Artikel wurde in folgenden Themenkategorien gefunden:

Fachthemen » IT-Sicherheit » Security Management
Zeitschriften » IT-SICHERHEIT » News und Artikel » Security Management

26.09.2013

10 Fragen an ... Beatrice Lange, tetraguard systems GmbH

IT-SICHERHEIT im Gespräch mit Beatrice Lange, Managerin bei tetraguard systems GmbH. Erfahren Sie u.a. mehr zum Thema "BYOD" oder zu Data Leakage in den eigenen Reihen. Viel Spaß beim Lesen!

IT-S: Das Thema PRISM verfolgt uns nun ja schon ein paar Wochen. Rufen bei Ihnen jetzt unentwegt Unternehmer an, die sich Sorgen um ihre Daten machen?

Beatrice Lange: Wider Erwarten nein. Es gibt einen geringen Anstieg, aber ich würde sagen, es ist immer noch nicht in den Köpfen angekommen, dass dies eine wirkliche Bedrohung für die Unternehmen ist. Die Fragen von Händlern verändern sich zwar, aber dass wir da jetzt einen absoluten Run hätten, kann ich nicht bestätigen. Es ist in unserem Metier immer schon so gewesen, dass man ganz gerne den Kopf in den Sand gesteckt und die Augen verschlossen hat. Es trifft einen schon nicht selbst, sondern immer nur die anderen. Das Problem bei gestohlenen Daten ist, dass die Daten ja nicht weg sind. sie bleiben ja weiterhin bestehen, allerdings woanders. Und das übereinander zu bekommen, scheint sehr schwierig zu sein.

IT-S: Angenommen, es gibt Unternehmen oder Geschäftsführer, die sich tatsächlich um die Sicherheit ihrer Daten sorgen. Wie könnten sie denn dafür sorgen, dass ihre Daten sicher sind – Stichwort „Bring Your Own Device" (BYOD) und Cloud Computing?

Beatrice Lange: Ganz wichtig für Unternehmen ist es, eine Software zu finden, die sie automatisch vor Datendiebstahl und Ausspähung bewahrt. Es gibt heutzutage Programme, die Daten in bestimmten Verzeichnissen, die man auf einer Festplatte anlegt, automatisch schützen. Zusätzlich gibt es den Schutz an den Schnittstellen. Das heißt, man kann es untersagen, dass Daten von dem Gerät herunter kopiert werden können. Oder wenn, dann nur in veränderter Form, sodass sie außerhalb vom Unternehmen nicht gelesen werden können. Und wenn man sich dann noch mit einer Netzwerk- und Cloud-Sicherheit ausstattet, damit Daten nicht ungeschützt durchs Netzwerk verschoben werden oder unverschlüsselt in die Cloud gelegt werden können, dann ist man schon einigermaßen sicher.

IT-S: An BYOD führt ja kein Weg mehr dran vorbei. Gibt es Verfahren, um diesen Trend möglichst sicher zu machen?

Beatrice Lange: Das ist ein ganz heißes Thema. Bei uns im Unternehmen ist es beispielsweise nicht gestattet. Und ich würde Unternehmen auch nicht empfehlen, es zu erlauben, weil sie nie wissen können, was mit ihren Daten passiert, wenn sie auf fremden Geräten sind.

IT-S: Aus dieser Ansicht heraus würden Sie also sagen, dass es auch kein Verfahren gibt, um diesen Trend wirklich sicher zu machen?

Beatrice Lange: Nein, das kann man nicht sicher. Wenn jemand das Recht hat, an Dokumenten zu arbeiten, sie zu löschen etc. und er das Recht hat, auf private Medien zu speichern, dann hat er auch die Möglichkeit, dieses Dokument ungeschützt auf einen privaten Rechner zu bringen. Es gibt sicher Unterlagen, bei denen es vielleicht nicht ganz so schlimm ist, aber wenn Sie in einem Konstruktionsbüro sind und die Zeichnungen dort einfach kopieren können, dann ist das natürlich fatal.

IT-S: Ja, das stimmt. Nun eine etwas generellere Frage: Meinen Sie, dass Unternehmen genug in IT-Sicherheit investieren?

Beatrice Lange: Nein. Weil eben das Bewusstsein in den Köpfen des Mittelstandes noch nicht angekommen ist – das betrifft eben auch das Mitbringen der eigenen Geräte. Man denkt nicht zu Ende, was eigentlich mit dem Unternehmens-Know-how passieren könnte. Teilweise haben die Mitarbeiter ja Zugriff auf die Kronjuwelen des Unternehmens, auf die Existenzgrundlagen. Und es gibt auch einige Beispiele hier in Deutschland, wo Erfindungen bzw. Entwicklungen abgegriffen wurden, die dann in anderen Ländern zur Patentschrift geführt haben. Und das Unternehmen, was es in Deutschland entwickelt hat, hat – wie man so schön sagt – in die Röhre geguckt.

IT-S: Es ist ja bekannt, dass ungewünschter Datenabfluss primär von den eigenen Leuten ausgeht. Was kann man denn gegen Datenklau in den eigenen Reihen unternehmen?

Beatrice Lange: Auch dafür gibt es Software. Der einfachste Weg, Daten mitzunehmen, ist ja heute immer noch die USB-Schnittstelle. Vor allen Dingen deswegen, weil es keine Protokollierung darüber gibt, was kopiert wird – anders als bei einem Druck oder einer Mail. Also muss man sich an der Stelle schützen. Empfehlenswert ist eine Software, die im Hintergrund arbeitet und die Daten, die dort unberechtigt kopiert werden, verschlüsselt, damit sie außerhalb des Unternehmens nicht mehr lesbar sind. Und natürlich muss man auch gut überlegen, wem man die Autorisierung gibt, Daten mitnehmen zu dürfen.

IT-S: Doch wie sollten Unternehmen vorgehen, wenn vertrauliche Daten bereits das Haus verlassen haben? Sollten sie offen auf ihre Kunden zugehen und „die Hosen runterlassen"?

Beatrice Lange: Gängige Praxis ist es, den Kopf in den Sand zu stecken, also nichts zu machen. Ich würde es auf den Fall beziehen: Wenn ein Unternehmen Daten von einem guten Kunden verloren hat, finde ich es eigentlich nur fair, wenn man ihm das auch mitteilt. Wenn Sie personenbezogene Daten verloren haben und diese öffentlich geworden sind, haben Sie schon aus datenschutzrechtlicher Sicht die Verpflichtung, die Menschen darüber zu informieren.

IT-S: Würden Sie sagen, es gibt gewisse Verfahren, die eigentlich jedes Unternehmen haben müsste, um seine IT-Infrastruktur bestmöglich zu schützen?

Beatrice Lange: Ich denke, es sollte im Sinne eines jeden Unternehmens sein, seine Daten, also sein Wissen, zu schützen. Und das einfachste ist in meinen Augen, dies mit Verschlüsselung zu tun.

IT-S: Inwieweit sollte man eigentlich die eigenen Mitarbeiter überwachen?

Beatrice Lange: Also wir haben ein Verfahren entwickelt, das Ihnen alle Vorgänge, die die Daten betreffen, protokolliert. Aber diese Protokoll-Dateien werden in verschlüsselten Datenbanken gehalten, und das kann man so einrichten, dass man das nur im Vier-Augen-Prinzip öffnen kann. Das heißt, unter Hinzuziehung des Betriebsrates. Zwei bestimmte Schlüssel müssen zusammen kommen, damit man eine Datei überhaupt öffnen kann, weil man natürlich die Möglichkeit haben muss, im Falle eines Falles da mal etwas nachzugucken. Aber man sollte nicht generell jeden Vorgang akribisch überwachen.

IT-S: Noch eine abschließende Frage: Was halten Sie vom IT-Sicherheitsgesetz?

Beatrice Lange: Es gibt ja bereits die Verpflichtung, Datenschutz-Vorfälle zu melden. Ich glaube, dass uns ein neues Gesetz nicht sehr viel weiterbringt. Man müsste das schon sehr genau differenzieren. Und ich bin der Ansicht, dass man so etwas auf keinen Fall von Politikern machen lassen sollte, sondern von wirklich fachkundigen Leuten. Ich denke, alles andere ist blinder Aktionismus.

IT-S: Vielen Dank für das Gespräch!

Das Gespräch mit Beatrice Lange führte Faatin Hegazi, Redaktion IT-SICHERHEIT.

zurück