CSI: INTERNET

Folge 3

Vergiftete Pakete

Geknackte User-Accounts bei Amazon und eBay sind nichts Ungewöhnliches. Doch dieser Fall ist mysteriös: Die CHIP-Spezialeinheit ermittelt in Sachen Paket-Terror. *Von Valentin Pletzer*

Schon wieder ein Amazon-Paket für Sie", staunt der Postbote. Denn sogar er weiß inzwischen, dass Herr S. gar nichts im Internet bestellt hat. Rene S. ist verzweifelt und wendet sich an CHIP: „Seit vier Wochen geht das schon so. Ich bekomme Waren von Amazon und eBay, obwohl ich gar nichts bestellt habe. Sie müssen mir helfen."

Unser erster Gedanke: Wieder mal ein Fall von Account-Hacking, und zwar ganz klassisch mit Spyware. Damit werden dann Passwörter ausspioniert, im schlimmsten Fall sogar Kreditkartennummern. eBay-Accounts missbraucht der Hacker normalerweise so: Unter falschem Namen bietet er teure Artikel zum Verkauf an. Per Vorkasse räumt er dann ab – natürlich ohne die Ware zu liefern. Das Ungewöhnliche am Fall von Rene S.: Dieser Hacker hat es scheinbar gar nicht aufs Geld abgesehen. Denn ein finanzieller Schaden ist Herrn S. bisher nicht entstanden: Er schickte die Pakete einfach wieder zurück.

Also kein gewöhnlicher Spionage-Angriff! Neugierig geworden und mit Erlaubnis von Herrn S. macht sich die CHIP-Spezialeinheit an die Spurensicherung. Denn wie in der TV-Serie CSI gilt es, die Beweise streng nach Plan zu sichern. Wird etwas am Rechner verändert, ist er als Beweismittel später vor Gericht nicht mehr zu verwenden. Der Beschuldigte könnte behaupten, dass wir die Beweise dort platziert hätten. Deshalb erst mal die Festplatte ausbauen und klonen. Mit der Kopie können wir jetzt sämtliche Software gefahrlos ausprobieren.

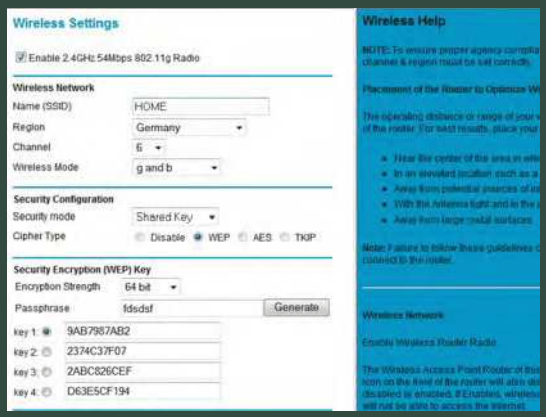
Forensische Festplatten-Analyse

Eine Internet Security Suite hat Herr S. nicht auf seinem Rechner, auch der Virenscanner ist schon lange nicht mehr auf dem aktuellen Stand. „Kein Wunder, dass sich hier unentdeckt Spyware einnisten konnte", meint einer vom CHIP-Team. Doch bei unserem Routinecheck finden wir weder Spyware noch Rootkits auf der Festplatte. Das kann aber auch darauf hindeuten, dass sich der Schädling nach seinem Auftrag selbst gelöscht hat, um die Spuren zu verwischen. Also versuchen wir im nächsten Schritt mit verschiedensten Undelete-Tools die

Paketlieferant

UNGEWOLLTE POST **Wer ungefragt Pakete von Online-Versandhäusern bekommt, hat wahrscheinlich ein Sicherheitsproblem in seinem Heimnetz – etwa mit Spyware und Rootkits.**

Erste Spur

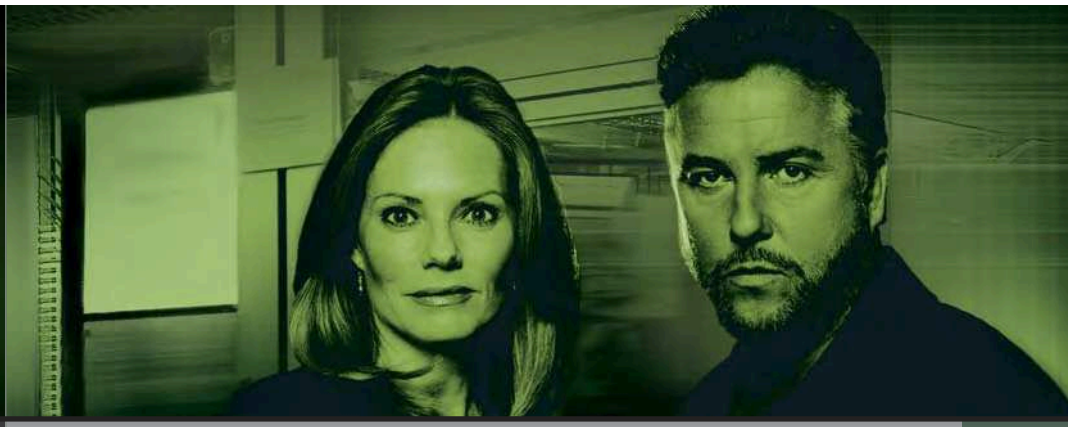


LEICHTE BEUTE **W-LAN-Netze mit schwacher WEP-Verschlüsselung lassen sich ganz einfach knacken. Viel sicherer sind die Standards WPA und WPA2.**

Fotos: M. Miller; Deutsche Post AG; 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.



Daten zu rekonstruieren. Doch auch hier: Fehlanzeige. Vermutlich wurde der betroffene Bereich bereits wieder überschrieben, die Daten unwiderruflich gelöscht. Also keine digitalen Spuren auf dem Rechner. Doch so schnell geben wir uns noch nicht geschlagen.

Gefährliche Peripherie

Wir weiten die Suche aus. Nicht immer ist der PC das Ziel des Hackers. Auch andere Geräte, die am Netz angeschlossen sind, kommen in Frage – zum Beispiel Drucker. Ist ein Netzwerkdrucker erst einmal unter der Kontrolle des Hackers, ist das fast genauso gefährlich wie Spyware auf dem Rechner. Denn dann kann er sämtliche Druckaufträge lesen. Und oft genug werden gerade sensible Daten wie Logins ausgedruckt.

Wir werfen einen Blick auf die Hardware im Netzwerk, doch bis auf ein Internetradio und einen W-LAN-Router gibt es dort nichts. Das schränkt die Auswahl für den Hacker ein. Zuerst nehmen wir das Radio unter die Lupe. Abermals eine Sackgasse. Das Gerät bietet kaum Manipulations-Möglichkeiten und ist ganz normal konfiguriert. Wir knöpfen uns den Router vor – und machen eine wichtige Entdeckung bei der W-LAN-Konfiguration: Statt einen sicheren Verschlüsselungsstandard wie WPA oder WPA2 einzusetzen, hat Rene S. die Funkverbindung nur mit WEP gesichert. Da selbst Anfänger diesen Schutz mit Tools wie WEPCrack oder AirSnort in wenigen Minuten knacken, prüfen wir noch einmal den Rechner von Herrn S. Dieses Mal suchen wir gezielt nach Sicherheitslücken und Netzwerkfreigaben, die dem Eindringling Zugriff auf die Daten erlauben könnten. Doch das Betriebssystem ist auf dem neuesten Stand und auch sonst entdecken wir keine Netzwerkzugänge.

Ein Köder für den Hacker

Da weder die Hardware noch die Software von Herrn S. angegriffen wurde, bleiben nicht mehr viele Möglichkeiten, sollte es sich tatsächlich um die Tat eines Hackers handeln. Wir haben einen Verdacht und konzentrieren uns auf einen alten, aber sehr wirkungsvollen Hacker-Trick: die Man-in-the-Middle-Attacke. Dabei klinkt sich der Angreifer ins Netzwerk ein, leitet den gesamten Datenstrom zu sich um und bekommt die volle Kontrolle über alle Daten. Er kann also Passwörter klauen und Inhalte manipulieren, bevor er die Daten an ihren eigentlichen Bestimmungsort weiterschickt.

Die Theorie steht – fehlt nur noch der Beweis. Wir beschließen, dem Hacker eine Falle zu stellen. Zunächst einmal muss Herr S. alle seine Passwörter neu setzen, das W-LAN-Passwort, den E-Mail-Account, das Amazon- und das eBay-Passwort.

Verdacht

HEIMLICHER LAUSCHER Bei einer Man-in-the-Middle-Attacke leitet der Hacker den Datenstrom zu sich um. Dazu gaukelt er dem Opfer vor, seine Rechner-IP sei die Adresse des Servers.

Damit wollen wir den Hacker aus seinem Versteck locken: Wenn er versucht, die Passwörter abermals zu klauen, soll die Falle zuschnappen. Um den Netzwerkverkehr zu überwachen, stellen wir zwei Beobachtungsrechner auf. Einer ist mit dem Tool „Netstumbler“ ausgerüstet und überwacht sämtliche Funknetzwerke in der Umgebung. Auf dem anderen Rechner läuft der Sniffer „Wireshark“, der alle Daten unseres Netzwerks aufzeichnet. Jetzt heißt es warten.

Die Falle schnappt zu

Eine Woche später ist es endlich soweit: Unser W-LAN-Beobachtungsposten schlägt Alarm. Der Hacker ist zurück! Wie vermutet, konnten wir ihn durch die geänderten Passwörter aus seinem Versteck locken. Wir beobachten, wie er die Netzwerkverbindung stört und so den PC von Herrn S. zwingt, sich am Router neu anzumelden. Der Trick ist bekannt und das erste Mal sind wir dem Hacker einen Schritt voraus. Er schickt jetzt genau die W-LAN-Signale an den Router, die er aufgezeichnet hat, als der PC sich dort neu angemeldet hat. Denn der WEP-Standard hat eine Schwäche: Manche W-LAN-Pakete verraten bei der Übertragung einen Teil des Passworts, allerdings nur einen kleinen. Der Angreifer braucht also sehr viele Pakete – etwa 70.000 bis 100.000. Wenn er einfach nur

DER EXPERTE

Max-Lion Keller, Rechtsanwalt und Spezialist für IT-Recht
www.it-recht-kanzlei.de

still lauscht, kann es Stunden oder sogar Tage dauern, bis die kritische Masse erreicht ist – falls Herr S. nicht zufällig lange surft und viele Pakete erzeugt. Unser Gegenspieler ist nicht so geduldig. Er startet eine so genannte Replay-Attacke: Mit einem Tool wie AirReply erzwingt er den Versand vieler Pakete. Für uns die ideale Gelegenheit, den Hacker ausfindig zu machen.

Mit drei Messgeräten bewaffnet, die die Feldstärke des Funknetzwerkes ermitteln, machen wir uns auf die Suche. Von drei Seiten bewegen wir uns auf das immer stärker werdende Signal zu. Dabei ist äußerste Vorsicht geboten, schließlich soll uns der Hacker nicht sehen und das Signal unterbrechen. Alles läuft nach Plan – und wir haben ihn: Der Hacker sitzt im Haus nebenan! Wir bleiben ruhig, beobachten, wie der Herr Nachbar weiter vorgeht. Und sammeln in aller Ruhe Beweise.

Hacker-Werkzeug

SIMPLER HACK **Mit Tools wie AirSnort kann jeder Anfänger W-LAN-Netze knacken. Einfach das Opfer eintragen und auf »Start« klicken – fertig.**

Plötzlich bricht die Replay-Attacke ab. Vermutlich hat der Hacker jetzt alles, was er braucht, um das WEP-Passwort zu knacken. Nun heißt es wieder warten. Je schneller ein PC ist, desto schneller knackt er ein WEP-Passwort. Unser Hacker braucht rund eine Stunde dazu. Mit dem gehackten Passwort meldet er sich sofort am W-LAN von Herrn S. an. Und beginnt mit der nächste Phase seines Angriffs: ARP-Poisening.

Der unsichtbare Dritte

Unser zweiter Beobachtungsposten schlägt Alarm und die Theorie von der Man-in-the-Middle-Attacke bestätigt sich. Bei ARP-Poisening wird das Netzwerk mit gefälschten ARP-Paketen überschwemmt. Also genau mit jenen Netzwerkpaketen, die einer MAC-Adresse die IP-Adresse zuordnen. In diesem Fall verbreitet der Hacker die Nachricht, dass die IP des Routers mit seiner MAC-Adresse verknüpft sei. Die Folge: Alle Netzwerkanfragen, die für den Router gedacht sind, landen erst einmal beim Angreifer. Damit die Verbindung für Herrn S. aber nicht abbricht, leitet der Nachbar die Pakete dann an die richtige MAC-Adresse weiter – also an den Router.

Welche Informationen der Angreifer aus dem Datenstrom ausliest, können wir nur vermuten – wahrscheinlich sämtliche Passwörter, die übertragen werden. Das betrifft zum Beispiel alle HTTP-Seiten mit einem Login, ebenso wie POP3-E-Mail-Accounts. HTTPS-Seiten sind zwar theoretisch geschützt, lassen sich aber durch einen Trick ebenfalls auslesen. Öffnet der Surfer eine HTTPS-Seite, werden Schlüssel und ein SSL-Zertifikat, das den Absender authentifiziert, ausgetauscht. Nur wenn das Zertifikat gültig ist, werden auch die Schlüssel akzeptiert. Ansonsten bekommt der Besucher eine Fehlermeldung, die darauf hinweist, dass das Zertifikat ungültig ist. Auf Wunsch des Besuchers wird der Schlüssel aber trotzdem akzeptiert. Diesen Umstand machen sich Hacker zunutze: Sie fahren ganz normal ihre Man-in-the-Middle-Attacke und schieben dem Opfer dann ein eigenes SSL-Zertifikat unter. Das verursacht zwar eine Fehlermeldung, doch die meisten Benutzer ignorieren diese Warnung – auch Herr S.: „Ich konnte mit dieser Fehlermeldung nichts anfangen. Und da ich anders nicht auf die Webseiten kam, habe ich die Meldung einfach ignoriert.“ Ein schwerer Fehler, denn genau da schlug der Hacker zu.

Konfrontation mit dem Hacker

Zusammen mit Rene S. stellen wir den hackenden Nachbarn. Der streitet alles ab und will nicht mit uns reden. Was ihn dazu bewogen hat, Herrn S. auf diesem Wege zu schikanieren, wird wohl erst vor Gericht geklärt. Die juristische Seite dieses Falls ist jedenfalls eindeutig, wie uns Rechtsanwalt Max-Lion Keller, Spezialist für IT-Recht, erklärt: „Greift jemand von außen unbefugt auf ein fremdes Funkdatennetz zu, das durch Verschlüsselung besonders gegen Zugriff gesichert ist, so macht er sich nach Paragraf 202a StGB strafbar, wenn er sich unbefugt Daten verschafft, die nicht für ihn bestimmt sind.“

Wie auch immer das Gericht entscheiden wird, Rene S. ist vor allem froh, dass der Paket-Terror jetzt ein Ende hat. Und zwar sowohl, was die Päckchen von der Post betrifft, als auch die „vergifteten“ Netzwerkpakete. In Zukunft will er sein Heimnetz besser absichern, öffentliche Hotspots ganz meiden. Wir drücken ihm noch unsere lückenlose Dokumentation in die Hand – und bekommen schon den nächsten Anruf. Mehr dazu in der nächsten Folge CSI:Internet. *valentin.pletzer@chip.de*

MEHR INFOS

www.oxid.it/cain.html: Hacker-Toolkit, das Netzwerke auf Man-in-the-Middle-Attacken hin überprüfen kann.