CHIP SERIE

CSI: INTERNET

Folge 1

Gefährliche Links

Mit einfachen Tricks knacken Hacker unbemerkt Online-Banken. Zum Auftakt der neuen Serie „CSI" zeigt CHIP, wie Profis solchen Attacken auf die Spur kommen. *Von Valentin Pletzer*

Michael M. wurde Opfer eines Hacker-Angriffs. Doch beweisen kann er das nicht. Keine offensichtliche Spur verrät die Tat: Das Server-Protokoll seiner Bank enthält nur seine IP-Adresse, sein Rechner ist frei von Viren, Spyware und Trojanern. Doch der Schaden ist da: Ein Rechnungsbeleg von über 2.000 Euro, ausgegeben für Elektronikzubehör in einem russischen Online-Versandhandel, beweist die Tat.

„Die PIN zu meinem Online-Konto kenne nur ich und die TANs sind sicher verwahrt", sagt Herr M. und beteuert: „Auf eine Phishing-Mail bin ich auch nicht hereingefallen. Ich weiß doch, dass mich die Bank nicht per E-Mail bittet, meine PIN und 20 TANs in ein Formular einzugeben."

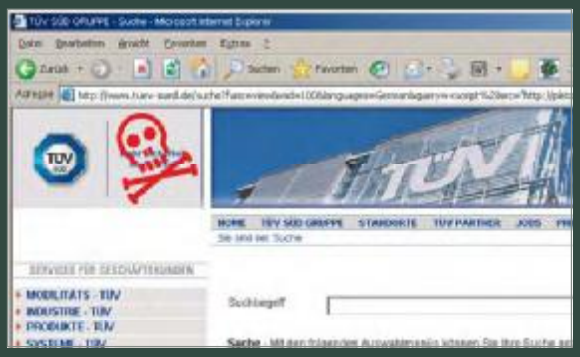
Fälle wie dieser gehören inzwischen zum Alltagsgeschäft von Betrugsermittlern. Denn extrem viele Webseiten weisen eine gefährliche Lücke auf, die es kreativen Hackern erlaubt, Cross-Site-Scripting-Angriffe zu starten. Zu den Betroffenen gehören zahlreiche bekannte Kreditinstitute – auf deren Seiten kann theoretisch jeder Opfer einer Hacker-Attacke werden. Auch Webseiten wie die des TÜV Süd, der doch mit seinem Namen für Sicherheit steht, konnten wir testweise hacken.

Zurück zu unserem Fall: In der Hoffnung, doch noch irgendwie an sein Geld zu kommen, bittet uns Herr M., der Sache nachzugehen. Gut, dass er seit dem Vorfall seinen Rechner nicht mehr angefasst hat. Denn wie die Forensiker in der Krimiserie „CSI" („Crime Scene Investigation"), dokumentiert eine CHIP-Spezialeinheit zur Spurensicherung den Tatort – also den PC und seinen Inhalt. Als Erstes können wir die Aussage von Herrn M. bestätigen: Der Rechner ist malwarefrei. Eine Manipulation durch Trojaner oder Keylogger können wir damit ausschließen. Der Fall bleibt rätselhaft. Wer hat sich Zugriff auf das Konto von Herrn M. verschafft? Und vor allem: Wie?

Spurensicherung am Tatort

Die erste Spur findet sich im E-Mail-Konto von Michael M.: eine Nachricht mit verlockenden Gewinnaussichten. »Klicken Sie hier um zum Gewinnspiel zu kommen.« Auf den ersten

TATORT WEBSITE



LEICHTE BEUTE **Viele Sites sind anfällig für Cross-Site-Scripting. Manche, wie die des TÜV Süd, wurden erst auf unseren Hinweis hin sicher. Jetzt stimmt auch der vom Hacker-Totenkopf überdeckte Slogan wieder: „Mehr Sicherheit, mehr Wert".**

WEITERE OPFER

Fotos: M. Miller Vox aus „CSI"

Neue 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.

Blick scheint die Nachricht unverdächtig, denn anders als bei einer Phishing-Mail verweist der Link tatsächlich auf den Bank-Server. Doch die Spur ist heiß: Die Webseite, die sich öffnet, kommt zwar von der Domain des Kreditinstituts, existiert dort aber nicht. Den Inhalt dieser Seite hat noch nie jemand anders zu Gesicht bekommen als Herr M. Hat ein Hacker den Inhalt per Man-in-the-Middle-Attacke in die Verbindung eingeschleust? Unmöglich: HTTPS, also die SSL-Verschlüsselung der Bankseite, verhindert derartige Angriffe.

Wir suchen weiter – und stoßen in der Mail auf eine weitere Spur. Die URL verweist auf die Suchseite der Bank, und dort, wo eigentlich ein Suchbegriff stehen müsste, findet sich eine ungewöhnlich lange Zeichenkette. Die Analyse ergibt: Es handelt sich um einen Hexcode, der sich beim Entschlüsseln in ein JavaScript verwandelt. Und zwar ein Script, das nicht auf den Servern der Bank liegt. Unser Verdacht: Herr M. wurde Opfer eines Cross-Site-Scripting-Angriffs (XSS).

Das Geheimnis des JavaScripts

Um zu verstehen, wie der Angriff abgelaufen ist, analysieren wir den JavaScript-Link im Labor. Erst einmal öffnen wir den Link, wie es auch Herr M. gemacht hat. Auf den ersten Blick passiert nichts Ungewöhnliches. Die Webseite lädt und präsentiert das angebliche Gewinnspiel. Ein Blick in den Quellcode der Webseite verrät jedoch mehr. Dort taucht nämlich der JavaScript-Code wieder auf, den wir bereits aus dem entschlüsselten Link kennen. Der Code steht genau an der Stelle, wo normalerweise der Inhalt der Suchmaske stehen sollte – ein klassischer Cross-Site-Scripting-Trick.

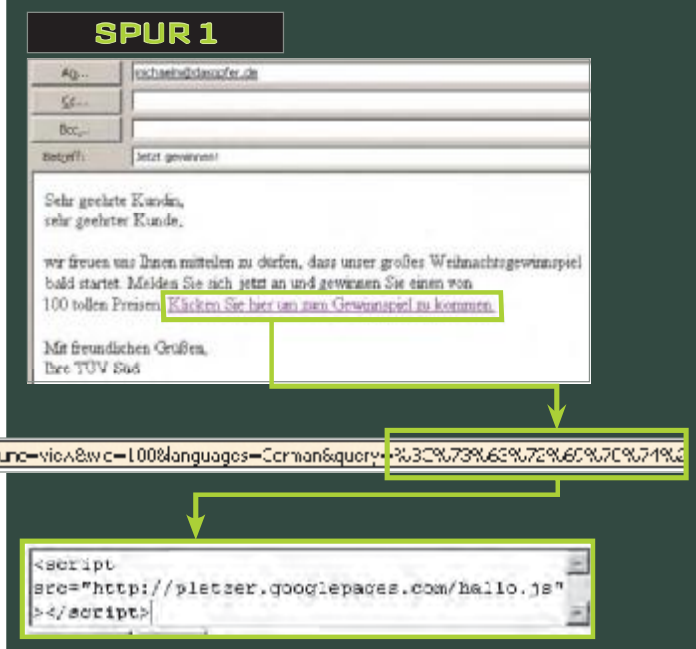
Uns ist sofort klar: Die Programmierer der Webseite haben versäumt, die Benutzer-Eingaben zu filtern. Der Hacker konnte deshalb das JavaScript-Tag ins Formular eingeben und musste nur auf »Suchen« klicken, um das Script in die Seite einzubauen. Auf der Ergebnisseite erschien dann nicht mehr: »Ihre Suche nach [Begriff] hat ergeben«, sondern »Ihre Suche nach hat ergeben«. Das JavaScript wurde automatisch an Stelle des Suchbegriffs eingebaut – und der Browser führte es aus. Danach musste der Hacker den Link der Ergebnisseite nur noch aus der Adresszeile in die E-Mail an Herrn M. kopieren.

Um die Theorie zu bestätigen, geben wir in die Suchmaske den ungefährlichen Testtext »';-"<XSS>=&{()}« ein – ein Trick, den wir uns bei Hackern abgeschaut haben. Und siehe da: Die unveränderten Zeichen »<XSS« im Quelltext der Bank-Webseite bestätigen die XSS-Verwundbarkeit.

Doch was bewirkt das JavaScript des Hackers? Um diese Frage zu klären, öffnen unsere Spezialisten die Datei und zerlegen die Funktionen. Ergebnis: Das JavaScript ist so angelegt, dass es die Bewegungen von Herrn M. auf der Homebanking-Seite überwacht. Bei seinem Versuch etwas zu überweisen, schlug der Hacker zu. Er blockierte den Versand der TAN und bat Herrn M. um eine neue. Mit der ergaunerten Kontonummer, der PIN und der TAN konnte der Hacker dann einkaufen gehen. Der Angriff ist also simpel – und der Hacker hatte Glück: Nur dadurch, dass sich Herr M. im richtigen Moment im Konto eingeloggt hat, konnte er die Bankdaten abgreifen.

So schützen Sie Ihre Website

Aktuelle Phishing-Filter sind machtlos im Kampf gegen Cross-Site-Scripting. Es gibt einfach zu viele Arten, den Inhalt einer Webseite zu manipulieren. Erschwerend kommt hinzu, dass die Angriffe nicht auf irgendeinem geknackten Webserver stattfinden, sondern auf den ansonsten sicheren Seiten einer Bank, eines Webshops oder eines Nachrichten-Magazins. Der einzige Rat kann also nur lauten: Nicht auf merkwürdige und vor allem sehr lange Links klicken, auch nicht, wenn es sich →



LOCKVOGEL E-MAIL XSS-Hacker müssen ihre Opfer dazu bringen, einen verseuchten Link zu besuchen. Hinter der URL verbirgt sich verschlüsselt ein bösartiges JavaScript.

DER EXPERTE

Johann-Peter Hartmann ist Geschäftsführer der Firma Mayflower. Sein Spezialtool Chorizo findet Sicherheitslücken in Webseiten.

um eine HTTPS-Seite handelt. Selbst bekannten Bank-Webseiten sollten Sie nicht bedingungslos vertrauen. Für sicheres Surfvergnügen kann im Prinzip nur einer sorgen: der Webmaster. Er muss die Eingabeformulare auf Webseiten gegen Manipulationen schützen. Im Idealfall heißt das: Bis auf Buchstaben und Zahlen sind alle Zeichen für die Eingabe in einem Formular tabu. Denn Sonderzeichen wie etwa die Spitzklammern < > interpretiert der Browser als Programmcode – und führt das möglicherweise gefährliche JavaScript aus.

Die dunkle Seite der Browser

Doch das simple Ausfiltern von JavaScript-Code reicht nicht, wie ein Blick in die Trickkiste der Hacker verrät. JavaScript braucht den HTML-Befehl »<script>« nämlich gar nicht unbedingt. Ein Skript lässt sich auch anders aufrufen, zum Beispiel über das »<img>«-Tag, das normalerweise Bilder in die Webseite einbindet. Der Befehl »<IMG SRC=jAVascriPt: alert(String.fromCharCode(88,83,83))« funktioniert in Opera 9.02 sowie Internet Explorer 6 und umgeht gleich mehrere Filter-Mechanismen. Denn er verzichtet weitestgehend auf Sonderzeichen und enthält gemischt Groß- und Kleinbuchstaben. Außerdem fehlt die abschließende Klammer. Dass die Browser diesen Befehl trotzdem ausführen, liegt an ihrer Fehlertoleranz. Da viele Webseiten kaputte HTML-Tags enthalten und ohne Fehlerkorrektur nicht funktionieren würden, sind die Browser-Entwickler dazu übergegangen, die Regeln etwas zu lockern. Aus dem Vorteil für die Nutzer wurde so eine Gefahr.

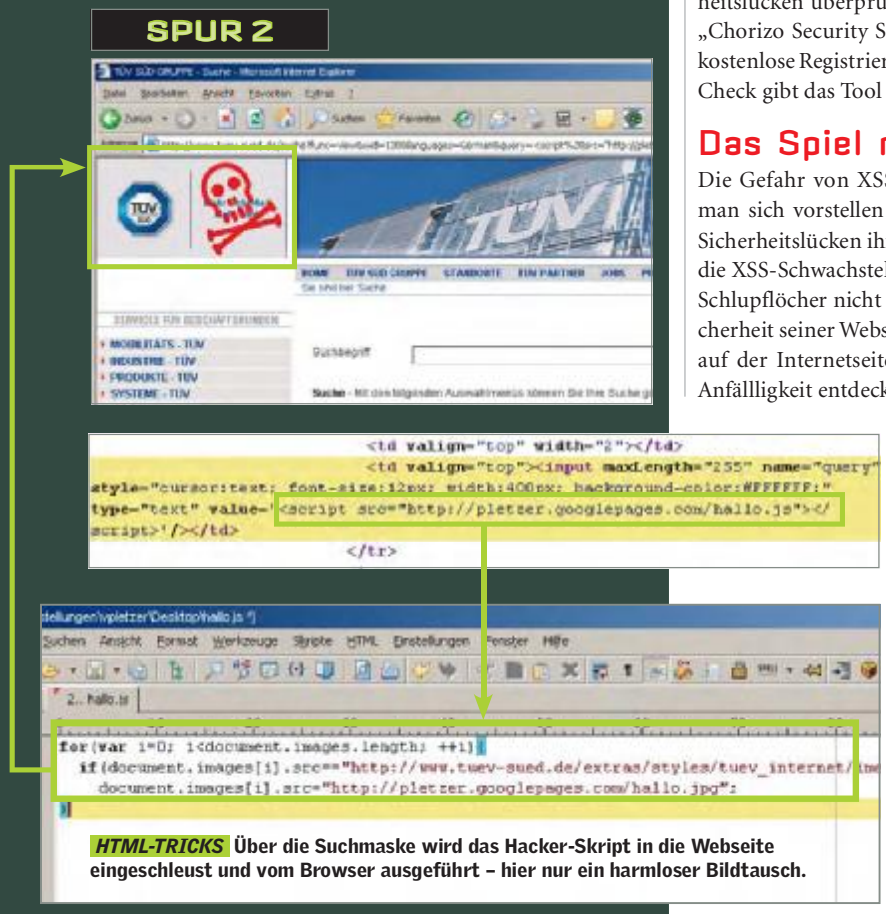
Wir wollten es genau wissen und befragten einen ausgewiesenen XSS-Experten. Johann-Peter Hartmann ist Sicherheitsexperte und Geschäftsführer der Firma Mayflower, die auf Anfrage Webseiten nach Sicherheitslücken durchsucht. Und Hartmann wird fast immer fündig: „Man glaubt gar nicht, wer alles betroffen ist." Wer seine eigene Webseite auf Sicherheitslücken überprüfen möchte, kann das mit dem Web-Tool „Chorizo Security Scanner" erledigen, Voraussetzung ist eine kostenlose Registrierung bei Mayflower. Nach dem Sicherheits-Check gibt das Tool an, wo genau sich die Lecks befinden.

Das Spiel mit der Sicherheit

Die Gefahr von XSS-Angriffen betrifft mehr Webseiten, als man sich vorstellen mag. Denn viele Webmaster kennen die Sicherheitslücken ihrer Seiten nicht einmal. Andere ignorieren die XSS-Schwachstelle geflissentlich. Doch wer solche Hacker-Schlupflöcher nicht so schnell wie möglich stopft, setzt die Sicherheit seiner Website aufs Spiel – und die ihrer Besucher. Als auf der Internetseite www.chip.de eine Cross-Site-Scripting-Anfälligkeit entdeckt wurde, haben die Programmierer sofort gehandelt und die Lücke geschlossen. Auch andere namhafte Firmen wie Apple oder Spiegel Online sind für Hinweise dankbar und schließen Schlupflöcher umgehend.

Doch damit sind längst nicht alle Gefahren gebannt, denn Hacker lassen sich ständig neue Angriffsmethoden einfallen. „Ihre Kreativität ist grenzenlos", bestätigt Johann-Peter Hartmann. Mehr dazu in der nächsten Folge von „CSI: Internet". *valentin.pletzer@chip.de*

SPUR 2



HTML-TRICKS **Über die Suchmaske wird das Hacker-Skript in die Webseite eingeschleust und vom Browser ausgeführt – hier nur ein harmloser Bildtausch.**

MEHR INFOS

https://chorizo-scanner.com: Hier gibt es das Web-Tool von Mayflower zum Aufspüren von Sicherheitslücken.