Schutz vor Daten-Dellen

Heute kommt mal wieder eines meiner Lieblingsthemen auf den Redaktionstisch, Kollege Zimmermann: Wie kann es anders sein – die Informationstechnologie. Ich würde sagen, diese Branche weiß um ihre große Verantwortung für die Zukunft. Denn über kurz oder lang werden weltweit alle technischen Systeme softwarebasiert und vernetzt funktionieren – mit all den möglichen Nachteilen wie großflächiger Manipulation und Totalausfall.

Jetzt überraschen Sie mich aber, Kollege Mühlberger. In der letzten KTM-Ausgabe waren Sie noch Feuer und Flamme für Industrie 4.0 – oder besser Krankenhaus 4.0 – und nun rudern Sie zurück. Das gibt mir zu denken, geschätzter Technikus.

Na, ja. Im Grunde sind diese Entwicklungen alternativlos. Schließlich locken die Vorteile der IT wie einfachere Handhabung, Beherrschung der Komplexität und Effizienzerhöhung nahezu überall – also auch im Gesundheitswesen. Wichtig finde ich allerdings, rechtzeitig und konsequent darauf aufmerksam zu machen, dass neben dem vielen Licht, das die IT spendet, auch der damit verursachte Schatten genügend Beachtung findet.

Dabei denken Sie sicherlich an die Mahnung von Ole Sieverding, Cyber-Experte beim Spezialversicherer Hiscox: „Die Kosten eines Cyberschadens nehmen für kleine Betriebe schnell existenzbedrohende Ausmaße an." Geld ist zwar das eine, Verfügbarkeit und Datensicherheit jedoch das andere. Fragen Sie mal die Krankenhäuser, die kürzlich den Krypto-Trojaner auf ihren Systemen hatten, der sich als Rechnung im E-Mail-Anhang getarnt hatte.

Ja, eine dumme Sache, Dr. Zimmermann – beim Öffnen hat er alle vom infizierten Computer aus erreichbaren Dateien verschlüsselt. Und für den Schlüssel sollte man dann zahlen. „Eine Cyber-Versicherung ist daher auch im Gesundheitswesen sehr sinnvoll und eine zusätzliche Schutzmaßnahme", sagt zumindest Ole Sieverding. Interessant finde ich, dass nicht nur die Kosten solcher Hackerangriffe übernommen würden, sondern auch die unmittelbare Unterstützung durch IT-Experten in den ‚passenden' Policen enthalten sein soll.

Na, dann wollen wir hoffen, dass die Schutz-Police in jeder Situation ‚passt'. Es ist bestimmt sinnvoll, frühzeitig nachzufragen, in welchem Verhältnis bei solchen Spezialversicherern Kosten und Leistung stehen. Und wenn beim Gespräch nur erörtert wird, ob derzeit überhaupt ein ausreichender Schutz für die IT gegeben ist. Denn dass es mitunter nicht so ist, hat Kaspersky Lab mit seinem Experiment ‚How I hacked my hospital' demonstriert und kurzerhand probehalber ein Krankenhaus gehackt.

Damit es nicht zu Szenen kommt wie im Fall der Ransomware mit Lösegeldforderungen, als Befunde wie in der ‚Steinzeit' teilweise per Telefon und Fax übermittelt werden mussten, sind Tests nicht das schlechteste. Jedenfalls rät Kaspersky Krankenhäusern, sensible Geräte und Systeme vom regulären IT-Netzwerk zu trennen. Auch sollten sich Krankenhaus-Chefs und Medizintechnikhersteller verstärkt mit dem Thema Cybersicherheit, IT-Sicherheitsschulungen und Sicherheitstests auseinandersetzen.

Dafür haben wir ein perfektes Forum: die conhIT (19. bis 21. April) in Berlin, Europas größter Event in der Gesundheits-IT. Wir beide, lieber Mühlberger, sind wie jedes Jahr dort dabei und sehen, wie rege diese Branche an der Zukunft der Informationstechnologie arbeitet. ‚Vernetzte Medizin' steht dort dieses Jahr ganz groß auf der Agenda. Der IT-Hersteller i-Solutions Health bietet beispielsweise in Kooperation mit dem Institut für Sicherheit und Datenschutz im Gesundheitswesen (ISDSG) IT-Sicherheitsschulungen und -analysen an.

Jetzt, wo das E-Health-Gesetz verabschiedet ist, steigt der Druck. Bestätigung kommt von Axel Wehmeier, Geschäftsführer der Telekom Healthcare Solutions: „Die Digitalisierung des Gesundheitswesens wird in diesem Jahr spürbar Fahrt aufnehmen."

Mancher IT-ler denkt sich vielleicht: „Bei den vielen Millionen IT-Systemen und IT-Netzwerken, die es weltweit gibt, müssen die Black-Hats erst einmal meine Sicherheitslücken finden." Mit Suchmaschinen im Internet der Dinge (IoT) lassen sie sich vergleichsweise einfach aufspüren: wie zum Beispiel mit Shodan, einer Plattform, die auf Knopfdruck zeigt, wo es hakt. Die Liste weiterer Zugangsmöglichkeiten ist lang: per E-Mail, mit verseuchten Datenträgern, die auf dem Mitarbeiterparkplatz gezielt als verloren ‚ausgelegt' werden, oder durch gezielte Anrufe vermeintlicher Krankenhausmitarbeiter, die ihren ‚Kollegen' telefonisch sensible Daten für den Netzwerkzugang entlocken.

Denkbar ist viel, Kollege Zimmermann – machbar allerdings auch. Deshalb braucht das Thema IT-Sicherheit in Zukunft noch sehr viel mehr Aufmerksamkeit. Denn das Gesundheitswesen hat eben eine deutlich größere Verantwortung als manch andere Branchen. Das Kaspersky-Experiment hat gezeigt: Es können kleine, unbeachtete Lücken sein, die den Zugang zum Gesamtsystem freigeben. Beim besagten Krankenhaus war es ein nicht sicher eingerichtetes lokales WLAN, von dem aus jemand in die Infrastruktur des Krankenhauses eingedrungen ist.

Lassen Sie uns, lieber Mühlberger, immer mal wieder das Thema IT-Sicherheit anschneiden, damit es nicht einschläft und Gesundheitseinrichtungen urplötzlich aus dem Schlaf gerissen werden.

Ich denke auch, dass es nicht schadet, wenn die Krankenhäuser als größte Einheiten unseres Gesundheitssystems die IT-Sicherheit ganz besonders ernst nehmen und darin investieren. Nur so lassen sich schmerzhafte Daten-Dellen auf lange Sicht vermeiden.

Eugen Mühlberger
Dr. Wolf Zimmermann