Honeypot

aus Wikipedia, der freien Enzyklopädie

Als **Honigtopf** oder auch englisch ***honeypot*** wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind vom eigentlichen Ziel ablenken soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte. Der Ursprung stammt aus der Überlegung, dass Bären mit einem Honigtopf sowohl abgelenkt als auch in eine Falle gelockt werden könnten.

Im übertragenen Sinne werden sehr verschiedene Dinge als „Honeypot“ bezeichnet.

Inhaltsverzeichnis

Computernetzwerke und -sicherheit

Als *Honeypot* (oder früher auch *Iron Box*) wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, der die Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Erfolgt ein Zugriff auf einen derartigen virtuellen Dienst oder Nutzer, werden alle damit verbundenen Aktionen protokolliert und gegebenenfalls ein Alarm ausgelöst. Das wertvolle reale Netzwerk bleibt von Angriffsversuchen möglichst verschont, da es besser gesichert ist als der Honeypot.

Die Idee hinter Honeypot-Diensten ist, in einem Netzwerk einen oder mehrere Honeypots zu installieren, die keine vom Anwender selbst oder seinen Kommunikationspartnern benötigten Dienste bieten und daher im Normalbetrieb niemals angesprochen werden. Ein Angreifer, der nicht zwischen echten Servern bzw. Programmen und Honeypots

unterscheiden kann und routinemäßig alle Netzkomponenten auf Schwachstellen untersucht, wird früher oder später die von einem Honeypot angebotenen Dienste in Anspruch nehmen und dabei von dem Honeypot protokolliert werden. Da es ein ungenutztes System ist, ist jeder Zugriff darauf als ein möglicher Angriffsversuch zu werten.

Honeypots, die Anwender simulieren (engl.: "honeyclients"), nutzen normale Webbrowser und besuchen Websites, um Angriffe auf den Browser oder Browser-Plug-ins festzustellen.

Mehrere "Honeypots" können zu einem vernetzten Honigtopf (engl. "Honeynet") zusammengeschlossen werden.

Kriterien zur Unterscheidung

Art der Implementierung

Ein *physischer* Honeypot ist ein realer Rechner im Netzwerk mit eigener Netzwerkadresse. Ein *virtueller* Honeypot ist ein logisch eigenständiges System, das durch einen anderen Rechner simuliert wird. Beim *Client Honeypot* wird ein realer Server von einer Honeypot-Software angesprochen. Beim *Server Honeypot* werden reale Clients von einer Honeypot-Software „bedient“.

Grad der Interaktion

Man unterscheidet unabhängig von der Art der Implementierung jeweils zwischen *low interaction* und *high interaction* Honeypots.

Typen

Low-Interaction Server Honeypots

Ein Low-Interaction *server* Honeypot ist meist ein Programm, das einen oder mehrere Dienste *emuliert*. Der Informationsgewinn durch ein Low-Interaction-Honeypot ist daher beschränkt. Er wird insbesondere zur Gewinnung statistischer Daten eingesetzt. Ein versierter Angreifer hat wenig Probleme, einen Low-Interaction-Honeypot zu erkennen. Um automatisierte Angriffe beispielsweise von Computerwürmern zu protokollieren, reicht ein Low-Interaction Honeypot allerdings vollständig aus. In diesem Sinne kann er zum Erkennen von Einbruchversuchen genutzt werden (engl.: Intrusion Detection System).

Einige Beispiele für Low-Interaction Honeypots sind:

- *honeyd*, unter der GPL veröffentlicht, kann gesamte Netzwerkstrukturen emulieren; eine Instanz der Software kann viele verschiedene *virtuelle Computer* in einem Netzwerk simulieren, die alle unterschiedliche Dienste anbieten.
- *mwcollectd* ist ein freier Honeypot unter der Lesser GPL für POSIX-kompatible Betriebssysteme mit der Zielsetzung, automatisierte Attacken von Würmern nicht nur zu erkennen und protokollieren, sondern die Verbreitungsmechanismen der Würmer zu nutzen, um eine Kopie des Wurms zu erhalten. Dazu werden als verwundbar bekannte Dienste nur so weit wie benötigt emuliert, ausgehend von verfügbaren Angriffsmustern.
- Nepenthes, ebenfalls unter der GPL veröffentlicht, ist wie *mwcollect* ein Honeypot für POSIX-kompatible Betriebssysteme mit dem Fokus, Würmer zu sammeln.
- *Amun* ist ein in Python geschriebener Honeypot, der sowohl unter Linux als auch auf anderen Plattformen

lauffähig ist. Amun ist unter GPL veröffentlicht. Durch die Simulation von Schwachstellen werden sich automatisiert verbreitende Schadprogramme geködert und eingefangen.

- honeytrap ist ein Open-Source-Honeypot für die Sammlung von Informationen zu bekannten und neuen netzbasierten Angriffen. Um auf unbekannte Angriffe reagieren zu können, untersucht honeytrap den Netzwerk-Stream auf eingehende Verbindungsanfragen und startet dynamisch Listener für die entsprechenden Ports, um die Verbindungsanfragen zu verarbeiten. Im „Mirror Mode“ können Attacken zum Angreifer zurückgespiegelt werden. Über eine Plugin-Schnittstelle ist honeytrap um zusätzliche Funktionen erweiterbar.

- *multipot* ist ein Honeypot für Windows; er emuliert wie *Nepenthes* und *mwcollect* Schwachstellen unter Windows, um Würmer zu sammeln.

Low-Interaction Client Honeypots

Low-Interaction Client Honeypots sind eigenständige Programme, die ohne die Verwendung von normalen WebBrowsern Webseiten besuchen und versuchen, Angriffe auf den emulierten Browser zu erkennen.

phoneyc ist ein in Python geschriebener Client Honeypot, der Websites besucht, um Angriffe auf bekannte Lücken in WebBrowsern und ihre Erweiterungen ("Brower-Plugins") zu finden. *phoneyc* nutzt die auch von Firefox verwendete Javascript-Engine SpiderMonkey, um Angriffe zu erkennen.

High-Interaction Server Honeypots

High-Interaction Honeypots sind zumeist vollständige Server, die Dienste anbieten. Sie sind schwieriger einzurichten und zu verwalten als Low-Interaction Honeypots. Der Fokus bei einem High-Interaction-Honeypot liegt nicht auf automatisierten Angriffen, sondern darauf, manuell ausgeführte Angriffe zu beobachten und protokollieren, um so neue Methoden der Angreifer rechtzeitig zu erkennen. Zu diesem Zweck ist es sinnvoll, dass es sich bei einem High-Interaction-Honeypot um ein scheinbar besonders lohnendes Angriffsziel handelt, d.h. einen Server, dem von potentiellen Angreifern ein *hoher Wert* nachgesagt wird (engl.: "high value target").

Sebek

Zur Überwachung eines High-Interaction-Honeypots wird eine spezielle Software eingesetzt, meist das frei verfügbare *Sebek*, die vom Kernel aus alle Programme des Userlands überwacht und die anfallenden Daten vom Kernel aus an einen protokollierenden Server sendet. Sebek versucht dabei unerkannt zu bleiben, d.h. ein Angreifer soll möglichst weder wissen, noch sollte er erahnen können, dass er überwacht wird.

Argos

Der auf QEMU basierende *Argos Honeypot* kommt ohne eine spezielle Überwachungssoftware aus. Um Angriffe über das Netzwerk zu erkennen, werden Speicherinhalte, die über das Netzwerk empfangene Daten enthalten, von dem modifiziertem QEMU als verseucht (engl.: "tainted" = „verunreinigt“) markiert. Neue Speicherinhalte, die durch bereits verseuchte Speicherinhalte erzeugt wurden, gelten ebenfalls als verseucht. Sobald verseuchter Speicherinhalt von der CPU ausgeführt werden soll, schreibt Argos den Datenstrom und Speicherinhalt für die weitere forensische Analyse nieder und beendet sich.

Durch den für die Emulation und Überprüfung des Speichers notwendigen Mehraufwand erreicht ein *Argos Honeypot* nur einen Bruchteil der Geschwindigkeit eines nativen Systems auf gleicher Hardware.

High-Interaction Client Honeypots

High-Interaction Client Honeypots laufen auf regulären Betriebssystemen und nutzen reguläre Webbrowser, um Angriffe auf Browser zu erkennen.

Capture-HPC nutzt eine Client-Server Architektur, bei der der Server die zu besuchenden Websites vorhält, die von den Clients besucht werden, und an den die Ergebnisse zurückgemeldet werden.

mapWOC lädt Seiten mit verwundbaren Webbrowsern, die zeitweise in einer virtuellen Maschine laufen. Durch Beobachtung des Datenverkehrs zur virtuellen Maschine werden Angriffe, wie "Drive-by-Downloads" erkannt.[1] MapWOC ist Freie Software (Open Source).[2]

Honeypot-ähnliche Ansätze

Tarpits

→ *Hauptartikel: Teergrube (Informationstechnik)*

Tarpits (engl. für „Teergrube“) dienen beispielsweise dazu, die Verbreitungsgeschwindigkeit von Würmern zu verringern. Das Verfahren ist auch unter dem Namen *LaBrea* (zur Namensgebung siehe hier) bekannt. Teergruben täuschen große Netzwerke vor und verlangsamen oder behindern so beispielsweise die Verbreitung von Internetwürmern oder die Durchführung von Netzwerkscans. Ebenso gibt es aber auch Teergruben, die offene Proxyserver emulieren und – falls jemand versucht, Spam über diesen Dienst zu verschicken – den Sender dadurch ausbremsen, dass sie die Daten nur sehr langsam übertragen.

Honeylinks

Angelehnt an das Honeypot-Konzept, existieren weitere Ansätze zum Entlarven von potenziellen Angreifern auf Web-Anwendungen. Spezielle Web Application Firewalls injizieren hierzu in HTML-Kommentaren versteckte Links auf nicht existierende Seiten bzw. potenziell interessante Teilbereiche einer Web-Anwendung. Diese sogenannten Honeylinks werden von den Nutzern nicht wahrgenommen, von potenziellen Angreifern im Rahmen einer Code-Analyse des HTML-Codes jedoch schon. Wenn nun ein solcher Honeylink aufgerufen wird, kann die WAF (Web Application Firewall) dies als Angriffsversuch werten und weitere Schutzmaßnahmen (z. B. ein Beenden der Web-Session) ergreifen.

Datenbank-Honeypots

Mit Hilfe sogenannter SQL-Injection-Attacken wird versucht, direkt auf die Datenbanken einer Webseite zuzugreifen. Da eine normale Firewall diese Zugriffe nicht erkennt (der Angriff kommt über die Webseite und somit nicht von einem als potenziellem Angreifer eingestuften System), verwenden Unternehmen sogenannte Datenbank-Firewalls. Diese können so konfiguriert werden, dass sie Angreifer glauben lassen, sie hätten erfolgreich Zugriff erlangt, während sie tatsächlich aber eine Honeypot-Datenbank sehen.[3]

Urheberrechtsverletzung

Auch im Zusammenhang mit der Verfolgung von Urheberrechtsverletzungen taucht manchmal der Begriff „Honeypot“ auf. In diesem Fall werden urheberrechtlich geschützte Werke von Organisationen wie der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) angeboten, um unvorsichtige Erwerber oder Anbieter über File Sharing zu fassen.

Verfolgung von Straftaten

Strafverfolgungsbehörden, insbesondere das US-amerikanische FBI, fahnden auch mit Hilfe von Honeypots z. B. nach Konsumenten von Kinderpornografie. Dazu werden Server eingerichtet, welche vorgeben, Kinderpornografie zum Herunterladen anzubieten. Tatsächlich werden strafrechtlich irrelevante Daten angeboten, die Zugriffe protokolliert und anschließend Strafverfahren gegen die zugreifenden Personen eingeleitet. Im Zuge dieser Strafverfahren werden über die Internetdienstanbieter die Identität der Personen ermittelt und Durchsuchungsbeschlüsse eingeholt. Dieses Verfahren wurde nach dem Einspruch eines Betroffenen durch ein Gericht für zulässig erklärt.[4] Auf mögliche Statistik-Verfälschungen durch diese Honeypot-Website-Strategien machte Bettina Winsemann 2010 aufmerksam.[5]

Ebenso wurden seit 2004 Webseiten des deutschen Bundeskriminalamts als Honeypot verwendet, um Mitglieder der linksradikalen militanten Untergrundorganisation „militante gruppe (mg)“ zu identifizieren. Dabei wurden nach einem getarnten Lockbeitrag in der Publikation *Interim* IP-Adressen der Besucher gespeichert, um diese Adressen bestimmten Kreisen zuzuordnen. Das Unternehmen war insgesamt erfolglos.[6] 2009 untersagte das Bundesinnenministerium die Überwachung von Verbindungsdaten, da es diese für einen schwerwiegenden „Eingriff in das Grundrecht auf informationelle Selbstbestimmung“ hält.[7]

Ähnlich ging die Polizei in Heilbronn vor, die während Mai 2007 und Januar 2008 ihre Internetseite als Honeypot verwendete. Die Besucher wurden mit Hilfe des Bundeskriminalamts registriert, in der Hoffnung, damit die Täter des zuvor ereigneten Polizistenmordes zu identifizieren. Die Zeitschrift Focus zitierte im Mai 2012 aus internen Akten, dass die Aktion rechtlich auf „sehr wackeligen Beinen“ stand und deswegen der Öffentlichkeit verschwiegen worden war. Auch diese Aktion war erfolglos.[8]

Einzelnachweise

1. *Über mapWOC (http://mapwoc.de/about-de.html).* Abgerufen am 12. Januar 2013.
2. *mapWOC - Lizenz (http://mapwoc.de/license-de.html).* Abgerufen am 12. Januar 2013.
3. Honigtopf - Architekturen unter Verwendung einer Datenbank-Firewall (http://www.dbcoretech.com/de/?p=437)
4. Heise online - FBI lockt Surfer in die Falle (http://www.heise.de/newsticker/FBI-lockt-Surfer-in-die-Falle--/meldung/105400)
5. Telepolis vom 8. Mai 2010: Honigtöpfe als Statistikfälscher (http://www.heise.de/tp/r4/artikel/32/32590/1.html)
6. Heise online: BKA-Honeypot www.bka.de (http://www.heise.de/newsticker/BKA-Honeypot-www-bka-de--/meldung/135343) vom 27. März 2009
7. Heise online: Innenministerium stoppt Überwachung der BKA-Seite (http://www.heise.de/newsticker/Spiegel-Innenministerium-stoppt-Ueberwachung-der-BKA-Seite--/meldung/134954) vom 21. März 2009
8. *Polizistenmord von Heilbronn: Ermittlern unterliefen mehrere schwere Pannen.* (http://www.focus.de/politik/deutschland/polizistenmord-von-heilbronn-schwere-vorwuerfe-gegen-ermittler_aid_755566.html) Focus, 21. Mai 2012, abgerufen am 21. Mai 2012.

Literatur

Klassische Fallbeschreibungen:

- Clifford Stoll: *The Cuckoo's Egg*. Doubleday, New York, 1989.
  - auf deutsch: „Kuckucksei“, erschienen im Fischer-Verlag.
- W. R. Cheswick, S. M. Bellovin: *An Evening with Berferd*. In: *Firewalls and Internet Security*. Addison-Wesley, 1994.
- Lance Spitzner: *Honeypots – Tracking Hackers*. Addison-Wesley, 2003, ISBN 0-321-10895-7.
- N. Provos, T. Holz: *Virtual Honeypots*. Pearson, 2008.
- Honeynet Projekt: *Den Feind Erkennen I / Know Your Enemy I* (http://old.honeynet.org/papers/trans/erkennen_I.txt), *Den Feind Erkennen II / Know Your Enemy II* (http://old.honeynet.org/papers/trans/erkennen_II.txt), *Den Feind Erkennen III / Know Your Enemy III* (http://old.honeynet.org/papers/trans/erkennen_III.txt) & *GenII Honeynets* (http://old.honeynet.org/papers/trans/gen2.html)

Weblinks

- *Honeypot Software, Honeypot Products, Deception Software* - Sammlung von Software-Links (http://www.honeypots.net/honeypots/products)
- Facharbeit *Sammeln von Malware in nicht nativer Umgebung* von Georg Wicherski (PDF-Datei; 731 kB) (http://web.archive.org/web/20090219063457/http://pixel-house.net/mwc_facharbeit.pdf)

Kategorien: IT-Sicherheit | Internetüberwachung
