Oliver-Christopher Rochford

ist Autor von „Hacken für Dummies“ und aktives Mitglied bei diversen Hackergruppierungen.

Derzeit beschäftigt er sich bei INSL, Oxford (www.insl.co.uk) mit den Themenbereichen IT-Security, Networking und Monitoring.

Peter S. Tippett

entwickelte die erste kommerzielle Anti-Virus-Software, aus der später Norton AntiVirus hervorging.

Er gilt als einer der führenden Experten auf dem Gebiet der IT-Security und ist Verfechter einer risiko-orientierten Strategie in diesem Bereich.

Tippett ist heute Chief Technologist der TruSecure Corporation (www.trusecure.com).

KISS,
„Keep It Simple, Stupid“

Interview mit Oliver-Christopher Rochford und Peter Tippett

Seit der Programmierung des ersten Computervirus vor gut 25 Jahren vergeht kaum ein Tag, an dem uns nicht neue Schrecksmeldungen über Viren, Würmer, Trojaner und andere Störenfriede erreichen. Ihre Anzahl wächst ebenso schnell wie die Schäden, die sie verursachen. Nicht zu Unrecht steht das Thema IT-Security deshalb ganz oben auf der Agenda vieler Risiko-Manager. Um heraus zu finden, wie man diese Bedrohung in den Griff bekommt, haben wir mit einem Hacker und einem Fachmann für IT-Security gesprochen. Das überraschende Ergebnis: Das Problem ist beherrschbar, wenn man ein paar einfache Regeln beherzigt. In einem Glossar erklären wir die wichtigsten Begriffe aus der Welt der Viren, Würmer und Trojaner.

RISKNEWS: Wir leben in einer immer stärker vernetzten Welt. Was sind aus Ihrer Sicht derzeit die wichtigsten Probleme und Entwicklungen beim Themenkomplex IT-Sicherheit und Risk Management?

Das Grundübel besteht darin, dass viele Internet-Benutzer dem Thema IT-Sicherheit noch viel zu wenig Aufmerksamkeit schenken.

Rochford: Das Grundübel besteht für mich darin, dass viele Internet-Benutzer dem Thema IT-Sicherheit noch viel zu wenig Aufmerksamkeit schenken. Selbst viele IT-Profis wissen kaum Bescheid. Vor allem kleinere Unternehmen leiden unter dem unzureichenden Know-how, da ihnen oftmals nicht nur das Verständnis, sondern auch das Budget fehlen, um sich mit solchen Fragen zu beschäftigen.

Die beiden wichtigsten Probleme – die sich größtenteils auf die gerade skizzierten Ursache zurückführen lassen – sind aus meiner Sicht die folgenden: Zum einen häufen sich die DDoS-Angriffe (Distributed Denial of Service), die nur möglich sind, weil zu viele Benutzer Ihre Rechner nicht ausreichend absichern. Erst dadurch stellen sie den böswilligen Angreifern ihre Waffen zur Verfügung.

Zum anderen nehmen auch die so genannten „Phishing"-Betrügereien stark zu, bei denen Netz-Kriminelle eine authentisch aussehende E-Mail an ahnungslose Opfer verschicken, um diese zu überreden, ihre privaten Daten Preis zu geben. Diese werden dann für betrügerische Zwecke missbraucht, etwa für Kreditkartenbetrügereien.

Tippett: Ich finde es bedenklich, dass wir immer weiter hinterherhinken. Jedes Jahr verdoppelt sich die Anzahl der entdeckten Sicherheitslücken. Die Zahl der erfolgreichen Angriffe, Würmer, Virus-Infektionen und die dadurch entstehenden Schäden steigen jährlich um 50 Prozent. Die Risiken durch Sabotage von Insidern (beispielsweise Mitarbeiter der eigenen Firma) nehmen um 15 Prozent zu. Auch die Bedrohung durch ganz gezielte Angriffe auf einzelne Organisationen steigt.

Die Risiken durch Sabotage von Insidern nehmen um 15 Prozent zu.

Und all das passiert, obwohl die Unternehmen nun schon seit sieben Jahren ununterbrochen ihre Investitionen in die IT-Security steigern. Für mich sieht das aus wie eine negative Rückkopplung: Immer weniger Leistung für immer mehr Geld. Irgendetwas scheint da grundlegend falsch zu laufen in unserem Handeln – und in unserem Denken. Wir handeln reaktiv. Wir machen das, was alle anderen auch machen. Wir lösen „Probleme", die eigentlich gar nicht existieren und kümmern uns überhaupt nicht um die relativ einfachen Lösungen für die wirklichen und dringenden Probleme. Wir konzentrieren uns auf Sicherheitslücken, Patches und Papierkram anstatt auf pragmatisches, ganzheitliches Risikomanagement.

... wir machen alles nur schneller anstatt schlauer.

RISKNEWS: Von der Gegenwart in die Zukunft, quasi ein Blick in die Kristallkugel. Was wird Ihrer Meinung nach das größte IT-Sicherheitsrisiko in den nächsten 12 Monaten sein?

Tippett: Schwer zu sagen … „Bot networks" – hunderttausende von Homecomputern, die von einigen wenigen Schurken kontrolliert werden … Würmer, die 25 Prozent bis 75 Prozent aller Organisationen befallen … Hacking aus Geldgier … ein Anstieg von zielgerichteten Angriffen … zunehmend effektives und überzeugendes Social Engineering der Öffentlichkeit durch Phishing … eigentlich all das, was auch in den letzten paar Jahren schon ein Problem war – nur viel mehr davon!

Rochford: Es werden noch weitere DDoS-Angriffe und einige Viren und Würmer auf uns zukommen. Der Virus (oder war's ein Wurm?) SoBIG richtete zum Beispiel einen anonymen Mailer auf dem Wirtsrechner ein, der dann von Spammern zum Versenden von E-Mails verwendet werden konnte. Gleichzeitig wurde der Start von DDoS-Attacken von diesen Maschinen ermöglicht, von denen auch sehr viele Antispam-Seiten betroffen waren. Einige mussten ihre Dienste sogar ganz einstellen. Diese Entwicklung ist recht beunruhigend. Die Spammer werden aggressiv. Inzwischen kann jemand mit sehr wenig Wissen und auf der Basis eines vorgefertigten Trojaners oder Virus immensen Schaden anrichten und plötzlich sehr viel Macht ergattern. Wer kann da schon wissen, was andere Verbrecher in den Tiefen des Internets vorbereiten und was uns noch alles erwartet?

Tippett: Vielleicht lässt sich die eskalierende „Bedrohung" auch ganz einfach durch unsere Versäumnisse erklären: Wir Security-Spezialisten konzentrieren uns auf Oberflächlichkeiten, wir versuchen jeden Angriffspunkt auszuschalten, wir spielen jeden Patch ein, wir verschlüsseln jede Datei … aber wir machen alles nur schneller anstatt schlauer.

RISKNEWS: Herr Rochford, Sie sprachen gerade „vorgefertigte" Viren und Würmer an. Tatsächlich werden die meisten „neuen" Schädlinge heute von so genannten „Script-Kiddies" mit Hilfe von Viren-Baukästen aus dem Internet gebastelt. Besteht überhaupt eine Chance, dass man dieses Risiko proaktiv vermeiden kann?

Rochford: Gegenfrage: Wenn schon Hobbybastler Milliardenschäden verursachen können – was passiert dann erst, wenn begabte Programmierer und IT-Profis Viren und Würmer entwickeln?

Die Viren- und Wurmbedrohung hat in den letzten Jahren geradezu epidemische Ausmaße angenommen – schlicht und einfach als Folge der immer engeren globalen Vernetzung. Aber insbesondere auch dadurch, dass viele Benutzer ohne Antiviren-Software ins Netz gehen.

Meiner Meinung nach hat jeder Einzelne eine Verantwortung und vernachlässigt oftmals seine Pflicht. Die zuständigen Leute zeigen alle nur mit dem Finger aufeinander, aber keiner tut was.

ISPs sollten aktiv Viren filtern, da sie die richtige Infrastruktur besitzen. Die Betriebssystem-Anbieter sollten den Benutzer zumindest irgendwie auf Sicherheitslücken aufmerksam machen – vielleicht durch ein Pop-Up Fenster, wenn keine Anti-Viren-Software installiert ist. Computerverkäufer sollten beim Verkaufsgespräch auf die Sicherheitsthematik aufmerksam machen. Statt haufenweise nutzlose, aber vielleicht hübsche Software (wie Bilder-Lexika) beizulegen, sollte zur Abwechslung auch mal Antiviren-Software „im Bundle" angeboten werden.

Mein letzter Punkt ist sicherlich umstritten, aber ich bestehe dennoch darauf: Wenn einem Nutzer nachgewiesen werden kann, dass er grob fahrlässig gehandelt hat, beispielsweise indem er seine Anti-Viren-Software nicht auf dem neuesten Stand hält oder möglicherweise gar keine hat, sollte er zur Verantwortung gezogen werden und auch entsprechende Strafen zahlen. Wenn jemand im Straßenverkehr betrunken fährt oder keine Bremsen hat, wird ja auch hart durchgegriffen.

RISKNEWS: Auf der einen Seite beobachten wir immer bessere und ausgefeiltere Schutzmechanismen auf der Hard- und Software-Seite. Denken wir nur an Firewalls, Virenscanner und Zugangssysteme. Auf der anderen Seite sagen Sicherheitsexperten immer wieder, dass uns nicht die Technologie sicherer machen wird, sondern die Menschen. Welche Rolle spielt der Mensch beim Thema IT-Risikomanagement? Welche Bedeutung kommt einer funktionierenden Risiko-Kultur im Vergleich zu den traditionellen Risiko-Vermeidungsstrategien zu?

Rochford: Wie schon angesprochen: Der „Risiko-Faktor Nummer Eins" ist der Mensch. Ich benutze einen Windows Rechner. Bis auf Anti-Viren-Software habe ich keinerlei Sicherheitssoftware am laufen. Es ist alles innerhalb der Einstellungen und Möglichkeiten des Betriebssystems abgesichert. NetBIOS und andere Dienste horchen nicht an der Verbindungsschnittstelle zum Netz, der Windows Portblocker ist an … und das war es auch schon. Gefahr besteht nur noch von Trojanern und anderer Malware, die aber vom Anti-Viren-Programm aufgespürt werden sollten, wenn man es auf dem aktuellen Stand hält. Man benötigt keinerlei separate Applikationen. Man benötigt lediglich das Wissen, was man wo und wie einstellt. Diese Sachen sollten an und für sich als Standard vom Systemanbieter eingerichtet sein. Microsoft hielt das jedoch nicht für nötig. Erst im Windows XP Service Pack 2 ist dies so konfiguriert und die eingebaute Firewall wird um einige Funktionen erweitert. Glückwunsch Redmond, es hat nur 8 Jahre gedauert!

Und wo wir gerade von Microsoft reden, bringt uns das gleich zum nächsten Punkt: Schlampige Programmierung. Es sollte in unserer Welt nicht möglich sein, dass es noch Buffer-Overflows in Programmen gibt, die schon mehrere Jahre und in der x-ten Version im Umlauf sind. Die Realität sieht aber leider anders aus. Programmierer sollten nicht nur an mehr Features denken, sondern auch an mehr Security! Über den Quelltext sollte ein Audit laufen. Das trifft aber bei weitem nicht nur auf Windows zu, sondern auf nahezu alle Betriebssysteme. Die Fehler sind wohlbekannt und dokumentiert, aber leider scheint das – bis auf die Hacker – kaum jemanden zu interessieren. Das Resultat sind dann solch nette Sachen wie der Slammer Wurm und SoBIG.

Auch die Fehlkonfiguration von Sicherheitstools sind ein leidiges Thema. IDSs, Logging, Firewalls, DMZs: Aus diesen Komponenten entsteht oft ein verwirrender, meistens undokumentierter Infrastruktur-Dschungel. Schon nach kurzer Zeit blickt da kein Mensch mehr durch. Ausgeworfen werden riesige Datenberge, die dann auch jemand auswerten sollte. Die teuerste Firewall nützt nichts, wenn sie jemand falsch einrichtet oder nicht so recht weiß, was er eigentlich tut. Unter Umständen überschneiden sich Firewall-Regeln und heben sich vielleicht sogar gegenseitig auf. Oder die Firma ist von unten bis oben abgeschottet, aber der Herr Direktor meint, er kann seinen PC an der Firewall vorbei ans Netz stöpseln, um Kazaa zu benutzen. Oder die Testmaschine vom letzten Jahr steht außen vor den Sicherheitsvorrichtungen und wird seit sechs Monaten als Warez-Server verwendet, oder

Wenn schon Hobbybastler Milliardenschäden verursachen können – was passiert dann erst, wenn begabte Programmierer und IT-Profis Viren und Würmer entwickeln?

Wenn einem Nutzer nachgewiesen werden kann, dass er grob fahrlässig gehandelt hat, sollte er zur Verantwortung gezogen werden und auch entsprechende Strafen zahlen.

Der „Risiko-Faktor Nummer Eins" ist der Mensch.

oder oder … damit wird die Zugbrücke weit heruntergelassen und die Tür weit geöffnet. Herzlich willkommen!

Das Netz ist eine große Gemeinschaft und das Rückgrat der westlichen Welt. Ich wünsche mir etwas mehr Verantwortungsbewusstsein der Mitglieder dieser Community.

Wichtig ist mir Folgendes: Das Netz ist eine große Gemeinschaft und das Rückgrat der westlichen Welt. Ich wünsche mir etwas mehr Verantwortungsbewusstsein der Mitglieder dieser Community. Sauber, überlegt, dokumentiert und praxisbezogen sind aber oftmals Fremdwörter. KISS – „Keep It Simple, Stupid", sollte die Leitregel sein!

Ich glaube, unser größter Fehler ist, dass wir Maßnahmen übertreiben, die eigentlich perfekt funktionieren.

Tippett: Genau richtig! Ich glaube, unser größter Fehler ist, dass wir Maßnahmen übertreiben, die eigentlich perfekt funktionieren. Policies, Arbeitsanweisungen, System-Architekturen, Antivirus-Software, Passwörter, Firewalls, Software-Patches, Sicherheitseinstellungen … all das sind grundlegende Schutzmechanismen. Sie funktionieren alle sehr gut. Jede Organisation muss sie in geeigneter Weise einsetzen. Aber wenn unsere Schutzmechanismen nicht gut genug arbeiten, haben wir nun mal die Tendenz, sie über das eigentlich sinnvolle Maß hinaus auszuweiten. Wir versuchen, die Nutzer zu zwingen, keine Fehler mehr zu machen, aktualisieren unsere Antivirus-Software noch öfter, machen unsere Passwörter noch stärker, schaffen noch mehr und noch bessere Firewalls an, spielen endlose Software-Patches ein und so weiter und so weiter …

Was dagegen wirklich funktioniert, ist jeden einzelnen Schutzmechanismus so zu adjustieren, dass er seinen optimalen Wirkungsgrad erreicht und ihn dann mit (vielen) weiteren Schutzmechanismen zu ergänzen. Sogar eine ziemlich lausige Maßnahme (beispielsweise eine, die einen bestimmten Angriff nur in 4 von 5 Fällen abwehren kann) wird dieses Risiko um immerhin 80 Prozent reduzieren. Drei von diesen 80 Prozent-Maßnahmen entfalten zusammen dann schon eine Schutzwirkung von über 99 Prozent. Es fällt nicht schwer, einige simple Schutzmechanismen (und damit meine ich nicht nur technische Maßnahmen, sondern insbesondere kulturelle und menschliche Faktoren) zu finden, die – isoliert betrachtet – einen Wirkungsgrad von 90 Prozent nicht einmal annähernd erreichen. Aber in Kombination sind sie dann doch äußerst wirkungsvoll. Und sie umzusetzen und einzuhalten ist in aller Regel auch viel billiger und einfacher als das, was wir heute machen.

Es ist ziemlich leicht, die Probleme, die eine Organisation mit Viren und Würmern hat, um 90 Prozent zu reduzieren.

Beispielsweise ist es ziemlich leicht, die Probleme, die eine Organisation mit Viren und Würmern hat, um 90 Prozent und mehr zu reduzieren.

Glossar

Bot:
Abkürzung für „Robot" – Software, die bestimmte Aktionen auf einem Internet-Server oder dem PC ohne weiteres Zutun immer wieder ausführt.

DDoS = Distributed Denial of Service:
Abschuss eines Servers durch verteilte Angriffe, die zur gleichen Zeit von vielen Standorten den jeweiligen Server mit Datenmüll bombardieren.

DMZ = Demilitarized Zone:
„Entmilitarisierte Zone". Eine DMZ ist ein eigenes, entkoppeltes und isoliertes Teilnetzwerk, das zwischen das zu schützende Netz (LAN, Intranet) und das Internet geschaltet wird.

DNS = Domain Name System:
Das DNS verwaltet die Domains und ordnet diesen eine eindeutige IP-Adresse zu. Dadurch gelangt ein Benutzer über die Eingabe des Domainnamens zur gewünschten Internetseite.

Firewall:
Filter zum Internet /Intranet. Rechner oder Software, die das lokale Netz gegen Zugriffe durch fremde Hacker, Viren u. ä. abschirmt.

IDS = Intrusion Detection System:
Bezeichnung für ein System, das abnormale Vorgänge in Netzwerken aufspürt. Ein IDS macht den zuständigen Administrator auf den Vorfall (beispielsweise geänderte Systemdateien, Port-Scans etc.) aufmerksam und sichert dadurch – genau wie Firewalls – Netzwerke ab.

IP-Adresse:
Numerische eindeutige Adresse für jeden Rechner im Internet (z. B. 195.0.21.23), über die ein Rechner eindeutig identifizierbar und adressierbar ist. Die Übersetzung von Domainnamen in eindeutige IP-Adressen geschieht mit Hilfe des DNS.

IPsec = Internet Protocol Security:
Übertragungsprotokoll, das eine sichere Übertragung von Informationen über das Internet ermöglicht.

ISP = Internet Service Provider:
Anbieter von Internetleistungen.

Logging:
Die Protokollierung der Ausführung bzw. versuchten Ausführung von Funktionen (insbesondere derer, die gegen die Sicherheitsrichtlinien verstoßen) zum Zwecke der Revision, der Entdeckung von Sicherheitsverstößen und der Beweisführung.

MMS = Multimedia Messaging Service:
Der MMS ermöglicht das Versenden von Multimedia-Nachrichten von MMS-kompatiblen Mobiltelefonen an E-Mail-Empfänger oder an andere MMS-taugliche Handys. Beispielsweise können via MMS Fotos, Animationen, Melodien und Texte versendet werden.

NetBIOS = Network Basic Input/Output System:
Ein von IBM entwickeltes Netzwerkprotokoll.

Proxy = Stellvertreterdienst:
Ein Proxy-Server ist ein Rechner, über den Anfragen aus dem Intranet ins Internet weitergeleitet werden und der damit eine Kontroll- und Schutzfunktion übernimmt.

RPC = Remote Procedure Call:
Ein vom Betriebssystem verwendetes Kommunikations-Protokoll. Ein RPC ermöglicht den Aufruf von Programmen oder Prozeduren über ein Netzwerk, so als wären diese auf dem eigenen Computer vorhanden.

Script-Kiddie:
Skript-Kiddies sind meistens zwischen 12 und 16 Jahren jung und gelten unter Hackern als eine eher niedere Lebensform. Skript-Kiddies sind keine Programmierkünstler und wissen in der Regel gar nicht genau, was sie tun, wenn sie Skripte aus dem Internet herunter laden, mit ihnen herumspielen und auf diese Weise neue Viren in die Welt setzen.

SSH = Secure Shell:
Sichere Alternative zu Telnet, mit der die Session verschlüsselt und somit abhörsicher gemacht wird.

SSID = Service Set IDentification:
WLAN-Clients nutzen die SSID, um sich in eine Funkzelle einzubuchen.

SSL = Secure Socket Layer:
Populäres Verschlüsselungsverfahren, das sichere Datenverbindungen ermöglicht.

Trojaner:
Getarntes oder verstecktes Computerprogramm, das sich in ein fremdes Computersystem einschleust.

VPN = Virtual Private Network:
Ein Netzwerk, mit dessen Hilfe unterschiedliche Standorte via Internet verbunden werden. Durch die verwendete Abschirmung (Tunneling) gilt ein VPN als abhörsicher.

Warez:
Raubkopierte bzw. illegale Software, Filme, Musik, Seriennummern etc.

WEP = Wired Equivalent Privacy:
Verschlüsselungsmethode, die in drahtlosen Netzen zum Einsatz kommt.

WiFi = Wireless Fidelity:
Kabelloses Netzwerk (Funknetzwerk).

Wurm:
Programm, das sich (weitgehend selbstständig) durch Kopieren von Computer zu Computer ausbreitet und die einzelnen Rechner schädigt.

Aber der Versuch, dies mit einem Update der Antivirus-Software zu erreichen, ist von vornherein zum Scheitern verurteilt. Über 600 Kunden wenden unser Risikomanagement-Programm an. Auf der Grundlage dieser Erfahrung kann ich Ihnen sagen, dass ein solcher Rückgang erst durch die Kombination von einem halben Dutzend gut aufeinander abgestimmten Maßnahmen erreicht wird, wie beispielsweise die richtigen Policies, genau definierte Prozesse, Filterung von E-Mail-Attachments, sinnvolle System-Konfiguration (besonders von Routern und Outlook) etc. Selbst mit der Anwendung einer drei Jahre alten Antivirus-Policy von TruSecure hätten Sie 2003 alle Virenangriffe unbeschadet überstanden – egal, ob Ihre Antivirus-Software auf dem neuesten Stand war oder nicht.

RISKNEWS: Herr Tippett, in einem Ihrer Thesenpapiere argumentieren Sie, dass ein stärkerer Passwortschutz die Risiken nur minimal reduzieren kann. Warum ist das so und was sollen wir dann tun?

Tippett: Cracking-Tools arbeiten unglaublich effizient, wenn sie gezielt gegen eine Organisation eingesetzt werden. Nehmen wir an, Sie haben 1.000 Angestellte und irgendjemand knackt ihre zentrale Passwort-Datei. Wenn Sie in Ihrer Organisation 5-stellige Passwörter verwenden, fallen dem Angreifer vielleicht 500 User-IDs und Passwörter in die Hände. Wenn Sie Ihre Mitarbeiter dazu zwingen, 8-stellige Passwörter mit Zahlen und Sonderzeichen verwenden und diese alle drei Monate wechseln, dann mögen es „nur“ 200 User-IDs und Passwörter sein … In beiden Fällen kann der Bösewicht hunderte von Benutzerkonten für seine heimtückischen Absichten nutzen. Sicherheitsexperten müssen aufhören, Ratschlägen zu folgen, die nur in sehr begrenzten Situationen einen Sinn ergeben. Stattdessen sollten sie lieber daran arbeiten, die Wahrscheinlichkeit zu verringern, dass irgendjemand die zentrale Passwort-Datei klaut.

Sicherheitsexperten müssen aufhören, Ratschlägen zu folgen, die nur in sehr begrenzten Situationen einen Sinn ergeben.

RISKNEWS: IT-Sicherheits-Experten diskutieren sehr häufig über Verletzbarkeit und Bedrohungen und nicht über Risiko. Aus Ihrer Sicht: Was ist der Unterschied zwischen IT-Security und IT-Risikomanagement?

Rochford: IT-Security sind die Methoden und die Werkzeuge, die benutzt werden, um etwas abzusichern. Dazu gehört auch das Wissen über sicherheitstechnische Methoden, wie etwa das Einrichten einer Firewall. Risk Management ist demgegenüber der Plan, der alles zusammenhält.

Risk Management ist der Plan, der alles zusammenhält.

Zum IT Risk Management gehören etwa eine IT-Security-Policy oder das Erstellen von Notfallplänen, basierend auf entsprechenden Risiko-Analysen. Selbstverständlich fallen auch die präventive Schadensminimierung sowie die Risiko-Einschätzung ins Aufgabengebiet des Risikomanagements. Welches Risiko kann toleriert werden? Lohnen sich bestimmte Risiko-Steuerungsmaßnahmen aus betriebswirtschaftlicher Sicht?

IT-Security-Experten vergessen oftmals, dass normalsterbliche Benutzer einfach nicht die Zeit oder den technischen Hintergrund haben, um sich mit der IT-Sicherheit herumzuschlagen. Denen sollte das IT-Risikomanagement unter die Arme greifen und sie dabei unterstützen, dass beide Seiten zu einer Übereinstimmung kommen. Wenn man es ganz einfach erklärt haben möchte: Security sind die Truppen, Risk Management das Offizierskorps.

Security sind die Truppen, Risk Management das Offizierskorps.

Ich denke schon, dass es einen klaren Trend zum Risk Management gibt. Risikomanagement ist sinnvoll, notwendig und effektiv. Auch aus einem recht kleinen Budget kann gutes Risikomanagement vieles für die IT-Sicherheit herausholen. Im heutigen Zeitalter der knappen IT-Budgets ist das sehr wichtig. Indem man Unmengen an Geld für IT-Sicherheit ausgibt, wird man noch lange nicht sicherer.

Tippett: Eigentlich sollte es gar keine Unterscheidung zwischen IT-Sicherheit und Risikomanagement geben. Risikomanagement ist ein Weg, die Sicherheit zu erreichen, die wir uns alle wünschen. Tatsächlich sind die meisten Sicherheitsexperten, Forscher und Anbieter aber Techniker, die größtenteils die Ausschaltung von Sicherheitslücken, Einzelplatzsysteme, Firewalls etc. propagieren und bestehende Probleme mit zweiwertigem Denken und Ingenieurslogik lösen wollen. Stattdessen bräuchten wir Risiko-Modelle, vernetzte Computer, synergistisches Denken und eine wissenschaftliche Herangehensweise. Wenn es uns nicht gelingt, auf Risikomanagement und wissenschaftliche Methoden umzuschalten, werden wir immer mehr Geld ausgeben und immer weniger dafür kriegen. Wie haben keine große Auswahl mehr.

Eigentlich sollte es gar keine Unterscheidung zwischen IT-Sicherheit und Risikomanagement geben.

RISKNEWS: „Wireless Networking“ und Funknetzwerke sind in aller Munde. Während viele Unternehmen diese Technologie aus Sicherheitsgründen ablehnen, setzen sie andere ohne jede Bedenken ein. Können Sicherheitsüberlegungen ein Argument gegen „Wireless LANs“ sein? Oder werden Anbieter von Netzwerkkommunikation dieses Problem lösen? Welche Maßnahmen können Unternehmen ergreifen, um solche Risiken zu reduzieren?

Tippett: Einerseits sind die Risiken der drahtlosen Vernetzung weit übertrieben. Sicher … in drahtlose Netze kann man unglaublich leicht einbrechen und sie ausspionieren. Sicher … die WEP-Verschlüsselung ist relativ einfach zu knacken. Aber wenn Sie einige einfache Dinge in Ihrem Büro umsetzen, wie z. B. einen externen drahtlosen Zugang zu ihrer DMZ nur über Ihr VPN-Gateway zu gewähren, wird es keinem User gelingen, irgendetwas zu tun, ohne dass er den verschlüsselten IPSec- oder einen ähnlichen VPN-Tunnel benutzt. Fügen Sie eine relativ schwache WEP-Verschlüsselung hinzu, wenn Sie noch etwas Schutz auf einer zweiten Ebene wollen. Vielleicht mit Ausnahme von raffinierten, gezielten Angriffen sind Sie damit schon ziemlich gut geschützt. Um drahtlos im Büro zu kommunizieren, nutzen Ihre Mitarbeiter nun das gleiche VPN, mit dem sie sonst von zu Hause arbeiten. Und wenn die Nutzer auch in ihrem Home-Office drahtlos arbeiten wollen (und 30 Prozent der technikbegeisterten User wollen das), hilft Ihr VPN auch bei der Absicherung dieses Bereichs.

Rochford: Das größte Problem bei WiFi ist, dass es nicht physisch begrenzt ist. Wenn ein Unternehmen ein verkabeltes Netzwerk baut, dann ist jedem klar, wo es beginnt und wo es endet. Ausgänge, wie etwa der Internet-Zugang, werden dann eben mit Firewalls und Ähnlichem abgeschottet. Beim Funkverkehr gestaltet sich das etwas schwieriger. Der Strippenzieher freut sich über weniger Arbeit. Der Hacker, der auf dem Parkplatz mit seinem Laptop steht, aber auch.

Bisher gehen die meisten Hersteller das Problem mit Verschlüsselung und Zugangscodes an, allerdings scheinen die meisten Algorithmen schlecht oder zu schwach konzipiert zu sein. Mit genügend Rechenzeit kann man viele durchbrechen … wenn der System-Administrator die Verschlüsselung überhaupt aktiviert hat. Vielleicht wird ein Hersteller eine gute Idee haben, um Funknetzwerke sicherer zu machen. Vielleicht wird es auch bessere Verschlüsselungsmethoden geben.

Tippett: Die kommenden Sicherheitsstandards für drahtlose Netze und viele der heute schon erhältlichen propriäteren Lösungen sind um Dimensionen robuster als WEP. Sie lassen sich auch viel besser an die Bedürfnisse von

professionellen Anwendern anpassen. Aber wenn ein drahtloses Netz Ihr Business effizienter macht, sollten Sie es trotzdem schon heute installieren.

RISKNEWS: Wir beobachten noch einen weiteren Trend. Informationstechnologie und andere Geräte, wie etwa Mobiltelefone, Fernseher oder der Kühlschrank, wachsen immer enger zusammen. Welche Sicherheitsargumente sollten in diesem Zusammenhang berücksichtigt werden?

Rochford: Spätestens wenn Sie nach Hause kommen und Ihre Küche wie ein Saustall aussieht, weil jemand die Kaffeemaschine und den Toaster angewiesen hat … Scherz beiseite – ich denke, dass ist schwer vorherzusagen.

Tippett: Momentan – und auch für die absehbare Zukunft – sind die Sorgen über Angriffe gegen PDAs und Handys (und ganz sicher auch Fernseher und Kühlschränke) größtenteils nur Panikmache. Theoretisch gibt es Angriffsmöglichkeiten, und einige davon lassen sich auch schön demonstrieren (beispielsweise gegen Bluetooth). Aber allein aufgrund der Tatsache, dass eine Angriffsmöglichkeit existiert und Ihnen irgendjemand zeigen kann, dass es funktioniert, entsteht noch kein ernst zu nehmendes Risiko.

Rochford: Ich kann Ihnen auch noch einige Gründe aufzählen, warum diese Anwendungsbereiche viele Vorteile gegenüber einer Bedrohung für den heimischen PC haben. Zum einen werden solche Geräte baugleich in großer Stückzahl hergestellt. Das heißt, dass sich die Hersteller nicht um unzählige Versionen kümmern müssen und die Software selbst hoffentlich ausgereifter auf den Markt kommen wird. Auch Security Updates können schneller bereitgestellt werden. Da viele dieser Geräte außerdem mit dem Netzwerk des Herstellers verbunden sind, können sie besser und ohne Aufwand des Benutzers auf den neuesten Stand gebracht werden. Ein Beispiel sind die Mobiltelefone, die Sie eben erwähnt haben. Beim Einschalten und im normalen Betrieb meldet sich das Telefon mehrmals beim zuständigen Netzbetreiber an. Ein Sicherheitsupdate einzuspielen oder sogar per Daten-MMS an das Gerät zu schicken, ist da eine effektive Möglichkeit für Software-Updates.

Ein weiterer Grund ist auch die Funktionsbeschränkung. Mit einem Kühlschrank etwa kann man nur wenig Schaden anrichten. Die Soft- und Hardware ist ja eher spartanisch ausgestattet. Also mit wenig Speicher, geringer Leistung und minimaler Software-Funktionalität. Dennoch wird es in der Zukunft sicherlich Probleme geben. Wie auch in anderen Bereichen wird momentan der ständige Wettkampf um Kunden mit immer neuen Funktionen angeheizt. Außerdem steigt das Tempo durch die kurze Lebensdauer einzelner Modelle. Viele Mobiltelefone werden daher schon mit fehlerhaftem Betriebsystem ausgeliefert. Bei anderen Geräten läuft es ähnlich. Mit der organizer-ähnlichen Ausstattung vieler Telefone – von Kamera- und GPS-Features ganz zu schweigen – werden diese auch für Verbrecher, Hacker und sogar Virenschreiber immer interessanter. Stellen Sie sich vor, Sie können ausspähen, wo sich jemand gerade aufhält und unter Umständen sogar die eingebaute Kamera seines Telefons benutzen, um zu sehen was er gerade macht? 1984 ist vielleicht doch 2004!

RISKNEWS: Herr Rochford, Herr Tippett … vielen Dank für das Interview!

<Das Interview führten Dr. Roland F. Erben und Frank Romeike>

<Allein aufgrund der Tatsache, dass eine Angriffsmöglichkeit existiert und Ihnen irgendjemand zeigen kann, dass es funktioniert, entsteht noch kein ernst zu nehmendes Risiko.