

Link: <https://www.cio.de/a/sichere-anwendungen-brauchen-mehr-als-software-codes,3102710>

Sichere Applikationen - aber wie?

Sichere Anwendungen brauchen mehr als Software-Codes

Datum: 28.01.2015

Autor(en): Sabine Koll

Sind Anwendungsentwickler auch für die Sicherheit ihres Codes verantwortlich? Die Antwort von Peter Maucher, Berater bei HP Enterprise Security Services, lautet: Es müssen viele mithelfen - von der IT über den Einkauf bis zu den Führungskräften.

Ganz gleich ob AOL, Amazon, Facebook, Paypal oder andere Unternehmen: Es vergeht kaum ein Tag ohne Meldung in den Medien, dass sich Hacker unerlaubten Zutritt zu Unternehmensnetzwerken verschafft haben und dabei an sensible Daten und Informationen gelangt sind. Die Folgen können Imageverluste, aber auch Umsatz- und Gewinneinbußen sein; außerdem kann es zu Rechtsstreitigkeiten kommen.



Peter Maucher, Berater HP Security Services: "Sichere Applikationsentwicklung erfordert ganzheitlichen Ansatz."

Foto: HP Deutschland

Dabei erfolgen 75 Prozent aller Hacker-Attacken auf dem Applikationslevel, wie Gartner feststellt. SQL Injection und Cross-site Scripting gehören dabei zu den beliebtesten Methoden der Eindringlinge.

Im krassen Gegensatz zur Wichtigkeit der Applikationssicherheit steht das Budget, das die Unternehmen dafür aufwenden: Gerade einmal 20 Prozent der IT-Security-Budgets in Deutschland entfallen nach der Studie "2013 Cost of Cyber Crime Study: Germany" des Ponemon Institute auf den Application-Layer. Sowohl dem Netzwerk- als auch dem Daten-Layer werden deutlich mehr Aufmerksamkeit und Geld gewidmet.

Doch letztlich reicht auch der Einsatz dieser Werkzeuge nicht, um die Sicherheit von Anwendungen dauerhaft zu gewährleisten. Denn das zunehmende Entwicklungstempo und die steigende Komplexität von Software stellen die Softwareentwickler und damit auch die Sicherheit der Anwendungen vor neue Herausforderungen.

Zudem stellt das Fehlen von Standardlösungen zum Beispiel für Identitäts- und Access-Management oder Verschlüsselung - die über ein Architektur-Management im Unternehmen definiert werden sollten - ein Problem dar. Hinzu kommt, dass Entwicklungsteams oft weltweit verteilt an einem Projekt arbeiten, unterstützt noch durch externe Partner.

Ganzheitlicher Ansatz über den gesamten Application Lifecycle

"Vor diesem Hintergrund wird klar, dass sichere Applikationsentwicklung einen ganzheitlichen Ansatz über den gesamten Lebenszyklus erfordert - angefangen bei der Projektbeantragung und -genehmigung über den Einkauf externer Leistungen, den Entwicklungsprozess, Änderungen während des operativen Betriebs bis hin zur Stilllegung der Applikation", sagt Peter Maucher, Experte bei HP Enterprise Security Services.

Entsprechende Prozesse, Regeln und Standards im Unternehmen sind die Eckpfeiler eines sicheren Software-Entwicklungslebenszyklus. Ausgangspunkt dafür kann Kapitel A14 der ISO 27001, der internationalen Zertifizierungsnorm für Informationssicherheitsmanagementsysteme, sein. In der 2013 veröffentlichten Neuerung geht es um Sicherheit in Entwicklungs- und Unterstützungsprozessen. Gefordert wird, Regeln und Grundsätze zur Entwicklung sicherer Software und sicherer Systeme aufzustellen und umzusetzen.

Ergänzende Kontrollen beinhalten das Entwickeln ausschließlich speziell gesicherter Entwicklungsumgebungen und die Durchführung gezielter Funktionstests der entwickelten Sicherheitsfunktionen. "Im Kapitel A14 der ISO 27001 geht es wirklich nur um Basics, die eine Anwendung definitiv noch nicht sicher machen. Doch selbst Unternehmen, die sich nach ISO 27001 zertifizieren lassen, klammern dieses Kapitel häufig noch aus", weiß Maucher aus Erfahrung.

Normative Vorgaben hinken hinterher

Konkret für die Applikationssicherheit bietet sich seiner Meinung nach eher die ISO 27034-1 (Guidelines for Application Security) an, die Ende 2012 veröffentlicht wurde. Dieser erste Teil der neuen Norm adressiert die Grundlagen für das Thema Applikationssicherheit und stellt Definitionen, Konzepte, Prinzipien und Prozesse vor. Hier gibt es Hinweise zur Integration von Sicherheit in das Applikationsmanagement, auf Rahmenwerke und auf Kontrollelemente.

"Ins Detail für die Umsetzung geht dieser Teil 1 jedoch nicht, dies soll in den Teilen 2 bis 5 erfolgen, die erst noch geschrieben werden müssen", so Maucher. "Insofern mangelt es für die sichere Anwendungsentwicklung immer noch an normativen Vorgaben, an denen sich die Unternehmen orientieren können - ganz im Gegensatz etwa zur Netzwerk- oder Serversicherheit. In beiden Bereichen existieren bereits seit vielen Jahren detaillierte Standards."

HP Enterprise Services hat daher ein eigenes Rahmenwerk entwickelt, das Unternehmen helfen soll, die richtigen Prozesse und Regeln für eine sichere Applikationsentwicklung aufzusetzen. Es fokussiert insgesamt fünf Bereiche von Richtlinien und Vorgaben über Prozesse, Tools und Werkzeuge sowie das Governance Modell bis hin zur Kommunikation und Schulung.

"Beim Thema Richtlinien und Vorgaben geht es darum zu beschreiben, was grundsätzlich im Unternehmen getan werden muss, um für eine sichere Anwendungsentwicklung zu sorgen. Dies sind zum einen Vorgaben für die Qualitätssicherung. Daneben sollten Organisationen auch eine Plattform mit spezifischen Entwickler-Leitfäden zur sicheren Anwendungsentwicklung aufbauen", rät HP-Experte Maucher.

Bei letzterer sollten Best Practices verschiedener Organisationen einfließen: Dazu gehören die Business Application Security Initiative (BIZEC), die Sicherheitsstandards für SAP-Systeme etabliert; Common Weakness Enumeration (CWE), ein Standardisierungsprojekt für die Beschreibung von Sicherheitsschwachstellen, getrieben durch die amerikanische Non-Profit-Organisation MITRE Cooperation; das Open Web Application Security Project (OWASP), das ebenso wie das Web Application Security Consortium (WASC) Web Anwendungen fokussiert.

Nicht nur die IT-Organisation sollte involviert sein

Das Thema Prozesse empfiehlt Maucher umfassender anzugehen, als dies die ISO 20000 beziehungsweise die IT Infrastructure Library (ITIL) als Quasi-Standard für das IT Service Management vorgeben: So sollten neben den klassischen, die IT-Organisation betreffenden ITIL-Disziplinen Demand Management, Change Management, Incident Management, Problem Management und Continual Service Improvement auch Abläufe im Einkauf und Beschaffung auf den Security-Prüfstand kommen.

"Wenn man Entwicklungsleistungen einkauft, muss beispielsweise sichergestellt sein, dass die Dienstleister entsprechende Vertraulichkeitserklärungen unterschrieben haben, dass man Zugriff hat auf den Code, den sie entwickeln und dass sie den Code mit den gleichen Tools und Sicherheitsstandards entwickeln wie die interne IT. Das muss rechtlich abgesichert sein", so Maucher.

Auch die in der Anwendungsentwicklung verwendeten Methoden und Werkzeuge sollten einem Sicherheits-Check unterzogen werden. Viele Unternehmen nutzen heute zwar Werkzeuge für - zum Teil automatisierte - Softwaretests.

Nicht einmal die Hälfte führt Sicherheitstests durch

Doch nicht einmal die Hälfte, nämlich 43 Prozent, führt Sicherheitstests durch, um die Risiken von Security Bugs oder Defekten in Anwendungen zu minimieren, wie die Studie "The State of Application Security" des Ponemon Institute vom Sommer 2013 belegt. Und nur 42 Prozent unterziehen demnach ihre Anwendungen manuellen Penetrationstests.

Mauchers Rat: "In der Regel hilft eine Konsolidierung auf wenige Frameworks, die gleichzeitig auch Sicherheitsmethoden zur Verfügung stellen oder eine gewisse Stringenz im Entwicklungsprozess fordern, sodass die Entwickler Sicherheitsthemen nicht ausgrenzen können."

Die Festlegung auf sichere Technologien, dazu gehören auch Entwicklungssprachen und -tools sowie Tools für Security Code Reviews, ist somit ein wesentlicher Schritt zur sicheren Anwendungsentwicklung. Für Maucher ist es somit trotz aller Diskussionen keine Frage, dass Entwickler für die Sicherheit ihres Codes Verantwortung übernehmen müssen.

Security-Governance ist mehr als ein IT-Infrastruktur-Thema

Ein weiterer Bestandteil ist für Maucher das Thema Governance, also die Steuerung. "In vielen Unternehmen ist das Thema Sicherheit in der IT traditionell ein Infrastrukturthema. Damit sind dann auch häufig die Security-Rollen stärker an der Infrastruktur ausgerichtet - und die Anwendungsentwicklung ist davon ausgenommen.

In dem Fall sollte man sich überlegen, wie man ein organisatorisches Bindeglied zwischen diesen beiden Welten schaffen kann, damit Sicherheit im gesamten Application Lifecycle, also auch in späteren Projekten, immer gewährleistet ist."

Schließlich dürfe nicht vergessen werden, alle Experten im Unternehmen, die an der Anwendungsentwicklung beteiligt sind, regelmäßig und individuell im Hinblick auf Security zu schulen: Das betrifft neben den Softwareentwicklern die Mitarbeiter im Einkauf sowie die Mitarbeiter im Demand Management, die Aufträge aus dem Business bereits auf die Sicherheitsbelange im Unternehmen abklopfen sollten.

"Schulungen für das Management darf man nicht vergessen, denn auch die Führungskräfte sollten für das Thema sensibilisiert sein", mahnt Maucher. "Und auch Mitarbeiter, die im Lenkungsausschuss von Entwicklungsprojekten sitzen, müssen bei entsprechenden Projektfreigaben wissen, welche Verantwortung sie bei der Überprüfung von Quality Gates im Hinblick auf Sicherheitsthemen haben. Das heißt, die Kommunikation muss quer durch das gesamte Unternehmen gehen. Denn es müssen wirklich alle einfangen sein, die am gesamten Applikationsentwicklungsprozess beteiligt sind."

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG 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.