Ein Klick zu viel und Locky lässt sich in Bitcoins auszahlen

Zusammenfassung: Unterweisungen können zur Sensibilisierung der Beschäftigten führen, so dass das Risiko, dass gefährliche Links in Mails angeklickt werden, deutlich reduziert werden kann. Allerdings muss die Sensibilisierung alle erreichen und regelmäßig wiederholt werden. Dazu sollten Praxisbeispiele verwendet werden, die realistisch genug sind, um glaubhaft zu wirken. Allerdings müssen trotzdem geeignete Notfallmaßnahmen eingerichtet werden, um die Verfügbarkeitskontrolle bei Virenbefall sicherzustellen. Datenschutzbeauftragte haben ein massives Eigeninteresse an funktionierender IT-Sicherheit und können in abgestimmten Schulungen viel zur Sensibilisierung der Beschäftigten beitragen. Im Notfall muss die IT so rasch als möglich wieder einsatzfähig sein. Dazu kann ein IT-Sicherheitskonzept mit einer Notfallkomponente einen wichtigen Beitrag leisten.

Praxisbeispiel: Eine Klinik in Nordrhein-Westfalen meldet, dass sich im System ein Virus („Locky“) ausgebreitet hat. Das Virus verschlüsselt sämtliche Dateien so intensiv, dass diese nicht mehr mit eigenen Mitteln entschlüsselt werden können. Zwar liegt ein Backup vor, aber der Schädling hat sich offenbar weiter im Netz verbreitet. Das eigentliche Problem ist, die Systeme vom Schadprogramm zu befreien. Auch mehrere Tage nach dem Vorfall war die IT der Klinik noch nicht wieder voll einsatzfähig. Pikant an der Angelegenheit: eine Klinik hat den Virenbefall mit Locky gemeldet, zahlreiche andere, die ebenfalls betroffen waren, taten dies nicht. Bleibt die Frage, den geforderten Bitcoin zu bezahlen oder nicht – aber im Zweifelsfall wird die Neigung eher zum Bezahlen gehen.

Rechtliche Situation: Es gibt eine ganze Reihe von rechtlichen Vorgaben, die auf die Sicherheit der IT abzielen. Am ehesten denkt man dabei an das IT-Sicherheitsgesetz, dass verhindern soll, dass gesamtwirtschaftliche Schäden durch Ausfälle der IT in Unternehmen oder Organisationen entstehen. Ob die Ausfälle durch Angriffe, durch interne Fehler, Fehler in der Software oder anderweitig ausgelöst werden, ist dabei erst einmal egal. Bestimmte Unternehmen aus so genannten kritischen Infrastrukturen (wie Energieversorger) haben darüber hinaus eine Meldepflicht an das BSI, wenn es zu IT-Ausfällen kommt. Aber auch eine ganze Reihe weiterer Gesetze verpflichten Unternehmen, für reibungskose Abläufe zu sorgen, beispielsweise das KonTraG, das Geschäftsführer für bestimmte Ausfälle haftbar macht.

Datenschutzrecht: Im Datenschutzrecht gibt es die allgemeine Organisationsverpflichtung in § 9 BDSG und die Anlage mit den technischen und organisatorischen Maßnahmen hierzu. Dort wiederum sind mehrere Maßnahmen für die Sicherheit relevant. Das beginnt mit der Zutrittskontrolle und der Zugangskontrolle, geht über die Zugriffskontrolle weiter zur Verfügbarkeitskontrolle. Hier sind auch Datenschutzbeauftragte gefordert, denen die IT-Sicherheit nicht egal sein kann.

Dokumentation der technischen und organisatorischen Maßnahmen: Zu den Aufgaben des Datenschutzbeauftragten gehört es unter anderem, den Stand der technischen und organisatorischen Maßnahmen zu dokumentieren. Ergeben sich hieraus potenzielle Schwachstellen, sind die Datenschutzbeauftragten gehalten, darauf hinzuwirken, dass die Vorgaben zum Datenschutz und zu den näheren Umständen des Datenschutzes eingehalten werden können. Selbst haben sie keine Durchgriffsmöglichkeit. Eine Geschäftsführung, die jedoch die Hinweise eines Datenschutzbeauftragten ignoriert, handelt ab diesem Moment nicht mehr fahrlässig, sondern mindestens grob fahrlässig. Ob dieses Risiko so ohne Weiteres eingegangen wird, muss sich dann in der Praxis zeigen.

Eigenes IT-Sicherheitskonzept ist unabdingbar: Für Unternehmen, die auf die IT angewiesen sind, ist ein eigenes IT-Sicherheitskonzept unabdingbar. Im IT-Sicherheitskonzept müssen alle einschlägigen IT- und TK-Systeme aufgeführt sein. Diese müssen grundsätzlich vor unbefugter Nutzung Dritter oder vor Ausfall geschützt werden. Wie das geschehen soll, ist zentraler Bestandteil des IT-Sicherheitskonzepts.

Sicherheitsziele definieren: Zunächst gilt es, die Sicherheitsziele zu definieren. Hierzu muss analysiert werden, welche Systeme wie wichtig für die Unternehmensabläufe sind. Anders ausgedrückt: Wie lange kann auf ein bestimmtes System verzichtet werden, ohne dass ein Schaden in definierter Höhe eintritt? Welche Sicherheitsvorkehrungen kommen in Frage, um die IT des Unternehmens oder der Organisation zu schützen? Und welche Maßnahmen davon sind in der konkreten Situation tauglich? Wie schnell kann bei einem Befall wieder gearbeitet werden?

Technische Maßnahmen definieren: In einem weiteren Schritt sind die technischen Maßnahmen zu definieren, die erforderlich sind, um den Betrieb wieder aufnehmen zu können, und die auch zur Organisation passen. Das ganze muss bezahlbar bleiben. Im konkreten

Fall sind Virenscanner weitgehend nutzlos, da die Betroffenen mit einer gefälschten Mail dazu gebracht werden sollen, die Schadsoftware herunterzuladen. Hier reichen die technischen Maßnahmen alleine nicht aus, zusätzlich müssen die Mitarbeiter sensibilisiert werden.

Sensibilisierung ist erforderlich: In dieser Situation kommt den Unterweisungen zum Datenschutz und zur IT-Sicherheit eine besondere Bedeutung zu. In jeder Datenschutzunterweisung muss grundsätzlich der Hinweis auf Phishing-Mails und andere entsprechende Techniken enthalten sein. Am besten zeigt man das mit Beispielen von gut gemachten Phishing-Mails und einer Beschreibung der Folgen. Wichtig ist hierbei, dass alle Beschäftigten erreicht werden.

Nachhaltigkeit anstreben: Anders als bei anderen Schulungen kommt es erfahrungsgemäß hier auf die Penetration, also die regelmäßige Wiederholung, an. Außerdem muss die Sensibilisierung auch wirklich alle Beschäftigten mit Account erreichen – auch, wenn diese das Postfach nur ab und an nutzen sollten.

Kritische Gruppe von Beschäftigten: Untersuchungen zeigen, dass sich das eigentliche Problem auf eine kleine Gruppe von Beschäftigten konzentriert. Werden regelmäßige Unterweisungen durchgeführt, halten 85 bis über 90 % der Beschäftigten in der Folge die Regeln ein. Was bleibt, ist eine besondere Risikogruppe, die es leider in allen Unternehmen gibt. Das sind Menschen, die grundsätzlich vieles besser wissen als andere und erst einmal alles anklicken, bevor es im Kopf Klick macht. Das Fatale dabei ist, dass sich diese Personen oft erst identifizieren lassen, wenn es zu spät ist, also im schlimmsten Fall eine Infektion schon stattgefunden hat. Umso wichtiger ist, dass diesen Personen die Folgen des unbedachten Anklickens eines Links mit der Folge einer Infektion deutlich vor Augen geführt werden.

Auch wenn es nerven sollte – regelmäßig sensibilisieren! Experten sehen auch hier nur die Möglichkeit, mit den Betroffenen gemeinsam Strategien zur Abwehr auszuarbeiten. Am besten scheint diese Gruppe noch anzusprechen zu sein, wenn man ihnen klarmacht, dass eine Infektion in aller Regel auf den Klicker zurückgeführt werden kann und dass sich die sonst sehr eingeschränkte Arbeitnehmerhaftung hier deutlich erhöht. Dies ist stets dann der Fall, wenn entgegen von klaren Anweisungen gehandelt wird. Dann gilt unter Umständen grobe Fahrlässigkeit oder gar Vorsatz, und in diesen Fällen können die Verursacher auch materiell für den Ersatz des entstandenen Schadens zur Verantwortung gezogen werden.

Praxisbeispiele sammeln: Ein Ordner, der in jedem Unternehmen vorhanden ist, ist der Spam-Ordner. Darin finden sich etliche Praxisfälle für gut gemachte Phishing-Mails. Zwar kann man einwenden, dass diese Mails ja schon im Spamordner „entschärft“ wurden. Andererseits sind Fälle bekannt, in denen aus dem Spam-Ordner Mails wieder reaktiviert wurden (weil man eine bestimmte Mail gesucht und dort vermutet hat). Dabei wurden auch andere Mails wieder reaktiviert – und geöffnet. Also haben selbst die Mails aus dem Spamordner noch ein Sprengpotenzial. Außerdem können die Beispiele gar nicht anschaulich genug sein.

Ausblick: Die Gefahr durch virenverseuchte Mails dürfte eher noch zu- als abnehmen. Durch die Tatsache, dass auch Windows 10 die unrühmliche Tradition von Microsoft fortsetzt und offenbar gravierende Sicherheitslücken aufweist, lässt für die Zukunft eher Schlimmes erahnen. Sensibilisierungen und angemessene begleitende Maßnahmen sind also auch für die Zukunft unverzichtbar.

Metatags: Locky, It-Sicherheitsgesetz, Vireninfektion, Mailanhang, Mailanhänge, Phishing, Spam, Sicherheitskonzept, IT-Sicherheitskonzept

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