01/08/2011

www.enisa.europa.eu

Web-Sicherheit: EU-Agentur für Cyber-Sicherheit ENISA zeigt Sicherheitsreparaturen für neue Web-Standards auf

Zu einem kritischen Zeitpunkt der Entwicklung von HTML5, dem neuen Kernstandard für das Web, stellt ENISA heute wichtige Sicherheitsreparaturen für 13 anstehende Web-Standards vor. ENISA hat 50 Sicherheitsbedrohungen identifiziert und Vorschläge zu deren Handhabung unterbreitet.

Banking, Social Networking, Shopping, Navigation, Kartenzahlungen und selbst der Umgang mit kritischen Infrastrukturen wie Versorgungsnetzwerken – fast jede Aktivität, die man sich vorstellen kann, findet heute innerhalb eines Browser-Fensters statt. „*Der Web-Browser ist inzwischen eine der am stärksten sicherheitsrelevanten Komponenten unserer Informationsinfrastruktur – ein immer lukrativeres Ziel für Cyberattacken,"* kommentiert Prof. Udo Helmbrecht, Geschäftsführender Direktor von ENISA.

Um Innovationen in Web-Anwendungen und deren Geschäftsmodelle zu unterstützen und das Web für noch mehr Menschen nutzbar zu machen, arbeitet das W3C („World Wide Web Consortium") derzeit an grundlegenden Korrekturen seiner Kernstandards.

ENISA hat diese Gelegenheit dazu genutzt, die Spezifikationen zu überprüfen und Verbesserungsvorschläge hinsichtlich der Browser-Sicherheit aller Nutzer zu machen. „*Bei vielen dieser Spezifikationen gibt es bald kein Zurück mehr. Wir haben ausnahmsweise die Gelegenheit, eingehend über Sicherheit nachzudenken – ehe der Standard unumstößlich wird –, anstatt zu versuchen nachträglich auszubessern. Dies ist eine einmalige Gelegenheit, die Sicherheit schon im Design mit einzuplanen,*" so Giles Hogben, Mitherausgeber des Berichts.

„Wir begrüßen diese sehr frühzeitige Sicherheitsprüfung von ENISA. Wir haben ENISA angehalten, die ermittelten Problematiken den entsprechenden W3C-Arbeitsgruppen mitzuteilen," so Thomas Roessler, Leiter für Versorgungssicherheit bei W3C.

Die ENISA-Analyse zeigt 50 Sicherheitslücken und Probleme wie:

- Ungeschützter Zugriff auf sensible Informationen
- Neue Methoden zum Triggern von Formularübermittlung an Angreifer
- Probleme bei der Bestimmung und Durchführung von Sicherheitsrichtlinien
- Potentielle Unstimmigkeiten bei der Rechteverwaltung des Betriebssystems

- Nicht ausreichend spezifizierte Funktionen, die zu widersprüchlichen oder fehleranfälligen Anwendungen führen können.
- Neue Methoden zum Unterlaufen von Zugangskontrollmechanismen und Schutz vor „Click-Jacking“ (den Nutzer dazu verleiten, gefährliche Links und Schaltflächen anzuklicken)

„Eine wichtige Schlussfolgerung aus dieser Studie lautet, dass in den Spezifikationen, die bereits einer ausführlichen Sicherheitsprüfung unterzogen worden sind, weitaus weniger Sicherheitsprobleme gefunden wurden. Das zeigt den Wert fundierter Sicherheitsprüfungen bei zukünftigen Spezifikationen,“ so Marnix Dekker, Mitherausgeber des Berichts.

Für Hintergrundinformationen: Digital Agenda for Europe, (2.3, Trust and Security).

Für das Gesamtdokument

Dieser Bericht wurde in Englisch verfasst; die vorliegende deutsche Version ist eine Übersetzung des Originals. ENISA hat maßgebliche Schritte unternommen, um die Genauigkeit der Übersetzung zu gewährleisten, aber durch Schwierigkeiten bei der Übertragung können geringfügige Unterschiede zwischen Original und Übersetzung bestehen, und die Übersetzung könnte in Teilen oder insgesamt unpräzise oder inkorrekt sein. Übersetzungen von ENISA-Arbeitsergebnissen werden nur zum Zwecke der Information und Dissemination herausgegeben.

Für Interviews oder weitere Informationen: Ulf Bergstrom, Sprecher von ENISA, press@enisa.europa.eu, Mobil: + 30-6948-460-143, oder Dr. Giles Hogben, Experte von ENISA, giles.hogben@enisa.europa.eu

http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch

Übersetzung. Das Englische Original bleibt die maßgebliche Fassung.