

Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

von

Cornelius Höchel-Winter

Inhaltsverzeichnis

INHALTSVERZEICHNIS		I
1	MOTIVATION	1-1
1.1	Eine erste Einordnung	1-3
2	EINE BEDROHUNGSANALYSE	2-7
2.1	Viren, Würmer, Tojaner	2-8
2.2	Externe Angriffe	2-9
2.3	Sonderfall „Wireless LANs“	2-11
2.4	Sonderfall „Mobile Clients“	2-13
2.5	Sonderfall „Remote Zugang“	2-14
2.6	Interne Angriffe	2-15
2.6.1	Beispiele für interne Angriffe	2-17
3	STANDARDS UND GRUNDLAGEN	3-35
3.1	IEEE 802.1X	3-35
3.1.1	Authenticator und Supplicant	3-35
3.1.2	Betriebsmodi	3-39
3.1.3	Sonderfall Shared LANs	3-40
3.1.4	Gegenseitige Authentifizierung	3-43
3.1.5	Authenticator und Authentication Server	3-45
3.1.6	Protokolle	3-47
3.1.7	Unterschiede zu IEEE 802.1X-2001	3-49
3.2	EAP	3-50
3.3	EAPoL	3-51
3.4	RADIUS	3-54
3.5	EAP-Methoden	3-60
3.5.1	EAP-MD5-Challenge	3-64
3.5.2	EAP-OTP	3-65
3.5.3	EAP-GTC	3-66
3.5.4	EAP-TLS	3-67
3.5.5	EAP-MS-CHAPv2	3-69

B	Freeradius	A-141
B.1	Zertifikatsserver	A-141
B.2	Installation des RADIUS-Servers	A-143
B.2.1	Automatisierte Installation	A-143
B.2.2	Installation über den Quellcode	A-144
B.3	Konfiguration des freeradius	A-145
B.4	Grafische Administrationsoberfläche	A-147

ABBILDUNGSVERZEICHNIS **149**

TABELLENVERZEICHNIS **152**

LITERATUR **153**