Der Spion, der Staub frisst

Zusammenfassung: Auch vor den Büros macht die smarte Technik nicht halt. Das kann anfangs recht lustig sein, wenn jedoch die Geräte anfangen, sensible Daten nach Hause zu telefonieren, hört der Spaß auf. So ist der Robotsauger, der alle Räume, in denen er ausgesetzt wird, kartographiert, keine Science Fiction mehr, sondern schon Realität. Neue Betätigungsfelder für Datenschutz und Informationssicherheit, aber auch für Hacker, tun sich auf, aber auch neue Verantwortung und Sorgfaltspflichten.

Der Praxisfall: Die Beschäftigten sind mal wieder mit dem Ergebnis der Reinigung im Großraumbüro nicht so ganz zufrieden. Die Reinigungskräfte kommen aber immer erst, wenn niemand mehr da ist, also ist es nicht so leicht, die Reklamation loszuwerden. Da kommt eine Kollegin eines Tages mit einem Reinigungsroboter unterm Arm an. Sie baut die Ladestation auf und lässt den „putzigen" Roboter frei. Der Aufmerksamkeitswert ist – ja nach Erfahrung mit diesen Dingern – selten kleiner, aber fast immer sehr groß. So zieht der Reinigungsroboter seine Runden. Manche werfen ihm Krümel hin, andere Fusseln – das Gerät ist der heimliche Star im Büro. Bis einer der Kollegen sagt: „Wisst ihr eigentlich, dass dieses Gerät einen Plan vom Büro anlegt und den Kolleginnen unter den Rock sieht?" Die Diskussion ist eröffnet.

Smart Home: Alle Welt spricht vom Smart Home. Glaubt man den Werbeversprechen der Hersteller, dann wird vieles im Haushalt der Zukunft wie von alleine gehen. Verlassen die Bewohner morgens das Haus, wird die Heizung gedrosselt, nähern sie sich dem smarten Heim wieder, was über Standortbestimmung erkannt wird, wird es wieder wärmer. Der Kühlschrank erkennt das Mindesthaltbarkeitsdatum von Speisen und meldet sich, wenn das Bier oder ein anderes Nahrungsmittel ausgeht. Die „zauberhaften" Helferlein, zunehmend smart und vernetzt, machen's möglich.

Smart Büro: Kaum jemand spricht bislang vom smarten Büro. Auch hier gibt es mittlerweile jede Menge dieser smarten Helferlein, die schon heute in den Arbeitsalltag eingreifen. Das beginnt bei Multifunktionsgeräten, die über NFC erkennen, wenn ein Berechtigter sich dem Gerät nähert. Ein im Mitarbeiterausweis oder Transponder integrierter RFID-Chip macht's möglich. Türen öffnen sich wie von Zauberhand, wenn die „richtige" Person darauf zugeht. Der Rechner wird von selbst gesperrt, wenn sich der autorisierte Benutzer entfernt. An der Kaffeemaschine wird mit dem Chip bezahlt, die Maschine speichert, welches die bevorzugten Getränke sind und macht entsprechende Angebote. Das Nummernschild wird bei der Einfahrt in die Tiefgarage ausgelesen und dem Einfahrenden wird ein Parkplatz zugewiesen, Lichtsignale führen die Fahrer dorthin. Diese kleine Auswahl soll hier genügen.

Personenbezogene Daten: Alle diese Smarten Helferlein müssen die Person identifizieren, um deren Berechtigung zu prüfen. Identifikation von Personen setzt immer die Verarbeitung personenbezogener Daten voraus. In etlichen dieser Fälle könnten mit den Daten auch Auswertungen erstellt werden, die eine Kontrolle von Verhalten und Leistung der Mitarbeiter ermöglichen. Daher ist – falls vorhanden – in allen diesen Fällen die Mitarbeitervertretung hinzuzuziehen. Ob eine Betriebsvereinbarung erforderlich ist, hängt von den Umständen ab. Klingt schon absurd, oder? „Betriebsvereinbarung zur Nutzung des Kaffeevollautomaten". Auf alle Fälle sind hier neben Datenschutzfragen auch Fragen zum Arbeitsrecht zu stellen und zu beantworten.

Datenschutz? War da was? Datenschutz soll den einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Die EU-DSGVO formuliert das so: Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 EU-DSGVO). Persönlichkeitsrechte an der Kaffeemaschine? Jetzt mal ernsthaft – werden viele Menschen jetzt sagen, die beim Umgang mit ihren personenbezogenen Daten schon „sturmreif geschossen wurden" und denen vieles mittlerweile gleichgültig ist. Der Schutz der Persönlichkeitsrechte gilt aber in jedem Fall, auch wenn es den Betroffenen gar nicht bewusst ist, dass möglicherweise durch smarte Anwendungen diese Rechte verletzt werden können. Datenschutz. Da war doch was.

Viele neue Geräte sind smart: Immer mehr Geräte sind mit dem Internet verbunden und senden Daten an die Betreiber der Geräte oder der Apps. Das ging vor ein paar Jahren los, als die Kopierer per Signal meldeten, dass einzelne Teile ausgetauscht werden müssen. So wusste der Wartungsdienst oft schon vor dem tatsächlichen Ausfall des Geräts von der Schwachstelle und konnte rechtzeitig reagieren. Heute hat nahezu jeder Beschäftigte mindestens ein multifunktionales smartes Gerät dabei – das Smart-

phone. Standorte werden getrackt, der Zugriff auf das Mikrofon, auf Bilder und Videos sowie die Kontraktilste wird erlaubt, oft ohne dass sich die Anwender darüber bewusst sind, welchen Umfang die per Klick eingeräumten Nutzerrechte der Hersteller tatsächlich haben.

Neue Dimension der smarten Haustechnik: Auch in Büros zieht smarte Haustechnik immer häufiger ein. In vielen Fällen macht das auch Sinn. Beleuchtung, die sich danach richtet, ob Personen im Raum sind oder nicht. Das kann zwar peinlich werden, wenn der Bewegungsmelder auf der Toilette zu kurz eingestellt ist. Dort bewegt man sich erfahrungsgemäß nicht allzu heftig, und im schlechtesten Fall sitzt man plötzlich im Dunklen. Hat man doppeltes Pech, reicht der Erfassungsbereich des Bewegungsmelders nicht in die Kabine, da kann man im Dunkeln fuchteln und zappeln, soviel man will. Aber vielleicht (Achtung – Verschwörungstheorie) ist das ja Absicht, damit die einschlägigen Sitzungen nicht zu lange dauern. Der Hinweis für den Besucher: „Achtung, machen Sie rasch auf der Toilette, sonst geht das Licht aus“ klingt jedenfalls lustig. Umgekehrt brennt die Beleuchtung auf den Toiletten dann nicht mehr unnötig.

Zutrittskontrollen ermöglichen Bewegungsprofile: Wird ein Unternehmen konsequent mit elektronischen Zutrittskontrollen gesichert, können beispielweise durch die smarte Technik komplette Bewegungsprofile erstellt werden. Auch diese können zur Kontrolle von Verhalten und Leistung herangezogen werden. Oder umgekehrt zum Aussperren von unerwünschten Personen. Umgekehrt birgt die alleinige Verwendung von Transpondern zur Identifikation die Gefahr, dass sich Angreifer einen solchen Transponder unbefugt aneignen. In der Folge können sie, als der eigentliche Inhaber des Transponders getarnt, in alle Bereiche gelangen, für die dessen Berechtigung eingestellt ist.

Licht und Schatten: An diesen wenigen Beispielen kann man schon sehen, dass dort, wo viele Licht ist, auch Schatten vorhanden ist. Ein zu rasches Einrichten der smarten Helferlein sollte zunächst unterblieben, erst prüfen, dann einrichten. So sollten immer Datenschutz und Informationssicherheit einbezogen werden. Rasch können Persönlichkeitsrechte verletzt werden, ohne dass das den Beteiligten bewusst ist.

Zurück zum Saugroboter: Hat der Kollege nun recht, wenn er behauptet, der Saugroboter zeichnet sich eine Karte des Raumes und sendet diese nach Hause? Wer schon einmal die nimmermüden Versuche eines solchen Saugroboters beobachtet hat, aus eine Ecke, in die er sich hineinmanövriert hat, wieder herauszukommen, zweifelt zunächst einmal an dieser Fähigkeit. Aber das Ziel, seine häuslichen Pflichten zu erfüllen, indem das Gerät in die Ecken fegt, Staub saugt, Tierhaare aufsammelt, vor Treppen zurückschreckt, den Kot der Hundewelpen sehr gleichmäßig verteilt und das möglichst kollisionsfrei, kann offenbar mit der richtigen Technik noch deutlich verbessert werden.

Der Spion, der in den Staub beißt: Der US-amerikanische Hersteller iRobot hat nun sein Spitzenmodell mit genau dieser Fähigkeit ausgestattet, eine Karte der Räume anzulegen, die Effizienz zu verbessern und gegebenenfalls auch die Karte zum Hersteller zu senden. Ziel ist es offenbar, Räume so exakt zu vermessen und zu kartographieren, dass andere Hersteller von Smart-Home-Technik davon profitieren können und bereit sind, dafür einen guten Preis zu bezahlen. Je nach Qualität der Software kann der kleine Spion dann Leitungswege identifizieren, erkenne, wo welche Büromöbel stehen, welche Technik im Raum eingesetzt wird. Für weitere Einsatzmöglichkeiten hätten die Drehbuchautoren der James-Bond-Filme hier jede Menge Anregung. Das saugende Heinzelmännchen könnte Kameras und Mikrofone mit sich führen, auf seinem Weg Funkimpulse auffangen und weiterleiten, Personen identifizieren, auch Besucher – kurz, vieles wäre möglich, und was möglich ist wird eines Tages sicher auch angeboten - oder von Angreifern installiert.

Neues Feld für Hacker: Auch für Hacker ergibt sich ein neues Betätigungsfeld. Die Erfahrungen mit dem Internet der Dinge zeigen, dass derartige Geräte gar nicht bis sehr schlecht abgesichert sind und leicht gehackt werden können. Das kann im privaten Bereich noch egal sein – spätestens im Büroeinsatz ist es das nicht mehr. Wozu solche Geräte sonst noch alles eingesetzt werden können kann man getrost der Fantasie der Leserinnen und Leser überlassen.

Neue Techniken mit Begeisterung und Respekt begegnen: Die Kollegin aus dem Praxisbeispiel hat das Gerät rasch wieder eingepackt, allerdings weniger wegen des Kommentars des Kollegen, sondern weil der Saugroboter kein CE-Zeichen hatte. Und weil eine andere Kollegin einen Rock anhatte und vermutete, dass der Roboter ihr unter den Rock schauen könnte. „Wenn der schon weiß, wo er langfahren soll, hat der doch bestimmt eine Kamera an Bord“, war die Vermutung. Aber auch sonst sollte dieser neuen Technik sowohl mit Begeisterung, aber auch mit einer gesunden Portion Respekt begegnet werden. Lieber zweimal zu viel auf Datenschutz und Informationssicherheit prüfen als einmal zu wenig.

Ein kleiner Ausblick in die Zukunft des Büros und auf den Feierabend der Zukunft: In einigen Jahren gibt es vermutlich personifizierte Roboter-Assistenten, die einem im Büro jeden Wunsch buchstäblich von den Augen ablesen. Sie begleiten einen zum Platz, gehen mit ins Meeting zeichnen alles auf, stellen Informationen auf Wunsch zur Verfügung, kochen einem Kaffee (wenn sie nicht schon eine Expressomaschien eingebaut haben), bringen einem Wasser, wenn man schon längere Zeit nichts mehr getrunken hat, schicken einen zum Betriebssport, erzählen dem Chef, wie oft man wieder über Fußball und andere Themen mit den Kollegen geredet hat, schickt einen verspätet in den Feierabend usw. Und der persönliche Robotassistent der Vorgesetzten kann Massagen vornehmen, der von noch höheren Chargen Snacks zubereiten und die Entwicklung der Aktienkurse selbsttätig auswerten und vorhersagen. Nur sollte man spätestens dann den Unterschied zwischen Firma und Zuhause beachten – das Kommando: „Bring mir meine Hausschuhe, aber flott“, könnte sonst in den falschen Hals geraten. Wenn man dann verlassen wurde, kommt der persönliche Robotassistent sicher gerne mit nach Hause. Schöne neue Datenwelt.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.