# Strategische Roadmap zur Entwicklung einer hohen Web-Sicherheit

06.03.2013, 14:58 | IT, New Media & Software

Pressemitteilung von: *mikado ag*
Presseagentur: *denkfabrik groupcom GmbH*

Zwar verlangen die Compliance-Vorschriften auch ein anforderungsgerechtes Sicherheitsprofil der Web-Anwendungen, tatsächlich bestehen hier in der Praxis häufig noch erhebliche Defizite. So ermittelte beispielsweise eine letztjährige Studie der mikado ag, dass die Unternehmen nur in jedem zehnten Fall wenigstens alle sechs Monate in ihren Portalen und Internetshops Sicherheitsanalysen vornehmen. Diese Zurückhaltung resultiert nicht zuletzt daraus, dass die Web-Sicherheit nur eine geringe Aufmerksamkeit genießt und die Konzentration stattdessen auf anderen Security-Prioritäten gerichtet ist.

„Die aktuell fast täglichen Meldungen über Hackerangriffe auf prominente Firmen zeigen, wie trügerisch die Sicherheit ist, in der sich viele Unternehmen wägen“, problematisiert mikado-Geschäftsführer Wolfgang Dürr. Als Ursache sieht er seinen Beratungserfahrungen zufolge jedoch weniger, dass das tatsächliche Bedrohungspotenzial ignoriert werde, sondern es an einem systematischen Zugang zu dem Thema fehle. Dürr hat deshalb eine Roadmap für den Aufbau der notwendigen Web-Sicherheit erarbeitet:

1. Den tatsächlichen Security-Bedarf präzise klären:
Nicht jede Web-Applikation hat zwangsläufig auch hohe Sicherheitsansprüche. Doch sobald eine Website nicht nur der reinen Informationspräsentation dient, sondern in weitere Unternehmenssysteme integriert ist, entsteht ein bedeutsames Risiko beispielsweise für unerlaubte Zugriffe auf vertrauliche Kundendaten, Unternehmensinformationen und Rechnungsdaten. Ebenso können dann bei fehlender Web-Sicherheit Eingriffe in die technische Infrastruktur mit zusätzlich problematischen Folgen vorgenommen werden. Diese Situation gilt etwa für alle Web-Shops. Insofern bedarf es zunächst einer Statusanalyse mit differenzierter Matrix der potenziellen Angriffsflächen. Aus ihr wird dann der individuelle Security-Bedarf mit gezielter Gewichtung der verschiedenen Risiken bei tiefen Eingriffen und ihren Konsequenzen abgeleitet.
2. Unklare Verantwortlichkeiten beseitigen:
Im Bewusstsein der Web-Verantwortlichen hat die Sicherheit auch deshalb vielfach noch keinen adäquaten Stellenwert, weil verschiedene funktionale Zuständigkeiten bestehen. So konzentriert sich die interne oder externe Web-Entwicklung auf die technische Lösung und der Provider widmet sich dem Hosting. Weiterhin kümmern sich der Vertrieb oder das Marketing um den Content und die Kommunikationsbelange. Außerdem gibt es noch die möglicherweise ganz woanders angesiedelt Funktion des Webmaster. Durch diese komplementäre Aufgabenstruktur verliert das Security-Thema im praktischen Alltag eine klare Zuordnung mit negativen Konsequenzen für das reale Niveau der Web-Sicherheit.
3. Umfassend den aktuellen Security-Status testen:
Fast 500 verschiedene Angriffsarten mit unterschiedlicher Gefährdungswirkung für die Web-Applikationen sind derzeit bekannt. Deshalb bedarf es Analysen über komplexe Penetrationsverfahren, in denen mögliche Zugriffsrisiken ermittelt werden. Eine relativ komfortable Methode bieten dafür Tools mit einem automatisierten Scanning der Web-Anwendungen. Deren Report gibt konkrete Hinweise darauf, welche möglichen Gefahren bestehen. Insbesondere bei kritischen Web-Applikationen wie etwa Internetshops empfehlen sich zusätzliche strukturierte manuelle Penetrationstests, in denen gleichzeitig auch die technischen und organisatorischen Bedingungen der Web-Sicherheit überprüft werden.
4. Security-Prozesse in das Change Management integrieren:
Weil Web-Applikationen durch funktionale Erweiterungen und technische Neuerungen kontinuierlichen Veränderungen unterliegen, kann eine permanent fragile Security-Situation entstehen. Aus diesem Grund sind systematische Sicherheitsmaßnahmen als integraler Bestandteil der Veränderungen notwendig, die sowohl prozessual als auch in den Verantwortlichkeiten klar abgebildet werden müssen. Zu den Grundpflichten gehören dabei auch regelmäßig neue Penetrationstests nach technischen Eingriffen in die Web-Anwendungen, um mögliche Auswirkungen auf die Sicherheit zu ermitteln.
5. Notfallmanagement praxisgerecht organisieren:

Selbst wenn optimale Sicherheitsvorkehrungen getroffen wurden, können Probleme angesichts der ständig neuen Angriffsmethoden nie ausgeschlossen werden. Dies verlangt die Entwicklung von Notfallszenarien mit unterschiedlichen Eskalationsstufen, um im Bedarfsfall nach definierten Vorgehensweisen schnell und wirksam handeln zu können. Die Erstellung und Pflege von Notfallplänen ist jedoch kein einmaliger Vorgang. Vielmehr handelt es sich hierbei um einen laufenden Prozess, der in seiner Komplexität häufig nur Tool-gestützt sinnvoll umgesetzt werden kann.

**Portrait**

Mehr über mikado ag
Seit fast drei Jahrzehnten beschäftigt sich die mikado mit dem effizienten Management und der kompromisslosen Sicherheit von IT-Strukturen. Wir entwickeln individuelle, präventive Strategien und Produkte, die auf die spezifischen Anforderungen der IT-Organisation der unterschiedlichsten Unternehmen und öffentlichen Einrichtung ausgerichtet sind. Mit dieser Ausrichtung bietet die Unternehmensberatung eine Fülle von Dienstleistungen zur Bewertung und Verbesserung Ihrer IT-Sicherheitssituation. Dazu gehören neben Penetrationstests beispielsweise das IT-Sicherheitsmanagement, das IT-Notfall- und IT-Risikomanagement sowie die Beratung zum Datenschutz und zum IT-Grundschutz. Zudem hält die mikado ag verschiedene Security-Services für unterschiedliche Anforderungen ihrer Kunden bereit. Zum Kundenstamm gehören u. a. Bundesministerien, Volkswagen, Investitionsbank Berlin, Total, KfW Kreditanstalt für Wiederaufbau, Sparkassen und Volksbanken. Firmensitz der mikado ag ist Berlin. mikado ist Mitglied bei BITKOM und dem SIBB.

News-ID: 703302 • Views: 103 (Stand: 25.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/703302/Strategische-Roadmap-zur-Entwicklung-einer-hohen-Web-Sicherheit.html