IT-Spezialist Grunow mit marktüblichem Patientenmonitor

Wehrlos 4.0

Internet Die Bedrohung durch Hacker hat eine neue Dimension erreicht. Sie erbeuten nicht nur Daten, sie kapern auch Geräte – und könnten damit Patienten oder Autofahrer gefährden. Die Konzerne fürchten, erpresst zu werden.

Ein Krankenhaus irgendwo in Süddeutschland. Ein Narkosegerät, wie es vielfach in deutschen Operationssälen steht. Der ziehharmonikaförmige Gummibalg, der die Beatmung regelt, pumpt auf und ab. Der Monitor zeigt Beatmungsfrequenz und Sauerstoffsättigung an. So weit, so normal.

Dann ertönt ein schriller Alarmton. Der Beatmungsbalg stoppt, die Steuerungsflächen auf dem Bildschirm sind wie eingefroren. Nichts geht mehr. Das Gerät wurde gehackt.

Es ist ein Test, den der Heidelberger IT-Spezialist Florian Grunow Ende Juli mit Einverständnis des Krankenhauses ausgeführt hat.

Selbstverständlich war kein Mensch an das Narkosegerät angeschlossen, hing kein Leben an der künstlichen Beatmung. Aber, so hat der Test gezeigt, eine Manipulation wäre möglich, während all jener OPs, bei denen der Apparat täglich eingesetzt wird.

Auf dem Video, das die Attacke dokumentiert, ist der Name des Herstellers verpixelt. Er soll Gelegenheit bekommen, die Sicherheitslücke zu schließen.

Florian Grunow hackt medizinische Geräte, um Sicherheitslücken zu entdecken. Bei Patientenmonitoren und MRTs ist es ihm bereits gelungen, sich Zutritt zu verschaffen und die Apparate zu übernehmen. Und nun das Narkosegerät, Fabrikat eines großen Herstellers.

Das Erschreckende: Die Attacke war nicht besonders schwierig. „Jeder mit mittlerem Know-how hätte das machen können“, sagt Grunow. Über das interne Netz-

FOTO: BERT BOSTELMANN / BILDFOLIO / DER SPIEGEL

werk des Krankenhauses schaffte er es, mit seinem Laptop auf die Software zuzugreifen. Mit wenigen Klicks fuhr er das Gerät herunter, die Beatmung stoppte, alle Funktionen waren blockiert.

Grunow hackt solche Geräte, um Unternehmen zu warnen. Doch wie viele Grunows mit weniger lauteren Absichten versuchen Ähnliches? Nicht einmal um tatsächlich einem Menschen während der Operation zu schaden – sondern um Krankenhäuser oder Hersteller zu erpressen?

Hacker gibt es so lange wie das Internet. Jedes digitale Geschäft steht unter dem Risiko, dass sich Fremde Zugang zu sensiblen Bereichen verschaffen. Doch seit das Internet nicht mehr nur Rechner miteinander verbindet, sondern Maschinen, Autos, Haushaltsgeräte, hat die Bedrohung eine neue Dimension. Auch für die Konzerne.

Mit dem Internet verbundene Dinge böten eine „riesige Angriffsfläche“, sagt Christof Paar, Professor für Cybersicherheit an der Ruhr-Universität Bochum. Bislang sei der Schaden etwa bei Angriffen auf PCs meist abstrakt. „Doch wenn Hacker in die physische Umwelt eingreifen, hat das eine neue Qualität.“

Eine gewöhnliche Hackerattacke bestand bisher im Kern meist aus dem Diebstahl von Daten. Das konnten Betriebsgeheimnisse sein, Kunden- oder Kontodaten. Ihr Verlust ließ sich jedoch vor den Kunden vertuschen. Banken ersetzten häufig stillschweigend den Schaden, der durch den Klau von Kreditkarteninformationen entstanden war. Wie gefährdet die eigenen Daten bei Internetanbietern waren, konnten die Kunden oft nicht einmal erahnen.

Wer bei Instituten wie Deutscher Bank und Commerzbank oder den Bankenverbänden nach Schäden durch Hackerangriffe fragt, erntet bis heute nur Schweigen: Nichts ist den Banken so heilig wie der Ruf, so sicher zu sein wie Fort Knox. „Die Dunkelziffer ist deshalb hoch“, sagt Peter Wirnsperger, Partner beim Prüfungs- und Beratungsunternehmen Deloitte.

Doch mit der Vernetzung von Maschinen, der Digitalisierung der Industrie und ihrer Produkte unter dem Schlagwort Industrie 4.0 rückt die Gefahr von Hackerangriffen dem Kunden näher – geradezu körperlich. Und das gefährdet das Geschäft. Wer würde sein Leben einem Narkosegerät anvertrauen, von dem er nicht weiß, wer es gerade in seiner Gewalt hat? Wer würde sich in ein Auto setzen, von dem er nicht weiß, wer es gerade lenkt? Und wer würde es kaufen?

Die neue Qualität der Bedrohung haben auch die US-Hacker Charlie Miller und Chris Valasek bewiesen. Sie ließen die Horrorvision eines jeden Autofahrers Realität werden: Er sitzt hinter dem Steuer, kann das Fahrzeug jedoch nicht lenken.

Es war ein Test für das Technikmagazin „Wired“, der weltweit für Aufsehen sorgte. Ziel der Attacke war ein Jeep Cherokee. Die Hacker beschleunigten das Auto, sie bremsten es ab und brachten es auf dem Highway zum Stehen. Sie hatten sich über die Internetverbindung des Unterhaltungs- und Navigationssystems Zugang zum Steuergerät des Fahrzeugs verschafft.

„Das Experiment hörte auf Spaß zu machen“, schrieb „Wired“-Reporter Andy Greenberg, der bei dem Test hinterm Lenkrad saß. Für den Fiat-Chrysler-Konzern, zu dem die Marke Jeep gehört, war es eine Imagekatastrophe. Das Unternehmen musste rund 1,4 Millionen Autos in die Werkstätten rufen, um das Einfallstor für Hacker zu verschließen. Die gesamte Autobranche ist alarmiert.

Erwartungsgemäß bekunden alle Hersteller, dass Ähnliches bei ihren Fahrzeugen nicht passieren könne, dass Fahrzeugsteuerung und Unterhaltungssysteme streng getrennt seien. Aber sie wissen, dass dies nur ein Teil der Wahrheit ist.

Zur ganzen Wahrheit gehört, dass sich Daimler, Toyota, Volkswagen, BMW und andere Autohersteller ein Technologierennen mit Google und Apple darum liefern, wer das erste autonom fahrende Fahrzeug auf den Markt bringt. Die neue E-Klasse, die Mercedes-Benz vom nächsten Jahr an verkaufen will, ist Teil des Wettkampfs. Das Auto soll beweisen: Die Zukunft des Automobils wird nicht im Silicon Valley gestaltet, sondern noch immer in Stuttgart, bei Daimler.

Die E-Klasse parkt auf Wunsch allein ein und aus, sie kann einem vorausfahrenden Fahrzeug bis Tempo 200 mit entsprechendem Sicherheitsabstand folgen, und sie leitet notfalls eine Vollbremsung ein.

Das Auto kann Schwächen des Fahrers ausgleichen, Unfälle vermeiden und Menschenleben retten. Aber es könnte auch selbst zur Gefahr für seinen Fahrer werden. Denn moderne Autos sind Computer auf Rädern. Sie verarbeiten Informationen von Satelliten, Sensoren und Kameras. Sie kommunizieren mit anderen Autos und sind ständig mit dem Internet verbunden. Und damit wachsen auch die Möglichkeiten, dass sich Hacker Zugriff verschaffen. „Das ist ein Riesenthema für alle“, sagt Daimler-Chef Dieter Zetsche.

Viele Autokonzerne führen deshalb einen besonderen Crashtest durch, bei dem Hacker versuchen, in die Fahrzeugsysteme einzudringen. Welche Spezialisten Daimler unter Vertrag hat, mag Konzernchef Zetsche nicht verraten. Er sagt nur, es seien Menschen „mit hoher Expertise, woher auch immer die stammen mag“.

Die Wahrscheinlichkeit, dass ein Autofahrer Opfer einer realen Attacke wird oder ein Patient stirbt, weil das Narkosegerät während einer OP abgestellt wird, ist gering. Wahrscheinlicher ist, dass Autokonzerne oder Krankenhäuser Opfer von Erpressungen werden.

In der kriminellen Hackerszene sei es schon jetzt eine verbreitete Methode, fremde Computer mithilfe einer Schadsoftware zu sperren und nur gegen Zahlung einer hohen Summe wieder freizuschalten, sagt Experte Paar. Ähnlich könne man auch mit gehackten Autos oder Heizungssystemen Geld erpressen. Oder Unternehmen damit drohen, Sicherheitslücken öffentlich zu machen.

Dass feindliche Übernahmen vernetzter Maschinen prinzipiell möglich sind, gehört vermutlich zu den Risiken, die unvermeidbar sind in einer digitalisierten Welt. So wie Unfälle in einer automobilen Gesellschaft. Blamabel wird es jedoch, wenn die Risiken nicht ernst genommen werden.

„Was die IT-Sicherheit betrifft, ist die Medizintechnik auf dem Stand der Neunzigerjahre“, sagt Hacker Grunow, „die meisten Geräte sind völlig ungesichert.“

Und das Bewusstsein für die Bedrohung ist offenbar gering. Beim Branchenverband

Vom Datenklau …

Ausgewählte Hackerangriffe

Januar
Die Bundesbehörde BSI meldet den Diebstahl von **16 Mio. E-Mail-Adressen und Passwörtern.**

April
AOL gesteht den Verlust einer „beträchtlichen Zahl“ von **Login-Daten** (etwa 2 Millionen).

Mai
Hacker stehlen **145 Mio. Datensätze** des Internet-Auktionshauses Ebay.

Juli
Hacker dringen in eine Datenbank der EZB-Website ein und erbeuten **20 000 E-Mail-Adressen und Kontaktdaten.**

August
Vermutlich über eine Sicherheitslücke in einem Cloud-Dienst erbeuten Unbekannte **private Fotos von rund 100 US-Stars** und veröffentlichen diese teilweise im Internet.

Oktober
100 000 bis 200 000 Fotos von Snapchat-Nutzern werden durch Unbefugte entwendet und teils im Internet verbreitet.

2014

… zur feindlichen Übernahme

Mai
Chris Roberts, Fachmann für Cybersicherheit, erklärt, er habe sich an Bord von Passagiermaschinen rund **15- bis 20-mal erfolgreich in die Flugelektronik eingehackt.**

Mai
Hacker gelangen an **intime Kundendaten des US-Datingportals** Ashley Madison.

Juni
Unbekannte erbeuten über das Netzwerk Parlakom des Deutschen Bundestags unter anderem **vertrauliche Mails von Parlamentariern.**

Juli
Chrysler ruft **1,4 Mio. Fahrzeuge** zurück, nachdem sich in einem Test die Steuerungselektronik kapern ließ.

2015

DER SPIEGEL

Spectaris, der Interessenvertretung der Medizintechnikindustrie, heißt es, man habe erst kürzlich begonnen, sich damit zu befassen. Noch fehle den Verantwortlichen das Know-how, um eine Einschätzung abzugeben, so ein Sprecher. Er müsse oft tagelang hin und her telefonieren, bevor er in den Unternehmen jemanden finde, der sich verantwortlich fühle, sagt Grunow.

Auch das Krankenhausnetzwerk war nur schlecht geschützt. Zwar hat die Klinik die Hacker für den Test des Narkosegeräts freiwillig in ihr System gelassen, doch ein halbes Jahr zuvor hatten sie im selben Haus die Steuerung eines MRT-Geräts übernehmen können – über das ungesicherte Gäste-WLAN, wie Grunow sagt.

Sicher scheint, dass der Kunde jedes Unternehmen abstraft, dessen Produkt als unsicher vorgeführt wurde. So wie es vor drei Wochen dem kanadischen Seitensprungportal Ashley Madison widerfuhr. Hacker erbeuteten die teils pikanten Daten der Kunden. Das Geschäftsmodell, das auf Anonymität und Verschwiegenheit beruht, war ruiniert. Von einem Börsengang ist nun keine Rede mehr.

Doch die Frage ist, ob es der Kunde honoriert, wenn ein Konzern sich bemüht, seine Systeme zu sichern. Der Energiekonzern RWE hatte bei seinem Start in das Geschäft mit dem vernetzten Zuhause eigens Hacker engagiert, um sich in Sicherheitsfragen keine Blößen zu geben.

Von Anfang an begleitete den Konzern die Angst, dass die übers Netz gesteuerten Thermostate, Bewegungsmelder und Stromschalter gekapert werden könnten. Gelänge es Kriminellen, ausgerechnet über RWE-Systeme Zugriff auf Tausende Häuser, Wohnungen und damit auf intime Daten von deren Bewohnern zu bekommen – das ohnehin schon ramponierte Image des Stromriesen wäre vollends dahin.

„Den Entwicklern wurde insofern von der ersten Minute eingetrichtert, dass Datensicherheit bei dem Projekt oberste Priorität hat“, sagt der zuständige Projektmanager Kai Daniel. Entsprechend beherzt gingen die Ingenieure zu Werke.

Sämtliche Funkverbindungen, über die Sensoren und Steuerzentrale im Haus kommunizieren, werden verschlüsselt. Offene Schnittstellen für den Anschluss von Fremdgeräten gibt es nicht. Kundendaten werden nur über gesicherte Verbindungen auf eigenen Leitungen und auf besonders geschützten RWE-Rechnern gespeichert. Zusätzlich engagierte der Konzern mehrere Spezialunternehmen, die Hackerangriffe simulierten.

Das Ergebnis: Der Markt der Haussteuerung und -überwachung per Funk und Internet boomt. Doch ausgerechnet am deutschen Marktführer, der RWE AG aus Essen, geht der Aufschwung ein Stück weit vorbei. Gerade einmal 100 000 Geräte konnte der Konzern trotz guter Tests und Kritiken seines Systems bislang verkaufen.

Das RWE-Produkt erhält von Experten zwar durchweg gute Noten in puncto Sicherheit. Doch es ist teurer als viele Systeme der Konkurrenten aus den USA und Fernost. Gravierender noch: Wegen der aufwendigen Entwicklung hat RWE Probleme, in dem sich rasant entwickelnden Markt mitzuhalten. So können Konkurrenten mit ihren offenen Systemen und Schnittstellen auf Hunderte Zusatzprodukte von Fremdherstellern zugreifen. RWE dagegen muss jede Lichtsteuerung, jede Kamera, jeden Rauchmelder und Wassersensor mühsam auf sein System anpassen.

Doch in einem funktionierenden Markt ist des einen Leid am Ende bloß des anderen Geschäftsmodell. In diesem Fall sind es die Versicherungen, die profitieren könnten – wenn Firmen sich über sogenannte Cyberpolicen gegen die Risiken der Cyberkriminalität absichern.

„Wir stellen eine erhebliche Zunahme an Anfragen fest, und auch die Zahl der Abschlüsse steigt“, sagt Jens Krickhahn, der bei der Allianz-Tochter AGCS für das Geschäft mit Cyberpolicen zuständig ist. Die Nachfrage komme aus allen Branchen, von der Spezialklinik über Handelsunternehmen bis hin zu klassischen Produktionsbetrieben und Energieversorgern.

Ein Industriekonzern habe berichtet, jeden Monat mehr als 1500 ernst zu nehmenden Hackerangriffen ausgesetzt zu sein. So ergäbe sich bei den Industrieversicherungskunden ein Bedarf für Versicherungssummen bis zu 250 Millionen Euro. Solche Schäden müssten allerdings über Versicherungskonsortien abgedeckt werden, erklärt Krickhahn, die Allianz könne einen Versicherungsschutz bis zu 100 Millionen Euro allein tragen.

Auch im Silicon Valley ist man längst dabei, aus dem Sicherheitsrisiko ein Geschäftsmodell zu bauen. „Security as a Service“, so der Branchenslang, boomt. Insgesamt flossen im ersten Quartal dieses Jahres rund eine Milliarde Dollar in Start-ups, die sich mit Sicherheit und Kryptografie beschäftigen.

Zunehmend investieren die Wagniskapitalgeber in Start-ups, die sich nicht auf Unternehmen, sondern auf Onlinesicherheit für Konsumenten konzentrieren. „Die Menschen beginnen sich zu Recht zu fragen, ob sie Technologiefirmen mit ihren privaten Informationen trauen können“, sagt Chris Dixon, Partner bei Andreessen Horowitz, einem der führenden Wagniskapitalgeber des Silicon Valley.

Seine jüngste Investition hat die Firma deswegen in Keybase getätigt, ein Start-up, das Verschlüsselungen für den Alltagsgebrauch tauglich machen will. Mit den Apps sollen Nutzer jede Form von Nachrichten – WhatsApp, Facebook, Twitter oder E-Mail – verschicken können, ohne dass Dritte Zugang erlangen.

Für die Unternehmen steht viel auf dem Spiel. Es geht um einen Milliardenmarkt, der gerade entsteht, und um das Vertrauen der Kunden. Doch das erlangt man nicht dadurch, indem man die Gefahren herunterspielt. Die Konsumenten sollten das Risiko kennen, bevor sie es eingehen.

Frank Dohmen, Dietmar Hawranek, Martin Hesse, Ann-Kathrin Nezik, Thomas Schulz

Hacker Valasek, Miller mit gekapertem Jeep: Auf dem Highway zum Stehen gebracht

FOTO: WHITNEY CURTIS / WIRED.COM