SICHERHEIT IM INTERNET.
BERICHT ZUR INFORMATIONS- UND INTERNETSICHERHEIT

Group Information Security I Februar 2013

ERLEBEN, WAS VERBINDET.

SICHERHEIT IM INTERNET.
VORWORT

Zum vierten Mal veröffentlicht die Telekom nun ihren Bericht „Sicherheit im Internet“ und informiert damit halbjährlich über die Bedrohungslage im Netz. Die letzten Monate waren unter andererm dominiert durch eine Diskussion um Schadcodes wie Duqu, Flame und Gauss, die mitunter eine sehr hohe technische Raffinesse aufwiesen. Ein Beispiel dafür sind die MD5 Kollisionsangriffe in der Flame Schadsoftware.

Anfang 2013 wurde mit der „Red October“ Schadsoftware eine weitere herausragende Schadsoftware entdeckt, deren Geburtsstunde nach Expertenaussagen schon auf das Jahr 2007 datiert ist. Wie kann es eine hoch komplexe Schadsoftware mit mehr als zehn verschiedenen Komponenten schaffen, Regierungsrechner weltweit zu infizieren und über nahezu sechs Jahre unentdeckt zu bleiben?

„Red October“ zeigt eindrucksvoll die Wichtigkeit eines funktionierenden Patchmanagements – auch und gerade auf normalen Büro-PCs. Alle bisher identifizierten Einfallstore (ausgenutzten Schwachstellen) der „Red October“ Schadsoftware waren bekannt und Sicherheitsupdates verfügbar.

Natürlich sind Updatevorgänge komplex und müssen sauber prozessiert werden. Die Regel sollte aber sein, jedes IT-System innerhalb weniger Stunden auf einen aktuellen Softwarestand zu bringen. Nur so lassen sich Einfallstore wie verwundbare Java-Versionen oder Adobe Flash Player wirkungsvoll schließen.

Hinzu kommt, dass es laut der Firma Kaspersky mehr als 200.000 neue Schadcodes pro Tag gibt, die die IT-Sicherheitsindustrie vor Herausforderungen bei der Analyse und Erkennung stellt. Trends in den letzten Wochen zeigen, dass Schadsoftware zunehmend beginnt, automatische Analysesysteme wie Virenscanner zu umgehen (siehe Highlights).

Ein weiterer Trend ist in der Ausnutzung von Schwachstellen innerhalb der Programmiersprache Java zu sehen. Bedingt durch die hohe Verbreitung von Java ist diese ein für Angreifer lohnenswertes Ziel. Mindestens zwei Lücken wurden in den letzten zwölf Monaten massiv ausgenutzt, um Rechnersysteme per sogenannten „Drive-By“-Angriffen zu infizieren. Auch die „Red October“ Schadsoftware enthält einen Angriffscode (Exploit) für eine Java-Schnittstelle. Interessant ist dabei, dass die zuletzt sehr breit ausgenutzte Java-Schwachstelle (CVE-2013-0422) offensichtlich schon Wochen vor der eigentlichen Entdeckung vereinzelt in kommerziellen Angriffstoolkits verwendet worden ist.

Zu erklären ist das dadurch, dass Entwickler entsprechender Angriffstoolkits offensichtlich vereinzelt soweit gehen, dass sie Informationen über Schwachstellen aufkaufen, um diese in ihr jeweiliges Toolkit zu integrieren. Diese Beispiele zeigen, wie sich die Bedrohungslage und die Kommerzialisierung der Angreifer weiterentwickelt hat. Mit diesem Bericht leisten wir einen Beitrag zur Aufklärung und Anpassung der heutigen Sicherheitsmodelle.

Ich wünsche Ihnen viel Spaß bei der Lektüre.

Ihr Thomas Tschersich

In eigener Sache: Der Bericht erscheint zweimal pro Jahr und ist über die Webseite www.telekom.com/sicherheit sowohl in deutscher als auch in englischer Sprache verfügbar.

INHALT

SICHERHEIT IM INTERNET.
SICHERHEITS-UPDATES

„Red October“ Schadcode

Die Firma Kaspersky berichtete erstmals Mitte Januar 2013 über die „Red October“- Kampagne. Diese versucht seit 2007 zielgerichtet, Regierungen, regierungsnahe Organisationen und Diplomaten zu belauschen. „Red October“ verwendet hierzu anders als andere prominente Schadcodes des vergangenen Jahres (Gauss, Flame) keine 0-day Schwachstellen, sondern nur bereits bekannte Schwachstellen in Microsoft Word und Java.

Die Kampagne zeichnet sich dadurch aus, dass die Schadcodes über nahezu sechs Jahre unentdeckt blieben, dass eine hohe Anzahl von Modulen existiert und dass die Command & Control (C&C) Infrastruktur mit über 60 Servern eine sehr hohe Komplexität aufweist. Ebenso raffiniert ist die Verseuchung ausgesuchter Smartphones über den Umweg der Synchronisierung mit einem verseuchten PC.

Ruby on Rails (RoR) Schwachstellen

RoR ist zu einer sehr beliebten Plattform für Web-Entwickler geworden. Im Januar 2013 wurden mehrere Schwachstellen bekannt, die dazu dienen können, beliebige Befehle mit den Rechten der RoR Anwendung (3.0.x und 2.3.x) auszuführen. Die neuerlich aufgetauchten Schwachstellen basieren darauf, dass Angreifer aus dem Internet eine Anfrage stellen, die dann falsch verarbeitet wird und im YAML Backend zu der Verwundbarkeit (Code-Ausführung) führt.

Weiterhin haben Sicherheitsexperten Ende 2012 das Authentisierungssystem von RoR im Detail betrachtet. Abhängig von dem verwendeten Authentisierungsmodell wird auf einen geheimen Schlüssel gesetzt, den RoR Anwendungen in der Datei secret_token.rb speichern. Dieser Schlüssel existiert einmal pro Anwendung. Viele Entwickler haben ihre kompletten Open Source-Quellcodes von RoR Anwendungen in öffentlichen Repositories wie Github gespeichert. Viele Benutzer dieser RoR Anwendungen haben den Schlüssel nie geändert, so dass allein durch die Kenntnis des Inhalts der secret_token.rb Datei das Sicherheitsmodell der jeweiligen Anwendung untergraben wird.

MySQL

Für die MySQL Datenbank-Software wurden im Dezember 2012 diverse Schwachstellen publiziert, die je nach Betriebssystem (Linux, Windows) auch eine Ausführung von Programm Code, der über das Netzwerk gesendet wird, zur Folge gehabt hätten. Da typischerweise Datenbanken in geschützten Zonen (sogenannten militarisierten Zonen, MZ) aufgebaut sind, ist die unmittelbare Gefahr eines Angriffs aus dem Internet als nicht hoch einzuschätzen. Dennoch sollte kurzfristig auch in solchen Fällen ein Sicherheits-Update eingespielt werden.

APT/ New York Times / Washington Post

Im Januar 2013 gaben diverse große amerikanische Medienunternehmen (im Februar folgten Unternehmen wie ThyssenKrupp und EADS) bekannt, dass sie von vermutlich chinesischen Hackern über einen langen Zeitraum ausspioniert worden seien. Hierfür sind im Fall der New York Times 45 auf Rechnern installierte Schadcodes gefunden worden. Hierbei wurde allerdings nur eine einzige Datei durch den verwendeten Virusscanner gefunden. Letztendlich heißt dies, dass man sich nicht auf Antivirensoftware allein verlassen sollte, sondern weitere Abwehrmaßnahmen (Logfile Analyse, SIEM, etc.) etablieren muss. Schadcodes werden heute mitunter nur für einen Angriffszweck/-ort konzipiert, so dass eine Erkennung jenseits von Heuristiken beziehungsweise verhaltensbasierten Ansätzen häufig unmöglich ist.

SICHERHEIT IM INTERNET.
SICHERHEITS-UPDATES

Java Schwachstellen

Nachdem in den letzten Jahren häufig Adobe Flash/PDF als Angriffsvektor ausgenutzt wurde, gelangte 2012 Java in den Fokus der Angreifer. Anfang 2012 wurde eine Schwachstelle zur Infektion von über 600.000 Mac OS X Rechnern ausgenutzt („Flashback“ Schadcode). Apple wurde in diesem Kontext massiv für die schleppende Update-Politik bei Java kritisiert.

Im vierten Quartal 2012 und Anfang 2013 wurden mehrere Schwachstellen innerhalb von Java bekannt, die über den Besuch einer infizierten Webseite („Drive by“-Angriffe) auszunutzen waren. Die Schwachstellen zwangen die Firma Oracle zu kurzfristigen Updates. Detailanalysen hatten ergeben, dass die jeweiligen Schwachstellen mitunter schon mehrere Wochen in verschiedenen Untergrund-Toolkits angewendet worden waren.

Bug bounty Programme

Im Kontext der Java Schwachstellen wurde ein neues Phänomen sichtbar. Mindestens ein Autor eines namhaften Untergrund-Toolkits hat eine Abwandlung einer populären Idee, nämlich die der Bug bounty Programme, für sich verwendet. Der Autor kauft nicht veröffentlichte Schwachstellen auf, um eine Exklusivität für sein Angebot zu realisieren.

SSL Certificate Authority gibt falsche Zertifikate aus

Der türkische SSL-Zertfikatsaussteller Türktrust hat durch einen Fehler zwei SubCA- Zertifikate ausgestellt, durch die sich beliebige gültige Zertifikate haben ausstellen lassen. Google hatte diesen Umstand Ende 2012 aufgedeckt, da ein von dieser SubCA ausgestelltes Zertifikat für *.google.com entdeckt wurde. Die Browserhersteller haben prompt reagiert und den SubCA-Zertifikaten die Vertrauenswürdigkeit entzogen. Auch wenn in diesem Falle das Zertifikat nicht wie in der Vergangenheit bei Comodo oder DigiNotar durch einen Hackerangriff erstellt wurde, zeigt der Vorfall doch erneut die Schwächen der Vertrauenswürdigkeit zertifikatsbasierter SSL-Infrastruktur.

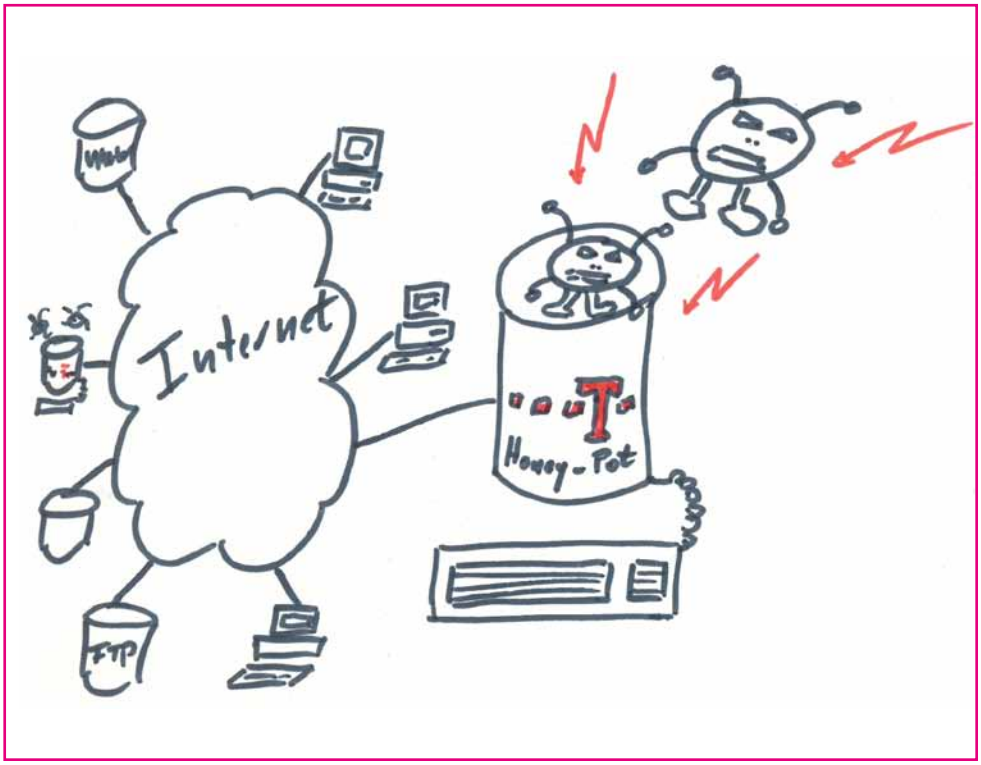
Angreifbare Smartphones

Bei gängigen Smartphones, die auf Exynos 4210 und 4412 CPUs basieren, wie beispielsweise dem Samsung Galaxy SIII, existiert eine Schwachstelle, die es ermöglicht, beliebigen Programm Code mit Kernel-Rechten auszuführen. Hierdurch kann ein User sich auf dem Telefon erweiterte Rechte verschaffen. Aber auch Schadsoftware ist in der Lage, systemweite Eingriffe auszuführen und das Smartphone für ungewünschte Zwecke zu missbrauchen. Das Sicherheitskonzept des Gerätes wird damit ausgehebelt. Samsung hat bereits einen Fix für die Schwachstelle angekündigt, aber auch andere Hersteller, die diese CPUs verwenden, sind betroffen. Anfang 2013 waren hierfür allerdings jenseits von Proof of Concept Codes keine Trojaner mit dieser Funktionalität verfügbar.

SICHERHEIT IM INTERNET.
FRÜHWARNSYSTEME: WAS SIE SIND UND WIE SIE FUNKTIONIEREN

Das Frühwarnsystem wird bei der Deutschen Telekom genutzt, um eine anbieterunabhängige Sicht auf die Sicherheit im Internet zu ermöglichen. Die derzeit im Internet verfügbaren Informationen zu diesem Thema kommen hauptsächlich von individuellen Sicherheitsanbietern und unterscheiden sich mitunter beträchtlich. Gerade im Umfeld des beobachteten Volumens an ungewollten E-Mails (Spam) und des Rankings der jeweiligen Ursprungsländer gibt es mitunter Diskrepanzen zu den Daten, die die Deutsche Telekom aus eigenen Quellen generiert (primär Abuse-Eingangskanäle).

Ziel ist es, unsere eigenen Erkenntnisse mit denen dieser Anbieter zusammenzufügen, um den Kunden der Deutschen Telekom bestmöglichen Schutz vor Online-Risiken zu bieten. Das hilft uns auch dabei, möglichen Änderungsbedarf in aktuellen Sicherheitssystemen oder Sicherheitsvorgaben frühzeitig zu erkennen.



Dabei lautet die generelle Faustformel: Je mehr Datenquellen eingebunden sind, desto effektiver arbeiten die Frühwarnsysteme und mehr Schaden kann von unseren Systemen, den angeschlossenen Partnersystemen und den Kundensystemen abgewendet werden.

Bereits in der Entwicklungsphase der Honeypotinfrastruktur haben wir die strikten (gesetzlichen) Regelungen bezüglich des Datenschutzes, der Sicherheit sowie der Vertraulichkeit berücksichtigt. Die Grafik zeigt, wie die verschiedenen Datenquellen und Systembestandteile zusammenarbeiten.

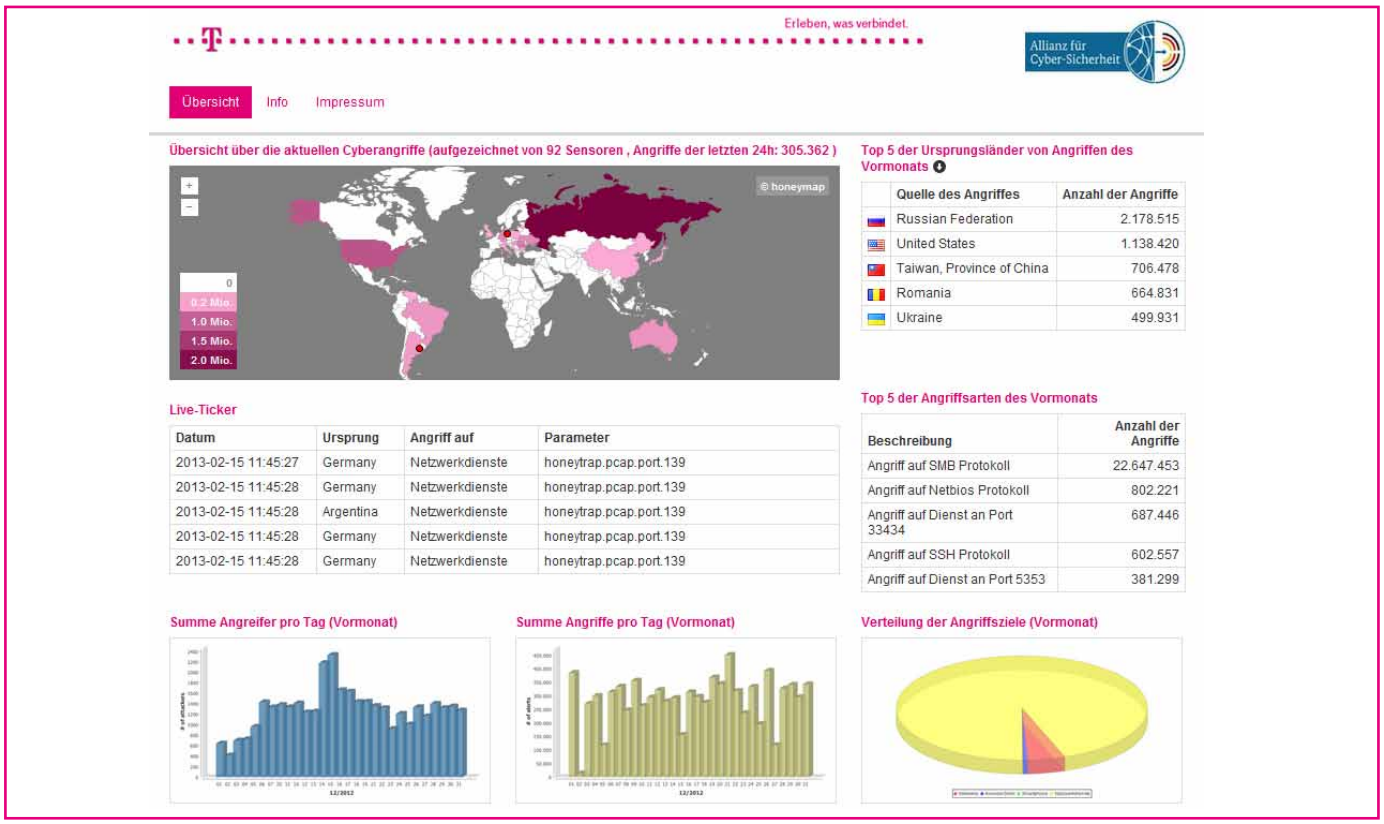
Die Deutsche Telekom nutzt unterschiedliche Datenquellen für ihr Frühwarnsystem beziehungsweise für die Sicht auf die Sicherheitslage im Internet. Die vier wichtigsten Elemente sind:

- Honeypot-Systeme (unter anderem zur Simulation von Webanwendungen, SSH und Datenbanken)
- Web Application Firewall Systeme
- Externe Hinweise (Abuse/vermuteter Missbrauch von Deutsche Telekom Diensten)
- CERT (Cyber Emergency Response Team) Informationsquellen

▶ Seite 6

SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 5 – Frühwarnsysteme: Was sie sind und wie sie funktionieren



Honeypot-Daten – visualisiert und nutzbar

Um einen noch schnelleren, aktuelleren Überblick über die Sicherheitslage zu bekommen, wird die Deutsche Telekom anlässlich der Cebit 2013 ein neues Webportal als Beitrag zur Cyberallianz der Bundesregierung veröffentlichen.

Das Portal www.sicherheitstacho.eu ist auf allen modernen Browserplattformen ohne vorherige Registrierung benutzbar.

Folgende Daten werden auf dem Portal angezeigt:

Übersicht über die aktuellen Cyberangriffe
Auf der hier dargestellten Weltkarte werden zeitgenau Angriffe auf das Sensornetzwerk (Honeypots) grafisch dargestellt. Zusätzlich werden die Länder in Abhängigkeit der Anzahl der erfolgten Angriffe farblich gekennzeichnet.

Top 5 der Ursprungsländer von Angriffen des Vormonats
Die oben beschriebene farbliche Markierung ist hier tabellarisch mit Werten der Top 5 Ursprungsländer für den Vormonat hinterlegt.

Verteilung der Angriffsziele (Vormonat)
Diese Grafik beschreibt die durch das verteilte Sensornetzwerk erkannten Angriffe getrennt nach Angriffsziel (Technologie).

Summe Angreifer pro Tag (Vormonat)
Die Grafik zeigt die Summe der Angreifer tageweise verteilt auf den jeweiligen Vormonat.

Summe Angriffe pro Tag (Vormonat)
Zu den zuvor dargestellten Angreifern pro Tag sind in dieser Grafik die jeweiligen Angriffe (alerts) tageweise verteilt auf den Vormonat dargestellt.

Verteilung der Angriffsziele (Vormonat)
Diese Grafik beschreibt die durch das verteilte Sensornetzwerk erkannten.

SICHERHEIT IM INTERNET.
DIE HONEYPOT-SYSTEME IM ÜBERBLICK

Ein Honeypot (deutsch: Honigtopf) ist eine Software, die Schwachstellen in Anwendungen simuliert, ohne dabei das hostende Wirtsystem selbst zu gefährden.

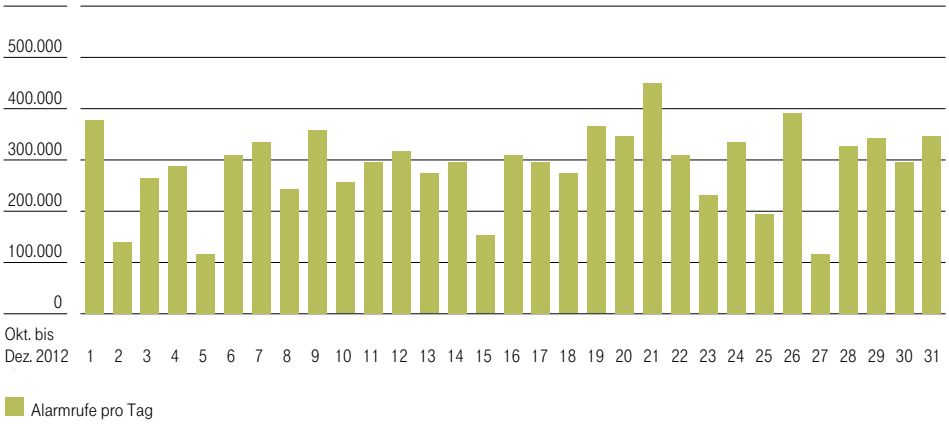
Ein Honeypot ist normalerweise eine Anwendung (oder eine Komponente wie eine Web Application Firewall im Loggingmodus), die Hacker von ihrem eigentlichen Ziel ablenken oder in speziell vorbereitete Bereiche locken/weiterleiten soll, wo diese keinen Schaden anrichten können. In der Natur ist diese Funktion vergleichbar mit Honigtöpfen, die benutzt werden, um wilde Bären von menschlichen Opfern abzuhalten.

Honeypots in der IT-Welt sind schon seit mehr als zehn Jahren bekannt, doch solche auf Webapplikationsebene sind jüngeren Datums – sie wurden erst in den vergangenen fünf Jahren eingeführt. Ein erster Honeypot-Ansatz wurde von dem Amerikaner Clifford Stoll umgesetzt und in dem Buch „Kuckucksei“ (1986) festgehalten. Letztendlich ging es in diesem speziellen Fall darum, aus Europa über Dialup-Verbindungen angreifende Personen so lange im System zu halten, um eine Rückverfolgung/Fangschaltung von den USA letztendlich bis nach Hannover zu ermöglichen.

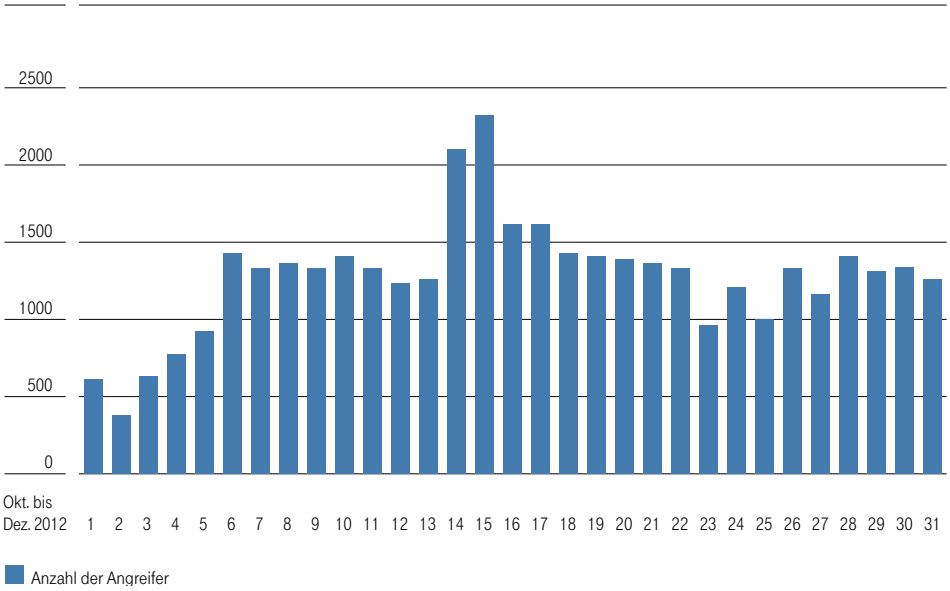
Die Deutsche Telekom hat letztere erstmals im April 2010 eingerichtet. Ursprünglich sollten sie nur Rückschlüsse auf Angriffe auf Web-Applikationen der Deutschen Telekom ermöglichen. Heute verwendet die Deutsche Telekom die Daten für verschiedenste Zwecke weiter, unter anderem auch für die Information von Endkunden und anderer ISPs (Internet Service Provider).

▶ Seite 8

Alarmrufe pro Tag im vierten Quartal 2012



Anzahl der Angreifer im vierten Quartal 2012



SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 7 – Die Honeypot-Systeme im Überblick

Honeypots sind grundsätzlich reaktiver Natur. Einzig clientseitige Honeypots stellen eine Ausnahme dar, da sie aus eigenem Antrieb heraus Webseiten aufsuchen, Daten abrufen und damit „Drive by"-Angriffe erkennen können.

Die Deutsche Telekom betreibt derzeit mehr als 92 Honeypot-Systeme, ein Großteil hiervon sind Web Application Honeypots. Auch in den internationalen Netzwerken und Systemen des Konzerns baut die Deutsche Telekom die Systeme kontinuierlich aus, um neue Formen von Hackerangriffen auf breiterer Ebene zu erkennen und ihnen vorzubeugen.

Aufgrund der Honeypot-Statistiken beziehungsweise der generellen Informationen aus den Honeypots ist keine Aussage möglich, ob die Produktionsinfrastruktur, etwa ein Portal wie www.musicload.de, im gleichem Ausmaß attackiert wird. Um ein praxisrelevantes Bild zu erhalten, hat die Deutsche Telekom das Frühwarnsystem zunehmend um Messpunkte auf Produktionsservern ergänzt (Webapplication Firewalls, die im Loggingmodus als Sensoren Daten an die zentrale Korrelationsengine liefern). Aktuell sind zum Beispiel einige Administrationsportale für Endkunden in den Scope mit einbezogen.

Honeypot-Systeme für Web-Applikationen

Die Honeypots jenseits der Web-Application-Firewalls-Module sind grundsätzlich von der Infrastruktur der Deutschen Telekom unabhängig, so dass eine Kompromittierung der Honeypots keine Gefahr für diese Infrastruktur darstellt. Die Web-Honeypot-Systeme der Deutschen Telekom sind selbstlernend, das heißt, sie identifizieren unbekannte Angriffe auf Basis heuristischer Methoden, analysieren diese und integrieren deren Schema in den eigenen Erkennungsprozess.

Vom 1. Januar bis 11. Februar 2013 haben die Honeypot-Systeme des Konzerns insgesamt 32.767 individuelle Angreifer registriert. Naturgemäß können von jedem Angreifer ein oder mehrere Angriffe ausgehen. Die Gesamtzahl individuell simulierter Schwachstellen belief sich zum 6. Februar 2013 auf 1.023.980 (im Vergleich hierzu betrug die Anzahl im September 2012 noch 816.270 Schwachstellen).

Die Analyse der am häufigsten attackierten Anwendungen hat sich durch ein breiteres Honeypot-Spektrum nur unwesentlich verschoben. Bei Webanwendungen sehen wir weiterhin eine sehr hohe Anzahl automatisierter Angriffe gegen simulierte Wordpress- und Typo3-Systeme.

REMOTE CODE EXECUTION/REMOTE FILE INCLUSION (RFI)

Als Remote Code Execution (RCE)/Remote File Inclusion (RFI) Angriffe bezeichnet man die Attacken, bei denen das angesprochene System Code ausführt, der von dem Angreifer übermittelt wurde. Im Fall von Webanwendungen wird häufig PHP-Code ausgeführt, den ein Angreifer bei seiner Attacke direkt mitgeschickt oder referenziert hat.

Hinsichtlich der Abwehrmaßnahmen der Angreifer gegen Honeypots sehen wir keinen neuen Trend.

Gerade bei sogenannten Remote Code Execution Angriffen im PHP-Umfeld ist es auffällig, dass sich die Maskierung/Kodierung des Schadcodes auf einem weiterhin hohen Niveau befindet. In der Vergangenheit wurde häufig nur ein PHP-Befehl zur Kodierung verwendet, heute dagegen werden häufig mehrere Kodierungen hintereinander verwendet.

Im Dezember 2012 kam neben den klassischen PHP Remote Code Execution noch der Fall der Remote Code Execution innerhalb von Ruby on Rails (ROR) Anwendungen hinzu (siehe hierzu auch die Details am Anfang des Berichts).

Von einigen dieser Sicherheitslücken wussten wir seit Mai 2010; entsprechende Updates sind lange verfügbar. Da die Angriffe dennoch durchgeführt werden liegt der Schluss nahe, dass auch heute noch ungepatchte Systeme im Internet mit veralteten Softwareversionen ansprechbar sind. Nach den vorliegenden Beobachtungen/Erkenntnissen waren die Angriffe auf diese Schwachstellen hochgradig automatisiert.

Die Angriffsmethoden sind in diesem Bereich die gleichen wie bereits im Quartal zuvor und spiegeln typische Angriffsmuster (manuell und automatisiert) wider:

- SQL Injection
- PHP Code Injection/Execution
- Remote File Inclusion

▶ Seite 9

SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 8 – Die Honeypot-Systeme im Überblick

Keiner der im vergangenen Quartal beobachteten Angriffe ist neuartig. Sie könnten auch leicht durch Einführung von strikter Inputvalidierung verhindert werden. Aktuelle Trends zeigen, dass trotz Verfügbarkeit von Best Practices zum Thema Inputvalidierung, Angriffe basierend auf einer fehlenden Inputvalidierung immer noch zu den häufigsten Angriffsformen gehören.

Ende 2011 belief sich die Zahl der in den Honeypots registrierten Schadprogramme auf 11201. In 2012 wurden nur 427 neue Schadcodes registriert. D.h. der Zuwachs an neuen Schadprogrammen ist in 2012 massiv abgeflacht.

Ursprungsländer der Angreifer

Land	Anzahl der Angriffe Okt. bis Dez. 2012
Russland (RU)	3.501.921
Rumänien (RO)	2.192.024
Taiwan (TW)	1.463.875
Ukraine (UA)	1.374.210
Australien (AU)	743.606

Secure Shell Honeypot-Systeme (SSH)

In Ergänzung der bestehenden Honeypot-Systeme für Web-Applikationen betreibt die Deutsche Telekom seit Dezember 2010 verschiedene Secure Shell Honeypots (SSH). Diese simulieren SSH-Server und ermöglichen es, den Ablauf eines Angriffs aufzuzeichnen und dabei die eingesetzten Schadprogramme und Authentisierungsinformationen für eine spätere Analyse zu sammeln. Es handelt sich hierbei um „low interaction" Honeypots, die einen eingeschränkten Funktionsumfang haben, doch gerade bei automatisierten Angriffen sehr gute Ergebnisse liefern.

Nach unseren bisherigen Erkenntnissen erfolgen viele Angriffe nach dem Brute-Force-Prinzip – das heißt, alle möglichen Kombinationen aus Usernamen und Passwörtern werden durchprobiert. Dies zeigen erfolglose Anmeldevorgänge, die je nach verwendetem Tool sogar exakt die gleiche Kombination und Abfolge von Username/Passwort-Kombinationen aufweisen.

Erwähnenswert ist auch, dass fast jeder erfolgreiche Angreifer überprüft, ob der übernommene Server über eine ausreichend breitbandige Internetanbindung verfügt. Um die Geschwindigkeit zu messen, werden üblicherweise Servicepakete von Microsoft-Produkten heruntergeladen, da diese eine ausreichende Länge für Geschwindigkeitstests aufweisen.

Die Beobachtungen der Deutschen Telekom zeigen weiterhin, dass bei der Verwendung von einem Standardpasswort mit acht Zeichen Länge die ersten Angreifer nach vier Stunden „erfolgreich" in den SSH-Honeypot eindringen konnten.

Die bisherigen Auswertungen zeigen primär wörterbuchbasierte Brute-Force-Angriffe und weniger Angriffe auf Basis von maschinell generierten Passwörtern (zum Beispiel AAAAA, AAAAB, AAAAC). In den SSH-Honeypots werden auch immer wieder Verbindungsabbrüche beobachtet, wobei nicht klar ist, ob diese gegebenenfalls auf gezielte Angriffe auf die SSH-Implementierung hindeuten oder „nur" Fehler der Angreifer darstellen.

Die nach einem erfolgreichen Hackerangriff hochgeladene Malware unterteilt sich in die folgenden Kategorien:

- Programme, die die Erlangung von Administratorenrechten ermöglichen (sogenannte Exploits, local privilege Escalation)
- Scannerprogramme, um andere verwundbare Systeme im Internet aufzufinden
- Programme, um die Authentifizierung anderer Systeme anzugreifen (Brute-Force-Angriffe)

Anmerkung: Nachdem das Passwort eines SSH-Honeypots durch ein komplexeres ersetzt wurde (indem es einfach nochmals wiederholt wurde), gab es in zwei Monaten zwei erfolgreiche Attacken. Daraus schließen wir, dass die Mehrzahl der Brute-Force-Angriffe auf vorhandene Listen mit Passwörtern zurückgreift und dass die Hacker keine oder deutlich weniger erfolgreiche Brute-Force-Angriffe auf Passwörter mit zwölf Zeichen durchführen.

Mobile Honeypots

Neben den bereits zuvor beschriebenen klassischen Honeypots, welche Daten aus Fixed-Line-Bereichen (Rechenzentren, virtuelle Server und Systeme an DSL-Anschlüssen) generieren, hat sich die Deutsche Telekom entschlossen, auch Honeypots zu betreiben, die die Betriebssysteme Android und iOS (iPhone, iPad) simulieren. ▶ Seite 10

SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 9 – Die Honeypot-Systeme im Überblick

Ziel war es, einen Honeypot zu entwickeln, der iOS-/Android-basierte Smartphones mit Zugang zum Mobilfunknetz simuliert und Hackerattacken gegen diese Geräte erfasst.

Diese neue, angepasste Form von existierenden Honeypots auf Basis unter anderem der OpenSource-Software „Kippo“ ist voll funktionstüchtig und zeigt, dass systematische Brute-Force-Attacken gegen offene Systeme in Mobilfunknetzen heute zum Alltag gehören.

Neben dem SSH-Honeypot Kippo verwendet die Deutsche Telekom auch die OpenSource-Software „Honeytrap“, um generische Angriffe in Mobilfunknetzen zu erkennen. Die bisherigen Beobachtungen zeigen allerdings eindeutig, dass die meisten Angriffe in allen Zugangsnetzen den gleichen Mustern folgen.

Die Technologie der Honeypot-Systeme für mobile Netzwerke hat die Deutsche Telekom Partnern weltweit zur Verfügung gestellt.

Datenbank-Honeypots

Datenbank-Honeypots stellen keine grundsätzlich neue Klasse von Honeypots dar. Erste Honeypots sind in diesem Umfeld seit 2006 verfügbar. Der ursprüngliche Fokus lag hierbei auf Microsoft SQL Server Emulationen, da gerade dieser Servertyp durch weitreichende Zugriffsmöglichkeiten auf das Filesystem bei Fehlkonfiguration einfach angreifbar und ein Defaultaccount (sa) bekannt war.

Im Jahr 2011 wurde das bekannte OpenSource-Projekt „Dianoea“ um eine Emulation von MySQL-Datenbanken erweitert. Die Deutsche Telekom hat auf dieser Basis erste MySQL-Datenbank-Honeypots im ersten Quartal 2012 etabliert und noch eine weitere eigene Lösung im Laufe des Jahres entwickelt.

Die Erfahrungen in 2012 zeigen, dass die MySQL-Honeypots nur in Schüben und vereinzelt angegriffen werden, die einzelnen Angriffe hier aber durchaus ein hohes Volumen mit mehr als 500 Anmeldeversuchen aufzeigen.

Die MySQL-Honigtöpfe werden in zwei unterschiedlichen Betriebsmodi verwendet:

1. Ablehnung jedes Anmeldeversuchs
   (Ziel: Sammlung von Zugangsdaten)

2. Akzeptanz jedes Anmeldeversuchs
   (Ziel: Vorgehen der Angreifer nach Login aufzeichnen und analysieren)

SSH:
Secure Shell oder SSH bezieht sich sowohl auf ein Netzwerkprotokoll als auch auf korrespondierende Programme, die dazu dienen, eine sichere Verbindung zum Remote-System auf Basis des SSH-Protokolls herzustellen.

SMTP:
Simple Mail Transfer Protokoll (SMTP) ist ein Internetstandard für elektronischen Mailverkehr (E-Mail) über Internet Protokoll (IP) Netzwerke.

iOS:
iOS (bis Juni 2010 als iPhone OS bezeichnet) ist das Betriebssystem für mobile Endgeräte von Apple.

MySQL:
Bei MySQL handelt es sich um eine OpenSource-Datenbank, die das Herzstück vieler Projekte ist. Der Hersteller der Datenbank wurde mittlerweile von Oracle übernommen, die freie OpenSource-Datenbank MySQL wird auch heute noch weiter entwickelt.

MALWARE:
Malware oder Schadprogramm werden typischerweise Programme bezeichnet, die schädliche Funktionen ohne Wissen des Benutzers ausführen. Hierzu gehören Trojaner, Viren und Würmer im engeren Sinne.

Ausblick: Client-Honeypots

Eine von der Deutschen Telekom heute noch nicht abgedeckte Honeypot-Form sind clientseitige Honeypots. Häufig diskutiert werden hier Automatismen, die Webseiten durch Webbrowserautomation zyklisch besuchen und danach Änderungen im Dateisystem analysieren, um sogenannte „Drive-By“-Attacken zu erkennen.

Bisher betrachtete OpenSource-Lösungen auf Basis von Wrappern um Javascript Engines haben sich als nicht produktiv einsetzbar erwiesen.

Eine Schadcode-Analyse kann dann im Nachgang auf Basis des bekannten Scanservices Virustotal, aber auch auf Basis der bekannten Sandboxlösungen erfolgen. Eine solche Drive-By-Angriff-Erkennung könnte auch im Rahmen der CERT-Aktivitäten Anwendung finden. Eine detaillierte Betrachtung dieser Honeypots beziehungsweise des Marktumfelds ist in den nächsten Monaten geplant.

SICHERHEIT IM INTERNET.

UMGANG MIT VERMUTETEM MISSBRAUCH/ABUSE: BEARBEITUNG EXTERNER HINWEISE UND BESCHWERDEN

Das Abuse-Team ist Ansprechpartner für Personen, die den Missbrauch von Internetdiensten der Deutschen Telekom melden wollen. Der Schwerpunkt liegt derzeit auf dem Deutschlandgeschäft, da hier unter anderem die bei der DSL-Einwahl ins Internet verwendeten IP-Adressen für sieben Tage zur Missbrauchsbekämpfung gespeichert werden.

Beispiele für Missbrauch beziehungsweise missbräuchliche Nutzung der Telekom-Dienste umfassen:

- den Erhalt/die Versendung ungewollter E-Mails, zum Beispiel mit werblichen Inhalten (Spam)
- den Erhalt/die Versendung von E-Mails, die Viren, Würmer oder Trojaner enthalten
- Hackerattacken auf Computer (Port Scans oder ähnliches)
- Verdacht auf Missbrauch von Zugangsdaten
- kriminelle Inhalte auf Homepages
- Phishing-Seiten von Internetportalen der Deutschen Telekom beziehungsweise generell von Firmen

Hierbei sei angemerkt, dass gerade die Versendung von E-Mail-Nachrichten mit Viren oder Trojanern im Anhang in den letzten Jahren deutlich abgenommen hat. Der Trend zur Kundeninfektion durch Besuch verseuchter Webseiten („Drive by“) ist also auch deutlich in den Hinweisstatistiken sichtbar.

Externe Berichte an das Missbrauchs-Team können in drei primäre Kategorien unterteilt werden:

1. Spam via IP
   Die Kategorie „Spam via IP“ bezieht sich auf ungewollte E-Mails mit Werbeinhalten (Spam), die unter Umgehung der regulären T-Online.de Mailserver direkt an andere Systeme im Internet versendet werden.

2. Hosting/Webpräsenzen
   Zu der Kategorie „Hosting/Webpräsenzen“ zählen E-Mail-Beschwerden, die thematisch Hostingspam (Spamversand über Homepages) und missbräuchlichen/strafrechtlichen Inhalten auf Kunden-Homepages zuzuordnen sind. Da es ab Mai 2011 einen signifikanten Anstieg missbräuchlicher Anlegung von Homepages gab, wurde auch die über diese Homepages versendete Spam-Anzahl deutlich größer.

3. Hinweise zu gehackten Kundenaccounts
   Im vergangenen Jahr war der Bereich „Hacking/Portscan“ hier mit aufgeführt. In dieser Kategorie wurden die Hinweise der Kunden historisiert, bei denen der Verdacht auf Portscans bestand. Die Kategorie wurde dahingehend geändert, dass hier jetzt die Beschwerden bezüglich kompromittierter Kundenaccounts, zum Beispiel auf Basis von Hinweisen der Shadow Server Foundation, gezählt werden.

MISSBRAUCHSABTEILUNG/ABUSE-TEAM:
Missbrauchsabteilungen von Internet Service Providern kümmern sich um (Kunden-) Beschwerden und helfen Kunden, deren Rechner von Schadcodes wie etwa Spam-Bots infiziert wurden.

Eingehende Hinweise/Berichte werden zunächst allgemein auf ihre Richtigkeit und Relevanz geprüft. Danach informiert das Abuse-Team den betroffenen Kunden über den Vorfall/Vorgang. Dies kann zum Beispiel eine Information über die wahrscheinliche Infizierung des Kundencomputers durch einen Virus oder Trojaner sein oder ein Hinweis auf Portscans, die von einem infizierten Computersystem ausgehen. Dem Kunden wird empfohlen, den Schadcode zeitnah mit einer aktuellen Virenschutzsoftware zu entfernen. Hierzu werden dem Kunden Beispiele und Bezugsquellen von Sicherheitssoftware genannt. Führt der Kunde die empfohlene Bereinigung nicht durch und attackiert der Kundenrechner auch weiterhin andere System mit zum Beispiel Spam, so kann das Abuse-Team weitere Schritte einleiten. In diesem Fall kann das Abuse-Team als Ultima Ratio die Sperrung einzelner Dienste wie des E-Mail-Versands veranlassen.

Das Abuse-Team der Deutschen Telekom benötigt externe Hinweise, um von Missbrauch/Infektion betroffene Kunden zu identifizieren und zu informieren.

Die wichtigsten externen Partner sind:

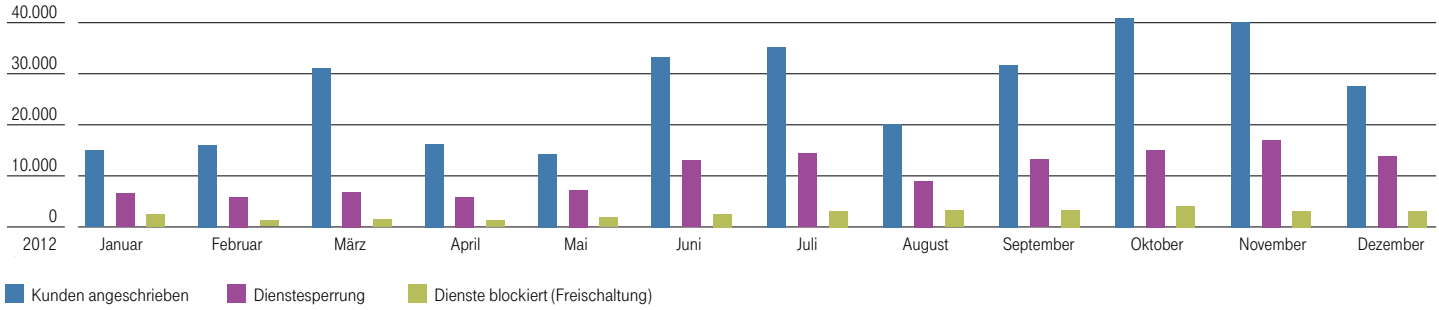
- Shadow Server Foundation
- Scomp
- Abusix Abuse Reporting Organisation
- Netcologne
- Uceprotect
- 1&1/United Internet
- JunkEmailFilter
- Trendmicro
- Gossler
- SpamVZ
- Freemailer-Hotmail

▶ Seite 12

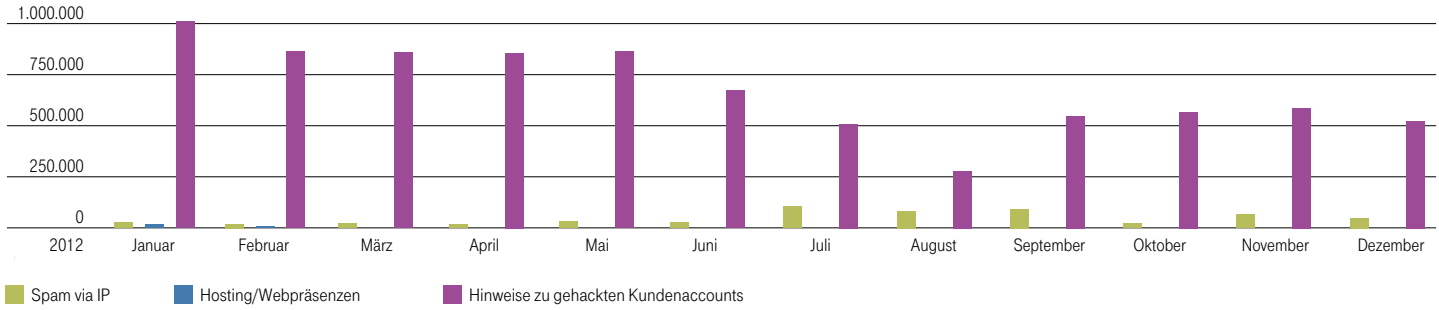
SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 11 – Umgang mit vermuteten Missbrauch/Abuse: Bearbeitung externer Hinweise und Beschwerden

Kundenkontakte



Beschwerdekategorien



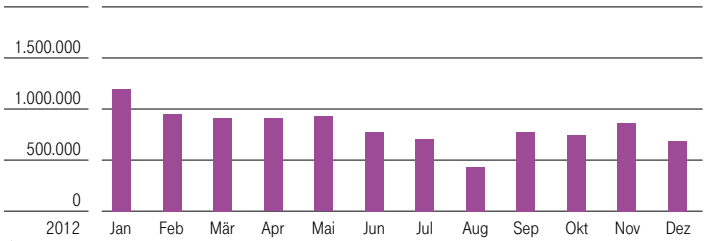
Die Honeypot-Infrastruktur liefert ebenfalls Daten an das Abuse-Team. Mit 12.000 Meldungen pro Jahr ist das Volumen bisher auf einem überschaubaren Niveau. Durch einen weiteren Ausbau der Honeypot-Infrastruktur wird eine deutlich größere Datenmenge erwartet.

Missbrauch von Diensten der Deutschen Telekom

Die Gesamtzahl der an die Deutsche Telekom übermittelten Missbrauchshinweise ist im Jahr 2012 auf 12,7 Millionen gestiegen. Nach dem Anstieg im ersten Halbjahr 2012 auf 6.996.309 Missbrauchshinweise (vgl. drittes Quartal 2011 3.278.947 und viertes Quartal 2011 2.611.136) sind im der zweiten Jahreshälfte nur noch 5,8 Millionen Beschwerden/Hinweise eingegangen.

Im ersten Halbjahr 2012 wurden 137237 Kunden der Deutschen Telekom durch das Abuse Team angeschrieben und informiert, dass ihre Rechner vermutlich mit Schadsoftware infiziert wurden (vgl. hierzu zweites Halbjahr 2011: 162.517). Im zweiten Halbjahr wurden 200.003 Kunden

Eingegangene Beschwerden



angeschrieben – das heißt, trotz eines zehnprozentigen Rückgangs der Beschwerdeeingänge wurden 50 Prozent mehr Kunden angeschrieben.

Insgesamt wurden bei 132.906 Kunden im Jahr 2012 (48.582 im ersten Halbjahr) Service-Einschränkungen (Port 25 Sperre) eingerichtet. Damit befinden sich die durchgeführten Sperrmaßnahmen wieder auf dem Niveau von 2011 (Quartal 1, 2011: 32.265).

SICHERHEIT IM INTERNET.
DEUTSCHE TELEKOM CERT: CYBER EMERGENCY RESPONSE TEAM

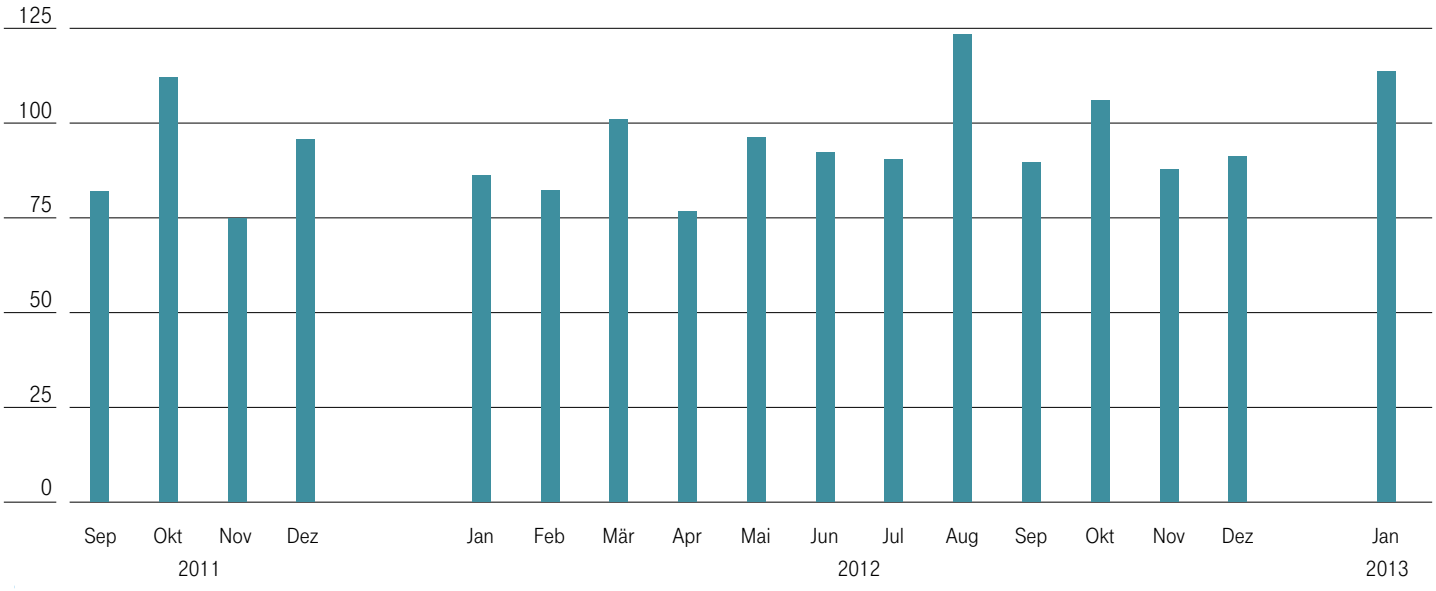
Das Cyber Emergency Response Team (CERT) der Deutschen Telekom hat die wichtige Aufgabe, das Unternehmen und dessen Kunden vor Gefahren aus dem Internet zu schützen. Das CERT ist das zentrale Eingangstor für Mitarbeiter, Kunden und Bürger, um Cyber Incidents zu melden, die dann durch das CERT bearbeitet werden. Darüber hinaus etabliert das CERT Mechanismen zur Früherkennung von Angriffen auf intern und extern erreichbare Systeme.

Die Aufgaben des Deutsche Telekom CERT umfassen:

- **Cyber Incident Management:** Koordination und Management von kritischen Sicherheitsvorfällen
- **Strategic Threat Radar:** Identifizierung und Bewertung von Bedrohungen im Kontext von aktuellen und zukünftigen Kerntechnologien des Konzerns
- **Advisory Management:** Bewertung und Verteilung von Sicherheitswarnungen und Handlungsempfehlungen innerhalb des Konzerns, sowie Monitoring der Umsetzung von kritischen Sicherheits-Updates
- **Security Audits:** Überprüfung und Bewertung von Sicherheitsarchitekturen, Sicherheitsprozessen und Systemlandschaft bei Unternehmensbereichen, die einem erhöhten Gefahrenpotenzial aus dem Internet ausgesetzt sind
- **Vulnerability Scanning:** Regelmäßige Durchführung von Sicherheits-Scans der aus dem Internet erreichbaren Portale und Systeme

Darüber hinaus ist das Deutsche Telekom CERT internationaler Ansprechpartner zu Themen der Internetsicherheit und Internetkriminalität. In diesem Bereich werden mit relevanten Stakeholdern wie beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA), der Kommission der Europäischen Union (EC), dem Bundeskriminalamt sowie den Branchenverbänden GSM Association (GSMA), ETNO, ETSI und dem Forum for Incident Response and Security Teams (FIRST) Projekte und Initiativen vorangetrieben, welche die Sicherheit im Internet verbessern. Im besonderen Fokus des Deutschen Telekom CERT steht derzeit die Bedrohung Advanced Persistent Threat (APT). Zu diesem Thema hat das Deutsche Telekom CERT ein Projekt gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik aufgesetzt, das geeignete Maßnahmen identifizieren soll. Die Ergebnisse werden der Allgemeinheit zur Verfügung gestellt. ▶ Seite 14

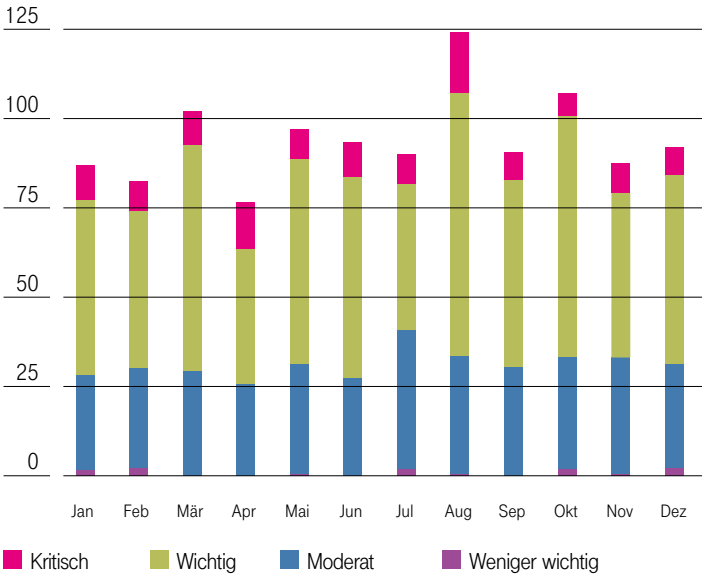
Advisories September 2011 bis Januar 2013



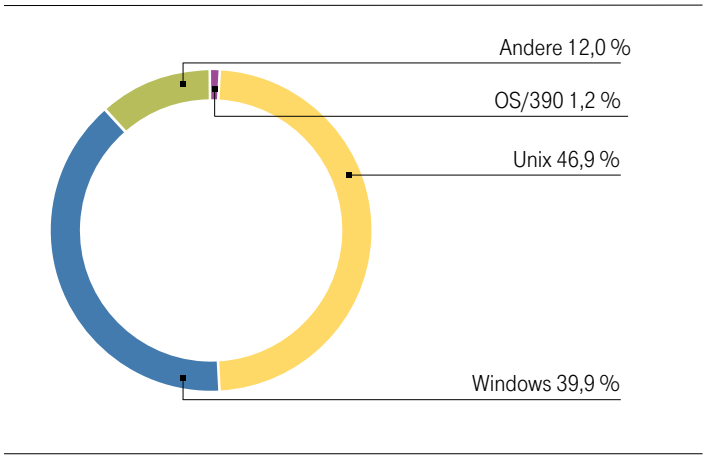
SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 13 – Deutsche Telekom CERT: Cyber Emergency Response Team

Advisories 2012



Betroffene Betriebssysteme



Statistische Informationen zu Schwachstellen

Die Abbildung auf Seite 13 zeigt die Verteilung der Security Advisories über die Monate. Im Jahresvergleich ergeben sich die folgenden Werte für die Anzahl der veröffentlichten Security Advisories:

2010 1.137 Security Advisories
2011 1.174 Security Advisories
2012 1.120 Security Advisories

Die Bewertung der Security Advisories hinsichtlich ihrer Kritikalität zeigt einen im Wesentlichen gleichbleibend hohen Anteil von Advisories, die als „Critical“ oder „High“ bewertet wurden. Viele dieser Advisories adressieren Schwachstellen, die zu Denial-of-Service-Angriffen oder sogenannten Drive-by-Infektionen führen können.

Beim Blick auf die betroffenen Betriebssysteme ist kaum ein Unterschied zu früheren Berichten festzustellen. Aufgrund der Marktdurchdringung von Unix und Windows-Systemen weisen beide Plattformen beinahe den gleichen Anteil von Schwachstellen auf: Im direkten Vergleich sind es bei Unix 47 Prozent und bei Windows-Systemen 40 Prozent.

Cyber Incident Management

Das Deutsche Telekom CERT ist international für das Management von Cyber Incidents durch Krisen- und Projektmanagement zuständig. Das CERT bewertet die Kritikalität des Incidents, bindet nach Bedarf Experten der Group Information Security sowie weitere Fachexperten ein und verantwortet das Reporting zu Top Management und Vorstand.

Bei Sicherheitsvorfällen innerhalb der Deutschen Telekom Group erstellt das Deutsche Telekom CERT, nach Bedarf und entsprechender Kritikalität des Vorfalls, sogenannte Info Advisories, um andere Konzernteile über den Sicherheitsvorfall zu informieren und Maßnahmenempfehlungen zu geben, die verhindern, dass sich der Vorfall auf andere Unternehmenszweige ausweitet. Sicherheitsvorfälle können via E-Mail an cert@telekom.de oder telefonisch unter 0800 DTAG CERT gemeldet werden.

Deutsche Telekom CERT Strategic Threat Radar

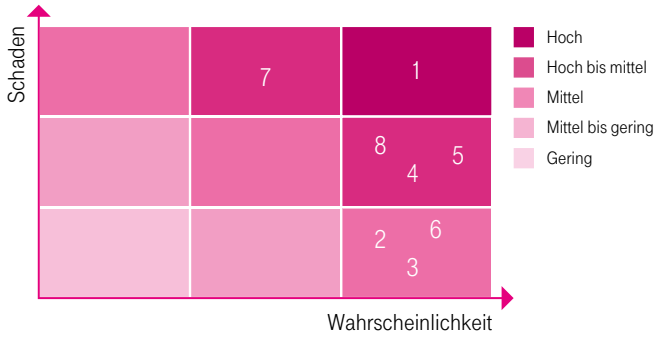
Das Management der Deutschen Telekom Group soll frühzeitig in die Lage versetzt werden, Bedrohungen hinsichtlich ihrer Auswirkungen auf das Business zu identifizieren und zu bewerten. Damit wird ein rechtzeitiges Planen von Sicherheitsmaßnahmen möglich. Im Rahmen des Strategic Threat Radars werden innovative Trends, Technologien der Zukunft sowie auch Technologien, die bereits heute im Einsatz sind, untersucht.

▶ Seite 15

SICHERHEIT IM INTERNET.

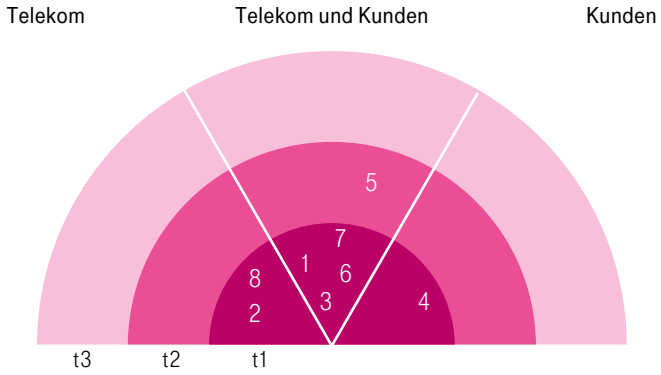
▶ Fortsetzung von Seite 14 – Deutsche Telekom CERT: Cyber Emergency Response Team

Risikoportfolio



1 Advanced persistent threats
2 Spear Phishing gegen DTAG
3 Mobiler Schadcode
4 Angriffe auf mobiles Banking
5 DoS auf DNS Infrastruktur
6 Angriffe auf DSL Router
7 Recovery Fehler bei Cloud Diensten
8 Shitstorm/„Empörungswelle“

Bedrohungsradar



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

Zentrale Inhalte des Strategic Threat Radar:
Die Trend Scouting Community ist ein neues Instrument der Strategic Threat Radar-Methodik. Es geht dabei um den internationalen Austausch von Sicherheitsexperten aus der IT und Netzwelt. Eigens hierfür nutzt die Deutsche Telekom eine Kollaborationssoftware, die es den Teilnehmern ermöglicht, Technologietrends und Bedrohungen zu benennen und zu diskutieren. Das Deutsche Telekom CERT nutzt diese Community, um auch sehr individuelle Technologien und Trends bei der Risikobewertung zu berücksichtigen.

Advanced persistent threats (APT):
APT beschreibt die Kombination von verschiedenen Angriffswerkzeugen und Techniken (zum Beispiel Social Engineering, SQL Injection, (Spear-)Phishing, Trojaner, Botnetze). Mittels des schleichenden APT-Angriffs werden Desktop bis hin zu Produktionssystemen über einen längeren Zeitraum kompromittiert und Unternehmensinformationen preisgegeben. Die Anzahl betroffener Unternehmen steigt stetig. Diebstahl und unautorisierte Veröffentlichung von Informationen sowie die Beeinträchtigung der Verfügbarkeit von Diensten führt zu immensen Reputationsschäden und damit zu Rückgang der Kundenanzahl.
Sicherheitsmaßnahme: Etablierung eines Sicherheits-Frameworks von organisatorischen und technischen Kontrollen; Identifizierung von kritischen Daten und Systemen; verstärkte Umsetzung von Sicherheitsanforderungen und Systemüberwachung gemäß Daten und Systemkritikalität.

Spear-Phishing (gegen Mitarbeiter der Deutschen Telekom):
Spear-Phishing ist ein Phishing-Angriff auf eine bestimmte Personengruppe oder Einzelperson, oft verbunden mit dem Ziel, Zugang zu Unternehmensinformationen zu erhalten oder diese zu kompromittieren.
Sicherheitsmaßnahme: Die Sensibilisierung für das Thema ist insbesondere für die Schlüsselrollen eines jeden Unternehmens entscheidend wichtig. Ein striktes Patchmanagement ist für die am häufigsten angegriffenen Systeme, wie zum Beispiel Webbrowser und Add-ons (flash/macromedia), Office Suite, Mail-Clients und Betriebssysteme notwendig. Eine weitere Maßnahme ist die Netzwerk- und Datensegmentierung.

Mobile Malware:
Bösartige und betrügerische Schadprogramme auf mobilen Endgeräten, die über AppStores ohne Qualitätsüberprüfung verteilt werden, können erheblichen Schaden anrichten. Mobile Schadprogramme für Smartphones können zum Beispiel mobile Botnetze aufbauen. Mögliche Angriffsziele sind hierbei die vom Internet aus erreichbaren Infrastruktur-Komponenten.

▶ Seite 16

SICHERHEIT IM INTERNET.

▶ Fortsetzung von Seite 15 – Deutsche Telekom CERT: Cyber Emergency Response Team

Sicherheitsmaßnahme: Installation von Anti-Virus- und Anti-Schadsoftware auf mobilen Endgeräten als Standardkonfiguration; User-Awareness-Kampagnen für die Identifizierung von sicheren Apps.

Angriffe auf Mobile Banking:

Diverse Techniken stehen heutzutage im Internet zur Verfügung, um den Einsatz von Authentisierungsverfahren beim Mobile Banking zu umgehen. In verschiedenen Ausgaben dieses Reports haben wir auf Varianten hingewiesen. Beispiele sind der sogenannte „Zeus"-Trojaner auf mobilen Endgeräten (auf BlackBerry, Symbian und Android) und SpyEye (PC-basierte Schadsoftware). Das Risiko liegt beim Endnutzer, der zumeist an der Ausführung der Schadsoftware unwissentlich beteiligt wird.
Sicherheitsmaßnahme: Umsetzung von Virenschutz auf Smartphones; Awareness-Maßnahmen des Bankensektors zu Angriffsvektoren und Schutzmaßnahmen, Awareness-Maßnahmen des Kunden.

DoS on DNS:

Mobile Schadprogramme für Smartphones errichten mobile Botnetze. Angriffsziel sind die vom Internet aus erreichbaren Netzkomponenten.
Sicherheitsmaßnahme: Härtung von Anwendungen und Systemen mit direktem Internet-Zugang, unterstützt durch Security Patch Management, Vulnerability & Advisory Management, Patchlevel-Scanning.

Attack on DSL router (Chuck Norris Wurm):

Durch Schadsoftware wie den Chuck Norris Wurm infizierte, aus dem Internet erreichbare Router werden Teil eines Botnets. Diese Schadsoftware befällt schwach konfigurierte Router und DSL-Modems. Der Schädling installiert sich, indem die Standard-Administrations-Passwörter erraten werden. Die vielfache Ausnutzung von schwachen Zugangskonfigurationen ist nachgewiesen. Manipuliert wurden unter anderem die DNS Server Einträge.
Sicherheitsmaßnahme: Verstärkte User Awareness-Maßnahmen zur Änderung von Standard-Passwörtern und Accounts bei dem Einsatz fabrikneuer DSL-Router/Internet Access Devices.

Cloud recovery failure:

Disaster Recovery-Ausfall bei Cloud-Diensten. Bedrohung von Verfügbarkeit und Vertraulichkeit der Cloud durch großflächigen Ausfall von Cloud-Diensten. Renommierte Cloud-Dienstleister erlitten in 2011/2012 folgenschwere Ausfälle ihrer Cloud-Dienste, die zu Datenverlust und tagelangen Dienstausfällen für ihre Kunden führte. Die Beeinträchtigung der Verfügbarkeit oder Vertraulichkeit führt zu Reputationsschaden und Rückgang der Kundenanzahl.

Sicherheitsmaßnahme: Datentrennung in der Cloud und Duplizierung von kritischen Daten auf Serverlandschaften in unterschiedlicher geographischer Lage. Kontinuierliche Überprüfung von geeigneten Backup- und Restore-Lösungen und Konzepten, die durch ein geeignetes Emergency Response Management bei der Disaster Recovery unterstützt werden sollten.

Shitstorm:

Shitstorm oder auch „Empörungswelle" ist ein Internet-Phänomen, bei dem in kürzester Zeit zahlreiche Internet-Beiträge entstehen, bei denen sich sachliche mit unsachlicher, korrekter und falscher Information mischt. Diese Informationen werden von den öffentlichen Medien aufgenommen und an das Management betroffener Unternehmen herangetragen. Die Konsequenz ist, dass auf Basis falscher Informationen und aufgrund des erheblichen öffentlichen Mediendrucks das Unternehmen genötigt ist, umgehend immensen Aufwand in die Problemuntersuchung sowie umfangreiche kommunikative Maßnahmen zu investieren und dadurch von wirklich kritischen Problemen abgehalten wird beziehungsweise diesen eine niedrigere Priorität zugewiesen wird.
Sicherheitsmaßnahme: Gezielte personenbezogene Awareness-Maßnahmen sollten durchgeführt werden, um auf das Risiko von übereilten Aktionen auf Basis von Shitstorm-Informationen hinzuweisen.

Einladung

Das Deutsche Telekom CERT lädt Experten aus allen Bereichen der Deutschen Telekom Group ein, als Trend Scout an der Aktualisierung des Strategic Threat Radars und der Bewertung der Bedrohungen mitzuwirken. Für nähere Information wenden Sie sich gerne direkt an cert@telekom.de.

Facts & Figures für das Jahr 2012

Zahl der von der Deutschen Telekom betriebenen Honeypot-Systeme	92
Gesamtzahl simulierter Schwachstellen in Honeypots	1.023.980
Zahl der einzelnen böswilligen Codes	11.628
Anzahl eingegangener Hinweise auf missbräuchliche Nutzung	12,7 Millionen
Anzahl Dienstsperrungen (zum Beispiel E-Mail)	132.906
Zahl aufgehobener Netzwerkzugriffseinschränkungen	33.693

SICHERHEIT IM INTERNET.

KONTAKT

Missbrauchs-Team/Abuse-Team
Deutsche Telekom AG
Group Information Security
Missbrauchs-Team
T-Online-Allee 1
64295 Darmstadt, Deutschland
E-Mail: Abuse@t-online.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.