CSI: INTERNET

Folge 4

Einbruch per Handy

Im neuesten Fall des CHIP-Teams geht es um knallharte Wirtschaftsspionage. Ein SMS-Trojaner von Hightech-Produktpiraten besorgt geheime Baupläne. *Von Valentin Pletzer*

Herr M. ist fassungslos. „Schauen Sie sich das an“, sagt er. „Von diesem neuen iPod-Adapter sind bei uns gerade mal ein paar Vorserienmodelle im Umlauf, und trotzdem gibt es schon eine Kopie.“ Kopfschüttelnd drückt der Unternehmer uns zwei Modelle in die Hand – Original und Kopie. Der Klon ist vom Original kaum zu unterscheiden. Sogar das Platinenlayout der zwei Geräte ist identisch.

Herr M. ist der Chef eines kleinen Unternehmens, das sich auf Zubehör für Autoradios spezialisiert hat. Produktpiraterie ist keineswegs selten. Doch für gewöhnlich wird die Ware zumeist in asiatischen Fabriken kopiert, nachdem sie im Handel erhältlich ist – nicht schon vorher. Ein kniffeliger Fall für die CHIP-Spezialeinheit, die sich sofort an die Spurensicherung im Netzwerk und an den PCs macht. Wie in der TV-Serie CSI gilt es, sich zuerst ein vollständiges Bild der Situation zu machen und dann die richtigen Schlüsse daraus zu ziehen. Kein Detail ist zu unwichtig bei der Suche nach dem Leck, über das die Baupläne für den Adapter verschwunden sind.

Tatwaffe Handy

SCHUTZLOSE TELEFONE **Gegen die Trojaner-SMS ist derzeit kaum ein Handy geschützt. Ein Fehler im Mobilfunksystem macht es den Hackern leicht.**

Zuerst legt das CHIP-Team eine Inventarliste der Rechner und des Zubehörs an. Dabei machen wir eine erste Entdeckung: Ein PC ist per ISDN an der Telefonanlage angeschlossen. „Das ist unser Transfer-Server für den Datenversand“, klärt uns Herr M. auf. „Bei uns im Hause werden nur die Prototypen und Vorlagen entwickelt. Die eigentliche Fertigung der Geräte findet im Ausland statt.“ Wir haken nach und lassen uns den Ablauf erklären. „Jeder Mitarbeiter hat eine eigene Arbeitsstation. Damit auch jeder mit einer aktuellen Version arbeitet, werden die Blaupausen auf dem Server zentral gespeichert.“

Suche nach Schwachstellen

Neugierig geworden nehmen wir den Server genauer unter die Lupe. Uns scheint dieser PC ideal für einen Trojaner oder Spyware, da er alle wichtigen Daten bereitstellt und gleichzeitig ein Einfallstor in das kleine Netzwerk der Firma darstellt. Doch die Suche bringt kein Ergebnis: Der Server scheint frei von Malware zu sein. Protokolle über ein- und ausgehende Verbindungen gibt es nicht – was geradezu fahrlässig ist!

Wir weiten die Suche auf die übrigen PCs aus. Doch auch hier: Fehlanzeige. Kein Rechner weist ungewöhnliche Spuren auf. Wir ändern deshalb unsere Taktik und lassen uns von Herrn M. die Design- und Produktionsabläufe genau erklären, in der Hoffnung, den Ansatzpunkt der Datendiebe zu finden.

Nach wie vor scheint uns die einzige Möglichkeit ein Einbruch über den Server mit dem Internet-Anschluss zu sein. Da das Passwort jedoch täglich geändert und nur per Telefon an die Partner durchgegeben wird, fragen wir uns, wie das möglich sein kann. Wir wollen gerade die Telefonanlage unter die Lupe nehmen, da lässt uns eine beiläufige Bemerkung der Sekretärin aufhorchen. „Da brauchen Sie eigentlich gar nicht schauen. Der Chef telefoniert sowieso nur mit dem Handy.“

Wir lassen uns das Telefon geben – und tatsächlich: die erste heiße Spur. Die Konferenzschaltung des Handys ist aktiv. Das heißt, zu jedem Gespräch wird unbemerkt ein weiterer Gesprächspartner hinzugeschaltet. Herr M. ist sichtlich über-

Fotos: M. Miller; Vox aus „CSI“; J. König, Stock4B

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 Computerkriminalität bekämpfen.

rascht. „Ich wusste gar nicht, dass mein Handy so etwas kann“, sagt er. Muss er auch nicht. Denn die Konferenzschaltung wird über den Provider eingerichtet. Das heißt: Jeder Anschluss kann diese Funktion nutzen! Aktivieren muss die Konferenzschaltung aber der Benutzer selbst. Da Herr M. dies natürlich nicht gemacht hat, tippen wir auf einen Trojaner in seinem Nokia N90 und fangen an zu suchen. Doch Fehlanzeige. Die Forensiker finden nicht einmal neue Logos oder Klingeltöne. Herr M. telefoniert mit dem Handy einfach nur.

Doch die Telefonrechnung bestätigt unseren Verdacht. Die Konferenzschaltung hat eine teure Spur hinterlassen: Jeder Anruf wurde auch zu einer Telefonzelle im Ausland vermittelt. Da wir weder Software noch Malware gefunden haben, bleibt nur eine plausible Erklärung dafür übrig: ein SMS-Trojaner.

Kein Handy ist sicher

Wir ziehen einen Experten hinzu. Wilfried Hafner, Sicherheitsexperte der Firma Securstar, kennt SMS-Trojaner gut. „Mit nur 130 Zeichen knacken Sie jedes Handy“, sagt er. „Die Service-SMS macht es möglich.“ Er fügt hinzu: „In so wenig Zeichen können Sie natürlich keinen Trojaner verpacken. Aber Sie können den Befehl geben, einen herunterzuladen. Oder Sie aktivieren einfach eine vorhandene Funktion – wie hier die Konferenzschaltung. Das hat gleich noch einen Vorteil: Sie müssen das Betriebssystem auf dem Handy des Opfers nicht kennen.“ Denn das Handy-System ist für jeden Angreifer das größte Problem. Fast jeder Hersteller nutzt sein eigenes Betriebssystem. Um einen Trojaner einzuschleusen, müsste der Angreifer wissen, welches System auf dem Opfer-Handy läuft.

„OTA“-Programmierung (over the air programming) heißt die Technik, die der Hacker wohl angewandt hat. Eigentlich soll dieses Verfahren den Handy-Besitzern die Konfiguration von Diensten wie WAP abnehmen – eine SMS vom Provider reicht aus, um alle Einstellungen automatisch vorzunehmen. Eine OTA-SMS kann aber nicht nur der Mobilfunkbetreiber verschicken. Das kann jeder. Mit beliebigen Inhalten. Das wäre nicht so schlimm, würde sich das Handy jede Konfigurationsänderung bestätigen lassen. Doch mit einem Trick lässt sich auch dieser Schutz knacken. Die Software, um OTA-SMS zu erstellen, gibt es im Web.

Da wir nun wissen, dass das Handy von Herrn M. der Schlüssel zum Datenklau war, haben wir eine gute Vorstellung, wie der Hacker an die Pläne der Firma kam: Zuerst hat der Angreifer das Handy von Herrn M. per OTA-SMS umkonfiguriert und per Konferenzschaltung einfach mitgehört, wenn Herr M. das Passwort für den Server telefonisch weitergab. Mit diesem Wissen konnte er sich die Pläne dann herunterladen.

DER EXPERTE

Wilfried Hafner ist Geschäftsführer und Sicherheitsexperte der Firma Securstar. Er warnt vor der Handy-Sicherheitslücke

Schutz durch Verschlüsselung

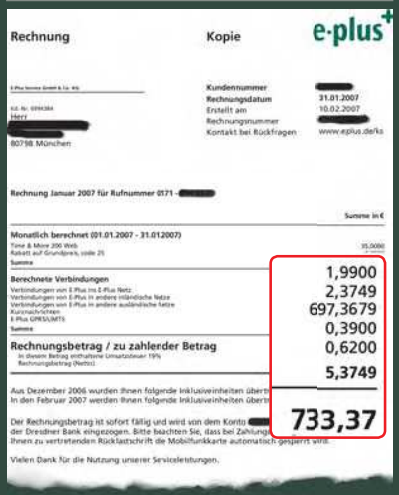
Wäre der Server so konfiguriert gewesen, dass er alle Verbindungen mitprotokolliert, wüssten wir zumindest, wohin die Daten gegangen sind. Aber auch dann wären wir vermutlich nicht weitergekommen. Führt die Spur etwa nach China, haben wir – und auch deutsche Behörden – kaum Möglichkeiten, den Hacker dort aufzuspüren.

Herrn M. bleibt die Erkenntnis, dass er sein geistiges Eigentum besser schützen muss. Die Passwörter wird er in Zukunft persönlich übergeben oder über eine verschlüsselte Verbindung verschicken. Außerdem darf nur noch von bestimmten IP-Adressen aus auf den Server zugegriffen werden. Das ist zwar nur eine kleine Hürde, aber sie verschafft Zeit bis zum nächsten Angriff der Produktpiraten. Weitere Tricks der Hacker in der nächsten Folge von „CSI:Internet“. *valentin.pletzer@chip.de*

MEHR INFOS

www.securstar.com: Auf der Webseite der Sicherheitsfirma gibt es das derzeit einzige Tool zum Schutz vor SMS-Trojanern.

Verräterische Spur


Rechnung

Kopie

e-plus

Kundennummer

Rechnungsdatum 31.01.2007

Erstellt am 10.02.2007

Rechnungsnummer

Kontakt bei Rückfragen www.eplus.de/ks

80798 München

Rechnung Januar 2007 für Rufnummer 0171 -

Summe in €

Monatlich berechnet (01.01.2007 - 31.012007)

Time & More 200 Web 15,0000

Rabatt auf Grundpreis, code 21

Summe

Berechnete Verbindungen

Verbindungen von E-Plus ins E-Plus Netz 1,9900

Verbindungen von E-Plus in andere inländische Netze 2,3749

Verbindungen von E-Plus in andere ausländische Netze 697,3679

Kurznachrichten 0,3900

E-Plus GPRS/UMTS 0,6200

Summe 5,3749

Rechnungsbetrag / zu zahlender Betrag 733,37

In diesem Betrag enthaltene Umsatzsteuer 19%

Rechnungsbetrag (Netto)

Aus Dezember 2006 wurden Ihnen folgende Inklusiveinheiten übert

In den Februar 2007 werden Ihnen folgende Inklusiveinheiten übert

Der Rechnungsbetrag ist sofort fällig und wird von dem Konto

der Dresdner Bank eingezogen. Bitte beachten Sie, dass bei Zahlung

Ihnen zu vertretenden Rücklastschrift die Mobilfunkkarte automatisch gesperrt wird.

Vielen Dank für die Nutzung unserer Serviceleistungen.

HOHE RECHNUNG
Die Telefonrechnung zeigt, dass etwas nicht stimmt. Hohe Gebühren für niemals erwünschte Telefonkonferenzen lassen uns sofort aufhorchen.