eco Kompetenzgruppe Sicherheit

Informationen zur Sicherheit im Netz

Schutz vor giftigen Webservern

Verband der deutschen Internetwirtschaft e.V.

Serverbetreiber

eco Kompetenzgruppe Sicherheit

Schutz vor Malware im Web ist ein besonders wichtiges Thema der Internet-Sicherheit, denn virenverseuchte, giftige Webserver sorgen für die meisten neuen Infektionen mit Viren, Trojanern und anderen Schädlingen. Giftige Webserver lassen sich verhindern, wenn die Betreiber von Servern und Websites umsichtig vorgehen und einige Regeln beachten. Auch der Internetnutzer kann sich beim Browsen geeignet schützen. Die eco Kompetenzgruppe Sicherheit hat neun Empfehlungen zusammengestellt, wie Serverbetreiber, Websitebetreiber und Nutzer gemeinsam der Verbreitung von Schadsoftware durch giftige Webserver Einhalt gebieten können.

Server härten

Die Sicherheit eines Systems zu erhöhen ist Ziel jedes Administrators. Dazu sollten Updates und Patches zeitnah eingespielt werden. Das Sammeln von Informationen über kritische Sicherheitslücken ist hierzu Voraussetzung und kann durch aktives Verfolgen von Newstickern oder Mailinglisten zum entsprechenden Thema gewährleistet werden. Als weiteres Mittel dient die Verwendung von nur geringstmöglichen Systemrechten zur Ausführung von Diensten – „principle of least privilege“ –, alle nicht benötigten Dienste sollten abgeschaltet werden. Die elementarste Maßnahme ist das Mitschreiben und Auswerten von Logdateien, hierauf lassen sich weitere Sicherheitsprozesse wie die Durchführung von Integritätsprüfungen – „hostbased intrusion detection system“ – aufsetzen.

Firewall vorschalten

Zur sicheren Verwaltung von Verbindungen von und zu einem System sollte man eine Firewall einsetzen. Nicht benötigte Serverdienste sollten abgeschaltet und für die verbleibenden nur geringstmögliche Systemrechte verwendet werden. Eine zusätzliche Maßnahme ist die Verwendung sicherer Authentifizierungsverfahren für Netzwerkdienste, indem man z. B. für die Mailabholung nur „IMAP over SSL“ erlaubt. Ein weiterer Aspekt ist die größtmögliche Einschränkung von sowohl eingehenden als auch ausgehenden Netzwerkverbindungen, man blockt also standardmäßig alle Verbindungen und öffnet nur die benötigten Ports für die Hosts, die den Zugriff benötigen. Durch Mitschreiben und Auswerten von Logdateien können Sicherheitslücken in der Firewall entdeckt werden.

Auf Schadsoftware prüfen

Um ein permanent sauberes und von Schadsoftware freies System zu haben, muss man einige Dinge beachten. Hierzu gehört, Dateien regelmäßig auf Fremdmodifikationen zu prüfen; eine Methode hierfür ist das Vergleichen von Hashwerten der Dateien. Es gibt diverse frei verfügbare Tools, die ein automatisches Aufspüren von Malware und infizierten Teilbereichen des Systems erlauben. Für Linuxdistributionen gehören hierzu „rkhunter“ zum Aufspüren von Rootkits und „ClamAV“, ein kostenloser Virenscanner. Auch die aktive Suche nach unbekannten Prozessen sollte regelmäßig z. B. anhand von Logdateianalysen durchgeführt werden. So kann man Schadsoftware erkennen und den Verbindungsaufbau z. B. zu einem Command & Control Center verhindern.

Sichere Softwarearchitektur und sichere Programmierung

Zur Beurteilung von Sicherheit bei Software stehen sowohl die Common Criteria (CC) und eine entsprechende Zertifizierungskette als auch ISO EN 61508 und davon abhängige weitere internationale Normen bei bestimmten Aufgabenstellungen, z. B. Kraftwerkssteuerungen, zur Verfügung. Letztere orientieren sich meist an der vollständigen Anlagenkomplexität und stellen Anforderungskataloge gemäß SIL 1-4 auf. Im kommerziellen Internetgebrauch ist CC EAL 4 zumeist die höchste Stufe, für die ein Investor bereit ist zu zahlen. Höhere Qualifizierungen sind nur mit speziellen und genau dazu evaluierten Entwicklungstechniken zu erlangen, aufgrund der damit verbundenen höheren Kosten sind sie fast ausschließlich im Umfeld von Prozessleitsystemen und oberen Geheimhaltungsstufen anzutreffen. Detaillierte Planung und sorgfältige Prüfung von sicherheitsrelevanten Aspekten einer Software stehen also notwendigerweise bereits zu Beginn neben der Funktionalität im Zentrum jeder Softwareentwicklung, die während der Nutzungsphase bestimmte Sicherheiten versprechen und halten soll. Ein nachträgliches Hinzufügen oder Implementieren von Sicherheit ist normalerweise unmöglich und in jedem Falle unverhältnismäßig; unsichere Betriebssysteme verhindern wirksame Sicherheit a priori.

Fremdprogramme aktuell halten

Auch – oder gerade – Webserver bieten nur dann sowohl für den Betreiber des Webservers als auch den Nutzer bzw. Kunden sicheren Schutz vor Schadsoftware, wenn die verwendete Software immer auf dem aktuellen Stand ist. Der Fachausdruck hierfür lautet patchen, englisch für flicken. Hinter einem Patch verbirgt sich ein vom Softwarehersteller bereitgestelltes größeres oder kleineres Softwarepaket, das bekannte Fehler oder Schwachstellen in der verwendeten Software schließen soll. Diese Fehler werden von Hackern genutzt, um ihre Schadsoftware auf dem Server einzuspielen.Während sich im Windows-Umfeld die verwendeten Rechner für ein automatisiertes Patchen konfigurieren lassen, ist dies bei Software für Webserver eher selten zu finden. Für den sicheren und stabilen Betrieb des Servers ist es daher

notwendig, für jede auf dem System verwendete Software regelmäßig auf den Webseiten des Herstellers bzw. Distributors nach neuen Patches bzw. Updates zu schauen und diese kurzfristig in das Produktivsystem einzuspielen. Wichtig ist dabei, wirklich alle verwendeten Softwareprodukte im Blick zu halten.

Web Application Firewall vorschalten

Eine Web Application Firewall (WAF) ist ein besonderes Firewall-Element, das zwischen Clients (Browsern) und Servern (Web-Anwendungen) die Kommunikation zum Schutz von Web-Anwendungen überwacht und reglementiert. Auf der Anwendungsebene werden der Kommunikationsablauf und die Inhalte des HTTP-Protokolls intensiv nach Angriffen analysiert. Falls ein WAF Angriffe über schädliche HTTP-Request und -Response erkennt, wird die Kommunikation blockiert, um einen Schaden zu verhindern. Angriffe, die typischerweise von einer WAF verhindert werden können, sind z. B. Cross-Site Scripting (XSS), SQL Injection, Command Injection, Hidden Field Tampering, Parameter Tampering, Cookie Poisoning usw. Außerdem können einige WAFs auch die als Antwort ausgelieferten Web-Seiten auf sensible Daten hin untersuchen, die nicht nach außen gelangen sollen (Verhinderung von Information-Leakage) oder eine vorgegebene Verschlüsselungsstärke der SSL/TLS-Layer erzwingen. Eine WAF kann integrativer Bestandteil einer Netzfirewall, ein separates Gateway oder ein Modul auf dem Webserver sein. Durch eine gut konfigurierte WAF kann die Sicherheit von Web-Applikationen erheblich verbessert werden. Ein besonderer Nutzen von WAFs liegt in der nachträglichen Absicherung bereits produktiver Web-Anwendungen, die ohne Änderung der Anwendung selbst und mit vertretbarem Aufwand umgesetzt werden kann.

Virenschutz aktuell halten

Ein Virenschutz ist heutzutage unabdingbar beim Umgang mit dem Thema Internetsicherheit. Schon Mitte der achtziger Jahre wurden die ersten MS-DOS-Viren entwickelt und verbreitet. Mittlerweile existieren im Bereich Malware neben Viren noch weitere Schädlingstypen, wie z. B. Würmer, Trojaner und Bots. Da täglich eine Vielzahl von neuen Schädlingen in Umlauf gelangt, ist nicht nur die Installation, sondern auch die regelmäßige Aktualisierung eines Virenscanners, insbesondere der Signaturen erforderlich. Dabei ist die automatische Update-Funktion wichtig für die Aktualisierung. Bei der Auswahl des Update-Intervalls für die Signaturen sollte immer der kleinstmögliche Zeitabstand gewählt werden. Bei den kommerziellen Antivirenprodukten sind die Zeitabstände für die Signaturaktualisierung kürzer (stündlich) als bei den Freeware-Produkten (täglich). Darüber hinaus ist der On-Access-Modus empfehlenswert, da der Virenscanner hierbei im Hintergrund aktiv bleibt. Diese Einstellungen sind nach einer Installation in der Regel automatisch aktiviert. Ein kompletter Scan des gesamten PCs sollte regelmäßig durchgeführt werden, um potenzielle Gefahren frühzeitig erkennen zu können. Zusätzlich zu einem installierten Virenscanner können Online-Scanner eingesetzt werden, wobei der PC aus einem Browser heraus gescannt wird.

Browser und wichtige Programme aktuell halten

Statistisch betrachtet weist jede Software zwei bis drei Fehler je 1000 Zeilen Programmcode auf. 30% der Fehler beinhalten Angriffsmöglichkeiten. Die Anzahl der Exploits, die Sicherheitslücken in Browser und Programmen ausnutzen, nimmt dadurch täglich zu. In der Regel steht Exploit-Code spätestens 30 Tage nach Veröffentlichung eines Patches zur Verfügung. Deshalb ist es notwendig, dass Programme und Browser stetig aktualisiert werden. Durch die Aktualisierung kann der Anwender proaktiv das Infektionsrisiko minimieren. Wenn es möglich ist, sollte die automatische Update-Funktion eingeschaltet werden. Durch ein mangelndes Verantwortungsbewusstsein des Anwenders hinsichtlich Sicherheit gehen die Hersteller zur Zeit dazu über, ihre Anwendungen automatisch im Hintergrund zu aktualisieren. Heutzutage umfassen Webseiten zunehmend dynamische

Funktionen, die über clientseitige Technologien wie JavaScript, Java, Adobe Flash oder Ajax bereitgestellt werden. Dies bietet dem Angreifer Möglichkeiten für einen Drive-by-Download. Um das Risiko hierfür zu reduzieren, sollte stets die neueste Browserversion inklusive Plug-ins installiert werden.

URL-Filter zwischenschalten

Wenn ein Webserver erst einmal von einem Schadprogramm befallen ist, greift nur noch der Schutz, der auf Seiten des Internet-Nutzers eingerichtet ist. Dazu gehört auch der URL-Filter, der beim Ansteuern einer beliebigen URL, beispielsweise einer Webseite prüft, ob diese Seite zu einer unerwünschten oder schädlichen Kategorie gehört. Wenn die Seite auf dem Index steht, wird der Zugriff und damit die Gefährdung verhindert. Dies dient außerdem der Verbesserung von Produktivität und Compliance, indem nur der Zugriff auf Webseiten zugelassen wird, die im Einklang mit der konkreten Geschäftstätigkeit stehen. Gute URL-Filter zeichnen sich durch die vollautomatische Auswertung verschiedener Informationsquellen aus, etwa der Auswertung von Links in Spam- und Virenmails. Wichtig ist auch, möglichst viele Webseiten im URL-Filter zu klassifizieren und dabei Deep Links einzubeziehen, denn auch bei einer „sauberen“ Homepage können natürlich Viren oder andere Schädlinge tiefer im Webangebot versteckt sein. Da der Schutz gegen eine neue Verseuchung möglichst schnell aktiv werden muss, ist ein Cloud-basierter Mechanismus für den URL-Filter von Vorteil. Einfache URL-Filter sind bereits in modernen Browser-Versionen aktivierbar. Für flexible, zentral administrierbare Lösungen gibt es Business-Angebote am Markt, und zwar sowohl als Software-Pakete wie auch als Managed Security Service mit komplettem Betrieb.

Autoren und Ziele

- **Dr. Kurt Brand,** Pallas GmbH
- **Stefan Haunß,** 1&1 Mail & Media GmbH
- **Johannes Hubertz,** hubertz-it-consulting GmbH
- **Prof. Norbert Pohlmann,** FH Gelsenkirchen
- **Markus Schaffrin,** eco e. V.
- **Rolf Schnitzler,** Unitymedia NRW GmbH

Die eco Kompetenzgruppe „Sicherheit“ beschäftigt sich mit allen Fragestellungen rund um die Sicherheit der (IT-) Infrastrukturen der deutschen Internetwirtschaft. Die Themen reichen dabei von der personellen und organisatorischen Sicherheit über den Schutz von IT- Systemen (Servern, Netzen), die Sicherheit mobiler Kommunikationstechnik (Pads, Smartphones, WLANs) bis hin zu Fragen des Sicherheitsmanagements und der Mitarbeitersensibilisierung.

Ziele der Kompetenzgruppe Sicherheit sind:

- die Erarbeitung von Positionspapieren
- die Bearbeitung zentraler Fragestellungen der IT-Sicherheit
- gemeinsame Veranstaltungen mit anderen Kompetenzgruppen oder Veranstaltern, der fachübergreifenden Bedeutung der Thematik entsprechend
- die Vernetzung der Kompetenzgruppe mit Aktivitäten anderer Verbände und Initiativen zur IT-Sicherheit

Kontakt

eco – Verband der deutschen Internetwirtschaft e.V.

Lichtstraße 43h, 50825 Köln

fon +49(0)2 21-70 00 48-0, fax +49(0)2 21-70 00 48-111

www.eco.de, ak-sicherheit@eco.de