kennwörter noch merken können. Es bringt ja nichts, wenn man jedes Mal beim Einloggen auf den ‚Kennwort vergessen?‘-Link klicken muss. Das führt nur zu Frustration und am Ende wieder dazu, dass man überall das gleiche Kennwort verwendet“, erklärt Götz Schartner. „Es gibt aber Mittel und Wege, wie man das vermeidet, beispielsweise indem man sich Sätze merkt und dabei nur die Anfangsbuchstaben der einzelnen Wörter benutzt. Zusätzlich kann man manche Buchstaben standardmäßig durch Sonderzeichen ersetzen und schon hat man ein komplexes und sicheres Kennwort.“

Ein Beispiel für diese Merktechnik: Der Satz „Ich fahre jeden Samstag und Sonntag mit meinem Fahrrad 20 Kilometer durch den Wald“ ergibt das Kennwort „1fj$&$mmF20KddW“. Dafür nimmt man jeweils nur die Anfangsbuchstaben jedes Wortes und nimmt folgende Ersetzungen vor: i=1, I=1, s=$, S=$, o=0, O=0 sowie „und“=&. Schartner erklärt:

Dabei spielt auch die Kennwortsicherheit eine Rolle und die Teilnehmer lernen, wie man sichere Kennwörter erstellt und mit welchen Techniken man sie sich merkt. Unsere Hoffnung ist, dass nach dem Programm keiner unserer Teilnehmer mehr Kennwörter wie ‚123321‘ oder ‚Passwortabc‘ nutzt und diesem Ziel kommen wir immer näher.“

Weitere Informationen finden Sie unter: www.spardasurfsafe-bw.de

Bild: © ra2 studio / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4943006/cybergefahr-handelsware-nutzerkonten/