

Security & Risk-Management

CON●ECT
INFORMUNITY



Dienstag, 4. Oktober 2011
9.00–13.15 Uhr

Haus der Industrie, Europasaal
1010 Wien, Schwarzenbergplatz 4

- Data Loss Prevention
- Anti-Leaking-Strategien
- Privacy Trends
- Compliance & Riskmanagement
- Cloud Computing & Security
- Standards ISO 27005 u. a.
- Mobile & Voice-Security, E-Mail-Security
- Endgerätesicherheit & Single Sign On
- Sicherheit von Web-Applikationen
- Sichere Softwareentwicklung
- Datensicherheit
- Best Practices vom Flughafen Nürnberg u. a.

Referenten:

Joachim Brandt (tripwire)
Clemens Cap (Universität Rostock)
RA Dr. Markus Frank
Edgar Weippl (SBA Research)
Jörg Ziegler (Airport Nürnberg GmbH)

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

Mit freundlicher
Unterstützung von:



secure
sba-research.org



Agenda

8.45 Registration

9.00 IT-Security am Airport Nürnberg

Jörg Ziegler (Airport Nürnberg GmbH)

9.50 Daten: Zwischen Leaks und Vertraulichkeit

Clemens Cap (Universität Rostock)

10.50 Integrierte Security-Controls für die transparente, intelligente und automatisierte Sicherheit von IT-Infrastrukturen

Joachim Brandt (tripwire)

11.30 Pause

12.00 Haftung bei Datenpannen: Haftungsminimierung durch eine ISO-27001-Zertifizierung

RA Dr. Markus Frank

12.45 Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space

Edgar Weipl (SBA Research)

13.15 Ende der Veranstaltung

Viele neue Begriffe der IT machen eines klar: die IT ist heute in den meisten Unternehmen eng mit dem Geschäftserfolg verbunden. Sicherheit der IT ist kein rein technisches Thema mehr, sie ist ein geschäftsrelevanter Aspekt geworden. IT-Entscheidungsträger sind Business Manager. Ausdrücke wie IT-Governance bringen diese Verantwortung klar zur Geltung.

Bis zum Jahr 2012 werden laut dem IT-Marktforschungs- und Beratungsunternehmen Gartner 60 Prozent der virtualisierten Server weniger sicher sein als die physikalischen Server, die von diesen ersetzt wurden. Auch wenn diese Zahl bis zum Jahr 2015 auf 30 Prozent sinken wird, warnen die Analysten, dass viele Virtualisierungsprojekte durchgeführt werden, ohne die Verantwortlichen für Informationssicherheit bereits in der frühen Planungsphase einzubeziehen.

IT-Security am Airport Nürnberg

IT-Security wurde als ganzheitlicher Prozess für den IT-Betrieb sowie IT-Neuprojektierungen eingeführt und in das IT-Service-management integriert. So gibt es ein enges Zusammenspiel zwischen den Anforderungen an die Systemverfügbarkeiten aus dem SLA-Management, den tatsächlichen und mittels Systemmanagement-Komponenten überwachten Verfügbarkeiten sowie den Sicherheitsanforderungen im IT-Security-Management selbst. Ziel des IT-Security-Managements ist es, den operativen Betrieb optimal zu unterstüt-



Jörg Ziegler (Airport Nürnberg GmbH)

zen und aufrechtzuerhalten. Zur Erreichung dieses Ziels werden verschiedenste organisatorische und technische Maßnahmen in der IT eingesetzt.

Daten: Zwischen Leaks und Vertraulichkeit

Die Verbreitung von Daten wird aus unterschiedlichen Perspektiven ein immer ernsteres Thema. Die Grenze zwischen Transparenz, Informations-Freiheit und Whistle-Blowing auf der einen Seite sowie Vertraulichkeit auf der anderen Seite ist begrifflich schwer zu ziehen. Der Vortrag gibt einen Überblick über technische Möglichkeiten, Leaks zu vermeiden sowie als Whistle-Blower unentdeckt zu bleiben.



Clemens Cap (Universität Rostock)

Integrierte Security-Controls für die transparente, intelligente und automatisierte Sicherheit von IT-Infrastrukturen

Bestehende Sicherheitslösungen sind oft gegen Cyber-Attacken machtlos, es sei denn, sie werden auf intelligente Weise verknüpft. Dazu sind vor allem neue Ansätze im Unternehmen notwendig, die die vorhandenen Systeme optimal ausnutzen und durch Korrelation mehr als die Summe der Einzelinformationen schaffen. Erfahren Sie von Joachim Brandt, warum IT-Security-Con-



Joachim Brandt (tripwire)

trols und digitale Forensik so wichtig sind bzw. immer wichtiger werden. Er stellt die erfolgskritischen 20 Sicherheitskontrollen vor und erklärt, wie diese einfach implementiert werden. IT- und Sicherheits-Verantwortliche erfahren, wie sie so ihr Leben leichter machen.

Haftung bei Datenpannen: Haftungsminimierung durch eine ISO-27001-Zertifizierung

Informationssicherheitssysteme beugen Datenpannen vor und verringern die Erfolgsaussichten von kriminellen Attacken. Die Legal Compliance einer Organisation verlangt neben der Beachtung der Gesetze auch die Einhaltung von anerkannten Normen und Standards. Denn bei Schadensersatzklagen und in Strafverfahren wird gerichtlich geprüft, ob das Unternehmen in Bezug auf die Informationssicherheit »nach dem Stand der Technik« und mit »angemessener Sorgfalt« gearbeitet hat, was häufig für den Prozessausgang entscheidend ist. In seinem Vortrag zeigt Rechtsanwalt Dr. Markus Frank, welche rechtliche Bedeutung der Zertifizierung eines Informationssicherheitssystems nach ISO 27001 zukommt und wie eine normkonforme Dokumentation die entscheidenden Beweise liefern kann. Ein geprüftes System für Informationssicherheit trägt also zur Schadens- und Haftungsminimierung im Unternehmen bei – aber auch im Management. Denn letzteres haftet seinem Unternehmen und unter Umständen sogar Dritten gegenüber bei Schäden, wenn kein gesetz-



RA Dr. Markus Frank

lich vorgeschriebenes IT-Sicherheitssystem (z. B. § 14 DSGVO) eingerichtet wurde.

Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space

Edgar Weippl (SBA Research)

During the past few years, a vast number of online file storage services have been introduced. While several of these services provide basic functionality such as uploading and retrieving files by a specific user, more advanced services offer features such as shared folders, real-time collaboration, minimization of data transfers or unlimited storage space. Within this talk we give an overview of existing file storage services and examine Dropbox, an advanced file storage solution, in depth. We analyze the Dropbox client software as well as its transmission protocol, show weaknesses and outline possible attack vectors against users. Based on our results we show that Dropbox is used to store copyright-protected files from a popular filesharing network. Furthermore Dropbox can be exploited to hide files in the cloud with unlimited storage capacity. We define this as online slack space. We conclude by discussing security improvements for modern online storage services in general and Dropbox in particular. To prevent our attacks cloud storage operators should employ data possession proofs on clients, a technique which has been recently discussed only in the context of assessing trust in cloud storage operators.

Seminar in Zusammenarbeit mit SBA Research gGmbH

Webanwendungen sicher entwickeln – Secure Coding I

Referenten: **Ulrich Bayer, Severin Winkler**
(SBA Research gGmbH)

Der Kurs behandelt die typischen und gefährlichsten Sicherheitsschwachstellen in modernen Webapplikationen. Behandelt werden unter anderem die OWASP Top Ten 2010, die laut der Organisation OWASP risikoreichsten zehn Sicherheitsschwachstellen in Webapplikationen.

Inhalt des Seminars

- Information Disclosure
- Cross-Site-Scripting
- SQL-Injections
- OS Command Injections
- Session Hijacking
- Session Authentication
- Cross-Site Request Forgery
- Unzureichende Sicherheitskonfiguration
- Unsichere Speicherung sensibler Informationen
- Unzureichende Rechteüberprüfung auf URLs
- Unzureichender Schutz auf der Transportschicht
- Open Redirects

Der Kursinhalt ist dabei unabhängig von einer bestimmten Programmiersprache, da sich die Angriffsszenarien für alle modernen Webapplikationen ähneln. Sicherheitsschwachstellen, die nur in systemnahen Code (C/C++) zu finden sind, wie zum Beispiel Buffer Overflows, Integer Overflows,

Format String Vulnerabilities werden in diesem Kurs nicht behandelt. Codebeispiele im Kurs sind in PHP, JAVA oder Pseudocode gehalten.

Kursziele

Der Kurs richtet sich an Entwickler von Webapplikationen ohne besondere Vorkenntnisse in der sicheren Entwicklung. Ziel ist es, die Entwickler über die häufigsten und gefährlichsten Programmierfehler bei der Entwicklung von Webanwendungen zu unterrichten.

Über die reine Vermittlung von Wissen hinaus steht das Schärfen des Sicherheitsbewusstseins der Entwickler im Mittelpunkt. Die theoretischen Konzepte des Kurses werden durch viele Live-Demos praktisch veranschaulicht. Dies gewährt Einblicke in die Arbeitsweise eines typischen Hackers, zeigt, wie einfach sich gewisse Angriffe dank ausgereifter Hackingtools realisieren lassen und zeigt die oft unterschätzten tatsächlichen Auswirkungen von Sicherheitslücken. Ziel ist es, die Entwickler von der Notwendigkeit eines sicheren Programmierstils zu überzeugen und ein Bewusstsein zu schaffen, das die Softwaresicherheit unabhängig von gerade aktuellen und im Kurs erläuterten Angriffsmethoden erhöht.

Referenten

Ulrich Bayer arbeitet als Senior Security Analyst bei SBA Research gGmbH und ist dort unter anderem für die Durchführung von Sicherheitsüberprüfungen sowie das Abhalten von Security-Schulungen verantwortlich. Davor arbeitete er als Projektassistent auf der TU Wien und forschte und programmierte auf dem Gebiet der Malware-Analyse.



Mag. Severin Winkler (CISSP, CEH, MCITP) hat langjährige Erfahrung in der Durchführung organisatorischer und technischer Sicherheitsaudits sowie der Einführung sichererer Entwicklungsmethoden in Softwareteams. Ebenfalls zu seinem Kerngebiet zählt die statische Source Code Analyse und die Durchführung von Design- und Architekturreviews. Durch die Abhaltung zahlreicher Workshops, Schulungen und eine Lehrtätigkeit an der FH Campus Wien zählt die Vermittlung von sicherheitsrelevantem Wissen zu seinen Kernkompetenzen.



Seminar in Zusammenarbeit mit SBA Research gGmbH

Webanwendungen sicher entwickeln – Secure Coding II

Referenten: Ulrich Bayer, Severin Winkler
(SBA Research gGmbH)

Der Kurs behandelt fortgeschrittene Sicherheitsthemen bei der Entwicklung von modernen Webapplikationen. Der Fokus liegt dabei auf aktuellen Angriffen inklusive möglicher Gegenmaßnahmen.

Inhalt des Seminars

- Sicherer Fileupload
- SSL-Angriffe, Gegenmaßnahmen
- Clickjacking
- Passwörter sicher speichern
- Ajax Security
- Advanced Cross-Site Scripting/Malicious Javascript
- Command & Control mit Javascript
- CSS History Hack
- Data URI
- Sicherheitskonzepte/Sichere Architektur

Der Kursinhalt ist dabei unabhängig von einer bestimmten Programmiersprache, da sich die Angriffsszenarien für alle modernen Webapplikationen ähneln. Sicherheitsschwachstellen, die nur in systemnahen Code (C/C++) zu finden sind, wie zum Beispiel Buffer Overflows, Integer Overflows, Format String Vulnerabilities werden in diesem Kurs nicht behandelt. Codebeispiele im Kurs sind in PHP, JAVA oder Pseudocode gehalten.

Kursziele

Ziel ist es die Entwickler über fortgeschrittene Themen bei der sicheren Entwicklung von Webanwendungen zu unterrichten. Im Vordergrund stehen aktuelle und noch weniger verbreitete Angriffe mit denen Webapplikationen in naher Zukunft zu rechnen haben. Die theoretischen Konzepte des Kurses werden durch viele Live-Demos praktisch veranschaulicht. Es sollen dadurch die Auswirkungen von Sicherheitslücken demonstriert werden. Gleichzeitig soll bei den Programmierern Verständnis für die Notwendigkeit und Sinnhaftigkeit der bereits bekannten Sicherheitsmaßnahmen geschaffen werden. Beispielsweise werden Cross-Site-Scripting-Attacks oft zu Unrecht unterschätzt.

Der Kurs richtet sich an Entwickler von Webapplikationen, die in Java, PHP, .NET, etc. programmieren, und bereits Vorwissen im Bereich der sicheren Entwicklung besitzen. Das Vorwissen stammt beispielweise von einem Besuch des »WEBANWENDUNGEN SICHER ENTWICKELN« Kurses oder anderen Security Workshops. Es wird erwartet, dass Teilnehmer die OWASP Top Ten und typische Sicherheitsschwachstellen wie SQL-Injections oder Cross-Site-Scripting bereits kennen.

Webanwendungen sicher entwickeln – Kombikurs Secure Coding I + II

Dieser Kurs ist eine Kombination der beiden Kursangebote »Webanwendungen sicher entwickeln« und »Webanwendungen sicher entwickeln für Fortgeschrittene«, der durch die Abstimmung der Inhalte besonders flexibel den Bedürfnissen der Teilnehmer angepasst werden kann. Die genauen Inhalte sind den jeweiligen Kursangeboten zu entnehmen.

Termin: 8./9. Dezember 2011

Ort: CON•ECT Eventcenter, 1070 Wien

Gebühr: Standard: € 1.290,-
Ermäßigt: € 1.200,- für SBA-Mitarbeiter und Mitglieder des Future Network sowie asf-Mitglieder

Alle Preise zuzüglich 20 % MwSt.

Weitere Informationen und Anmeldung unter
www.conect.at

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: Unternehmensleitung, Sicherheitsverantwortliche, IT-Vorstand, IT-Entscheider, IT-Verantwortliche sowie 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 Werktage vor Veranstaltungsbeginn. Danach bzw. bei Nichterscheinen stellen wir eine Bearbeitungs-

gebühr 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

- Ich melde mich zu »Security & Risk-Management« am 4. 10. 11 kostenfrei an.
- Ich möchte in Zukunft weitere 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)