



Anoubis – die Security Suite

Sicherheitslösung ermöglicht anwendungsbezogene Zugriffsregeln

Die neue Sicherheits-Suite Anoubis ist eine frei verwendbare Open Source Software. Sie kontrolliert anwendungsbezogene Netzwerk- und Dateizugriffe und schützt vor Manipulationen durch Anwendungen.

Anders als vergleichbare Lösungen bietet Anoubis die Möglichkeit, mit Hilfe eines sicheren File-Systems die Datenintegrität tatsächlich durchzusetzen. Darüber hinaus lässt sich Anoubis über eine grafische Bedienungsoberfläche besonders leicht konfigurieren.

Vielfältige Gefahren durch Missbrauch von Zugriffsrechten

Angriffe auf IT-Systeme und Daten basieren auf dem Missbrauch von Zugriffsrechten. Je großzügiger solche Rechte vergeben werden, desto einfacher werden erfolgreiche Attacken. Im schlimmsten Fall kann z. B. ein Fehler im Browser oder eine unvorsichtige Einstellung in dessen Konfiguration einem Angreifer vollen Zugriff auf alle Daten des Anwenders ermöglichen. Da der Browser mit den Rechten des Benutzers läuft, ist der Zugriff auf dessen Daten nicht weiter beschränkt.

Hier liegt das Grundproblem: Die Rechtevergabe erfolgt benutzerbasiert, d. h. sie weist Benutzern individuelle Zugriffsrechte zu. Einem Programm, das mit den Rechten eines Benutzers läuft, stehen dessen gesamte Rechte zur Verfügung. Dadurch hat eine Anwendung wesentlich mehr Rechte, als sie für ihren eigentlichen Zweck benötigt. Ein Benutzer hat praktisch keine Kontrolle über die Zugriffsrechte der von ihm ausgeführten Anwendungen. Im Falle von Fehlern in Applikationen sind die Benutzerdaten unmittelbar bedroht.

Die Tatsache, dass der Benutzer beim Schutz seiner Daten auf das korrekte Verhalten von Anwendungen angewiesen ist, wirft außerdem die Frage auf, ob die Integrität dieser Anwendungen sichergestellt ist.

Sicherheits-Suite Anoubis für Unix-Systeme

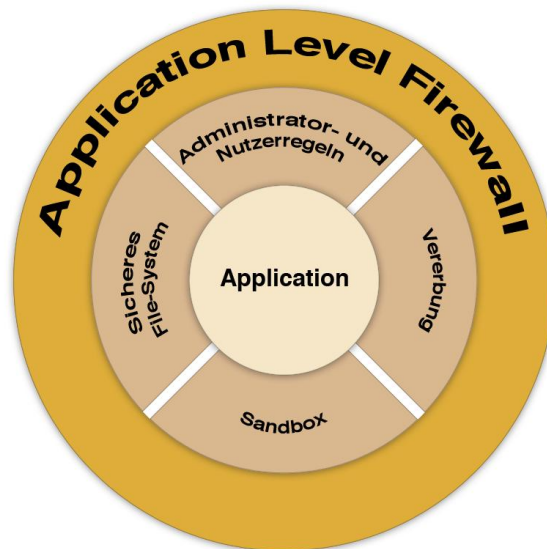
Um dieses Problem zu lösen, müssen neben dem Benutzer auch die Anwendungen in das Rechtesystem einbezogen werden. Das bedeutet konkret: Die Frage, ob der Zugriff auf eine Datei oder eine andere Ressource zugelassen wird, darf nicht mehr ausschließlich vom Nutzer abhängig sein. Die Frage, welche Anwendung den Zugriff durchführt, muss in diese Entscheidung einbezogen werden.

Selbstverständlich muss hierbei sichergestellt sein, dass diese anwendungsbasierte Rechtevergabe die bewährten Schutzmechanismen ergänzt und nicht ersetzt. Der durch Benutzer-, Gruppen- und Zugriffsrechte garantierte grundlegende Schutz soll uneingeschränkt bestehen bleiben.

Anoubis bietet die Lösung: Die Security Suite wurde für Unix-Systeme entwickelt und ermöglicht eine anwendungsbezogene Rechtezuweisung. Sie umfasst eine Application Level Firewall, eine Sandbox und ein sicheres File-System. Darüber hinaus bietet sie eine



grafische Oberfläche, die speziell für eine Bedienung durch unerfahrene Anwender ausgelegt ist.



Die Komponenten von Anoubis im Überblick

- **Application Level Firewall**

Mit der Application Level Firewall kann beispielsweise dem Acrobat-Reader der Zugriff auf das Netzwerk vollständig untersagt werden, während der Web-Browser auf ausgewählte Dienste (HTTP, HTTPS, DNS) zugreifen darf.

Im Unterschied zu einer externen Firewall erkennt die Application Level Firewall, welche Applikation auf das Netzwerk zugreifen möchte. Durch den gezielten Einsatz von Regeln können die Netzwerk-Zugriffe in Abhängigkeit der einzelnen Anwendungen feingranular überwacht werden. Unerwünschte Zugriffe werden bemerkt und lassen sich somit unterbinden.

So können unter anderem Trojaner, die man versehentlich über einen USB-Stick auf das System kopiert hat, keine Verbindung zum Internet herstellen, um etwa das Adressbuch des Benutzers an Spammer zu schicken. Darüber hinaus kann der Benutzer bei einem solchen Vorgang alarmiert werden und somit den Trojaner aufspüren und entfernen.

- **Sandbox**

Die Maßnahmen einer Firewall helfen nicht, wenn Schadsoftware einen Rechner durch Netzwerk-Zugriffe erreicht, die zum normalen Verhalten des Programms gehören. Diese müssen erlaubt sein, damit das Programm reibungslos funktioniert.

Hier hilft Anoubis durch Regeln, die den Zugriff von Programmen auf das Dateisystem einschränken. Für einen Web-Browser genügt es z. B., wenn er seine eige-



ne Konfiguration schreiben kann. Eventuell wird noch Schreibzugriff für einen Download-Bereich benötigt. Im gesamten Rest des Dateisystems genügt lesender Zugriff. Mit Hilfe von Anoubis kann dies sichergestellt werden. So wird verhindert, dass ein Programm versehentlich oder in Folge eines Angriffs Änderungen an Dateien außerhalb eines genau eingegrenzten Bereichs vornimmt.

Anoubis unterscheidet hier nicht nur zwischen lesenden und schreibenden Zugriffen. Auch das Ausführen einer anderen Anwendung gilt als Zugriff und kann gesondert geregelt werden.

- **Sicheres File-System zur Integritätsprüfung**

Anoubis bietet die Möglichkeit, durch Verwendung von Prüfsummen die Integrität des Systems zu überwachen und mit Policies durchzusetzen.

Mit einem komfortablen Datei-Browser kann jederzeit überprüft werden, ob der Inhalt von Dateien noch mit den früher hinterlegten Prüfsummen übereinstimmt. Diese Prüfung kann unabhängig von einem konkreten Zugriff auf eine Datei durchgeführt werden.

Zur Durchsetzung der Datenintegrität kann mit Hilfe von Policies genau definiert werden, welche Rechte bestimmten Dateien bei abweichender Prüfsumme entzogen werden sollen. Kommt es zu einer Abweichung zur hinterlegten Prüfsumme, dann darf eine verdächtige Anwendung beispielsweise nicht mehr ausgeführt werden oder sie verliert ihre Schreibrechte.

- **Administrator- und Nutzerregeln**

Der Administrator kann seinen Nutzern verbindliche Regeln vorgeben. Dieser Regelsatz kann von den Nutzern lediglich weiter eingeschränkt werden. Es ist den Nutzern jedoch nicht möglich, Einschränkungen des Administrators durch eigene Regeln aufzuheben.

Darüber hinaus kann jeder Nutzer selbständig Zugriffsregeln festlegen. Diese gelten nur für die von diesem Nutzer ausgeführten Programme und können von ihm selbst jederzeit angepasst, ergänzt oder verändert werden.

- **Dialog zur Konfiguration**

Für Nutzer und auch Administratoren ist es schwierig, individuelle Regeln für alle Anwendungen zu formulieren. Denn Programme benötigen für den ganz normalen Betrieb zumindest lesenden Zugriff auf eine Vielzahl von Dateien, wie z. B. Bibliotheken oder temporäre Dateien. Welche genau das sind, ist aber normalerweise nicht oder nur sehr vage bekannt.

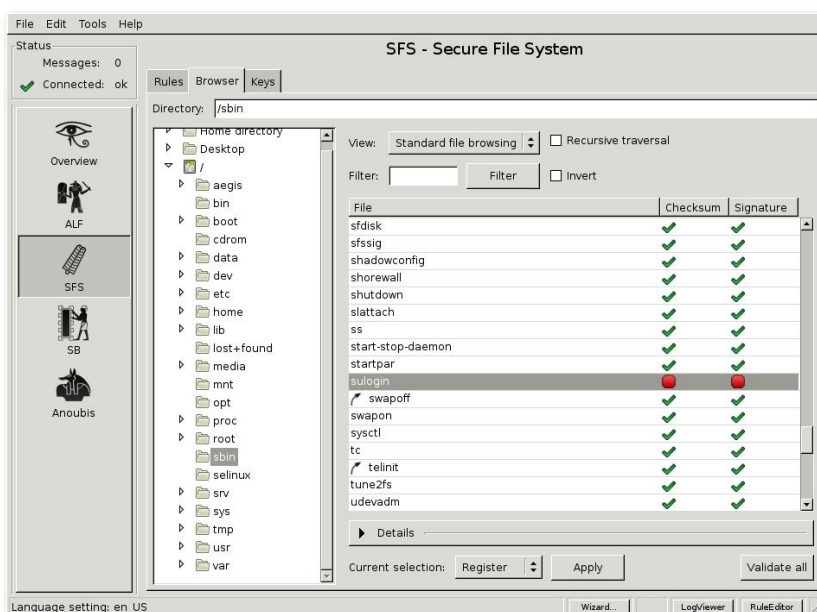
Anoubis führt mit einem Dialog durch die Erstellung von geeigneten Regelsätzen. Es wird also ein Zugriff nicht sofort erlaubt oder verboten, sondern der Nutzer kann über einen Dialog entscheiden, wie in diesem Fall weiter zu verfahren ist. Mit der Entscheidung über den konkreten Zugriff können dabei automatisch Regeln für



diesen und ähnliche zukünftige Zugriffe angelegt werden. Dazu werden dem Nutzer von Anoubis konkrete Vorschläge unterbreitet.

- **Benutzerfreundliche Bedienungsoberfläche**

Für die Konfiguration bietet Anoubis eine komfortable grafische Benutzeroberfläche. Mit einem einfach zu bedienenden Regeleditor werden Regelsätze erstellt und geändert. Darüber hinaus können Regelsätze für einzelne Anwendungen mit Hilfe eines Regel-Wizards erzeugt werden. Dadurch sind auch weniger erfahrene Nutzer in der Lage, einen sinnvollen initialen Regelsatz für eine Anwendung zu erstellen.



Datei-Browser für das sichere File-System von Anoubis

Auch die Verwaltung und Überprüfung von hinterlegten Prüfsummen kann mit Hilfe eines Dateisystembrowsers in der grafischen Benutzeroberfläche durchgeführt werden.

- **Verschiedene Profile**

Um verschiedenen Einsatzumgebungen eines Rechners gerecht werden zu können, bietet Anoubis die Möglichkeit, verschiedene Profile zu verwalten. Über die grafische Benutzeroberfläche kann auf einfache Weise zwischen den einzelnen Profilen gewechselt werden. So kann etwa ein Profil für die Arbeit im Intranet am Arbeitsplatz und eines für die Heimarbeit eingerichtet werden. Je nach aktueller Anforderung wird dann das passende Profil vom Nutzer gewählt.



- **Vererbung**

Eine bisher noch nicht betrachtete Frage ist, was mit den Regeln einer Anwendung geschieht, wenn diese eine andere Anwendung ausführt. Dies ist beispielsweise der Fall, wenn ein Browser einen PDF-Reader startet. Grundsätzlich werden in einem solchen Fall die Regeln der ausführenden Anwendung (im Beispiel die des Browsers) beibehalten. Dies verhindert, dass eine Anwendung ihre Regeln einfach durch die Ausführung einer anderen Anwendung umgehen kann. Für ausgewählte Anwendungen kann aber festgelegt werden, dass diese nicht die Regeln der aufrufenden Anwendung übernehmen. Stattdessen kommen dann speziell für die aufgerufene Anwendung definierte Regeln zum Einsatz. So kann es sinnvoll sein, einem im Browser gestarteten PDF-Reader Schreibrechte zuzuweisen, um PDF-Dateien speichern zu können.

- **Playground**

Im Normalfall führen Prozesse im Dateisystem Schreib- und Leserechte aus. Dies kann jedoch bei bestimmten Anwendungen wie z. B. bei einem Internet-Browser unerwünscht sein, da ansonsten infizierte Dateien ins System gelangen können. Anoubis wird daher zukünftig die Möglichkeit bieten, Anwendungen in abgesicherten Bereichen – so genannten Playgrounds – zu starten.

Wird eine Anwendung in einem Playground ausgeführt, kann sie keine Änderungen verursachen, die Auswirkungen auf das Dateisystem haben. Wird z. B. ein Browser in einem Playground verwendet, hinterlässt er demnach keinerlei Spuren außerhalb des gesicherten Bereichs.

Sollen Daten aus einem Playground ins Dateisystem übertragen werden, dann muss der Benutzer diesen Prozess ausdrücklich anstoßen. Dabei lässt sich ein Datentransfer aus dem Playground in das Dateisystem je nach Bedarf z. B. durch einen Virensch scanner absichern. Darüber hinaus kann der Anwender am Ende einer Session entscheiden, ob Daten innerhalb des Playgrounds behalten oder gelöscht werden sollen.

Anwendungsszenarien

Für folgende Anwendungsfälle ist Anoubis konzipiert:

Ein Benutzer hat einen Laptop, den er in verschiedenen Umgebungen einsetzt.

Büro: Bei der Arbeit im Büro braucht die Policy auf dem Laptop nicht besonders streng zu sein, da der Netzwerk-Administrator starke Sicherheitsmaßnahmen implementiert hat und der Benutzer ohne große Einschränkung die internen Dienste nutzen können soll. Zugriffe auf alle möglichen Dienste sind erlaubt und es dürfen sogar eigene Dienste angeboten werden.

Zu Hause: Hier gibt es keine externe Firewall, die den Laptop schützen könnte. Deshalb erlaubt hier eine Home-Policy keine Zugriffe von Außen und nur bestimmte Applikationen dürfen Verbindungen ins Internet öffnen. Beispielsweise darf nur der Browser HTTP/S-Ver-



bindungen öffnen, der VPN Client eine Verbindung ins Firmennetz herstellen und der Virens Scanner Updates ziehen.

Fremdes WLAN: Will der Benutzer auf dem Flughafen über ein WLAN arbeiten, muss die eingesetzte Policy sehr restriktiv sein. Nur der Browser darf über HTTP in das Internet, der Mail Client nur über verschlüsselte Kanäle (S/POP und S/HTML) zum Mail Host, der VPN-Tunnel kann nur zur Gegenstelle in der Firma aufgebaut werden. Alle anderen Verbindungen werden geblockt.

Durch die einfache Auswahl der geeigneten Sicherheits-Policy im GUI kann der Benutzer in jeder Umgebung seinen Aufgaben ungestört nachkommen und ist trotzdem überall maximal geschützt.

Auch an Arbeitsplätzen, an denen sensitive Informationen verarbeitet werden, wie z. B. personenbezogene Daten in Krankenhäusern, ist eine Absicherung durch Anoubis sinnvoll. Um den Abfluss von Daten zu verhindern, kann z. B. einer Fachanwendung mit Zugriff auf sensitive Informationen untersagt werden, Verbindungen über das eigene Netz hinaus aufzubauen. Programmen, die Internetverbindungen benötigen, wird dagegen der Zugriff auf die sensitiven Daten verboten – obwohl der Benutzer prinzipiell die Daten lesen und sogar ändern dürfte.

Diese Policies können zentral vom Systemadministrator vorgegeben und von den Benutzern nicht aufgehoben oder umgangen werden.

Fazit

Mit Anoubis können Benutzer durch anwendungsbezogene Zugriffsrechte den Schutz ihrer Unix-Rechner erhöhen. Die Lösung bietet ein auf höchste Sicherheitsanforderungen zugeschnittenes File-System und eine benutzerfreundliche Oberfläche.

Als Open Source Software ist Anoubis frei verwendbar und kann unter www.anoubis.org inklusive Informationen zur Installation und zum Betrieb heruntergeladen werden.

Anoubis-WP-0410-1-D

So erreichen Sie uns:

GeNUA mbH • Domagkstraße 7 • 85551 Kirchheim b. München
tel +49 (89) 99 19 50-0 • fax +49 (89) 99 19 50-999 • info@genua.de • www.genua.de