Application Scanner nützen in den Händen von Unkundigen nur wenig – Experten finden Schwachstellen schnell

Coding-Richtlinien sichern E-Business

Bei Webanwendungen stecken Security-Ansätze in vielen E-Business-Unternehmen noch in den Kinderschuhen. Im Unterschied zu qualitätssichernden Funktions- und Lasttests ist die systematische Betrachtung der Sicherheit bisher kaum in den Prozessen verankert.

So erklärt sich auch, warum nach wie vor bei einer Vielzahl von Webanwendungen Schwachstellen zu beobachten sind. Dabei ist gerade das E-Business, also die Abwicklung von Geschäftsprozessen im Internet, betroffen, stützt es sich doch zu einem hohen Grad auf Individualsoftware.

Am Anfang eines Softwareprojektes steht der Vertrag. Und Schwachstellen sind zu einem großen Teil Programmierfehler. Im Falle der Entdeckung greift also die Gewährleistungspflicht des Dienstleisters.

Aber nicht nur, weil sie als Grundlage für den Vertrag benötigt werden, sollte ein Unternehmen seine individuellen Secure Coding Guidelines erarbeiten. Web Application Security ist komplex und steht zumeist in enger Abhängigkeit mit der Host- und Netzwerksicherheit. Allgemeingültige Guidelines sind daher ein wichtiges Instrument, um Vereinfachung zu erreichen, interne Standards zu schaffen und die abteilungsübergreifende Verlässlichkeit zu erhöhen.

Ob eine Webanwendung wirklich sicher ist, zeigt erst die Sicherheitsuntersuchung. Im Unterschied zur Netzebene, wo der Blackbox-Ansatz in Gestalt von Penetrationstests ein geeignetes Mittel ist, sollte bei der Web Application Security (WAS) in Richtung Whitebox-Untersuchung gegangen werden. Die Masse der Angreifer hat in Summe in der Regel mehr Zeitbudget zur Verfügung als der Tester. Softwaretechnologie und -architektur sollten dem Prüfer daher offen gelegt, eingesetzte Standardsoftware genannt und sämtliche Dialoge mit der dahinter stehenden Businesslogik transparent gemacht werden.

Ein partielles Codereading deckt insbesondere die weit verbreiteten Fehler bei der Data Validation schnell auf. Die Erfahrung hat gezeigt, dass ein erfahrener WAS-Spezialist die häufigsten Sicherheitsprobleme relativ leicht durch Codeinspektion auffinden kann und damit dem ungezielten Stochern zumeist weit überlegen ist.

Zweifelhaft ist der Nutzen von Web Application Security Scannern. In der Hand des Fachunkundigen liefern sie kaum brauchbare Ergebnisse, und der Experte ist in vielen Fällen schneller und treffsicherer ohne ein solches Tool.

Eine Webanwendung steht in der Regel völlig ungeschützt im Internet, denn die herkömmliche Netzwerk-Firewall lässt alles ungehindert passieren, was Port 80 für Http-Verkehr oder Port 443 mit Https-Daten ansteuert. Eine Schwachstelle in einer Anwendung wird damit sofort zum Ernstfall. Dabei ist es keineswegs so, dass eine unsichere Webanwendung alleine die eigene Sicherheit kompromittiert. Da zumeist mehrere Anwendungen auf demselben Host bereitgestellt werden, sind diese schnell ebenfalls in Mitleidenschaft gezogen.

Mithilfe der mittlerweile ausgereiften Webshields, auch Application Firewalls genannt, kann eine zusätzliche Schutzlinie hergestellt werden. Diese Appliances, die auch den Inhalt der Datenpakete untersuchen, können viele der Angriffsmuster auf Anwendungsebene erkennen und unterbinden. Sie sind immer als ein zusätzliche Schutzlinie einzusetzen und sollten nicht als Ersatz für die Herstellung in sich sicherer Webanwendungen verstanden werden.

Damit das E-Business seinen Nutzen dauerhaft und umfassend entfalten kann, ist es wichtig, dass das Vertrauen in die Sicherheit der Systeme nicht gestört wird. Die Sicherheit auf Ebene der Webanwendung ist dabei ein entscheidender Faktor und sollte mit entsprechender Priorität verfolgt werden.

Thomas Schreiber, Geschäftsführer, Securenet/pg

Die Fachabteilung muss ran

Die Sicherheit schaffenden Stellen im Unternehmen sind in der Regel um das Netzwerk herum angesiedelt und ihre Expertise liegt bei Betriebssystem, Netzwerk und Firewall. Vielfach wird **die Zuständigkeit für die Sicherheit** von Webanwendungen ebenfalls dort angesiedelt. Dabei wird übersehen, dass zur Sicherstellung der Web Application Security ein breites Verständnis der Softwareentwicklung erforderlich ist.

Hinzu kommt: Fachliche und die Logik der Geschäftsprozesse haben bedeutenden Einfluss auf die Sicherheit einer Webanwendung. Die Verantwortung für diesen Bereich muss sich zu aus den Netzwerkabteilungen heraus und in die Fachabteilung hinein verlagern. Sie gehört in die Hände der Software- und nicht der Netzexperten.

Thomas Schreiber, Geschäftsführer, Securenet/pg