# Die fiesen Tricks der Hutträger

Hacker und Onlinespione haben ganz fiese Tricks, um an ihre Ziele zu gelangen: Datenklau oder (Zer-)Störung des gesellschaftlichen Zusammenlebens. Und sie prophezeien, worauf sich speziell die Gesundheitsbranche einzustellen hat. Einer dieser Hacking-Naturen heißt Götz Schartner. Er ist Gründer und Geschäftsführer des IT-Security Unternehmens 8com.

Ich erinnere mich an ihn, Mr. Mühlberger. Wird dieser Profi-Hacker nicht auch beim 14. Wümek in Würzburg den Medizintechnikern richtig einheizen (ab Seite 16)? Nach Auskunft des Organisators Dr. Jürgen Nippa, Präsident des Fachverbands Biomedizinische Technik e. V., will der ‚Tele-Techi' (abgeleitet von technologist) den Teilnehmern zeigen, wie einfach es heute sein kann, vernetzte Systeme zu manipulieren und zu infiltrieren.

Dr. Nippa wird wissen, weshalb er diesen visionären Referenten nach Würzburg holt, Kollege Zimmermann.

Ich stimme ihnen zu, Kollege Mühlberger. Über die vielen Vorteile der Telemedizin haben wir ja schon oft berichtet. Medizintechniker sollten aber wissen, dass nicht alles, was technisch möglich ist, auch erlaubt ist. Kritische Aspekte sieht Oliver Weger von der Kanzlei WWS Wirtz, Walter, Schmitz in Mönchengladbach: Er konzentriert sich mehr auf die juristische Relevanz rund um Ferndiagnosen und Ferntherapien (ab Seite 26). Darüber müssen Ärzte Bescheid wissen.

Zweifelsohne, lieber Dr. Zimmermann, wird das Leben in einer softwaregestützten Hightech-Welt mit fortschreitender Vernetzung sicherheits- und datentechnisch sehr kompliziert werden. Allerdings verbinden die meisten ‚Gesundheits-Apostel' mit der Vernetzung vollkommen hehre Ziele. Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Bitkom rechnet laut einer Studie des Fraunhofer Instituts mit einer jährlichen Einsparung von knapp zehn Milliarden Euro im deutschen Gesundheitssystem. Diese Größenordnung ist demnach aber erst realistisch, wenn eine vollständige Vernetzung und Digitalisierung der Prozesse erfolgt ist.

Wo viel Licht ist, ist bekanntlich auch reichlich Schatten, mein lieber Mühlberger. Mit steigender Komplexität des Gesundheitswesens steigt natürlich die Fehleranfälligkeit. Auch ohne kriminelle Energie durch die ‚Black Hat' – um Ihr Eingangsszenario nochmals aufzugreifen – sind Risiken omnipräsent. Deshalb hat die International Electrotechnical Commission (IEC) die Norm IEC 80001-1 für das Risikomanagement in der medizinischen Informationstechnologie im Oktober 2010 veröffentlicht. VDE und DIVI haben hierzu ein Positionspapier herausgegeben, das Empfehlungen für die praktische Umsetzung gibt. Das Positionspapier Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin gibt es kostenlos zum Download im InfoCenter unter www.vde.com.

Vielen Dank für die praktische Alltagshilfe, geschätzter Dr. Zimmermann. Wer im Januar das Symposium Medizintechnik Aktuell in Ulm – kurz Ulmek (www.ulmek.org) – besucht hat, weiß ebenfalls Bescheid.

Ralf Classen hat dort zum Thema Risikomanagement für IT-Netzwerke mit Medizinprodukten referiert. Wie wichtig diese Norm für Krankenhäuser ist, vermittelt unter anderem die Einschätzung der Rhön-Klinikum AG. Demnach sollen schon im Jahr 2015 Medizingeräte 50 Prozent an den Netzknoten ausmachen.

Mein spontaner Eindruck – ein Eldorado für Digital-Desparados. Deshalb wird künftig dem MIT-Risikomanager wachsende Bedeutung zukommen. Für den einen oder anderen Medizintechniker bestimmt eine interessante Facette für seine Karriere. Sehr vieles, was man dazu wissen sollte, erfährt man auf dem diesjährigen Wümek in einer eigenen Themenschiene Medizin- und Informationstechnik.

Solche Foren sind nicht hoch genug zu bewerten, angesichts dieser Schlagzeile des Antivirussoftware-Herstellers Bitdefender: „Hacking-Attacken auf IT-Systeme und lebenserhaltendes Equipment in Krankenhäusern". Demnach sind Defibrillatoren, Herzschrittmacher, Insulinpumpen und andere softwaregesteuerte medizinische Geräte potenzielle Ziele für Malware- und Hacking-Angriffe.

Tja, lieber Mühlberger. Wir beide werden die rasante technische Vernetzung nicht aufhalten. Trotzdem wird uns dieses Thema künftig begleiten – und natürlich Sie, liebe Leser, Medizintechniker, IT-ler, Manager. Entscheidend ist, abseits der Horrorszenarien rechtzeitig praktikable Abwehrstrategien zu entwickeln. Hören Sie sich in Würzburg an, was Götz Schartner und seine Mitstreiter berichten, und stimmen Sie sich so darauf ein, künftig stärker auf der Hut vor ‚Hutträgern' zu sein!

Eugen Mühlberger
Dr. Wolf Zimmermann