Phishing – eine aktuelle und zunehmende Gefahr

Die Nachrichten über Phishing-Attacken sind zu einem ständigen Begleiter geworden. Beinahe jede Woche liest man neue Meldungen über E-Mail-Aufforderungen, seine Bank-, Ebay-, E-Mail- oder sonstige persönliche Angaben preiszugeben. Ein Klick auf den beiliegenden Link genügt und ein Formular ermöglicht die Eingabe dieser Daten. Der Richtlinientext 2006/42/EG kann unter http://eur-lex.europa.eu/ aufgerufen und in allen EU-Amtssprachen kostenlos heruntergeladen werden.

Im Juni 2005 wurde zum ersten Mal auch ein Schweizer Finanzinstitut Ziel einer Phishing-Attacke. Ein auf Englisch formuliertes E-Mail forderte Yellownet-Benutzer auf, die Logindaten sowie die nächsten drei unbenutzten Streichlistennummern zur Datenkontrolle einzugeben. Der in der Email enthaltene Link führte zu einer perfekt nachgebildeten Internetseite in Russland.

Eigentlich sollten in einem solchen Fall die Alarmglocken läuten, doch trotzdem folgten rund ein Dutzend Kunden diesem Aufruf. Blitzschnell wurden diese Konten leer geräumt. Zum guten Glück der Geprellten übernahm die Schweizerische Post kulant den Schaden und erfreulicherweise war der finanzielle Schaden in diesem Fall gering. Dies kann sicher auch auf die zahlreichen Warnungen im Radio und Fernsehen zurückzuführen sein.

Die Gefahr von Phishing-Attacken hat in den vergangenen Wochen weiter zugenommen. Jedoch sind es nicht mehr plumpe Versuche via Email, sondern es kommen ausgefeiltere Methoden zum Einsatz. Zum Beispiel Trojanische Pferde, die jede Tastatureingabe aufzeichnen und augenblicklich weitermelden. Auch besteht die Gefahr, dass ein korrekter Aufruf einer Webseite unbemerkt auf einen anderen Server umgeleitetet wird. Diese Technik wird schon von einigen Viren ausgenutzt und verhindert unter anderem das Aufrufen bekannter Antivirenhersteller-Homepages.

Gegen diese neuen Tricks hilft nur, den eigenen Rechner immer aktuell zu halten. Sei dies nun der Virenscanner, das System oder die (Desktop-)Firewall. Ebenfalls gilt es, nicht wild auf Links zu klicken, sondern sich zuerst klar zu sein, wohin man verlinkt wird. Viele Phishing-Mails sind schon an der holprigen oder fremden Sprache zu erkennen.

Gesunder Menschenverstand und aktuelle Systeme bewahren auch in Zukunft zuverlässig vor Missbrauch und Manipulation.

ZUM AUTOR
Andreas Wisler –
IT-Redaktion Maschinenbau