Offen und gefährlich

In immer mehr deutschen Haushalten stehen Geräte, die sich über das Internet fernbedienen lassen. Viele der Webcams und Festplatten sind jedoch nicht geschützt. Bilder aus dem Kinderzimmer, Kontoauszüge, Passwörter – alles landet im Netz. Jeder kann sie finden, und das auch noch legal. Ergebnisse einer monatelangen SZ-Recherche

Von Johannes Boie, Catharina Felke, Vanessa Wormer, Süddeutsche Zeitung – Buch Zwei, 26.11.2016

Jäger sitzt am Küchentisch, es gibt Kaffee und Cola. In der Hand hält er sein Handy, ein paar Meter von ihm entfernt glimmt ein iPad an der Wand. Stefan Jäger, Vater von zwei Kindern und in der Automobilbranche angestellt, sagt, er könne mit den Geräten und einem Internetzugang die ganze Welt steuern. Er meint seine Welt.

Jägers Welt ist ein Smarthome, ein Haus also, das weitgehend von digitaler Technik gesteuert wird. Entweder automatisch, oder, wenn der Besitzer das möchte, auch von seinem Handy aus. Er hat das Haus in der Nähe von Aachen einrichten lassen, 30000 Euro hat er für die digitale Technik und deren Einbau bezahlt.

Jäger kann zum Beispiel seine Steckdosen ein- und ausschalten, wenn seine Kinder in ihrer Nähe spielen. Er kann Lichtschalter so programmieren, dass sie im Sommer die Terrassenbeleuchtung regeln und im Dezember die des Weihnachtsbaums. Er kann über sein System seine Garage öffnen und schließen, Rollos hoch- und runterfahren, er kann die Zimmertemperatur prüfen und sehen, welche Fenster offen oder geschlossen sind. Die Technik, verborgen in einem grauen Kasten im Hauswirtschaftsraum, kennt kaum Grenzen, sie ist nahezu beliebig erweiterbar. Das klingt futuristisch,

ist aber längst Alltag: Bis 2018 werden in Deutschland etwa 720000 vernetzte Häuser stehen.

Es gibt nur ein Problem. Stefan Jäger kann seine Welt steuern – aber auch jeder andere kann Jägers Welt steuern. Weil die zentrale Bedienung seiner Haustechnik für jeden aufrufbar ist, der einen Computer mit Internetzugang hat. Jägers Haus ist komplett ungeschützt. Ein Phänomen der modernen Technik, von dem mittlerweile nahezu jeder Deutsche betroffen sein dürfte, mal mehr, mal weniger direkt.

Mehrere Monate lang recherchierte ein Team der S*üddeutschen Zeitung* Fälle wie den von Stefan Jäger. Dabei geht es nicht nur um ungesicherte Smarthomes, sondern auch um die unterschiedlichsten Geräte, um Fahrzeuge, um Gebäude, die mit dem Internet verbunden sind. Dazu zählen längst auch Toaster, Waschmaschinen, Gewehre, Autos, Saunen, Briefkästen, Kinderpuppen, sogar Sexspielzeug… die Liste ließe sich beliebig fortsetzen.

Während der Recherche fanden SZ-Reporter Webcams, die schlafende Babys zeigen. Bilder aus dem Kinderzimmer, frei verfügbar im Netz. Externe Festplatten, auf denen geheime Dokumente oder private Fotos liegen, intimste Details fremder Leben. Da sind Industrieanlagen, etwa Klärwerke, deren Technik offen liegt, und Geschäfte wie die Tausende Quadratmeter großen Möbelfilialen, deren Heizung jedermann nach Belieben von außen hoch- und runterdrehen kann.

Man muss kein Hacker sein dafür. Im Netz gibt es spezielle Suchmaschinen für Geräte, so wie Google eine Suchmaschine für Webseiten ist. Für diese Recherche verwendete die *Süddeutsche Zeitung* die Suchmaschine Shodan, erreichbar unter shodan.io. Sie spuckt auf Anfrage eine zufällige Liste aller ans Internet angeschlossenen, ungeschützten Geräte aus, die sie findet. Die Liste lässt sich filtern, etwa nach Ländern.

Diese Suche funktioniert recht zuverlässig, weil die Geräte, sei es eine Webcam oder eine externe Festplatte, in der Regel immer online sind. Viele Menschen möchten ihre Heimtechnik schließlich auch dann steuern, wenn sie unterwegs sind.

Ein Beispiel: Jemand stellt eine Webcam im Haus auf und verbindet sie so mit seinem Wlan, dass das Gerät online ist und er somit von unterwegs über das Internet

sehen kann, was die Webcam gerade filmt. Viele Nutzer in dieser Situation glauben, dass die Verbindung sicher ist, weil sie ihr Wlan verschlüsselt haben. Tatsächlich müssten sie aber die Webcam selbst sichern, zum Beispiel mit einem eigenen Passwort. Ohne diese Extra-Sicherung reißt die Webcam eine Lücke ins eigentlich sichere Netzwerk. Die Bilder der Kamera sind nun theoretisch für alle Menschen im Netz einsehbar. Bei ihrer Recherche entdeckten die SZ-Reporter Tausende solcher ungeschützten Zugänge, nicht nur über Webcams, sondern über verschiedenste Geräte. So wie die Steuerung von Jägers Smarthome.

Wer mit Shodan das vernetzte Haus der Familie Jäger gefunden hat, kann dessen Steuerung einfach im eigenen Browser aufrufen. Also in dem Standardprogramm, mit dem man ansonsten auf sueddeutsche.de oder spiegel.de Nachrichten lesen würde. Und schon ließe sich bei den Jägers die Garage öffnen. Wer wissen will, wo genau das Haus steht, um dort einzubrechen oder das Auto zu klauen, muss nur ein wenig kombinieren: Auf Shodan ist der ungefähre Standort des Hauses zu erkennen, in der Haussteuerung, die im Netz einsehbar ist, stehen Hinweise auf den Nachnamen der Familie (der deshalb in diesem Text geändert ist). Der Rest ergibt sich aus dem Telefonbuch und aus Facebook.

Nicht alle Geräte und Gebäude sind so anfällig wie die der Jägers. Atomkraftwerke oder Flugzeuge sind – falls überhaupt – nur von professionellen Hackern zu knacken. Auch mit Passwörtern versehene Geräte können gut geschützt sein. Darum soll es hier aber nicht gehen. Hier geht es um die sehr vielen anderen, ungeschützten Geräte, die bereits zu unserem Alltag gehören. Und in naher Zukunft werden viele Produkte nur noch mit Internetanschluss angeboten werden. Nicht nur, weil die neue Technik bequem für die Kunden ist. Sondern auch, weil einige Hersteller dadurch Nutzungsdaten sammeln – zum Zweck der unauffälligen Marktforschung.

Dass Geräte ungeschützt sind, liegt an Herstellern wie an Kunden. Die Nutzer wollen ein bequemeres Leben. Eine Webcam im Kinderzimmer verspricht Eltern einen entspannten Abend in der Stadt, eine externe Festplatte daheim, auf die man auch vom Arbeitsplatz aus zugreifen kann, erleichtert den Alltag. Jäger etwa sagt über sein Haus: „Wenn wir abends wegfahren und wir fragen uns, ob das Bügeleisen ausgeschaltet ist, schalte ich einfach vom Handy aus die entsprechende Steckdose aus.“ Sich um Sicher-

heitseinstellungen zu kümmern, Passwörter festzulegen und immer wieder einzutippen, das passt nicht zu einem bequemeren Leben.

Es gibt allerdings auch Billig-Produzenten, deren Geräte sich nicht aktualisieren, nicht updaten lassen,wenn eine Sicherheitslücke bekannt wird. Häufig hat es ein Kunde mit zwei Herstellern zu tun – dem Hardware-Produzenten, der zum Beispiel die Webcam baut, sowie dem Software-Produzenten, der für das Betriebssystem des Geräts verantwortlich ist. Das macht die Sache kompliziert. Wer für entstandene Schäden haftet, bleibt häufig unklar.

In Häusern oder Anlagen wird die neue Technik normalerweise von Installateuren und Elektrikern angeschlossen. Für die besteht die Frage nach der Sicherheit oft nur darin, die Drähte hinter der Steckdose sauber voneinander zu trennen. Tatsächlich ist Sicherheit bei digitalen, internetfähigen Geräten aber komplex. In Jägers Fall schreibt Siemens, Hersteller der wichtigsten Teile des Smarthome, der „Inbetriebnehmer“ müsse „im Rahmen der Planung ein passendes Schutzkonzept erstellen.“ Das hat Jägers Elektriker versäumt.

Bevor das SZ-Team zu recherchieren begann, hatte es einen Kodex unterschrieben. Darin steht unter anderem: „Wenn wir auf einer Steuerungsoberfläche landen, drücken wir keine Knöpfe oder ändern Einstellungen.“ Das bedeutet: Erst nachdem die Betroffenen explizit ihr Einverständnis gegeben hatten, wurden Geräte wie Jägers Haussteuerung bedient. So konnte die SZ-Redaktion von einem Rechner in München aus, während sie mit dem Mann telefonierte, in seinem Haus das Licht ausschalten. Meistens aber musste der letzte Beweis aus ethischen Gründen an Ort und Stelle erbracht werden.

Und so begann eine Reise quer durch Deutschland. Oft führte sie zu Menschen, die rein zufällig Opfer unsicherer Technologie wurden, ohne selbst ein Gerät gekauft zu haben. In Köln zum Beispiel arbeitet Claudia B. seit viereinhalb Jahren als Leiterin einer Bäckereifiliale. Das Geschäft gehört zur Marke „Backwerk“, einem Franchise-Unternehmen. Dessen Chef, er heißt in diesem Text Jan Kahrmann, betreibt mehrere Filialen in Köln, eine in Österreich. Kahrmann hat seine Bäckereien mit Sicherheitstechnik ausgestattet, jeder Quadratmeter der Verkaufsräume ist überwacht. Doch alle Kameras sendeten, ohne dass Kahrmann davon wusste und ohne dass Claudia B. es

ahnte, alle Bilder frei ins Internet. Wer B. oder eine ihrer Kolleginnen beobachten wollte, – sei es, um ihnen nachzustellen, sei es, um in ihre Wohnungen einzubrechen, während sie bei der Arbeit waren –, der konnte das jederzeit tun.

Während der Recherche konnten die SZ-Redakteure in München am Bildschirm verfolgen, wie zwei ihrer nach Köln gereiste Kollegen durch die dortige Backwerkfiliale spazierten; wie die beiden in die Sicherheitskameras, die über den Theken mit den Laugenzöpfen und den frischen Baguettes montiert sind, fröhlich hinüber nach Bayern winkten. Oder sonst wohin, man weiß ja nicht, wer gerade noch alles zuschaute.

Kahrmanns Techniker sagte dazu auf Anfrage: „Da haben wir ein größeres Problem, da fehlt ein Update." Für eine Weile waren die Backwerk-Kameras dann auch nicht mehr im Netz zu finden. Doch am Ende gewann das Problem gegen den Techniker. Nach ein paar Tagen konnte wieder jeder Claudia B. bei der Arbeit, Hunderten Kunden beim Einkauf zuschauen. Das ist bis heute so geblieben. Für den unter anderem auf Internetrecht spezialisierten Düsseldorfer Rechtsanwalt Udo Vetter ist das ein Skandal: „Neben der Persönlichkeitsrechtsverletzung ist das auch ein Verstoß gegen das Datenschutzrecht."

Die Bäckereien nutzen die Überwachungssoftware „go1984", hergestellt von der logiware GmbH aus Nordhorn in Niedersachsen. Auch in vielen anderen Fällen stieß die SZ auf eben diese Software. Auf eine detaillierte Anfrage antwortete der Pressesprecher der Firma: „Vielen Dank für Ihre E-Mail, deren unqualifizierten Inhalt wir nicht näher kommentieren möchten."

Auch Gesetzgeber und Verbraucherschutz halten sich zurück, wenn es um das „Internet der Dinge" geht. Ein Gütesiegel auf den Verpackungen, das die Sicherheit von Geräten bewertet, gibt es nicht. So ist eine Welt entstanden, in der Gebrauchsgegenstände, aber auch Gebäude und Industrietechnik zur Bedrohung der Menschen werden können. Die Dinge, die uns umgeben, entwickeln ein Eigenleben, werden zu Augen und Ohren unserer Feinde.

Was nach Thriller klingt, ist längst Normalität. Diese Normalität ist gefährlich. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilt mit, die meisten

Geräte seien „im Auslieferungszustand unzureichend gegen Cyber-Angriffe geschützt und können somit von Angreifern leicht gefunden werden“. Oft bekommen die Betroffenen das gar nicht mit. Der Perverse, der Kinder über die ungeschützte Webcam ihrer Eltern beobachtet, wird die Sicherheitslücke kaum selbst bekannt machen. Der Geheimdienst, der die externe Festplatte eines Bundeswehroffiziers kopiert, wird keine Grußnachricht hinterlassen. Und wer vorhat, Jägers Garage zu öffnen, um dessen Mercedes zu stehlen, wird seine Methode kaum heraus posaunen.

Am Ende machen viele Geräte, die für Sicherheit sorgen sollen, das Leben der Beteiligten gefährlicher. Die wichtigste Komponente in Jägers Smarthome ist seine Alarmanlage. Sie soll sein Haus im einbruchgeplagten Dreiländereck zwischen den Niederlanden, Deutschland und Belgien schützen. In Tür- und Fensterklinken sind Sensoren, die Alarm schlagen, wenn sie sich unerwartet bewegen. Bei Gefahr heult die Anlage auf. Es sei denn, der Einbrecher schaltet sie vor dem Aufbrechen der Tür einfach aus. Auch das war bis vor ein paar Tagen für jeden Netznutzer möglich.

Jäger hat inzwischen reagiert – und am Technikschrank im Erdgeschoss das Internetkabel aus der Wand gezogen. Sein 30000 Euro teures System ist offline. Als Alarmanlage dient ab sofort Ricki. Der Deutsche Schäferhund, zehn Monate alt, ist nicht ans Internet angeschlossen. Zumindest bisher nicht.

Elektronisches Schlüsselloch

Ob Schlafzimmer oder Verkaufsraum – wo Überwachungskameras laufen, finden sich die gefilmten Menschen schnell im Netz wieder

Eine junge Frau, fast noch ein Mädchen, eingehüllt in ihren Wintermantel, starrt auf den Spielautomaten. Immer wieder drückt sie denselben Knopf. Halb zwölf in einer Spielhalle nördlich von Dortmund, es ist die größte Spielhalle in der näheren Umgebung, gleich ist Mittag. Über der Frau hängen Überwachungskameras an der Decke. Der Betreiber der Spielhalle legt Wert darauf, seine Gäste dabei zu beobachten, wie sie ihr Geld verlieren. Doch die Kameras dieser Spielhalle streamen live ins Internet, die Überwachungsbilder von Billardtischen, Geldwechsel- und Spielautomaten sind dort für alle Menschen, die zuschauen wollen, verfügbar. 24 Stunden lang, sieben Tage die

Woche: Theoretisch kann jeder Mensch auf der Welt mit einem Internetanschluss der jungen Frau dabei zusehen, wie sie wie gebannt auf den Spielautomaten starrt, wieder und wieder den Knopf drückt.

Als die SZ die Geschäftsführung konfrontiert, meldet sich ein Techniker: „Es läuft alles über Logins, nur drei Leute kennen die Passwörter." Er irrt. Ein Passwort war nicht nötig, das Überwachungssystem der Spielhalle stand offen.

Und es ist kein Einzelfall. Hunderte Webcams in Deutschland sind wie jene in der Dortmunder Spielhalle online abrufbar, ganz offensichtlich ohne dass ihre Nutzer – oder die Menschen, denen man über die Webcams zusehen kann – davon wissen. Wer sich durch die Streams klickt, sieht etwa Babys in ihren Gitterbettchen. Oder zum Beispiel eine schlafende dunkelhaarige Frau – die Webcam zielt direkt auf ihren Körper. Oder das Mädchen mit blondem Zopf, das auf einer braunen Ledercouch liegt und fernschaut.

Die Sicherheitslücken bieten Fremden an vielen Orten Zutritt: zum Schlafzimmer, Wohnzimmer, Badezimmer, zu Geschäften und Betrieben wie der Spielhalle bei Dortmund oder zu einer Apotheke in Stade. Offen stehen ein asiatisches Restaurant in Hamburg oder Boutiquen in Nordrhein-Westfalen. Gefilmt werden nicht nur die Kunden, sondern oft auch die Mitarbeiter – die Betroffenen wissen davon nichts. Ihr Persönlichkeitsrecht wird dauerhaft verletzt.

Wer Schuld trägt? Mal haben die Hersteller der Webcams oder die Programmierer der Software geschlampt, dann wieder haben die Techniker oder die Nutzer die Geräte einfach zu nachlässig eingerichtet.

Digitaler Tsunami

Wie Kriminelle mit Bot-Netzen Staaten und Firmen angreifen.

Rob Graham, ein IT-Experte aus den USA, bestellt für 55 Dollar eine Überwachungskamera bei Amazon. Kaum geliefert, verbindet er die Kamera mit dem Internet und drückt auf eine Stopp-Uhr. Lange muss er nicht warten. Genau 98 Sekunden dauert es, bis er feststellt, dass das Gerät von einem Computerprogramm aus dem Internet

attackiert wird: Der Angreifer funktioniert Grahams Kamera über das Netz um, ohne deren ursprüngliche Funktion außer Kraft zu setzen.

Es ist eine besonders raffinierte Art des Angriffs. Dabei geht es nicht darum, den Besitzer der Kamera auszuspionieren. Es geht darum, die Kontrolle über das fremde Gerät zu übernehmen und damit eine weit größere Attacke zu starten. Die Netzkriminellen unternehmen solche Angriffe tagtäglich unzählige Male; in aller Regel werden die Geräte dann als Teil eines Netzes aus gekaperten Geräten verwendet: Man spricht von einem „Bot-Netz“. Die Betreiber der Netze, die aus Tausenden oder Millionen einzelner Geräte bestehen, verwenden diese Waffe, um Webseiten wie etwa sueddeutsche.de durch schiere Überlastung zusammenbrechen zu lassen.

Die Internetkriminellen machen sich zunutze, dass internetfähige Geräte – also Kameras, Drucker, Router, Webcams – wie jeder normale Internetnutzer Webseiten aufrufen können. Wenn mithilfe eines Bot-Netzes sehr viele Geräte eine bestimmte Webseite gleichzeitig aufrufen, wird sie überlastet und stürzt am Ende ab. Man spricht in diesem Fällen von einer DDoS-Attacke. Die Abkürzung steht für Distributed Denial of Service, das bedeutet: ein Angriff, der von vielen Geräten gleichzeitig auf ein gemeinsames Ziel erfolgt.

Weil immer mehr Geräte zwar zu Hause stehen, aber von unterwegs gesteuert werden sollen und deshalb viele ungeschützt ans Internet angeschlossen werden, sind manche Bot-Netze mittlerweile riesig und sehr angriffsstark. Die Besitzer der gekaperten Geräte sind ahnungslos. Jan-Peter Kleinhans, der für den Berliner Think-Tank „Stiftung Neue Verantwortung“ das Internet der Dinge erforscht, sagt: „Wenn mein Router infiziert ist und nachts um drei Uhr einen DDoS-Angriff fährt, merke ich das nicht.“

Die Attacken müssen nicht teuer sein, kleine Bot-Netze werden ab 30 Euro pro Tag auf digitalen Schwarzmärkten vermietet. Kriminelle setzen die Netze unterschiedlich ein. Manche wollen die Webseite eines politischen Gegners aus dem Netz schießen, andere den Börsenkurs eines Unternehmens nach unten zwingen, indem sie dessen Angebot aus dem Netz kippen. Auch viele Geheimdienste nutzen die Technologie für ihre politischen Ziele.

Die Attacken werden immer heftiger. In diesem Herbst zielte ein Bot-Netz bislang ungekannter Größe mit Namen Mirai auf einen zentralen Teil der globalen Internet-Infrastruktur. Viele Webseiten waren nicht mehr erreichbar, darunter Amazon und Paypal. Ausgeführt wurde die Attacke hauptsächlich über schlecht geschützte, infizierte Überwachungskameras und digitale Videorekorder eines chinesischen Billigherstellers. Eine weitere Mirai-Attacke traf Internetanbieter in Liberia. Der Angriff war so massiv, dass befürchtet wurde, das ganze Land müsse offline gehen.

Tag der offenen Tür

Smarthomes sind bequem und energiesparend. Wenn sie aber ungeschützt sind, locken sie Einbrecher und Voyeure an

Wer kommt schon gern heim, wenn vor dem eigenen Haus zwei Journalisten stehen und erklären, warum gerade dieses Haus so gefährdet sei? Sandra Wiesel (Name geändert) würde an diesem Herbstabend wirklich lieber weiter telefonieren. Als sie aber begreift, worum es dem Überraschungsbesuch geht, nämlich um die Sicherheit ihrer Familie, bricht sie das Telefonat sehr schnell ab. Ob ein internetaffiner Jugendlicher auf Honolulu, eine sich langweilende Frau in Singapur oder ein Einbrecher aus Regensburg – jeder kann das Haus der Wiesels im beschaulichen Ostbayern steuern: Garagentor auf und zu, Jalousien, Beleuchtung, Temperatur rauf und runter. Selbst der Springbrunnen im Garten lässt sich ein- und ausschalten. Das bestätigt Sandra Wiesel Befürchtungen. Sie hat schon immer gewarnt, dass das Hobby ihres Mannes zu nichts Gutem führen würde. Und das, obwohl der bei der digitalen Technik vom Fach sei.

Wie den Wiesels und den Jägers (siehe Seite 11) ergeht es Tausenden in Deutschland. Häuser, die sich per Internet und Smartphone steuern lassen, sind der neue Standard. Mal rüstet der Eigentümer selber nach, mal baut der Elektriker gar nichts anderes mehr ein. Die Vorteile: die zentrale Steuerung soll durch intelligente Planung Strom und Energie sparen und gleichzeitig den Bewohnern Flexibilität ermöglichen. Der Nachbar will ein Paket abgeben, man ist aber außer Haus? Kein Problem, die Haustür lässt sich unterwegs mit dem Handy öffnen. Zudem sollen die intelligenten Häuser mit ihren ausgeklügelten Alarmsystemen vor Einbruch schützen.

Wer heute baut, setzt auch auf Digitaltechnik, um den Wiederverkaufswert des Hauses hochzuhalten. Hersteller wie Bosch und Siemens haben ihr Angebot erweitert, von der Zentralsteuerung bis zum digital vernetzten Thermostat ist alles zu bekommen. Vorbild ist der US-Konzern Nest. Der ist Teil von Alphabet, jenem Konzern, dem Google gehört. Weil die Hersteller mittlerweile dafür sorgen, dass Produkte verschiedener Marken in einem Haus zusammen funktionieren, erwarten Analysten, dass die Nachfrage weiter wächst. Doch dem bequemen Leben im vernetzten Haus stehen erhebliche Risiken gegenüber: Mit dem Smarthome wird das Zuhause im Wortsinn mit dem Internet verbunden. Das kommt bestimmten Kriminellen besonders gelegen: Einbrechern.

Schiffbruch im Netz

Ein Offizier der Bundesmarine sichert geheime Daten und Dokumente
auf einer offenen Festplatte – jeder kann sie einsehen.

Der Festplattenhersteller Western Digital bewirbt die externe Platte „MyCloud“ wie folgt: „Greifen Sie von jedem beliebigen Ort mit Internetverbindung aus über Ihren Computer, Ihr Tablet oder Ihr Smartphone auf Ihre Lieblingsfotos und -videos zu und teilen Sie diese.“ Das Gerät ist ein Massenprodukt. Menschen sichern damit ihre Daten und freuen sich, auch unterwegs bequem darauf zugreifen zu können.

Einer der Kunden arbeitet im Verteidigungsministerium. Der Kapitän zur See stellt die Platte in seiner Wohnung auf. Er speichert sein komplettes Leben auf ihr ab, privat wie dienstlich. Die Platte dient ihm als Sicherungskopie seines Computers. Da finden sich Kontoauszüge, Kontakte, Fotos, detaillierte Informationen über Familienmitglieder, Kontodaten, E-Mail-Passwörter, ein Lebenslauf seines Kindes samt Foto liegen offen im Netz. Unter den dienstlichen Dokumenten sind eingescannte Truppenausweise, Versetzungsankündigungen, Flottenlisten. Die Namen zahlreicher deutscher Soldaten, Details zu Besatzungen deutscher Marine-Boote, Telefonnummern, Abrechnungen, Dienstzeugnisse, ein für Staatssekretäre vorbereitetes Dokument und ein de-

taillierter, eingescannter Kalender, der über Termine im Verteidigungsministerium aufklärt.

Nichts davon sollte öffentlich sein. Alles davon ist öffentlich.

Die SZ ruft den Offizier an und klärt ihn über die Datenlücke auf. Er sagt, ihm sei bewusst, dass die Festplatte auch von außen zu erreichen sei – „aber doch nur mit Passwort“. Als ihm bewusst wird, dass dem keineswegs so ist, zieht er noch während des Telefonats den Stecker der Festplatte. Details zur Konfiguration des Geräts möchte er nicht preisgeben, es liegt aber nahe: Der Mann hat Fehler gemacht. Western Digital teilt auf Anfrage mit, das Problem ohne weitere Details nicht analysieren zu können.

Die Festplatte des Soldaten wäre ein Volltreffer für Terroristen und Geheimdienste, für Kriminelle, die Identitäten stehlen, Konten plündern oder auch nur Familienmitgliedern des Offiziers nachstellen wollen. Im Rahmen der Recherche finden sich Hunderte solcher Festplatten im Netz, darunter kleine für den Privatgebrauch, wie jene des Offiziers, aber auch ganze Server. Auf vielen von ihnen lagern sensible Daten: Geschäftsgeheimnisse, Passwörter, Fotos von Affären – es gibt nichts, das nicht gespeichert wird.

Klärwerk ohne Filter

Fast alle Industrieanlagen sind heute ans Internet angeschlossen – sehr viele davon mangelhaft. Ihre Technik ist im Netz offen einsehbar.

Er ist Meister im Bereich Abwasserversorgung, im Blaumann sitzt er vor dem Bildschirm und reißt die Augen auf: „Das gibt’s doch gar nicht.“ Neben ihm schaut sein Chef ebenso ungläubig auf den Laptop. Auf dem Rechner ist ein Computerprogramm zu sehen, mit der eine Kläranlage aus der Ferne kontrolliert werden kann. Die Männer kennen die Oberfläche nur allzu gut: Es ist ihr Job, sich um diese Industrieanlage zu kümmern. Aber der Laptop, auf dem nun die Steuerung der Kläranlage in Echtzeit zu sehen ist, der gehört den angereisten SZ-Journalisten. Der Computer ist auch nicht im Netzwerk ihres Arbeitgebers angemeldet, einem Verband aus Wasser- und Abwasserversorgern in Thüringen – der Laptop ist einfach nur mit dem Internet verbunden. Doch ist da der Wasserstand der Kläranlage ablesbar, ebenso die Störmeldungen. „Das ist krass“, sagt der Chef, der als technischer Leiter für 24 Kläranlagen

zuständig ist. Vor zwei Jahren wurden die Klärwerke aufgerüstet; die Techniker können jetzt auch aus der Ferne gucken, ob die Maschine ordentlich läuft, das vereinfacht die Arbeit enorm.

Immerhin: Über das Netz steuern kann man die Kläranlage nicht, weder als Mitarbeiter noch als Eindringling von außen. Lediglich der Status der Maschine ist im Netz abzulesen. Der Hersteller der eingebauten Technik erklärt auf Anfrage allerdings, dass er nicht ausschließen könne, dass man manche seiner Anlagen „auch von außen steuern kann“. Für die Datenverbindung der Anlage ist wiederum ein weiteres Unternehmen zuständig: Unklar ist, wer für den Fehler verantwortlich ist.

Während der Recherchen finden SZ-Mitarbeiter neben Abwasseranlagen auch Heiz-, Belüftungssysteme, Pumpen, Klimaanlagen kompletter Einrichtungshäuser und ein voll automatisiertes Gemeindezentrum frei zugänglich im Netz.

Nicht alle online gefundenen Systeme lassen sich im Netz auch steuern, viele, wie die Kläranlage in Thüringen, zeigen lediglich an, ob das System funktioniert oder ob ein Techniker vorbeischauen sollte. Was ein Angreifer mit der Information anfangen kann, hängt von dessen Absicht ab. Klar ist, dass Sicherheitslücken auch in kritischeren Systemen als Kläranlagen bestehen. Ähnliche Technik wie jene in Thüringen setzt der Hersteller auch in Trinkwasseranlagen ein.

Lücke schließen

Wie man sich vor fremdem Zugriff schützen kann.

Die allermeisten Geräte, sei es eine Webcam, eine Festplatte oder die Steuerung für die Temperatur im Wintergarten, werden mit standardisierten Voreinstellungen geliefert. Voreingestellt sind oft auch Passwörter. Diese werden aber in den Betriebsanleitungen genannt oder lassen sich schnell erraten. So haben Hacker besonders leichtes Spiel, wenn der Benutzername für das Kamera-Babyfon „admin“ (steht für Administrator) und das Passwort „0000“ lautet.

Deshalb sollten diese Einstellungen nach dem Kauf sofort geändert werden; wie das geht, steht in der Bedienungsanleitung, diese lässt sich per Google im Internet

finden, falls man sie verlegt hat. Vor dem Kauf sollte man sich unbedingt vergewissern, dass sich die Einstellungen überhaupt verändern lassen; bei manchen Geräten ist das nicht der Fall. Das BSI hat sämtliche Hersteller aufgefordert, den Nutzern diese Möglichkeit zu geben. Doch der Markt ist sehr unübersichtlich. Es empfiehlt sich daher, beim Kauf auf Markennamen zu achten und Produkte von Herstellern zu bevorzugen, die auf ihrer eigenen Webseite Angaben zur Sicherheit der Geräte machen sowie regelmäßig Updates für die Software bereitstellen.

Diese Updates müssen allerdings auch installiert werden, nur manche Geräte erledigen das automatisch. Sobald eine Sicherheitslücke in einem Gerät bekannt wird, versuchen professionelle Hersteller idealerweise, den Kunden sehr schnell ein Update zur Verfügung zu stellen. Solange es aber nicht installiert ist, bleibt das Gerät verwundbar: Die bekannte Sicherheitslücke kann dann von jedem Angreifer ausgenutzt werden. Das BSI empfiehlt außerdem, die UPnP-Funktion direkt am Router zu deaktivieren. UPnP steht für „Universal Plug and Play“ und ist ein Standard, mit dem Geräte innerhalb eines Netzwerkes kommunizieren. UPnP erleichtert den Nutzern das Leben, leider aber auch Angreifern. Über den Router – also das Gerät, über das alle anderen Geräte zu Hause ins Internet gelangen – kann das UPnP abgeschaltet werden.

Eine komplexere, aber relativ sichere Lösung ist es, die eigenen Geräte in einem VPN zusammenzufassen. Die Abkürzung VPN steht für Virtual Private Network, also für ein privates Netzwerk, das sich allerdings auch durch das öffentliche Internet ziehen kann. Mithilfe eines VPN ist es sehr wohl weiterhin möglich, das eigene Smarthome oder die Webcam zu Hause aus der Ferne über das Internet zu steuern. Aber es geht eben nur mit einem Gerät, zum Beispiel einem Handy, das im selben VPN angemeldet ist wie das Smarthome: Dazu müssen beide Geräten mit dem VPN verbunden sein. Steht diese Verbindung erst einmal, sind die darin verbundenen Geräte für alle anderen Nutzer im Internet unsichtbar und damit geschützt. Voraussetzung ist, dass das VPN ordentlich eingerichtet ist. Weil das nicht immer einfach ist, sollte man sich im Zweifel Hilfe vom Experten holen.