IT-Sicherheit

Phishing – allgegenwärtig und gefährlich

Phishing ist zu einem grossen Ärgernis geworden. Fast täglich treffen neue Versuche ein, um an die persönlichen Daten zu gelangen. Gemäss dem aktuellen MELANI Halbjahresbericht 2015/2 wurden über 2500 Phishing-Angriffe gemeldet.

Phishing, ein Kunstwort aus Password Harvesting Fishing, bezeichnet das Angeln von Passwörtern, dem Versuch also, an vertrauliche Informationen der Opfer zu gelangen. Die E-Mails haben dabei verschiedene Formen und Inhalte. Oft werden dazu bekannte Firmen als Absender verwendet, mit dem Versuch, Vertrauen zu erwecken. Beispielsweise Credit Suisse als Absender, der Online-Banking-Account musste infolge eines Hackingangriffs gesperrt werden. Zum Reaktivieren müsse nur auf den untenstehenden Link geklickt werden. Oder ein weiteres Beispiel: DHL wollte ein Paket zustellen, da aber niemand zu Hause war, müsse nun ein Formular ausgefüllt werden, wann man wieder zu Hause ist und der DHL-Bote vorbeikommen könne. Ein drittes Beispiel: ein perfekt auf die Firma abgestimmtes Bewerbungsschreiben. In perfektem Deutsch und mit der richtigen Anrede. Bei allen Angriffen ist grösste Vorsicht geboten. Immer wieder wird versucht, beim Aufruf der verlinkten Seite oder einem angehängten Dokument eine Malware (Virus, trojanisches Pferd oder dergleichen) zu installieren. Und dies auch, wenn das Formular gar nicht ausgefüllt wird. Daher gilt, diese E-Mails umgehend in den Papierkorb (Trash) zu verschieben.

Viele Menschen sehen sich nicht im Fokus eines Angriffs. „An meinen Daten hat eh niemand Interesse“, ist eine Aussage, die oft gemacht wird. Dies kann vielleicht stimmen, denn auf ein Unternehmen bezogene Angriffe sind doch eher die Ausnahme. Aber irgendwo in einem Gästebuch einen Eintrag mit der eigenen E-Mailadresse getätigt, an einem Wettbewerb mitgemacht oder auf der eigenen Homepage die E-Mail in ungeschützter Form angebracht, und schon ist die E-Mailadresse auch für einen Angreifer sichtbar. Es gibt auch einen Handel mit diesen Adressen. Für wenige Dollar können tausende (gültige!) E-Mailadressen gekauft werden. Wer sich nun hinter einer der E-Mailadressen „versteckt“, ist für den Käufer unerheblich. Hauptsache, es wird auf den Link geklickt. Wenn von 1000 angeschriebenen Personen nur eine auf diesen Angriff hereinfällt, kann sich dies bereits für einen Angreifer lohnen.

In der immer stärker vernetzten Welt hinterlässt jede und jeder unbewusst seine Spuren. In den Nachrichten des Vereins wird von einem Wettkampf oder einem Anlass erzählt und die Personen mit Namen veröffentlicht. Diese dann mit Facebook, Xing, Twitter oder dergleichen kombinieren und viele Informationen über einen Menschen kommen zusammen. Spezielle Suchmaschinen haben sich zum Ziel gesetzt, diese Informationen einfach und übersichtlich zusammen zu ziehen Anschliessend werden diese für einen personenbezogenen Angriff verwendet werden. Im geschäftlichen Umfeld könnte die E-Mail dann vom Chef kommen, mit der Bitte eine spezielle Seite zu besuchen, im privaten Umfeld von einem ehemaligen Schulkollegen, den man schon lange nicht mehr gesehen hat. Werden in der E-Mail Dinge erwähnt, die eigentlich niemand anderes kennen kann, ist das Vertrauen bereits viel höher und der Drang auf den Link zu klicken nicht mehr so weit entfernt.

Daher gilt vermehrt, vorsichtig zu sein. Besser zwei Mal überlegen, ob dies wirklich sein kann, bevor auf den Link geklickt wird. Mit gesundem Misstrauen und der nötigen Vorsicht können Sie sich auch heute noch sicher im Internet bewegen.