Sophos-Serie zu IT-Sicherheit und Recht:

Die Belegschaft als Sicherheitsrisiko: wie lässt sich die Security auch rechtssicher im Unternehmen verbessern?

Sicherheit muss im Unternehmen zur allgemeinen Routine werden. Ein effektives IT-Sicherheitssystem ist ein Teil davon. Mindestens ebenso wichtig ist aber auch der Mensch als Anwender der Systeme. Sophos zeigt auf, welche organisatorischen und praktischen Maßnahmen Unternehmensdaten schützen sowie das Unternehmen vor rechtlichen Folgen von IT-Sicherheitsvorfällen bewahren können.

Wiesbaden, 19. Oktober 2017. Für die IT-Sicherheit im Unternehmen stellt der Mitarbeiter nach wie vor die größte Sicherheitslücke dar. Die Folgen fehlerhaften Verhaltens sind weitreichend: von Serverabstürzen, technischen Defekten oder Vireninfektionen – die zu Arbeitszeitausfällen führen – bis zu Wettbewerbsnachteilen durch Verlust firmeninterner Daten oder erheblichen Imageverlust.
Nicht minder weitreichend können die rechtlichen Konsequenzen aus möglichen Schäden sein: Neben Lieferausfällen, Prozessverzögerungen und ähnlichem kann beispielsweise der Zugriff durch nicht autorisierte Dritte auf Kunden- oder Mitarbeiterdaten zu hohen Schadensersatzansprüchen führen. Dies betrifft insbesondere Fälle, bei denen aufgrund des Bekanntwerdens von personenbezogenen Kunden- oder Mitarbeiterdaten das allgemeine Persönlichkeitsrecht verletzt wird oder Fälle, wo Geschäftsgeheimnisse bekannt werden. Hierbei stellt sich häufig die Frage, ob der Unternehmer oder der den Schadensfall auslösende Mitarbeiter den Schaden zu tragen hat.

Es zeigt sich also: auch ein komplexes technisches Sicherheitssystem greift bei absichtlichem oder unbedarftem Handeln der Belegschaft nicht. Das Sicherheitsniveau im Unternehmen steht und fällt mit den Mitarbeitern.

Im Wesentlichen lassen sich für das hohe Sicherheitsrisiko Mitarbeiter drei Gründe ausfindig machen:

1. Unkenntnis
Die Email bleibt das wichtigste Kommunikationsmedium im Business. 2016 wurden in Deutschland rund 626 Milliarden Emails verschickt (Quelle: Statista). Mittlerweile gibt es kaum noch Branchen, in denen nicht via PC verwaltet, kommuniziert oder gearbeitet wird. Doch nicht jeder ist im Bilde, was Trojaner und Phishing sind, wie sie ein sicheres Passwort vergeben und welche allgemeinen Sicherheitskriterien man beachten muss. Abseits der technischen Aspekte sind vielen Mitarbeitern auch juristische Standpunkte nicht bewusst. Darf er etwa den nicht fertig geschriebenen Text auf seinen privaten USB-Stick ziehen? Oder eine E-Mail mit sensiblen Daten an einen externen Dienstleister versenden? Es ist Sache des Arbeitgebers, dafür Sorge zu tragen, dass der Mitarbeiter über die Gefahren, die mit dem Umgang sensibler (Kunden-)Daten einhergehen, aufgeklärt ist. Versäumt der Unternehmer die Aufklärung seiner Mitarbeiter, spricht man von einem sogenannten Organisationsverschulden, das dem Unternehmer zugerechnet wird. Für die Haftung aufgrund Organisationsverschuldens spielt es auch grundsätzlich keine Rolle, ob der Unternehmer die oben genannten Pflichten vorsätzlich oder fahrlässig verletzt hat.

2. Gedankenlosigkeit
Wer denkt schon bei der Flut an täglichen Emails bei jedem Anhang darüber nach, ob sich Schadsoftware dahinter verbirgt. Die hohe Arbeitsverdichtung erfordert schnelle Reaktionen.

Deswegen kleben für den raschen Zugriff Passworte an Post-it‘s am Computer. Vertragsunterlagen landen im Papierkorb statt im Schredder, Adressen werden auf der Schreibtischunterlage notiert. Social Engineering kann hier sehr kreativ werden. Und mintunter gefährlich für Unternehmen und Mitarbeiter – dann nämlich, wenn der Mitarbeiter auf diese Weise grob fahrlässig oder sogar vorsätzlich sensible Daten preisgegeben hat. Wird der Mitarbeiter zuvor durch seinen Arbeitgeber über den Umgang mit den Daten eingewiesen, kommt je nach den Umständen des Einzelfalles, die Haftung des Mitarbeiters gegenüber seinem Arbeitgeber im Rahmen eines sog. Regressanspruches in Betracht.

3. Komplexe Sicherheitsanforderungen
Gestalten umfangreiche Sicherheitsmechanismen Arbeitsprozesse schwergängig und umständlich, steigt das Risiko, die Sicherheitsaspekte zugunsten eines reibungslosen Ablaufes zu vernachlässigen. Sicherheit und Arbeitsvorgänge sollten sich nicht gegenseitig behindern. Hier treffen die Organisationspflichten und die Verhaltenspflichten des Mitarbeiters zusammen: Je komplexer die Sicherheitsanforderungen werden, desto höher steigen die Anforderungen an die Organisation und somit auch die Verantwortung des Arbeitgebers. Werden jedoch die Sicherheitsanforderungen – aus der Perspektive des Arbeitnehmers – einfach gehalten, liegt die Verantwortlichkeit tendenziell eher beim Arbeitnehmer.

Welche Maßnahmen können Unternehmen einsetzen, um das Sicherheitsrisiko Mitarbeit zu verringern?
Unabhängig von den gängigen technischen Instrumenten zur IT-Sicherheit sind vier organisatorische Aspekte zu beachten, die das Sicherheitsniveau deutlich verbessern können:

1. Sicherheitsbewusstsein schaffen – im gesamten Unternehmen
Sicherheit sollte im Unternehmen zum Leitgedanken werden. Und sowohl für Mitarbeiter, Dienstleister und Führungskräfte gelten. Diese sollten die Belegschaft nicht alleine lassen mit der Sicherheitsbedrohung oder sie mit rechtlichen Schritten unter Druck setzen. Wichtige Rahmenbedingung können Unternehmen mit regelmäßige Schulungen schaffen. Sie bauen nicht nur Unsicherheiten und Unkenntnis ab, sondern zeigen den Mitarbeitern auch, dass sie vom Unternehmen bei der Bewältigung von Sicherheitsproblemen unterstützt werden.

2. Kenntnisse erweitern
Zusätzlich zum Sicherheitsbewusstsein benötigt der Mitarbeiter grundlegende Kenntnisse zur Gefahrenlage. Diese sollen und können natürlich keinen Security-Experten aus ihm machen. Aber sie können dafür sorgen, dass er wachsam bleibt – die Raffinesse von Cyberkriminellen ist grenzenlos – und selbstständig kritische Situationen erkennt. Workshops können Szenarien durchspielen, konkrete Handlungsempfehlungen geben und somit eine Routine bei der Anwendung von Sicherheitsmaßnahmen aufbauen. Juristische Grundlagen sollten in einem separaten Papier verfasst werden, die der Rechtsklarheit dienen. Unternehmen sollten – schon zur eigenen rechtlichen Sicherheit – darauf achten, dass die Mitarbeiter das Papier nicht nur kennen, sondern auch unterzeichnen.

3. Sicherheitsrichtlinien vereinfachen
„Hier muss die Devise lauten: einfach, aber wirksam“, sagt Michael Veit, Security Experte bei Sophos. „Ein Mitarbeiter, der die Richtlinie nicht versteht oder sie für zu aufwändig hält, um seine Arbeit effizient erledigen zu können, wird sie nicht umsetzen. Eine komplizierte Sicherheitsrichtlinie ist dann quasi eine nicht existente Sicherheitsrichtlinie. Übersichtliche und begründete Maßnahmen, auf 2-5 Seiten als Orientierungshilfe zusammengefasst, erhöhen die Akzeptanz der Mitarbeiter, sich an diese zu halten.“ Diese Richtlinien sollten als Anlage im Arbeitsvertrag beigefügt werden. Dadurch werden die Maßnahmen verbindlicher Bestandteil des Arbeitsvertrages und erwachsen - je nach konkreter Ausgestaltung - zu sogenannten Haupt- oder Nebenleistungspflichten des Arbeitnehmers.

4. Keine Vermischung von Betriebs- und Privatgeräten
Soll der Mitarbeiter auch von unterwegs Zugriff auf seine Emails und Daten haben, empfiehlt es sich, ihm dafür ein Betriebs-Gerät mitzugeben. So ist die Trennung von Firmen- und Privatdaten sichergestellt. Das Unternehmen kann hier eigene Verschlüsselungslösungen (bei Diebstahl oder Verlust) und Schutzsoftware (vor Viren) installieren und so den Zugriff Fremder auf vertrauliche Daten minimieren. Auch die Verpflichtung zur Nutzung von Betriebsgeräten unter gleichzeitigem Verbot der geschäftlichen Kommunikation mit privaten Endgeräten sollte bereits im Rahmen des Arbeitsvertrags geregelt werden.

Rechtsberatung: RA Sebastian Müller, Magdeburg

Dieser Artikel ist Teil einer von Sophos initiierten Reihe, die sich mit der rechtlichen Seite von IT-Sicherheitsvorfällen in Unternehmen beschäftigt.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de