Kleine Geräte mit großem Zerstörungspotenzial

Zusammenfassung: Selbst wenn eine Sicherheitsrichtlinie verbietet, dass nicht zugelassene USB-Sticks verwendet werden, bedeutet das nicht, dass sich alle daranhalten. Dabei ist es egal, ob die Sticks beschriftet sind oder nicht. Gefahren scheinen nicht im Bewusstsein zu landen. Strenge Regeln alleine reichen nicht. Ohne die Überzeugung, dass die Anordnungen richtig sind, fehlt es an der Konsequenz beim Einhalten der Regeln. Zusätzliche Maßnahmen sollten eingeleitet werden wenn das Unternehmen nicht eines Tages Opfer eines gelungenen Cyber-Angriffs werden will.

Der Praxisfall: Auf dem Firmengelände wurden einige unscheinbare USB-Sticks gefunden. Einige waren beschriftet, andere nicht. Auf den beschrifteten stand beispielsweise „Fotos Herr Abele“ (Abele heißt der Geschäftsführer). Laut eindeutiger Arbeitsanweisung hätte keiner der USB-Sticks in eines der Geräte gesteckt werden dürfen. Tatsache war aber, dass etwa ein Drittel der aufgefundenen Sticks ausprobiert wurden, sowohl Sticks mit der Foto-Aufschrift als auch ohne Beschriftung. Ein weiteres Drittel wurde bei der IT abgegeben. Dieses Verhalten entsprach den Sicherheitsanforderungen. Ein weiteres Drittel der Sticks wurden von den Findern mit nach Hause genommen. Was die Finder nicht wissen konnten: Alle Sticks waren speziell präpariert, so dass sie sich bei einer bestimmten Internet-Adresse meldeten, sobald sie mit einem Rechner verbunden wurden. Es handelte sich um einen Versuch von Studenten zur Überprüfung der Sicherheitsmaßnahmen im Unternehmen.

Durchgefallen! Hätte es sich um einen tatsächlichen Angriff gehandelt, wären die unternehmenseigenen Rechner mit einer Schadsoftware verseucht worden. Selbst die Sticks, die mitgenommen wurden und außerhalb des Unternehmens eingesteckt wurden, meldeten sich der Reihe nach. Damit hätten sich die vermeintlich schlauen Finder ein gewaltiges Eigentor geschossen, denn ihre privaten Rechner wären damit verseucht worden.

Solche Gefahren lauern: Wenn USB-Sticks mit Schadsoftware präpariert sind, können sie auf unterschiedliche Weise Schaden anrichten. Sie können Programme enthalten, die sich im Netz verbreiten können, wenn sie die Sicherheitsmaßnahmen einmal überwunden haben. Sie können Erpressungssoftware in die Netze einschleusen oder sie können Daten abgreifen. Es gibt eine ganze Reihe weiterer Gefahren, die es sehr angeraten sein lassen, dafür zu sorgen, dass nicht zugelassene USB-Sticks verwendet werden können.

Geräte sperren: Per Gruppenrichtlinie können USB-Sticks, die nicht eigens zugelassen sind, gegen unbefugte Nutzung gesperrt werden. Mit entsprechenden Einstellungen in den Windows-Servern kann dieses Ziel erreicht werden. Damit kann verhindert werden, dass Massenspeicher, die die USB-Ports nutzen, unerlaubt verwendet werden können.

Zielgerichtet Nutzung erlauben: Mit derselben Richtlinie können umgekehrt aber auch einzelne USB-Massenspeicher für die Nutzung auf einzelnen Systemen erlaubt werden. So können USB-Sticks überall dort, wo sie benötigt werden, auch eingesetzt werden.

Erlaubte USB-Sticks kennzeichnen: Um den Prozess weiter zu unterstützen, sollten USB-Massenspeicher, die zur Nutzung zugelassen sind, eigens gekennzeichnet werden. Dies kann mittels einer Inventarisierungsnummer geschehen. Die Kennzeichnung sollte so gut aufgebracht werden, dass sie nicht aus Versehen entfernt werden kann. So kann man auf einen Blick sehen, ob ein eingesetzter USB-Stick zugelassen ist oder ob da jemand etwas tut oder tun will, was nicht den Richtlinien entspricht.

Verbot der privaten Nutzung: Ein weiterer Baustein für die Informationssicherheit ist das Verbot der privaten Nutzung der Sticks. Sonst ist folgendes Szenario möglich: Der USB-Stick, der eigentlich nur für die Verwendung im Unternehmen gedacht ist, wird mit nach Hause genommen und dort in einem privaten Rechner verwendet. Dieser ist, ohne Wissen des Anwenders, mit einer Schadsoftware befallen. Diese kopiert sich auf den USB-Stick und kommt auf diesem Wege bei der nächsten beruflichen Nutzung auf ein unternehmenseigenes Gerät. Da der Stick dort zugelassen ist, hat der potenzielle Angreifer schon die erste Hürde auf dem Weg zur Überwindung der Sicherheitsmaßnahmen erreicht.

Verschlüsselung der zugelassenen Sticks: Damit solche Angriffe auf unerlaubt eingesetzte Sticks zumindest erschwert werden, kann eine Verschlüsselung des Sticks vorgenommen werden. Diese kann mit einer zweiten Komponente versehen werden, die testet, ob der Stick in der zugelassenen Umgebung verwendet werden soll. Damit kann ein weiterer Baustein zu mehr Sicherheit verwendet werden. Sind die Systeme allerding zur Nutzung im häuslichen Büro zugelassen, ist diese Hürde vermutlich auch wirkungslos, denn darf der Stick normalerweise auch auf diesem Rechner ge-

nutzt werden. Hier müssen dann andere Sicherheitsmaßnahmen greifen.

Überzeugungsarbeit: Neben allen technischen Maßnahmen muss auch Überzeugungsarbeit geleistet werden. Was die Studenten in unserem Fallbeispiel getan haben, kann auch zu einer Vorführung im Rahmen einer Schulungsmaßnahme genutzt werden. Wenn bei einer Schulung vorgeführt wird, wie schnell sich ein aufgespieltes Schadprogramm vom USB-Stick auf die Systeme überträgt und von dort aus weiter verbreiten kann, lässt sich vorführen. In der Folge sollten die Teilnehmer an der Unterweisung dann sensibler sein, wenn es auch keine Garantie für den Erfolg gibt.

Man kann nie sicher sein: Selbst wenn Anwender auch zuhause alle Sicherheitsmaßnahmen eingeleitet haben, damit ihre Systeme nicht von Schadsoftware befallen werden, kann man nie sicher sein. Das zeigt der Fall einer Software für Werbung, die auf Foto-CDs aufgebracht wurde. Anwender, die ihre digitalen Fotos zur Entwicklung und zum Ausdruck abgegeben haben, erhielten neben den ausgedruckten Bildern auch eine CD, auf der die Bilder archiviert waren. Auf der CD befand sich auch ein Programm, das den Herstellern der CD ermöglichen sollte, Werbung für die Kunden einzuspielen. Diese Software war von Angreifern gehackt und manipuliert worden. Ein Anwender hatte sich Urlaubsbilder auf die CD geholt und wollte diese den Kollegen im Unternehmen vorführen. Über die CD wurde auch die manipulierte Software für die Werbung eingespielt. Damit waren die Systeme offen für weitere Manipulationen der Angreifer. Auch solche Informationen sollten im Rahmen von Unterweisungen an die Beschäftigten weitergegeben werden.

Falsche Sicherheit: Man sollte sich auch ab und zu fragen, ob sich die Beschäftigten überhaupt real über die Angriffsgefahren im Klaren sind. Woher sollten sie die Angriffe auch kennen? Schließlich sind die Sicherungsmaßnahmen der IT so erfolgreich, dass sie abgeblockt werden, ohne dass die Beschäftigten das mitbekommen. In der Folge glauben sie dann möglicherweise, dass dieses ganze Gerede von den Angriffen weit übertrieben sei. Es kann nicht schaden, anlässlich von Datenschutzschulungen oder Sicherheitsunterweisungen auch einmal über die zahllosen Angriffsversuche, die tagtäglich von den Sicherheitseinrichtungen abgewehrt werden, zu informieren.

Keine Paranoia: Allerdings sollte das auch nicht übertrieben werden. Wenn bei jeder Meldung über einen Erpressungstrojaner eine seitenlange Mail der IT kommt, mit dem Inhalt, dass keine unbekannten Mails geöffnet werden dürfen, dann verliert diese Meldung irgendwann ihren Schrecken. Denn bei den Mitarbeitern kommt wieder an, dass nichts passiert und damit auch keine so große Gefahr vorliegen kann. Wie leicht kann hier der Eindruck entstehen, dass sich „die von der TI“ nur wichtigmachen wollen!

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.