Cyberkriminelle verstärkt in der mobilen Welt unterwegs

Mit Viren und Schadprogrammen werden inzwischen alle mit dem Internet verbundenen Endgeräte attackiert. Das ist einer der auffälligsten Trends, den der Virenspezialist Kaspersky Lab in seiner Jahresstatis-tik für 2012 ermittelt hat. Im letzten Jahr haben die Antivirenspezialisten über ihre Schutzprogramme mehr als 1,5 Milliarden webbasierte Angriffe abgewehrt, und damit das 1,7-fache des Vorjahres. Mehr als drei Milliarden infizierte Dateien wurden identifiziert. Täglich wurden 200.000 neue Schadprogramme entdeckt. Bei den Smartphones steht vor allem Googles Android im Visier der Angreifer. 99 % der entdeckten mobilen Schadprogramme hätten sich gegen diese Plattform gerichtet. *dpa*

Mehr Privatsphäre auf Facebook

Facebook vergibt seinen Mitgliedern mehr Kontrolle über ihre Privatsphäre. Dafür werden die Einstellungen zur Privatsphäre eindeutiger sortiert und sollen über weniger Klicks erreichbar sein, so Facebooks Datenschutz-Chefin Erin Egan. Facebook sei bewusst, dass Menschen die Plattform nur dann aktiv nutzen werden, wenn sie darauf Vertrauen können, die Kontrolle über ihre Informationen zu haben, betonte Egan. „Wir wollen, dass niemand böse Überraschungen erlebt." Dafür wird nun auch klarer gewarnt, dass Bilder oder Texte trotzdem für andere sichtbar sein können, wenn sie aus der eigenen Chronik entfernt wurden. Das gehörte zu den Empfehlungen der irischen Datenschützer, die Facebook in Europa beaufsichtigen. *dpa*

Health-Cloud im Kommen

Auf der Medica 2012 in Düsseldorf wurde auch deutlich: Die Hersteller von Praxis- und Klinik-IT setzen 2013 auf mobile Kompaktlösungen, die ganze IT-Systeme auf Smartphone und Tablet-PC holen. Es geht also weg von Insellösungen, hin zu vernetzten Systemen – auch bei den mobilen Devices. Aber die Vernetzung von Leis-tungserbringern untereinander, aber auch mit Patienten sowie Medizintechnik- und Telemedizinanbietern wird in diesem Jahr weitaus mehr Raum einnehmen. Die Health-Cloud ist im Kommen: Sie könnte alles vereinen – eine Kommunikationsplattform, aktuelle Praxis-Software ohne hohe Investition und den Datenspeicher. *eb*

gung nur, wenn nicht etwa eine äußere Einwirkung wie eine Überspannung, ein Sturz des Speichersystems vom Tisch oder ein Brand- oder Wasserschaden zur Folge hat, dass gleich mehrere in der RAID-Station verwendete Festplattenlaufwerke gleichzeitig zerstört werden.

Die Krux mit dem Datenschutz

Eine kluge Archivierungsstrategie sieht deshalb auch die räumliche Trennung von Sicherheitskopien und Datenbeständen vor. So kann es sinnvoll sein, eine Kopie der gesicherten Daten auf einem externen Speichermedium nicht in der Praxis, sondern zu Hause oder in einem Bankschließfach zu hinterlegen. Dazu allerdings zwei Hinweise: Zum einen muss natürlich auch eine solche Kopie von Zeit zu Zeit auf ihre Funktionsfähigkeit und Vollständigkeit überprüft werden. Zum anderen sollte der Datenschutz berücksichtigt werden: Patientendaten sind vertrauliche Unterlagen, bei denen Diebstahl oder Verlust sehr unangenehme und aufwändige Konsequenzen haben können. Eine gute Empfehlung zur Absicherung gegen diese Risiken ist eine Verschlüsselung der Daten. Die meisten RAID-Anbieter haben eine Verschlüsselungstechnik gleich mit im Gepäck. Molzen: „Mit Secure Lockware bieten wir ein kostenloses Dienstprogramm zur Verschlüsselung von Daten an. Damit lassen sich komplette Speicherlaufwerke so schützen, dass der Zugriff auf ihre Inhalte nur durch Eingabe eines Kennworts möglich ist. *Hannes Rügheimer*

KBV plant großräumige Vernetzungsoffensive

Die Selbstverwaltung sieht die Hoheit über ihr sicheres Online-Netzwerk in Gefahr – und hat ihr Schicksal damit verknüpft.

Die Vernetzung von Ärzten untereinander muss in den Händen der ärztlichen Selbstverwaltung liegen, so will es die KBV. Die Delegierten der KVen gingen sogar so weit, die Hoheit über die „Online-Vernetzung" der Ärzte mit dem Sicherstellungsauftrag zu verknüpfen. Sie solle als achter Punkt die sieben Bedingungen ergänzen, unter denen die Ärzte bereit sind, auch nach 2017 noch den Sicherstellungsauftrag zu erfüllen.

Hintergrund des Vorstoßes aus dem KBV-Vorstand sind Äußerungen eines Managers der Deutschen Telekom. „Im westlichen Europa sind wir das einzige Land, das im Gesundheitswesen auf einen sicheren Online-Austausch von Daten verzichtet. Dabei ist doch längst unstrittig, dass wir eine gute Online-Vernetzung mit einer einheitlichen Infrastruktur und einem hohen Sicherheitsniveau brauchen", hatte der Leiter des Geschäftsfeldes Gesundheit der Telekom, Dr. Axel Wehmeier, in einem Interview für das Branchendossier „Healthcare 2020" des Marktforschungsinstituts Lünendonk gesagt. Diese Äußerung haben die Ärzte mit Befremden zur Kenntnis genommen. „Gerade die Telekom als zugelassener KV-SafeNet-Provider sollte eigentlich wissen, dass es bereits eine funktionierende Vernetzung gibt", wunderte sich KBV-Chef Dr. Andreas Köhler. Das sichere Netz der KVen werde von 35.000 Ärzten und Psychotherapeuten genutzt und werde von den Landesdatenschützern empfohlen.

Köhler unterstellte Wehmeier einen Angriff auf die Souveränität der ärztlichen Selbstverwaltung. Dessen Äußerung, die Telekom wolle „der zentrale Partner für das gesamte Gesundheitswesen sein, der alle Teilnehmer zusammenbringe", mache die Ambitionen des Dax-Schwergewichts im Gesundheitswesen deutlich. Köhler brachte stattdessen das sichere Netz der KVen als Alternative zur Netzhoheit der gematik über die Telematik-Infrastruktur im Zusammenhang mit der elektronischen Gesundheitskarte ins Spiel. Der KBV-Vorstand erneuerte die Kritik der Ärzte und Psychotherapeuten an den Plänen der gematik zu dieser Infrastruktur, wandte sich gleichzeitig aber gegen einen Ausstieg aus der Entwicklungsgesellschaft. Die Ärzte sollten die Entwicklung der gematik und der Gesundheitskarte aber weiter begleiten, „um Schlimmeres zu verhindern", so Köhler. *Anno Fricke*