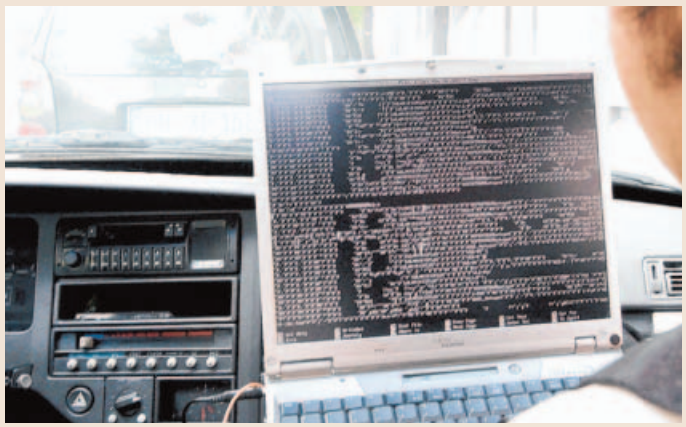
Mit Datenpiraten auf Beutezug

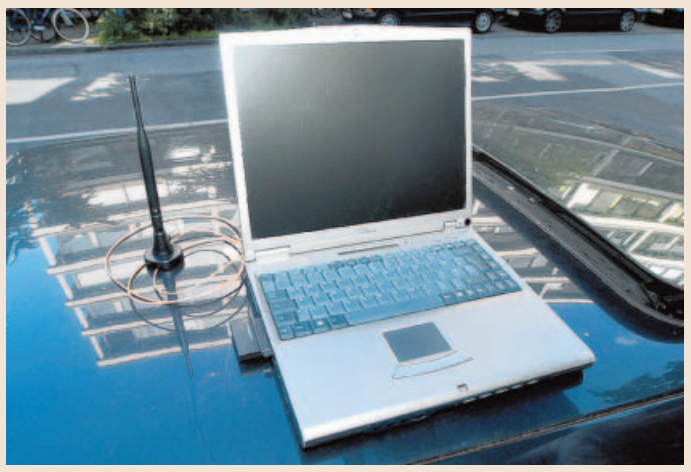
Beim Einkaufen: Wenn wir mit Karte zahlen, lesen sie von der Straße aus mit / W-Lan machts möglich

HAMBURG

Nennen wir ihn Horst Müller. Er kauft sich an diesem Nachmittag in einem Geschäft in Hamburg einen Anzug und zahlt mit Kreditkarte. Als die Kassiererin die Karte durchzieht, um die Daten auszulesen, sitzen draußen auf der Straße zwei Männer im Auto. Auf dem Laptop, das der eine auf dem Schoß hat, laufen im selben Moment Daten ein: Wertvolle Daten. Horst Müllers Name,seine Kreditkartennummer und deren Gültigkeitsdauer. Kurz: alles, was ein Betrüger wissen muss, um nach Herzenslust im Internet einkaufen – auf Horst Müllers Rechnung.



Einbruch in ein fremdes Netz per Funk: Die Daten sprudeln nur so auf den Rechner



Das Handwerkszeug der Datenspione: Laptop, W-Lan-Karte, Antenne

Betrug mit Kreditkarten – kein anderes Verbrechen boomt so wie dieses. Anders als bei ec-Karten werden bei der Bezahlung mit Kreditkarten keine Pin-Nummern benötigt. Umso unglaublicher ist es, wie fahrlässig Firmen mit den Daten ihrer Kunden umgehen.

Thorsten und Tobias sind zwei Hacker, so genannte „Wardriver", aus Hamburg. Die beiden Männer müssen anonym bleiben, weil das, was sie tun, illegal ist. Es ist ihr Hobby, in fremde Computer-Netzwerke einzubrechen. Eines Tages bemerken die beiden bei einer Tour durch die City, dass selbst namhafte Handelshäuser per W-Lan unverschlüsselt Kreditkarten-Transaktionen abwickeln. Sie informieren Mister X. Der will ihnen erst nicht glauben. Also bieten Thorsten und Tobias an, den Beweis anzutreten.

W-Lan bedeutet: kabelloses Netzwerk. Mehrere Rechner – in diesem Fall Kassen – sind nicht über Kabel, sondern per Funk mit dem Zentralrechner, dem Server, verbunden. Die Kasse sendet Daten, der Server fängt sie auf. So funktionierts. Eine äußerst praktische Erfindung – es gibt keinen Kabelsalat mehr. Andererseits: Jeder andere Empfänger im Umkreis kann die gefunkten Daten auffangen, wenn sie nicht verschlüsselt sind. Eine 100prozentige Garantie bietet aber auch eine Verschlüsselung nicht. Experten brauchen zwei Tage, um sie zu knacken.

Vergangene Woche Freitag: Lokaltermin. Nur 30 Minuten ist Mister X mit Thorsten und Tobias in der City unterwegs. 153 W-Lan-Netzwerke finden sie, davon 100 unverschlüsselt. Auf dem Laptop der beiden Datenspione gehen die E-Mails eines Rechtsanwalts ein. Auch auf das Netzwerk einer Baufirma hätten die beiden Zugriff nehmen können. Und – das schlägt dem Fass den Boden aus – sogar die W-Lan-Netzwerke von Ladenketten liegen offen vor ihnen. Unter dem Datenwust: jede Menge Kreditkartennummern.

„Kriminell" findet Oliver Bienkowski solche Fahrlässigkeit. Der 22-Jährige ist Boss der Firma iQ-Dynamix, die sich darauf spezialisiert hat, EDV-Anlagen sicherer zu machen. „Wir haben solche Tests auch schon durchgeführt. Wir wissen, dass jede größere Ladenkette mit unsicheren Funksystemen arbeitet."

Viele Unternehmen ahnen nicht mal, dass sie eine Sicherheitslücke haben. „Es kommt vor, dass es sich beispielsweise ein Versicherungsmitarbeiter bequemer machen will. Er installiert sich ein Funknetzwerk an seinem Arbeitsplatz." Bienkowski: „Wenn er die Verschlüsselung vergisst, haben Fremde plötzlich Zugriff auf sämtliche Versicherungsdaten." Dies sei keine Ausnahme. Bienkowski: „Das passiert täglich. Überall."

IT-Experte Oliver Bienkowski: „So viel Fahrlässigkeit ist geradezu kriminell"

OLAF WUNDER

SICHERHEITS-CHECK

Sind Sie sich ganz sicher, dass das EDV-System Ihrer Firma keine Sicherheitslücken aufweist? Lassen Sie es testen. „iQ-Dynamix" (www.iQ-Dynamix.de) führt **kostenlose Sicherheits-Checks** durch. Zwei Beratungsstunden sind gratis. Zum Zuge kommen die ersten 50 Unternehmen (keine Privatleute!), die heute diese Telefonnummer anrufen: **(040) 69 21 21 80.**

Fotos: Wunder

DIE GAUNER SIND ERFINDERISCH

Tricks der Karten-Mafia

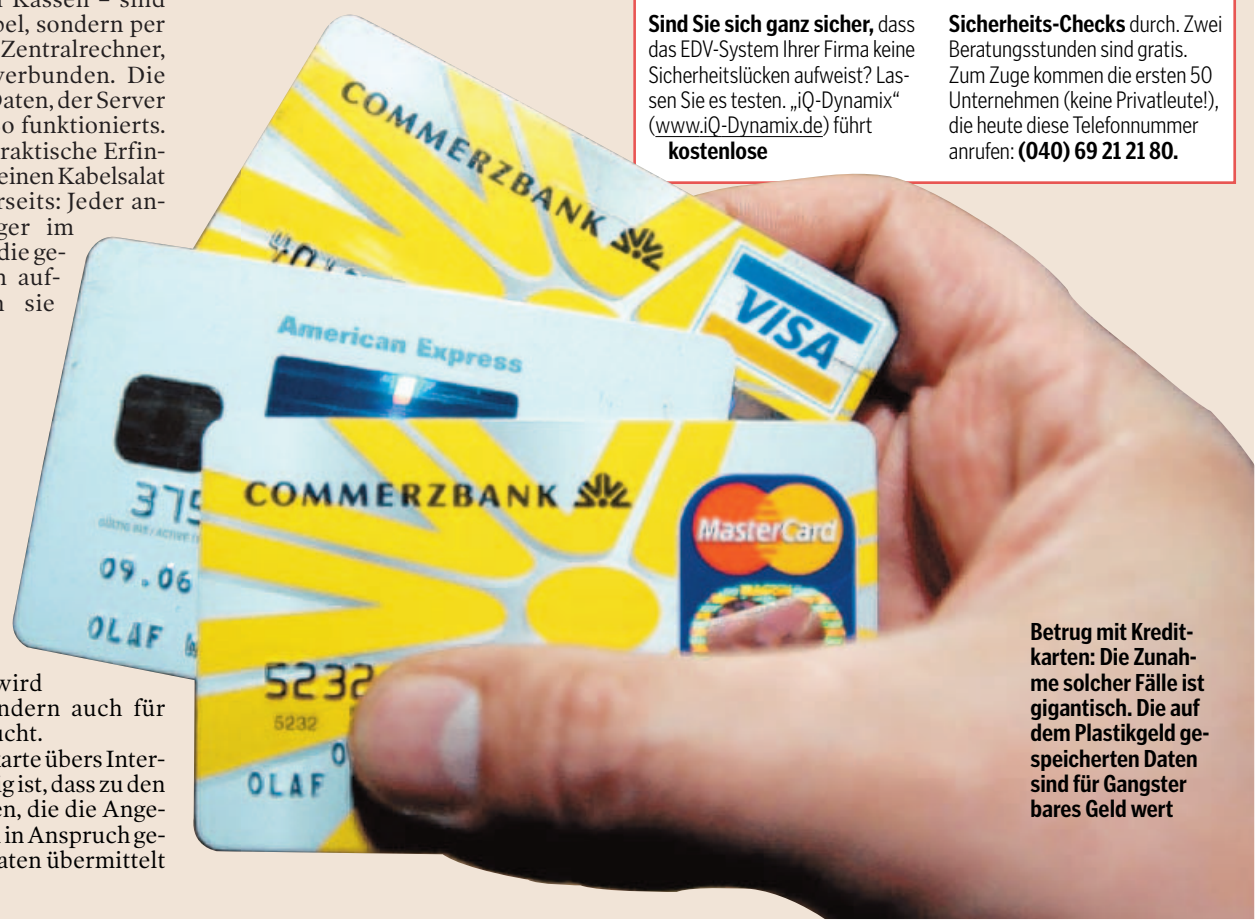
Neueste Masche: Sie schicken einfach eine E-Mail

Betrug mit Kreditkarten. Die Zunahme ist gigantisch: 64 507 Fälle gabs im vergangenen Jahr. Gegenüber 2002 ein Anstieg von 60 Prozent.

Die Tricks, wie die Gauner an die Kreditkarten-Daten kommen, sind vielfältig: Betrüger gehen raffiniert vor. Sie senden E-Mails, die den Eindruck erwecken, als stammten sie von einer Kreditkartenfirma. Darin wird den Empfängern vorgetäuscht, ihre Kreditkarten-Daten würden im Internet für Einkäufe missbraucht. Angeblich um diesen Missbrauch zu stoppen, werden die Karteninhaber aufgefordert, sämtliche Kartendaten per E-Mail zurückzuschicken.

Eine andere Methode: Ein Restaurantgast will seine Rechnung bezahlen. Der Kellner verschwindet mit der Karte - und kopiert sie heimlich. Später wird nicht nur Geld fürs Steak, sondern auch für Schmuck und Elektronik abgebucht.

Auch das Bezahlen per Kreditkarte übers Internet birgt große Gefahren: Auffällig ist, dass zu den Betrogenen oft Personen gehören, die die Angebote von Internet-Sex-Anbietern in Anspruch genommen und dazu ihre Kartendaten übermittelt haben.



Betrug mit Kreditkarten: Die Zunahme solcher Fälle ist gigantisch. Die auf dem Plastikgeld gespeicherten Daten sind für Gangster bares Geld wert