Marc Heuse

Senior Consultant – IT Sicherheitsberater

Telefon: +49 (0) 177 9611560

e-Mail: mh@mh-sec.de

Zur Person

Zusammenfassung

- Kommunikativ, teamorientiert, engagiert
- Schnelle Erfassung komplexer Zusammenhänge
- Zielorientiert, pragmatisch
- Verantwortungsbewusst, sorgfältig und genau
- 21 Jahre Erfahrung in IT-Sicherheit
- Projektmanagementerfahrung in Training und Praxis bis 300 MT
- Teamführung Erfahrung (bis 6 Personen, 7 Jahre)
- Sicherheitsdienstleistung qualititätszertifiziert nach ISO 9001:2015
- Sicherheitszertifiziert für TISAX 3.0 hoher Schutzbedarf & Prototypenschutz
- Englisch fließend (business fluent) in Wort und Schrift

Spezialisierung

Tiefes Experten Know-how mit Jahrzehntelanger Erfahrung

IT-Sicherheitsberatung im Bereich von:

- Sicherheitsanalysen und Penetrationstests von komplexen Infrastrukturen (Netzwerke, proprietäre Applikationen, WebApps, WLAN, PABX, etc.)
- Auditing (Betriebssysteme, Netzwerkkomponenten und Applikationskonfigurationen)
- Analyse von Quellcode und Binärprogrammen/Reverse Engineering (Malware Analyse, Sicherheitsrisiken)
- Threat Modelling, Policies und Procedures (Hardening Guidelines, ISO 17799/2700x, IT-GSHB, ITIL) und Risikomanagement (ALE/EAL, CRAMM, etc.)
- Sicherheitsschulungen bis Experten-Level (in den oben genannten Bereichen)
- Spezial Know-how in Automotive Security (CAN, Flexray, LIN, BR-Ethernet, Autosar, SOME/IP, etc.)

IT-Sicherheitsbereiche

- Netzwerk (Firewall, Router, Switche, VPN, Sicherheitsserver wie Webfilter, WAF)
- Unix (Linux, Solaris, AIX, HPUX, Mac OS X, FreeBSD, OpenBSD)
- Windows Server und Desktop
- Programmiersprachen (Assembler, C, C++, Perl, PHP, Shell, Delphi, Pascal, Basic, Javascript, Java, Python, Tcl/Tk)
- Datenbanken (Oracle, MS-SQL, Mysql)
- TCP/IP/IPv6 (inkl. aller üblichen und ungewöhnlichen Protokolle)
- Standards (ISO 17799/BS 7799, ISO 27001++, ISO 13335, ISO 14971/EN 1441, IT Grundschutzhandbuch)
- Risikomanagement und Threat Modelling

Werdegang

Stationen bei Banken Finanzdienstleistungen

Seit 07/2007	Unabhängiger IT-Sicherheitsberater
07/2004 – 06/2007	n.runs AG IT-Security Teamleiter
01/2003 – 06/2004	Unisys GmbH Manager IT-Security Services
01/1999 – 12/2002	KPMG AG Manager/Prokurist, Leiter IT-Security Services
09/1997 – 12/1998	Deutsche Bank AG Firewall Engineer
07/1998 – 12/2006	SuSE/Novell Gründer und Leiter des SuSE Security Teams

Branchenerfahrung

Breite Branchenkenntnis

- Automotive
- Banken
- Telekommunikation
- Versicherungen
- Öffentliche Institutionen

Projekte (Auszug)

Breite Projekterfahrung im IT-Security Umfeld

- Weltweit führender Autohersteller – Komplexe Sicherheitsanalysen der IT in kommenden Autogenerationen sowie dazugehörigen Front- und Backend Infrastrukturen

- UNO Institution – Verdeckter Penetrationstest des internen Netzwerk inkl. physischer Angriffe
- Einer der größten Einzelhändler Europas: Internationale interne und externe Penetrationstests (Europa, Asien)
- Eine Zentralbank – Sicherheitsexperte für Design und Abnahme der kompletten neuen Firewall Infrastruktur
- International führender Mobilfunkprovider – Sicherheitsüberprüfung des neuen Kunden Webmail Systems (Web, SMTP, POP3) und regelmäße Überprüfung der Änderungen
- Deutsche öffentliche Institution – Sicherheitsüberprüfung der Firewall Umgebung (Penetrationstest, Konfigurationsprüfung, Prozessprüfung)
- Mehrere europäische Zentralbanken – IT-Sicherheits-überprüfung einer zentralen Vernetzungsschnittstelle (Penetrationstests und Konfigurationsreview)
- UNO Institution – Organisationsabgleich gegenüber ISO 27001++

Publikationen

- C't 11/13 und iX Sonderheft 4/13 – Sicherheitsüberprüfung von IPv6 Firewalls
- C't 16/11 – "Safer Six"
- Der Standard 01/2011 - "IPv6 ein Security Albtraum?"
- SuSE - Installation of a secure SuSE Linux Enterprise Server 8 and 9
- SuSE - Installation of a secure web server
- Computerwoche Extra 5/2001 – "Irgendwo ist immer eine Lücke"
- C't 26/00 – "Authentifizierung unter Linux mit PAM"

Konferenzen

- Keynote Speaker: HES 04/12, Paris; H2HC 10/2012, Brasilien; PHDays III 05/2013 Moskau, Cybercamp 12/2014, Madrid; Mundo Hacker Day 04/2015, Madrid; Navaja Negra V 10/2015, Albacete
- Heise IT-Security Konferenzen 2011 (zu den Themen IPv6 Sicherheit und DNSSEC)
- Hiding in Complexity: GSEC 10/2015, Singapur
- IPv6 Insecurity Revolutions: HITB 10/2012, Malaysia; H2HC 10/2012, Brasilien; SecurityZone 12/12, Kolumbien
- IPv6 Security revisited: Deepsec 11/2010, Wien; CCC Congress 12/2010, Berlin; IPv6 Kongress 2011, Frankfurt
- IPv6 Security: Pacsec 11/2005, Tokyo; CCC Congress 12/2005, Berlin; Eusecwest 02/2006, London; Cansecwest

04/2006, Vancouver; Hack in the Box 09/2006, Kuala Lumpur; Hack LU 10/2006, Luxemburg; VNSec 08/2007, Saigon

- Euroforum - Sicherheit 2003, 11/2003, Hamburg, Präsentation “Gefahrenabschätzung durch Konsolidierung und Korrelation von Intrusion Detection”
- IDC - Security Conference 2003, 09/2003, Frankfurt, Präsentation “IT-Sicherheit im Unternehmen dauerhaft messbar machen”
- Information Systems Security Society of the Philippines - Manila Security Convention, 05/2003, Manila/Philippines, Präsentation “Global Intrusion Tracing”
- Fraunhofer Institut - CAST Forum, Thema “Secure Networks”, 04/2003, Darmstadt, Präsentation “Firewalls und Infrastrukturen”
- Fraunhofer Institut - CAST Forum, Thema “Secure Operating Systems”, 04/2002, Darmstadt, Präsentation “Sicheres Linux in 30 Minuten”
- Euroforum - 1. eSpionage Forum, 01/2002, Düsseldorf, Präsentation “Wie Hacker sich unsichtbar machen”
- CCC Congress 1999, “Prüfung von Quellcode auf Schwachstellen“

Konferenzorganisation

- Mitglied des Steering Committees der DIMVA Konferenz (Detection of Intrusions and Malware & Vulnerability Assessment – www.dimva.org)
- Mitglied der Programm Komitees von DFN CERT, DIMVA, 44Con und Hackito Ergo Sum Konferenzen
- Gastdozent der MCAST Universität auf Malta für IT-Sicherheit (im Rahmen einer Zusammenarbeit mit dem Fraunhofer Institut)