Phishingmails verweisen auf verseuchte Webseiten

Betrüger versuchen derzeit, durch das massenhafte Versenden von Phishingmails Rechner mit Schadcode zu infizieren. Der Schadcode ist auf den Webseiten eingebunden, auf die die Phishingmails verlinken.

Heise meldet, dass derzeit massenhaft Phishingmails versendet werden, die angeblich von der Sparkasse stammen. In Wahrheit versuchen Betrüger, die Rechner der Mailempfänger mit Schadcode zu infizieren. Der Schadcode ist nicht in den Mails direkt eingebettet, sondern ist auf Webseiten hinterlegt, die durch Links in den Phishingmails aufgerufen werden. Weist der Browser des Benutzers eine Sicherheitslücke auf, besteht die Gefahr, dass der Schadcode sich auf dem System des Benutzers einnistet. Da auf den Webseiten zusätzlich die Verifizierung angeblicher "Bestelldaten" dargestellt wird, wirkt der Angriff auf den ersten Blick wie eine klassische Phishingattacke, die erst durch das Interagieren des Benutzers zum Erfolg für die Betrüger führt.

Die Mails verlinken auf unterschiedliche Server, was das Sperren der Phishingseiten erschwert. Mailempfänger sollten den Link in dieser Phishingmail auf keinen Fall anklicken, da dies bereits zum Infizieren des Rechners führen kann. Aktuell haben wir nur Kenntnis von Phishingmails dieser Art, die im Namen der "Sparkasse" versendet werden. VR-Banken scheinen aktuell nicht hierfür missbraucht zu werden.

Die Mails sind nach folgendem Muster aufgebaut (Variationen wahrscheinlich):

Guten Tag,

im Auftrag unseres Kunden haben wir eine Einzahlung in Höhe von 15.000,00 Euro auf Ihr Sparkasse-Bankkonto vorgenommen.

Unsere Bank hat uns mitgeteilt, dass die Überweisung aufgrund eines Fehlers in der Angabe Ihrer Zahlungsdaten nicht abgeschlossen werden kann.

Bitte überprüfen Sie die Angaben und Bestelldaten auf unserer Webseite.

Bestelldaten überprüfen

Falls Sie Rückfragen haben, nehmen Sie bitte Kontakt mit uns auf.

Abteilung Rechnungswesen

Quelle: heise.de