

Wer gläsern ist, kann leicht zerbrochen werden

Auch Arbeitnehmer sind von vernetzter Datenerhebung betroffen

Wir haben bereits festgestellt, dass es einen wesentlichen Bereich Ihres Alltags gibt, in dem Sie Zwängen zur Anwendung rechnergestützter, vernetzter Systeme in der Regel nicht entgehen können: Die Rede ist von Ihrem Arbeitsplatz. Gerade die Entwicklung alltagsgegenwärtiger Datenverarbeitung ("ubiquitous computing") kann geeignet sein, Sie in Ihrem Job einer verschärften Kontrolle und massivem Druck auszusetzen, mit allen daraus erwachsenden Gefahren. Wenn Sie als Arbeitnehmer gläsern werden, können Sie leicht zerbrochen werden.

In Untersuchungen wurde nachgewiesen, dass die stark vernetzte Chip- und Sensorwelt, von der wir hier reden, häufig Einführungsmängel aufweist. Das kann beispielsweise daran liegen, dass bei ihrer Konzeption aus Zeit- oder Kostengründen zu hastig geplant wurde; gerade in der Arbeitswelt, etwa in Betrieben unter Wettbewerbsdruck, kann das eine zentrale Fehlerquelle sein.

Schwachstellen führen aber zu Sicherheitslücken, die dann schwer nachweisbaren Datenmissbrauch begünstigen. Solche Angriffe kommen zwar meist von außen und richten sich gegen den Betrieb; das kann und darf Ihnen nicht egal sein, soll allerdings von den Risiken, denen Sie als Arbeitnehmer durch innerbetriebliche Strukturen alltagsgegenwärtiger Datenverarbeitung ausgesetzt sind, hier nicht ablenken.

Klar, bei jedem Einsatz digitaler Techniken durch Ihren Arbeitgeber haben Sie gewisse Schutzrechte. Aber Sie wissen doch: Recht haben und Recht bekommen ist zweierlei. Falls Sie keinen wachen betrieblichen Datenschutzbeauftragten und/oder selbstbewusste Betriebs- und Personalräte einschalten können, stehen wir als Ihre Datenschutzbehörde Ihnen jederzeit mit Rat und Hilfe zur Seite. Wir wollen Ihnen hier zeigen, wie sinnvoll es sein kann, sich einen solchen Schritt ernsthaft zu überlegen. Lassen Sie uns gemeinsam einen kleinen Ausflug in die Zukunft machen, durch einen Arbeitstag in Ihrer aus betriebswirtschaftlichen Gründen vollständig vernetzten Firma. Beginnen wir unser Szenario wieder frühmorgens, diesmal allerdings nicht bei Ihnen zuhause (da waren wir ja eben), sondern vorm Werkstor beziehungsweise dem Haupteingang des Bürogebäudes, in dem Sie arbeiten:

Sie wollen zu Ihrem Arbeitsplatz. Zunächst müssen Sie dazu entweder eine Einlasskarte mit Magnetstreifen in einen entsprechenden Schlitz stecken oder einen kleinen Chip an ein Lesegerät halten, vielleicht tragen auch Ihre Karte oder Ihre bereits angelegte Berufskleidung einen RFID-Chip: Die Firma hat Sicherheitskriterien geltend gemacht bei Einführung dieser Einlasssysteme. Das mag stimmen oder auch nicht – auf jeden Fall erleichtert es der Geschäftsführung die Kontrolle über Sie und gegebenenfalls auch eine zeitabhängige Lohnabrechnung.

Sie begeben sich zu Ihrer Werkbank oder Ihrem Büro. Auf dem Weg dorthin passieren Sie mehrere Türen oder Tore. Die könnten mit Lesegeräten ausgestattet sein, die nun registrieren, wann und wie schnell Sie sich durch das Gebäude oder die Hallen bewegt haben. Möglicherweise sind aus Sicherheitsgründen sogar Kameras in den Fluren und Treppenhäusern installiert. Ein kleiner Schnack mit einem Kollegen oder einer Kollegin auf dem Flur? Das kann wegen Vergeudung bezahlter Arbeitszeit Minuspunkte einbringen – vielleicht nicht sofort, die Firma ist ja großzügig; aber die Daten werden gespeichert und falls Sie sich je ein Fehlverhalten zuschulden kommen lassen, können so gesammelte Informationen Ihnen zusätzlich angekreidet werden.

Sie glauben, Sie können heute – weil Sie draußen arbeiten müssen und es so heiß ist – auf Ihren Sicherheitshelm verzichten oder auf Ihre mit Schutzpolstern ausgestattete Arbeitsjacke? Vorsicht! Beide könnten mit Chips versehen sein, die das Tragen dieser Ausrüstung registrieren und speichern. Auch dies kann im aktuellen Moment für Sie folgenlos bleiben; nur sollten Sie sich davon nicht täuschen lassen: Falls Ihnen mal ein Unfall zustoßen sollte, könnten Krankenkasse oder Berufsgenossenschaft – gestützt auf die Daten, wie oft Sie Sicherheitsvorschriften missachtet haben – Ihnen die Unterstützung kürzen oder verweigern.

Sie haben Ihr Büro betreten und kochen sich und Ihren Kollegen erst mal Kaffee. Stopp! Sind Sie sicher, dass nicht die Zeit zwischen Ihrem registrierten Betreten des Raums und Ihrer Anmeldung am PC Ihres Arbeitsplatzes erfasst und gespeichert werden?

Irgendwann melden Sie sich an, gehen aber zunächst ins Internet und schauen per Webmail nach Ihrem privaten Mailkonto: Mal sehen, was Freund oder Freundin als Morgengruß geschickt haben. Sie sind wirklich leichtsinnig! Jedes Programm, das Sie starten, jede Webseite, die Sie aufrufen, jede Datei, die Sie öffnen – alles kann protokolliert werden. Und Sie können in der Regel weder beurteilen noch ermesen, wie lange die entsprechenden Daten gespeichert werden oder wer sie wann wie auswertet. Kommen Sie ja nicht auf die Idee, ein privat empfangenes Gimmick über das Intranet an Kollegen zu posten; und schon gar nicht sollten Sie die vielleicht zufällig missverständlich formulierte Anweisung Ihres Vorgesetzten als netten Gag Ihrem Freund nach Hause schicken: Weder haben private Nachrichten im Firmennetz etwas zu suchen noch Firmennachrichten auf Ihrem privaten Mail-Kanal; beides kann lange stillschweigend toleriert werden, aber im Ernstfall einer beabsichtigten Disziplinierung wird Ihnen das vielleicht vorgehalten.

Sie beginnen mit Ihrer Arbeit. Vielleicht wird Ihr handwerkliches Tun per Kamera in der Halle oder per RFID-Chip an Werkzeugen und Produktteilen erfasst; vielleicht wird Ihr Arbeitstempo am Schreibtisch durch Registrierung Ihrer Tastaturanschläge protokolliert wird; vielleicht registriert Ihre Berechtigungskarte Häufigkeit und Intensität Ihrer Nutzung des Kopiergeräts; vielleicht speichert Ihre Telefonanlage gewählte Nummern und Gesprächsdauer; vielleicht messen RFID-Chips auf

die eine oder andere Weise nicht einfach Ihre Geschwindigkeit, sondern auch Ihre Sorgfalt im Zuge einer umfassenden Qualitätskontrolle: Jede Minute Ihrer Arbeitszeit, jeder Handgriff kann – theoretisch – in einer Umgebung alltagsgegenwärtiger Datenverarbeitung unbemerkt kontrolliert werden. Und Sie haben in der Regel kaum eine Möglichkeit, auf die Speicherung und Verarbeitung der so erzeugten Daten über Ihr Verhalten Einfluss zu nehmen.

Ah, endlich Zeit für die fällige Pause! Sie verlassen Ihren Arbeitsplatz und gehen erst einmal vor die Tür, auf ein Zigarettenchen. Vielleicht wird Ihr Verlassen des Gebäudes protokolliert oder Sie werden draußen vor der Tür – zufällig oder nicht – von einer Sicherheitskamera erfasst: Sind Sie sicher, dass derart erzeugte Daten Ihnen nicht später einmal angelastet werden? Klar, Sie haben Pause und dürfen vielleicht nach draußen – aber falls die Firma Sie im Zuge einer geplanten Rationalisierung im Visier haben sollte, könnte Ihre nächste Bronchitis mit Ihrem Nikotinkonsum in Verbindung gebracht werden...

Sie schlendern durch den Betrieb. Ein kleiner Klönschnack mit dem Kollegen am Arbeitsplatz, der im Unterschied zu Ihnen noch keine Pause hat, kann Sie und ihn in Schwierigkeiten bringen; irgendwann, wenn derartige Datennutzung dem Vorgesetzten günstig erscheint. Sie erreichen die Kantine, holen Ihr Essen, bezahlen mit Ihrem chip-bewehrten Firmenausweis zwecks Abbuchung von Ihrem Lohnkonto. Gegen Ende der Pause suchen Sie vor Rückkehr an den Arbeitsplatz noch eben die Toilette auf, die Bewegungsmelder an den Zwischentüren registrieren auch das. Es gibt nichts, was nicht erfassbar wäre in einer vernetzten Umgebung; alle Daten könnten gespeichert werden und beitragen zu einem Profil über Sie, dessen Details Sie ebenso wenig kennen wie den Zeitpunkt, wann es zu Ihren Gunsten oder Ungunsten benutzt wird. Ganz abgesehen davon, dass all diese gespeicherten Daten in einem möglicherweise löcherigen Sicherheitssystem theoretisch auch von außen abgreifbar sein und Ihnen bei missbräuchlicher Nutzung massiv schaden könnten.

Wir wollen Ihnen weder Angst machen noch Ihnen – oder gar alle – Arbeitgeber verteufeln. Im Gegenteil: Es gibt viele vernünftige Gründe, rechnergestützte Netzwerke in der Arbeitswelt zu nutzen. Das kann der Produktivität zugute kommen und damit der Sicherheit Ihres Arbeitsplatzes dienen, es kann auch Ihren Arbeitskomfort oder Ihre Sicherheit verbessern helfen. Es ist aber nicht zu bestreiten, dass alles, was Daten erzeugt, auch Schutzmaßnahmen verlangt. Die werden, weil teuer, oft zurückgefahren oder unterlassen. Das ist ebenso falsch wie die schon mehrfach zitierte Haltung "Ich habe nichts zu verbergen". Doch: Auf Ihre Privatsphäre haben Sie auch am Arbeitsplatz ein Recht.