

Phishing hat Hochkonjunktur

Passwörter von Privatpersonen und Firmen im Visier von Betrügern

Die Kriminalität hat sich in den vergangenen Jahren immer mehr ins Netz verlagert. Das Ergebnis: eine Flut von Cyberkriminalität. Ein besonders trickreiches Vorgehen ist dabei bekannt als Phishing.

Als Phishing werden Versuche bezeichnet, über gefälschte Internetadressen an die geheimen persönlichen Daten eines Internet-Benutzers zu gelangen. Der Begriff kommt aus dem Englischen und ist angelehnt an das englische Wort „fishing“, was für „Fischen“ oder „Angeln“ steht und meint konkret das Angeln von Passwörtern mit ausgelegten Ködern.

Phishing-Aktionen sind in aller Regel als kriminelle Handlungen einzustufen. Die Cyber Kriminellen setzen dazu oft auch Techniken des *Social Engineering* ein. Social Engineers versuchen über die zwischenmenschliche Manipulation und unter Vortäuschungen falscher Identitäten Daten oder geheime Informationen ihres Opfers auszuspielen.

So geben sich Phisher als vertrauenswürdige Personen oder Institutionen aus und versuchen, durch gefälschte elektronische Nachrichten an kritische Daten wie User Names und Passwörter zu gelangen. Beispielsweise imitieren und fälschen diese Cyber Kriminellen Mails von Banken, Kreditinstituten oder sozialen Einrichtungen täuschend echt und mit der Aufforderung, einem Link zu folgen, um so an lukrative und prekäre Daten für Online-Banking oder Kreditkarteninformationen zu gelangen. Dieser Link führt den Nutzer dann auf eine Phishing-Seite, die von der Originalseite nur schwer zu unterscheiden ist. Folgt der User der nachfolgenden Aufforderung zur Eingabe der Daten, werden diese Daten gespeichert und können von dem Phisher verwendet werden.

Der Nutzer ist dann beispielsweise im guten Glauben eine Online-Transaktion auf der Homepage seines Bankinstitutes zu tätigen und gibt vertrauensvoll seine Bankdaten und die TAN-Nummer ein. Da es sich bei der Landing Page aber nicht um die tatsächliche Homepage seiner Bank handelt, sondern um eine gut gestaltete Imitation, wird seine Transaktion in Wirklichkeit nicht entgegengenommen, d.h. die TAN ist in Wirklichkeit nicht verbraucht. Stattdessen werden diese Daten vom Phisher abgefangen, der damit dann eine Transaktion durchführen kann. Somit kann der kriminelle Phisher dem Opfer erheblichen finanziellen Schaden zufügen.

Für den Laien ohne entsprechende Aufklärung und Hintergrundinformationen ist es oftmals schwierig diese Phishing-Nachrichten als solche einzustufen.

Deshalb sind offizielle Dienste und Ämter als Informationsplattform umso wichtiger für alle Internetuser. In einer aktuellen Pressemitteilung vom 03.02.2010 veröffentlichte das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** einen Artikel über die neuesten Bedrohungen aus dem Internet inkl. Tipps, wie man den gerissenen Attacken der Kriminellen entgehen kann.

Hier ein Auszug der Meldung:

Phishing-Mails, mit denen Computerkriminelle PC-Nutzer auf gefälschte Internetseiten locken und Passwörter stehlen, sind an sich nicht neu. ...

Nicht nur Privatanwender stehen im Fokus der Kriminellen. Lukrativ ist Phishing auch im Unternehmensumfeld. Hier wird die Gefahr zunehmend größer, jedoch oft verkannt. „Das Gießkannen-Prinzip wird zwar noch praktiziert, im Trend liegen aber individualisierte Angriffe auf kleinere Zielgruppen“, sagt Matthias Gärtner, Pressesprecher des Bundesamts für Sicherheit in der Informationstechnik (BSI). ...

Was können Internetnutzer tun, um sich gegen Phishing-Angriffe zu schützen? Das BSI rät:

- Klicken Sie generell niemals auf in E-Mails enthaltene Links, sondern tippen Sie die Internetadressen gewünschter Seiten manuell ein oder nutzen im Browser gespeicherte Lesezeichen und überprüfen Sie nach dem Laden der Seite die URL erneut. Auch durch Tippfehler können Nutzer auf eine von Betrügern registrierte Webseite gelangen.
- Nutzen Sie starke Passwörter, wechseln Sie diese in regelmäßigen Abständen und verwenden Sie für unterschiedliche Online-Anwendungen unterschiedliche Kennwörter.
- Aktive Inhalte wie zum Beispiel Javascript werden oft zu Angriffszwecken missbraucht. Schalten Sie die Funktion "Aktive Inhalte ausführen" am besten generell aus und nur bei vertrauenswürdigen Webseiten bewusst wieder an.

Lesen Sie hier die vollständige Meldung des BSI:

https://www.bsi.bund.de/cln_165/sid_5BCF51441D7C98E1000A2C07B25D6571/ContentBSI/Presse/Pressemittellungen/Phishing_030210.html



Sie haben Fragen zu Social Networking, Phishing oder anderen Cyber Attacken? Unter 0621-728485-1000 berät sie unser kompetentes Vertriebsteam gerne über effizienten Schutz für Ihr Unternehmen. Oder nehmen Sie hier Kontakt mit uns auf!