

Menschliche Schwäche, die Achillesferse der Cybersicherheit

# Phishing nutzt die Gutgläubigkeit aus

Das Wort «Pishing» stammt aus dem Englischen und ist aus «password» (Passwort) und «fishing» (fischen) zusammengesetzt. Mit dem Begriff wird eine Methode bezeichnet, mit der persönliche Daten erschlichen werden mit dem Ziel, diese ohne Wissen und Zustimmung der betroffenen Person zu nutzen.

*Martina Guillod*

**D**er Datenklau kann über fingierte Websites, Mails oder Benachrichtigungen erfolgen, die das Opfer im Glauben lassen, es wende sich an einen vertrauenswürdigen Dritten (Bank, Behörde, Arbeitgeber). Das Opfer wird dann dazu verleitet, persönliche Auskünfte wie ein Passwort oder die Nummer einer Kreditkarte weiterzugeben. Die Betrüger können anschliessend Geschäfte im Namen ihrer Opfer tätigen und sich auf ihre Kosten bereichern. Phishing nutzt menschliche Schwächen aus und missbraucht das Vertrauen und die Gutgläubigkeit der Opfer.

Aus rechtlicher Sicht ist es schwierig, Phishing zu erfassen. Das Schreiben und der Versand von Phishing-Mails sind nur dann strafbar, wenn eine Urkundenfälschung (Art. 251 StGB) vorliegt. Das kann

beispielsweise der Fall sein, wenn der Betrüger den Adressaten dazu auffordert, den Benutzernamen und das Passwort mitzuteilen, weil anderenfalls das Konto gesperrt würde. Eine Urkundenfälschung kann auch vorliegen, wenn eine gefälschte Website eine E-Banking-Sitzung eröffnet mit einer optischen Ansicht, die jener der tatsächlichen Website täuschend ähnlich sieht. Der Täter muss vorsätzlich handeln mit der Absicht, den anderen zu schädigen und seine eigene Situation zu verbessern, etwa indem er die erschlichenen Daten verkauft. Urkundenfälschung wird mit einer Freiheitsstrafe bis zu fünf Jahren oder einer Geldstrafe bestraft.

Betrüger begnügen sich selten damit, Phishing-Mails zu versenden, ohne die dabei erhaltenen Daten weiterzuverwenden. Sobald ein Betrüger die mittels Phishing erworbenen Daten verwendet – beispiels-

weise, indem er sich in das E-Banking einwählt und online eine Geldübermittlung vornimmt –, macht er sich des betrügerischen Missbrauchs einer Datenverarbeitungsanlage strafbar (Art. 147 StGB). Voraussetzung ist, dass er vorsätzlich handelt und mit dem Ziel, sich unrechtmässig zu bereichern. Der Täter riskiert eine Freiheitsstrafe bis zu fünf Jahren oder eine Geldstrafe. Handelt der Täter gewerbmässig, so wird er mit einer Freiheitsstrafe bis zu zehn Jahren oder einer Geldstrafe nicht unter 90 Tagessätzen bestraft. Der betrügerische Missbrauch einer Datenverarbeitungsanlage kann in unserem Land verfolgt werden, wenn die Betrüger die unrechtmässig beschafften Daten dazu verwenden, sich in ein E-Banking eines Schweizer Finanzinstituts einzuwählen, und dies selbst dann, wenn sich die Täter physisch nicht in der Schweiz befinden.

