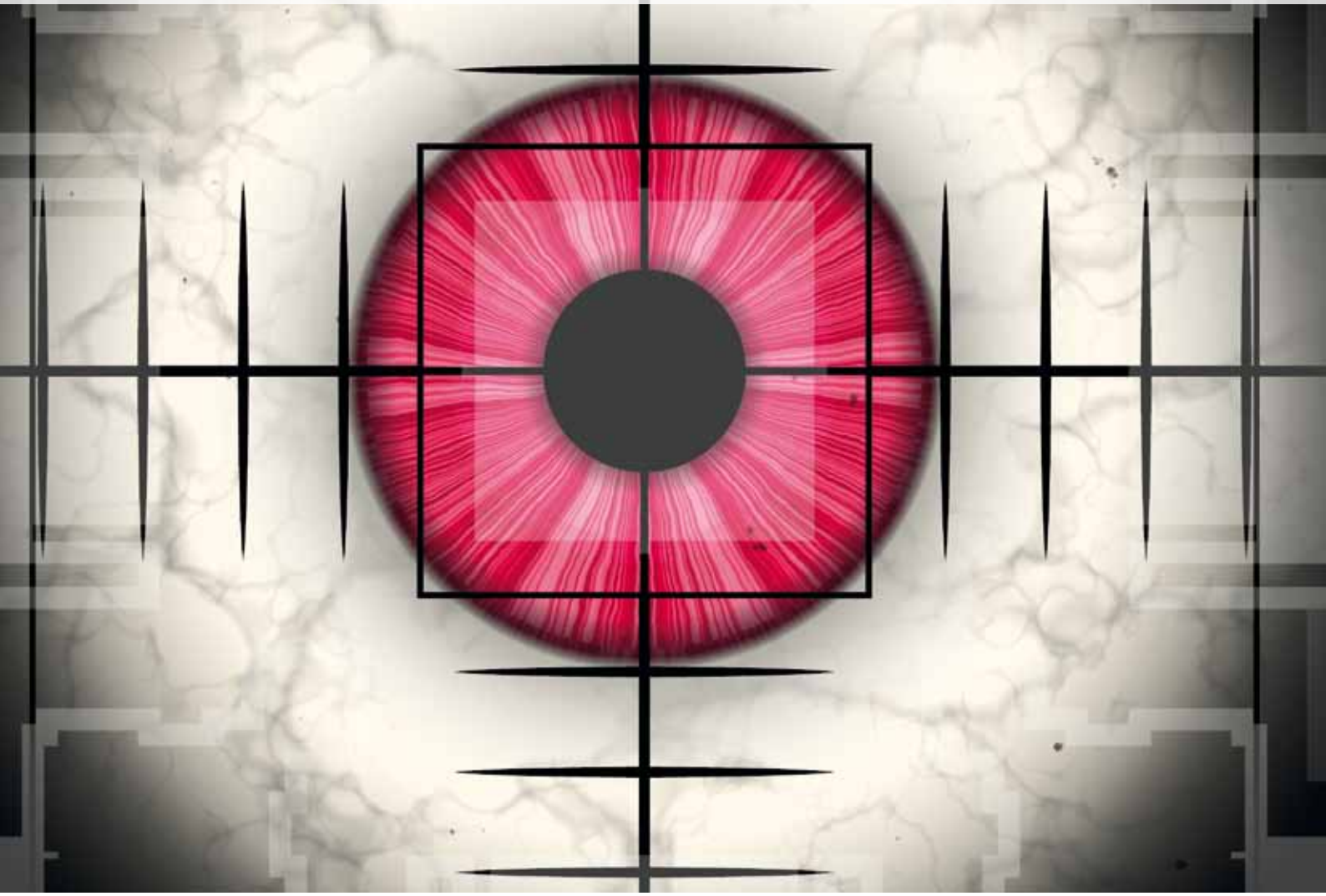
Scan- und Sniffer-Tools in Unternehmensnetzen

„Böses“ für „Gutes“



Hacker-Werkzeuge sind sogenannte Dual-use-Tools: Software-Programme, die sowohl von einem Administrator für seine legitimen Aufgaben benutzt werden können als auch von einem Hacker zur Vorbereitung oder Durchführung einer Straftat. Typische Dual-use-Tools sind Sniffer, (Port-)Scanner und WLAN-Tools. Folgender Beitrag beleuchtet deren Einsatz zunächst unter rechtlichen Aspekten, um anschließend einige der jeweils wichtigsten Werkzeuge aus jeder Kategorie im Einzelnen vorzustellen.

Das Bundesverfassungsgericht kommt in seinem Beschluss[1] vom 18. Mai 2009 zu dem eindeutigen Ergebnis, dass Dual-use-Software von der Strafvorschrift nicht erfasst wird. Der § 202c StGB wurde im Rahmen der Umsetzung des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001 und des Rahmenbeschlusses 2005/222/JI des Rates der Europäischen Union vom 24. Februar 2005 über Angriffe auf Informationssysteme in das Strafgesetzbuch eingefügt. Das Bundesverfassungsgericht führt dazu aus: Im Wege eines vernünftigen Kompromisses beschränke das Übereinkommen seine Anwendbarkeit auf Fälle, in denen Vorrichtungen objektiv in erster Linie dazu gestaltet oder eingerichtet worden sind, eine Straftat zu begehen. Dies allein werde „Dual-use-Vorrichtungen” in der Regel ausschließen. In Bezug auf das Gesetzgebungsverfahren heißt es dann weiter: „Bereits die objektive Beschränkung des Tatbestands auf Computerprogramme, deren Zweck die Begehung einer Computerstraftat sei, stelle sicher, dass keine Computerprogramme erfasst würden, die beispielsweise der Überprüfung der Sicherheit oder Forschung in diesem Bereich dienten.“ Wissenschaftler und IT-Sicherheitsexperten, die Dual-use-Software im Rahmen ihrer legitimen Tätigkeit einsetzen, verstoßen damit nicht gegen den Hackerparagraphen.[2]

Sehr viel kritischer ist die Weitergabe von Dual-use-Software zu bewerten. Im Grunde muss man sich vor der Weitergabe davon überzeugen, dass der Empfänger die Software ausschließlich für legitime Zwecke verwendet. Dies mag in einer IT-Sicherheitsvorlesung oder einer Weiterbildungs-

veranstaltung für IT-Sicherheitsexperten recht einfach sein, auf einem Hackerkongress ist dies schon schwieriger. Grundsätzlich sollte die Software – zur eigenen Absicherung – mit einer klaren Zweckbindung versehen werden. Der Kasten auf der nächsten Seite zeigt ein Beispiel für einen derartigen Text.

Rechtliche Bewertung

Der sogenannte Hackerparagraph schränkt die Nutzung von Dual-use-Tools nicht ein, solange diese von den berechtigten Administratoren im Rahmen ihrer legitimen und vom Arbeitgeber beziehungsweise Auftraggeber vorgegebenen Tätigkeit benutzt werden. Jede eigenmächtige Nutzung aus persönlichem Interesse oder im Interesse eines Dritten zu illegalen Zwecken – etwa die Ausnutzung von Schwachstellen zum Eindringen in ein fremdes Netz ohne Auftrag – ist jedoch strafbar. Je nach Konstellation können die Straftatbestände des Ausspähens von Daten (§ 202a StGB), des Abfangens von Daten (§ 202b StGB), der Datenveränderung (§ 303a StGB) oder der Computersabotage (§ 303b StGB) vorliegen.

Von einer Weitergabe von „Hacker-Tools" an Personen außerhalb des unmittelbaren Kreises der Administratoren des Unternehmens ist abzuraten.

Da alle Kontroll- und Überwachungsmaßnahmen mit den unten aufgeführten Software-Werkzeugen eine Verhaltens- und Leistungskontrolle im Sinne des § 87 BetrVG darstellen, ist die Mitbestimmung des Überwachten zwingend zu beachten. Die Verarbeitung personenbezogener Daten ist rechtswidrig, wenn sie unter Verstoß gegen § 87 BetrVG erfolgt.

Gemäß § 88 TKG dürfen die Telekommunikationsdaten (Inhalte oder nähere Umstände der Telekommunikation) bei erlaubter privater Nutzung nur verarbeitet werden, wenn es zur geschäftsmäßigen Erbringung der Telekommunikationsdienste einschließlich des Schutzes der technischen Systeme des Unternehmens erforderlich ist.

Portscanner und Scanner

Der Ziel sollte es sein, möglichst wenige Tools – im Idealfall jeweils nur ein einziges –für einen Zweck einzusetzen. Mit Portscannern kann ein Netzwerkgerät daraufhin überprüft werden, welche Dienste es anbietet. Einfache Scanner prüfen unter Umständen nur, ob ein Netzwerkgerät vorhanden ist.

Der Einsatz dieser Software zur Untersuchung von Klienten erfordert dessen Mitbestimmung. Darüber hinaus sollten die Beschäftigten zumindest in pauschaler Weise (zum Beispiel in einer Nutzerordnung) darauf hingewiesen werden, dass derartige Tools regelmäßig eingesetzt werden. Eine regelmäßige Analyse des gesamten Netzes ist sinnvoll, um zusätzliche (Fremd-)Rechner zu erkennen. Eine systematische und regelmäßige Untersuchung aller Systeme eines Klienten auf zusätzliche Software und Konfigurationsänderungen bedarf einer Regelungsabsprache mit dem Betriebsrat. Eine nachträgliche Information der Beschäftigten sowie eine detaillierte Information der Nutzer auffälliger Systeme ist erforderlich, damit in jedem Einzelfall geklärt werden kann, ob die Auffälligkeit auf Missbrauch beruhte oder auf einer dienstlichen Notwendigkeit. Die formalen Details (Löschen beziehungsweise Anonymisieren der Berichte, Häufigkeit der Scans) sind mit dem Betriebsrat zu regeln.

NMAP

Nmap[3] ist ein Werkzeug, um Rechner in einem Computernetzwerk zu scannen und zu analysieren. Somit fällt es in die Kategorie der Portscanner. Das Tool zeichnet sich vor allem durch die aktiven Techniken zum Erkennen des eingesetzten Betriebssystems auf dem Zielrechner aus. Es erkennt außerdem aktive Hosts.

Nessus/OpenVAS

Nessus[4] ist ein Vulnerability-Scanner für Linux-, Unix-, Windows- und OS X-Systeme. Nessus basiert auf dem Client-Server-Prinzip. Das heißt, dass auf einem Rechner der Nessus-Server gestartet wird und man sich anschließend per Client mit dem Server verbinden kann. Der Scan wird vom Server durchgeführt. Wurde der Scan gezielt auf einem Rechner ausgeführt, gibt der Nessus-Client eine Übersicht über die offenen Ports (Nessus scannt die Ports mit NMAP) und eventuell gefundene Sicherheitslücken aus.

Nessus steht bis einschließlich Version 2.2 unter der GNU-Lizenz; ab Version 3.0 ist Nessus ein kommerzielles Produkt. Das Open Vulnerability Assessment System (OpenVAS)[5] basiert auf Nessus 2.2 (den letzten frei verfügbaren Quellen) und ist insofern die freie Weiterentwicklung von Nessus. Die Weiterentwicklung von OpenVAS wird in Deutschland ganz wesentlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorangetrieben.

„Ping"-Skripte

Einfache selbst geschriebene Skripte, mit denen nur geprüft wird, ob unter einer angegebenen Adresse ein Rechner aktiv ist, sind rechtlich unbedenklich. Der Betriebsrat sollte aber über den Einsatz informiert sein, wenn Beschäftigten-Rechner „angepingt" werden, da auch dies eine Verhaltenskontrolle mit technischen Mitteln darstellt. Eine Überwachung von Servern ist nicht mitbestimmt.

Sniffer

Ein Sniffer liest den Netzwerkverkehr mit. Dazu wird eine spezielle Hardware oder ein Rechner mit entsprechender Software an einem Messpunkt (spezieller Port einer Netzwerkkomponente oder ein angezapftes Kabel) eingebracht, sodass der gesamte Netzwerkverkehr an dieser Stelle mitgelesen werden kann. Besonders einfach ist es, in einem unverschlüsselten FunkLAN mitzulesen.

Sniffer greifen auf Inhalte des Telekommunikationsverkehrs zu, womit potenziell der Tatbestand des Abfangens von Daten erfüllt ist. Das Sniffen von Datenverkehr ist nur zur Fehlersuche und Problemanalyse zulässig. Die Betroffenen müssen im Vorfeld über das Vorgehen informiert werden. Ist dies nicht möglich, unverzüglich da-

---

1 *http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html*
2 *Siehe dazu detailliert: H. Schuster, DuD 33, 742 (2009)*
3 *http://nmap.org/*
4 *http://www.nessus.org/nessus/*
5 *http://www.openvas.org/index-de.html*

nach. Es versteht sich von selbst, dass die Administratoren über alles, was sie beim Sniffen mitbekommen, absolutes Stillschweigen bewahren.

Ein Sniffer wird eingesetzt, wenn konkrete Fehler- und Problemsituationen auftreten, oder aufgrund eines konkreten Verdachtes. Dieser Verdacht muss vorher dokumentiert werden.

Wird ein Sniffer über einen längeren Zeitraum hinweg oder gar dauerhaft eingesetzt – etwa um Angriffe zu erkennen –, muss von Anfang an detailliert dokumentiert werden, warum diese Maßnahme erforderlich ist. Im Allgemeinen ist dies für Außenstehende nur schwer zu erkennen. Diese „Vorratsdatenspeicherung" entbehrt einer notwendigen Rechtsgrundlage, da die Kommunikationsinhalte bei Bedarf ausgewertet werden können.

Ein Sniffer darf nicht mit einem Intrusion Detection System (IDS) verwechselt werden. Auch wenn ein IDS den Netzwerkverkehr mitliest, ist es kein Sniffer im eigentlichen oder engeren Sinne. Die Besonderheit eines IDS liegt in der unmittelbaren Auswertung der mitgelesen Datenpakete auf potenzielle Angriffe, ohne dass ein Mensch die Kommunikationsinhalte zur Kenntnis nimmt. Ein IDS meldet (von Fehlalarmen einmal abgesehen) nur erkannte Angriffe, also illegitime und unerwünschte Datenkommunikation.

Wireshark

Das Programm Wireshark[6] stellt Daten während oder nach der Aufzeichnung von Verkehr einer Netzwerk-Schnittstelle (typischerweise eine Netzwerkkarte mit dem Protokoll TCP/IP) in Form der einzelnen Pakete dar, so wie sie übertragen wurden. Dabei werden die Daten übersichtlich und nachvollziehbar analysiert. So kann der Inhalt der mitgeschnittenen Pakete betrachtet oder nach Inhalten gefiltert werden. Wireshark generiert auch Statistiken zum Datenfluss und extrahiert binäre Inhalte (beispielsweise Bilder).

Wireshark gilt als eines der besten Sniffer-Tools. Es sollte immer die aktuellste Version eingesetzt werden, da es auch in diesem Programm schon kritische Sicherheitslücken gegeben hat.

Ettercap

Ettercap[7] ist ein Programmpaket, um sogenannte Man-in-the-middle (MITM)-Angriffe im Netzwerk durchzuführen. Neben dem normalen Sniffen kann Ettercap sehr einfach nach beispielsweise Benutzername/Passwort-Paaren suchen. Es führt automatisiert sogenannte Arp-Poisoning-Angriffe durch, um auch in geswitchten Netzen Daten sniffen zu können. Über die MITM-Techniken belauscht das Programm auch verschlüsselte Protokolle im Klartext. Dazu gibt es sich gegenüber dem Klienten als Server und gegenüber dem Server als Client aus. Das dazu erforderliche Umschlüsseln der Daten erlaubt ein Mitschneiden der Daten im Klartext.

Es muss detailliert begründet werden, warum die Notwendigkeit besteht, dieses Programm einzusetzen. Solche Notwendigkeiten dürften nur in sehr seltenen Ausnahmefällen gegeben sein.

Mustertext für die Weitergabe von Datenträgern im Rahmen von Vorlesungen und Seminaren

Es empfiehlt sich, den Datenträger mit dem Text zu „versiegeln" beziehungsweise einen Download nur nach Kenntnisnahme zu ermöglichen.

Die Software auf dieser CD ist ausschließlich zur Benutzung durch die Schulungs-Teilnehmer gedacht. Sie darf nicht in Firmennetze (Intranet) oder das Internet eingestellt werden. Eine Vervielfältigung ist nur mit schriftlicher Einwilligung zulässig.

Es wird ausdrücklich darauf hingewiesen, dass jegliche Software ausschließlich von den an dieser Schulung teilnehmenden Datenschutz- und IT-Sicherheitsfachkräften/an dieser Vorlesung teilnehmenden Studenten und nur zu berechtigten Zwecken im Rahmen ihrer vertraglichen Aufgabenerfüllung/im Rahmen ihres Studiums eingesetzt werden darf. Die Software darf weder auf Rechnern Dritter installiert noch Dritten zur Nutzung überlassen werden. Dritte sind hierbei sowohl externe als auch interne Dritte. Bei einem Einsatz außerhalb dieses berechtigten Bereiches, insbesondere bei einer unbefugten Weitergabe von Software an Dritte, besteht das Risiko einer Strafbarkeit nach § 202c Abs. 1 Nr. 2 Strafgesetzbuch.

WLAN-Tools

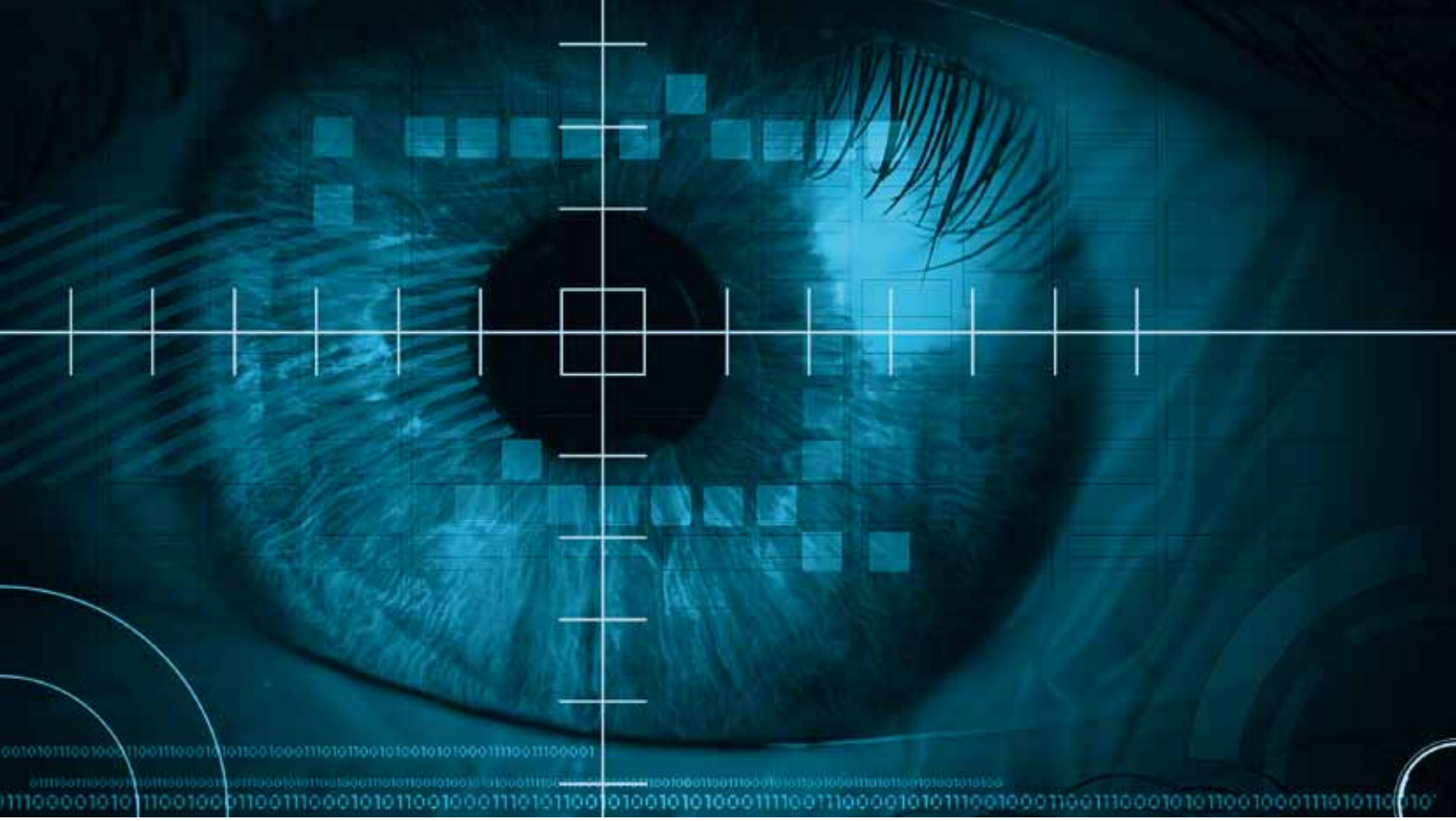
WLAN-Tools sind spezialisiert auf den Einsatz in Funk-Netzen. Hier sind zwei wesentliche Funktionskomponenten verfügbar. Die einen erkennen Funk-Netze und messen auch die Signalstärke, um die Reichweite der Funknetze zu überprüfen. Die anderen versuchen, die Verschlüsselungspasswörter (WEP, WPA, WPA2) zu knacken.

Es gibt aktive und passive WLAN-Scanner. Aktive WLAN-Scanner senden sogenannte Probe-Request-Pakete an den Access Point, welcher daraufhin mit einem Probe-Response-Paket antwortet. Es findet also eine explizite Abfrage statt. Ein passiver Scanner empfängt nur Daten und wertet diese aus. Während ein aktiver WLAN-Scanner in den Log-Dateien eines Access Points entdeckt werden kann, ist ein passiver WLAN-Scanner nicht detektierbar, da er nichts sendet. Ein passiver WLAN-Scanner erkennt nur Funk-Netze, in denen tatsächlich Funk-Aktivität stattfindet.

Der Einsatz eines solchen Programms dient in erster Linie dem Auffinden unbekannter (zum Beispiel von Mitarbeitern eingerichteten) WLAN Access Points und zur Mes-

[6] *http://www.wireshark.org/*

[7] *http://ettercap.sourceforge.net/*



sung der Signalstärke (Reichweite) der eigenen Access Points.

Netstumbler

NetStumbler[8] ist ein lizenzfreier, aktiver WLAN-Scanner für Windows. Das Programm findet WLAN Access Points und erkennt, wenn diese nicht autorisiert sind („rogue APs"). Dazu scannt es die WLAN-Kanäle auf verfügbare Netzwerke (Access Points, Ad-Hoc-WLANs). Auch Hotspots lassen sich auf diese Weise ausfindig machen.

Der Einsatz eines solchen Programms dient in erster Linie dem Auffinden unbekannter (zum Beispiel der von Mitarbeitern eingerichteten) WLAN Access Points und dazu, die Signalstärke (Reichweite) der eigenen Access Points zu messen.

Kismet

Kismet[9] ist ein ebenfalls lizenzfreier passiver WLAN-Sniffer, der Funknetzwerke aufspürt.

Wie Netstumbler wird auch Kismet in der Praxis dafür eingesetzt, sein eigenes WLAN auf Sicherheit zu überprüfen und die Signalstärke (Reichweite) festzustellen. Besonderheit: Kismet entdeckt und zeigt auch Netze, die das Ausstrahlen (Broadcast) der SSID abgeschaltet haben, sobald in einem solchen Netz Datenverkehr stattfindet.

AirSnort

AirSnort[10] ist ein WLAN-Tool, das in der Lage ist, Verschlüsselungsschlüssel (WEP) zu knacken. AirSnort schneidet die Übertragungen im WLAN mit und berechnet den Schlüssel, sobald genügend Datenpakete gesammelt wurden.

Die Notwendigkeit, einen WLAN-Verschlüsselungsschlüssel zu knacken, besteht bei normaler Administrationstätigkeit nicht. Bei den Access Points, die der Administrator verwaltet, kennt er die Schlüssel und alle anderen Schlüssel sind nicht für ihn bestimmt. AirSnort wird seit Anfang 2005 nicht mehr weiterentwickelt. Es gibt aber Nachfolge-Projekte, die aktiv weiterentwickelt werden.

Empfehlung

Die im Unternehmen eingesetzten Tools sollten auf einige wenige konsolidiert werden. Diese Tools sollten für den entsprechenden Einsatz durch einen formalen Akt des IT-Sicherheitsbeauftragten freigegeben werden. Sie gelten dann für die entsprechenden Zwecke als die Standard-Tools des Unternehmens.

Der Einsatz aller anderen Programme durch Administratoren des Unternehmens muss hinsichtlich Einsatzzweck und Erforderlichkeit dokumentiert und begründet werden. Eine Freigabe durch den IT-Sicherheitsbeauftragten erfolgt dann im Einzelfall. ■

Prof. Dr. Rainer W. Gerling,
Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft

[8] *http://www.stumbler.net/*
[9] *http://www.kismetwireless.net/*
[10] *http://airsnort.shmoo.com/*