

Sichere Webapplikationen m. Best Practices Compliance – Kosten & Privacy Trends 2011

CONNECT INFORMUNITY

Freitag, 10. Juni 2011
9.00–14.30 Uhr

CHSH Cerha Hempel Spiegelfeld Hlawati
Partnerschaft von Rechtsanwälten
1010 Wien, Dr.-Karl-Lueger-Platz 2

Sichere Webapplikationen

- Internationale und nationale Behandlung von Sicherheitsvorfällen
- Sichere Webapplikationen mit ISO 27001
- Applikationssicherheit im gesamten Entwicklungszyklus mit Hilfe von OpenSAMM und BSIMM

Compliance – Kosten – Privacy Trends 2011

- Privacy Studie von Ernst & Young
- Kosten von Compliance

Referenten: Joachim Brandt (Tripwire), Alfred Heiter (Ernst & Young), Johannes Mariel (Bundesrechenzentrum), Krzysztof Müller (A1 Telekom), Karin Peyerl (Rechtsanwaltskanzlei CHSH) Christian Proschinger (Cert.at), Lucas van Stockhausen (Fortify), **Moderation:** Markus Klemen (SBA Research)



Johannes Mariel

Karin Peyerl

Christian
Proschinger

Lucas van
Stockhausen

Beschränkte Teilnehmerzahl!
Anmeldung erforderlich!
Bei freiem Eintritt für IT-Anwender!

Mit freundlicher Unterstützung von:



Agenda

Sichere Webapplikationen

- 9.00 Internationale und nationale Behandlung von Sicherheitsvorfällen**
Christian Proschinger (CERT.at)
- 9.40 Sichere Webapplikationen**
Johannes Mariel (Bundesrechenzentrum)
- 10.20 Applikationssicherheit im gesamten Entwicklungszyklus**
Lucas van Stockhausen (Fortify)
- 10.50 Pause**

Compliance – Kosten – Privacy Trends 2011

- 11.30 Privacy Studie**
Alfred Heiter (Ernst & Young)
- 11.45 Kosten von Compliance**
Joachim Brandt (Tripwire)
- 12.15 Best Practices**
- 13.00 Podiumsdiskussion zu Compliance, Riskmanagement und sichere Webapplikationen mit Beitrag**
- 13.40 Arbeitnehmerdatenschutz**
Mag. Karin Peyerl (Rechtsanwaltskanzlei CHSH)
- 14.05 Schutz der vertraulichen Daten mit Data Loss Prevention – Praxisbericht**
Krzysztof Müller (A1 Telekom)
- 14.30 Ende der Veranstaltung**

Internationale und nationale Behandlung von Sicherheitsvorfällen

CERT.at ist das österreichische nationale CERT (Computer Emergency Response Team). Als solches ist CERT.at der Ansprechpartner für IT-Sicherheit im nationalen Umfeld. Es vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur, IKT (Informations- und Kommunikationstechnik) und gibt Warnungen, Alerts und Tipps für KMUs (kleine und mittlere Unternehmen) heraus. CERT.at ist eine Initiative von nic.at, der österreichischen Domain-Registry und wird von nic.at gesponsert. Gemeinsam mit dem österreichischen Bundeskanzleramt betreibt CERT.at das GovCERT Austria für die öffentliche Verwaltung und die strategische Informations-Infrastruktur (CIIP) Österreichs. CERT.at und GovCERT Austria nahmen 2008 deren Betrieb auf.



Christian Proschinger
(CERT.at)

Sichere Webapplikationen mit ISO 27001

Das Bundesrechenzentrum als IKT-Dienstleister des Bundes ist gegenwärtig mit zahlreichen herausfordernden Rahmenbedingungen konfrontiert. Zu diesen Rahmenbedingungen zählen die immer mehr werden Verwaltungsanwendungen, die im Internet verfügbar sind und die



Johannes Mariel
(Bundesrechenzentrum)

häufigen Attacken auf IKT-Systeme mit Webanwendungen erfolgen. Es handelt sich dabei um Angriffsszenarien, die eine relativ kleine Anzahl von typischen Softwarefehlern nützt, die durch Information, Schulung und Qualitätssicherung leicht vermeidbar wären. Die gesteckten Ziele des BRZ lauten das Vertrauen der Kunden und Bürger zu gewinnen und eine Compliance zu den gesetzlichen Pflichten zu entwickeln. Um diese Ziele zu erreichen betreibt das BRZ ein Informations-Sicherheits-Management-System (ISMS) nach ISO 27001, das Schwachstellen von unsicheren Codes aufzeigt und Audits über konkrete Schwachstellen hervorbringt.

Applikationssicherheit im gesamten Entwicklungszyklus mit Hilfe von Open-SAMM und BSIMM

Software-Entwickler sind darauf geschult, Code mit guter Funktionalität, Benutzbarkeit und Zuverlässigkeit zu erstellen und konzentrieren sich daher darauf, dass ein Programm das tut, was es tun soll. Das Thema Sicherheit kommt in der Regel zu kurz. So bleiben potentielle Verwundbarkeiten im Code, welche die Applikation zu einem offenen Scheunentor für Angriffe machen, unberücksichtigt. Bei der IT von Firmen und der öffentlichen Hand entsteht heutzutage ein wachsendes Bewusstsein, dass Ihre Software anfällig für Angriffe ist. Deshalb fangen Entwickler, Projekt-Manager wie auch Sicherheits-Teams



Lucas van Stockhausen
(Fortify)

an, sich Gedanken über die Sicherheit Ihrer Anwendungen zu machen. In dieser Diskussion wird aufgezeigt, wie BSIMM und OpenSAMM Ihnen bei dieser Herausforderung helfen können.

Privacy Studie

Lange Zeit ermöglichten die vier Wände eines Büros in Form einer physischen Grenze, Unternehmen die Vertraulichkeit ihrer Daten sicherzustellen. In einer Zeit, in der der Zugriff auf Informationen immer und überall möglich ist, verschwinden diese Grenzen zunehmend. Wir befinden uns mittlerweile

in einer technologiegetriebenen, vernetzten, globalisierten Welt, die neue Herausforderungen für den Schutz der Privatsphäre bietet.

Bereits in einer 2010 durchgeführten Umfrage von Ernst & Young zum Thema IT-Security meinten 81% der befragten Führungskräfte, Datenschutz sei ein kritischer Faktor für ihre Organisation und erhöhen die Investitionen in diesem Bereich. Aber welches sind diesbezüglich die richtigen Investitionen? In Privacy Trends 2011 ist Ernst & Young dieser Frage nachgegangen.



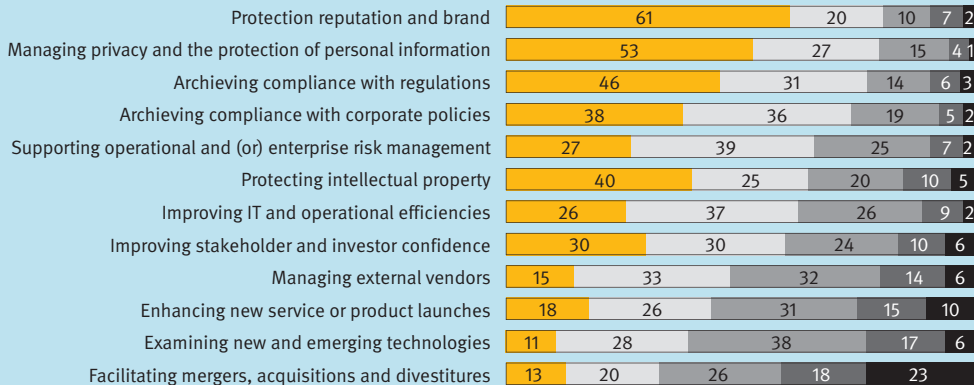
Alfred Heiter (Ernst & Young)

Kosten von Compliance

Joachim Brandt (Tripwire)

Multinationale Unternehmen aller Branchen sind dazu verpflichtet, Datenschutzgesetze, Vorschriften und Richtlinien einzuhalten, die dem Schutz sensibler und vertraulicher Daten einer Einzelperson dienen. Die Einhaltung dieser Gesetze und Richtlinien erfordert die Einführung und Implementierung einer Reihe kostspieliger Aktivitäten hinsichtlich der Durchführung sowie der Mitarbeiter und Technologien. Das Ponemon Institut und Tripwire, Inc. führten eine Studie über »Die tatsächlichen Compliance-Kosten« durch und bestimmten anhand einer repräsentativen Umfrage bei 46 multinationalen Unternehmen die gesamtwirtschaftlichen Auswirkungen der Compliance-Aktivitäten. Ein Ergebnis unserer Studie ist, dass die Kosten für Non-Compliance, die sich durchschnittlich auf 9,4 Millionen USD belaufen, im Vergleich zu den durchschnittlichen Compliance-Kosten von 3,5 Millionen USD sehr viel höher sind.

Regulatory compliance continues to be one of the top priorities for organizations and an important objective of the information security function



Shown: percentage of respondents

Very important 4 3 2 Not important

Quelle: Ernst & Young's 12th annual global information security survey

Secure Coding aus Sicht der Compliance- & Security-Verantwortlichen

Kein Monat ohne gestohlene Kreditkarten- oder Gesundheitsdaten, keine Security-Studie ohne Referenz auf Applikationssicherheit. PCI & Co schreiben uns vor, was uns Dutzende Pressemitteilungen jeden Monat bestätigen. (Web-)Applikationen stellen eines der Toprisiken im Bezug auf unsere externe & interne Informationssicherheit dar. Und so ist jeder CISO oder IT-Leiter angehalten, Schritte in diese Richtung zu setzen. An technischen und

organisatorischen Maßnahmenoptionen mangelt es nicht, jedoch wird die Komplexität der Umsetzung oft unterschätzt. Zwar sind Penetrationstests, Webapplikations-Firewalls usw. wichtige und sinnvolle Mittel, jedoch werden diese meist nur zur Symptombekämpfung benutzt. Der einzig nachhaltige Weg und holistische Ansatz ist deswegen die Etablierung eines sicheren Softwareentwicklungsprozesses und Kultur im Unternehmen. Im Prinzip können die dafür notwendigen Maßnahmen in 4 große Kategorien eingeteilt werden:

- Überwachung und Steuerung der sicheren Softwareentwicklung
- Sicherer Entwicklungsprozess
- Verifikation der Softwaresicherheit
- Deployment

Nur wenn die Informationssicherheit schon von Anfang an in den Entwicklungsprozess einbezogen wird, kann die Qualität und Sicherheit der Software langfristig gesteigert werden. Natürlich können all diese Schritte nicht gleichzeitig und innerhalb weniger Tage umgesetzt werden und verlangen nach entsprechenden zeitlichen und budgetären Ressourcen. Als Belohnung wartet aber nicht nur ein sichereres Endprodukt sondern auch neue Erkenntnisse und Optimierungspotentiale in den Bereichen Sicherheitskultur, Anforderungsanalyse, Entwicklung und Prozesse.

Arbeitnehmerdatenschutz

Welche Rechtsprobleme ergeben sich bei der Internetnutzung von Mitarbeitern im Unternehmen? Der Vortrag zeigt wie mit der Einführung von IT-

Richtlinien und Policies klare Strukturen für die IT-Nutzung in Unternehmen geschaffen werden können. Weiters werden Grenzen im Bereich der Kontrolle und Überwachung von Mitarbeitern bei der Nutzung neuer Medien aufgezeigt und anhand praxisnaher Fälle erläutert.



Mag. Karin Peyer
(Rechtsanwaltskanzlei CHSH)

Schutz der vertraulichen Daten mit Data Loss Prevention – Praxisbericht

Die Presseberichte über Datenverluste sensibilisieren die Öffentlichkeit. Der Gesetzesgeber verpflichtet die Firmen zu mehr Schutz der Daten. Durch neue Arbeitsmethoden (Mobilität der Mitarbeiter) steigt das Risiko des Datenverlustes. Firmen stehen also vor einer neuen großen Herausforderung und müssen andere Methoden finden, um den Schutz der Daten zu gewährleisten. Eine der dafür geeigneten Technologien ist Data Loss Prevention (DLP). Im Gegensatz zu den herkömmlichen Maßnahmen, die eher auf den Schutz der IT-Infrastruktur fokussiert sind, konzentriert sich DLP vollkommen auf die Daten und hilft den erforderlichen Sicherheitslevel zu etablieren.



Krzysztof Müller
(AI Telekom)

Webanwendungen sicher entwickeln – Secure Coding I+II

Referent: Severin Winkler (SBA Research gGmbH)

27.–28. Juni 2011, CON•ECT Eventcenter

Alle Infos unter diesem Link: http://www.conect.at/de/conect_eventmanagement/veranstaltungen.html

An
CON•ECT Eventmanagement
1070 Wien, Kaiserstraße 14/2
Tel.: +43 / 1 / 522 36 36-36
Fax: +43 / 1 / 522 36 36-10
E-Mail: registration@conect.at
<http://www.conect.at>

Zielgruppe:

Geschäftsführer, Unternehmensleitung, Sicherheitsverantwortliche, IT-Leiter, IT-Vorstand, IT-Entscheider, IT-Verantwortliche, Projektverantwortliche, Prozessverantwortliche, Verantwortliche für Marketing, Sales und Human Resources von großen Unternehmen wie etwa Finanzdienstleister, IT & Telekom oder öffentliche Verwaltung & Gemeinwirtschaft sowie Consultants, Softwarehäuser und Vertreter von Medien und Wissenschaft.

ANMELDUNG: Nach Erhalt Ihrer Anmeldung senden wir Ihnen eine Anmeldebestätigung. Diese Anmeldebestätigung ist für eine Teilnahme am Event erforderlich.

STORNIERUNG: Sollten Sie sich für die Veranstaltung anmelden und nicht teilnehmen können, bitten wir um schriftliche Stornierung bis 2 Werktagen vor Veranstaltungsbeginn. Danach bzw. bei Nichterscheinen stellen wir eine Bear-

beitungsgebühr in Höhe von € 50,- in Rechnung. Selbstverständlich ist die Nennung eines Ersatzteilnehmers möglich.

ADRESSÄNDERUNGEN: Wenn Sie das Unternehmen wechseln oder wenn wir Personen anschreiben, die nicht mehr in Ihrem Unternehmen tätig sind, teilen Sie uns diese Änderungen bitte mit. Nur so können wir Sie gezielt über unser Veranstaltungsprogramm informieren.

Anmeldung

CON•ECT
EVENTMANAGEMENT

- Ich melde mich zu »Compliance, Riskmanagement und sichere Webapplikationen« am 10. Juni 2011 an:
 - Als IT-Anwender aus Wirtschaft und öffentlicher Verwaltung kostenfrei
 - Als IT-Anbieter/-Berater zu € 390,- (zuzügl. 20 % MwSt.)
- Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder Post übermittelt bekommen.

Firma:

Titel:

Vorname:

Nachname:

Funktion:

Straße:

PLZ:

Ort:

Telefon:

Fax:

E-Mail:

Datum:

Unterschrift/Firmenstempel:

- Ich erkläre mich mit der elektronischen Verwaltung meiner ausgefüllten Daten und der Nennung meines Namens im Teilnehmerverzeichnis einverstanden.
- Ich bin mit der Zusendung von Veranstaltungsinformationen per E-Mail einverstanden.
(Nichtzutreffendes bitte streichen)