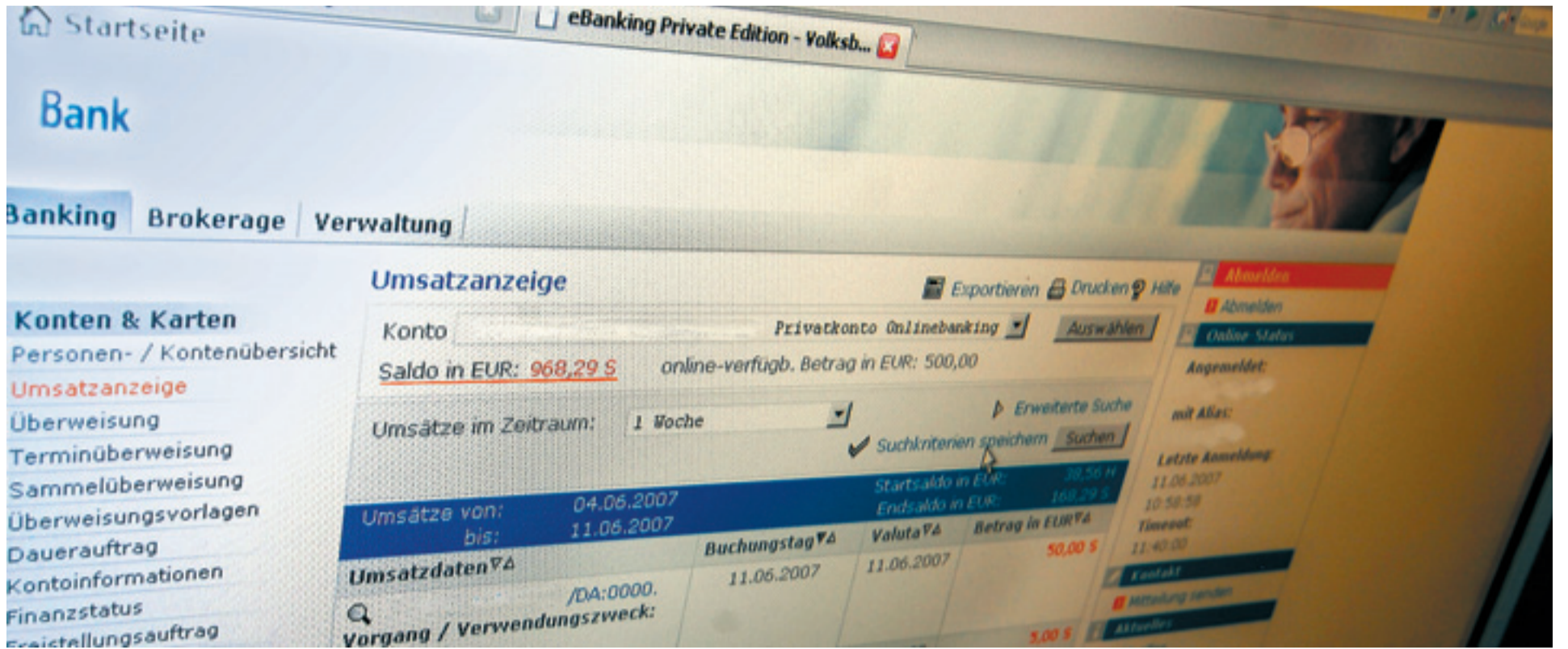


EINE NEUE STRATEGIE GEGEN PHISHING

Das Geld fremder Leute

Wie hoch der Schaden ist, den der Diebstahl von Zugangsdaten im Internet verursacht, weiß man nicht. Banken reden ungern darüber. Eine von einem Studenten der IT-Sicherheit entwickelte Technik könnte Abhilfe schaffen.



Ein Konto rutscht schnell tief ins Minus, wenn kriminelle Phisher zuschlagen: Mit gestohlenen Zugangsdaten wird Geld auf die Konten von Gaunern oder deren Kurieren überwiesen. Foto StZ

„Phisher greifen immer das schwächste Glied an“

Dominik Birk studiert an der Ruhr-Uni in Bochum IT-Sicherheitstechnik und hat ein Verfahren gegen Phishing entwickelt

Dominik Birk will Phisher rephishen. Das klingt rätselhaft, ist aber ein vom Bundesamt für Sicherheit in der Informationstechnik ausgezeichnetes Konzept. Im Gespräch mit Sandro Mattioli erklärt der Student, wie er Datendiebe im Internet mit ihren eigenen Waffen schlagen will.

Herr Birk, die virtuelle und digitale Welt ist schnelllebig. Manche sagen, auch die Zeit von kriminellen Maschen im Internet sei rasch vorbei. Ist denn das Phishing heute noch von Bedeutung? Werden Internet-Nutzer immer noch ihre Zugangsdaten von Gaunern entlockt?

Ja. Allerdings haben sich die Methoden geändert. Anfangs war der Trend, Phishing-E-mails zu verschicken. Da hieß es dann: „Wir aktualisieren derzeit unsere Datenbank. Bitte folgen Sie diesem Link und bestätigen Ihre Bankdaten.“ Jetzt geht der Trend mehr zu Phishing-Schadprogrammen. Die gab es damals noch nicht. Zugleich nimmt die Zahl der Phishing-E-mails ab. Sie werden wohl aussterben, weil sie nicht mehr effizient sind. Der größte Teil der Leute weiß jetzt Bescheid. Phishing wird aber aktuell bleiben, weil die Phisher es ausnutzen, dass die Leute auf ihre sich ändernden Strategien reinfallen. Klärt man die Leute über Phishing-E-mails auf, dann kommen die Schadprogramme. Dann wird es schon wieder schwierig, die Leute zu sensibilisieren, weil sie sich damit nicht auskennen.

Wie bekommt man diese Schadprogramme denn untergejubelt?

Da kommt eine E-Mail mit einem gefälschten Absender, etwa vom Internet-Anbieter 1&1. Angehängt ist eine Datei namens rechnung.pdf.exe, vielleicht noch mit einem Hinweis auf einen sehr hohen Rechnungsbetrag. Klickt man sie an, installiert sich ein Programm. So eine Datei öffnet man schnell mal.

Was tut dieses Programm Böses?

Es schaltet sich zum Beispiel zwischen Sie und den Server Ihrer Bank, wenn Sie das

nächste Mal Online-Banking machen. Sobald Sie Ihre Zugangsdaten und ihre Tan für die Buchung eingeben haben, unterbricht das Programm beispielsweise die Verbindung und meldet: „Die Verbindung wurde aus technischen Gründen geschlossen“. Zu der Zeit sind Ihre Daten schon auf dem Weg zum Phisher, der damit illegales Geld von ihrem Konto überweisen wird. Das betrifft natürlich nicht nur das Online-Banking, sondern auch Dienste wie Paypal, Amazon oder Ebay.

Sie haben eine Methode entwickelt, wie man dem begegnen kann. Welche?

Der normale Ablauf des Phishings ist, dass das Opfer auf einer gefälschten Seite seine Daten eingibt und glaubt, auf der Seite der Bank zu sein. Unser Konzept ist, dass wir uns als gefälschtes Opfer ausgeben. Das heißt, wir füllen nach der gleichen Methode wie potenzielle Opfer die Formulare der Phishing-Webseiten aus. Wir schieben dem Phisher dabei aber keine gültigen Anmeldedaten zu, die er benutzen kann, um illegale Transaktionen zu tätigen, sondern so genannte



Ich bin davon überzeugt, dass dieses Konzept den Banken, die stark von Phishing betroffen sind, enorm viel bringt. Zudem schreckt es ab.

Dominik Birk, ein Phishing-Experte

markierte Zugangsdaten, die wir Phoneytokens nennen. Diesen Sender für Phoneytokens habe ich bereits implementiert und er könnte prinzipiell in der Praxis eingesetzt werden. Der nächste Schritt ist dann, dass der Phisher versucht, sich mit diesen Daten auf der eigentlichen Seite anzumelden, um die illegale Geldüberweisung vorzunehmen. Die Web-Anwendung erkennt den Phisher automatisch und leitet ihn auf eine Seite weiter, auf der dann die Transaktion erfolgt – aber nur als Simulation. Das merkt der

Phisher aber nicht. Wir nennen dieses zweite System, auf das er umgeleitet wird, den Phoneypot.

Damit ist dann aber doch nur die illegale Überweisung verhindert. Hat das Verfahren auch noch andere Vorteile?

Wir erstellen dabei ein netzwerkspezifisches Profil. Wir analysieren verschiedene Attribute, unter anderem die IP-Adresse. Aus ihnen lässt sich dann ein Angreifer-Profil gewinnen, mit dem der Phisher eindeutig im Internet identifiziert werden kann. Tritt der Phisher wieder in Erscheinung, erkennt ihn das System automatisch. Der große Vorteil davon ist: Selbst wenn der Login dann mit gültigen Kundendaten stattgefunden hat, merkt das System, dass es sich um einen Phisher handelt – und leitet ihn auf den Phoneypot um. So können illegale Transaktionen unterbunden werden. Außerdem lassen sich strafrechtlich verwertbare Daten gewinnen, um die Phisher zu verfolgen.

Weiß das System denn immer zweifelsfrei, ob es sich um einen Phisher handelt?

Wir haben dafür einen Begriff definiert, die Phishiness, der aus verschiedenen Werten berechnet wird. Dazu wird das Anmeldeprofil mit Werten aus der Datenbank verglichen. Die Phishiness gibt an, zu welchem Prozentsatz wir vermuten können, dass es sich um einen normalen Login-Prozess handelt oder um einen Phishing-Angriff. Wenn meine Eltern etwa sich anmelden, dürfte die Phishiness bei zehn bis zwanzig Prozent liegen, wenn überhaupt. Bei Phishern liegt dieser Wert weit höher, etwa bei 80 Prozent. Liegt er über einem bestimmten Grenzwert, wird die Anmeldung umgeleitet. Das versuchen wir in die Praxis umzusetzen.

Was heißt das?

Es ist nicht ganz einfach, die Funktion, die die Phishiness bestimmt, festzulegen. Meine Arbeitsgruppe nimmt gerade Fallstudien vor und simuliert diverse Phishing-Angriffe, um eine ideale Gewichtung für die Attribute, die wir schon haben, herauszufinden. Diese Gewichtung ist schwierig.

Wann glauben Sie, ist das gesamte System marktreif, sprich: der Phoneytoken-Sender und der Phoneypot?

Der Sender ist fertig, der Phoney Pot wohl Ende des Jahres.

Haben Sie Ihre Methode auch schon in der Praxis testen können? Es dürfte nicht leicht sein, eine Bank dafür zu gewinnen.

Wir haben noch keine Institution gefunden, die gesagt hat, wir wollen das ausprobieren. Das Online-Banking ist für die Banken der heilige Gral, da darf niemand ran. Man sagte mir, ein Eingriff dort verlangt die Absegnung von höchster Ebene. Das ist also rein bürokratisch nicht machbar. Unser Konzept setzt diverse Eingriffe in die bestehende Infrastruktur voraus. Deshalb bin ich, was die praktische Anwendung in Banken anbelangt, sehr skeptisch. Aber es gibt ja viele andere Anwendungsmöglichkeiten, etwa bei Ebay. Für das Konzept selbst habe ich nur positive Rückmeldungen bekommen, da sagte keiner, es sei Blödsinn.

Nützt es Ihnen da etwas, dass Ihr Konzept vor Kurzem als bestes studentisches Papier bei einem Kongress des Bundesamts für Sicherheit in der Informationstechnik ausgezeichnet worden ist?

Das ist eine gute Frage. Ich habe diverse Anfragen von Journalisten bekommen, aber sonst mache ich mir keine großen Hoffnungen. Ich arbeite an der Uni, und das sind theoretische Ansätze. Für mich ist es ein wissenschaftlicher Mehrwert, der dabei rauskommt. Wenn sich jemand meldet, wäre das eine super Sache. Ich bin davon überzeugt, dass dieses Konzept den Banken, die stark von Phishing betroffen sind, enorm viel bringt. Zudem schreckt es ab. Der Phisher wird immer das schwächste Glied angreifen und sich nicht mit Banken, die moderne Abwehrsysteme wie die Phoneypot-Technik installiert haben, anlegen.

Ist es denn so, dass die Banken lieber Schäden ausgleichen als zu investieren?

Richtig, ja.

Ein kühler Kopf hilft

Phisher setzen auf Erschrecken

Großbritannien ist noch ein Paradies für Phisher. Konten sind dort nicht wie bei uns mit Pin- und Tan-Nummern geschützt. Im Sommer wollen englische Banken die Sicherheit für alle Kunden mit Lesegeräten für EC-Karten erhöhen. Welchen Schutz gibt es in Deutschland?

Von Sandro Mattioli

Vorsichtig zu sein ist die wichtigste Regel. Das heißt zunächst: Sich keinen Schreck einjagen zu lassen – egal, was in der eingehenden Mail auch behauptet wird. Denn ein Trick der Phisher ist, Mails zu verschicken, die aussehen, als kämen sie von renommierten Unternehmen, tatsächlich aber den Zweck haben, dem Empfänger Angst zu machen. Das Kalkül der Versender dieser Mail ist, dass die Menschen nicht mehr überlegt handeln, sondern im Schrecken die Datei im Anhang öffnen, die Schadprogramme enthält. Anstatt sich erschrecken zu lassen, sollte man lieber schauen, welche Endung die angehängte Datei hat: Beliebt ist beispielsweise die Bezeichnung Rechnung.pdf.exe; dabei verrät das „exe“, dass es sich nicht um ein Dokument im pdf-Format handelt, sondern um ein Programm.

Auch die Empfängeradresse ist einen genauen Blick wert. Wenn man weiß, dass man dem Absender nie die entsprechende E-Mail-Adresse gegeben hat, sollte man dem Inhalt der Email getrost misstrauen.

Grundsätzlich empfiehlt sich, den Rechner regelmäßig auf Schadprogramme durchsuchen zu lassen. Dazu gibt es viele Programme im Internet. Empfehlenswert sind das martialische benannte Search & Destroy, Ad-Aware und A-squared. Für den privaten Gebrauch sind diese Programme kostenlos. Es empfiehlt sich, die Software vor dem Überprüfen des Rechners zu aktualisieren.

http://www.safer-networking.org/de/index.html, http://www.ad-aware.softonic.de, http://www.emsisoft.de/de/software/download

SPIELSTATION

Strategie für unterwegs

„Anno 1701“ für den Nintendo DS: der Urlaub kann kommen

Die Urlaubssaison naht – mobile Spiele sind wieder gefragt. Eines, das den Sprung vom PC auf die kleine Nintendo-DS-Konsole geschafft hat, ist „Anno 1701“. Das beliebte Strategiespiel funktioniert auch per Hand- und Stiftsteuerung.

Von Thomas Schneider

Mit der Anno-Reihe setzte das deutsche Sunflowers-Studio vor fast 15 Jahren neue Maßstäbe bei Strategiespielen. Vor allem hier zu Lande punkteten alle Anno-Spiele bei den Freunden gepflegter Unterhaltung beim Erforschen und Erobern mittelalterlicher Paradiese. Das zuletzt erschienene „Anno 1701“ hat nun auch den Sprung auf den Handheld Nintendo DS geschafft und bietet sich so als idealer Reisebegleiter an.

Entwickelt wurde die komplette Neuprogrammierung nicht bei Sunflowers, sondern von Keen Games in Frankfurt. Dort hat man vor allem die Aufgabe gehabt, die auf zwei Bildschirmen basierende Technik der DS-Minikonsole in den Griff zu bekommen. Das ist ganz wunderbar gelungen. Schon nach wenigen Sekunden sind wir mit der Steuerung des Spieles (am unteren Bildschirm mit dem Stift oder dem Finger) und der Aufteilung der Bildelemente warm geworden.

„Anno 1701“ für DS entpuppt sich als ein umfangreiches Spiel mit hohem Strategieanteil. Viel Raum nehmen wieder das Siedeln auf unentdecktem Land sowie der Aufbau neuer Siedlungen ein. Ach, wie einfach das



Grafisch und technisch gut ist das Spiel Anno 1701 für den Nintendo. Foto Disney Interactive

mit dem sensitiven Bildschirm des DS-Handhelds geht. Drei Modi sind spielbar – dabei ist der normale Modus Kampagne besonders geeignet für Einsteiger. Auch ein Endlosspiel für den Urlaub ohne Grenzen sowie ein Modus für bis zu vier Spieler ist möglich. Der Urlaub kann kommen, dieses Spiel reist mit.

Verlosung und Bildergalerie unter www.stuttgarter-zeitung.de/spiele

Muskelkater

„Dragon Ball Z“ macht fit

Den Namen dieses Spieles muss man sich auf der Zunge zergehen lassen: „Dragon Ball Z Budokai Tenkaichi 2“. Beim Spielen sind dann allerdings andere Körperpartien gefragt – insbesondere die Rücken- und Armmuskulatur. Das im Mangastil gezeichnete Spiel gehört zu den Beat'em Ups – das sind Sportspiele mit asiatischen Kampfsportarten, die aber, weil das Spiel sich auch schon an Kinder ab sechs Jahren wendet, sehr lustig animiert sind. Im Gegensatz zu den vielen anderen Spielen des beliebten Genres hat dieses aber einen entscheidenden Vorteil: Der Spieler sitzt nicht faul auf dem Sofa, sondern muss schon selbst mit Hand und Fuß und besagten Muskelsträngen aktiv werden. Das ist fraglos eine ganz besondere Art von Fitnesstraining.

Entwickelt wurde das Spiel in Japan, in Deutschland wird es nun von Atari vertrieben. Um es spielen zu können, benötigt man die Nintendo-Spielekonsole Wii – und genau die ist auch für die sportliche Note des Haudraufspiels zuständig. Das innovative Steuerungskonzept mit der Wii-Fernbedienung und dem Nunchuck (einem kleinen Gerät, das räumliche Bewegungen am Bildschirm darstellen kann) ermöglicht ein Sport- und Kampfspiel, wie es bisher nicht möglich war. Gegenüber der bereits für die PS2-Konsole erschienenen Version hat die Wii-Variante übrigens zusätzliche Inhalte parat. Ein Spiel für Fans – und Untrainierte. ts

Verlosung und Bildergalerie unter www.stuttgarter-zeitung.de/spiele

Wasservogel

Niedlich: „Reise der Pinguine“

Der Dokumentarfilm „Die Reise der Pinguine“ hat Millionen Film- und Tierfreunde begeistert. Mit einem Abstand zu der Präsentation im Kino ist nun ein Spiel zu diesem Titel erschienen. Im gleichnamigen Computerspiel, das an der Handheld-Konsole Nintendo DS gespielt werden kann, geht es aber weit weniger dramatisch als im Film. Die Geschichte und das Leben der Kaiserpinguine im ewigen Eis bietet lediglich den Rahmen für eine Reihe von Minispielen. Bei allen 12 Aufgaben werden vor allem die logischen und taktischen Fähigkeiten der Spieler gefordert. Immer, wenn ein Ziel erreicht ist, gibt es kleine Videos zum Leben der echten Pinguine. Die Animation der digitalen Wasservogel ist gelungen und die Spielanforderung sehr abwechslungsreich. Das von Midway Games vertriebene Spiel ist ohne Altersbeschränkung im Handel. Wir empfehlen nach unserem Test ein Alter ab etwas sechs Jahren. ts



Pixelige Pinguine auf der Reise Foto Midway

Dicke Hilfe

Questbücher für Onlinespieler

Jeder, der schon einmal bei einem Computerspiel nicht mehr weiterwusste, hat sich vielleicht insgeheim einen guten Tipp oder gar eine Lösung zum Schummeln gewünscht. Lösungsbücher nannte man schon vor Jahren solche Druckwerke, die meist mit vielen Bildern versuchten, die Komplexität manch eines Spieles einzufangen. Der Fan spricht hier von einem Walkthrough und meint damit eine Handreichung, wie man durchs Spiel marschiert von A bis Z. Bei den nur online spielbaren Rollenspielen (MMOG) allerdings versagten solche Lösungshilfen bisher. Denn Spiele wie „World of Warcraft“ sind in viele hunderte kleiner Miniaufgaben unterteilt, die so genannten Quests. Es gibt keine festgelegte Reihenfolge und oft auch keinen definitiven Lösungsweg – wie will man da dem verzweifelten Spieler helfen?

Der Verlag Data Becker hat es dennoch geschafft. Zu „World of Warcraft“ ist soeben ein über 900 Seiten starker Questguide erschienen, der mehr als 2700 Aufgaben im Spiel beschreibt – sauber geordnet nach Zone und Landschaft und mit einigen Tipps zur Lösung angereichert. Ein zweiter, dünnerer Gameguide von Stefan Knaak bietet zusätzliche Hilfe für Warcraft-Spieler, ohne auf die Quests des Spieles einzugehen. Beide Bücher zusammen dürften sich in kürzester Zeit zu Standardwerken für Warcraft-Spieler entwickeln. Und auch für das erst kürzlich gestartete „Herr der Ringe Online“ ist seit wenigen Tagen ein Lösungsbuch verfügbar, das im Juli durch ein 500 Seiten dickes Kompendium ergänzt werden wird. ts