Praxistipp Datenschutz 01 | 2019

Sesam öffne dich – USB-Ports und Informationssicherheit

USB-Ports sind die kleinen Alleskönner unter den Schnittstellen – und damit ein beliebtes Angriffsziel im Unternehmen. Werden Ports nicht gesichert und Beschäftigte nicht geschult, sind die Gefahren für die Informationssicherheit vielfältig. Achtlos eingesteckte USB-Sticks können nach sich ziehen, dass Unbefugte das Unternehmens-Netz schädigen oder unbemerkt Daten abgreifen – mit immensen Risiken für betriebliche und personenbezogene Daten. Da gilt es in Sachen Datenschutz und IT-Sicherheit so einiges zu beachten.

Praxisfall: Alle Beschäftigten eines Unternehmens haben eine Arbeitsanweisung für mehr Informationssicherheit unterschrieben: Fremde USB-Sticks oder andere mobile Massenspeicher dürfen nicht in betriebliche IT-Geräte eingesteckt werden, sondern müssen bei der IT abgegeben werden. Um die Regelung in der Praxis zu testen, ließ die Geschäftsführung auf dem Unternehmensgelände mehrere präparierte USB-Sticks verteilen – zwölf Stück insgesamt. Sie waren teilweise beschriftet, beispielsweise mit „Fotos Paul Gruber“ (dem Namen des Geschäftsführers), „Daten Betriebsrat“ usw. Die Sticks waren so präpariert, dass sie keinen Schaden anrichteten, sondern sich mit einem Server verbanden. So ließ sich verfolgen, welche Sticks gefunden und eingesteckt wurden. Ergebnis: Bis auf einen wurden alle Sticks – elf Stück an der Zahl – in Arbeitsrechner gesteckt. Hätte jemand die USB-Sticks in böser Absicht auf dem Gelände verteilt, wäre der Angriff auf das Unternehmens-Netzwerk ein voller Erfolg geworden.

Schnittstelle für unterschiedliche Aufgaben: USB-Ports dienen in erster Linie als Schnittstelle für Komponenten, die im Arbeitsalltag benötigt werden. Dabei kann es sich um alltägliche Komponenten wie Tastatur und Maus handeln, um mobile Arbeitsspeicher auf USB-Sticks, aber auch um mehr oder weniger exotische Komponenten wie kleine Ventilatoren gegen sommerliche Hitze im Büro. Eine praktische Sache. Nur – wer garantiert, dass der Ventilator mit USB-Stecker keinen Speicherchip enthält? Nur so als kleinen Nebenverdienst für die Hersteller

Universelles Sesam-öffne-Dich: Tatsache ist, dass die seinerzeit von Intel „erfundene“ einheitliche Schnittstelle zu einer Art universellem „Sesam-öffne-Dich“ geworden ist, das aus dem Arbeitsalltag nicht mehr wegzudenken ist. Ob die Aufgabe als Massenspeicher angesichts zahlreicher Cloud-Lösungen noch zeitgemäß ist, ist eine andere Frage. Auch wenn Mäuse und Tastaturen immer häufiger mittels Bluetooth betrieben werden, kann in den übrigen Fällen in aller Regel nicht auf USB-Ports verzichtet werden.

USB-Sticks in allen Varianten: USB-Ports stellen die Informationssicherheit in Unternehmen vor Herausforderungen. Werden USB-Sticks als Speichergerät verwendet, können damit Daten in Systeme gelangen. Ob das nun unbeabsichtigt oder unrechtmäßig geschieht, macht laut europäischem Datenschutzrecht bekanntermaßen keinen Unterschied. Ebenso können Daten des Unternehmens kopiert und abgeschöpft werden. Dabei sollte man bedenken: Speichersticks sind mitunter so klein, dass sie selbst ein geübtes Auge nicht immer sofort erkennt, wenn sie im Gerät stecken. Erst recht nicht, wenn die Farbe geschickt gewählt wurde. Auch was den Speicherplatz angeht, sind USB-Sticks äußerst flexibel. Können schon beim Diebstahl von wenigen Gigabytes an Daten erhebliche Schäden entstehen, wie viel mehr Schaden mag jemand erst mit den heute erhältlichen Sticks mit Platz für mehrere Terabytes anrichten?

USB-Ports als Einfallstor für Schadsoftware: Über USB-Ports können per präpariertem USB-Stick die IT-Sicherheit umgangen und Schadprogramme auf Rechnern aufgespielt werden. Nicht in jedem Fall beginnen sie sofort mit ihrer schädlichen Arbeit. Es kann durchaus sein, dass über USB-Sticks auf die Rechner eingebrachte Schadprogramme zuerst installiert werden, sich dann beim Angreifer melden und mitteilen, dass sie einen neuen Rechner „entdeckt“ haben. Daraufhin könnte

das Programm zunächst inaktiv gesetzt und gut getarnt werden – die schädliche Aktion erfolgt zu einem beliebigen späteren Zeitpunkt. Das bringt mit sich, dass schädliche Software nicht immer sofort erkannt und entfernt werden kann.

USB-Ports als Ausfallstor für Daten: Mittels USB-Massenspeicher lassen sich innerhalb kürzester Zeit große Mengen an Daten kopieren. Dies gilt auch für Geräte, bei denen man auf den ersten Blick nicht unbedingt an Informationssicherheit denkt. Multifunktionsgeräte etwa, die Tausendsassas im Büroalltag. Diese Geräte können kopieren, Daten einscannen, Faxe versenden und empfangen und – natürlich – Dokumente ausdrucken. Um die Arbeit zu erleichtern, haben die meisten dieser Geräte einen USB-Stecker. So lassen sich auch von mobilen Komponenten wie USB-Sticks Daten ausdrucken oder anderweitig weiterverarbeiten. Entsprechend präparierte Sticks – klein und unscheinbar, beispielsweise von einer Reinigungskraft nach Büroschluss eingesteckt und später unauffällig abgezogen – könnten im schlimmsten Fall alle Daten von der Festplatte des Multifunktionsgerätes abgreifen. Also auch gescannte Konstruktionsunterlagen, gefaxte Patientendaten und was sonst noch so Spannendes auf dem Gerät zu finden ist.

USB-Standard: Der universelle serielle Bus (USB) wurde 1996 vom Chiphersteller Intel entwickelt und ersetzte eine nicht mehr überschaubare Vielfalt anderer Steckverbindungen. Dieser USB-Standard wurde als USB 1 bezeichnet. Die Übertragungsrate betrug zunächst (für damalige Verhältnisse sagenhaft schnelle) 400 MBit pro Sekunde. Im Jahr 2000 wurde der Standard USB 2 entwickelt. Er ist heute in den meisten USB-Komponenten enthalten und hat eine dreifache Übertragungsrate von bis zu 1,2 GBit pro Sekunde. Seit 2008 gibt es den USB-Standard USB 3, der Übertragungsraten von 5 GBit pro Sekunde ermöglicht. Beim 2014 eingeführten Standard USB 3.1 Gen 2 beträgt die maximale Datentransferrate für SuperSpeed+ 10 GBit pro Sekunde. Im Jahr 2017 wurde USB 3.2 mit einer Übertragungsrate von bis zu 20 GBit pro Sekunde spezifiziert.

Risiko Nr. 1: Schadcode: USB-Sticks können Schadcode enthalten. Die Gefahr ist groß, dass durch nicht geprüfte Geräte, die über USB-Ports an das System gelangen, schädliche Software übertragen wird. Je nach Virenprogramm oder Trojaner dauert es einige Zeit, bis die Schädlinge entdeckt werden. In der Zwischenzeit – wenige Sekunden genügen – können sie ordentlich Schaden anrichten. Über USB-Sticks mit eigenem Betriebssystem lassen sich Schadprogramme leichter in Computersysteme einschleusen als über das Internet, das ja in aller Regel von einer Firewall gesichert ist. Hinzu kommt, dass Angriffe über USB-Sticks von den üblichen Log-Dateien nicht registriert werden. Sie erfahren also nicht einmal im Nachhinein, wenn entsprechende Aktivitäten stattgefunden haben.

Abhilfe für das Risiko Schadcode: Um zu verhindern, dass Angreifer unbemerkt einen USB-Stick vorübergehend entwenden und mit Schadcode versehen, gilt es, Speichersticks zuverlässig zu sichern, etwa mittels starker Passwörter. Um zu verhindern, dass Beschäftigte von Externen eingebrachte USB-Sticks (beispielsweise mit Angeboten oder Präsentationen) ungeprüft einstecken, gilt es, die Möglichkeiten der Informationssicherheit zu nutzen. USB-Ports sollten seitens der Server gesperrt sein. Um auch mit fremden Sticks arbeiten zu können, sollte die IT solche Sticks vor dem ersten Gebrauch prüfen – anschließend kann man sie an eigens dafür eingerichteten Geräten nutzen. Um das Risiko insgesamt zu verringern, sollte ein Unternehmen alle Beschäftigten im Umgang mit USB-Sticks sensibilisieren. Denn: Wer die Gefahren kennt, kann sich dagegen wappnen.

Risiko Nr. 2: USB-Sticks von Beschäftigten: Bringen Beschäftigte Daten von ihren Privatrechnern per USB-Stick mit, beispielsweise um den Kollegen Fotos vom Malediven-Urlaub zu zeigen oder die neueste Lieblingsmusik zu tauschen, besteht grundsätzlich die Gefahr, dass der Arbeitsrechner infiziert wird – nämlich dann, wenn sich auf dem privaten Rechner Schadcode befindet. Vor allem, wenn sich Beschäftigte privat dubioser Quellen bedienen, um Filme oder Musik herunterzuladen, ist diese Gefahr nicht zu unterschätzen. Ein Grund mehr, die Nutzung von USB-Ports nur für eigens zugelassene Geräte zu erlauben.

Auch zugelassene Sticks können Schadcode enthalten: Auch der umgekehrte Fall ist problematisch: Wenn Beschäftigte auf einem von der IT zugelassenen USB-Stick Dateien mitnehmen, um zu Hause weiterzuarbeiten, kann es zu einer Infizierung des Arbeitsrechners kommen. Eine Prüfung auch erlaubter USB-Sticks auf Virenbefall ist daher unverzichtbar.

Risiko Nr. 3: Datendiebstahl: Wird per USB-Schnittstelle eine Verbindung zu einem

Massenspeicher aufgebaut, der mit Schadcode versehen ist, kann Datendiebstahl die Folge sein. Steckt ein Externer einen Stick in einen Unternehmensrechner und erlangt dadurch Zugang zum Netzwerk, kann in der Folge so ziemlich alles geschehen – von der Infektion der Systeme bis zu unkontrolliertem Datenabfluss.

Risiko „verlorener" Sticks: Mittels USB-Sticks werden verstärkt Angriffe auf IT-Systeme von Firmen lanciert. Ähnlich wie im genannten Praxisfall „verliert" ein Externer irgendwo auf dem Firmengelände einen USB-Stick in der Erwartung, dass ein Mitarbeiter ihn findet und, um herauszubekommen, wem der vermeintlich verlorene Stick gehört, in einen der Computer steckt. Dort beginnt die Schadsoftware ihre Arbeit in zweierlei Hinsicht: Dateien werden im ersten Schritt ausspioniert und im zweiten via Internet – oft in kleinere unauffällige Pakete zerlegt – mit ausgehender elektronischer Post an die Adresse der Eindringlinge geschickt. Dagegen hilft nur eine hohe Sensibilität aller Mitarbeiter und eine Absicherung der USB-Ports gegen unbefugte Nutzung.

Risiko Notebooks: Häufig verfügen Arbeitsplätze, an denen mit Notebooks gearbeitet wird, über eine Docking-Station, also eine Vorrichtung, in die das Notebook beim Arbeiten am Schreibtisch eingebracht wird. Hier verbindet es sich mit dem Netzwerk des Unternehmens. Sind die Beschäftigten unterwegs und arbeiten mobil, nutzen sie entweder das Internet zum Datenaustausch – oder eben einen USB-Stick. Eine Herausforderung für die Informationssicherheit, denn damit ist ein Notebook ein mögliches Angriffsziel. Auch für dieses Risiko müssen geeignete Gegenstrategien entwickelt werden. Im Zeitalter der Cloud-Speicherung sollten USB-Sticks überflüssig werden – könnte man meinen. Aber Gewohnheiten sind nun einmal Überlebenskünstler. Es gilt also, mit geeigneten Sensibilisierungsmaßnahmen Sorge zu tragen, dass die Beschäftigten die Risiken kennen – ebenso wie ihre persönliche Verantwortung, falls sie gegen verbindliche Vorgaben verstoßen.

Risiko Werbegeschenke: Auf Messen verteilen Hersteller immer wieder USB-Sticks mit ihren Angeboten. Sie sind bei Messebesuchern in der Regel sehr beliebt, nicht immer nur wegen der enthaltenen Angebotsdaten, sondern als praktische Datenträger für den eigenen Bedarf. Aber: Auch solche Sticks können eine Gefahr darstellen. Zwar werden die wenigsten Messeaussteller absichtlich Schadcode auf verteilten Sticks aufbringen, doch darauf verwendete Software kann von Dritten als Backdoor missbraucht werden.

Risiken für betroffene Personen: Aus Sicht betroffener Personen kann es zu Verletzungen ihrer Rechte und Freiheiten kommen, wenn die Schnittstellen der informationstechnischen Systeme nicht hinreichend geschützt sind. Neben der Informationssicherheit und den übrigen Risiken besteht also auch die Gefahr einer Verletzung des Schutzes personenbezogener Daten. Hier sind die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um unter anderem folgende Risiken zu entschärfe folgende Risiken zu entschärfen:

- Das Risiko der **Vernichtung von Daten**. Beispiel: Es gelangt Schadcode ins System, der Daten dauerhaft sperrt oder löscht. Das Risiko ist besonders hoch bei Geräten, auf denen nicht oder noch nicht synchronisierte Daten gespeichert sind.
- Das Risiko des **Verlusts von Daten**. Beispiel: Unbefugte ziehen Kopien personenbezogener Daten mittels präparierter oder einfach nur als Arbeitsspeicher verwendeter USB-Speichersticks ab.
- Das Risiko der **Veränderung von Daten**. Beispiel: Ein Unbefugter zieht vorübergehend personenbezogene Daten ab und spielt sie später verändert wieder ein.
- Das Risiko der **unbefugten Offenlegung**. Beispiel: Ein Außenstehender kopiert personenbezogene Daten über einen USB-Stick, der in einen nicht hinreichend gesicherten USB-Port gesteckt wurde.
- Risiko des **unbefugten Zugangs**. Beispiel: Ein Außenstehender kopiert personenbezogene Daten über einen USB-Stick, der in einen nicht hinreichend gesicherten USB-Port gesteckt wurde, und verarbeitet diese Daten anschließend weiter.

Mögliche Meldepflicht: Sollte es durch unsachgemäßen Einsatz von Massenspeichern, hier der USB-Sticks, zu einer Schutzverletzung personenbezogener Daten kommen, ist zu prüfen, ob eine Meldepflicht des Vorfalles an die zuständige Aufsichtsbehörde für den Datenschutz erforderlich ist. Auf die Meldung kann verzichtet werden, wenn der Vorfall nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Entsprechendes gilt für die Benachrichtigung der Betroffenen. Entsteht diesen durch die Schutzverletzung ein hohes Risiko, muss das Unternehmen sie über den Vorfall informieren – unter

anderem, um ihnen mögliche Schutzmaßnahmen zu ermöglichen. Ob ein Risiko vorliegt und wenn ja, wie gravierend es ist, kann jedoch nur geprüft werden, wenn bekannt ist, welche Daten auf dem entsprechenden USB-Stick gespeichert sind. War der Stick verschlüsselt, kann unter Umständen auf die Meldung bei der Aufsicht und die Benachrichtigung der Betroffenen verzichtet werden. Ist die Verschlüsselung in ihrer Wirkung fragwürdig – kann sie also möglicherweise mit überschaubaren Mitteln überwunden werden – müssen beide Maßnahmen unter Umständen dennoch erfolgen. Eine sichere Verschlüsselung von USB-Massenspeichern ist also in jedem Fall zu empfehlen.

Fazit: So vielfältig die Gefahren sind, die via USB das Firmen-Netzwerk und den Datenschatz des Unternehmens bedrohen, so überschaubar und unkompliziert sind die Maßnahmen, die Verantwortliche vorbeugend ergreifen können. Mit entsprechender Einstellung der IT-Komponenten, klaren Regelungen und gezielter Sensibilisierung der Beschäftigten ist viel erreicht – und das Unternehmen gegen Angriffe mittels USB-Schnittstelle gewappnet.

Rechtsquellen zum Nachlesen

Zur **Meldepflicht** bei der zuständigen Aufsichtsbehörde: Art. 33 DSGVO

Zur **Benachrichtigung Betroffener** bei einem Datenschutz-Vorfall: Art. 34 DSGVO

Alle Praxistipps gibt es auf team-datenschutz.de

Hier schreibt Eberhard Häcker, Externer Datenschutzbeauftragter, Datenschutzberater, Fachautor und Kongressredner, Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und der HäckerSoft GmbH (Datenschutz-Software DATSIS und Lernplattform Optilearn.de). Er ist überzeugt, „den spannendsten Beruf der Welt“ zu haben, denn Datenschutz unter der DSGVO ist „wie die Besiedlung Amerikas – weißes Land, das es zu entdecken und sinnvoll zu füllen gilt“. (Eberhard Häcker)