



Interview

Interview mit Christoph Baumgartner

Über Katz-und-Maus-Spiel zwischen Malware-Schreibern/ Spammern/Crackern und Sicherheitssystementwicklern, Anfang bei OSSTMM und kommerzielle und Open Source Security-Applikationen und deren Anwendung sprechen wir mit Christoph Baumgartner.

hakin9: Sie sind Inhaber der auf IT Security Consulting tätigen OneConsult GmbH, Sie auditieren seit 2002 nach OSSTMM, sind zertifizierter OSSTMM Professional Security Tester und Mitglied des ISECOM Core Teams und realisieren Projekte in der Schweiz, Deutschland, Liechtenstein, Österreich und Frankreich. Scheint ziemlich viel für eine Person zu sein. Haben Sie noch ein Privatleben oder haben Sie aus Ihrer beruflichen Tätigkeit Privatleben gemacht?

Christoph Baumgartner: (Lacht) Für eine Person wäre es wirklich ein sehr hohes Pensum, aber unsere Firma beschäftigt mittlerweile 11 Mitarbeiter – vor gut einem Jahr waren wir noch zu Zweit. Ohne dieses gut eingespielte Team wären wir sicherlich nicht so erfolgreich. Obwohl ich das Glück habe, mein Hobby zum Beruf machen zu können, musste ich mein Privatleben in den letzten Jahren stark zurückstellen, aber ich hoffe, dass sich dies in den nächsten Jahren ändert.

h9: Haben Sie von Anfang an Ihre professionelle Karriere so geplant oder ist dies eher Zufall?

ChB: Das war geplant. Ich habe an der Universität Zürich studiert und während des ganzen Studiums zu mindestens 50% im Informatikbereich gearbeitet. Obwohl ich hauptsächlich als

Berater tätig war, arbeitete ich auch als Projektleiter, Software-Architekt, Lösungsverkäufer und Marketingleiter bei Security-Integratoren.

h9: Ihre Spezialgebiete sind technische und organisatorisch/konzeptionelle Audits, Sicherheitsrichtlinien und -konzepte, BCM- und DR-Coaching und strategische Beratung. Welches ist das am meisten satisfaktionsbringende? Oder kann man diese überhaupt nicht vergleichen?

ChB: Die genannten Aktivitäten lassen sich in eher technisch und eher konzeptionell ausgeprägte Aktivitäten gliedern. Beides hat seinen Reiz, wobei ich mich einerseits dank sehr guten Mitarbeitern seit 1.5 Jahren eher im konzeptionell ausgerichteten Security Consulting und der strategischen Beratung betätige. Andererseits beanspruchen Verkaufs- und administrative Tätigkeiten einen namhaften Teil meiner Agenda. Weil technische Audits topaktuelle Kenntnisse über derzeitige Bedrohungen und Hacking-Techniken voraussetzen, fehlt mir mit zunehmender Unternehmensgröße die Zeit, mich seriös auf dem neuesten Wissensstand zu halten. Bei konzeptionell/organisatorischen Tätigkeiten ist die Halbwertszeit des Wissens wesentlich größer. Somit überlasse ich meinen Spezialisten das Feld der technischen Audits.

h9: Was halten Sie eigentlich von der IT-Security Szene? Hat die Entwicklung den richtigen Kurs eingeschlagen?

ChB: Vom Katz-und-Maus-Spiel zwischen Malware-Schreibern/Spammern/Crackern und Sicherheitssystementwicklern profitiert eine ganze Industrie. Würden nicht ständig neue Exploits und Malware entwickelt, würden wir alle noch mit Firewalls aus den 80-er Jahren arbeiten und die Hard-/Softwarehersteller und IT-Beratungsunternehmen würden entweder nicht existieren oder wären viel kleiner – die OneConsult in der heutigen Form als spezialisierten Nischenanbieter gäbe es gar nicht.

h9: Die Kompetenzen Ihres Unternehmens liegen ausschließlich in hersteller- und produkteunabhängigen Beratungsleistungen in den Bereichen IT-Security und Strategie. Erfüllen alle zugänglichen Security-orientierten Produkte keine Bedingungen, die Sie sich zum Ziel gesetzt haben oder baut diese Philosophie auf einer anderen Grundlage auf?

ChB: Gerade sicherheitsorientierte Branchen wie beispielsweise das Bank- oder Versicherungswesen und das Militär legen bei der Wahl ihres Beratungspartners Wert auf diese Unabhängigkeit – andernfalls besteht die Gefahr, dass das Beratungsunternehmen *zufälligerweise* nur Produkte empfiehlt, welche es selbst im Angebot hat.

h9: In Projekten setzen Sie oft selbst entwickelte bzw. programmierte Tools ein. Und was halten Sie von den kommerziellen und Open Source Security-Applikationen? Sind diese wirklich empfehlenswert und wenn ja, dann für Jeden geeignet?

ChB: Wir halten sehr viel von Open Source Software und setzen diese systematisch in technischen Security Audit-Projekten ein. Dies hat mehrere Gründe. Viele kommerzielle Tools unterscheiden sich, wenn überhaupt, nur in der aufwändiger gestalteten Reporting-Engine im Vergleich zu Open Source Tools. Dies ist aus unserer Sicht aber kein Nachteil, da wir unsere Reports selbst gestalten. Wir legen Wert darauf, dass wir die Funktionalität der von uns eingesetzten Tools kennen, was bei Open Source Tools einfach, aber bei Closed Source Tools erschwert wird, da man üblicherweise keinen Zugriff auf den Source Code hat. Ein aus Kundensicht wichtiger kommerzieller Vorteil ist, dass wir damit unseren Kunden eine Tool-Zuschlagspauschale für in Projekten zum Einsatz kommende kommerzielle Tools ersparen, deren Lizenzen wir kaufen müssten. Generell haben aber sowohl kommerzielle wie auch Open Source Tools ihre Daseinsberechtigung. Vor wenigen Jahren gab es kaum Support-Anbieter für Open Source Software. Dies war der Hauptgrund für viele Unternehmen, zwangsläufig kommerzielle Software einsetzen zu müssen, weil sie sich keine eigenen Open Source Supporter leisten wollten/konnten.

h9: Können Sie unsere Leser kurz an das Open Source Security Testing Methodology Manual erinnern. Womit befasst sich diese Methode, was hat sie zum Ziel und von wem wird sie in der Regel verwendet?

ChB: Das von ISECOM entwickelte OSSTMM ist eine frei verfügbare Methode zur Planung, Durchführung und Dokumentation von technischen Security Audits und der

Beurteilung der Ergebnisse. außerdem wird das Sicherheitsniveau der untersuchten Umgebung bei OSSTMM-konformen Test als Zahlenwert, dem sogenannten *Risk Assessment Value (RAV)*, wiedergegeben. Dies macht die Vergleichbarkeit mit anderen Projekten möglich, ohne Details preisgeben zu müssen. Das OSSTMM wird vom BSI empfohlen und ist compliant zu den gängigen Standards und Regulatorien wie beispielsweise ISO/IEC 27001, IT GSHB, ITIL, SOX, Basel II und SET.

h9: Und Ihr Anfang bei OSSTMM war...

ChB: Bei meinem vorherigen Arbeitgeber durften wir im Jahr 2002 für eine Sicherheitsorganisation mehrere Tausend Systeme auditieren. Der Auftraggeber verlangte ein systematisches Vorgehen, wenn immer möglich nach einer anerkannten Methode. Deshalb evaluierten wir alle verfügbaren Methoden und entschieden uns für das OSSTMM.

h9: Aus welchem Grunde haben Sie sich entschieden, an diesem Projekt teilzunehmen?

ChB: Im Jahr 2002 war das OSSTMM im deutschsprachigen Raum fast unbekannt. Weil ich an das OSSTMM glaube und noch immer glaube, sah ich dessen fehlende Bekanntheit als Hauptproblem. Deshalb promote ich seit 2002 das OSSTMM in Form von Fachartikeln und Referaten.

h9: Können Sie mehr von diesem Teil Ihrer Aktivität erzählen? Was ist dabei der Kern der Sache?

ChB: Die Hauptschwierigkeit besteht darin, die Brücke zwischen der Security Tester-Fraktion, welche nach Möglichkeit eher kreativ, d. h. ohne fixe Methodik vorgeht und der Fraktion der Compliance Officer, welche Wert auf Standard-konformes Vorgehen legt, zu schlagen. Weil das OSSTMM aus dem Open Source-Bereich stammt, gilt es diesbezügliche Vorurteile ebenfalls zu widerlegen – doch in diesem Bereich hat sich die allgemeine Grundhaltung glücklicherweise in den letzten Jahren zugunsten von Open Source Tools stark verbessert. Generell verfassen meine Mitarbeiter und ich Artikel und Referate zielgruppengerecht. So interessieren beispielsweise die Eigenschaften des OSSTMM *frei verfügbar* und *Checklisten-basiert* eher die technisch orientierten Security Tester und die Attribute *vollständig*, *nachvollziehbar* und *Standard-compliant* primär die Compliance Officer und die Geschäftsleitung.

h9: Wie beurteilen Sie unser Magazin im Bereich Hilfsquelle für die IT-Lösungen?

ChB: Ich finde hakin9 ein sehr gutes Magazin, welches primär sehr profunde Hilfestellungen aus der technischen Perspektive bietet. Außerdem hat sich das Magazin in den letzten Jahren hinsichtlich der Qualität und des Spektrums der Beiträge und hinsichtlich der optischen Aufmachung stark verbessert und ist nun ebenbürtig mit einem anderen bekannten technisch orientierten IT-Magazin aus Deutschland.

h9: Das ist natürlich nett zu hören! Vielen Dank für das Interview! ●

Mit Christoph Baumgartner sprach Anna Dorazińska.