

Sicherheit bei Online-Bezahldiensten

Geschickte Betrüger, überrumpelte Opfer

Von Simone Wroblewski



Prepaid-Online-Zahlungsmittel wie paysafecard oder Ukash werden als alternative Bezahlssysteme im Internet immer beliebter. Der Vorteil: Man kann auch kleine Beträge bei Online-Käufen bequem bezahlen, ohne dabei private Daten wie Name oder Kontoverbindung angeben zu müssen. Aber auch für Betrüger sind die digitalen Zahlungsmittel attraktiv: Kommen sie etwa in Besitz von PINs, die der Kunde für seine Käufe nutzt, können sie selbst damit im Internet auf Shoppingtour gehen. Häufig werden die PINs auch im großen Stil durch Betrügereien und Erpressungen erlangt und am Ende „ausgecasht“, also wieder in Bargeld umgewandelt.

Prepaid-Onlinebezahlssysteme funktionieren ähnlich wie eine Wertkarte für Mobiltelefone. Man kauft zunächst die Wertkarte an einer der Verkaufsstellen – das können etwa Kioske, Tankstellen oder Supermärkte sein. Dort erhält man an der Kasse einen Ausdruck mit einer PIN im Gegenwert des bezahlten Betrages. In autorisierten Online-Shops im Internet kann man nun mit dieser PIN bezahlen – so lange bis das eingezahlte Guthaben aufgebraucht ist. Genutzt werden können diese Bezahlssysteme etwa bei Anbietern aus den Bereichen Games, Social Media & Communities, Musik, Film und Entertainment. „Wichtig ist dabei, dass man seine PIN wie Bargeld behandelt und sie niemals an Dritte weitergibt“, betont Maximilian von Both.

Betrüger sind dreist und einfallsreich

Angriffsszenarien im Bereich Online-Bezahlssysteme gibt es viele. Ziel von Betrügern sind dabei einerseits die Ausgabestellen der PINs, also das Kassenpersonal in Supermärkten oder an Tankstellen, aber auch die Nutzer selbst. Ziel ist es dabei immer, an PINs zu kommen. „Die Betrüger gehen dabei sehr geschickt vor und versuchen entweder, Druck bei den Opfern aufzubauen oder sie mit finanziellen Vorteilen zu locken“, erklärt Bernd Fox aus dem Sachbereich „Organisierte Kriminalität“ der Polizeidirektion Osnabrück.

Häufig seien zum Beispiel Gewinnversprechen, bei denen gezielt ältere Menschen angerufen und zu Geldzahlungen per Online-Bezahlssystem aufgefordert würden. Die Betrüger erklären den Opfern, dass sie erst eine bestimmte Summe zahlen müssten, bevor ein Gewinn ausgeschüttet werden könne.

Da das Geld aus dem Ausland komme und dort Steuern beglichen werden müssten, solle dazu das Online-Bezahlssystem genutzt werden. Die Opfer geben dann die geldwerten PINs an die Betrüger heraus.

Aber auch bei so genannter „Ransomware“, also Software, die von Kriminellen eingesetzt wird, um Computernutzer zu erpressen, wird als Zahlungsmittel unter anderem paysafecard genutzt. Bei einem solchen Angriff erscheint auf dem Rechner zum Beispiel die Meldung, dass man illegale Musikdownloads oder kinderpornografisches Material auf dem Rechner hätte und deshalb Strafe zahlen müsse. Oder die Festplatte wird verschlüsselt und die Angreifer drohen damit, die Daten zu löschen, falls man nicht die geforderte Summe zahlt. „Voraussetzung für solch einen Angriff ist die vorherige Infektion des Rechners mit Schadsoftware – etwa über manipulierte Webseiten oder infizierte E-Mail-Anhänge“, erklärt Bernd Fox. „Die Opfer eines solchen Erpressungsversuchs sind meist völlig überrumpelt und zahlen die geforderte Summe, weil sie Angst um ihre Daten haben. Es gibt Fälle, bei denen Opfer 3.000 Euro in Form von PINs gezahlt haben“, so der Experte. Bei weiteren Betrugsvarianten geht es beispielsweise um den Erlass von Schulden oder aber darum, das Guthaben einer paysafecard vermeintlich zu verdoppeln. „Der Kreativität der Betrüger sind dabei keine Grenzen gesetzt“, so Fox.

Eine beliebte Masche beim Betrug an den Verkaufsstellen: Ein Anrufer täuscht vor, Angestellter des paysafecard-Technikservices zu sein. Er gibt zum Beispiel vor, dass es beim Generieren der PINs ein Problem gibt und fordert den Kassierer

auf, testweise Codes zu generieren und diese telefonisch durchzugeben. „Obwohl unsere Distributoren und das Kassenpersonal ausführlich und intensiv geschult werden sowie ausführliche Informationsmaterialien erhalten, kommt es immer wieder dazu, dass PINs am Telefon herausgegeben werden. Die Betrüger haben sich auf diese Anrufe gut vorbereitet und verfügen zum Teil über gut recherchierte Informationen – wie etwa Namen von Vorgesetzten oder interne Abläufe“, weiß Maximilian von Both.



Online-Bezahlsysteme können z.B. über Verkaufsstellen in Kiosken und Tankstellen erworben werden.



EKKH Bernd Fox aus dem Fachbereich „Organisierte Kriminalität“ der PD Osnabrück gibt Tipps für den richtigen Umgang mit Online-Bezahlsystemen.



Maximilian von Both, Niederlassungsleiter paysafecard Deutschland, betont neben der Aufklärung der Nutzer auch die Schulung von Verkaufspersonal

Vorgehen im Betrugsfall

Wurde eine PIN an Betrüger herausgegeben, kommt es vor allem auf eines an: Schnelligkeit. Denn es besteht die Möglichkeit, den Code beim Anbieter sperren zu lassen, noch bevor die Betrüger ihn einlösen können. „Wenn die betroffene Person selbst noch keinen Kontakt zum Anbieter des Bezahlendienstes aufgenommen hat, sollte dies spätestens der Beamte tun, der die Anzeige aufnimmt“, betont Bernd Fox. „Der erste Ansatz muss sein, den Schaden so gering wie möglich zu halten und zu versuchen, ob noch etwas zu retten ist. Kennt man sich mit der Bearbeitung solcher Fälle nicht gut aus, sollte man unbedingt einen erfahrenen Kollegen hinzuziehen“, so der Experte. Im Weiteren muss geklärt werden, wie der Betrug vorstatten ging. Handelt es sich um einen Erpressungsversuch, bei dem der Rechner infiziert wurde? Oder wurde man per Post mit einem Gewinnversprechen angeschrieben? „Für Erpressungsoffer haben wir ein Merkblatt vorbereitet, das wir den Betroffenen schicken können. Darin werden wichtige Angaben zur Straftat erläutert und aufgezeigt, was der Betroffene jetzt tun sollte, etwa, wie der „gesperrte“ PC ggf. wieder lauffähig gemacht werden kann. Der Betroffene sollte vor der Rücksprache mit der Polizei keine Veränderungen am PC vornehmen und der Polizei mitteilen, womit die Täter drohen, welches Bezahlssystem genutzt werden soll und ob zusätzlich eine alternative E-Mail-Adresse als Kontakt angegeben ist. Es ist außerdem hilfreich, wenn der Betroffene den Bildschirm mit der konkreten Forderung fotografiert und uns das Foto für weitere Ermittlungen zur Verfügung stellt“, so Fox. Wichtig dabei: Die Beamten sollten immer darauf hinweisen, dass kinderpornografisches Material, das bei solchen Erpressungsversuchen gelegentlich mit abgebildet wird, beim Fotografieren abgedeckt werden muss, da man sich sonst aufgrund des Abspeicherns oder Ausdrucks von Kinderpornografie strafbar machen kann. Interessant ist auch die Frage, wie der Virus auf den Rechner gekommen ist: Wurde eine bestimmte Webseite besucht? Oder hat man einen infizierten E-Mail-Anhang geöffnet? „Je mehr Informationen man über den Hergang sammelt, desto besser. Das ist sehr hilfreich für die Fragestellung, ob es sich um einen bekannten oder einen neuen Trojaner handelt. Nicht zuletzt sollten die Kollegen die

Betroffenen aber auch noch einmal über grundlegende IT-Sicherheit aufklären bzw. Hinweise zur sicheren Nutzung von Online-Bezahlsystemen geben“, betont Bernd Fox.

Aufklären und schulen

Um Online-Bezahlsysteme sicher nutzen zu können, muss man sich zwingend an die vorgegebenen Sicherheitsregeln halten. paysafecard investiert deshalb viel Geld in Schulungen und die eigene Sicherheitsabteilung. „Wir bieten Präsenzs Schulungen bei unseren Distributoren an, es gibt Schulungsunterlagen für die Beschäftigten sowie Merkblätter. Außerdem entwickeln wir gerade ein Online-Tool, das die Mitarbeiter in den Verkaufsstellen noch gezielter aufklären soll“, erklärt Maximilian von Both. Technisch unterstützt wird das Kassenspersonal außerdem durch automatische Abfragen. Immer wenn eine neue PIN generiert werden soll, erscheint auf dem Monitor die Abfrage „Werden Sie gerade am Telefon oder per E-Mail dazu aufgefordert, eine PIN zu erstellen?“ Drückt man auf „Ja“, bricht der Vorgang sofort ab. Zusätzlich erscheinen Hinweise zu aktuellen Betrugs maschen auf dem Kassenterminal. Erstattet ein Geschädigter Anzeige bei der Polizei, stellt das Unternehmen auf Anfrage der Beamten alle Daten, die für die Ermittlungen nötig sind, zur Verfügung. Da die IP-Adressen nur sehr kurze Zeit gespeichert werden dürfen, sollte eine Kontaktaufnahme möglichst schnell erfolgen. „Wenn die Polizei sich mit einem Betrugsfall bei uns meldet, wird dieser mit Priorität behandelt, so dass wir die benötigten Daten innerhalb von ein bis zwei Stunden zur Verfügung stellen können“, betont der Geschäftsführer. Sinnvoll sei es auch, den betreffenden Sachverhalt kurz zu schildern, damit die Sicherheitsexperten gegebenenfalls noch weiter unterstützend tätig werden können. „Uns ist sehr daran gelegen, die Ermittlungsbehörden bestmöglich zu unterstützen. Wendet sich ein Kunde mit einem Betrugsfall an uns, raten wir grundsätzlich immer dazu, Anzeige bei der Polizei zu erstatten. Je mehr Fälle gemeldet werden, desto besser kann die Polizei diese bündeln und bearbeiten.“

ZUM SICHEREN UMGANG MIT ONLINE-BEZAHLDIENSTEN:

Um diese Dienste sicher nutzen zu können, ist es dringend notwendig, sich an die Sicherheitsanforderungen und -anweisungen des jeweiligen Anbieters zu halten, z.B.: Die PIN nur bei offiziellen Verkaufshops einkaufen; niemals die PIN per Mail oder am Telefon herausgeben; bei Internetkäufen die PIN nur in autorisierten Online-Shops einsetzen; im Betrugsfall schnell den Anbieter kontaktieren. Mehr Infos zur Sicherheit bei der Nutzung von Online-Bezahlsystemen gibt es in der Regel beim jeweiligen Anbieter.

GRUNDLEGENDE IT-SICHERHEIT:

Auf jedem Rechner sollten sowohl ein Antivirenschutzprogramm als auch eine Firewall installiert sein. Das Betriebssystem sowie alle eingesetzte Software sind stets auf dem aktuellen Stand zu halten, Aktualisierungen sowie Sicherheitspatches sollten umgehend nach Erscheinen installiert werden. Eine regelmäßige Datensicherung macht Nutzer weniger angreifbar – etwa für Erpressungsversuche. E-Mail-Anhänge oder Web-Links in E-Mails, in sozialen Netzwerken oder Chats sollten nur mit besonderer Vorsicht geöffnet werden, auch wenn sie von bekannten Quellen stammen. Gegebenenfalls sollte beim Absender nachgefragt werden. Empfehlenswert sind mehrere Benutzerkonten für den Rechner. Ein allgemeiner „Administrator“-Account ermöglicht einem potenziellen Angreifer unter Umständen den Zugriff auf sämtliche Daten. Für alle Online-Dienste sollten sichere Passwörter gewählt werden, die regelmäßig gewechselt werden. Für verschiedene Dienste sollte niemals das gleiche Passwort verwendet werden. Verständlich aufbereitete Infos zum Thema Internetsicherheit gibt es zum Beispiel beim Bundesamt für Sicherheit in der Informationstechnik (BSI) unter www.bsi-fuer-buerger.de oder bei der Polizei Niedersachsen www.polizei-praevention.de.