



Kolloquium des Graduiertenkollegs „Mathematische und ingenieurwissenschaftliche Methoden der sicheren Datenübertragung“

12. Mai 2005, 15.00 Uhr c. t.
FernUniversität in Hagen, Universitätsstr. 11, 58084 Hagen
Raum C 13, 3. Etage im TGZ

"IPsec-basierte VPNs: Anforderungen und Lösungen"

Herr Dr. Bernhard Löhlein

T-Systems International GmbH

Zusammenfassung:

Seit der Standardisierung der IKE/IPSec Protokollfamilie im Jahr 1998 (RFC 2401 und weitere) haben sich neue Anforderungen an VPN-Technologien ergeben, die in den ursprünglichen IKE/IPSec Standards nicht oder unzureichend berücksichtigt wurden. Im Vortrag werden einige dieser Anforderungen diskutiert und mit Vorschlägen aus der IETF und den VPN-Produktherstellern erläutert. Dazu zählen u.a.:

- XAUTH und OTP-Systeme
- NAT-Traversal
- DPD (Dead Peer Detection)
- Redundanzkonzepte

Der Vortrag endet mit der Besprechung eines Fallbeispiels.

"Sicherheitscheck (BIA/TCVA)"

Herr Dr. Burkhard Heyber

SPS Privacy & Security

E-Plus Mobilfunk GmbH & Co. KG

Zusammenfassung:

Es handelt sich um eine Methode, schnell und strukturiert die Sicherheitsrisiken einer IT-Anwendung oder eines IT-Systems zu bestimmen. Als Ergebnis erhält der Auftraggeber eine Einschätzung, wie kritisch das System bzw. die Anwendung für das Unternehmen sind und ob damit zu rechnen ist, dass es zu Sicherheitsvorfällen kommt, die dem Unternehmen schaden könnten. Interessant ist diese Prüfung für neu zu integrierende DV-Lösungen aber auch für Systeme, die bereits seit Jahren im Einsatz sind. Das Vorgehen gliedert sich in drei Phasen.

Phase 1: Schadens-klassifizierung - BIA (Business Impact Assessment) Ein strukturiertes Interview bestimmt das Gefährdungspotenzial des Systems und somit den damit verbundenen Schutzbedarf.

Phase 2: Bedrohungsanalyse - TCVA (Threats, Control and Vulnerability Assessment) In einem moderierten Mini-Workshop von bis zu vier Stunden werden die Wahrscheinlichkeiten geschätzt, dass es tatsächlich zu Sicherheitsvorfällen kommen kann. Dies meist unter Berücksichtigung der bereits bestehenden Sicherheitsmaßnahmen.

Phase 3: Auswertung. In der Auswertung werden die Ergebnisse aus den vorangegangenen Phasen in einer Risikomatrix kombiniert. Das Ergebnis ist eine aussagekräftige, leicht verständliche Darstellung der Risiken und des bestehenden Handlungsbedarfs.

Vorgehen und Inhalte der einzelnen Phasen werden im Rahmen des Vortrags erläutert und mit Beispielen aus der Praxis unterlegt.