



Anoubis begrenzt Zugriffsrechte für mehr Sicherheit

Neue Open Source-Sicherheitslösung für UnixClients

Angriffe auf IT-Systeme und Daten basieren auf dem Missbrauch von Zugriffsrechten. Je großzügiger solche Rechte vergeben werden, desto einfacher werden erfolgreiche Attacken. Problematisch ist deshalb die gängige Praxis, allen Anwendungen auf einem Client pauschal alle Zugriffsrechte des eingeloggtten Benutzers einzuräumen.

Typische Beispiele: Ein Anwender surft mit einem gängigen Internet-Browser und besucht eine Seite, die einen Verweis auf ein Skript enthält. Der Browser lädt dieses Skript herunter und führt es aus. Das Skript sammelt verfügbare Daten ein und sendet diese über das Internet an einen fremden Server.

Im schlimmsten Fall kann 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 Benutzer läuft, ist der Zugriff auf dessen Daten nicht weiter beschränkt.

Aber nicht nur der Browser eröffnet Möglichkeiten für einen Angriff. Genauso gut kann ein modernes Textverarbeitungssystem wie z. B. OpenOffice missbraucht werden, indem ein Dokument an einen Anwender geschickt wird, das ein böses Makro enthält. Solche Makros können, genau wie Aktive Inhalte, Code auf dem Rechner ausführen. Öffnet der Benutzer dieses Dokument, wird das Makro geladen und ausgeführt. Dass der Benutzer auf die Existenz eines Makros hingewiesen wird und die Ausführung bestätigen muss, ist kein echter Schutz, da Makros verbreitet sind und der Benutzer solche Hinweise oft schlichtweg ignoriert.

Auch diese Makros verfügen über alle Rechte des Benutzers. Das heißt, das Makro ist in der Lage, persönliche Daten des Benutzers zu lesen, an Unbefugte zu schicken oder im Zweifelsfall sogar zu verändern. „BadBunny“ [1] ist ein Proof of Concept für einen Makro-Virus, der eine solche Schwachstelle aufzeigt, jedoch keine echte Schadfunktion beinhaltet.

Diese Beispiele zeigen ein Grundproblem bei der Rechtevergabe: Die Zugriffsrechte schützen das System vor den Benutzern und isolieren die einzelnen Benutzer untereinander. Eine Applikation, die mit den Rechten eines Benutzers läuft, ist aber nicht weiter eingeschränkt. Ihr stehen sämtliche Rechte dieses Benutzers selbst offen. Dadurch hat eine Anwendung wesentlich mehr Rechte, als sie für ihren eigentlichen Zweck benötigt.

Ein Anwender hat praktisch keine Kontrolle über die Zugriffsrechte der von ihm ausgeführten Applikationen und muss sich auf deren korrektes Verhalten und Design verlassen. Im Falle von Fehlern in Applikationen sind die Nutzerdaten unmittelbar bedroht.

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



Lösungsansatz

Um diese Probleme 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 nur vom Nutzer allein abhängig sein. Die Frage, welche Anwendung den Zugriff durchführt, muss in diese Entscheidung mit einbezogen werden.

Auf diese Weise kann zum Beispiel der Zugriff einer Office-Anwendung auf Dateien unterhalb des Heimatverzeichnisses eines Nutzers eingeschränkt werden. Die Office Suite hat dann auf andere Daten keinen Zugriff mehr, obwohl der Nutzer selbst auf diese Daten zugreifen dürfte.

Selbstverständlich muss hierbei sichergestellt sein, dass diese anwendungsbasierten Zugriffsregeln die bewährten Mechanismen zum Zugriffsschutz ergänzen und nicht ersetzen. Der durch Benutzer-, Gruppen- und Zugriffsrechte garantierte grundlegende Schutz soll uneingeschränkt bestehen bleiben.

Sicherheits-Suite Anoubis für Unix-Clients

Für Unix-Clients hat das IT-Sicherheitsunternehmen GeNUA mit Anoubis eine Lösung entwickelt, die eine anwendungsbezogene Rechtezuweisung ermöglicht. Die Sicherheits-Suite umfasst eine Application Level Firewall, eine Sandbox und ein sicheres File-System und bietet ein GUI, das speziell für die Bedienung durch unerfahrene Anwender ausgelegt ist. Anoubis ist eine Open Source-Lösung für Linux- und OpenBSD-Betriebssysteme und wurde von GeNUA im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelt.

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 sich 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

Diese Beschränkungen helfen allerdings nicht, wenn die Schadsoftware den 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 eigene 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

Darüber hinaus bietet Anoubis die Möglichkeit, die Integrität des Systems durch die Verwendung von Prüfsummen sicherzustellen. Dazu können beim Anoubis-System Prüfsummen hinterlegt werden. Es kommen SHA-256 Hashes (<http://tools.ietf.org/html/rfc3174>) zum Einsatz. Diese können auf zweierlei Arten zur Sicherstellung der Integrität des Systems eingesetzt werden:

Mit Hilfe eines komfortablen Datei-Browsers 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.

Zudem kann für bestimmte Bereiche des Dateisystems vorgegeben werden, dass nur auf Dateien zugegriffen werden darf, wenn für diese eine Prüfsumme hinterlegt ist und der aktuelle Inhalt zu dieser Prüfsumme passt.

Auf diese Weise kann z. B. für ausführbare Dateien sichergestellt werden, dass diese nicht manipuliert sind.

Nutzer- und Administratorregeln

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

Der Administrator kann darüber hinaus seinen Nutzern verbindlich 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.

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 zum Beispiel Bibliotheken oder temporäre Dateien. Welche dies genau sind, ist aber normalerweise nicht oder nur sehr vage bekannt.

Anoubis unterstützt Anwender und Administratoren bei der Erstellung von geeigneten Regelsätzen durch einen Dialog. 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.

Grafische Oberfläche

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 Applikationen 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.

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 eines Prozesses geschieht, wenn dieser ein anderes Programm ausführt. Grundsätzlich werden in einem solchen Fall die Regeln des ausführenden Programms beibehalten. Dies verhindert, dass eine Anwendung ihre Regeln einfach durch die Ausführung eines anderen Programms umgehen kann. Für ausgewählte Anwendungen kann aber festgelegt werden dass diese nicht die Regeln der aufrufenden Anwendung übernimmt. Stattdessen kommen dann speziell für diese Anwendung definierte Regeln zum Einsatz.

Technische Realisierung

Realisiert wird Anoubis unter Linux auf Basis der LSM-Schnittstelle. Diese wurde eigens für die Implementierung von speziellen Sicherheitsfunktionen geschaffen und wird auch von anderen Sicherheitsprodukten, wie z. B. SELinux, genutzt. Ereignisse, die aus der Sicht von Anoubis einer genaueren Prüfung bedürfen, werden mit Hilfe dieser Schnittstelle registriert und über eine weitere, eigens geschaffene Schnittstelle an einen Daemon-Prozess weitergeleitet.

Dieser trifft entweder selbst anhand der konfigurierten Regeln eine Entscheidung oder leitet das Ereignis an ein zur Entscheidung berechtigtes User-Interface weiter. Bis die Entscheidung endgültig getroffen ist, wird der betroffene Prozess blockiert.



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.

Zuhause: 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 Verbindungen 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 Daten 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.

Ausblick

Mit der veröffentlichten Version von Anoubis können Benutzer den Schutz ihrer Unix-Rechner erhöhen. Keine Grenzen setzt Anoubis derzeit einem Benutzer mit root-Rechten. Dieser ist jederzeit in der Lage, das Anoubis System auszuhebeln. Um diese Lücke zu schließen, sind Mechanismen erforderlich, die den Kernel und den Anoubis-Daemon auf ihre Integrität hin überprüfen. Dies soll zu einem späteren Zeitpunkt durch Verwendung kryptographischer Token oder durch auf dem Rechner vorhandenen TPM-Chips (Trusted Platform Module) gewährleistet werden.

Diese Mechanismen können dann auch für eine Dateiverschlüsselung und sichere Login-Verfahren verwendet werden.



In Planung ist auch ein „Playground“. Hier wird eine Applikation eingesperrt und hat zwar eine transparente Sicht auf alle ihr erlaubten Systemdaten, aber alle Schreibzugriffe finden in einem isolierten Bereich statt. Wird die Applikation beendet, wird dieser isolierte Bereich gelöscht und das System ist wieder in dem Zustand, in dem es vorher war. Einzelne Dateien können durch eine mit Virenscannern geschützte Schleuse ins Produktivsystem übernommen werden.

Darüber hinaus ist eine verteilte Authentisierung angedacht. So sollen sich Anoubis-Instanzen auf verschiedenen Rechnern gegenseitig authentisieren können und damit gewährleisten, dass Applikationen netzweit auf vertrauenswürdige Ressourcen und Daten zugreifen können. Beispielsweise kann der Web-Browser so eingeschränkt werden, dass er Daten nur von einem durch Anoubis geschützten Webserver erhalten darf.

Für solche Anoubis-Netze soll auch ein zentrales Management ermöglicht werden, damit ein Administrator ganz komfortabel eine große Anzahl von Anoubis-Systemen auf einem einheitlichen Stand halten kann.

*****|Infokasten*****

Anwendungsfälle:

- Application Level Firewall: Nur der eingetragene Web-Browser und der Virenscanner dürfen auf externe Webserver zugreifen (Port 80,443/TCP), allen anderen Programmen wird dieser Zugriff verweigert. Andere Applikationen, die z. B. via Internet Updates abrufen möchten, werden dadurch geblockt, obwohl sie dies auch über Port 80/TCP versuchen.
- Profile: Der Webbrowser darf im Home-Profil auf das Internet (Port 80,443/TCP) zugreifen. In einem speziellen Büro-Profil darf er nur auf den internen Proxy zugreifen, alle anderen Verbindungen werden geblockt. Die Profile können im GUI einfach gewechselt werden.
- Kontext-Wechsel: Der PDF-Viewer darf – direkt gestartet – nicht auf das Internet zugreifen (Port 80/443/TCP). Das verhindert, dass er automatisch nach neuen Updates fragt. Wenn er aber vom Web-Browser aufgerufen wird, darf er die entsprechende PDF-Datei herunterladen und im Web-Browser anzeigen. Diese Option ist für jede Applikation separat konfigurierbar.
- Sandbox: Der Web-Browser darf nur in das Home-Verzeichnis des Benutzers schreiben. Wenn er versucht, an anderer Stelle eine Datei zu schreiben, wird der Benutzer um Erlaubnis gefragt. Der Benutzer kann dann z. B. einstellen, dass der Web-Browser ab jetzt in ein unkritisches Verzeichnis wie z. B. /tmp immer schreiben darf und in ein Programmverzeichnis wie /usr/local/bin nur dieses eine Mal.
- Sicheres Filesystem: Bei einem Update wurde die allgemeine SSH-Konfigurationsdatei überschrieben. Dies würde der Benutzer im Normalfall nicht bemerken. Da der Benutzer die Konfigurationsdatei vorher mit einer signierten Prüfsumme



versehen hatte, wird der Lesezugriff darauf beim Start einer neuen SSH-Verbindung geblockt und der Vorgang gemeldet. Der Benutzer kann nun geeignet darauf reagieren.

Als Open Source Software ist Anoubis frei verwendbar und kann hier inklusive Informationen zur Installation und zum Betrieb heruntergeladen werden:

www.anoubis.org

[1]

<http://arstechnica.COM/news.ars/post/20070522-cross-platform-openoffice-macro-virus-revealed.html>

von Joachim Ayasse und Dr. Christian Ehrhardt, beide Auftragsentwicklung GeNUA mbH