

Link: <https://www.computerwoche.de/a/sichere-applikationen-helfen-gegen-datenklau,2485688>

Cloud Computing

Sichere Applikationen helfen gegen Datenklau

Datum: 17.05.2011

Autor(en): Thomas Pelkmann

Bei Diskussionen um die Sicherheit in der Cloud stehen bisher primär die Netzwerke im Vordergrund. Zu Unrecht, meint HP-Manager Arved Graf von Stackelberg: Es sei dringend nötig, sich auch um die Sicherheit der Anwendungen zu kümmern.



Hände weg vom Code: Wer seine Anwendungen sichert, schützt auch seine Daten.
Foto: Fotolia, WoGi

Arved Graf von Stackelberg, Country Manager D-A-CH Fortify bei HP, weiß von einer interessanten Geschichte zu berichten, die illustriert, wie Internet-Gangster heutzutage an Geld kommen: Über eine **Cross-Site-Scripting**¹-Angriffe (XSS) waren Hacker in das Computersystem einer Bank gelangt. Dort haben sie in Anwendungen, die mit Kunden kommunizieren, Code eingefügt, der Login und Passwörter abgriff. Die wurden allerdings nicht dazu genutzt, direkt an die Gelder auf den Konten zu kommen - das wäre viel zu auffällig gewesen und daher schnell bemerkt worden. Sie dienten vielmehr weiteren Hacks sowie so genannten **Brute Force**²-Angriffen.

Am Ende einer ganzen Kette von Aktionen gelang es den Angreifern schließlich, sich eines "Send Message"-Buttons zu bemächtigen. Über den wurden vermeintliche Kaufempfehlungen der Bank für eine **Penny-Stock-Aktie**³ verschickt, mit der sich die Gangster zuvor reichlich eingedeckt hatten. Durch die "Empfehlung" der Bank stieg der Wert der Aktie innerhalb kürzester Zeit so massiv, dass die Angreifer nur wenige Stunden später die Aktie mit hohem Profit verkaufen konnten. Die Bank, berichtet von Stackelberg, habe diesen Angriff erst drei Jahre später und nur durch Zufall entdeckt.

Wie lassen sich Daten und Anwendungen, auf die Mitarbeiter, Kunden und Partner über das Internet zugreifen können, sichern? Bisherige Technologien zum Schutz von Daten sind praktisch ausgereizt, meint HP-Manager von Stackelberg: "Die Investitionen in Firewalls und Antivirenprogramme sind in den vergangenen Jahren massiv gestiegen. Dennoch hat auch die Zahl der Angriffe auf Firmennetze massiv zugenommen". Traditionelle Schutzmaßnahmen seien zwar wichtig, so von Stackelberg, lösten aber das Sicherheitsproblem in der Cloud nicht.

In die Unternehmenssoftware brechen Hacker nicht über das Netz ein, sondern direkt mit Methoden wie Cross Site Scripting, SQL-Injection oder **Information Leakage and Improper Error Handling**⁴ - um nur drei einer **ganzen Reihe von Möglichkeiten**⁵ zu nennen.

Sicherung der Netze ist weitgehend ausgereizt

Insofern empfiehlt es sich laut von Stackelberg, nicht nur auf die Netzsicherheit zu fokussieren, sondern auch die Anwendungen möglichst sicher zu machen. Die Netzsicherheit sei im Wesentlichen auf dem neusten Stand, konstatiert der HP-Manager, für Anwendungssicherheit hingegen gelte das noch lange nicht.

Auf den Servern in Unternehmen und zunehmend auch in der **Cloud**⁶ liegen Anwendungen, die zu einem Großteil in einer Zeit entwickelt wurden, als es noch gar keine flächendeckende Kommunikation über das Internet gab. Dabei handelt es sich zu einem guten Teil um Individualentwicklungen. Hinzu kommen Unternehmensanwendungen und **Open-Source-Lösungen**⁷, die oft angepasst und weiterentwickelt wurden.

Sicherheit in der Anwendungsprogrammierung ist kein neues Thema. Im Gegenteil: Die klassischen Methoden, mit denen Hacker von außen in Anwendungen eindringen können, um sie fremdzusteuern oder zweckzuentfremden, sind bereits seit Jahren bekannt. "Aber mit Cloud Computing stellt sich das Thema neu", gibt von Stackelberg zu bedenken. "Systembedingt kommunizieren alle Anwendungen in der Cloud nach außen." **Unsichere Anwendungen**⁸ seien daher zunehmend das Einfallstor für Angreifer, die in den Unternehmen systematisch auf Datenklau aus seien.

Der HP-Manager empfiehlt deshalb Unternehmen, sich stärker als bisher dem Thema Applikationssicherheit zuzuwenden. "Wir hoffen, dass die Unternehmen auch an dieser Stelle aufwachen", so von Stackelberg. Ein höherer Schutz für unternehmenskritische Daten in der Cloud sei vor allem durch sichere Anwendungen gewährleistet.

HP bietet mit dem **Application Security Center**⁹ eine ganze Reihe von Werkzeugen und Methoden an, um den Code von Anwendungen sicherer zu machen. Grundsätzlich gilt: Je eher man mit der Code-Kontrolle beginnt, desto ist höher die Erfolgsquote, und desto niedriger sind die Kosten.

Programmfehler, Hintertürchen, bewusste Lücken

Im Wesentlichen arbeiten die Tools beim Aufspüren von Schad- und Fehler-Code nach drei Szenarien: Sie suchen zunächst nach schlichten Programmfehlern, forschen aber auch nach (leichtsinnig) eingefügten Hintertürchen, die etwa für spätere Wartungsarbeiten offengehalten werden. Schließlich gibt es auch böswillig erzeugte Lücken, die Angreifern Tür und Tor öffnen sollen. "Insgesamt haben wir 400.000 Kategorien, nach denen wir arbeiten", erläutert von Stackelberg. "Wir schauen uns die Anwendungen an und prüfen, was man im schlimmsten Fall aus schlecht geschriebenem Code machen könnte."

Im Idealfall finden solche Source-Code-Analysen (SCA) bei der Programmierung neuen Codes oder bei Arbeiten an Release-Wechseln täglich statt, um die jeweils aktuellste Arbeit auf mögliche Fehler und Einfallstore für Angreifer zu bewerten. Die Entwickler erhalten dann Übersichten über die gefundenen Fehler und Tipps, wie sie diese Problemzonen behandeln sollen.

Rund 90 Prozent aller Schwachstellen werden bei dieser statischen Source-Code-Analyse aufgestöbert. Allerdings sind darunter auch Schwachstellen, die allenfalls theoretisch Probleme bereiten, in der Praxis aber nicht. Diese im Grunde falschen Alarme ("**False Positives**")¹⁰ werden jedoch in Kauf genommen, um zu verhindern, dass echte Probleme beim Review übersehen werden ("False Negatives").

Weitere 30 Prozent möglicher Lücken werden nach Fertigstellung des Codes bei so genannten Penetration Tests mit dem Program Trace Analyzer (PTA) und dem Real Time Analyzer (RTA) aufgespürt. Dabei probieren beide Tools im Grunde immer wieder, mit bekannten Methoden in die Anwendungen "einzubrechen". Gelingt das, wird das Wissen dazu genutzt, diese Fehler zu beheben und potenzielle Einfallstore zu verschließen.

Viele der hierbei gefundenen Fehler sind mit den Schwachstellen identisch, die schon bei der Source-Code-Analyse gefunden werden - hier gibt es rund 20 Prozent Übereinstimmung. Demnach mag es unsinnig erscheinen, fertigen Code mit PTA und RTA überhaupt noch zu überprüfen. Das ist es aber nicht: Zum einen stöbern die Tools so genannte logische Fehler auf, die bei einer statischen Analyse nicht zu erkennen sind. Zudem werden hier die vielen False Positives bewertet: Handelt es sich dabei um echte Probleme, die es zu behandeln gilt? Und schließlich sind PTA und RTA die Werkzeuge der Wahl, wenn es um die Überprüfung bereits fertiger Programme geht. "In der Regel fangen wir bei unseren Überprüfungen ja nicht bei Null an", beschreibt von Stackelberg typische Szenarien, wie HP sie in den Unternehmen vorfindet. Viele Anwendungen sind seit Jahren im Einsatz, weisen aber trotzdem Sicherheitslücken auf. Mit den Analyseprogrammen ist es möglich, auch diese Applikationen - sogar im laufenden Betrieb - auf Fehler zu prüfen, die Sicherheitsprobleme hervorrufen könnten.

Offene Flanken auch in fertigen Programmen erkennen

In der Summe finden die Testverfahren in aller Regel eine Vielzahl von Fehlern. Laut von Stackelberg lassen sich Durchschnittswerte hier nicht benennen, in der Spitze seien eine Million Fehler bei 1,5 Millionen Zeilen Code allerdings durchaus möglich. Auch in kleineren Dimensionen heißt das: Es sind auf jeden Fall zu viele, um sie alle auf einen Schlag zu beheben.

Das bedeutet: Bei der Applikationssicherheit müssen Prioritäten gesetzt werden. Dem HP-Experten zufolge ist dafür ein strategischer Ansatz für das Risiko-Management erforderlich. Demnach gilt es für Unternehmen zunächst zu überlegen, welche Daten in den Anwendungen tatsächlich schützenswert sind und welche nicht. Danach wird das Risiko bewertet, dass diese Daten Ziel von Angriffen werden können. Anschließend werden nach den Reviews und Penetration Tests vorrangig diese Probleme in Angriff genommen, bevor man sich - wenn überhaupt - auch an Aufgaben mit niedriger Priorität macht.

Mit einer guten **Risiko-Management-Strategie**¹¹ verbunden ist ein vernünftiges **Change Management**¹²: "Im Grund genommen ist das Managen der notwendigen Veränderungen unsere Hauptaufgabe, wenn wir in die Unternehmen gehen", betont von Stackelberg. Die Produkte für die Applikationssicherheit würden dort sofort akzeptiert, weil sie weitgehend selbsterklärend seien. "Aber wir müssen dafür sorgen, dass sich die Entwickler und die Verantwortlichen in den Unternehmen dieses Themas überhaupt annehmen und sich bewusst werden, wie wichtig Applikationssicherheit ist - und welche Auswirkungen sie auf die bisherigen Abläufe bei der Anwendungsentwicklung hat."

Nach Angaben des HP-Experten gilt es zum einen, Regeln für möglichst fehlerfreie Programmierung aufzustellen, zum anderen muss gewährleistet sein, dass die regelmäßigen Tests und die Fixes der gefundenen Fehler die Release-Zyklen nicht durcheinanderbringen. In konkreten Projekten, so von Strackelberg, sei man zudem sehr damit beschäftigt, neue Rollen zu definieren: etwa Security Leads, die sich grundsätzlich um die Anwendungssicherheit kümmern, oder Auditoren, die sich mit der Code-Kontrolle beschäftigen, beziehungsweise Koordinatoren, die für die Priorisierungen verantwortlich sind. All das münde in ein ganzheitliches Maturity-Modell für Applikationssicherheit, der **Software Security Assurance (SSA)**¹³ von **Fortify**¹⁴. "Hier lernen die Unternehmen, sich selbst einzuordnen und zu ermitteln, was genau die Mitarbeiter tun müssen, um die Anwendungen sicher zu gestalten."

Mehr zum Thema

- **Warum Software-Anwendungen sicher sein müssen - und was Sie dafür tun können**¹⁵
- **Wie sicher ist Ihre SaaS-Software?**¹⁶
- **Eine Checkliste für den Schutz digitaler Informationen**¹⁷
- **Eine Checkliste für die Sicherheit von Standard-Software**¹⁸
- **Security and Cloud Services**¹⁹

Einen 100-prozentigen Schutz vor Angriffen bietet das jedoch nicht, tatsächlich ist dieser nicht möglich - weder bei Unternehmen, die ihre Daten in der eigenen Organisation vorhalten, noch bei Firmen, die auf Public Clouds setzen. "Unserer Erfahrung nach ist die Anwendungssicherheit aber der beste Ansatz, um den Sicherheitsproblemen wirksam zu begegnen", meint HP-Experte von Stackelberg. "Das wird die Sicherheit in der Cloud deutlich erhöhen."

Links im Artikel:

¹ <https://www.computerwoche.de/security/1898982/>

² <http://de.wikipedia.org/wiki/Brute-Force-Methode>

³ <http://de.wikipedia.org/wiki/Pennystock>

⁴ <https://www.computerwoche.de/security/1898982/index7.html>

⁵ https://www.owasp.org/index.php/Category/OWASP_Top_Ten_Project

⁶ <https://www.computerwoche.de/management/cloud-computing/>

⁷ <https://www.computerwoche.de/schwerpunkt/o/Open-Source.html>

⁸ <https://www.computerwoche.de/schwerpunkt/a/Anwendungssicherheit.html>

⁹ https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200_4000_5__

¹⁰ <https://www.computerwoche.de/security/1911699/index2.html>

¹¹ <https://www.computerwoche.de/security/1863034/index3.html>

¹² <https://www.computerwoche.de/karriere/karriere-gehalt/1929790/>

¹³ <https://www.fortify.com/ssa-elements/about-ssa.html>

¹⁴ <https://www.computerwoche.de/security/2351672/>

¹⁵ http://whitepaper.computerwoche.de/index.cfm?cid=EL_1305549217155546014776&pkdownloads=4522

¹⁶ <http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=4523>

¹⁷ <http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=4524>

¹⁸ <http://whitepaper.computerwoche.de/index.cfm?cid=38&pkdownloads=4525>

¹⁹ <https://www.computerwoche.de/filesserver/idgwpcw/files/1914.pdf>

Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.