

IT-Security-Day Kiel 2010

Die Informations- und Kommunikationstechnologien sind das zentrale Nervensystem eines jeden Unternehmens. Gleichzeitig ist die IT die kritischste Infrastruktur: In den letzten Jahren ist eine zunehmende Professionalisierung der Angriffe sowie der eingesetzten Schadprogramme und Werkzeuge zu beobachten; das Thema Wirtschaftsspionage wird immer relevanter. Hier setzt der 1. IT-Security-Day Kiel an und informiert zu den neusten Bedrohungsszenarien und Schutzmechanismen. Die Optimierung des unternehmensinternen Sicherheitsmanagement, der Schutz von Web Services in Service-orientierten Architekturen und das aktuelle Thema Mobile Security sind Themen des Nachmittags. Das besondere Highlight: ein Live-Hacking von iPhone, Blackberry & Co.

Datum

16. September 2010

Uhrzeit

14.45 bis 18.30 Uhr

Ort

Konferenzzentrum Hafenhäuser Kiel
Bollhörnkai 1, 24103 Kiel
www.port-of-kiel.com

Agenda

- | | |
|-----------|---|
| 14.45 Uhr | Empfang |
| 15.00 Uhr | Grußwort & Moderation
Nina Prigge, Projektleiterin Clustermanagement DiWiSH |
| 15.05 Uhr | Keynote „360° IT-Security“, Dr. André Hojka, Vater Solution GmbH |
| 15.50 Uhr | Fachvortrag “Schutz von Web Services in Service-orientierten Architekturen”,
Prof. Dr. Norbert Luttenberger, Institut für Informatik der Christian-Albrechts-
Universität zu Kiel |
| 16.20 Uhr | Kaffeepause |
| 16.30 Uhr | Live-Demonstration: Angriffsszenarien auf mobile Dienste – Wie (un)sicher
sind Laptop, iPhone, Blackberry & Co.?
Marco Di Filippo, Compass Security AG |
| 17.30 Uhr | Fachvortrag “Dieses Spiel kann man nicht gewinnen – Sicherheit mobiler
Nutzer“
Martin Seeger, NetUSE AG |
| 18.00 Uhr | Ausklang bei einem Abendbuffet |

Anmeldung

Da die Teilnehmerzahl begrenzt ist, bitten wir Sie, sich bis zum 9. September 2010 telefonisch, per E-Mail oder mit beiliegender Faxantwort anzumelden.

Clustermanagement DiWiSH, Frau Kubovcsik
Tel 0431.666 66 859, mail@diwish.de

Abstracts

360° IT-Security

Referent: André Hojka, Vater Solution GmbH

Ist die Bedrohungslage für Informationssicherheit ein Fall von Paranoia oder real? Zunehmende Datenpannen und damit drohender Imageverlust sowie grenzübergreifende Wirtschaftsspionage zwingen immer mehr Unternehmen ihre Sicherheitsstrukturen und -prozesse zu überdenken. Fragestellungen zum physischen und technischen Perimeterschutz, Zugriff auf Unternehmensdaten, Umgang mit Sicherheitsvorfällen sowie angemessenen Berechtigungsstrukturen sind häufig Anlass, sich um eine angepasste Informationssicherheitsstrategie Gedanken zu machen.

Die Optimierung des unternehmensinternen Sicherheitsmanagements führt oft vom reinen Grundschutzansatz zur risikoorientierten Steuerung. Die notwendige Risikoanalyse schafft die Möglichkeit die identifizierten Risiken innerhalb oder außerhalb des unternehmensspezifischen Toleranzbereichs zuzuordnen und damit eine zielgerichtete Risikominimierung und verlässliche Budgetsteuerung zu erreichen. Mittels definierter Risikokennzahlen wird ein transparentes Berichtswesen zur Lage der Informationssicherheit im Unternehmen geschaffen, welches die Weiterentwicklung, sowie das rechtzeitige Gegensteuern bei Fehlentwicklungen der Informationssicherheit ermöglicht.

Der Vortrag beschreibt Lösungsansätze, wie knappe IT-Sicherheitsressourcen sinnvoll einzusetzen sind.

Schutz von Web Services in Service-orientierten Architekturen

Referent: Prof. Dr.-Ing. Norbert Luttenberger, Leiter der Arbeitsgruppe Kommunikationssysteme im Institut für Informatik der Christian-Albrechts-Universität zu Kiel

Web Services bilden die Infrastruktur in den meisten modernen Service-orientierten Architekturen (SOAs). Der Vortrag diskutiert zunächst die neuartigen Verwundbarkeiten, die Web Services (WS) insbesondere dadurch aufweisen, dass die Verarbeitung von XML-codierten Nachrichten oftmals sehr hohen Speicher- und Rechenaufwand erfordert.

Damit Web Services verlässlich genutzt werden können, sollten sie deshalb vor nicht regelkonformen Anfragen geschützt werden, damit u. a. also auch vor Anfragen, die ihre Ursache in gezielten Angriffen haben. Es wird vorgeschlagen, die Verlässlichkeit von Web Services durch eine effiziente dreiteilige Validierung von WS-Nachrichten zu steigern: WS-Nachrichten werden dazu vor der Verarbeitung durch den Web Service Server syntaktisch validiert, WS-Nachrichten werden gegen ein zugehöriges Sicherheitsregelwerk (security policy) validiert, und innerhalb einer Komposition von Web Services wird überprüft, ob eine korrekte Nachrichtenabfolge eingehalten wird. Es wird gezeigt, wie entsprechende Validierungsregeln automatisch aus den mit einem Web Service verbundenen Meta-Informationen generiert werden können, und wie die Effizienz der Validierung durch die durchgängige Verwendung des sog. ereignisbasierten Nachrichtenverarbeitungsmodells (event-based message parsing and processing) erreicht wird. Der Vortrag schließt mit der Vorstellung ausgewählter WS-Firewall-Systeme.

Live-Demonstration: Angriffsszenarien auf mobile Dienste – Wie (un)sicher sind Laptop, iPhone, Blackberry & Co.?

Referent: Marco Di Filippo, Regional Director Germany, Compass Security AG

Mobile Security warum? Betrifft mich das? Ich bin doch nicht so wichtig! - Laptop, iPhone, Blackberry & Co. sind heute und morgen die Kommunikationsmittel, die uns überall hin begleiten und offen wie ein Scheunentor sind. Ohne Mobiltelefon fühlt man sich nicht komplett. Die Funktionsvielfalt der Smartphones nimmt rasant zu und die Möglichkeiten sind fast unbegrenzt. Was vertrauen wir ihnen nicht alles an: Kontaktdaten, Termine, vertrauliche Nachrichten, (intime) Bilder, Zugangsdaten für Konten, usw. Jeder der ein wenig technisch versiert ist, kann den Standort des Handy's ermitteln, fremde SMS-Nachrichten lesen, es als Gateway benutzen und sogar Gespräche belauschen.

Anhand von unterschiedlichen Szenarien wie SAT (Application Toolkits), Early Media Angriffe (Freizeichentöne), Call-ID-Spoofing, abhören von Nachrichten, mit lauschen von Gesprächen und Daten, Ortung, Handy Trojanern, Bluetooth- und WLAN-Hacking werden im Workshop verschiedene Angriffsszenarien erläutert und demonstriert. Ergänzt werden diese durch Erfahrungsberichte aus verschiedenen Feldversuchen.

„Dieses Spiel kann man nicht gewinnen“ – Sicherheit mobiler Nutzer

Referent: Martin Seeger, Gesellschafter NetUSE AG

Wer sich mit der Sicherheit mobiler Benutzer beschäftigt, hat das Gefühl, das "Spiel" nicht gewinnen zu können. Den Benutzern ist die einfache Bedienbarkeit wichtiger als die eigene Sicherheit; die finanziellen Vorgaben schließen allzu kostspielige Lösungen aus. Dieser Vortrag soll die Optionen darstellen, die Unternehmen in diesem Spannungsfeld haben, und wie Firmen sich ihre individuelle IT-Sicherheitsstrategie erarbeiten und Risiken minimieren können.

IT-Security-Day Kiel 2010

Faxantwort: 0431.666 66 769

Zu der Veranstaltung „**IT-Security-Day Kiel**“ am 16. September 2010 um 14.45 Uhr im Konferenzzentrum Hafenhäus (Bollhörnkai 1, 24103 Kiel) melde ich folgende Personen an:

Name(n) _____

Telefon _____

E-Mail _____

Firma/Institution _____

Adresse _____

"Ich bin / wir sind damit einverstanden, dass meine / unsere Angaben WTSH-intern in automatisierten Verfahren verarbeitet, genutzt und auf einer Teilnehmerliste veröffentlicht werden (§4 BDSG)."

Unterschrift (ggf. Firmenstempel)