Digitale Spurensuche

Assoziiert man mit Spurensuche gerne das Bild von Sherlock Holmes und Dr. Watson, die mit Lupen einen Tatort untersuchen, so sind bei der digitalen Spurensuche die Werkzeuge und Vorgehensweisen etwas anders. Schon allein die Feststellung eines Verbrechens ist im digitalen Zeitalter nicht unbedingt einfach: Erkennt jeder Nicht-Kriminologe, wenn eine Leiche in einer großen Blutlache liegt und ein Messer daneben, dann handelt es sich um Mord, also ein Verbrechen. Dagegen sieht man, ganz gleich, wie gut geschult und misstrauisch Administratoren sind, einem Word-Dokument nicht gleich an, dass es soeben unrechtmäßig an die Konkurrenz weitergegeben wurde. Systemeinbrüche sind oft nicht auf den ersten Blick zu erkennen und häufig werden „Unregelmäßigkeiten" im System fälschlicherweise als Datendiebstahl „erkannt".

Stufen eines Angriffs auf Computersysteme

Anders als beim herkömmlichen Kapital-Verbrechen, muss man als Computer-Forensiker möglichst exakte Kenntnisse von Angriffszenarien haben, um einen Angriff und seine Folgen richtig bewerten zu können.
So haben Angriffe oft identische Muster, die es gilt zu erkennen. Digitale Angriffe erfolgen in verschieden Stufen, die vom Administrator erkannt werden müssen. Hier ein Beispielszenario für einen Hackerangriff:

1. Stufe: Der Angreifer sucht seinen Zielbereich aus. Dabei sondiert er aus den verfügbaren Zielen die IP-Adressen aus, die interessant und möglicherweise ungesichert sind.
2. Stufe: Mit gezielten Scans (Port- und Protokollscans) sucht er sich die lohnenswerten Ziele mit Sicherheitslücken aus.
3. Stufe: Im dritten Schritt versucht der Angreifer die Systeme zu kontaktieren, um Anwendungen, Betriebssysteme sowie Versionen und Patch-Level heraus zu bekommen. Zusätzlich versucht er Informationen aus Veröffentlichungen zu sammeln (Jobangebote, Support-Anfragen, etc.) um das System besser kennen zu lernen.
4. Stufe: Jetzt werden gezielt Schwachstellen in der Software ausgenutzt, um ins System einzudingen, denn häufig stellen Programmierer und Administratoren die Funktionalität ihrer Systeme über deren Sicherheit.
5. Stufe: In dieser Phase legt sich der Angreifer einen administrativen Zugang, um das gehackte System auch weiterhin nutzen zu können.
6. Stufe: In der letzten Phase verwischt der Angreifer seine Spuren und schließt oft sogar Sicherheitslücken, um nicht durch andere Hacker „belästigt" zu werden.

Überraschender Weise, finden diese Angriffe nicht vorzugsweise nachts oder an Wochenenden statt, sondern zu den üblichen Bürozeiten. (siehe Symantec Internet Security Threat Reports) Da nicht anzunehmen ist, dass es eine Hackergewerkschaft gibt, die über die Arbeitszeiten wacht, dürfte der vornehmliche Grund sein, dass Angriffe in den üblichen Netzwerkzugriffen der Benutzer untergehen sollen. Tätigkeiten außerhalb der Geschäftszeiten fallen zu sehr auf. So wurde in einem psychiatrischen Krankenhaus IT-Großalarm ausgelöst, weil der Assistenz-Arzt nachts außerhalb der Arbeitszeiten im Internet surfte und Daten verschob. Das vermeintliche Kopieren von geheimen Patientendaten stellte sich nach kurzer Zeit als harmlos heraus, denn der arme Mann war (aus seiner Sicht völlig korrekt) außerhalb der Arbeitszeit in Internet-

Kontaktbörsen unterwegs. Statt Anzeige und fristlose Kündigung gab es nur eine Abmahnung und den Hinweis, dass privates Surfen auch außerhalb der Arbeitszeit verboten sei.
Um unnötige Aufregung und überzogene Maßnahmen zu vermeiden, sollte in erster Linie Ruhe bewahrt werden und schon im Vorfeld eine Art Checkliste erstellt werden, anhand derer entschieden wird, ob es sich um einen digitalen Angriff oder um eine lästige Betriebsstörung handelt. Wenn auch schon etwas antiquiert, so kann doch der RFC2186 zu Rate gezogen werden, der einen guten Überblick über die Symptome eines gehackten Systems gibt: Systemabstürze, neue unbekannte Benutzerkonten mit ungewöhnlichen oder administrativen Rechten, neue Dateien mit auffälligen Namen oder abgewandelten Namen von Systemdateien sowie schlechte Systemleistung und gelöschte oder manipulierte Daten können einen Hinweis geben, ob das System korrumpiert wurde.

Digitale Spurensuche am „lebenden Objekt"

Anders als bei klassischen Verbrechen steht bei der Computer-Forensik das „Opfer" nicht unbegrenzt für forensische Untersuchungen zur Verfügung. Im Fall der Computer-Forensik wird das „Opfer", das gehackte System, umgehend wieder benötigt, um dem produktiven Betrieb nicht noch mehr Schaden zuzufügen. Die Spurensuche muss schnell und ohne weitere Beeinträchtigung des Arbeitsablaufs geschehen. Digitale Spurensuche bewegt sich immer zwischen Beweissicherung und schneller Wiederherstellung der betroffenen Systeme. Zudem muss ein besonderes Augenmerk auf die Persönlichkeitsrechte von Mitarbeitern, Kunden und anderen Partnern gelegt werden. Eine Datenanalyse bringt Forensiker und Ermittler auch immer in Kontakt mit personenbezogenen Daten. Auch im Fall einer Cyber-Straftat dürfen die Datenschutzrichtlinien nicht verletzt werden.

Fundorte digitaler Spuren

Digitale Spuren lassen sich in zwei Gruppen unterteilen: zum einen die technisch vermeidbaren Spuren in Protokolldateien oder im Dateisystem und zum anderen technisch unvermeidbare Spuren. Die letzte Gruppe ist die eigentlich interessante Gruppe. In gelöschten Dateien, Stackframes oder der Master File Table lassen sich Spuren von Systemmanipulationen nachweisen. Weitere Orte von digitalen Spuren sind neben div. Cache-Dateien, Protokolldateien, Datensicherungen, Firewalls, Virenscanner, History, temporäre Dateien, Cookies und Suchmaschinen auch Orte, die auf den ersten Blick nicht unbedingt als digitale Datenspeicher gelten: Überwachungskameras, Geldautomaten und andere Bezahlsysteme, Wiederwahl-Funktion an Telefonen, Abrechnungsdaten, Einlog-Daten des Handys und sogenannte „Wayback-machines" im Internet, die textliche Inhalte von Web-Seite noch auf Jahre hinaus speichern.

Steganographie

Ein Klassiker beim Verstecken von Daten ist u.a. die Steganographie, das Verbergen von Daten, dass Dritten neben den offensichtlichen Informationen des Trägermediums nichts auffällt. Dieses Verfahren ist in nicht-digitaler Form bekannt aus Jugendzeiten, in denen Briefe mit Zitronensaft geschrieben wurden und später mit Wärme sichtbar gemacht wurden. Heute dienen als Träger von geheimen Informationen Bild- und Tondateien, in denen Daten versteckt werden. Simple Verfahren sind zum Beispiel Internetseiten mit schwarzer Schrift auf schwarzem Grund oder das Verstecken von Kinderpornobildern in der Mitte des neuen James-Bond-Filmes. Wichtig dabei ist, dass die Trägerdaten nur minimal

verändert werden und die Aufmerksamkeit des Forensikers von den versteckten Daten abgelenkt wird. Etwas komplexer ist das Verstecken von Daten in Bilddateien. Dazu macht sich der Cyberkriminelle zu Nutzen, dass bei Bildern das Verändern weniger Bits nur geringe Auswirkungen auf das dargestellte Bild hat, und bei einem Bild mit viel Himmelanteil fallen leichte Unschärfen nicht auf. Mit – zum Teil frei verfügbaren Programmen – werden Daten im Bild gespeichert und der entsprechende Empfänger kann diese dann mit demselben Programm wieder sichtbar machen. Es muss nur darauf geachtet werden, dass das Bildformat beibehalten wird und Bilder nicht in andere Formate konvertiert werden, denn sonst gehen die versteckten Daten verloren. Analog gibt es Verfahren, in Audiodateien Daten zu verstecken. Auch da gehen die verstecken Daten im „allgemeinen Rauschen" unter. Der Anteil von Rauschen, das zum Verstecken von Informationen zum Beispiel in einem Bild zur Verfügung steht, kann extrem hoch sein. Viele digitale Bilder halten 32 Bits für jeden Bildpunkt bereit. In jeweils 8 Bit werden die Anteile an Rot, Blau und Grün eines jeden Pixels gespeichert, also sind 24 Bit verbraucht. Wenn pro Pixel nur je ein Bit pro Farbwert zum Verstecken von Informationen verwendet wird, kann man 10 % der Dateigröße dafür verwenden. Das ist eine relativ hohe Ausbeute, um Textnachrichten zu verstecken. Ohne konkrete Hinweise sind diese versteckten Informationen in unseren derzeitigen Datenmengen fast nicht zu finden und führt jeden Ermittler an die Grenzen der digitalen Spurensuche. Zumal Cyberkriminelle nicht netterweise die Daten in ihrer Originalform speichern müssen, sondern Komprimierung und Verschlüsselung noch zusätzlich einsetzen können.

Beweiskraft der digitalen Spuren

Nicht immer lassen sich die digitalen Spuren eindeutig Personen zuordnen. Um ganz sicher zu gehen, müssen physische Spuren hinzugezogen werden.
Sind z.B. im Cache und in der History des Benutzers „Hans" Hinweise auf Kinderpornos zu finden, so kann nicht mit letzter Gewissheit behauptet werden, dass Hans Kinderpornos konsumiert. Das Benutzerkonto „Hans" kann von einer anderen Person verwendet worden sein. Es müssen andere Bewiese sicherstellen, dass das Konto „Hans" nur ausschließlich von seinem rechtmäßigen Benutzer verwendet wurde (z.B. eigenes Konto auf dem Rechner mit komplexem Passwort, kein anderer Bewohner in der Wohnung oder „auf frischer Tat ertappt", d.h. die Webseiten standen zum Zeitpunkt der Durchsuchung offen).
Der große Nachteil von digitalen Spuren ist, dass sie leicht manipuliert werden können. Als erster kommt dafür natürlich der Cyber-Kriminelle selbst in Betracht, der geschickt seine Spuren verwischen oder den Verdacht auf andere lenken kann. Eine weitere Quelle für Manipulation ist – absichtlich oder unabsichtlich – der Ermittler selbst. Durch unbedachtes Handeln, Unwissenheit oder mangelnde Fachkenntnis können Spuren verfälscht werden. Ob Spuren manipuliert wurden oder nicht, lässt sich nicht immer so leicht feststellen. Allerdings haben digitale Spuren auch Vorteile: Sie sind duplizierbar, das heißt, man muss nicht an der Originalfestplatte nach Spuren suchen, sondern kann hierfür ein Abbild verwenden. Anhand eines Vergleichs zwischen Abbild und Original kann so auch der Manipulationsverdacht ausgeräumt werden. Zudem sind digitale Spuren nur schwer zu vernichten (vgl. Festplattenwiederherstellung in forensischen Labors) und entstehen überall im Umgang mit elektronischen Geräten.

Grenzen der digitalen Spurensuche

Der digitalen Spurensuche sind auch Grenzen gesetzt: komplexe Verschlüsselungen machen die Spurensuche oft unmöglich, große Datenmengen

verzögern die Beweisaufnahme und legen Ressourcen für lange Zeit lahm. Zudem erfordern die Vielfalt von Datenträgern und –formaten, sowie volatile Daten ein hohes Maß an Equipment. Digitale Daten sind zudem nicht manipulationsresistent und die örtliche Entfernung der Täter erschwert die Strafverfolgung, da sich die Rechtsordnungen zwischen dem Ort der Tat und dem Ort der Tatausübung unterscheiden können. Es gibt also nicht einen Tatort, wie bei den klassischen Verbrechen.
Wie verwirrend dies werden kann, soll folgendes Beispiel illustrieren: Einem Home-Anwender wird remote das Passwort für die Spielplattform „Second life" ausgespäht. Da unser Home-Anwender ein recht erfolgreicher Spieler war, hat er sich jede Menge Waffen erworden. Der Cyber-Kriminelle logt sich nun mit den falschen Daten ein und übergibt die Waffen an andere Mitspieler, nachdem er sie zuvor bei ebay versteigert hat. Unserem Home-Anwender fehlen nun die Waffen, die er hätte selbst versteigern können. Folglich ist ihm ein finanzieller Schaden durch Betrug entstanden. Und jetzt stellt man sich das Gesicht des Beamten vor, der diese Anzeige aufnehmen muss: in der irrealen Welt von „Second life" wurde eine virtuelle Waffe gestohlen und real bei Ebay versteigert, der kompromittierte PC steht irgendwo in Deutschland und der Täter weit im Osten des Kontinents.

Weiterführende Literatur:

Geschonneck, Alexander: Computer Forensik, 3., aktualisierte Auflage
http://de.wikibooks.org/wiki/Disk_Forensik
http://computer-forensik.org
http://www.rfc-ref.org