Interview mit Matthias Leu - Autor des Buches „Check Point Next Generation AI – Das Standardwerk für FireWall-1/VPN-1“

Marc Ruef, scip AG, maru-at-scip.ch

Marc Ruef, scip AG: Hallo Matthias, schön, dass Du Dir die Zeit für dieses Interview nimmst. Ich möchte Dir zur neuen und erweiterten Auflage Deines Buches "Check Point Next Generation AI - Das Standardwerk für FireWall-1/VPN-1"gratulieren. Die Neuauflage ist noch dicker als die Erstausgabe. Wie lange hast Du an dem Buch geschrieben?

Matthias Leu, AeraSec: Erstmal danke für Dein Lob. Ja, das aktuelle Buch ist dicker, wobei einige Teile, die noch mit hineinsollten, dann doch im Internet veröffentlicht wurden. Kein Wunder eigentlich, weil mit NG AI hat sich einiges getan und die Funktionalität stark zugenommen, vor allem gegenüber Version 4.1. Natürlich weiss ich auch, was ich nicht bis in die volle Tiefe behandelt habe. Insofern wollte ich als Untertitel eigentlich den Satz "Eine Einführung". Aber das geht natürlich nicht bei so vielen Seiten...

Das Buch habe ich neben der Arbeit geschrieben. Das musste so sein, weil ich in den letzten Jahren eine Firma aufgebaut habe. Und so wurden es dann ungefähr anderthalb Jahre "nebenbei" am Schreibtisch.

Wie bist Du auf die Idee gekommen, ein Buch über CheckPoint Firewalls zu schreiben?

Ungefähr Weihnachten 1999 hatte ich das erste Buch über diese Firewall in der Hand. Natürlich auf englisch. Und von Kunden hatte ich immer wieder die Frage, ob es hierzu nicht auch Literatur auf Deutsch gibt. Nein, die gab es damals noch nicht. Also meinte ich, dass ich hierzu ein Buch schreiben könnte, wobei es nicht nur einfach eine Bedienungsanleitung sein sollte, sondern viele Tipps und Tricks aus der Praxis gibt. Und die wollte ich reinbringen, zumal ich seit Version 1.02 mit der Check Point FireWall-1 intensiv arbeite.

Handelte es sich dabei um eine Auftragsarbeit, die Dir durch den Vertrag zugeteilt wurde, oder hast Du die Mühe aus freien Stücken auf Dich genommen und erst danach potentielle Verläge angeschrieben?

Zum Computer- & Literaturverlag hatte ich schon Kontakte, weil hier im Februar 1997 mein erstes Buch erschienen ist. Anfang 2000, nachdem ich ein Konzept gemacht hatte, habe ich beim Verlag angefragt. Schliesslich kam die Zusage, und auch das Eingeständnis, dass ich mich nicht auf einen festen Abgabetermin festlegen möchte oder kann. Auch das erste Buch über die Check Point FireWall-1 habe ich in meiner Freizeit geschrieben, und nach ungefähr zwei Jahren war es dann im Handel. Dem Verlag bin ich vor allem auch für seine Geduld mit mir sehr dankbar.

„Das Buch habe ich neben der Arbeit geschrieben, weil ich zusätzlich eine Firma aufgebaut habe.“

Die erste Auflage des Buches ist Ende 2001 erschienen. Die zweite ist Ende 2003 auf den Markt gekommen. Dies ist keine schlechte Leistung für ein technisches Buch in dieser Preisklasse. Ist schon eine neue Auflage geplant?

Seit Ende 1999 bzw. Anfang 2000 war ich in der Freizeit eigentlich (fast) immer am Schreibtisch - und bin mit meiner Traumfrau verheiratet. Nein, eine neue Version habe ich noch nicht angefangen. Vier Sommer habe ich mehr oder weniger am Schreibtisch verbracht, da brauche ich auch mal eine Pause. Und Check Point ist so nett, dass sich seit Erscheinen des aktuellen Buchs nicht soo viel getan hat. Wenn eine vollständig neue Version herauskommen würde, käme ich ins Überlegen, im Herbst wieder anzufangen...

Gab es beim Ausarbeiten des Buchs eine Zusammenarbeit mit CheckPoint? Falls ja, wie sah eine solche aus? Haben sie Dir vorgeschrieben, über was Du wie zu schreiben hattest? Sahen sie Dich als eher Verbündeten oder unliebsamen "Schnüffler"?

Also hier muss ich Check Point Deutschland erstmal herzlich für die Zusammenarbeit danken. Nein, sie haben mir nicht vorgeschrieben, was ich
schreiben soll oder darf und ich bin auch dort nicht angestellt. Es hat sehr viel gebracht, hier Ansprechpartner zu haben, um Fragen zu stellen und mir das eine oder andere nochmal genau erklären zu lassen. Kritische Stellen wurden nicht "zensiert", sondern eher ausdiskutiert. Es war

also kein "Meinungsaustausch", nach dem ich dann mit einer anderen Meinung wieder heimkam.

Als ich mit dem ersten Buch über die Check Point anfing, meinte ich genug zu wissen, um es zu schreiben. Aber, wenn man dann richtig "abgetaucht" ist und die Testumgebung "glüht", kommen nach und nach immer mehr Fragen - und da hat der direkte Kontakt zu Check Point wirklich viel gebracht. Und, ich konnte dann auch sicher sein, dass später keine grundsätzlich falschen Dinge zu lesen sind.

Es gibt mittlerweile eine ganze Reihe von Büchern zu den Themen Computersicherheit und Firewalling. Hast Du Kontakt mit Autoren vergleichbarer Werke (z.B. Firewall-Systeme von Dr. Norbert Pohlmann) und wie siehst Du den Vergleich Deines Buches mit anderen?

Ja, die Anzahl der Bücher über Sicherheit, Firewalls und verwandte Themen wird immer mehr. Natürlich kenne ich auch andere Autoren. Der Vergleich eines eigenen Buches mit anderen ist nicht ganz leicht. Trotzdem versuche ich es mal. Allgemeine Bücher über Netzwerksicherheit und anderen Gebieten geben oft einen guten Überblick zum Thema, ohne zu tief in Details zu gehen. Das ist für Leute, die neu in das Gebiet kommen, genau richtig. Dann gibt es noch wirkliche Spezialbücher wie z.B. die "Kurzanleitung" zu Sendmail. Die sind dann so speziell, dass sie dem Experten eigentlich in allen Fragen weiterhelfen, der normale Leser ohne Vorwissen aber nach den ersten Seiten fast nichts mehr versteht.

Mit meinem Buch habe ich versucht, die Bedienung der Check Point FireWall-1 zu erklären. Dabei war und ist mir sehr wichtig, dass die Administratoren "wissen, was sie tun". Daher die ersten vier Kapitel mit den Grundlagen. Die braucht ein erfahrener Administrator nicht, klar. Aber ohne diese Kapitel bestünde die Gefahr, dass der unerfahrene Leser zwar lernt, wo er bei dieser Firewall klicken muss - und dann nicht weiss, was überhaupt eine IP-Adresse ist. Das Buch sehe ich als Mittelding zwischen einem Nachschlagewerk und einem Buch, mit dem sich die Bedienung erlernen lässt. Auch wenn es über 1'000 Seiten hat, wurden einige Dinge nur gestreift und nicht ausführlich behandelt. Der Grund hierfür ist einerseits der Platz, andererseits gibt es einige Konfigurationen, die nur sehr selten eingesetzt werden. Trotzdem glaube ich, die wichtigsten Punkte angesprochen zu haben.

Du bist nun auch schon einige Jahre im IT-Business tätig. Mir gegenüber hast Du einmal erwähnt, dass Du die CheckPoint-Lösung seit den ersten Versionen kennst. Was hast Du für ein Gefühl, wie haben sich die CheckPoint-Firewalls entwickelt, welche Marktposition hat das Produkt und in welche Richtung wird es weiterhin gehen?

Der letzte Teil ist eher schwierig zu beantworten, ehrlich. Wer hätte bei Version 3.0 gedacht, wie NG AI R55 aussieht? Die ersten Versionen waren richtig gut und einfach zu bedienen, auch ohne Lesen des Handbuchs. Neben der eingesetzten Technologie war, glaube ich, dies ein Grund, warum sich diese Firewall so weit durchgesetzt hat.

„Mit meinem Buch habe ich versucht, die Bedienung der Check Point FireWall-1 zu erklären."

Jetzt habe ich hier keine genauen Zahlen, aber diese Firewall ist schon sehr weit verbreitet und kommt bei sehr vielen Unternehmen unterschiedlichster Grösse zum Einsatz. Da zeigt sich die Flexibilität und Skalierbarkeit dieser Firewall. Inzwischen ist die Bedienung nicht mehr so ganz einfach, wobei hier der Grund nicht das GUI, sondern die inzwischen erreichte Komplexität ist. Genau die aber möchte der Markt scheinbar, insofern ist dies nicht als Nachteil zu sehen. War bei den ersten Versionen noch eine Bedienung ohne Blick ins Manual möglich, sollte der Administrator von heute doch einen Kurs drüber besuchen. Danach ist vielen auch das heutige GUI mit all seinen Optionen übersichtlich.

Wo es hingeht, weiss ich nicht genau. Ich schätze aber, dass es weiter zum wirklich zentralen Sicherheitsmanagement gehen wird. Das hat Check Point bereits lange, aber vielleicht kommen früher oder später noch weitere Funktionen dazu. Die zentrale Verwaltung hat den Vorteil, dass ein Administrator nur mit einem GUI arbeitet und daher die Gefahr, dass etwas vergessen wird, niedriger ist. Insgesamt wird dadurch die Sicherheit also erhöht.

Woran sollte Deiner Meinung CheckPoint am ehesten an ihrer Firewall feilen? In welchem Bereich ist das Produkt am schwächsten?

Wenn die Frage vor zwei Jahren gekommen wäre, fiele die Antwort leicht. Check Point hat

Next Generation neu herausgebracht und da war doch die eine oder andere "Kinderkrankheit" dabei. Seit "Next Generation with Application Intelligence" sind diese grösstenteils behoben – und auch die Geschwindigkeit zur Einführung neuer Features hält sich momentan in Grenzen. Jetzt scheint Check Point eher an der Qualität zu feilen, und das macht sich inzwischen bemerkbar.

Direkte Schwächen sehe ich im Moment nicht. Kaum eine andere Firewall ist so flexibel und individuell zu konfigurieren (und lizenzieren). Von den kleinen bis zu den grössten Unternehmen kann diese Firewall eingesetzt werden, bei gleichem, zentralen Management. Gut, wenn ich etwas "finden" muss - bei den Zertifikaten, wie sie bei der Verschlüsselung eingesetzt werden, könnte noch was verbessert werden. Manchmal ist's hier ein wenig eigen.

Einige bemängeln bei Check Point, dass sie eine "unsichere Firewall" ist, weil Hotfixes herausgegeben werden, die kritische Probleme beheben. Aufgrund der Komplexität heutiger Firewalls kann es aber passieren, dass unter gewissen Bedingungen auch sicherheitsrelevante Fehler erkannt werden. Hier ist Check Point aber meist schnell mit der Veröffentlichung von Verbesserungen. Diese Vorgehensweise finde ich besser als die Behauptung, dass eine Firewall von Haus aus sicher ist und immer sicher sein wird.

Und was würdest Du bei der Entwicklung einer Firewall grundsätzlich anders machen?

Den Preis? (grinst) Im Ernst, diese Firewall ist meines Erachtens sehr gut, flexibel, bedienbar, ausbaubar... Insofern würde ich nichts Grundsätzliches anders machen. Andererseits sollten, das habe ich mal vor vielen Jahren gelernt, Sicherheitsprodukte möglichst einfach sein. Das ist die FireWall-1 nun wirklich nicht, eher megakomplex. Aber das sind wohl die Anforderungen des Marktes, und der bestimmt letztendlich, welche Features eine Firewall bieten soll oder muss.

Was macht für Dich ein gutes Firewall-Produkt aus?

Eine gute Firewall zeichnet sich meines Erachtens dadurch aus, dass sie so flexibel ist, dass sie den Anforderungen des Unterhehmens wirklich entspricht, ohne wenn und aber. Dass eine Firewall wirklich die notwendige Sicherheit bietet, setze ich einfach mal voraus. Neben der Flexibilität finde ich die Funktionalität wichtig. Wenn die Firewall als zentrales Gateway für die Sicherheit eingesetzt wird, sollte sie Sachen wie VPN und Authentisierung können. Viele Unternehmen wünschen ausserdem die Möglichkeit zum Accounting, Bandbreitenmanagement oder auch die Option, die Firewall von speziellen Anbietern managen zu
lassen.

Die Sicherheit hatte ich schon angesprochen. Für mich gehört zwingend dazu, dass die Firewalls auch in einer komplexeren Umgebung noch zu managen sind und vor allem der Administrator die Übersicht behält. Oft ist dies das A und O für die Sicherheit. Check Point ist hier eine Art Vorreiter gewesen und hat das Management von Haus aus zentral. Wenn ich das mit anderen Anbietern vergleiche... Anders gesagt: Nicht bei allen Anbietern von Firewalls ist ein zentrales und übersichtliches Management vorhanden.

„Die Anforderung des Marktes bestimmt letztendlich die implementierten Features einer Firewall."

Die Meinungen zu Personal Firewalls (PF) sind gespalten. Auf der einen Seite sind Leute, die derlei Lösungen als grösstes Übel des Internetzeitalters sehen, da sie falsche Sicherheit versprechen. Andere widerum halten die zusätzlichen Schutzmassnahmen für hilfreich und in der heutigen Zeit unabdingbar. Wie stehst Du Produkten wie ZoneAlarm oder BlackICE PC Protection gegenüber?

Personal Firewalls verteufle ich nicht, wenn der Benutzer mit ihnen richtig umgeht. Sicherlich hat der Benutzer nur eine (gefährliche) Scheinsicherheit, wenn er vor zwei Jahren mal eine Personal Firewall mit den Default-Einstellungen installiert und sich nie wieder drum gekümmert hat. Aber ich kenne auch Benutzer, die ihre Personal Firewall sorgfältig konfiguriert haben und immer auf dem aktuellen Stand der Technik halten. Dann ist so eine Software wirklich gut für den Benutzer, der sich mit seiner ISDN- oder DSL-Anbindung nicht hinter der Firewall seiner Firma verstecken kann. Eigentlich sollten alle Benutzer eine aktuelle Personal Firewall in Kombination mit einem guten Virenschutz einsetzen. Es ist doch zum Teil erschreckend, wie leicht Recher in den Einwahlbereichen der Provider angreifbar sind.

Intrusion Prevention-Systeme (IPS) sind immer mehr im Kommen. Durch das grundlegende Einschränken der Möglichkeiten eines Systems sollen klassische Angriffsformen (z.B. Pufferüberlauf-Schwachstellen) verhindert werden. Denkst Du, dass diese Technik heutige Firewalls überflüssig machen und die IT-Security revolutionieren werden?

IPS sehe ich als eine Weiterentwicklung von Intrusion Detection Systemen, die ja eigentlich eine reine Alarmanlage sind. Und dann kommt die Frage an den Administrator eines IDS, was passiert, wenn nachts um drei ein Alarm kommt. Mit Hilfe von IPS lassen sich einige Angriffsformen erkennen und verhindern. Vor allem im internen Netzwerk können solche IPS die Sicherheit erhöhen, indem sie z.B. Angriffe von Würmern erkennen und die befallenen Systeme ggf. gleich isolieren. Allerdings glaube ich nicht, dass IPS Firewalls ersetzen werden. Eine Firewall sehe ich als Pförtner, der gewisse (harmlose) Pakete durchlässt und andere eben nicht. Das IPS entdeckt Unregelmäßigkeiten und verhindert diese. Zwar geht die Entwicklung bei Firewalls zum Teil dahin, dass auch ein Angriff wie z.B. ein potenzieller Pufferüberlauf erkannt und automatisch gesperrt wird. Aber ich glaube, es wird (noch) keine gravierenden Änderungen in der IT-Security geben, vielmehr ein sinnvolles, sich gegenseitig ergänzendes Miteinander von Firewalls und IPS.

Die letzten Monaten hatte Dein Unternehmen AeraSec mit Advisories zum Thema Denial of Service gegen diverse Antiviren-Lösungen für Aufsehen gesorgt. Längerfristiger Gewinner der Publikation sind die Kunden, die mit einer Verbesserung ihrer Produkte rechnen können. Welche Informations-Politik scheint für Dich im Bereich der Computersicherheit angemessen? Müssen die Leute schnellstmöglich informiert werden oder kann Sicherheit nur durch Geheimhaltung "gefährlicher Informationen" erfolgreich umgesetzt werden?

Vorweg möchte ich erst einmal feststellen, dass es weder eine fehlerfreie Software gibt, noch die ab und zu zitierte Sicherheit von 100 %. Die Hersteller von Software wissen auch, dass in den von ihnen vertriebenen Produkten Fehler sein können, die sie noch nicht entdeckt haben. Bei sicherheitskritischen Lücken sollte auf jeden Fall zuerst der Hersteller davon erfahren, damit er eine Chance hat, den Fehler möglichst zügig zu verbessern. Wenn er es allerdings nicht nötig hat, auf einen kritischen Fehler zu reagieren, dann sollte auch ohne die Veröffentlichung eines Patches auf den entsprechenden Seiten und Listen im Internet auf den Fehler hingewiesen werden - möglichst auch mit der Anleitung zu einem Workaround, der die Konsequenzen des Fehlers möglichst verhindert.

Meine Erfahrung ist, dass sich die meisten Hersteller bei der Meldung eines Fehlers sehr kooperativ verhalten und auch relativ schnell einen Patch herausgeben. Insofern wäre es fast unfair, erst einen Exploit zu veröffentlichen und dann den Hersteller darauf hinzuweisen.

Und wie stehst Du dem Patchday-Prinzip von Microsoft gegenüber?

Diese Sache sehe ich eher zweispältig. Hotfixes sollten einerseits möglichst zügig erscheinen, damit die Lücken geschlossen werden können. Andererseits waren gewissenhafte Administratoren von Microsoft Windows bisher wirklich nicht zu beneiden. Sie sind ja mit dem Test und der Installation von Hotfixes ja bald nicht mehr nachgekommen. Insofern ist das Patchday-Prinzip gut für die Administratoren - aber nicht unbedingt gut für die Sicherheit der Systeme selbst. Und einige Lücken werden schon vor der Veröffentlichung des Patches im Internet diskutiert. Das kann zur Folge haben, dass gewisse Insider möglicherweise die Server schädigen können, ohne dass der Administrator eine Idee hat, dass sein Server unsicher sein könnte. Also, das Ganze sehe ich wirklich mit einem lachenden und einem weinenden Auge.

„Ich möchte feststellen, dass es weder fehlerfreie Software noch 100 %ige Sicherheit gibt..“

Die IT-Branche hat nach dem Boom in den Jahren 2000 und 2001 enorme Einbussen verkraften müssen. Der Markt scheint sich aber langsam wieder zu erholen. Wie hat Dein Unternehmen diese Krise erlebt und welche Prognosen stellst Du für die kommenden Jahre?

Die Zeiten der Internet-Blase sind zum Glück vorbei. Es war ja nicht wirklich natürlich, dass ein kleines Unternehmen mit einer guten Idee besser bewertet wurde als ein seit Jahrzehnten erfolgreich produzierendes Unternehmen. Die AEARsec wurde Mitte 2000 gegründet. Da könnte man sagen, dass hiermit die Krise

begann (lacht). Auch heute ist es noch nicht einfach, sich weiter am Markt zu platzieren und neue Projekte zu akquirieren. Die Unternehmen sparen noch immer sehr und es wird wirklich nur das nötigste investiert. So sind die Bereiche Weiterbildung und Einführung neuer Systeme noch immer sehr gebremst. Aber ich bin optimistisch, dass es mit den Jahren wieder besser wird.

Unser Unternehmen hat die Krise so erlebt, dass von Kunden und Interessenten viele Dinge in die Zukunft verlagert wurden. Wir haben bisher die Krise gemeistert, weil wir Qualität liefern und einen hohen Wert auf eine langfristige Kundenbindung legen. Auch ist der Wachstum unseres Unternehmens eher vorsichtig und konservativ.

Die Zukunft sehe ich nicht so, wie die Neunziger Jahre ausgeklungen sind. Vielmehr schätze ich, dass der Markt eher langsam wieder besser wird und die Unternehmen, die die Krise überstehen, langfristig ein gesundes Wachstum zeigen werden. Die Zeiten, in denen man im Alter von 20 seine ersten 10 Millionen verdient hatte, sind vorbei.

Noch eine in solchen Gesprächen eher untypische Frage: Wenn Du auf eine einsame Insel gehen müsstest, was würdest Du am liebsten mitnehmen oder was würdest Du vermissen?

Gute Frage, vor allem weil Du nicht eingeschränkt hast, wie viel ich mitnehmen kann und ob auf der Insel eine Satellitenanbindung an das Internet ist (lacht).

Mitnehmen würde ich auf jeden Fall meine Frau, und wenn ich ehrlich bin, wären Dinge wie Handy, Internet oder CD-Sammlung gar nicht so notwendig. Insofern kann ich nur verweisen auf Seite 13 im aktuellen Buch (lacht).

Ich möchte mich für diesen unterhaltsamen und interessanten Dialog bedanken und wünsche Dir weiterhin viel Glück.

Ich danke Dir auch sehr herzlich für Deine Zeit und wünsche auch Dir alles Gute für die Zukunft!

Der Autor

Marc Ruef arbeitet als Security Consultant bei der schweizer Firma scip AG (http://www.scip.ch), welche sich auf Sicherheitsberatungen im Bankenumfeld spezialisiert hat. Er hat eine Vielzahl an Artikeln, Büchern und Übersetzungen im Bereich Computersicherheit publiziert, betreut einige namhafte internationale Projekte auf diesem Gebiet und unterrichtet an diversen Fachhochschulen sowie Universitäten.

Impressum

scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 44 445 1818
mailto:info-at-scip.ch
http://www.scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.