CSI: INTERNET

Folge 5

Diebstahl per Mail

Die Phishing-Mafia wird immer raffinierter. Das CSI-Team deckt einen gezielten Angriff in einem Internetcafé auf – und weist den Hacker in seine Schranken. *Von Valentin Pletzer*

Wenn das so weitergeht, kann ich meine Internetcafés dicht machen", schimpft Herr D. „Die ersten Kunden habe ich schon verloren." Er zeigt uns die Ausdrucke von Mails, die seit etwa zwei Wochen nur an Kunden seiner Internetcafé-Kette geschickt werden. Entsprechend verunsichert sind die Kunden und der Café-Besitzer.

Diese Phishing-Mails sind nahezu fehlerfrei formuliert und sprechen die Empfänger sogar mit ihrem richtigen Namen an. Von legitimen E-Mails sind sie so auf den ersten Blick nicht zu unterscheiden. Der Inhalt: „Im Zuge von Wartungsarbeiten prüfen wir derzeit sämtliche Benutzerkonten. Bitte besuchen Sie umgehend folgende Webseite. Falls Sie dieser Aufforderung nicht innerhalb von 24 Stunden nachkommen, sehen wir uns gezwungen, Ihr Konto aufzulösen und Ihr Guthaben verfällt. Bitte beachten Sie: Kein Mitarbeiter würde Sie per E-Mail um persönliche Daten bitten."

Die ungewöhnliche Phishing-Mail ist nicht alles: Einige Kunden glauben auch, dass ihre Kreditkartennummern über die Internetcafés ins Internet gelangt sind. Das lässt sich zwar nicht beweisen, doch der Imageschaden für die Kette ist enorm. Da die jeweils angegebene Webseite immer nur sehr kurz online ist, weiß Herr D. nicht viel über sie. Nur so viel: Passwörter oder Kundendaten, wie sonst auf Phishing-Seiten üblich, werden nicht abgefragt. Unser Team muss deshalb zunächst herausfinden, was der Täter überhaupt bezweckt.

Wir sehen uns erst einmal das Internetcafé genauer an. Es funktioniert so, wie ähnliche Einrichtungen auch: Gegen ein Entgelt darf der Kunde im Internet surfen, entweder über eine Surfstation oder mit dem eigenen Laptop per W-LAN. Bezahlt wird an der Kasse oder per Kreditkarte. Jeder Kunde bekommt sein ganz persönliches Konto, so dass das bestehende Guthaben in jedem Café der Kette genutzt werden kann.

Opfer werden zu Angreifern

Unser Team startet die Jagd beim einzigen Ansatzpunkt: der Phishing-Mail. Allerdings haben wir wenig Hoffnung: Für gewöhnlich werden solche Mails, wie auch Spam, über ein Botnetzwerk versendet. Das macht es fast unmöglich, die Verursacher zu finden. Die Versender sind in diesen Fällen selbst nur Opfer eines Hackers. Wir bitten Herrn D., uns die E-Mails in elektronischer Form zu zeigen. Denn was auf dem Ausdruck nicht zu sehen ist, sind die Kopfzeilen, die so genannten E-Mail-Header. Mit etwas Glück verraten sie uns, von welchem Server aus die E-Mails verschickt wurden.

Fehlanzeige! Wie befürchtet wurden die E-Mails nicht über einen regulären Server verschickt. Immerhin finden wir schnell heraus, dass der angegebene E-Mail-Server die IP-Adresse eines polnischen DSL-Providers hat. Vermutlich ist ein Kunde des Providers ebenfalls Opfer des Angreifers geworden. Auf unsere Anfrage erfahren wir vom Provider allerdings nur, dass es sich bei der IP tatsächlich um die Adresse eines Kunden handelt. Weitere Hilfe bleibt verwehrt. „Datenschutz", sagt der Provider. Immerhin wird uns versprochen, dass der betroffene Kunde über den Angriff informiert wird.

Tatort Internetcafé

DIE OPFER **Viele Besucher eines Internetcafés haben keinen eigenen PC und kennen sich nur oberflächlich aus – die perfekte Zielgruppe für jeden Hacker.**

Fotos: M. Miller; Vox aus „CSI"; CHIPimages

CHIP-Serie

In der US-Krimireihe CSI (in Deutschland bei RTL, VOX und 13th Street zu sehen) klären Forensiker Verbrechen mit wissenschaftlichen Methoden auf. CHIP nimmt CSI zum Vorbild für eine Serie, die zeigt, wie Profi-Ermittler die ausufernde Computer-kriminalität bekämpfen.

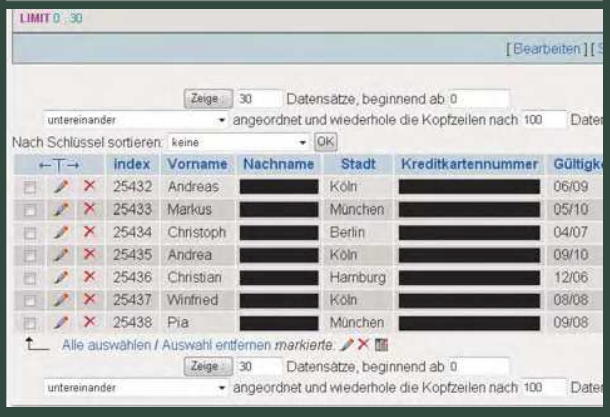
Und auch unsere zweite Spur, der Link in der E-Mail, bringt uns nicht weiter. Die Adresse ist längst nicht mehr erreichbar. Wenig überraschend, denn für gewöhnlich bleiben die Seiten nur kurz aktiv. Die Idee: Selbst wenn diese Seite geblockt wird, kommt der nächste Angriff von einer neuen Seite – und meistens wechselt der Server gleich in ein anderes Land. Eine Strafverfolgung ist so kaum möglich.

Eine Falle für den Hacker

Jetzt müssen andere Mittel ran: Wir stellen dem Hacker eine Falle. Wir melden uns als Kunden bei dem Internetcafé an. Mit einem Account an der Surfstation und einem per W-LAN und Notebook. Was dann passiert, überrascht uns. Bereits wenige Minuten später bekommen wir die erste Phishing-Mail. Zu schnell für bloßen Zufall. Wir forschen nach – und finden kurz darauf den Grund: der Chatraum des Cafés. Wer gerade online ist, wird automatisch auch dort angemeldet. Das Problem: Der Benutzername ist die E-Mail-Adresse – und diese setzt sich aus der Formel „Vorname.Nachname@domain.de“ zusammen. Für den Hacker ist es einfach, nicht nur die Adressen herauszufinden, sondern die Adressaten gezielt anzusprechen.

Dann geht es Schlag auf Schlag. Nun haben wir zwei weitere Spuren. Einerseits den in der E-Mail angegebenen Link, der so frisch ist, dass er noch zu einer existierenden Seite führt. Andererseits wissen wir jetzt, dass der Hacker ein ständiger Besucher des Chats sein muss – und damit werden wir seine IP-Adresse im Logfile des Servers finden.

Die Beute



GOLDGRUBE **Die kompletten Kundendatensätze aus gepflegten Datenbanken sind das begehrte Hacker-Ziel.**

Tatsächlich ist die Webseite des Hackers noch online – und sie enthüllt das Geheimnis um sein Motiv: Der Hacker hat es auf die zentrale Datenbank des Internetcafés abgesehen. Hier holt er sich die Kundendaten wie Kreditkartennummern sowie E-Mail-Adressen. Und dabei helfen ihm seine Opfer: Da das Netz des Internetcafés mit einer Firewall abgeschirmt ist, braucht der Hacker jemanden, der ihm von innen heraus ein Einfallstor öffnet – durch den Klick auf den Link in der E-Mail. Denn jedesmal, wenn jemand hinter der Firewall die Webseite öffnet, wird ein besonderes JavaScript aktiv. Mit einer Mischung aus Cross-Site-Scripting und SQL-Injection holt sich der Hacker die sensiblen Kunden-Informationen von dem Datenbankserver des Internetcafés. „Drive-by-Hacking“ heißt dieser Angriff im Fachjargon.

DER EXPERTE

Zulfikar Ramzan ist Sicherheitsexperte der Firma Symantec. Er warnt vor den Drive-by-Hacks, bei denen schon der Besuch einer manipulierten Seite reicht.

Einfallstore schließen

Wir ziehen einen Experten hinzu. „Nicht nur Firmen müssen sich vor dieser Art von Angriff in Acht nehmen“, sagt Zulfikar Ramzan von Symantec. „Vor allem W-LAN- und DSL-Router können Opfer von Drive-by-Hacking sein.“ Der Trick ist immer derselbe wie in unserem Fall: Der Hacker verschickt einen Link auf eine präparierte Seite. Sobald sie das Opfer öffnet, startet ein JavaScript im Browser und damit hinter der Firewall. Dann ist es ein Leichtes, den Router zu manipulieren und das Tor ins Netzwerk zu öffnen.

Jetzt würden wir den Hacker gerne für seinen Angriff zur Verantwortung ziehen. Doch wieder hat er vorgesorgt. Zwar hat er eine IP-Adresse im Protokoll des Chatservers als zweite Spur hinterlassen, doch diese führt uns nur zu dem Server eines Anonymisierungsdienstes. Unsere Spur endet hier. Einen kleinen Erfolg können wir dennoch verzeichnen. Herr D. wird seine Server – und damit auch die Kunden – in Zukunft besser schützen. Das Einfallstor des Hackers wird geschlossen und die Benutzernamen werden nicht mehr einsehbar sein. Allerdings kein endgültiger Schutz. Hacker finden immer neue Tricks – schon in der nächsten Ausgabe von „CSI: Internet“ werden wir weitere davon enthüllen. *valentin.pletzer@chip.de*

MEHR INFOS

www.symantec.com: Die Sicherheitsfirma beschäftigt sich mit den zunehmenden Gefahren des Drive-by-Hackings.