Video: Mehr Sicherheit durch Fahrerassistenzsysteme >
< Die Strategie hängt vom Spielplan ab

Gefährlicher als Phishing?

Pharming-Angriffe bedrohen Rechner von Verbrauchern

Ziel des Pharming ist dasselbe wie beim Phishing: an Zugangsdaten kommen

Das Pharming ist eine relativ neue Form der Cyberkriminalität, die dem Phishing ähnelt: Eine schadhafte Internetadresse führt den ahnungslosen Nutzer auf eine manipulierte Webseite, wo anschließend seine Benutzerdaten abgegriffen werden. Verbraucherschützer gehen davon aus, dass sich Pharming sogar zu einer noch größeren Bedrohung für die Sicherheit im Netz entwickeln könnte als das Phishing. Tatjana Halm ist Rechtsanwältin und als Referatsleiterin des Bereichs „Markt und Recht“ bei der Verbraucherzentrale Bayern tätig. Sie erklärt, wo die besonderen Tücken der neuen Betrugsmasche liegen und welche Maßnahmen dabei helfen können, die Gefahren rechtzeitig abzuwenden.

Frau Halm, wie funktioniert das Pharming und wie unterscheidet es sich vom Phishing?

Sowohl beim Phishing als auch beim Pharming versuchen Betrüger, Passwörter und Geheimnummern von Internetnutzern abzugreifen. Beim Phishing geschieht das in der Regel über gefälschte E-Mails, die angeblich von Banken oder Firmen stammen. Sie fordern Nutzer dazu auf, über schadhafte Links Webseiten zu öffnen und dort ihre Benutzerdaten einzugeben. Beim Pharming ist das Besondere, dass man nicht per E-Mail angeschrieben wird. Stattdessen gelangt man über die eigenständige Eingabe einer Webseitenadresse (URL), etwa die meiner Hausbank, meines meistbesuchten Onlineshops oder Auktionshauses, auf eine nachgebaute Betrugsseite. Der Nutzer merkt davon üblicherweise nichts, weil die betrügerische Webseite genauso aussieht wie die Zielseite, die er eigentlich aufrufen wollte.

Nichtsahnend gibt er die geforderten Zugangsdaten ein, die anschließend von den Betrügern ausgelesen werden. Grundsätzlich kann man also sagen, dass Pharming eine Weiterentwicklung bzw. eine anspruchsvollere Variante des Phishing-Betrugs ist. Die Täter werden im Netz immer kreativer.

Seit wann grassiert die Betrugsmasche im Netz?

Das ist schwer zu sagen. Wir von der Verbraucherzentrale in Bayern haben keine Erkenntnisse darüber, wann es hierzulande oder bundesweit die ersten Fälle gegeben hat. In der Regel ist es bei solchen „neuen“ Betrugsphänomenen ja auch so, dass sie erst eine lange Zeit unbemerkt ausgeübt werden, bis die Polizei, Verbraucherschützer oder die Öffentlichkeit darauf aufmerksam werden. Von daher gehen wir davon aus, dass das Phänomen schon länger im Umlauf ist.

Woher stammt der Begriff? Die Bezeichnung „Pharming“ ist ein Kofferwort, das sich aus den Begriffen „Phishing“ und „Farming“ zusammensetzt. „Pharming“ wird verwendet, da die Betrüger eigene große Server-Farmen mit statischen IP-Adressen unterhalten, auf denen die gefälschten Webseiten abgelegt sind.

Was können die Betrüger mit den gestohlenen Benutzerdaten anstellen?

Sie auf vielfältige Art und Weise missbrauchen. Handelt es sich bei der nachgebauten Betrugsseite etwa um ein Auktionshaus, können sie unter der Benutzerkennung des Opfers zum Beispiel bei hochpreisigen Internetauktionen mitbieten. Im Fall eines betrügerischen Bankenportals oder gefälschten Onlineshops ist es möglich, dass die Täter das Girokonto des Nutzers unbemerkt leer räumen oder Kreditkartenabbuchungen tätigen.

Wie kann ich feststellen, dass ich auf einer gefälschten Webseite gelandet bin?

Auf den ersten Blick in der Regel leider gar nicht. Da die betrügerische Webseite der Originalseite so professionell nachempfunden ist, fällt das oft selbst sorgfältigen und routinierten Internetnutzern nicht auf. Man kann versuchen, bei der Adresseingabe von Webseiten immer besonders wachsam zu sein. Taucht bei der Weiterleitung auf die Seite zum Beispiel plötzlich eine andere Endung in der URL auf, kann das ein Indiz dafür sein, dass es sich nicht um die Originalseite handelt, die man aufrufen möchte. Das ist natürlich aufwendig und macht in der Praxis kaum jemand. Es gibt jedoch einige Anzeichen, bei denen ich nachträglich stutzig werden sollte. Wenn ich etwa feststelle, dass unter meinem Namen falsche Einkäufe getätigt worden sind oder ich Unstimmigkeiten auf meinem Konto oder Online-Account bemerke, ist es sehr wahrscheinlich, dass ein Identitätsdiebstahl stattgefunden hat. Hat man den Verdacht, dass vertrauliche Daten gestohlen wurden, ist es sinnvoll, sich seinen Rechner genauer anzuschauen. Denn damit Pharming funktioniert, muss vom Betrüger zuvor in der Regel ein Schadprogramm darauf aufgespielt worden sein, etwa über ein Virus oder einen Trojaner.

Welche Möglichkeiten haben Verbraucher, sich gegen Pharming zu wappnen?

Das Wichtigste, das man tun kann, ist regelmäßig die Antivirensoftware zu aktualisieren. Das ist zwar keine Garantie dafür, dass sich keine Viren oder Trojaner auf dem Rechner installieren können, reduziert das Risiko aber erheblich. Bevor man Passwörter und vertrauliche Zugangsdaten auf einer Webseite eingibt, sollte man außerdem immer prüfen, ob es sich um eine sichere Internetverbindung handelt. Das erkennt man am Schloss-Symbol in der Adresszeile des Browsers und daran, dass die Webseite mit „https://“ beginnt.

Tatjana Halm

Rechtsanwältin und Referatsleiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Bayern, © Marcus Schlaf/Verbraucherzentrale Bayern

Was kann man tun, wenn man Pharming dennoch zum Opfer gefallen ist?

Das hängt sicherlich vom Einzelfall ab. Auf jeden Fall sollte der Rechner auf Hinweise geprüft werden, die Rückschlüsse auf den Täter geben können. Der Virus oder Trojaner sollte von einem Fachmann entfernt werden. Außerdem ist es wichtig, seine Passwörter schnellstmöglich zu ändern – denn die sind bei den Internetkriminellen ja schon im Umlauf. Sind mit den gestohlenen Daten bereits Einkäufe oder Kreditkartenabbuchungen getätigt worden, sollte man dies dringend den beteiligten Banken mitteilen. Letztendlich ist es unserer Meinung nach auch unbedingt empfehlenwert, Anzeige bei der Polizei zu erstatten. Denn das ist auch häufig die Voraussetzung, dass Banken überhaupt erst aktiv werden und versuchen können, das verschwundene Geld wieder zurückzubuchen. KF (27.09.2019)

Folgende Artikel könnten Sie auch interessieren:

- Bestellt und nichts geliefert
- Bankgeschäfte und Einkaufen im Netz
- Phishing – so können Sie sich schützen

Alle Artikel dieser Kategorie

Weitere Infos für Gewerbetreibende

Mit Peter Werkmüller, Polizeiliche Beratungsstelle Düsseldorf

Video: Einbruchschutz in Gewerbeimmobilien

In diesem Video befasst sich Hauptkommissar Peter Werkmüller von...[mehr erfahren]

Mehr Sicherheit mit intelligenten Fahrzeugen

Autonomes Fahren

Noch ist es eine Zukunftsvision. Doch vielleicht wird uns unser Auto...[mehr erfahren]

Das neue Gesetz hat sich bewährt

Mehr Verbraucherschutz bei Versicherungsverträgen

Seit Januar 2009 gilt das neue Versicherungsvertragsgesetz, das...[mehr erfahren]

Falsche Chefs erschleichen hohe Geldsummen

CEO-Fraud auf dem Vormarsch

Seit 2014 beobachtet man in Deutschland ein neuartiges, speziell...[mehr erfahren]

Illegaler Handel mit Kunst- und Kulturgut

Geplündert, geschmuggelt, verscherbelt

Die weltweite Kunst- und Kulturgutkriminalität ist ein großes...[mehr erfahren]
