

SPIEGEL ONLINE - 10. September 2007, 19:12

URL: <http://www.spiegel.de/netzwelt/web/0,1518,504934,00.html>

SICHERHEITSLÜCKE

Betrüger bedienen sich in Ebay-Datenbanken

Von Christian Stöcker und Frank Patalong

Ein neuer Betrugstrick kann Ebay-Käufer teuer zu stehen kommen. Die Täter können direkt auf interne Datenbanken des Auktionshauses zugreifen und sich so E-Mail-Adressen und Daten über den Wohnort aktuell Bietender verschaffen. Die werden dann gezielt angesprochen - und ausgenommen.

Der Mechanismus funktioniert beängstigend gut. Und er macht es möglich, völlig automatisiert sehr echt aussehende E-Mails zu verschicken, die unterlegenen Bietern nach verllorener Auktion Hoffnung machen: "Ich habe gesehen, dass Sie bei meiner Auktion mitgeboden haben. Umständen zufolge, die sich meiner Kontrolle entziehen, muss ich die Ware so schnell wie möglich verkaufen. Ich habe mir erlaubt, eine direkte Ebay-Transaktion unter Squaretrader-Überwachung einzuleiten." Die Ware müsse nur noch bezahlt werden. Die Post kommt an die eigene E-Mail-Adresse - und wenn man dem Link zur "Zahlungsabwicklung" folgt, steht dort schon der eigene Wohnort und die eigene Postleitzahl.

EBAY-BETRUG: "HERZLICHEN GLÜCKWUNSCH"



Fotostrecke starten: Klicken Sie auf ein Bild (5 Bilder)

Wer auf die Lockmail und die gefälschte Seite hereinfällt, die zwar täuschend echt aussieht, aber eine für Ebay eher merkwürdige URL hat - der wird aufgefordert, die glücklich erstandene Ware mit einer Western-Union-Transaktion zu bezahlen. So kommt das Geld der ahnungslosen vermeintlichen Käufer zwar bei den Betrügern an, aber es kann nicht nachvollzogen werden, wo es hingegangen ist.

Mit einem Skript, das auf einer offen zugänglichen Webseite für jedermann abrufbar ist, sind die notwendigen Daten für solche Aktionen kinderleicht zu bekommen. Man braucht nur die Transaktionsnummer einer bestimmten Auktion in ein Fenster zu kopieren, auf "Start" zu klicken, schon werden die Betrüger-E-Mails an die unterlegenen Bieter geschickt. Das dürfte gar nicht möglich sein, denn die Mail-Adressen sollten innerhalb des Ebay-Systems nicht offengelegt werden.

Betrugssystem von Nutzern aufgedeckt

Der Betrügertrick kommt aber nicht nur an die E-Mail-Adressen heran, sondern ordnet einem Ebay-Namen eines ahnungslosen Opfers auch noch dessen Wohnort und Postleitzahl zu. Die ganze Kette steht jedem, der die richtigen Web-Adressen kennt, vollkommen offen.

SPIEGEL ONLINE hat das System ausprobiert und Test-Betrugsmails an Redakteure verschickt. Von Ebay war bis zum Abend kein Kommentar zum Thema zu erhalten.

Aufgedeckt haben den Betrugsmechanismus die Mitglieder der privaten Initiative [Falle-Internet.de](http://www.falle-internet.de). Die Gruppe besteht aus Nutzern, die sich über Ebay-Foren kennengelernt haben und nun gemeinsam im Netz auf Verbrecherjagd unterwegs sind, um aufzuklären und vor

Betrugsversuchen zu warnen.

Nach Einschätzung von Falle-Internet.de gibt es verschiedene Betrügergruppen, die auf die offen zur Verfügung stehenden Skripte zugreifen. Die Köder-Mails würden in verschiedenen Sprachen verschickt. Die Betrüger versuchten einander bei hochpreisigen Auktionen so verzweifelt zu überflügeln, dass die vermeintlichen Sofort-Kauf-Angebote noch vor dem Ende der Auktionen versandt werden.

Ebay Deutschland wartet auf Anweisungen aus den USA

Den Zweitplatzierten einer Auktion zu kontaktieren, um ihm ein vermeintlich lohnendes, in Wirklichkeit aber betrügerisches Angebot zu machen, sei "eine gängige Betrugspraxis", sagt ein Mitglied von Falle-Internet.de. Die automatisierte und flächendeckende Ansprache solcher unterlegenen Bieter wird aber erst durch offenkundige Lücken im Ebay-Sicherheitssystem möglich.

Bei Ebay ist man sich der Lücke offenbar durchaus bewusst - auch weil in den Foren des Auktionshauses schon heftig darüber debattiert wird. Eine Stellungnahme oder gar Ankündigung von Gegenmaßnahmen gibt es bislang nicht. Aus der Deutschland-Zentrale erfuhr SPIEGEL ONLINE am Montagabend nur, man warte auf Nachricht aus dem US-Mutterhaus.

Für Ebay-Nutzer ergibt sich aus der Betrugsmasche eine schlichte Vorsichtsmaßnahme. Wenn Sie ein Angebot erhalten, das angeblich von einem Anbieter stammt, von dem Sie eben etwas ersteigern wollten: Ignorieren Sie es am besten, oder gehen Sie zumindest sehr vorsichtig damit um. Kontaktieren Sie den tatsächlichen Anbieter über die Ebay-interne Kommunikationsfunktion und fragen Sie ihn, ob er Sie tatsächlich angeschrieben hat. Wenn nicht, melden Sie den Vorfall Ebay.

EBAY-BETRUG: SO LÄUFT DER DATENWEG

Die Täter hinter dem Betrugs-Skript, mit dem derzeit Adressen aus Ebay abgefischt werden, versenden ihre Daten über ein Forschungsnetzwerk in Luxemburg. Obwohl die Daten über ein Hochgeschwindigkeitsnetz laufen, verhalten sie sich teils erratisch, der Datenfluss ist ungewöhnlich zäh. Ausgangspunkt ist scheinbar eine technische Berufsschule, was aber durchaus täuschen könnte: Wahrscheinlicher ist, dass sich die Täter auf den dortigen Servern eingehackt haben und ihren Datenverkehr nur darüber routen. Zugangspunkt ist möglicherweise ein mit dem Luxemburger Forschungsnetz verbundener Rechner in Großbritannien.

Darauf deutet auch die Betrugsseite hin, über die die Opfer der Masche ihre angeblichen Käufe abwickeln sollen. Dieser Server steht in England und gehört keinem Freehoster, wo jeder Daten ablegen kann: Die Seite ist angebunden an eine Serviceseite, über die zahlende Kunden ihre Web-Accounts verwalten können. Zumindest dem dortigen Provider liegen also auch Namen vor - ob diese allerdings echt sind, sei dahingestellt.

Nicht auszumachen ist bisher jedenfalls, ob die Namen der beiden Begünstigten der betrügerischen Überweisungen echt sind oder nicht. Hier sind nicht nur Identitäten genannt, sondern auch vollständige Adressen - das schafft fehlgeleitetes Vertrauen. Die großen Telefonverzeichnisse kennen keine Personen, die die angegebenen Namen trugen. Auch die Websuche verläuft im Sand, wenn man so will - oder präziser im Mutterboden: Zwei Personen, die die angegebenen Namen trugen, lebten offenbar in London im 19. Jahrhundert.

Alles deutet also auf ein mehrstufiges Betrugsmanöver hin, mit dem die Täter ihre Spuren recht effektiv verwischen. Ein wichtiges Indiz ihrer Herkunft liefern sie trotzdem. Die Skriptmaske selbst, die SPIEGEL ONLINE vorlag und von uns getestet wurde, ist in einer klar identifizierbaren Sprache beschriftet: Rumänisch.

pat

© SPIEGEL ONLINE 2007

Alle Rechte vorbehalten

Vervielfältigung nur mit Genehmigung der SPIEGELnet GmbH

Zum Thema im Internet:

▸ Privatinitiative "Falle-Internet.de": Ziel Gefahrenaufklärung

<http://www.falle-internet.de>
