Hintergrundinformation

Daten und Fakten aus dem 12. Internet Security Threat Report von Symantec

Der Symantec Internet Security Threat Report bietet eine umfassende Übersicht der aktuellen Gefahrenpotenziale aus dem Internet. Neben detaillierten Ergebnissen werden auch die Methoden der Datenerhebung und Analyse vorgestellt. Unternehmen und Endanwender erhalten damit notwendige Informationen, um ihre Systeme entsprechend abzusichern.

Der Report, der seit sechs Jahren im halbjährlichen Turnus erscheint, ist nunmehr in der zwölften Ausgabe verfügbar. Die Daten wurden im Zeitraum vom 1. Januar 2007 bis zum 30. Juni 2007 erhoben.

Die Daten und Fakten aus dem Internet Security Threat Report in der 12. Ausgabe beinhalten:

I. Fakten und Trends: Professionalisierung und Kommerzialisierung einer Untergrundwirtschaft
II. Fakten und Trends: Neue Angriffstechniken und Paradigmenwechsel in der Methodik
III. Fakten und Trends: Highlights aus dem Internet Security Threat Report XII

I. Fakten und Trends: Professionalisierung und Kommerzialisierung einer Untergrundwirtschaft

Das Gefahrenpotenzial aus dem Internet hat sich über die letzten zwei Jahre grundsätzlich verändert. Angreifer von heute verfolgen klare finanzielle Interessen, und auch das Vorgehen hat nichts mehr mit der zerstörerischen Motivation früherer Virenschreiber zu tun. Die neue Herangehensweise fußt auf zwei Säulen: Zum einen organisieren sich die Angreifer und entwickeln Techniken, die der traditionellen Software-Entwicklung immer ähnlicher werden, zum anderen verfeinern sie die Angriffsstrategien und übernehmen Geschäftspraktiken aus der realen Welt.

Bereits im Frühjahr 2006 hatte der Internet Security Threat Report IX (ISTR) auf die Entstehung einer Untergrundwirtschaft hingewiesen, die über IRC, Webseiten und Schwarzmarkt-Auktionen Zeroday-Schwachstellen und entsprechende Angriffstools anbietet. Innerhalb kürzester Zeit hat sich diese Kommerzialisierung zu einem milliardenschweren

kriminellen Zweig entwickelt und auch die Entwicklung, Verbreitung und Implementierung vieler bösartiger Codes und Aktivitäten zeugt von einer hochgradigen Professionalität.

1.000 Dollar für Angrifftools

Ein Beispiel hierfür ist das Angriffs-Toolkit MPack, welches im Berichtszeitraum auf Untergrundservern für 1.000 US-Dollar angeboten wurde. Es handelt sich dabei um eine Sammlung von mehrstufigen Angriffs-Modulen, die über eine Management-Konsole gesteuert wird. Zuerst wird die Schadsoftware auf einer präparierten Webseite hinterlegt. Sobald die Webseite vom Anwender besucht wird, lädt der Browser weitere Schadcodes nach. Dabei probiert das Angriffsmodul nach Analyse des Betriebssystems und Browsers mehrere Angriffe, bis es Erfolg hat. Programmierung und Umfang der Software lassen auf eine professionelle Entwicklung schließen.

Phishing-Toolkits im Baukastensystem

Ein weiteres Indiz für die Kommerzialisierung von Internetangriffen ist das verbreitete Auftreten von Phishing-Toolkits; hierbei handelt es sich um eine Reihe von Skripts, die einem Angreifer die automatische Einrichtung von Phishing-Webseiten ermöglichen, welche die Webseiten von Markenunternehmen vortäuschen – inklusive der zugehörigen Bilder und Logos. Parallel lassen sich über die Skripts korrespondierende Phishing-Mails generieren, um den Anwender auf die Webseite zu locken. Im Berichtszeitraum stammten 86 Prozent der Phishing-Webseiten von lediglich 30 Prozent der erfassten Phishing IP-Adressen – ein Indikator dafür, dass solche Phishing-Toolkits regelmäßig zum Einsatz kommen.

Hohe Anzahl an Untergrund-Servern

Die Existenz einer immer weiter ausufernden Anzahl von "Untergrund-Servern" unterstreicht ebenfalls die negative Entwicklung hinsichtlich der Kommerzialisierung und Professionalisierung der Angreifer. Auf den Servern vermarkten Kriminelle gestohlene Informationen – in den meisten Fällen handelt es sich um Identitätsnachweise wie beispielsweise Ausweis- und Kreditkartennummern, PINs, Benutzerkonten und Listen mit E-Mail-Adressen.

Im Berichtszeitraum befanden sich 64 Prozent der Untergrund-Server in den USA. Bei 22 Prozent der angebotenen Waren handelte es sich um Kreditkarten-Informationen. 85 Prozent der Kreditkarten waren von US-amerikanischen Banken ausgestellt. Dadurch lässt sich resümieren, dass Angreifer größtenteils in ihren Regionen operieren und sich auf Ziele in ihrem Sprachraum und in ihrer Online-Infrastruktur fokussieren.

Regionale Angriffsziele

Die Regionalisierung verdeutlicht auch die Verbreitung von Schadcode. 44 Prozent aller im Berichtszeitraum erfassten Trojaner wurden in Nordamerika gefunden, wo hingegen 43 Prozent der durch Würmer infizierten Rechner in der EMEA-Region zu finden sind. Einer der Gründe hierfür ist, dass die E-Mails mit den Schadcodes in der jeweiligen Landessprache verfasst werden. Auch hier sind Ausnahmen wie der Massenversender Sober.AA zu nennen, der sowohl in Englisch als auch auf Deutsch verfasst wurde. Dieses Beispiel verdeutlicht, dass sich mit der weltweit steigenden Verfügbarkeit von Breitbandzugängen auch die Operationsgebiete der Angreifer entsprechend ausweiten werden. So wurde bereits der E-Mailwurm Rontokbro auf Englisch und Indonesisch verfasst.

Breitband versus Sicherheit

In den vergangenen Internet Security Threats Reports (ISTR) wurde bereits auf die wachsende Verbreitung von Breitband-Internetzugänngen und dem oft fehlenden Bewusstsein für die damit verbundenen Risiken hingewiesen. Gerade viele neue Breitband-Nutzer sind sich nicht darüber bewusst, dass sie sich besonders gegen die Bedrohungen aus dem Internet schützen müssen, da sie meistens deutlich mehr Zeit online verbringen. Ein weiterer Fakt ist, dass mit der Expansion der Breitband-Infrastruktur viele neue Internet Service Provider in den Markt drängen, bei denen der Sicherheitsaspekt nicht im Vordergrund steht. Diese Entwicklung ist weltweit zu beobachten, besonders in Regionen, in denen die Infrastruktur gerade noch entsteht oder sich rasant entwickelt wie in China, wo 29 Prozent aller Bots zu finden sind.

II. Neue Angriffstechniken und Paradigmenwechsel in der Methodik

Während traditionelle Internet-Angriffsaktivitäten bislang meist aus Einzelattacken bestanden – mit dem Ziel, sich unbefugt Zugang zu einem Rechner oder dessen Daten zu verschaffen – handelt es sich bei den aktuellen Angriffstechniken oft um mehrstufige Angriffe, bei denen zunächst eine Erstattacke erfolgt, um einen "Brückenkopf" zu bilden, über den dann später weitere Attacken lanciert werden. Derartige mehrstufige Attacken deuten darauf hin, dass Angreifer vermehrt auf verdeckte Techniken ausweichen müssen, um starke Netzwerk-Sicherheitsmaßnahmen wie IDS/IPS und Firewalls zu überwinden. Diese Schutztechnologien haben als Abwehr gegen den massiven Einsatz von Internetwürmern und groß angelegte DoS-Attacken bereits gute Wirkung gezeigt. Die neue Technik führt aber auch zu einem Paradigmenwechsel in der Angriffsmethodik: Wurden in der Vergangenheit direkte und gezielte Angriffe gegen Einzelpersonen und Unternehmen durchgeführt, so legen sich die Angreifer heute auf die Lauer und warten bis ihr Angriffsziel selbst auf sie zukommt, wie das MPack-Beispiel, der "gestaffelten Downloader" (Staged Downloader) oder auch "modularer

Schadcode" verdeutlichen. Angreifer sind dadurch in der Lage, die Komponenten für jede beliebige Art von Bedrohung, wie beispielsweise Identitätsdiebstahl, zu modifizieren und für eigene Zwecke zu missbrauchen.

Sicherheitsrisiko Web 2.0

"Social Networking"-Webseiten und Webapplikationen haben sich für die Hacker als besonders ergiebig erwiesen, da sie Angreifern Zugang zu einer Vielzahl von Personen bieten, von denen viele blind darauf vertrauen, dass diese Webseiten sowie ihr Inhalt sicher sind; solche Webseiten lassen sich aber aufgrund der gegebenen Schwachstellen in den Web-Anwendungen oft leicht ausnutzen. Dies hat ernste Konsequenzen für die Anbieter, da das Vertrauen in die bekannten und beliebten Webseiten verloren gehen kann. Der bislang gängige Rat, “schlechten Umgang” im Internet zu vermeiden, reicht heutzutage nicht aus.

Angriffe auf Social Networking-Seiten haben für Angreifer einen hohen Nutzen, da sie auf diese Weise an vertrauliche Benutzerinformationen gelangen können, die sich wiederum für Identitätsdiebstahl und Betrugsdelikte oder für Zugriffe auf andere Webseiten nutzen lassen, über die dann weitere Folgeattacken möglich sind. Dieser Angriffstrend beschädigt das Ansehen von Unternehmen, bedroht die Identität von Einzelpersonen und gefährdet das Vertrauen in die digitale Welt.

II. Highlights aus dem Internet Security Threat Report XII

Wie bereits in den letzten Internet Security Threat Reports gibt auch die Ausgabe XII eine detaillierte Übersicht über die jeweiligen Sicherheitsbedrohungen:

Internetattacken – USA weiterhin führend, Israel mit hohen Aktivitäten

- Die USA waren im ersten Halbjahr 2007 mit 61 Prozent Hauptangriffsziel von Denial of Service-Attacken (DoS)
- Israel verfügte über die größte Anzahl an schädlichen Aktivitäten pro Internetnutzer, gefolgt von Kanada und den USA
- 46 Prozent der Daten- und Identitätskriminalität resultieren aus dem Diebstahl und/oder Verlust von Laptops und Speichergeräten
- Mit 22 Prozent waren Kreditkarten-Informationen die meist gehandelte Warengruppe auf Untergrund-Servern
- China verfügt mit 29 Prozent über die größte Anzahl von Bot infizierten Rechnern
- Sieben Prozent aller weltweiten Bots stehen in Peking

Sicherheitslücken – Browser als Hauptschwachstelle

- Symantec dokumentierte im Berichtszeitraum 39 Sicherheitslücken im Microsoft Internet Explorer, 34 in Mozilla Browsern, 25 in Apple Safari und sieben in Opera. Besonders bei Apples Safari ist ein Anstieg der Sicherheitslücken festzustellen. Im zweiten Halbjahr 2006 waren es nur vier.
- 90 Sicherheitslücken in Applikationen wurden von den Herstellern nicht geschlossen. Die meisten noch offenen Sicherheitslücken stammen von Microsoft.
- Im Berichtszeitraum wurden 237 Sicherheitslücken in Browser Plug-ins festgestellt. Im zweiten Halbjahr 2006 waren es noch 74.
- 89 Prozent der Sicherheitslücken in Plug-ins betreffen ActiveX-Komponenten. Im Vorberichtszeitraum waren es nur 58 Prozent
- Mehr als 50 Prozent der durch die Betriebssystemanbieter geschlossenen Sicherheitslücken mit hoher Gefahrenstufe betrafen Web-Browser.

Schadcodes – Wachstum um 185 Prozent

- Im ersten Halbjahr 2007 wurden 212.101 neue Schadcodes erfasst. Das entspricht einer Steigerung um 185 Prozent gegenüber dem Vorberichtszeitraum.
- 73 Prozent der Top-50 Schadcodes waren Trojaner.
- 43 Prozent der durch Würmer infizierten Rechner sind in der Region EMEA.
- In Nordamerika sind 44 Prozent der durch Trojaner infizierten Rechner zu finden
- Neun von zehn Stage Downloadern waren Trojaner.
- Sieben von zehn der von Stage Downloadern nachgeladenen Komponenten waren Trojaner und drei von zehn Backdoors.
- Fünf der Top-50 Schadcodes sind für Online-Spiele konzipiert.

Phishing und Spam – Toolkits auf dem Vormarsch

- Drei Phishing-Toolkits waren für 42 Prozent der Phishing-Attacken im Berichtszeitraum verantwortlich.
- Symantec blockierte 2,3 Milliarden Phishing-Mails. Das entspricht einem Anstieg um 53 Prozent gegenüber dem Vorberichtszeitraum.
- 59 Prozent der Phishing-Webseiten waren in den USA gehostet.
- 86 Prozent der Phishing-Webseiten stammen von 30 Prozent der IP-Adressen, die als Phishing-Server enttarnt wurden.
- 60 Prozent der Spam E-Mails waren in englischer Sprache verfasst – ein Rückgang um fünf Prozent gegenüber dem zweiten Halbjahr 2006.
- 47 Prozent der Spam E-Mails haben ihren Ursprung in den USA.
- Mit 10 Prozent haben Spam-Zombies die größte Verbreitung in den USA.

In den letzten zwei Jahren hat die Professionalität und Kommerzialisierung bei der Entwicklung, Verbreitung und Implementierung vieler bösartiger Codes und Aktivitäten deutlich zugenommen. In vielerlei Hinsicht sind heutige Angriffstools ein Spiegelbild der ausufernden Untergrundwirtschaft – und zwar insofern, als dass professionelle Tools benötigt werden, um den Anforderungen einer inzwischen milliardenschweren kriminellen Branche gerecht zu werden. Ebenso wie frühere GUI-basierte Angriffstools wie Back Orifice — ursprünglich eine Fernverwaltungs-Software für Sicherheitsprofis — von der Hacker-Gemeinde als Mittel zur Kontrolle von Fremdsystemen übernommen wurden, erinnern auch heutige Toolkits stark an professionell entwickelte und vermarktete Software-Produkte.

Trotz dieser Professionalisierung ist auch der Anwender nach wie vor ein Sicherheitsrisiko. Denn sein oft fehlendes Sicherheitsbewusstsein beim Umgang mit dem Internet oder im Social Web machen sich die Angreifer zu nutze. Doch auch vorsichtige Anwender sind nicht gegen Fallen gefeit, denn immer öfter manipulieren die Angreifer vertrauenswürdige Webseiten und/oder Anwendungen, so dass sie bei einem Benutzerzugriff in den Rechner ihres Opfers eindringen können.

Durch den Einsatz von mehrstufigen Angriffsmethoden, die es jederzeit erlauben, alle möglichen Schadcodes wie Trojaner, Bots, Backdoors, Spam und Phishing einzuschleusen sind nicht nur einzelne Anwender, sondern ganze Unternehmensnetzwerke betroffen. Besonders für große IT-Abteilungen ist es deshalb an der Zeit, die einzelnen Verantwortungsgebiete für die Sicherheit von Netzwerken, Desktops, Viren- und Spam-Schutz zusammenzuführen, um gegen die Komplexität des Risikopotenzials gewappnet zu sein.

Symantec Internet Security Threat Report

Der "Symantec Internet Security Threat Report" bietet einen umfassenden Überblick über aktuelle Bedrohungen aus dem Internet und ist der einzige öffentlich zugängliche Bericht seiner Art, der nicht nur eine eingehende Analyse relevanter Daten und Trends veröffentlicht, sondern auch umnfangreich Aufschluss gibt über die Verfahren und Methoden, mit denen diese Ergebnisse erzielt wurden. Aufgabe dieses Berichts ist es, alle Informationen bereitzustellen, die Privatpersonen und Unternehmen benötigen, um ihre Systeme jetzt und in Zukunft wirksam schützen zu können.

Der Bericht bietet einen halbjährlich aktualisierten Überblick über Internet-Bedrohungen; die aktuelle Ausgabe XII deckt den Zeitraum vom 1. Januar 2007 bis zum 30. Juni 2007 ab.

Um dem neuen Trend zu regionalen Bedrohungsmustern Rechnung zu tragen, gibt Symantec neben dem genannten Hauptbericht drei weitere Berichte heraus:

- den "EMEA Internet Security Threat Report" (für die Regionen Europa, Mittlerer Osten und Afrika)
- den "APJ Internet Security Threat Report" (für die Region Asien/Pazifischer Raum/Japan)
- den "Government Internet Security Threat Report", der sich in erster Linie mit Bedrohungen und Trends befasst, die speziell für Regierungsorganisationen und Behörden sowie kritische Infrastrukturbereiche wie die Öl- und Gasbranche, Energie- und Stromversorger und Finanzdienstleister interessant sind.

Weiterführende Informationen zur Datenerhebung

Die im 12. Internet Security Threat Report analysierten Daten stammen aus verschiedenen Informationsquellen von Symantec und sind zusammen genommen die weltgrößte Ressource für Datensicherheit:

- Symantec DeepSight Threat Management System und Symantec Managed Security Services – mehr als 40.000 Sensoren, die die Netzwerkaktivitäten in 180 Ländern überwachen.
- Symantec Virenschutzlösungen – mehr als 120 Millionen Installationen auf Clients, Servern und Gateways erfassen Schadcodes, Spyware und Adware.
- Schwachstellen-Datenbank – mehr als 22.000 erfasste Sicherheitslücken aus mehr als 50.000 Technologien von über 8.000 Anbietern seit mehr als zehn Jahren.
- BugTraq – Forum mit über 50.000 Abonnenten, die täglich neue Gefahrenpotenziale diskutieren und Lösungsansätze austauschen.
- Symantec Probe Network – ein System mit mehr als zwei Millionen E-Mail Accounts, als Köder in 20 Ländern installiert, um weltweite Spam- und Phishing-Aktivitäten zu analysieren.
- Symantec Phish Report Network – eine umfangreiche Community, deren Mitglieder, Unternehmen und Endkunden, betrügerische Webseiten aufdecken, indem sie Informationen zu Phising-Webseiten an das Netzwerk weiterleiten und im Gegenzug weiterführende Daten zu aktuellen Phising-Aktivitäten erhalten.

Weitere Details, Grafiken sowie den kompletten Sicherheitsbericht finden Sie im Symantec Online-Pressezentrum unter:
http://www.symantec.com/de/de/about/theme.jsp?themeid=threat_report

Umfassendes Hintergrundmaterial zum Symantec Global Intelligence Network ist unter folgendem Link erhältlich:
http://www.symantec.com/about/news/resources/press_kits/securityintelligence/

Über Symantec
Symantec ist ein weltweit führender Anbieter von Software, mit der sich Unternehmen und Privatpersonen sicher und vertrauensvoll in einer vernetzen Welt bewegen können. Das Unternehmen unterstützt Kunden mit Software und Dienstleistungen beim Schutz ihrer Infrastrukturen, Informationen und Interaktionen. Symantec hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in 40 Ländern. Mehr Informationen unter www.symantec.de

Hinweis für Redakteure:
Wenn Sie mehr über Symantec und seine Produkte erfahren möchten, dann besuchen Sie unser Online-Pressezentrum unter www.symantec.com/presse
Dort liegt auch Bildmaterial von Personen und Produkten für Sie bereit.

Symantec (Deutschland) GmbH, Humboldtstraße 6, 85609 Aschheim
Telefon: +49 (0) 89 / 94302 - 100
Telefax: +49 (0) 89 / 94302 – 950

Ihr Ansprechpartner (NUR PRESSE!) für Rückfragen:

Corinna Spohr
PR Manager
Symantec (Deutschland) GmbH
Telefon +49 (0) 89-94302-620
Fax: +49 (0) 89-94302-450
E-Mail: corinna_spohr@symantec.com

Suemer Cetin
PR Consultant
Trimedia Communications Deutschland GmbH
Telefon +49 (0) 211-96485-54
Fax +49 (0) 211-96485-45
E-Mail: suemercetin@dus.trimedia.de