

Security Research Newsletter 1/2010

- Auf zu neuen Höhen

Neue Technologien, wie beispielsweise der kontinuierliche Aufschwung von Cloud Computing und Virtualisierung, bieten Ihnen 2010 noch mehr Möglichkeiten, Schwung in Ihr Unternehmen zu bringen und gleichzeitig die Effektivität und Effizienz Ihrer Prozesse zu steigern. Eine angemessene Technologiebewertung erfordert jedenfalls die Gegenüberstellung von Risiken und Chancen.

Wir freuen uns darauf, Sie auch dieses Jahr mit unserem 25 köpfigen Team bei Ihrem Aufstieg zu neuen Höhen absichern zu können!

Security Research - Meet the Experts!

An folgenden Terminen können Sie direkt mit Experten von Security Research über Themen wie z.B. Virtualisierungs- & Cloud Security, Security & Code Audits, ISMS und Security Governance diskutieren. Im Folgenden sehen Sie eine Übersicht unserer nächsten Termine.

Microsoft Big Days - 18.03., Graz & 23.03., Wien

Die Microsoft Big Days sind auch in diesem Jahr das Premium Event von Microsoft in Österreich. Nutzen Sie die Chance und erleben Sie neue Technologie und ihre Einsatzmöglichkeiten.

Im Rahmen unseres Standes in Wien & Graz haben Sie die Möglichkeit, alles zu den Themen Security in Microsoft Infrastrukturen & Online Services, Secure Coding & Development sowie SharePoint 2010 zu erfahren.

Mehr dazu unter: <http://www.microsoft.com/austria/events/bigdays2010/>

Big Days Aktion

Nutzen Sie die kostenlose Möglichkeit, auf den Big Days die Sicherheit Ihres Clients & oder ein erstes Code Security Audit durchführen zu lassen. Wir zeigen Ihnen in Echtzeit Schwachstellen in Ihrem Code oder in Ihrer Infrastruktur und stehen mit Lösungsvorschlägen zur Seite. Anmeldungen zu dieser Aktion bitte direkt an bigdays@securityresearch.at

L.S.Z - Security & Risk-Management-Kongress 2010, 16. und 17. März, Waidhofen/Ybbs

Der L.S.Z Security-Kongress ist ein herausragendes Event von L.S.Z Consulting und kommt dem unmittelbaren Informations- und Erfahrungsaustausch von IT-Managern, Sicherheitsverantwortlichen und Anbietern entgegen. Die Teilnehmer sind aufgefordert, ihr Fachwissen in den Arbeitsgruppen sowie Diskussionen nach dem Open Space-Prinzip einzubringen.

Mehr dazu unter: http://www.lsz-consulting.at/veranstaltungen/event/lsz_security2010/index.htm

ConhIT – Der Branchentreff für Healthcare IT, 20.-22. April, Berlin

Die ConhIT-Industrie-Messe bietet dem Besucher eine umfassende Präsentation der Healthcare-IT. Etablierte Lösungen, neueste Technologien und zukünftige Entwicklungen werden auf hohem Niveau ausgestellt.

Mehr dazu unter: <http://www.conhit.de/>

6. Information-Security-Symposium, 14. April, Wien, 13.30-19.00 h / Open End

Secure Your Business: Vorsprung durch ISO-Standardisierung. Lernen Sie wie Sie auf Basis von Microsoft SharePoint Ihr ISMS implementieren und optimieren können und sich auf zukünftige ISO 27001 Audits vorbereiten.

Mehr dazu unter: <http://at.cis-cert.com/Pages/de/Galerie/Programm-2010.aspx>

Forensik Workshop: Speicheranalyse mit Andreas Schuster

Andreas Schuster wird am 22. und 23. April, 2010 einen 2-tägigen Forensik Spezialworkshop zum Thema Speicheranalyse halten. Folgende Themen werden schwerpunktmäßig behandelt: Intel x86 Hardware Plattform, Random Access Memory (RAM) Adressierungsarten, Forensische Sicherung des Arbeitsspeichers, Methoden und Werkzeuge, Architektur des Microsoft Windows Betriebssystemkerns, Windows Speicherwaltungs-Objekte des Betriebssystemkerns, Analysetechniken, Einsatz des Microsoft Debuggers und des Volatility Frameworks sowie Übungen an Speicherabbildern. Weiterführende Informationen und Informationen zur Anmeldung finden Sie auf unserer Homepage.

Mehr dazu unter:

<http://www.securityresearch.at/en/2010/02/24/forensik-workshop-speicheranalyse-mit-andreas-schusterforensik-workshop-speicheranalyse-mit-andreas-schuster/>

CISSP Workshop (03.-07.05) und CISSP Prüfung (08.05) in Wien

Die Prüfung zum CISSP am 08.05.2010 in Wien umfasst 10 Bereiche der Sicherheit, welche für die essentielle Absicherung von Informationssystemen, Unternehmen und nationalen Infrastrukturen notwendig sind. Die Kandidaten bekommen durch diese Zertifizierung ein breites Verständnis für die technischen, organisatorischen und menschlichen Faktoren, welche für eine ganzheitliche Absicherung zusammenspielen müssen.

Security Research bietet dazu einen Vorbereitungskurs mit folgenden Kerndaten an:

- Dauer: 5 Tage
- Sprache: Deutsch (Kursmaterial ist Englisch)
- Format: Vermittlung des Wissens durch Trainer, Umfangreiches Kursmaterial
- Kursmaterial: Shon Harris' all-in-one Kursbuch, Foliensammlung
- Voraussetzungen: Es kann jeder an diesem Kurs teilnehmen, wobei Personen mit Erfahrung im Sicherheitsbereich und solidem technischen Verständnis am meisten von diesem Kurs profitieren werden.

Mehr dazu unter: <http://www.securityresearch.at/is-services/training/>

Anmeldungen an: atomek@securityresearch.at

Produkt News 2010

Microsoft SharePoint 2010

SharePoint 2010 steht vor der Tür. Unser Team hat sich für Sie entsprechend vorbereitet und ist startklar um mit Ihnen auf diese neue Plattform umzusteigen. Ob Migration von SharePoint 2007 oder der Aufbau einer neuen SharePoint 2010 Umgebung, wir unterstützen Sie in Ihren Vorhaben.

Microsoft SharePoint Server 2010 ist die Plattform für die geschäftliche Zusammenarbeit in Unternehmen und im Web, mit der Sie es Ihren Mitarbeitern aufgrund integrierter und umfangreicher Features ermöglichen, in Verbindung zu bleiben und produktiv zu arbeiten.

Unabhängig davon, ob die Bereitstellung vor Ort oder als gehosteter Dienst erfolgt – aufgrund der einheitlichen Infrastruktur können Sie mit SharePoint Server 2010 Kosten senken und schnell auf Unternehmensanforderungen reagieren.

ISMS & Auditplanung mit SharePoint

Unternehmensdokumente wie Policies, Richtlinien und Standards bilden das Rückgrat Ihrer Unternehmensprozesse. Strategieerfüllung und Einhaltung von organisatorischen, technischen und regulativen Anforderungen sollen erreicht werden. Komplimentiert mit Strategie, Kontrollen, Maßnahmen, Audits, Assessments und deren Ergebnissen entsteht ein unternehmensspezifisches Information Security Management System.

Basierend auf der SharePoint-Technologie hat Security Research eine Suite entwickelt mit der sich sämtliche relevanten Unternehmensdokumente veröffentlichen, verwalten und steuern lassen. Um den Anforderungen eines ISMS gerecht zu werden, sind Funktionen wie z.B. Review Workflows und Genehmigungsworkflows nur einige Höhepunkte, die sich in der Suite wieder finden lassen.

Microsoft Forefront UAG & TMG

Das **Microsoft Forefront Unified Access Gateway (UAG)** ermöglicht die Implementierung einer zentralen Remote Access Plattform, sowohl für interne Mitarbeiter als auch für externe Partner.

Das UAG erlaubt eine sichere Bereitstellung unternehmensinterner Dienste wie Outlook Web Access, SharePoint oder Microsoft CRM über ein zentrales Portal und erleichtert die Anwendung durch den Enduser mit Hilfe von Single-Sign-On (SSO) Technologien. Die Fähigkeiten einer Application Layer Firewall sowie die Möglichkeit zur Erhebung des Client Health States runden das Gesamtpaket ab.

Einige der wichtigsten Features:

- Konsolidierung von Online Services in ein gemeinsames Portal mit SSO Unterstützung
- SSL VPN und Direct Access Integration
- End Point Security und Client Health State Assessment (auch für Linux und MAC OS Clients)
- Application Intelligence und Information Leakage Prevention
- NAP und Terminal Services Integration
- Microsoft Forefront Threat Management Gateway

Das **Microsoft Forefront Threat Management Gateway (TMG)** ist eine umfassende Web-Gateway und Perimetersicherheitslösung. Das TMG bietet sowohl die klassischen Funktionen einer Edge Firewall als auch erweiterte Features in den Bereichen Client Sicherheit und

Applikationsbereitstellung. Dazu zählen Features wie URL Filtering, Malware Detection und SSL Inspection.

Außerdem beinhaltet das TMG ein voll ausgerüstetes Network Intrusion Prevention System (NIS), welches Sie rechtzeitig vor externen und internen Bedrohungen warnt.

Zu den wichtigsten Features zählen:

- Network und Application Firewall
- Web Proxy inkl. URL Filtering, Malware Detection und SSL Inspection
- Site to Site und Remote Endpoint VPN (SSTP, PPTP, L2TP)
- Network Intrusion Prevention (NIS) und Network Access Protection (NAP) Support
- ISP-Failover / ISP-Loadbalancing (z.B.: automatischer Failover bei Ausfall eines ISP)
- Preauthentication und Single-Sign-On (SSO) für veröffentlichte Dienste

Microsoft Online Services

Die Microsoft Business Productivity Online Suite umfasst von Microsoft gehostete Lösungen für Messaging und Zusammenarbeit. Exchange Online, SharePoint Online, Office Live Meeting und Office Communications Online sind die Komponenten der Suite. Die Onlinedienste sorgen dafür, dass Ihr Unternehmen optimierte Kommunikationsmöglichkeiten mit hoher Verfügbarkeit, umfassender Sicherheit und vereinfachter IT-Verwaltung nutzen kann. Ihr Unternehmen profitiert von Technologien, die immer auf dem neuesten Stand sind und schnell bereitgestellt werden können, sodass Sie Ihre wertvollen IT-Ressourcen maximieren und die Notwendigkeit von Infrastrukturinvestitionen reduzieren können.

Fortify 360

Zehntausende, hunderttausende, Millionen Zeilen Source Code? Fortify 360 kennt keine Grenzen bei der automatisierten Source Code Überprüfung und zeichnet sich durch Sprachunabhängigkeit, Flexibilität und Qualität aus. Als exklusiver Fortify Partner stehen wir Ihnen als Erstkontakt hinsichtlich qualitativ hochwertiger Source Code Analysen jederzeit zur Verfügung.

Splunk

Sie suchen eine Lösung mit der Sie ihre Loginformationen nach Ihren eigenen Bedürfnissen auswerten können? Ihre Logdaten reichen von wenigen Megabyte hinweg zu mehreren Terrabyte? In diesem Fall ist Splunk die ideale Lösung für Sie. Indizierung jeglicher Daten (Logfiles, Scripts, Konfigurationen, Tickets etc.) und Echtzeitreporting sind nur ein Bruchteil der Vorteile, die sich durch Splunk realisieren lassen. Starten Sie heute noch ein Testprojekt, sie werden erstaunt sein!

Symantec Data Loss Prevention & Control Compliance Suite

Wir sind Ihre zertifizierten Symantec Partner für die Produkte Data Loss Prevention (DLP) und Control Compliance Suite (CCS). Sie suchen eine Möglichkeit Datenströme in Ihrer Infrastruktur zu kontrollieren und Informationsverluste zu verhindern, dann ist DLP genau die richtige Lösung für Sie!

Mit Hilfe der Control Compliance Suite erfahren Sie weitreichende Möglichkeiten sämtliche Unternehmenswerte in Ihrer Infrastruktur zu erfassen und gegen eigene Compliance Anforderungen oder Best Practice Ansätze zu validieren.

Infrastruktur Security Monitoring mit Microsoft SCOM & Splunk

Nachvollziehbarkeit ist eine der essentiellsten Anforderungen an eine ordentlich geführte IT Landschaft. Das Konsolidieren und revisionssichere Aufbewahren von Log-Daten ist demnach eine Basisanforderung an jedes IT System. SCOM & Splunk sind zwei Lösungen, die Log Informationen nicht nur zentralisieren, sondern darüber hinaus die Möglichkeit bieten, diese sinnvoll auszuwerten, um organisatorische Kontrollen darauf aufzusetzen. Erst dadurch ergibt sich ein unternehmerischer Mehrwert.

Dienstleistungs News 2010

Wirtschaftlichkeitsbetrachtung & Sourcing Strategien

Sourcing Strategien müssen bedacht und sorgfältig entschieden werden. Dies beinhaltet die Erhebung funktionaler Faktoren und wirtschaftlicher Größen, die Festlegung von Bewertungsfaktoren, Analysen und Verifikation der Ergebnisse. Wir unterstützen Sie gerne bei der Entwicklung von Sourcing Strategien, Wirtschaftlichkeitsbetrachtungen und bei der Suche von geeigneten Sourcing Partnern.

Business Continuity

Ausfallssicherheit, Redundanz, Fortführung der Unternehmensprozesse im Katastrophenfall sind Ihnen wichtig? Uns auch! Wir begleiten Sie bei der Analyse, Bewertung und Priorisierung der wichtigsten Unternehmensprozesse, bei der Erstellung von BCM und Wiederaufbauplänen als auch beim Testen und der Umsetzung bestehender BCM-Strategien. Im Fokus unseres Teams aus zertifizierten Business Continuity Management Mitarbeiter steht Kosteneffizienz und Wirtschaftlichkeit.

Auf technischer Seite werden Sie von unserem System Enablement Team bei der Umsetzung von BCM-bezogenen Infrastrukturmaßnahmen begleitet.

Audit Vorbereitung

Die Wirtschaftsabschlussprüfung steht an oder der SAS 70 Bericht wird wieder einmal fällig? Unser Team erfahrener IT-Auditoren hilft bei der Vorbereitung auf anstehende Audits und bei der Aufbereitung und Umsetzung geforderten Maßnahmen.

Audits sollten als Bereicherung und nicht als Last gesehen werden. Unsere Audits helfen mögliche Schwachstellen in Ihrer Infrastruktur oder in Ihren Prozessen aufzufinden und können als entscheidungsunterstützend bei der Umsetzung von Maßnahmen gewertet werden. Ob nun organisatorische Betrachtung oder technische Analyse, ein Spezialist der Security Research steht für Sie bereit.

ISMS Begleitung

Das Information Security Management System (ISMS) gilt als das Herzstück Ihrer IT-Governance Bemühungen. Erst durch die Umsetzung eines integrierten und individuellen ISMS erfährt ein Unternehmen jene Kontrolle, (Rechts-)Konformität und Transparenz, die es in einer wettbewerbsfähigen Organisation umzusetzen gilt.

Erfahrene Spezialisten der Security Research begleiten sie bei der Etablierung eines maßgeschneiderten ISMS in Ihrem Unternehmen oder analysieren und optimieren Ihr bestehendes System.

Penetration Tests & Source Code Analyse

Wir überprüfen Ihren Source Code auf höchstem Niveau, dies kann sowohl manuell oder automatisiert z.B. mit Unterstützung von Fortify 360 erfolgen. Source Code Reviews können eigenständig oder im Rahmen einer Web Applikation Penetration stattfinden. Um den technologischen Herausforderungen gerecht zu werden, verwenden Mitarbeiter der Security Research eigens entwickelte Penetration Testing und Web Application Penetration Testing Methodologien.

Impressum & Kontakt

nach § 5 Abs. 1 [ECG \(E-Commerce-Gesetz\)](#)

Firmenname: Security Research Sicherheitsforschung GmbH

Firmensitz: Favoritenstrasse 16, 1040 Wien

Firmenbuchnummer: FN271386 y

Firmenbuchgericht: Handelsgericht Wien

Umsatzsteuer-Identifikationsnummer: ATU62478955

Büroadresse: Sommerpalais Harrach, Favoritenstrasse 16, 2. Stock, 1040 Wien

Anfragen an anfragen@securityresearch.at