AK Sicherheit, 03.09.2008, Protokoll

13:00 Registrierung

13:30 Begrüßung und Vorstellung

13:45 Wie der CISO wirkt - Qualitative Wirkungsanalyse, Ergebnisse einer tiefenpsychologischen Studie
Dietmar Pokoyski, known_sense

Herr Pokoyski erläuterte die Ergebnisse einer tiefenpsychologische Security-Studie zu Selbstbild und Wirkungsanalyse des CISO (Chief Information Security Officer), die unter der Leitung von known_sense mit den Partnern EnBW, Pallas, SAP, SonicWALL, Steria Mummert Consulting und Trend Micro kürzlich erarbeitet wurde. Für die Studie wurden 30 Sicherheitsverantwortliche mithilfe morphologischer Markt- und Medienforschung befragt. Die psychologischen Tiefeninterviews dauerten 2 Stunden und wurden mit Vertretern aus Unternehmen zwischen 50 und 110.000 Mitarbeitern geführt (gerundeter Durchschnitt aller Firmen 20.000 Mitarbeiter).

Ziel war die Darstellung und Erforschung des CISO-Berufsbilds, wobei hierunter leitende IT-Sicherheitsbeauftragte und verwandte Berufsvertreter verstanden werden. Dabei ging es nicht wie in quantitativer Forschung um Kennzahlen und weniger um das Technische oder Organisatorische der Informationssicherheit, sondern mehr um das Menschliche und (Unternehmens)-"Kulturelle".

CISOs agieren oft in einer Spaltung, weil sie spüren, dass Sicherheitsrisiken eingegangen werden müssen, um insgesamt für eine stabilere Sicherheitskultur zu sorgen. Sie arbeiten im Verborgenen ("Digitaler Untergrund"), müssen aber in der analogen Realität wirken. Welche Strategie sie dabei anwenden, hängt davon ab, wie stark die in der Studie herausgearbeiteten drei Basistypen in ihnen vertreten sind: der zentrale Kontrolleur, der unauffällige Helfer und der bewegliche Streetworker. Pokoyski schlägt vor, dass CISOs eine Marke in ihrem Unternehmen bilden sollen, um Sicherheit lebendig zu halten und ein hohes Involvement zu erreichen.

In der anschließenden Diskussion wurde deutlich, dass tiefenpsychologische Befragungen noch ungewohnt sind, aber einen weiterführenden Beitrag leisten können.

Die Folien des Vortrages sind im Dokumentenweb des Arbeitskreises verfügbar.

14:30 Rechtliche Stellung des CISO
Jens Eckhardt, JUCONOMY Rechtsanwälte

Herr Eckhardt führte zunächst aus, dass kein allgemein einheitlich gesehenes CISO-Berufsbild existiert. Auch kann man aus dem rechtlichen Umfeld (insbesondere TGK und BDSG) zwar Hinweise auf Verantwortungsbereiche herauslesen, aber eigentlich "kenne das deutsche Recht den CISO nicht". Um so wichtiger ist eine möglichst konkrete Beschreibung seiner Tätigkeit im Arbeitsverhältnis. Bei der Haftung muss zwischen Außen- und Innenhaftung unterschieden werden, für eine Haftungsbegrenzung ist seine Arbeitnehmerstellung und sein Sorgfaltsverhalten zu beachten.

In der Diskussion wurde besonderes Gewicht auf die Stellenbeschreibung und ihre regelmäßige Prüfung und ggf. Überarbeitung etwa alle 2 Jahre gelegt.

Die Folien des Vortrages sind im Dokumentenweb des Arbeitskreises verfügbar.

15:15 Kaffeepause & Networking

15:45 Aktuelle Lage im Sicherheitsbereich
Dr. Kurt Brand, Pallas GmbH

Herr Dr. Brand erläuterte die Lage auf der Basis aktueller Security-Studien, insbesondere von IBM und Commtouch. Die meisten Angriffe haben danach das Ziel, den Rechner zu übernehmen und in ein Botnet zu integrieren. Die Botnets stellen deshalb weiterhin die größte Bedrohung dar, sie liefern 85 % des Spam und fast alle Malware. Die Spamquote hat weltweit durchschnittlich 77 % erreicht, große Firmen bekommen häufig schon deutlich über 90 % Spam. Der klassische content-basierte Filteransatz wird mit den ständig variierten Bedrohungen allein nicht mehr fertig, Real-Time-Verfahren zur Abwehr werden immer wichtiger.

In der Diskussion zeigte sich, dass das Thema Botnets in einer Folgesitzung noch vertieft werden sollte.

Die Folien des Vortrages sind im Dokumentenweb des Arbeitskreises verfügbar.

16:00 Ziele und Themen des Arbeitskreises

Die folgenden möglichen Themen für die künftige Arbeit wurden genannt und diskutiert:

- Botnetze
- Schutz und Prävention gegen Denial of Service Attacken
- Sicherheitsprobleme bei großer Systemlast
- BGP-Sicherheit
- DNS-Sicherheit
- Elektronische Gesundheitskarte, Sicherheit usw.
- Mobile Sicherheit

- Sicherheitsbedrohungen für den Mittelstand
- Datenschutzanforderungen im Internet/Plattformen/Web 2.0
- Rechtliche Aspekte, SPAM
- Organisation von IT-Sicherheit und Hilfsmittel hierfür
- Sinn und Unsinn von Audits
- Kosten für Sicherheit und von Sicherheitsbedrohungen/Spam
- Spannungsfeld: Security aus Unternehmenssicht vs. Arbeitnehmervertretung
- Security as a Service

- CISO: Aus- u. Weiterbildung
- Security Awareness
- Sicherheitskultur
- Kommunikation für IT-Sicherheit: Welche Wünsche und Erwartungen haben IT-Anbieter und Anwender an Verbände und Initiativen

16:45 Verschiedenes, nächster Termin

Für den nächsten Termin ist Dezember 2008 (erste Hälfte) oder Januar 2009 (zweite Hälfte) angedacht.

17:00 Ende der Veranstaltung

gezeichnet: Dr. Kurt Brand (Arbeitskreisleiter), 12.09.2008