Unternehmenseigene Virenscanner nicht zum Test privat empfangener Mailanhänge verwenden

Zusammenfassung: Wenn Beschäftigte die unternehmenseigenen Sicherheitsmaßnahmen dazu missbrauchen, privat empfangene Mails auf Viren zu testen, handeln sie unerlaubt. Falls es zu einem Virenbefall durch eine dieser weitergeleiteten Mails kommt, kann der Beschäftigte unter Umständen für entstehende Schäden in Regress genommen werden. In jedem Fall können jedoch arbeitsrechtliche Konsequenzen gezogen werden, da es sich um eine unerlaubte Handlung mit erheblichem Gefährdungspotenzial handelt.

Situation: Der Datenschutzbeauftragte wurde von der IT informiert, das von einem bestimmten Beschäftigten immer wieder Mails mit Anhängen an seinen Mailaccount im Unternehmen weitergeleitet wurden, die in weiten Teilen mit Malware befallen waren. Die erste Vermutung, dass der Beschäftigte dem Unternehmen bewusst Schaden zufügen wolle, bestätigte sich nicht. Auf Nachfragen erfuhr der Datenschutzbeauftragte dann die ganze Geschichte.

Entwarnung war dennoch nicht angesagt: Der Beschäftigte hatte wiederholt in seinem privaten Postfach zuhause dubiose Mails mit noch dubioseren Anhängen empfangen. Da er seinem eigenen Virenscanner offenbar nicht traute, kam er auf die glorreiche Idee, diese Mails einfach ungeöffnet an sein Postfach im Unternehmen weiterzuleiten. Offenbar hatte er großes Vertrauen in die Sicherheitsstrategie des Unternehmens, denn er sagte auf Nachfrage, er sei davon ausgegangen, dass die IT im Unternehmen so gut aufgestellt sei, dass er, wenn die Mail in seinem Postfach dort unbeanstandet ankommt, davon ausgehen kann, dass die Anhänge harmlos seien und daher – so seine Schlussfolgerung – unbesorgt geöffnet werden könnten.

Quasi Brandschutz mit Brandbeschleunigern testen: Der Beschäftigte war sich keiner Schuld bewusst. Erst als er mit dem folgenden drastischen Beispiel konfrontiert wurde, konnte man eine gewisse Nachdenklichkeit erkennen.

Wenn ein Beschäftigter einmal testen möchte, ob ein Brandbeschleuniger für das Anzünden des Holzkohlegrills geeignet ist, dann sollte er nicht auf die Idee kommen, den Brandbeschleuniger zuvor im Unternehmen zu zünden, mit der Vermutung, dass der Brandschutz schon greifen wird.

Gefährdung: Auch wenn es banal erscheint, muss doch immer wieder darauf hingewiesen werden, dass Virenscanner dazu da sind, Viren, die trotz aller anderen Sicherheitsmaßnahmen in die Unternehmens-IT gelangt sind, unschädlich zu machen. Es ist nicht Sinn und Zweck der Virenscanner, diese darauf zu testen, ob ein Virus nicht erkannt wird und zu diesem Zweck die Viren bewusst einzuschleusen. Außerdem müssen sich alle Beteiligten darüber im Klaren sein, dass es täglich mehrere Tausend neue Virensignaturen gibt, die - zumindest bis sie erkannt sind und in den Virenscannern integriert werden – unter Umständen zu einer Infektion der unternehmenseigenen IT führen können.

Mögliche Folgen: Wenn sich bei einem solchen Mini-Penetrationstest tatsächlich eine Schadsoftware in den unternehmenseigenen IT-Systemen ausbreitet, können die Schäden enorm sein. Zumindest wird die Beseitigung der Schadsoftware und deren Folgen einige Zeit in Anspruch nehmen und damit Aufwand und Kosten in erheblichem Umfang auslösen. Bei schlimmeren Fällen kann Produktionsausfall die Folge sein.

Rechtslage: Fügt ein Beschäftigter dem Unternehmen wissentlich Schaden zu oder nimmt er eine Schädigung des Unternehmens bei seinem Handeln billigend in Kauf, kann er zum Ersatz des entstehenden Schadens oder zumindest eines Teils des Schadens herangezogen werden. Außerdem stellt ein solches Vorgehen in der Regel einen eklatanten Verstoß gegen die IT-Richtlinien des Unternehmens dar. Ein solcher Verstoß wird in der Regel auch arbeitsrechtliche Konsequenzen nach sich ziehen.

Gegenstand von Unterweisungen: – ja oder nein? Hier gibt es keine „richtige“ Antwort. Datenschutzbeauftragte und IT-Verantwortliche müssen von Fall zu Fall entscheiden, ob sie diese Geschichte zum Gegenstand von Unterweisungen machen wollen oder nicht – zum einen sollen Mitarbeiter nicht auf solche Ideen gebracht werden, zum anderen wäre im vorliegenden Fall der unfreiwillige Mini-Penetrationstest sicherlich unterblieben, wenn dem Beschäftigten die Rechtslage klar gewesen wäre.

Gegenstand der Datenschutz- und IT-Richtlinie: Unstrittig ist, dass Beschäftigte in der Datenschutz- und IT-Richtlinie des Unternehmens darüber informiert werden müssen, was erlaubt und was nicht erlaubt ist, also dass das absichtliche Einspielen von Schadsoftware oder der fahrlässige Umgang mit verdächtigen Mailanhängen in der hier geschilderten Form untersagt ist. Bei Zuwiderhandlung werden in der Regel arbeitsrechtliche Konsequenzen ge-

zogen. Da die Datenschutz- und IT-Richtlinie regelmäßig Gegenstand von Unterweisungen und Datenschutzschulungen ist, werden in diesem Zusammenhang auch die Gefahren eines derartigen Vorgehens behandelt.

Handlungsempfehlung: Datenschutz- und IT-Richtlinie prüfen und gegebenenfalls ergänzen.

Eberhard Häcker, Ensdorf