



Ist die Online Hilfe ein Sicherheitsrisiko ?

Ein WebWorks.com White Paper

© 2010 – Quadralay Corporation. Alle Rechte vorbehalten.

Inhaltsverzeichnis

Übersicht und Hintergrund	1
Wir waren nicht die Einzigen	2
Und noch mehr	2
Es geht nicht nur um die Delivery Plattform	2
Warum sind Online Hilfen besonders gefährdet ?	2
Die internen Gefahren nicht übersehen	3
Sicherheit ist ein Prozess	3
Erste Schritte, die Ihre Sicherheit garantieren	3
Zusammenfassung	4
Über ePublisher und WebWorks	4

Ist die Online Hilfe ein Sicherheitsrisiko ?



Übersicht.

Dieser Aufsatz beschäftigt sich mit Problemen, die im Bereich der Sicherheit von Online Hilfen auftreten und mit entsprechenden Maßnahmen, die man gegen möglichen Gefährdungen unternehmen kann.

Hintergrund.

“Ich habe nie in Betracht gezogen, dass meine Online Hilfe ein potentieller Angriffsvektor sein könnte.“
Dieses Zitat eines WebWorks ePublisher Kunden, das sich in einer Email versteckte, hat wirklich unsere Aufmerksamkeit auf sich gezogen. In vielerlei Hinsicht hat uns diese Aussage wachgerüttelt und uns als Leitfaden dafür gedient, uns nicht nur genauer mit der Sicherheit unseres eigenen, plattformübergreifenden Produkts WebWorks Help, sondern auch mit der Sicherheit von Online Hilfen im Allgemeinen zu beschäftigen. Diese Email erreichte uns, als wir mit einem Kunden arbeiteten, der eine potentielle Gefahr durch Cross-Site Scripting in unserer WebWorks Help 5 Online Hilfe entdeckt hatte. Unter Cross-Site Scripting versteht man einen bösartigen Angriff durch das Einfügen eines clientseitigen Scripts in eine Webseite, wobei die Sicherheitseinstellungen des Browsers umgangen werden.

Mit unserem Kunden und einer unabhängigen Sicherheitsfirma gingen wir schnell dazu über, Schritte zur Schließung dieser Sicherheitslücke in WebWorks Help zu untersuchen, zu entwickeln und zu testen. Als Ergebnis konnten wir am 15. Dezember 2009 das WebWorks Security Advisory herausgeben. Das Advisory beinhaltet sowohl einen Code Fix als auch dokumentierte Anweisungen zur Schließung potentieller Sicherheitslücken. Die entsprechenden Änderungen wurden in die 2009.3 und 2009.4 Versionen der ePublisher Plattform integriert. Dadurch wird sichergestellt, dass alle mit diesen und späteren WebWorks Versionen erstellten Hilfen nicht mehr gefährdet sind.

Wir hätten es dabei belassen können, aber im Laufe unserer Untersuchungen kamen wir zu der Überzeugung, dass diese Thematik offener diskutiert werden sollte. Wir sahen die Notwendigkeit, ein Bewusstsein dafür zu schaffen, wie und weshalb man seine Online Hilfe auch als potentielles Sicherheitsrisiko betrachten sollte.

Ein WebWorks.com White Paper

Wir waren nicht die Einzigen.

Im Jahr 2007 dokumentierte die Sicherheitsfirma Symantec, dass Cross-Site Scripting für 80% aller Sicherheitsschwachstellen¹ verantwortlich ist. Die Auswirkungen reichten von bloßen Beeinträchtigungen bis hin zu mit erheblichen Sicherheitsrisiken verbundenen Angriffen.

Andere Online Hilfesysteme haben sich in den letzten Jahren als ebenso anfällig für Sicherheitsangriffe erwiesen. Adobe hat zwischen 2007 und 2009² insgesamt neun Security Advisories, sowohl für RoboHelp als auch für RoboHelp Server, herausgegeben.

Adobe, wie auch WebWorks, haben alle Details dieser Ratgeber auf Ihren Websites veröffentlicht. Während unserer Recherche haben wir herausgefunden, dass andere Unternehmen aus der Editing/ Content Management/ Publishing Branche für ihre Kunden entsprechende Ratgeber herausgegeben haben, diese Informationen jedoch nicht notwendigerweise online zur Verfügung gestellt haben.

-
- 1 Symantec Internet Security Threat Report
See http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
- 2 Adobe
See <http://www.adobe.com/support/security>
-

Und noch mehr.

Während viele Unternehmen daran arbeiten, diese Schwachstellen zu bekämpfen, wenden sich Hacker und Verfasser bössartiger Codes anderen Zielen zu. Eine der gebräuchlichsten Alternativen zur Veröffentlichung von Online Hilfen in einem Browser ist die Produktion seitenbasierter Handbücher, die im PDF-Format online zur Verfügung gestellt werden.

Das PDF-Format ist jedoch genau so anfällig für bössartige Angriffe. Dem von McAfee, der führende Anbieter von Sicherheitssoftware, herausgegebenen 'Threat Report' von 2010³ zufolge sollte dem PDF-Format besondere Aufmerksamkeit zuteil werden. In diesem Bericht wird die These aufgestellt, dass im Jahr 2010 "Adobe Software, insbesondere Acrobat Reader und Flash den ersten Platz" unter den beliebtesten Zielen der Hacker einnehmen wird. Bereits im Februar 2010 hat Adobe ein Sicherheitsupdate für den Acrobat Reader herausgegeben⁴.

-
- 3 McAfee
See http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf
- 4 Adobe
See <http://www.adobe.com/support/security/bulletins/apsb10-07.html>
-

Es geht nicht nur um die Delivery Plattform.

Im Jahr 2009 wurden über 110 Sicherheitsschwachstellen in gebräuchlichen Browsern, Webanwendungen und Betriebssystemen gemeldet. Im Januar 2010 hat Microsoft nur zwei Wochen voneinander entfernt zwei verschiedene Advisories publiziert, die sich mit Sicherheitslücken der jeweiligen Versionen ihres Browsers Internet Explorer beschäftigen.

Warum sind Online Hilfen besonders gefährdet?

Abgesehen von potentiellen Schwachstellen in Delivery Plattformen und Browsern, kann die Online Hilfe selbst aus verschiedenen Gründen viel anfälliger als andere webbasierte Anwendungen sein.

> Traditionellerweise werden Online Hilfen nach dem Muster "Veröffentlicht-und-Vergessen" erstellt. Das Hilfesystem ist mit einer bestimmten Version eines Produktes oder Projektes verbunden. Wenn ein Projekt abgeschlossen ist, verlagert man seinen Fokus auf das nächste Produkt. Online Hilfesysteme werden deshalb oft nicht gepflegt.

Ein WebWorks.com White Paper

- > Sogar wenn ein Online Hilfesystem nicht länger aktiv ist, bleiben viele als Altsysteme erhalten. Um zu einem potentiellen Angriffsvektor zu werden, müssen sie nur einmal mit einer eingebauten Schwachstelle versehen worden sein. Die Tatsache, dass Hilfesysteme unter Sicherheitsaspekten oft übersehen werden, macht sie zu attraktiven Zielen für bössartige Codes.
- > Online Hilfesysteme bleiben statisch, sie werden mit älteren Browserversionen geliefert und bleiben an diese gebunden. Diese Browserversionen werden aber mit der Zeit immer anfälliger.
- > Online Hilfen werden in IT Sicherheitsaudits oft übersehen, da sie im Allgemeinen nicht als Teil der IT-Infrastruktur betrachtet werden, sie sind "ja nur Dokumentation".

Die internen Gefahren nicht übersehen.

Während die meisten Unternehmen den Großteil ihrer IT Sicherheitsüberwachungen auf externe Gefahren ausrichtet, stellen interne Gefahren ein weitaus größeres Gefahrenpotential dar. Mit internen Phishing Attacken lässt sich Datenverlust bestens bewerkstelligen. Gleichzeitig sind diese für Cross-Site Scripting sehr anfällig. Böswillige Mitarbeiter können sich so Zugang zu Passwörtern für Systeme beschaffen, zu denen sie normalerweise keinen Zugang haben, z.B. zu Personalakten oder zu Gehaltslisten. Während Unternehmen ihren Mitarbeitern an sich vertrauen sollten, haben gerade diese Mitarbeiter verstärkt die Möglichkeit, unternehmensweite Systeme zu beeinträchtigen.

Vertrauenswürdige Mitarbeiter können aber auch von externen Elementen gefährdet werden, insbesondere insofern als immer mehr Unternehmen ihre Interneteinschränkungen aufheben, um ihren Mitarbeitern die Teilnahme an sozialen Netzwerken und Online Communities zu ermöglichen. Diese gemeinschaftliche Teilnahme macht einen immer größeren Anteil geschäftlicher Beziehungen aus und spielt auch eine zentrale Rolle in der Wettbewerbsfähigkeit in einer sich verändernden digitalen Landschaft.

Sicherheit ist ein Prozess.

Eine gutes Sicherheitsmanagement sollte nicht nur Flickschusterei sein; es sollte einen Prozess entwickeln, der das aktuelle Problem sowohl behebt als auch gegen zukünftige Gefahren schützt. Während ein einzelnes Deliverable Schwachstellen aufweisen kann, sollte ein gut definierter Prozess dem Rechnung tragen und es über die Zeit kurieren. Für die Produktion von Dokumenten empfehlen wir einen Prozess der regelmäßigen Aktualisierung. Microsoft z.B. hat einen "Patch Dienstag": an jedem zweiten Dienstag eines jeden Monats werden neue Sicherheitspatches heraus gegeben. Während Sie Ihre Online Hilfeprodukte evtl. nicht einem solch strengen Plan unterziehen müssen, sollten sie doch darauf achten regelmäßige Updates auch für Ihre Dokumentation anzusetzen.

Erste Schritte, die Ihre Sicherheit garantieren.

Im Laufe unserer Untersuchungen haben wir folgende Vorschläge entwickelt, um die Gefahr zu reduzieren, die Ihre Online Hilfe zu einem Sicherheitsrisiko werden lassen.

- > Pflegen Sie Ihre Online Delivery Plattformen. Verwenden Sie immer die aktuellsten Softwareversionen, die für Ihre Produktion zur Verfügung stehen. Halten sich über Upgrades und Patches auf dem Laufenden.
- > Benutzen Sie nach Möglichkeit immer die aktuellsten Browser.
- > Informieren Sie sich über Security Advisories, die von den Herstellern Ihrer Produkte herausgegeben werden. Fragen Sie bei Ihren Herstellern auch wirklich nach (beachten Sie, dass nicht alle ihre Advisories öffentlich zur Verfügung stellen).
- > Geben die Hersteller Ihrer Produkte Security Advisories heraus, lesen Sie diese, finden Sie heraus, ob die beschriebenen Punkte Ihre Arbeit betreffen und wenn, dann HANDELN Sie entsprechend. Führen Sie alle zur Schließung der Sicherheitslücke empfohlenen Schritte aus und upgraden Sie bei Ihrem nächsten Release.
- > Entwickeln Sie einen Prozess, der Ihre Online Hilfeprodukte regelmäßig auf den neuesten Stand Ihrer Produktionstools bringt.

Ein WebWorks.com White Paper

Zusammenfassung.

Bedenken Sie IMMER, dass eine Online Hilfe ein potentieller Angriffsvektor sein könnte!

- > Erstellen Sie einen systematischen Prozess, um solche Lücken zu identifizieren und sich vor Angriffen zu schützen.
- > Aktualisieren Sie Ihre Tools und Deliverables regelmäßig.
- > Bedenken Sie, dass nicht alle Sicherheitsangriffe von außen kommen.
- > Hinsehen, zuhören, handeln.

Über ePublisher.

ePublisher ermöglicht kosteneffektive Prozesse für das effiziente Verfassen, Präsentieren und Einsetzen von Online- und Printpublikationen. Durch die Nutzung dieser drei Komponenten können Organisationen bereits bestehende Authoring Tools und Content Management Systeme wirksam einsetzen und unternehmensweite Publishingbedürfnisse erfüllen, ohne dafür teure Trainings oder Software aufzuwenden. Die offene Systemarchitektur, die auf dem XSL-Standard basiert, ermöglicht größtmögliche Flexibilität, Anpassungsfähigkeit und Schutz vor Fehlinvestitionen in aufwändige Migrationsprozesse. ePublisher wird Ihrem Unternehmen viel Zeit sparen und sich nahtlos in Ihren Writing Workflow einfügen. So geben Sie Ihren Autoren mehr Zeit, das zu tun, was sie am besten können – schreiben.

Über WebWorks.com.

WebWorks.com, eine Marke der Quadralay Corporation, ist der führende Anbieter für umfassende Lösungen im Bereich Online Publishing und Hilfe System-Erzeugnisse. Die WebWorks Produkte und Leistungen bieten die komplette Single Source-Umgebung für all Ihre ePublishing-Bedürfnisse. Wir spezialisieren uns auf Software zur Konvertierung von Content, die Output in Web-, Online Hilfe-, Wiki- und elektronischen Publikationsformaten erstellt. Unsere ePublisher Plattform kann die Konvertierung von Quelldokumenten in gängige Authoringformate wie DITA-XML, FrameMaker oder Word automatisieren und sie dann in vielfältige Enduserformate wie z.B. Wikis, mobile Geräte, WebWorks Help, HTML, CHM und PDF konvertieren. Unser Konvertierungssystem ist XSL-basiert, so dass Outputformate angepasst oder sogar ganz neu entwickelt werden können.

Über SQUIDDS | People.Products.Passion. e.K.

Ihr Partner für Technische Dokumentation: Produkte + Know-How.