SICHERHEIT IM INTERNET
BERICHT ZUR INFORMATIONS- UND INTERNETSICHERHEIT

Group Information Security | Oktober 2013

© Vicente Barcelo Varona - depositphotos.com

ERLEBEN, WAS VERBINDET.

NACHRICHTEN

4 – 5 +++ SICHERHEITSLECK BEDROHTE HIGHTECHHEIZUNGEN +++ FEINDLICHE ÜBERNAHME DER SIM-KARTE +++ HACKER SABOTIERTEN NEW YORK TIMES +++ TAUSENDE WEBSEITEN FÜR MALWAREVERBREITUNG MISSBRAUCHT +++ SMART TV SPÄHT NUTZER AUS +++ PING OF DEATH TREIBT ERNEUT SEIN UNWESEN +++ ROUTERBOTNET VOM NETZ GENOMMEN

LERNEN

6 **HACKERFALLEN RUND UM DEN GLOBUS**
Die Telekom betreibt ein Frühwarnsystem, um sich ein eigenes Bild von der Gefahrenlage im Internet zu machen. 180 Honeypots detektieren täglich bis zu 800.000 Hackerangriffe.

9 **UMFASSENDES LAGEBILD**
Der runderneuerte Sicherheitstacho bietet neue Funktionen: Fokussierung der Anzeige auf ein bestimmtes Zielland.

SCHÜTZEN

10 **KEINE CHANCE FÜR SMARTPHONE-HACKER**
Hacker haben Smartphones mittlerweile genauso im Visier wie PCs. Wer fünf einfache Regeln beachtet, muss sich jedoch wenig Sorgen um die Sicherheit seines mobilen Endgeräts machen.

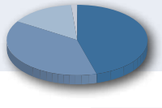
13 **CYBERZOMBIES**
Botnetze machen Opfer zu Tätern. Weltweit sind Millionen von Computern Teil eines Botnetzes, ohne dass ihre Besitzer davon wissen.

14 **16.762 KUNDEN IN EINER WOCHE**
Nach Aushebung des Citadel-Botnetzes erreichte eine Flut von Missbrauchshinweisen das Abuse-Team der Telekom. Innerhalb einer Woche kontaktierten die Mitarbeiter 16.762 Kunden – mehr als dreimal so viel wie gewöhnlich.

EINGREIFEN

16 **NEUE GEFAHR FÜR WEBINFRASTRUKTUR**
Reflected-Denial-of-Service-Angriffe sind bis zu 60 Mal stärker als herkömmliche DoS-Attacken. Sie gefährden nicht nur die ITK-Systeme der angegriffenen Unternehmen, sondern auch Teile der Webinfrastruktur.

18 **SICHERHEITSLÜCKEN AUF DER SPUR**
Interview mit **Bernd Eßer**, dem Leiter des Deutsche Telekom CERT, über das Management von Sicherheitswarnungen, mit denen Hard- und Softwarehersteller über Schwachstellen in ihren Produkten informieren.



20 **RECHTZEITIG GEWAPPNET**
Mit dem Bedrohungsradar stellt das Deutsche Telekom CERT die Entwicklung von Cybergefahren dar. Das Werkzeug dient dem Unternehmen dazu, Bedrohungen frühzeitig zu identifizieren und Sicherheitsmaßnahmen zu planen.

TEILEN

22 **MEHR TRANSPARENZ BITTE**
Im Gespräch mit **Sebastian Neef**, Mitgründer und Betreiber des Projekts „Internetwache“, über die Suche nach Schwachstellen in Webanwendungen und den Umgang der Unternehmen mit dem Thema Sicherheit.

Thomas Tschersich
Leiter IT-Sicherheit
Deutsche Telekom

LIEBE LESERIN, LIEBER LESER,

Transparenz und Kooperation sind die Leitmotive unserer Arbeit, mit der wir den Kampf gegen Cyberkriminalität antreten. Die Telekom informiert Sie zweimal jährlich über die aktuelle Bedrohungslage im Netz. Im vorliegenden fünften Bericht zur „Sicherheit im Internet“ zeigen wir Ihnen, welche Trends wir bei den Angriffen von Cyberkriminellen auf unsere eigens dafür aufgebaute Honeypotinfrastruktur beobachten. Wir informieren Sie darüber, wie wir unser Sensornetzwerk nicht nur quantitativ ausbauen, sondern auch kontinuierlich um neue Prototypen erweitern, um Sie auch künftig bestmöglich vor Gefahren aus dem Netz schützen zu können.

Wir teilen unser Wissen gerne mit Ihnen und kooperieren, wo immer es möglich ist, mit Forschungseinrichtungen, Industriepartnern, öffentlichen Institutionen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und anderen Internet Service Providern auf der ganzen Welt. Unser Ziel ist es, das Internet für Sie, für uns und für alle Menschen sicherer zu machen. Je besser wir zusammenarbeiten und je offener wir unser Wissen miteinander teilen, desto erfolgreicher halten wir mit Cyberkriminellen nicht nur Schritt, sondern versuchen ihnen eine Nasenlänge voraus zu sein.

In den vergangenen Monaten hat sich die Bedrohungssituation im Bereich mobiler Endgeräte verschärft. Der bislang komplexeste Trojaner für Android-Smartphones wurde entdeckt. Mobile Botnetze tauchen auf und es ist damit zu rechnen, dass sich dieser Trend in Zukunft fortsetzen wird. Wir haben einige nützliche Hinweise für Sie zusammengestellt, mit denen Ihre Daten und Ihre mobilen Endgeräte sicher bleiben.

Cyberkriminelle haben sich auch etwas Neues einfallen lassen, um die Infrastruktur von Unternehmen mit gezielten Denial-of-Service-Attacken (DoS) anzugreifen: Verstärkte Angriffe mit bis zu 60-facher Bandbreite gegenüber herkömmlichen DoS-Attacken markieren den neuesten Trend. Die Telekom arbeitet im Rahmen einer koordinierten Providerinitiative bereits mit dem BSI zusammen, um Maßnahmen gegen die neue Angriffsvariante zu entwickeln.

Machen Sie sich selbst ein Bild von der aktuellen Bedrohungssituation und verschaffen Sie sich einen Überblick über die Aktivitäten der Deutschen Telekom, mit denen wir die Gefahren und Risiken bekämpfen. Tragen Sie selbst zur Verbesserung der Sicherheit im Internet bei und teilen Sie uns mit, wenn Sie Sicherheitsschwachstellen entdecken. Wir freuen uns über Ihre Hilfe und stehen neuen Kooperationen offen gegenüber. Unsere Philosophie ist einfach: Security is for Sharing.

Herzlich Ihr

Thomas Tschersich

SICHERHEITSLECK BEDROHTE HIGHTECHHEIZUNGEN

Im April alarmierte der Hersteller Vaillant seine Kunden: Aufgrund eines Sicherheitsrisikos im Steuerungssystem liefen Mikroblockheizkraftwerke (BHKW) vom Typ ecoPower 1.0 Gefahr, von Fremden über das Internet manipuliert zu werden. Diese Hightechheizungen können nicht nur am Gerät selbst, sondern auch per iPad-App gesteuert werden. Sie lassen sich mit dem Internet verbinden und erlauben den Vaillant-Technikern, die Geräte aus der Ferne zu warten. Die Firma forderte ihre Kunden auf, das Netzwerkkabel vom Steuergerät der Anlage abzuziehen, um die Internetverbindung zu kappen.

© so47 – fotolia.com

MEHR SCHUTZ MIT VPN-TUNNEL

Weil es laut heise.de bis zu diesem Zeitpunkt sehr einfach war, an die Klartextpasswörter für die Fernwartung zu gelangen, hätten sich Dritte gegenüber der Heizung als Besitzer, Techniker oder Entwickler ausgeben können. Inzwischen gibt es ein Sicherheitsupdate des Steuerungsherstellers Saia-Burgess. Dennoch raten er und andere IT-Experten, die Anlage zusätzlich mit einem verschlüsselten VPN-Tunnel zu sichern.

FEINDLICHE ÜBERNAHME DER SIM-KARTE

Ältere SIM-Karten, die noch den Kryptografiestandard DES und 56-Bit-Schlüssel verwenden, können per SMS geknackt werden. Hacker nutzen dafür die Over-the-Air-Kommunikation (OTA) zwischen Mobilfunkprovider und SIM-Karte des Kunden aus. Darüber spielen Provider unter anderem regelmäßig Updates auf die mobilen Geräte ihrer Kunden, ohne dass die jeweiligen OTA-Nachrichten angezeigt werden. Schickt ein Hacker –„getarnt“ als Server des Providers – eine OTA-SMS an ein Mobiltelefon mit DES-Verschlüsselung, sendet das Gerät eine Antwort, über die sich der SIM-Schlüssel ableiten lässt. Mit dessen Hilfe kann der Hacker das Handy übernehmen, mithören und mitlesen sowie für kriminelle Zwecke umprogrammieren. Experten schätzen, dass weltweit noch mindestens 500 Millionen SIM-Karten mit DES verschlüsselt sind, die Ziele für potenzielle SMS-Attacken bieten. In Deutschland setzen die Netzbetreiber bereits seit rund zehn Jahren auf die sicherere 3DES- und AES-Verschlüsselung.

© leonardo255 – istockphoto.com

SMART TV SPÄHT NUTZER AUS

© manaemedia – fotolia.com

Sicherheitsexperten der TU Darmstadt wiesen im Mai darauf hin, dass über den TV-Standard HbbTV Daten über das Nutzungsverhalten mitgeschickt werden. Das Kürzel steht für Hybrid Broadcast Broadband TV und regelt die Art, wie TV-Geräte im laufenden Fernsehbetrieb auf Onlineinhalte zugreifen können. Bereits bei der Senderwahl, so die Forscher, kommuniziere der Fernseher mit dem Server der Sendeanstalt. Die dabei übertragenen Nutzerdaten könnten die Fernsehsender in Zukunft für personalisierte Werbung heranziehen. Ohne entsprechende Absicherung könne der Standard missbraucht werden: Es sei denkbar, dass unbefugte Personen Zugriff auf Funktionen wie die Kamera des Fernsehers erhalten.

FEHLANZEIGE BEI SCHUTZ VOR HACKERN

Anfang August demonstrierten die IT-Sicherheitsexperten Aaron Grattafiori und Josh Yavor auf der Sicherheitskonferenz Black Hat in Las Vegas, wie simpel es ist, Smart TVs von Samsung zu hacken. Angreifer können Zugriff auf Webcam und Mikrofon des Fernsehers erlangen und den Besitzer aus der Ferne ausspionieren. Möglich machen das vor allem vorinstallierte Apps wie Skype. Offenbar, so die Experten, wurde der Programmcode – er besteht aus HTML- und JavaScript-Code – fehlerhaft entwickelt. Weil die Skype-App auf die Benutzerschnittstelle von Kamera und Mikrofon zugreift, sind Wohnzimmerüberwachungen möglich. Der vorinstallierte Browser, der auf der HTML-Rendering-Engine WebKit beruht, ist eine weitere Gefahrenquelle: Wenn Hacker den Nutzer auf eine mit Schadcode infizierte Webseite lockten, könnten sie über eine klassische Drive-by-Attacke Kontrolle über den Fernsehapparat gewinnen.

PING OF DEATH TREIBT ERNEUT SEIN UNWESEN

© hainichfoto – fotolia.com

Im Rahmen seines monatlichen „Patchday“ hat Microsoft im August 2013 Maßnahmen gegen einen alten Bekannten ergreifen müssen: die „Ping-of-Death“-Attacke, bei der Angreifer via Internet Protocol (IP) gezielt große Datenpakete versenden, um beim Empfänger einen Pufferüberlauf nebst Rechnerabsturz zu verursachen. Die Schwachstelle war zu Zeiten von Windows 95 in Erscheinung getreten und galt längst als behoben. Nun ist sie mit der Protokollumstellung von IPv4 zu IPv6 wieder aufgetaucht und betrifft alle Windows-Versionen außer XP. Ein zweiter Ping-of-Death-Patch wurde für Windows-NAT-Treiber fällig.

UPDATES MANUELL INSTALLIEREN

Neben diesen beiden mit Schweregrad „hoch“ klassifizierten Patches hatte Microsoft unter anderem drei weitere Security Bulletins zu „kritischen“ Sicherheitslücken veröffentlicht. Darunter fiel ein Sammelupdate für den Internet Explorer, das Nutzer vor manipulierten Internetseiten und Malware schützt. Ebenfalls kritische Priorität erhielt ein Paket für Systeme mit Windows XP und Server 2003, das eine Sicherheitslücke im Unicode-Schriftengenerator schließt. Der dritte als kritisch eingestufte Patch dichtet ein Leck im Dateikonvertierer „Oracle Outside In“ ab, das in Exchange-Server-Versionen 2007 bis 2013 besteht.

Zum Patchday im September folgten 13 weitere Sicherheitshinweise. Microsoft stufte vier davon als kritisch ein, die Schwachstellen im Betriebssystem, im Internet Explorer sowie in Office und im SharePoint Server betreffen. Insgesamt schloss das Septemberupdate 47 Sicherheitslücken. Bei einigen Nutzern mit Windows Vista und Windows 7 traten jedoch Installationsprobleme auf. Sie sollten „automatische Updates“ in der Systemsteuerung deaktivieren und „Updates herunterladen, aber Installation manuell durchführen“ einstellen.

HACKER SABOTIERTEN NEW YORK TIMES

Syrische Unterstützer von Präsident Assad legten im August die Webseite der New York Times für mehrere Stunden lahm. Zeitweise war unter der Webadresse das Logo der „Syrian Electronic Army“ zu sehen. Die Angreifer hatten zuvor eine gezielte Phishingattacke auf den Domain Name Registrar Melbourne IT verübt und mit den erbeuteten Accountdaten die Verknüpfung zwischen der Webadresse www.nyt.com und der dazugehörigen IP-Adresse geändert. Die Times-URL führte fortan auf die Webseite der Angreifer. Das Domain Name System (DNS) ist für die Zuordnung der IP-Adresse eines Servers zur leichter lesbaren URL zuständig.

© WoGi – fotolia.com

DNS IM VISIER

Die „Syrian Electronic Army“ bekannte sich auf Twitter zu der Attacke und teilte mit, dass sie zeitweise auch die britische Ausgabe der Huffington Post sowie die Website Twitter.com unter ihre Kontrolle gebracht habe. Auch die Twitter-Profile großer Medienunternehmen standen bereits im Visier der Gruppe: Von Hackerangriffen waren die Financial Times, die britische BBC und die US-Nachrichtenagentur AP betroffen.

TAUSENDE WEBSEITEN FÜR MALWAREVERBREITUNG MISSBRAUCHT

Die niederländische Domainregistrierungsstelle SIDN, das Pendant zur deutschen DENIC, wurde Ziel eines Hackerangriffs. Betroffen waren Webseiten, die von den Anbietern Digitalus, Webstekker und VDX gehostet werden. Darunter befand sich auch die Seite der niederländischen Conrad-Electronic-Tochter. Besucher wurden zu einer „Under Construction“-Seite weitergeleitet, die deren Rechner über ein iFrame mit dem gefährlichen Blackhole-Trojaner infizierte.

© KAR – fotolia.com

Die Hacker hatten die DNS-Einträge derart modifiziert, dass die URLs auf Server zeigten, über die Malware verbreitet wurde. Obwohl der Angriff rasch entdeckt wurde, blieben die falschen DNS-Einträge in den Caches der meisten Endkunden-Internetdienstanbieter einen ganzen Tag lang erhalten, da ihre sogenannte „Time to Live“ (TTL) auf 24 Stunden festgelegt ist. Für SIDN war es bereits die zweite Attacke innerhalb weniger Wochen, nachdem Angreifer die Systeme zuvor per SQL-Injection kompromittiert und mit Malware verseucht hatten.

ROUTERBOTNET VOM NETZ GENOMMEN

Die Fachzeitschrift c’t berichtete, das Botnetz entdeckt und das LKA über den Fall informiert zu haben. Laut c’t hatten Hacker ein Schnüffelprogramm auf einer Vielzahl von Routern installiert, das Zugangsdaten aus dem Netzwerkverkehr extrahierte und an verschiedene FTP-Server übertrug. Der oder die Täter nutzten eine vier Jahre alte Schwachstelle der Routerfirmware DD-WRT aus, um eine manipulierte Firmware auf den Geräten zu installieren, die um ein Schnüffeltool ergänzt wurde, das unverschlüsselt übertragene Zugangsdaten aus dem Netzwerkverkehr entnimmt. Auf einem der FTP-Server befanden sich Zehntausende Dateien mit gestohlenen Zugangsdaten, etwa zu den E-Mail-Konten einer Anwaltskanzlei und den Bildern von Überwachungskameras einer Bäckereikette.

Gemäß Herstellerangaben war die ausgenutzte Schwachstelle der Firmware bereits kurz nach Bekanntwerden im Jahr 2009 geschlossen worden. Viele Internetnutzer aktualisieren die Firmware ihrer Router jedoch nicht und bieten Hackern langfristig ein Angriffsziel, wenn sie ihre Router über das Internet erreichbar machen. Telekom-Router waren nicht von dem Vorfall betroffen. Kunden erfahren unter nachfolgendem Link, wie sie das Problem der fehlenden Firmwareaktualisierung bei Telekom-Routern durch automatische Updates vermeiden können:

© Rynio Productions – fotolia.com

HACKERFALLEN RUND UM DEN GLOBUS

180 HONEYPOTS DETEKTIEREN TÄGLICH BIS ZU 800.000 HACKERANGRIFFE

Die Deutsche Telekom betreibt ein Frühwarnsystem, um sich ein eigenes, von Sicherheitsanbietern unabhängiges Bild von der Gefahrenlage im Internet zu machen. 180 Honeypotsysteme detektieren täglich Angriffe, die sich etwa ... ... gegen Standard-PCs, Smartphones und Serversysteme richten. Seit Kurzem zählen rund 100 neue Honeypots dazu, die auch Angriffe gegen die Telekom-Landesgesellschaften aufzeichnen und auswerten.

Honeypots sind Systeme, die Schwachstellen in Computersystemen simulieren, um Hackerangriffe anzuziehen. Ein Honeypot gibt etwa vor, ein Windows-basierter PC zu sein, der noch nicht mit dem letzten Sicherheitspatch des Herstellers versehen wurde. Die Telekom macht diese Systeme an strategisch wichtigen Zugangspunkten wie den eigenen Rechenzentren, DSL-Anschlüssen und dem Mobilfunknetz über das Internet zugänglich. Angreifer scannen sie und nutzen ihre Schwachstellen aus, um beispielsweise Schadsoftware einzuschleusen oder den vermeintlichen Rechner unter ihre Kontrolle zu bringen. Das alles findet in einer kontrollierten Umgebung statt, in der die Hacker keinen wirklichen Schaden anrichten können.

Die Honeypotsysteme zeichnen auf, wie die Angreifer vorgehen, welche Tools sie benutzen, von welchen IP-Adressen sie ihre Attacken ausführen, und leiten die entsprechenden Informationen in Echtzeit an das Frühwarnsystem der Telekom weiter. Dieses System wertet die Daten vollautomatisch aus und spielt sie an das Abuse-Team des Konzerns weiter, wenn es feststellt, dass die angreifenden IP-Adressen Kunden der Telekom zugeordnet werden können. „In diesem Fall“, sagt André Vorbach, einer der Sicherheitsexperten der Deutschen Telekom, die das Frühwarnsystem betreiben, „handelt es sich aller Wahrscheinlichkeit nach um Kundenrechner, die von Cyberkriminellen gekapert wurden, um als Teil eines Botnetzes andere Systeme zu attackieren.“ Das Abuse-Team informiert die betroffenen Kunden und sorgt dafür, dass sie diese Malware von ihren Computern entfernen können (mehr zu den Aktivitäten des Abuse-Teams lesen Sie auf Seite 14).

Mit dem Frühwarnsystem verfolgt die Telekom vier aufeinander aufbauende Ziele, die dem Schutz des Kunden dienen. Sie will eine eigene, **anbieterunabhängige Sicht auf die Angriffslage im Internet** gewinnen. Andere Informationsquellen stammen in der Regel von verschiedenen Sicherheitsanbietern. Deren Ergebnisse unterscheiden sich mitunter beträchtlich voneinander. Die Telekom führt ihre eigenen Erkenntnisse mit denen weiterer Quellen zusammen und erfüllt damit das zweite Ziel: ihren Kunden **bestmöglichen Schutz vor Onlinerisiken** zu bieten. An dritter Stelle steht der **Schutz der eigenen Systeme:** Indem die Telekom nachvollzieht, von welchen IP-Adressen Angreifer ihre Attacken ausführen, kann sie diesen Systemen den Zugang zu ihren Diensten erschweren.

NEUE SCHUTZFUNKTION ERSCHWERT HACKERN DEN ZUGRIFF

Ganz aktuell arbeiten Sicherheitsspezialisten des Konzerns im Bereich Forschung an einer neuen Schutzfunktion für Webseiten, dem „Dynamic Web Application Protector“, der bereits als erster Prototyp vorliegt. Diese Schutzvorrichtung soll Hackern künftig den Zugang zu Webseiten und Webapplikationen der Telekom und ihrer Kunden erschweren. „Versucht ein Internetnutzer zum Beispiel, eine Webseite der Telekom aufzurufen“, erklärt André Vorbach, „gleicht das System die IP-Adresse des Besuchers mit den IP-Adressen ab, die das Frühwarnsystem innerhalb der letzten 30 Minuten als Angreifer identifiziert hat.“ Stellt die Schutzfunktion eine Übereinstimmung fest, muss der Besucher eine nutzerfreundliche Captcha-Aufgabe (Completely Automated Public Turing test to tell Computers and Humans Apart) lösen, bevor er die Seite besuchen darf. So weist er nach, dass ein Mensch und nicht ein automatisiertes Computersystem hinter der Anfrage steckt, das einen Angriff ausführen könnte. Befindet sich die IP-Adresse des Besuchers nicht auf der sogenannten Blacklist des Frühwarnsystems, wird der Internetnutzer ohne Sicherheitsabfrage auf die gewünschte Seite weitergeleitet. Dies kann zielgerichtete Angriffe zwar nicht verhindern, erschwert aber automatisierte Attacken.“

Nicht zuletzt dient das Frühwarnsystem dem Ziel, die **Sicherheit des Internets für die breite Allgemeinheit zu erhöhen**. Die Telekom teilt ihre Erkenntnisse mit einer Reihe von Kooperationspartnern, die an das System angeschlossen sind. Dazu zählen Forschungseinrichtungen, Industriepartner und die Allianz für Cybersicherheit, eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die im Jahr 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde. Grundsätzlich gewährt die Telekom jedem Unternehmen und jeder Institution Zugriff auf die Daten, die ihre Honeypotinfrastruktur generiert, wenn der Partner seinerseits Informationen beiträgt. Transparenz und Kooperation sind die Basis für mehr Sicherheit im Internet. „Die Telekom ist offen für neue Kooperationspartner“, betont André Vorbach. „Je mehr Quellen der Sicherheitscommunity zur Verfügung stehen, desto besser können wir die Angriffslage einschätzen und darauf reagieren.“

HIMBEERKUCHEN MIT HONIG – 100 NEUE SENSOREN VERBESSERN DIE DATENBASIS

Zwischen Februar und Oktober 2013 hat die Telekom die Zahl ihrer Honeypots auf 180 aktive Sensoren erhöht. Der Großteil wurde auf Basis von Raspberry Pis aufgebaut, also sehr günstigen, kreditkartengroßen Einplatinencomputern. Auf diesem Wege war es möglich, die Sensorbreite äußerst effizient zu erweitern. Ein erster Prototyp entstand Anfang des Jahres als mobiler Raspberry-Pi-Honeypot, der die Eigenschaften eines Mobilfunkgeräts simulierte und Angriffe auf Smartphones registrierte. Die Daten, welche die Honeypots durch Attacken sammeln, senden sie zur weiteren Auswertung und Verteilung direkt an das Frühwarnsystem. „Wir haben die neuen Honeypots vor allem an unsere internationalen Landesgesellschaften ausgegeben“, berichtet Vorbach. „Dadurch erhalten wir eine verbesserte Sicht auf die aktuelle Situation.“

Im Bereich des mobilen Internets konnten die Sicherheitsexperten bereits einen Trend erkennen. „Etwa 75 Prozent aller Angriffe auf IP-Adressen, die wir an mobile Geräte vergeben, stammen aus China.“ Die überwiegende Zahl aller anderen Attacken geht in der Regel ebenfalls von China sowie Ländern wie Russland und den USA aus. Auch Deutschland befindet sich meistens unter den Top-5-Ländern, von denen Angriffe ausgehen. „Das sagt allerdings nichts darüber aus, in welchen Ländern die Angreifer beheimatet sind“, erklärt Vorbach. „Wir sehen lediglich, in welchen Ländern die Systeme stehen, die von ihnen über das Netz kontrolliert werden. Es sind größtenteils mit Schadprogrammen versehene Systeme, die aufgrund fehlender Sicherheitspatches infiziert wurden.“

Computersysteme, die keine Sicherheitspatches vom Hersteller erhalten, sind besonders anfällig, um von Cyberkriminellen gekapert und für Angriffe missbraucht zu werden. Internetkriminelle setzen diese und andere eroberte Rechner in erster Linie für den Versand von Spam, das Ausspähen von Kreditkarten- und Onlinebankingdaten sowie Denial-of-Service-Angriffe (DoS) ein, mit denen sie Webseiten und ganze Firmeninfrastrukturen lahmlegen können (mehr zu DoS-Angriffen finden Sie im Beitrag auf Seite 16). „Je besser das Frühwarnsystem funktioniert“, so Vorbach, „desto besser können wir Trends der Angreifer erkennen und entsprechend vorbeugen.“

Die Telekom erweitert ihre Honeypotinfrastruktur fortlaufend und entwickelt immer neue Prototypen, um einerseits mehr darüber zu erfahren, wie Cyberkriminelle vorgehen, und andererseits dazu beizutragen, dass infizierte Rechner möglichst schnell von Schadsoftware befreit werden.

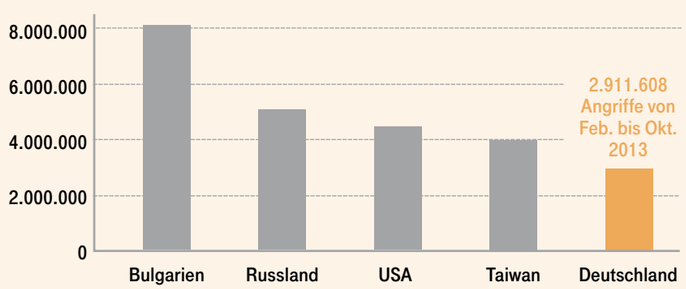
HONEYPOTVARIANTEN

Die Telekom setzt bei den verwendeten Frühwarnkomponenten auf quelloffene Software. Der generische Honeypot **Honeytrap** registriert eingehenden Netzwerkverkehr, und ist zudem in der Lage, auch bisher unbekannte Angriffe festzuhalten. Der dienstspezifische Honeypot **Kippo** simuliert den Konsolenzugang zu einem Server über SSH (Secure Shell) und erlaubt, Angriffe in Echtzeit nachzuvollziehen. Bei **Dionaea** handelt es sich um einen Multiprotokollhoneypot, der verschiedene Dienste simuliert, die aufgrund einer Vielzahl von Schwachstellen häufig angegriffen werden. Hinzu kommt die Software **Glastopf**, die angreifbare Webseiten simuliert. Neben diesen Open-Source-Systemen setzt die Telekom Eigenentwicklungen ein, die sie der Sicherheitscommunity ebenfalls quelloffen zur Verfügung stellt: Der **MySQL-Pot** simuliert einen erreichbaren Datenbankserver und registriert alle Verbindungsversuche. **Servletpot** simuliert eine weitere Webanwendung.

André Vorbach
Sicherheitsexperte
bei der Deutschen Telekom

DIE TOP 5 DER URSPRUNGSLÄNDER VON ANGRIFFEN

Im Zeitraum von Februar bis Oktober 2013 gingen die meisten Angriffe gegen die Honeypots der Telekom von Bulgarien, Russland und den USA aus. Hacker setzen unterschiedlich viele gekaperte Rechner für einen Angriff ein. Die meisten gekaperten und für Angriffe missbrauchten Rechner wurden in China, den USA und Deutschland lokalisiert.



Der Prototyp eines mobilen Honeypots der Telekom besteht aus einem kreditkartengroßen Einplatinencomputer mit UMTS-Stick, SIM-Karte, Display und zusätzlichem Akku.

EXPERIMENTE MIT NEUEN HONIGFALLEN
ANZAHL SIMULIERTER DIENSTE STEIGT

Drei neue Typen von Open-Source-Sensoren messen, wie und ob Industriesteuerungen, E-Mail-Konten und Konfigurationsmanagementsysteme angegriffen werden. Ein Ausbau der Testläufe in neuen Umfeldern ist geplant.

Die neuen Honeypots der Telekom detektieren auch Angriffe auf SCADA-Systeme, die in der Industriesteuerung zum Einsatz kommen.

Die Deutsche Telekom baut ihr Frühwarnsystem weiter aus und testet dabei neue Typen von Honeypots. Unter den Neuzugängen befinden sich drei weitere Open-Source-Sensoren. Zwei dieser Open-Source-Lösungen sind Fremdprodukte.

KONFIGURATIONSMANAGEMENT

Der dritte Sensor ist eine Eigenentwicklung der Telekom. Er gibt Aufschluss über Attacken, die sich gegen das Konfigurationsmanagementsystem Puppet richten. Mitte 2013 wurde eine aus dem Internet ausnutzbare Puppet-Schwachstelle veröffentlicht, was zur Entwicklung des Honeypots führte. Die Veröffentlichung des vollen Quelltextes ist geplant. Angriffe wurden noch keine gemessen.

E-MAIL

Im Juni hat die Telekom einen weiteren Honeypot eingeführt, der Spamangriffe aufzeichnet. Eingangstor ist eine IP-Adresse, an die unter normalen Umständen keine E-Mails gelangen können, weil die entsprechende Mailadresse unbekannt ist. „Wir dürften auf dem Zielrechner also keinen regulären Verkehr sehen. Daher lässt sich jeder Verbindungsaufbau als Angriff bzw. SPAM werten“, erläutert Markus Schmall, der das Honeypotprogramm der Deutschen Telekom leitet. Der neue Sensor ist ein Open-Source-Produkt, das der Entwickler Karl Krueger unter dem Namen smtpot veröffentlicht hat. Die Java-basierte Lösung registrierte bisher nur vereinzelte SPAM-Nachrichten. „Auch hier ist kein Ergebnis ein Ergebnis. Dieser erste Testlauf zeigt uns, dass keine flächendeckenden Scans auf offene E-Mail-Server ohne vorab bekannt gemachte E-Mail-Adressen durchgeführt werden. Die Ergebnisse müssen natürlich anhand weiterer Installationen validiert werden“, sagt Markus Schmall.

INDUSTRIESTEUERUNG

Seit Mai simuliert die Telekom mit einem Honeypot erstmals eine industrielle Steuerung (Supervisory Control and Data Acquisition, SCADA). Mit Conpot von Lucas Rist kommt eine weitere Open-Source-Entwicklung zum Einsatz. Der Sensor verwendet die Protokolle Modbus und SNMP. Beide Protokolle sind vergleichsweise schlecht abgesichert und bieten zahlreiche Angriffspunkte. Bisher beobachtete das Honeypot-Team 600 Zugriffe, die sich gegen das SNMP-Protokoll richteten und als Versuche zur Angriffsvorbereitung gewertet wurden. „Dieses Ergebnis sagt nichts über die generelle Angriffshäufigkeit auf Industrieanlagen aus. Sicherlich sind Angriffe auf SCADA-Systeme aber noch nicht so weit verbreitet wie automatisierte Angriffe auf Webportale“, kommentiert Markus Schmall. Zukünftig würden weitere SCADA-Honeypots an relevanten Stellen etabliert, um unterschiedliche Umgebungen besser abzudecken.

NEUER PROTOTYP: HONEYDROID
MOBILER HONEYPOT AUF ANDROID-SMARTPHONES

Ein neuer Prototyp bringt Honeypots auf speziell angepasste Android-Smartphones. Bereits seit Anfang 2011 betreibt die Deutsche Telekom als erstes Telekommunikationsunternehmen dedizierte Honeypots, die softwareseitig Netzwerkeigenschaften von Smartphones simulieren. Diese bisher auf einem Standard-Linux-System aufgesetzten mobilen Honeypots verhalten sich wie ein iPhone mit Jailbreak und ein Android-Smartphone mit Root-Zugang. Über gekoppelte UMTS-Sticks mit SIM-Karte sind sie an das Mobilfunknetz angeschlossen und bieten sich als attraktives Ziel für Hackerangriffe an. Was bisher in Rechenzentren betrieben wurde, hat die Telekom nun auf Smartphones gebracht. Der speziell an Android angepasste mobile Honeypot mit dem Namen „Honeydroid“ läuft zurzeit auf zwei Android-Endgeräten: einem Samsung Galaxy S4 und einem HTC Desire. Beide Smartphones lassen sich nahezu in vollem Funktionsumfang nutzen, während die installierte Software Angriffe aus dem mobilen Internet detektiert und an das Frühwarnsystem der Deutschen Telekom weiterleitet. Mit dieser Erweiterung ihrer Honeypotinfrastruktur verbessert die Telekom die Datenbasis ihres Frühwarnsystems erneut, um ihre Kunden auch künftig bestmöglich vor Hackerangriffen schützen zu können.

Der mobile Honeypot „Honeydroid“ läuft auf angepassten Android-Smartphones

UMFASSENDES LAGEBILD
SICHERHEITSTACHO NOCH GENAUER

Der runderneuerte Sicherheitstacho bietet neue Funktionen: Fokussierung der Anzeige auf ein bestimmtes Zielland.

Die Deutsche Telekom hat den Messradius ihres frei zugänglichen Sicherheitstachos erweitert. Das zur CeBIT 2013 vorgestellte Informationsportal hatte sich zunächst darauf konzentriert, Honeypotangriffe nach ihren Ursprungsländern darzustellen. Ab Mitte Oktober rücken auf der überarbeiteten Plattform (**www.sicherheitstacho.eu**) nun auch die Zielländer ins Blickfeld.

Das zugrunde liegende Sensornetzwerk besteht aus 180 Honeypots, die in zwölf verschiedenen Ländern aufgestellt sind. Der Sicherheitstacho zeigt Land für Land in Echtzeit, welche Angriffe auf die dortigen Sensoren erfolgen. Neben dem Liveticker hat die Telekom die „Top-15-Übersicht der Ursprungsländer“ länderspezifisch angepasst. Tachobesucher können sich seit dem Relaunch für jedes einzelne der zwölf Zielländer anzeigen lassen, aus welchen Ländern die meisten gegen sie gerichteten Angriffe stammen.

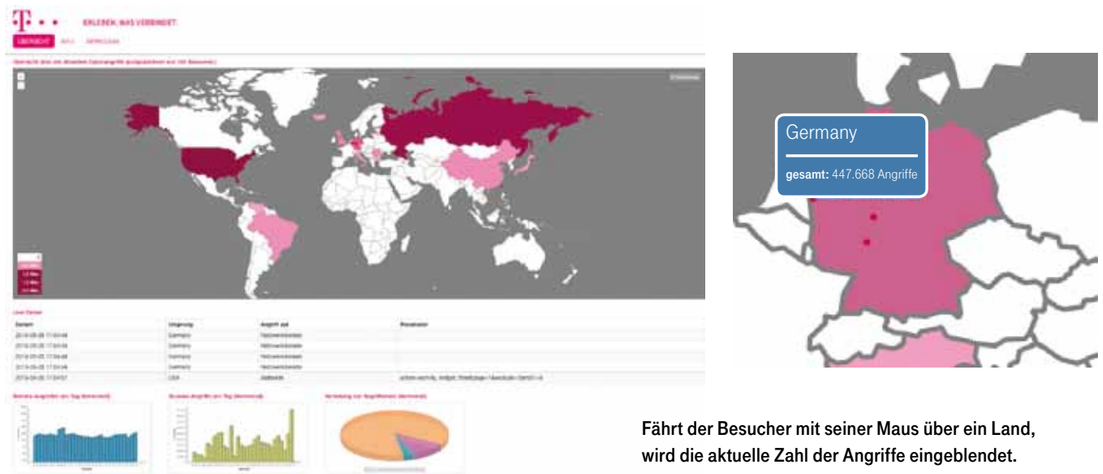
INFORMATIONEN ZUR ANGRIFFSSEITE

Die digitale Weltkarte illustriert das aktuelle Lagebild: Je dunkler ein Staat eingefärbt ist, desto mehr Angriffe wurden dort in den vergangenen 30 Tagen registriert. Bewegt der Tachobesucher den Mauszeiger auf eines der eingefärbten Länder, wird die absolute Zahl der Angriffe auf dieses Land eingeblendet. Fährt die Maus auf einen roten Punkt in der Karte, zeigt sie die Zahl der Angriffe und die Geokoordinaten des betroffenen Honeypotstandorts an. Aus welchen Ländern die Urheber der Angriffe stammen, lässt sich aus den Daten des Sensornetzwerks nicht ableiten. Bei der Mehrzahl der angreifenden IP-Adressen handelt es sich um Bot Clients, die über das Internet ferngesteuert werden. Die Standorte der im Hintergrund arbeitenden Command-and-Control-Server bleiben für die Honeypots unsichtbar.

Der Sicherheitstacho bietet eine Reihe grafischer Auswertungen, welche Aufschluss über die monatliche Verteilung und die technische Ausrichtung der Angriffe geben. Im Fußbereich des Portals findet der Besucher drei Diagramme mit Informationen zum Vormonat. Zwei Grafiken geben die Tagessummen sowohl der Angreifer als auch der Angriffe wieder. Während die Angreiferzahlen relativ konstant bleiben, offenbart die Verteilung der Angriffe deutliche Unterschiede, die auf die Art der zugrunde liegenden Attacken zurückgehen. Wesentlich hierfür sind wiederum die Botnetze. Je nach Auftragslage führen sie sehr unterschiedliche Angriffe aus, sowohl quantitativ als auch qualitativ. Das dritte Diagramm spiegelt die Verteilung der Angriffsziele wider. Die Grafik zeigt, dass sich 90 Prozent der aufgezeichneten Angriffe auf Netzwerkdienste beziehen, die von den Honeypots simuliert werden.

NEU: CYBERANGRIFFE JE ZIELLAND

Auf Wunsch zeigt der Liveticker des Sicherheitstachos laufende Angriffe auf Sensoren in einem bestimmten Zielland.
Der Tacho bereitet die Informationen der Honeypots aus dem gewählten Land in Echtzeit auf.



Fährt der Besucher mit seiner Maus über ein Land, wird die aktuelle Zahl der Angriffe eingeblendet.

SCHÜTZEN

KEINE CHANCE FÜR SMARTPHONE-HACKER
EINFACHE REGELN FÜR MOBILE SICHERHEIT

Hacker haben Smartphones mittlerweile genauso im Visier wie PCs. Wer fünf einfache Regeln beachtet, muss sich jedoch wenig Sorgen um die Sicherheit seines mobilen Endgeräts machen.

Mit einem Gerätekennwort schützt der Smartphone-Nutzer seine Inhalte vor fremdem Zugriff. Am besten ist eine Kombination aus Buchstaben und Zahlen.

Es ist wahr: Smartphones erfreuen sich in der Hackerszene wachsender Beliebtheit. Gefahr droht dabei grundsätzlich von zwei Seiten. Cyberkriminelle haben es einerseits darauf abgesehen, persönliche Daten auszuspionieren, und andererseits versuchen sie, mobile Geräte vollständig zu übernehmen, um sie für ihre Machenschaften zu missbrauchen. Mit Zugangsdaten für das Onlinebanking oder Kreditkarteninformationen wollen sie die Konten des mobilen Nutzers plündern. Kontaktdaten aus dem Adressbuch und andere persönliche Informationen dienen dem Social Engineering. Bei dieser Angriffsmethode täuscht der Hacker mithilfe ausspionierten Wissens eine falsche Identität vor, um geheime Informationen oder Dienstleistungen von bestimmten Personen zu erlangen. Je mehr der Hacker über seine Zielperson weiß oder je besser er die Person kennt, die er anderen gegenüber vortäuschen will, desto erfolgreicher kann er betrügen.

Die komplette Kontrolle über ein Gerät zu gewinnen, ist für Hacker aus verschiedenen Gründen attraktiv: Angreifer lassen gehackte Smartphones etwa teure Premium-SMS-Dienste nutzen oder Telefonate initiieren, ohne dass der Besitzer etwas davon merkt. Am Ende des Monats folgt dann das böse Erwachen, wenn die Telefonrechnung üppiger ausfällt als erwartet. Andere Hacker haben sich darauf spezialisiert, mit gekaperten Geräten Spam zu versenden oder sie als Teil eines mobilen Botnetzes Serversysteme angreifen zu lassen (mehr zu Botnetzen finden Sie im Beitrag auf Seite 13). Prinzipiell lassen sich mit Schadsoftware infizierte Smartphones für alle Untaten nutzen, die Hacker auch mit gekaperten PCs ausführen. Schließlich sind die mobilen Begleiter keine bloßen Telefone mehr, sondern äußerst leistungsfähige Computer im Hosentaschenformat.

MOBILE BOTNETZE SIND BESONDERS ATTRAKTIV

„Im Unterschied zu PCs“, weiß Wolfgang Bollenbach, Leiter des Teams Sicherheit in Office- und Kommunikationsdiensten bei der Deutschen Telekom, „sind mobile Endgeräte quasi rund um die Uhr online. Das macht sie für Hacker besonders interessant.“ Will ein Angreifer eine koordinierte Attacke zu einem bestimmten Zeitpunkt ausführen, gibt ihm ein mobiles Botnetz mehr Planungssicherheit. Während die meisten PCs berufstätiger Privatpersonen tagsüber ausgeschaltet sind, kann der Hacker davon ausgehen, dass die weit überwiegende Zahl der von ihm kontrollierten mobilen Geräte zu jedem beliebigen Zeitpunkt mit dem Internet verbunden ist. „Und durch die neuen Datendurchsätze mit LTE“, ergänzt Bollenbach, „hat ein mobiles Botnetz bald mehr Schlagkraft als ein traditionelles Botnetz, das aus gehackten PCs besteht.“

Smartphones werden Teil eines solchen Botnetzes, wenn sich der Nutzer eine App herunterlädt, die Sicherheitslücken oder Schwachstellen des mobilen Betriebssystems ausnutzt. Er kann sich auch mit Malware infizieren, indem er einen entsprechenden Link in einer E-Mail anklickt. Gegen Ende des Jahres 2012 wurde in den USA das erste größere Botnetz für das Android-Betriebssystem mit mehr als 10.000 Nutzern gefunden. Und im Sommer 2013 erregte ein komplexer Android-Trojaner Aufsehen, der drei bislang unbekannte Schwachstellen des Betriebssystems ausnutzte. Der Trojaner konnte alle möglichen Daten auslesen und über das Internet an den Angreifer verschicken, unbemerkt kostenpflichtige Premium-SMS-Dienste nutzen und sich über Bluetooth und WLAN auf benachbarte Geräte übertragen. Allerdings war die Installation der Schadsoftware nur möglich, wenn der Nutzer die Installation von Apps aus anderen Quellen als dem Google Play Store freigegeben hatte. „Diese Option in den Systemeinstellungen“, rät Bollenbach, „sollte der Anwender nicht freigeben.“

JAILBREAK HEBELT SICHERHEITSFUNKTIONEN AUS

„Die größte Bedrohung für mobile Endgeräte“, erklärt Wolfgang Bollenbach, „liegt in den unterschiedlichen Versionsgraden ihrer Betriebssysteme.“ Insbesondere bei Android-Geräten gibt es eine Vielzahl unterschiedlicher Endgeräte, die teils mit veralteten Versionen des Betriebssystems verkauft werden. In einigen Fällen schaffen es die Hersteller auch nicht, Betriebssystemupdates kurzfristig zur Verfügung zu stellen. Geräte mit einem veralteten Betriebssystem entsprechen dann nicht dem aktuellen Sicherheitsstandard und sie verfügen über Schwachstellen, die in neueren Versionen bereits geschlossen wurden. Besonders gefährlich wird Malware für Geräte, die durch einen Jailbreak (iOS) oder durch Rooten (Android) manipuliert wurden: Durch die Manipulation hebelt der Nutzer grundlegende Sicherheitsfunktionen aus und gestattet Apps den potenziellen Zugriff auf Systemfunktionen, die der Hersteller gesperrt hat. „Aus diesem Grund“, empfiehlt Wolfgang Bollenbach, „sollte jeder Nutzer regelmäßig Softwareupdates aufspielen und sein Smartphone keinesfalls selbst manipulieren oder manipulieren lassen.“

Aber auch ganz gewöhnliche Apps können ein Sicherheitsrisiko für die Daten des Nutzers darstellen. Bei der Installation verlangt eine Applikation Zugriff auf bestimmte Funktionen des Betriebssystems, um ordnungsgemäß funktionieren zu können. Eine Navigationssoftware etwa benötigt den Zugriff auf den GPS-Empfänger des Smartphones, um den Standort des Geräts bestimmen zu können. Kommunikations-Apps wollen in der Regel das Adressbuch auslesen, um die Kontakte des Benutzers ihrer Programmoberfläche hinzuzufügen. Viele Apps fordern jedoch fragwürdige und mitunter zusätzliche Rechte ein, die mit ihrer eigentlichen Funktionalität nichts zu tun haben. Muss die Kommunikations-App die Kontaktdaten des Nutzers in einen Cloud-Speicher übertragen? „Das mag für den einen oder anderen Nutzer praktisch sein“, sagt Wolfgang Bollenbach, „aber zumindest im Geschäftsumfeld ist davon unbedingt abzuraten.“ Spätestens, wenn eine Taschenlampen-App Zugriff auf das Adressbuch verlangt, sollten die Alarmglocken läuten. „Um sensible Daten zu schützen“, rät Bollenbach, „sollten sich Smartphone-Besitzer die Nutzungsbedingungen ganz genau durchlesen, bevor sie eine App installieren.“ Fordert eine Software zu viele Berechtigungen an, sollte er sie nicht installieren.

SICHERHEIT AM TELEKOM HOTSPOT

Die Deutsche Telekom hat ihre HotSpots kürzlich noch sicherer gemacht: Smartphone- und Tablet-Besitzer mit iOS- und Android-Geräten können ihre Verbindungen mit dem Telekom HotSpot durch einen sicheren VPN-Tunnel vollständig verschlüsseln. Die Einrichtung der Verschlüsselung ist in wenigen Schritten erledigt und steht dem Nutzer kostenfrei zur Verfügung.

Weitere Informationen zur VPN-Verschlüsselung bietet die Telekom unter:
www.telekom.de/hotspot-verschluesselung

FÜNF TIPPS FÜR MOBILE SICHERHEIT

Ob im beruflichen oder privaten Kontext: Wer folgende einfache Hinweise beachtet, muss sich keine Sorgen um die Sicherheit seines mobilen Endgeräts machen.

1. NICHT MANIPULIEREN

Manipulieren Sie Ihr Endgerät nicht durch einen Jailbreak (iOS) oder durch Rooten (Android). Damit hebeln Sie die Standardsicherheit des mobilen Betriebssystems aus.

2. NUR OFFIZIELLE QUELLEN NUTZEN

Laden Sie sich Apps ausschließlich aus den offiziellen App Stores (Apple App Store, Google Play) herunter. Apps haben die Sicherheitsprüfung der Hersteller bestanden, wenn sie dort angeboten werden.

3. APP-BERECHTIGUNGEN PRÜFEN

Prüfen Sie vor der Installation, welche Rechte eine App anfordert. Häufig verlangen insbesondere kostenlose Apps fragwürdige Zugriffsrechte, um etwa die Kontaktdaten auf dem Smartphone auszulesen.

4. VERTRAULICHKEIT BEACHTEN

Beachten Sie bei der Ablage von Unternehmensdaten in Cloud-Speichern wie Dropbox oder iCloud, dass Sie dort ausschließlich Dokumente mit der Vertraulichkeitsstufe „öffentlich“ ablegen. Das US-amerikanische Gesetz Patriot Act etwa erlaubt US-Behörden potenziell, auf diese Daten zuzugreifen.

5. PERSÖNLICHE DATEN SICHERN

Überprüfen Sie die Sensibilität von Inhalten, wenn Sie soziale Netzwerke wie Facebook nutzen. Geben Sie Hackern keine Möglichkeit, Identitäten und somit Wissen und Werte zu stehlen.

ROUTERINNOVATION VERHINDERT SPAM-VERSAND

Die neuen Speedport-Router der Telekom verfügen über eine Funktion, die den Versand von Nachrichten nur an eine vorgegebene, durch den Benutzer änderbare Liste von E-Mail-Servern erlaubt. Alle Router des Modells Speedport W724V und alle nachfolgenden Routergenerationen sind mit dieser Funktion

Der Speedport-Router W724V verfügt über eine neue Funktion der Telekom, um Spamversand automatisch zu verhindern.

ausgestattet, die standardmäßig aktiviert ist. Der Kunde kann die Liste bei Bedarf manuell erweitern oder die Funktion abschalten. Versucht ein Mailprogramm auf dem Rechner des Nutzers, einen anderen Postausgangsserver für den Mailversand zu verwenden, wird die Nachricht automatisch gestoppt. Damit verhindert der Router, dass eine Schadsoftware, die gegebenenfalls auf dem Kundenrechner installiert ist, Spam verbreitet. Diese Innovation wurde von der Telekom selbst entwickelt und ist zurzeit ausschließlich in ihren Speedport-Routern enthalten.

SPAM WIRD AUTOMATISCH GELÖSCHT

© victorschoffe – fotolia.com

„Mehr als zwei Drittel des gesamten E-Mail-Verkehrs weltweit bestehen aus Spam", kommentiert Rainer Schmidt, einer der Sicherheitsexperten der Telekom, der die Routerspezifikation geschrieben hat. Ein großer Teil der unerwünschten Nachrichten geht indirekt von den infizierten Rechnern von Privatpersonen aus. Eine installierte Schadsoftware verfügt häufig über ein integriertes Mailprogramm. Der Schädling liest nun etwa die Kontaktdaten im Outlook-Adressbuch des Nutzers aus oder erhält Adressen für den Spamversand über seine Steuerungsinstanz. Nun versucht er, Spam an die ermittelten oder erhaltenen Adressen zu verschicken. Häufig umgeht der Schadcode die eigentliche E-Mail-Infrastruktur (etwa der T-Online E-Mail-Server) des infizierten Kunden und kommuniziert direkt mit dem Eingangsserver des anzusprechenden Kontaktes. Verfügt der Kunde über einen der neuen Speedport-Router, endet die Reise an dieser Stelle: Befindet sich die URL oder IP-Adresse des E-Mail-Servers nicht auf der Liste vertrauenswürdiger Postausgangsserver, wird die Nachricht automatisch gelöscht.

E-MAIL MADE IN GERMANY

© bannosuke – fotolia.com

Kunden der Deutschen Telekom versenden ihre E-Mails seit Kurzem noch sicherer. Im August 2013 gaben die Deutsche Telekom und United Internet bekannt, die Nachrichten ihrer Nutzer von GMX, T-Online und Web.de ab sofort auf allen Übertragungswegen zwischen ihren Rechenzentren automatisch zu verschlüsseln und nur in sicheren Rechenzentren in Deutschland zu speichern. Die Partner trafen diese Vereinbarung im Rahmen der Brancheninitiative „E-Mail made in Germany", mit der sie die E-Mail-Kommunikation ihrer Kunden um einen weiteren Sicherheitsstandard ergänzen.

Beide Provider verarbeiten alle Daten ausschließlich gemäß den Vorgaben des deutschen Datenschutzes. Sie verschlüsseln die E-Mails ihrer Kunden automatisch. Weder technisches Know-how noch zusätzlicher Aufwand sind erforderlich. Außerdem führen sie eine Kennzeichnung für E-Mail-Adressen ein, anhand derer ein Nutzer bereits vor dem Mailversand erkennt, ob der Empfänger seiner Nachricht den Sicherheitsstandards des Mailverbundes entspricht. Der Weg vom Endgerät zum Mailserver war bereits zuvor für alle Kunden verschlüsselt, die eine Mailanwendung der Partner einsetzen, bzw. SSL-Verschlüsselung in ihren E-Mail-Programmen wie Outlook aktiviert haben. Ab April 2014 akzeptieren Telekom und United Internet konsequent nur noch SSL-verschlüsselte Mails, sodass der Datenverkehr, der bereits heute zwischen Serversystemen verschlüsselt übertragen wird, auf allen Übertragungswegen im Mailverbund sicher ist.

Weitere Informationen zu den Details der sicheren E-Mail aus Deutschland finden sich im Internet unter:
www.e-mail-made-in-germany.de

© cirquedesprit – fotolia.com

POST VOM ABUSE-TEAM MIT SIGNATUR

Das Telekom Abuse-Team versendet Kundenanschreiben künftig mit digitaler Signatur. Im E-Mail-Center der Telekom erscheinen Nachrichten von Mitarbeitern des Abuse-Teams ab Ende Oktober 2013 mit einem grünen Häkchen (trustedDialog), das Nutzer bereits von geprüften Absendern wie eBay, Otto und der Postbank kennen. „Wir versenden jeden Monat bis zu 25.000 E-Mails an unsere Kunden", sagt Nicol Riese, Mitarbeiterin des Abuse-Teams. „Manchmal sind sich die Kunden unsicher, ob diese Nachrichten tatsächlich von uns stammen." Um die Echtheit des Absenders nachzuweisen, setzt Abuse künftig auf das Signaturverfahren DKIM (DomainKeys Identified Mail). Es nutzt eine asymmetrische Verschlüsselung, um Nachrichten digital zu signieren und die Authentizität des Absenders sicherzustellen.

CYBERZOMBIES
BOTNETZE MACHEN OPFER ZU TÄTERN

Weltweit sind Millionen von Computern Teil eines Botnetzes, ohne dass ihre Besitzer davon wissen. Häufig zeigt ein Zombierechner nicht einmal Symptome, während der Bot seine Arbeit unbemerkt im Hintergrund verrichtet.

© jim – fotolia.com

Botnetze setzen ihren Vormarsch fort. Botfrei.de, das Anti-Botnet-Beratungszentrum des Branchenverbands eco, schätzt, dass rund ein Viertel aller Internetrechner Teil eines ferngesteuerten Computernetzwerks ist. Wie stark sich die illegalen Netze bereits ausgeweitet haben, lässt sich auch an den Preisen ablesen, die Cyberkriminelle für deren Nutzung zahlen: Für gerade einmal 10 Euro am Tag mieten Angreifer eine Bandbreite von 2 Gigabit pro Sekunde. Genug Schlagkraft, um mit einem Denial-of-Service-Angriff (DoS) so ziemlich jedes Unternehmen in ernsthafte Schwierigkeiten zu bringen.

BOTNETZVERBREITUNG DURCH INFEKTION

Wurden Schadcodes früher noch primär über verseuchte Dateianhänge in E-Mails verbreitet, so besteht der primäre Infektionsweg heute in sogenannten Drive-by-Attacken beim Besuch einer verseuchten Webseite. Weiterhin sind Microsoft-Windows-basierte PCs immer noch Angriffsziel Nummer eins. Konkret zielen die Angreifer seit 18 Monaten auch immer stärker auf Schwachstellen in der Java-Laufzeitumgebung ab, wohingegen noch vor zwei Jahren die Produkte der Firma Adobe (Acrobat und Flash) im Fokus standen.

Infektionen erfolgen heutzutage zumeist auf Basis kommerzieller Angriffswerkzeuge wie des Exploit Toolkit Blackhole und anderer. Diese Toolkits können auf Wochenbasis gemietet werden und bieten meist innerhalb von Tagen nach der öffentlichen Verfügbarkeit einer neuen Schwachstelle eine entsprechende Unterstützung an. Einige Entwickler gehen sogar so weit, dass Schwachstellen auf dem Schwarzmarkt speziell eingekauft werden.

BOT-CLIENT MUTIERT ZUM MEHRFACHTÄTER

Nach der initialen Infektion werden meistens weitere Schadcodes nachgeladen. Die Einsatzmöglichkeiten reichen vom SPAM-Versand für Werbezwecke bis zum groß angelegten Denial-of-Service-Angriff, der eine Vielzahl von Bot-Clients gleichzeitig nutzt. In Abhängigkeit von der aktuellen Auftragslage binden die Botnetze ihre Clients in die unterschiedlichsten Aktivitäten ein. Nicht zuletzt richten sich die Angriffe auch gegen den Client selbst. Da sich dessen Systemdateien vollständig auslesen lassen, werden zum Beispiel die Tastatureingaben mitgeloggt, um an Passwörter und Zugangsdaten des Nutzers zu gelangen.

Der Vielfalt der Szenarien entsprechend kommen sehr unterschiedliche Malwareprogramme zum Einsatz. Bot-Clients haben es daher keineswegs nur mit einem einzigen Trojaner zu tun, was viele Internetnutzer irrtümlicherweise annehmen. Mit der Zeit entwickeln sich die gekaperten Rechner zu einer Art Farm für Malware-schädlinge. Auf diese Weise mutiert der Bot-Client mehr und mehr zum multiplen Täter. Um wieder Herr im eigenen Haus zu werden, ist es ratsam, externen Rat einzuholen. Wertvolle Informationen liefert beispielsweise das bereits erwähnte Portal botfrei.de. Zudem bietet jeder Internet Service Provider einen sogenannten Abuse-Dienst, der die Kunden über relevante Gefahren aufklärt und im Infektionsfall Hilfe zur Selbsthilfe leistet. Das Abuse-Team der Deutschen Telekom ist erreichbar unter: abuse@telekom.de.

i

BOTNETZ

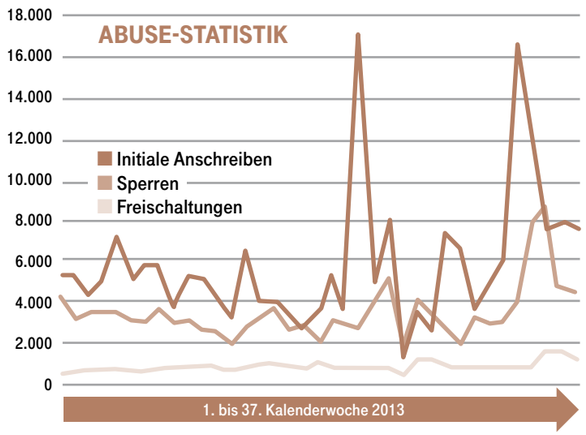
Botnetze sind illegal betriebene Computernetzwerke, die internetfähige Rechner ohne das Wissen ihrer Nutzer einbinden. Ist ein Computer Teil eines Botnetzes, lässt er sich über einen sogenannten Command-and-Control-Server (C&C) fernsteuern. Botnetze bestehen in der Regel aus zahlreichen kleineren, regional strukturierten Netzen. Auf diese Weise erlangen ihre Betreiber die Fähigkeit, weltweit flächendeckend aktiv zu werden. Als das FBI gemeinsam mit Microsoft Mitte 2013 das Citadel-Netzwerk aushob, stießen die Ermittler auf mehr als 1.000 kleinere Netzwerke in 80 Ländern.

SCHÜTZEN

16.762 KUNDEN IN EINER WOCHE
FAHNDUNG SORGT FÜR ABUSE-REKORD

Nach Aushebung des Citadel-Botnetzes erreichte eine Flut von Missbrauchshinweisen das Abuse-Team der Telekom. Innerhalb einer Woche kontaktierten die Mitarbeiter 16.762 Kunden – mehr als dreimal so viel wie gewöhnlich.

Bis Ende Mai lief alles in regulären Bahnen. Woche für Woche informierte das Abuse-Team der Deutschen Telekom durchschnittlich 5.000 Kunden darüber, dass ihre IP-Anschlüsse missbräuchlich genutzt werden (siehe Infobox Abuse-Management). Ende Mai änderte sich die Lage jedoch schlagartig: Innerhalb einer einzigen Woche versendeten die Abuse-Mitarbeiter dreimal so viele Anschreiben wie gewöhnlich. Wenige Tage zuvor hatte die amerikanische Bundespolizei weite Teile des weltweit operierenden Citadel-Botnetzes ausgehoben. Dieses Netzwerk hat sich auf den Raub von Bankkundendaten spezialisiert. Seine Betreiber sollen innerhalb von 18 Monaten mehr als 500 Millionen US-Dollar erbeutet haben. Selbst heute noch gilt das Netzwerk als teilweise aktiv. Die Betreiber wurden noch nicht gefasst.



DIE HÄLFTE DER KUNDEN REAGIERT

Der Schlag gegen das Netzwerk förderte bisher 93.885 IP-Adressen zutage, die von Kunden der Deutschen Telekom stammen. Im Rahmen der Abuse-Bearbeitung wurden alle Kunden identifiziert und angeschrieben. Erfahrungsgemäß berücksichtigt etwa die Hälfte der angeschriebenen Kunden die Empfehlungen der Missbrauchsspezialisten und reinigt ihre Computer von Malware. Bei den übrigen Kunden wiederholt das Abuse-Team die Ansprache. Nach einer Karenzzeit von vier Tagen sperrt die Telekom einzelne Dienste dieser Kunden, um die Verbreitung der Schadsoftware zu unterbinden und andere Internetnutzer zu schützen. Nach deren Ablauf stieg der Wochenwert der Sperren vorübergehend auf über 8.000, um sich Ende Juni wieder bei den üblichen 3.000 Sperren pro Woche einzupendeln.

ABUSE-MANAGEMENT

Das Abuse-Team der Deutschen Telekom nimmt jeden Monat etwa 1 bis 1,2 Millionen Hinweise über den vermuteten Missbrauch (engl. Abuse) ihrer Internetdienste entgegen. Missbrauch liegt etwa dann vor, wenn ein mit Malware

© alphaspirit – fotolia.com

infizierter Kundenrechner über einen Internetanschluss der Telekom andere Rechner attackiert oder Spam versendet. Sicherheitsorganisationen, Internet Service Provider und die Honeypots der Deutschen Telekom zählen zu den wichtigsten Hinweisgebern. Das Abuse-Team prüft die Hinweise auf ihre Relevanz, identifiziert die betroffenen Kunden und schickt ihnen per E-Mail und Briefpost einen Leitfaden zu, mit dessen Hilfe sie den Schadcode von ihren Rechnern entfernen können. Gehen von einem Kundenrechner weiterhin Angriffe aus, leiten die Abuse-Mitarbeiter zusätzliche Schritte ein: Um andere Nutzer zu schützen, können sie einzelne Dienste wie den E-Mail-Versand vorübergehend sperren.

SIEBEN TAGE, UM ZU REAGIEREN

Das Abuse-Team hat sieben Tage Zeit, um externen Hinweisen nachzugehen und die betroffenen Kunden zu ermitteln.

© Alexey Potapov – Fotolia.com

Nach Ablauf der sieben Tage werden die gespeicherten IP-Adressen gelöscht. Diese Praxis stimmt mit dem deutschen Telekommunikationsgesetz überein und wurde zuletzt am 28. August 2013 vom OLG Frankfurt als rechtmäßig bestätigt.

INTERVIEW

ACHTUNG, UPDATE!

Markus Weyrich
Mitarbeiter des
Telekom Abuse-Teams

Phishing war gestern. Botnetze haben inzwischen weit wirksamere Mittel, um Fremdrechner in ihre Dienste zu spannen. Markus Weyrich, Mitarbeiter des Telekom Abuse-Teams, erklärt, was Anwender wissen müssen und wie sie sich mit einfachen Mitteln erfolgreich zur Wehr setzen.

Wie schaffen es Botnetze, Internetrechner unter ihre Kontrolle zu bringen?
Markus Weyrich: Die Möglichkeiten sind sehr vielfältig. E-Mail-Phishing galt lange als Königsweg. Hier ist das Bewusstsein der Anwender jedoch so stark gestiegen, dass sich kaum noch jemand auf dem falschen Fuß erwischen lässt. Entsprechend wenden sich Botnetzaktivisten anderen Methoden zu. Das mit Abstand am häufigsten genutzte Mittel sind sogenannte Drive-by-Infektionen. Hierbei kommt gut getarnte Schadsoftware zum Einsatz – so zum Beispiel der Trojaner ZeroAccess, der unseren Kunden derzeit den meisten Ärger bereitet. Ende August mussten wir dreimal mehr Kunden über eine Infektion ihrer Rechner informieren, als dies in normalen Wochen der Fall ist (siehe Abbildung auf Seite 14).

Wie geht ein solcher Schädling vor?
Markus Weyrich: Ausgangspunkt sind infiltrierte Webserver, auf denen die Angreifer ihre Malware in Stellung bringen. Typischerweise laufen Drive-by-Infektionen dann in mehreren Schritten ab, die aufeinander aufbauen. Besucht ein Internetnutzer eine infiltrierte Webseite, überprüft die Malware dessen Rechner erst einmal auf gängige Schwachstellen. Häufig nutzen die Angreifer auch nur die Gutgläubigkeit der Opfer aus. Einem Opfer wird etwa suggeriert, dass ein neues Softwareupdate für eine populäre Anwendung vorliegt oder dass eine Zusatzkomponente installiert werden muss, um einen bestimmten Film abzuspielen. Tückischerweise setzen die Angreifer exakt bei solchen Technologien an, bei denen sich die Anwender bereits an häufige Updates gewöhnt haben. So etwa bei Java, den Adobe-Produkten oder den Add-ons ihres Internetbrowsers. Wer die gefälschte Updateaufforderung dann bestätigt, öffnet dem Botnetz Tür und Tor, um beliebigen Schadcode auf seinen Rechner zu laden.

Wie kann ich als Normalsterblicher überhaupt noch entscheiden, welchen Updatenachrichten zu trauen ist?
Markus Weyrich: Nun, selbst ein Profi muss schon sehr genau hinschauen, um eine seriöse Nachricht von einer gut gemachten Fake-meldung zu unterscheiden. Daher raten wir jedem Nutzer, die aufpoppenden Checkboxen konsequent zu verwerfen und stattdessen auf die Webseite des betreffenden Softwareherstellers zu wechseln, um sich das erforderliche Update von dort aus zu holen. Zugegebenermaßen wird das Leben dadurch nicht gerade einfacher. Andererseits hat eine solche Vorkehrung aber auch ihr Gutes. Sie ist ein ausgesprochen wirksames Mittel, um den Wildwuchs auf unseren Rechnern zu begrenzen. Sobald wir die Aktualisierung einer Software selbst in die Hand nehmen, werden wir uns viel genauer überlegen, ob und wozu wir diese Applikation brauchen.

Gibt es zusätzliche Dinge, die Internetnutzer beachten sollten?
Markus Weyrich: Die gibt es. Im Endeffekt sind es aber gar nicht einmal sonderlich viele Dinge. Der allerwichtigste Rat gleich vorneweg: Gehen Sie nur dann ins Netz, wenn Sie als dedizierter Nutzer an Ihrem Rechner angemeldet sind. In diesem Fall hat die angreifende Malware keinen Zugriff auf Administratorrechte, um sich auf Ihrem Rechner festzusetzen. Wer demgegenüber als Administrator im Netz unterwegs ist, geht volles Risiko. Darüber hinaus sollten Sie sicherstellen, dass sich Ihr Betriebssystem regelmäßig aktualisiert und die mitgelieferten Sicherheitswerkzeuge, allen voran die Firewall des Betriebssystems, eingeschaltet sind. Wenn Sie dann noch einen aktuellen Virenscanner nutzen, haben Sie alles getan, was ein normaler Internetnutzer tun sollte.

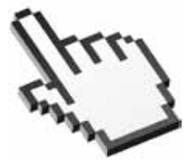
© shockfactor – fotolia.com

ZEROACCESS

Der Trojaner „ZeroAccess“ befällt Microsoft Windows-Betriebssysteme. Er lädt weitere Schadsoftware auf ein infiziertes System, um ein Botnet aufzubauen. Mithilfe von Rootkittechniken verbirgt sich ZeroAccess vor dem Nutzer.

NEUE GEFAHR FÜR WEBINFRASTRUKTUR

GEFÄHRLICHE FEHLKONFIGURATIONEN IN DNS-SERVERN

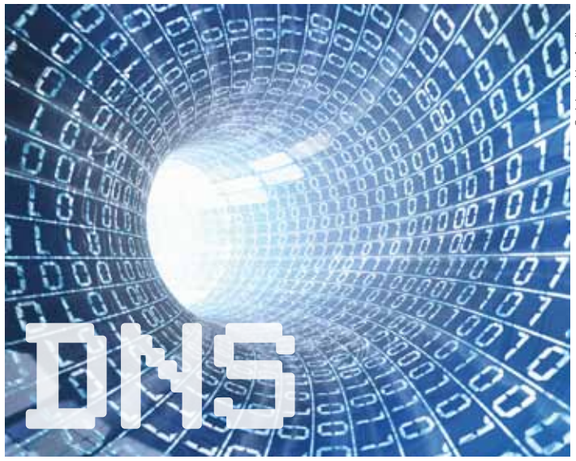


© pico – fotolia.com

Reflected-Denial-of-Service-Angriffe (DoS) sind bis zu 60 Mal stärker als herkömmliche DoS-Attacken. Sie gefährden nicht nur die ITK-Systeme der angegriffenen Unternehmen, sondern auch Teile der Webinfrastruktur. Die Deutsche Telekom beteiligt sich an einer vom Bundesamt für Sicherheit in ... ... der Informationstechnik (BSI) koordinierten Providerinitiative, um zeitnah Maßnahmen gegen die neue Angriffsvariante zu entwickeln. Im Fokus der Zusammenarbeit stehen offene DNS-Server, die Cyberkriminelle missbrauchen, um die Bandbreite ihrer Angriffe um ein Vielfaches zu steigern.

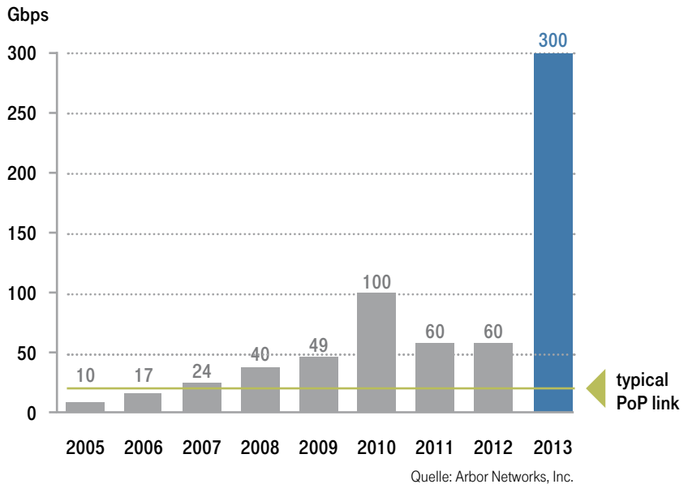
Die Abwehr von DoS-Angriffen gehört zum Tagesgeschäft jedes Internetproviders. Seit Ende 2012 hat sich die Bedrohungssituation deutlich verschärft. Neben klassischen DoS-Attacken (siehe Infobox) treten nun auch Reflected-DoS-Angriffe in Erscheinung. Bei einer solchen Attacke nutzt der Angreifer für jedermann erreichbare offene DNS-Server, um die Bandbreite seines DoS-Angriffs um das 30- bis 60-fache zu steigern.

Der vorläufig stärkste Angriff dieser Art richtete sich gegen die Anti-Spam-Organisation Spamhaus Project, bei der im März Verkehrsspitzen von bis zu 300 Gigabit pro Sekunde (Gbit/s) gemessen wurden. Mehr als genug, um nicht nur das eigentliche Angriffsziel, sondern auch die mit ihm verbundene Netzinfrastruktur zu überlasten. Die Zugangsserver eines Breitbandnetzes sind typischerweise auf einen Datendurchsatz von 20 Gbit/s ausgelegt. Ein Reflected-DoS-Angriff erschöpft diese Bandbreite auf einen Schlag, was zu Dienstausfällen an allen Firmen- und Privatkundenanschlüssen führt, die den Zugangsserver nutzen.



© alphasprint – fotolia.com

DIE GRÖßTEN DDOS-ATTACKEN



Quelle: Arbor Networks, Inc.

Das Balkendiagramm zeigt die größten bekannten DDoS-Angriffe seit 2005. Die Linie bei 20 Gbit/s markiert die typische Kapazität eines Breitbandzugangsservers. Im Jahr 2013 ereignete sich die bislang heftigste bekannt gewordene DDoS-Attacke in der Geschichte des Internets. Sie richtete sich gegen die Anti-Spam-Organisation Spamhaus.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

Denial-of-Service-Attacke (DoS) ist der Oberbegriff für Angriffe auf die Verfügbarkeit von Netzwerkdiensten. Die gängigste Angriffsform besteht darin, ein Zielsystem wie zum Beispiel einen Webserver mit Anfragen zu überfluten, sodass es auf die Anfragen regulärer Nutzer kaum oder gar nicht mehr antworten kann. Nutzt ein Angreifer eine Vielzahl synchronisierter Rechnersysteme für eine Attacke, spricht man von einem Distributed-Denial-of-Service-Angriff (DDoS).

REFLECTED-DENIAL-OF-SERVICE-ANGRIFFE

Ein Reflected-Denial-of-Service-Angriff geht wie eine reguläre DoS-Attacke von Computern aus, die Cyberkriminelle ohne das Wissen der Anwender übernehmen und zu einem Botnetz zusammenschalten (siehe Beitrag auf Seite 13). Der erste grundlegende Unterschied besteht jedoch darin, dass der angreifende Bot-Client seine Anfrage nicht direkt an das Opfer schickt. Stattdessen adressiert er einen offenen DNS-Server, der netzwerkübergreifend erreichbar ist und die Anfragen jedes Internetteilnehmers beantwortet. Die gängigste Anfrage lautet: „Nenne mir die IP-Adresse einer Internetdomain“, wie zum Beispiel www.telekom.de. Der Angriff setzt sich dadurch fort, dass der DNS-Server seine Antwort nicht an den ursprünglich anfragenden Bot-Client schickt, sondern an den Zielrechner des Angriffs. Das Umleiten der Antwort geht auf das Konto einer Tarntechnik, die IP-Spoofing genannt wird. Die Technik erlaubt es Angreifern, die IP-Adresse des Opferrechners als Absender der Anfrage einzusetzen (siehe Infobox „Rückverfolgung ausgeschlossen“).

© jorgophotography – fotolia.com

RÜCKVERFOLGUNG AUSGESCHLOSSEN

Eine Reflected-DoS-Attacke lässt sich nicht zurückverfolgen. Die Tarntechnik IP-Spoofing ermöglicht einem Botnetz, die Absenderkennung seiner Anfragen auszutauschen. Statt der IP-Adressen des anfragenden Bot-Clients erhält der angefragte DNS-Server die IP-Adresse des Opferrechners. Im Logsystem des Opfers erscheint lediglich die IP-Adresse des missbrauchten DNS-Dienstes. Eine Rückverfolgbarkeit des Angriffs ist daher unmöglich. Um auszuschließen, dass gefälschte Anfragen aus dem eigenen DSL-Netz versendet werden, überprüft die Deutsche Telekom alle ausgehenden Anfragen auf IP-Spoofing. Ob Anfragen aus anderen Netzen korrekte Absender haben, kann die Telekom nicht nachvollziehen. Die entsprechende Kontrollfunktion liegt ausschließlich im Zuständigkeitsbereich des jeweils anderen Netzbetreibers.

Viele Reflected-DoS-Angriffe entwickeln einen erheblichen Hebel, um ihre Schlagkraft um ein Vielfaches zu steigern. Ein Angreifer kann etwa einen offenen DNS-Server dazu auffordern, alle IP-Adressen einer Internetdomain auf einmal zu schicken. So löst eine wenige Byte große Anfrage die Rücksendung eines Datenpakets in Kilobytegröße aus. Indem sie die Mechanismen der Protokolle maximal ausreizen, können Botnetze die Bandbreite eines Reflected DoS-Angriffs um den Faktor 30 bis 60 steigern. Nutzt ein Angreifer beispielsweise 200 Bot-Clients, die jeweils an einer 1-Megabit-DSL-Verbindung hängen, lässt sich ein Anfragevolumen von bis zu 0,2 Gbit/s erzeugen. Mit einem Verstärkungsfaktor von 50 wächst die potenzielle Schlagkraft des Angriffs auf 10 Gbit/s. Auf diese Weise gefährdet selbst ein kleineres Botnetz den Anschluss eines Großunternehmens.

DNS-SCHWACHSTELLEN PROVIDERÜBERGREIFEND SCHLIEßEN

Um Reflected-DoS-Angriffe zu vermeiden, müssen Internet Service Provider die offenen DNS-Server in ihren Netzen kontrollieren. Dabei geht es keineswegs nur um anbietereigene Systeme – hier lassen sich eventuell vorhandene Schwachstellen mit vergleichsweise geringem Aufwand schließen. Die Hauptlast der Arbeit liegt vielmehr auf DNS-Diensten, die in den ITK-Systemen der Kunden verbaut sind. Nach einer vorläufigen Marktein-schätzung geht die Deutsche Telekom davon aus, dass es mindestens 25 Arten von DNS-Systemen gibt, die in Hunderten höchst unterschiedlichen ITK-Produkten integriert sind.

Insgesamt gesehen haben es die Provider mit einer außerordentlich heterogenen Systemwelt zu tun. Dessen ungeachtet müssen sie ihren Kunden leicht verständliche Anleitungen an die Hand geben, mit denen diese die DNS-Dienste ihrer Produkte so konfigurieren, dass sie nur für autorisierte Nutzer erreichbar sind. Um die erforderliche Dokumentationsarbeit auf möglichst viele Schultern zu verteilen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Arbeitsgruppe führender Internetprovider eingesetzt. Die Deutsche Telekom beteiligt sich intensiv an dieser Zusammenarbeit, die im Oktober 2013 startet. Ziel ist es, bis Mitte 2014 ein Webportal zu errichten, auf dem Handlungsanleitungen für alle gängigen DNS-Server hinterlegt sind.

EINGREIFEN

SICHERHEITSLÜCKEN AUF DER SPUR
INTERVIEW MIT BERND EßER

Das Management von Sicherheitshinweisen zählt zu den Kernaufgaben des Deutsche Telekom CERT. Ausgangspunkt sind Sicherheitswarnungen, mit denen Hard- und Softwarehersteller über Schwachstellen in ihren Produkten informieren. Monatlich treffen mehr als 100 dieser sogenannten Security Advisories beim CERT ein. Die Advisories enthalten eine erste Risikobewertung sowie grundlegende Hinweise zum Umgang mit den Schwachstellen. Mitarbeiter des CERT untersuchen, welche Schäden von den Sicherheitslücken auf die ITK-Systeme von Kunden und Mitarbeitern ausgehen können. Zeigt sich ein Handlungsbedarf, klärt das CERT die Systemverantwortlichen in der Deutsche Telekom Gruppe mit einem Leitfaden darüber auf, wie sich die jeweilige Sicherheitslücke schließen lässt. CERT-Leiter Bernd Eßer erläutert, welche Technologien am stärksten betroffen sind und wie sich kritische Sicherheitslücken zeitnah erkennen lassen.

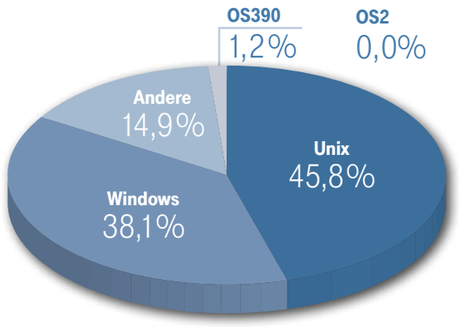
Bernd Eßer
Leiter Deutsche Telekom CERT

Die Zahl der aufgedeckten Schwachstellen ist unverändert hoch. Ist dies ein Dauerzustand, an den wir uns gewöhnen sollten?
Bernd Eßer: Nun ja, die Hoffnung stirbt zuletzt. Realistisch gesehen müssen wir aber davon ausgehen, dass sich das jetzige Niveau halten wird. Selbst bei IT-Produkten, die bereits seit Jahren auf dem Markt sind und häufig aktualisiert und verbessert wurden, öffnen sich immer wieder neue Sicherheitslücken. Ein Außenstehender könnte auf die Idee kommen, dass die Schwachstellensuche hier kaum noch Chancen auf Erfolg hat. Doch das Gegenteil ist der Fall.

Entwarnung kann somit nirgends gegeben werden?
Bernd Eßer: Ich wüsste nicht, wo. Um eine Vorstellung davon zu bekommen, welche Dynamik im Spiel ist, lohnt der Blick auf zwei grundsätzliche Trends, die uns auch in den kommenden Jahren weiter begleiten werden. Der eine Trend ist der anhaltende Siegeszug des Internetprotokolls (IP). Mit jedem IT-System und jedem Kommunikationsdienst, den das Protokoll durchdringt, gewinnen IP-gestützte Angriffsmethoden eine zusätzliche Zielscheibe. Deutlich wird das im Bereich der Unterhaltungselektronik: Immer mehr Geräte wie etwa Fernseher haben Zusatzfunktionen, für die sie mit dem Internet verbunden sein müssen. Die Hersteller müssen Vorkehrungen treffen, damit Hacker hier keine Chance haben, zum Beispiel Kontrolle über Kameras zu gewinnen oder sich in Mailkonten einzuhacken.

Wo zeigt sich der zweite Trend?
Bernd Eßer: Bei den Betriebssystemen. Hier findet bereits seit Jahren eine sehr weitreichende Standardisierung statt. Aus Sicht der Angreifer ergeben sich daraus zwei Vorteile auf einmal. Zum einen können sie ihre Ressourcen auf wenige Plattformen konzentrieren, um neue Schwachstellen aufzudecken. Zum anderen können sie ihr Hackerwissen zu einem deutlich höheren Preis verkaufen, wenn das betroffene Betriebssystem einen zunehmend größeren Teil des Anwendermarktes abdeckt.

VERTEILUNG DER SECURITY ADVISORIES PRO BETRIEBSSYSTEM IM ZEITRAUM JANUAR BIS AUGUST 2013

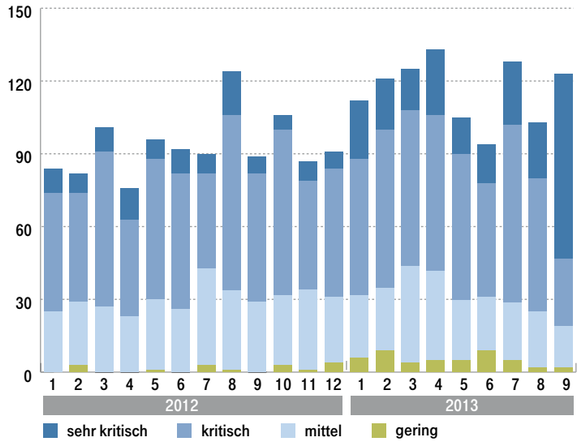


Apropos Betriebssysteme. Auch jetzt noch betreffen die weitaus meisten Sicherheitshinweise Microsoft und Unix. Unix führt das Ranking sogar an. Weshalb?
Bernd Eßer: Aus Kommunikationsgründen. Im Fall von Microsoft haben wir es mit einem Prozess zu tun, den der Hersteller kontrolliert. Demgegenüber gehen die Informationen in der Unix-Welt von den Nutzern aus. Mit Linux dominiert dort ein offenes Betriebssystem, in dem jeder User Schwachstellen suchen und sein Wissen darüber publizieren kann. Den Typ dieses Responsible Users gibt es zwar auch bei Microsoft, doch haben sich die externen Schwachstellenforscher in der Regel dazu verpflichtet, ihr Wissen nicht eigenständig publik zu machen.

So viel zu den Betriebssystemen. Wie sieht es auf der Seite der Anwendungen aus? Wo liegen hier die größten Baustellen?
Bernd Eßer: Nach wie vor bereiten uns Java, der Internet Explorer und Adobe die meiste Arbeit. Die Java-Plattform führt dieses fast schon klassisch zu nennende Trio auch in diesem Jahr an. Seit Januar erhalten wir beinahe wöchentlich Security Advisories zu gravierenden Java-Schwachstellen. In puncto Kritikalität hatten es die Hinweise zum Internet Explorer allerdings ebenfalls in sich. Zwei Fälle haben für besonderes Aufsehen gesorgt. Die Gegenmaßnahmen des Herstellers ließen so lange auf sich warten, dass sich das Bundesamt für Sicherheit in der Informationstechnik veranlasst sah, den Anwendern die Nutzung von anderen Internetbrowsern zu empfehlen. Aus Sicht des Advisory Managements ist eine solche Maßnahme das letzte Mittel.

Wie bewertet die Deutsche Telekom die Kritikalität von Schwachstellen? Gibt es für jedermann nachvollziehbare Wege, die zu belastbaren Zahlen führen?
Bernd Eßer: Die gibt es. Wir nutzen den Industriestandard CVSS, um aus der Flut von Schwachstellenhinweisen diejenigen herauszufiltern, die für unsere Geschäftslösungen und die Systeme unserer Kunden handlungsrelevant sind. CVSS steht für Common Vulnerability Scoring Standard, was so viel bedeutet wie Standard zur Bewertung von Verwundbarkeiten. Der Standard stützt sich auf drei Arten von Kriterien. Zunächst untersucht er, wie aufwendig es für Angreifer ist, eine Schwachstelle auszunutzen. Kriteriengruppe zwei gibt Aufschluss darüber, wer über welches Wissen zu einer Schwachstelle verfügt. Hierbei lautet die Kernfrage, ob es bereits funktionierende Abwehrmechanismen gibt oder potenzielle Angreifer aktuell noch die Nase vorn haben. Die dritte Kriteriengruppe berücksichtigt, welche ITK-Systeme von einer Schwachstelle betroffen sind und wie hoch ihr konkretes Gefährdungspotenzial ist. Anhand dieser Kriterien gibt der CVSS einen Wert zwischen 0, unkritisch, und 10, sehr kritisch, aus. Wir nutzen diesen Wert, um die für uns und unsere Kunden wichtigen Schwachstellen in vier Kategorien einzustufen. Wirklich handlungsrelevant sind dabei nur die Kategorien „critical“ und „high“.

ANZAHL DER MONATLICHEN SECURITY ADVISORIES NACH KRITIKALITÄT



DEUTSCHE TELEKOM CERT

Das Cyber Emergency Response Team (CERT) sorgt dafür, dass die Informations- und Netzwerktechnologien der Deutsche Telekom Gruppe auch im Angriffsfall zuverlässig weiterarbeiten. Neben einem Höchstmaß an technischem Sachverstand bringen die CERT-Mitarbeiter fundierte Kenntnisse über die Geschäftsfeldern und Arbeitsabläufen des Konzerns mit. Auf diese Weise können sie zuverlässig einschätzen, wie stark neu aufgedeckte Technologieschwachstellen die Telekom oder ihre Kunden bedrohen. Das Deutsche Telekom CERT ist rund um die Uhr erreichbar – für Kunden unter der E-Mail-Adresse cert@telekom.de.

MIT KOOPERATION ZU MEHR SICHERHEIT

Wenn externe Hinweisgeber das CERT darauf aufmerksam machen, dass ein Telekom-Dienst eine Schwachstelle aufweist, nimmt das CERT sofort die Arbeit auf. So auch, als bekannt wurde, dass sich Hackern die theoretische Möglichkeit bot, E-Mails von Kunden zu löschen, die sich beim Verlassen des E-Mail-Centers nicht abmelden. Mit einem sogenannten Workaround – einer ad hoc programmierten Umgehung der Schwachstelle – sorgten die CERT-Mitarbeiter dafür, dass sich die Schwachstelle nicht mehr ausnutzen ließ. Nach der provisorischen Erstversorgung setzte die Telekom das betroffene Servicemodul im E-Mail-Center neu auf und schloss die Sicherheitslücke dauerhaft. In der Regel entwickeln die CERT-Mitarbeiter einen Workaround binnen weniger Stunden. Bis die Schwachstelle dauerhaft beseitigt ist, vergehen häufig nur ein bis eineinhalb Tage.

RECHTZEITIG GEWAPPNET
STRATEGISCHER BEDROHUNGSRADAR KLÄRT CYBERGEFAHREN FRÜHZEITIG AUF

Mit dem Bedrohungsradar stellt das Deutsche Telekom CERT die Entwicklung von Cybergefahren dar. Das Werkzeug dient dem Unternehmen dazu, Bedrohungen frühzeitig zu identifizieren und Sicherheitsmaßnahmen zu planen.

Wer Gefahren sicher einschätzen und sich dagegen rüsten möchte, muss sie möglichst frühzeitig kennen. Darum betreibt das Deutsche Telekom CERT einen Bedrohungsradar, der aktuelle Entwicklungen stets im Blick hat. So auch eine Präsentation des US-amerikanischen Sicherheitsexperten Charlie Miller, die im August 2013 auf der Hackermesse Defcon für Wirbel sorgte. Gemeinsam mit seinem Forscherkollegen Chris Valasek war es Miller gelungen, in die Computersteuerung eines Toyota Prius und eines Ford Escape einzudringen und die Kontrolle über die Fahrzeuge zu übernehmen. Die IT-Spezialisten hackten auch kritische Fahrfunktionen und bedienten Lenkrad, Bremse und Gaspedal von ihrem Laptop aus. Als Einfallstor nutzten sie das CAN-Bus-System der Autos: ein gängiges Industrieprotokoll, über das die Mikrokontroller der Fahrzeuge Nachrichten untereinander austauschen.

„Dass sich CAN-Bus-Systeme kompromittieren lassen, war in der Theorie seit Jahren bekannt. Nun haben die US-Kollegen den praktischen Nachweis dafür erbracht, den Proof of Concept“, erläutert Bernd Eßer, der Leiter des CERT der Telekom. Bedrohungssituationen verschärfen sich durch die praktische Beweisführung generell grundlegend. „Der Proof of Concept ist ein wichtiger Meilenstein in unserer Gefahrenaufklärung. Wird er für eine Schwachstelle erbracht, entwickeln wir Methoden, um die Lücke zu schließen, bevor sie ein Angreifer ausnutzen kann. In diesem Fall war die Telekom nicht von einer veränderten Gefahrenlage betroffen, aber es wird deutlich, dass eine industrieübergreifende Zusammenarbeit im Austausch von Schutz- und Sicherheitskonzepten erforderlich ist“, erklärt Eßer. Schutzmaßnahmen, die aus klassischen IT-Umgebungen bekannt sind, könnten auf neue Anwendungsgebiete wie die Fahrzeugsteuerung übertragen werden. „Es ist wichtig, den Betrachtungsfokus zu Bedrohungen nicht zu eng zu wählen, da auch Szenarien mit umgekehrten Rückschlüssen möglich wären“, so Eßer weiter.

VORBEUGENDE AUFKLÄRUNGSARBEIT

Sobald sich das Bedrohungspotenzial einer Schwachstelle ändert, informiert das CERT Partner oder alle Produkt- und Systemverantwortlichen innerhalb der Telekom, deren Geschäftsfelder davon betroffen sind. Als zentrales Kommunikationsmittel setzt das CERT den strategischen Bedrohungsradar (engl. Strategic Threat Radar) ein. Er liefert den Fachbereichen belastbare Informationen, um die Geschäftsrisiken einzuschätzen, die von Cybergefahren ausgehen. Die vorbeugende Aufklärungsarbeit erlaubt es der Telekom, erforderliche Sicherheitsmaßnahmen vorausschauend zu planen und punktgenau auszuführen.

RADAR BEWERTET JEDE NEUE BEDROHUNG

„Jährlich kommen zwischen 15 und 25 Bedrohungen hinzu, die für die Geschäftsfelder der Deutschen Telekom relevant sind“, beziffert CERT-Leiter Bernd Eßer die Zahl der Neuzugänge. Bevor eine Bedrohung aufgenommen wird, klären die Radarentwickler der Deutschen Telekom drei zentrale Fragen:

1. In welchem Entwicklungsstadium befindet sich die Schwachstelle, von der die Bedrohung ausgeht? Ist sie nur theoretisch bekannt? Gibt es eine praktikable Angriffsmethode? Wenden Hacker eine solche Methode bereits an?
2. Wie wahrscheinlich ist es, dass die Schwachstelle tatsächlich ausgenutzt wird? Welchen Aufwand müssen Angreifer betreiben, um sich Zugang zu den betroffenen Systemen zu verschaffen?
3. Welche Schäden können für die Deutsche Telekom und ihre Kunden entstehen?

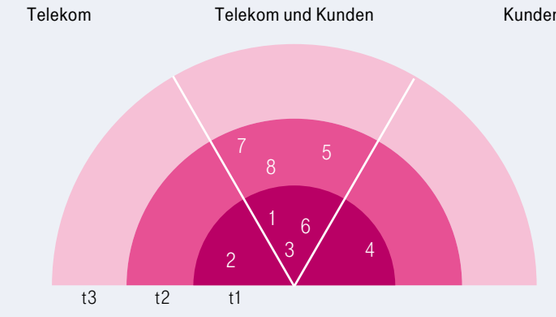
„Wenn möglich, beziffern wir die Frage nach den Schäden“, erläutert Bernd Eßer. „Konkrete Eurobeträge zu hinterlegen ist jedoch nicht trivial. Wir haben es zumeist mit theoretischen Gefährdungen zu tun. Belastbare Informationen zu den Absichten eines potenziellen Täters und entsprechenden Angriffsszenarien sind rar.“ Neue Bedrohungen zuverlässig einzustufen zählt zu den anspruchsvollsten Aufgaben der Radarentwicklung. Um die Ergebnisse ihrer Arbeit nachvollziehbar zu machen, stützt sich die Telekom auf standardisierte Methoden wie das CVSS-Verfahren (siehe Interview auf Seite 19).

BOTATTACKEN ERFOLGREICH ABGEWEHRT

Die differenzierte Betrachtung verschafft den Produktverantwortlichen einen wertvollen Informationsvorsprung, um ihre Systeme frühzeitig abzusichern. So auch die Angebote für das mobile Internet. Im Frühjahr 2012 rückte eine Bedrohung in den Mittelpunkt des Radars, die bis dato als theoretisch galt. Im Kern geht es darum, Smartphones zu Botnetzen zusammenzuschalten, um wesentliche Teile der Netzinfrastruktur zu schädigen. Potenzielles Angriffsziel sind die DNS-Server eines Mobilnetzes, die den Klartextnamen einer Internetseite mit der zugehörigen IP-Adresse verknüpfen. Der Ausfall eines DNS-Servers hätte zur Folge, dass mobile Surfer eine Internetseite nur noch erreichen können, wenn sie deren IP-Adresse im Kopf haben. Ein Ding der Unmöglichkeit.

„Wir haben die Bedrohung sehr ernst genommen und sind umgehend auf die Kollegen zugegangen, die mit dem Ausbau der mobilen Netze befasst sind. Obwohl die Kollegen alle Hände voll damit zu tun haben, die Netzkapazitäten der stark steigenden Nachfrage anzupassen, haben wir in kurzer Zeit eine Lösung aufgesetzt, mit der wir die DNS-Server nachhaltig absichern“, erinnert sich CERT-Leiter Bernd Eßer. Das schnelle Handeln hat sich gelohnt: Seit Ende 2012 verzeichnet die Deutsche Telekom Botattacken auf DNS-Server in mobilen Netzen. Dank der frühzeitigen Gefahrenaufklärung ließen sich sämtliche Angriffe erfolgreich abwehren.

GEFAHRENRADAR



BEDROHUNGEN

1 Advanced Persistent Threats (APT)
2 Spear Phishing gegen Telekom-Mitarbeiter
3 Mobiler Schadcode
4 Angriffe auf mobiles Banking
5 Denial-of-Service-Angriffe auf DNS-Infrastruktur
6 Angriffe auf DSL-Router
7 Angriffe auf CAN-Bus von Fahrzeugen
8 Angriffe auf Smart TVs

ENTWICKLUNGSSTADIEN

t1 Aktive Ausnutzung einer bekannten Schwachstelle
t2 Schwachstelle vorhanden und Ausnutzbarkeit nachgewiesen
t3 Schwachstelle vorhanden und theoretisch ausnutzbar

WER WIRD BEDROHT?

Der Radar zeigt, wer von einer Bedrohung betroffen ist: der Kunde, der Produkte und Dienste von der Telekom bezieht (rechter Sektor), die Telekom mit ihren internen Systemen (linker Sektor) oder beide gemeinsam (mittlerer Sektor).

WELCHE BEDROHUNGEN GIBT ES?

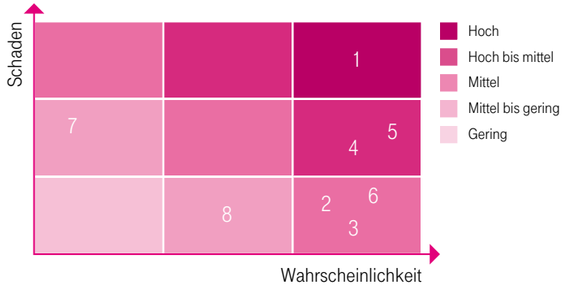
Aktuell beobachtet das CERT 60 Bedrohungen. Die Auswahl zeigt acht der populärsten Bedrohungen. Sechs davon betreffen sowohl den Kunden als auch die Deutsche Telekom selbst:

- **Advanced Persistent Threats (1)**: Privat- und Geschäftsanwender werden lang anhaltenden Angriffen ausgesetzt, die unterschiedliche Werkzeuge kombinieren.
- **Mobiler Schadcode (3)**: Malware gelangt über App-Stores auf mobile Endgeräte, um diese etwa in Botnetze einzubinden.
- **Denial-of-Service-Angriffe auf DNS-Infrastruktur (5)**: Mobile Schadprogramme greifen IP-basierte Netzkomponenten an, um mobile Botnetze zu errichten.
- **Angriffe auf DSL-Router (6)**: Schadsoftware befällt Router und Modems, deren Sicherheitseinstellungen zu schwach konfiguriert sind.
- **Angriffe auf CAN-Bus von Fahrzeugen (7)**: Angreifer dringen in die Computersteuerung von Fahrzeugen ein und übernehmen die Kontrolle von Fahrfunktionen.
- **Angriffe auf Smart TVs (8)**: Schwachstellen in Smart TVs und Set-Top-Boxen ermöglichen Angreifern, Nutzerdaten auszuspionieren.

WIE WEIT IST EINE BEDROHUNG ENTWICKELT?

Je fortgeschrittener das Entwicklungsstadium einer Bedrohung ist, desto zentraler ist ihre Position im Radar. Im inneren Ring **(t1)** erscheinen bekannte Sicherheitsschwachstellen, die Hacker bereits aktiv ausnutzen. Der mittlere Ring **(t2)** ist Schwachstellen vorbehalten, deren Ausnutzbarkeit nachgewiesen wurde. Im äußeren Ring **(t3)** finden sich theoretische Bedrohungen. Als der Proof of Concept der CAN-Bus-Bedrohung bekannt wurde (siehe Beitrag oben), rückte sie vom äußeren in den mittleren Ring vor.

RISIKOPORTFOLIO



1 Advanced Persistent Threats (APT)
2 Spear Phishing gegen Telekom-Mitarbeiter
3 Mobiler Schadcode
4 Angriffe auf mobiles Banking
5 Denial-of-Service-Angriffe auf DNS-Infrastruktur
6 Angriffe auf DSL-Router
7 Angriffe auf CAN-Bus von Fahrzeugen
8 Angriffe auf Smart TVs

Das Risikoportfolio dokumentiert die Ergebnisse: Eintrittswahrscheinlichkeit und Höhe der potenziellen Schäden stehen im Zentrum der Analyse. Eine Matrix zeigt, wie die Sicherheitsexperten die Situation aktuell einschätzen.

MEHR TRANSPARENZ BITTE
IM GESPRÄCH MIT DER INTERNETWACHE

Sebastian Neef und Tim Schäfers sind zwei technikbegeisterte junge Hacker, die sich für die Sicherheit im Internet einsetzen. Gemeinsam betreiben sie das Projekt „Internetwache“, bei dem sie die Sicherheit von Webseiten überprüfen und deren Betreiber auf Schwachstellen aufmerksam machen, wenn sie fündig werden. Auch der Deutschen Telekom haben sie bereits mehrfach geholfen. Im Gespräch mit dem Sicherheitsreport erklärt Sebastian Neef, welche Beweggründe ihn antreiben und wie Unternehmen reagieren, wenn er sie kontaktiert.

„Ich wünsche mir, dass mehr Unternehmen transparent machen, wie sie die Sicherheit ihrer Internetdienste verbessern.“

Sebastian Neef
Medieninformatiker und einer der Gründer und Betreiber des Sicherheitsportals internetwache.org

Herr Neef, was genau tun Sie bei der Internetwache?
Sebastian Neef: Wir sehen uns Webseiten ganz unterschiedlicher Unternehmen an und prüfen, ob wir Sicherheitsschwachstellen entdecken. Finden wir etwas, kontaktieren wir den Seitenbetreiber, damit er die Lücke schließen kann. Wir hacken die Seiten aber nicht selbst, sondern prüfen nur, ob das möglich wäre. Oft zeigt uns schon das Verhalten einer Webseite, dass sie eine Schwachstelle aufweist. Wir nutzen auch Tools wie die Intercepting Proxys BURP und ZAP, um eine Seite genauer zu untersuchen. Mit diesen Werkzeugen fangen wir den HTTP-Verkehr zwischen Internetbrowser und dem Server der Webseite ab und betrachten jede einzelne Abfrage.

Warum tun Sie das?
Sebastian Neef: Als ich damit begonnen habe, selbst Webseiten und kleinere Projekte zu programmieren, fielen mir viele Nachrichten über gehackte Unternehmen und Kundendaten auf. Ich wollte wissen, wie das funktioniert. Dann wurde mir klar, dass ich selbst auch Webseiten und Onlinedienste nutze. Also begann ich damit, diese Seiten auf Schwachstellen zu überprüfen. Aus Neugierde und Spaß an der Sache wurde schließlich unser Projekt Internetwache. Wir wollen, dass das Internet sicherer wird. Und ganz nebenbei ist die Internetwache ein gutes Referenzprojekt für mein späteres Berufsleben. Im Augenblick studiere ich Informatik im dritten Semester. Gemeinsam mit Herrn Schäfers biete ich aber auch Security Audits an.

Welche Sicherheitsschwachstellen entdecken Sie in der Regel?
Sebastian Neef: Es gibt eine gemeinnützige Organisation namens OWASP, die sich ähnlich wie wir zur Aufgabe gemacht hat, die Sicherheit von Anwendungen und Diensten im Internet zu verbessern. Das Kürzel steht für Open Web Application Security Project. Einmal im Jahr gibt OWASP eine Top-Ten-Liste der verbreitetsten Sicherheitsschwachstellen heraus. Die stimmt mit unseren Beobachtungen überein. Ziemlich weit oben auf der Liste stehen sogenannte Cross-Site-Scripting-Lücken, die auch als XSS-Lücken bezeichnet werden. Das sind Schwachstellen, die es einem Hacker etwa erlauben, JavaScript-Code im Kontaktformular eines Webshops oder eines Forums auszuführen.

Normalerweise erlaubt die Programmierung einer Webseite nicht, dass solcher Code im Kontext einer Webseite ausgeführt wird. Schon ein kleines Versäumnis bei der Programmierung der Wiederausgabe kann allerdings dafür sorgen, dass das doch funktioniert und ein Hacker seinen Code sozusagen in die Webseite einschleusen kann. Besucht nun ein anderer Internetnutzer das manipulierte Eingabeformular, können die vom Hacker manipulierten Daten an dessen Browser gesendet werden. So führen Hacker zum Beispiel Phishingangriffe durch. Darüber hinaus finden wir häufig SQL-Injection-Lücken, Local-File-Inclusion-Schwachstellen und die weniger weit verbreiteten Open-Redirect-Lücken.

Wie reagieren die Seitenbetreiber, wenn Sie auf sie zugehen?
Sebastian Neef: Das ist ganz unterschiedlich. Bei vielen Unternehmen fängt das Problem bereits damit an, dass wir gar nicht wissen, an wen wir unsere Hinweise weitergeben können. Es fehlt eine entsprechende Kontaktadresse und die erreichbaren Mitarbeiter fühlen sich nicht zuständig. Bei Unternehmen wie der Telekom oder auch Google sieht das anders aus. Die Telekom betreibt ein CERT, das genau für solche Anfragen zuständig ist und sehr schnell reagiert. Das CERT schickt uns in der Regel innerhalb eines Tages eine Bestätigungs-E-Mail mit dem Hinweis, dass die entsprechenden Fachbereiche auf die Sache angesetzt wurden oder die Lücke bereits geschlossen wurde. Aber natürlich kann sich nicht jedes Unternehmen ein CERT leisten. Gerade von kleineren Firmen kann man das nicht erwarten. Und dann gestaltet sich die ganze Kommunikation etwas langwieriger.

Was wünschen Sie sich von Webseitenbetreibern, um die Sicherheit im Internet zu verbessern?
Sebastian Neef: Unternehmen sollten transparent machen, welche Maßnahmen sie ergreifen, um die Sicherheit ihres Angebots zu verbessern. Außerdem wünsche ich mir, dass jedes Unternehmen mit einer Webseite oder einem Onlinedienst ein Responsible-Disclosure-Programm betreibt. Sicherheitsforscher sollten die Möglichkeit haben, Schwachstellen vertraulich zu melden, bevor ein Cyberkrimineller sie ausnutzen kann. Schön wäre es, wenn Unternehmen die kostenlose Arbeit der Analysten mit einem Eintrag auf ihrer Webseite oder einer kleinen Prämie für eine aufgedeckte Schwachstelle honorieren würden.

In Europa ist das noch nicht weit verbreitet. US-amerikanische Unternehmen gehen da anders vor. Viele von ihnen betreiben, Bug-Bounty-Programme und erwähnen Hinweisgeber lobend in einer „Hall of Fame“ auf ihren Seiten. Um ein solches Programm zu betreiben muss man natürlich die Stärke haben, sich einzugestehen, dass Sicherheitsschwachstellen vorkommen können. Wären mehr Unternehmen dazu bereit, sich offen und aktiv mit diesem Thema auseinanderzusetzen, hätten Cyberkriminelle deutlich weniger Chancen, ihr Unwesen zu treiben.

VERBREITETE SICHERHEITSSCHWACHSTELLEN

Eine **SQL-Injection-Lücke** erlaubt einem Angreifer, MySQL-Code in einem System auszuführen und möglicherweise Daten auszulesen, zu verändern oder zu löschen.

Local-File-Inclusion-Schwachstellen in Skript-basierten Webanwendungen ermöglichen einem Hacker, Programmcode in den Webserver einzuschleusen und auszuführen.

Eine **Open-Redirect-Lücke** gestattet es Angreifern, die Links einer Webseite zu manipulieren und den Besucher an andere Ziele weiterzuleiten.

© Pashalgnatov – istockphoto.com

TELEKOM STARTET BUG-BOUNTY-INITIATIVE

Am 28. Oktober 2013 startet die Deutsche Telekom ein Bug-Bounty-Programm. Externe Hinweisgeber werden gebeten, Sicherheitsschwachstellen in Webportalen der Domäne *telekom.de vertrauensvoll zu melden. Die Initiative basiert auf einer Responsible Disclosure Policy: Die Telekom bittet Sicherheitsforscher, Schwachstellen verantwortungsvoll zu enthüllen. Sie verpflichtet sich dazu, gemeldete Sicherheitslücken in einem angemessenen Zeitrahmen schnellstmöglich zu schließen. Das Engagement der Hinweisgeber wird belohnt: Eine einzige Remote-Code-Execution-Schwachstelle kann bis zu 5.000 Euro Prämie in Abhängigkeit von der Kritikalität des verwendeten Systems geben.

Teilnahmebedingungen und weitere Informationen zur Responsible Disclosure Policy der Telekom finden sich ab dem 28. Oktober unter: **www.telekom.com/bug-bounty**

© niarchos – istockphoto.com

WLAN TO GO MIT EINGEBAUTER SICHERHEIT

Mit WLAN TO GO entsteht das größte HotSpot-Netz der Welt. Die Deutsche Telekom sorgt mit einer speziellen Routerspezifikation dafür, dass Kunden die ungenutzte Bandbreite ihres DSL-Anschlusses ohne Sicherheitsbedenken mit anderen teilen können. Um an WLAN TO GO teilnehmen zu können, braucht der Kunde neben seinem IP-basierten Telekom-Anschluss den Router Speedport W724V. Die Sicherheitsexperten aus dem Bereich Group Information Security der Deutschen Telekom haben die notwendigen Sicherheitsanforderungen gegenüber den Herstellern dieses Routers formuliert und deren Umsetzung überprüft. Der Speedport-Router sendet zwei unabhängige WLAN-Signale aus und erstellt damit zwei vollkommen getrennte Netzwerke. Das eine Netzwerk ist verschlüsselt und bleibt privat, das andere erscheint einem HotSpot-Nutzer als Zugangspunkt mit der Kennung Telekom_FON. Loggt sich ein HotSpot-Nutzer in das zur Verfügung gestellte FON-Netzwerk ein, hat er keine Möglichkeit, auf das private WLAN des Anschlussinhabers zuzugreifen. Damit bleiben auch daran angeschlossene Netzwerkgeräte vom Notebook bis zum Netzwerkspeicher vollkommen sicher. In umgekehrter Richtung gilt das genauso: Auch der HotSpot-Nutzer muss sich keine Gedanken darüber machen, dass der Besitzer des Routers auf sein mobiles Endgerät zugreifen könnte.

SICHERHEIT IM INTERNET.

KONTAKT

Missbrauchsteam/Abuse-Team
Deutsche Telekom AG
Group Information Security
Missbrauchsteam
T-Online-Allee 1
64295 Darmstadt, Deutschland
E-Mail: Abuse@telekom.de

Deutsche Telekom CERT
Deutsche Telekom AG
Group Information Security
Landgrabenweg 151
53227 Bonn, Deutschland
E-Mail: CERT@telekom.de

Redaktionsbüro
Deutsche Telekom AG
Group Information Security
Friedrich-Ebert-Allee 140
53113 Bonn, Deutschland
E-Mail: CERT@telekom.de

ERLEBEN, WAS VERBINDET.