/ Stichwort „E-Raids“: Gericht der Europäischen Union unterstreicht die zentrale Rolle von IT-Bereichen bei Dawn Raids

27.11.2014

Kartellrecht | IT & Outsourcing | Compliance & Interne Ermittlungen | Brüssel

Das Gericht der Europäischen Union (EuG) hat eine von der Europäischen Kommission im Jahr 2012 aufgrund von Art. 23 Abs. 1 VO 1/2003 verhängte Geldbuße wegen Nichtduldung einer kartellbehördlichen Durchsuchung bestätigt (Urteil ECLI:EU:T:2014:995 vom 26. November 2014).

Ermittlungsmaßnahmen dürfen nicht behindert werden

Die Kommission hatte gegen die durchsuchten Unternehmen eine Geldbuße von 2,5 Mio. Euro verhängt, weil es bei der Durchsuchung im Hinblick auf E-Mail-Konten und den Zugang zu elektronischen Aufzeichnungen zu einer Reihe von Vorfällen gekommen war. So wurde ein E-Mail-Konto nicht wie angeordnet gesperrt und eingehende E-Mails wurden auf den Unternehmensserver umgeleitet. Damit, so die Kommission, hätten die Unternehmen gegen die Duldungspflicht von Art. 20 Abs. 4 VO 1/2003 verstoßen. Nach dieser Bestimmung müssen Unternehmen durch Entscheidung angeordnete Nachprüfungen dulden. Ein Verstoß gegen diese Duldungspflicht liegt nach Ansicht der Kommission schon dann vor, wenn die zulässigen Ermittlungsmaßnahmen der Kommission verzögert oder behindert werden. Zu diesen Ermittlungsmaßnahmen gehört u.a. die Sperrung von E-Mail-Konten konkreter Mitarbeiter während der Nachprüfung zwecks Beweissicherung.

Im konkreten Fall hatte die Kommission die Sperrung (d.h. die zentrale Änderung der Passwörter und Neuvergabe von nur der Kommission bekannten Passwörtern) von vier E-Mail-Accounts angeordnet. Dem kam die – hier externe – IT-Abteilung nach. Einer der von der Sperrung betroffenen Mitarbeiter arbeitete zu dieser Zeit von zuhause aus und beklagte sich über den nicht mehr funktionierenden E-Mail-Zugang. Ein Mitarbeiter der IT-Abteilung, in Unkenntnis der Durchsuchung und der E-Mail-Sperre, setzte das Passwort erneut zurück und ermöglichte dem Mitarbeiter so den Zugang zu dem eigentlich gesperrten Konto. Zusätzlich hatte der Geschäftsführer eines der durchsuchten Unternehmen am zweiten Tag der Durchsuchung ohne Absprache mit den Kommissionsbeamten in der IT-Abteilung angeordnet, eintreffende E-Mails auf dem Unternehmensserver zu behalten und nicht in die Inbox weiterzuleiten. Dies wurde von den Beamten 24 Stunden später bemerkt.

Pflicht zur unverzüglichen Information relevanter IT-Mitarbeiter über Dawn Raid

Die Klägerinnen hatten u.a. in der Nichtigkeitsklage hinsichtlich der „Entsperrung“ argumentiert, die Ermittlungsmaßnahmen seien von den handelnden Bediensteten nicht vorsätzlich oder fahrlässig behindert worden. Dies ließ das Gericht nicht gelten. Die Unkenntnis der betreffenden Mitarbeiter sei irrelevant. Es sei die Pflicht des IT-Leiters gewesen, seine Mitarbeiter über die Durchsuchung und die damit einhergehenden Anweisungen der Kommissionsbeamten zu informieren und sicherzustellen, dass diese Anweisungen befolgt werden.

Hinsichtlich der Umleitung eingehender E-Mails war der Standpunkt der Unternehmen, dass die Daten auf dem Unternehmensserver nicht manipuliert oder gelöscht worden seien und dass darüber hinaus von der Umleitung nur wenige irrelevante E-Mails betroffen gewesen seien. Dies war nach Ansicht des Gerichts unerheblich, da es sich bei den bußgeldbewehrten Verfahrensverstößen in Art. 23 Abs. 1 VO 1/2003 um schlichte Tätigkeitsdelikte in der Form abstrakter Gefährdungsdelikte handelt und daher auch die Relevanz und Anzahl der betroffenen E-Mails keine Rolle spiele.

Dawn Raid-Schulung für interne und externe IT-Abteilungen

Aus diesem Urteil, welches ähnliche Aspekte betrifft wie die berühmte „Siegelbruch“-Entscheidung gegen E.on („fahrlässiger Siegelbruch“ durch Reinigungsfirma, EuGH v. 22.11.2012, ECLI:EU:C:2012:738), ergibt sich aus Compliance-Gesichtspunkten für Unternehmen, dass bei einem zunehmenden Schwerpunkt von kartellbehördlicher Durchsuchungen im elektronischen Bereich

(„E-Raids“) insbesondere eine umfassende Vorbereitung der IT-Abteilung im Hinblick auf mögliche Dawn Raids dringend geboten ist. Um Verfahrensverstöße zu vermeiden, müssen die Mitarbeiter in diesem sensiblen Bereich gut und umfassend geschult werden und im Ernstfall wissen, was zu tun und was in jedem Fall zu unterlassen ist. Dies gilt auch, wenn die IT-Abteilung teilweise oder vollständig ausgelagert ist.

In diesem Zusammenhang lesenswert ist die „Explanatory Note“ der EU-Kommission, in welcher die Kommission aus ihrer Sicht die Rechte und Pflichten von durchsuchten Unternehmen erläutert. Dort heißt es mit Bezug auf IT-Ermittlungsmaßnahmen:

*„The undertaking may be required to provide **appropriate representatives or members of staff to assist** the Inspectors, not only for explanations on the organisation of the undertaking and its IT environment, but also for **specific tasks such as the temporary blocking of individual email accounts, temporarily disconnecting running computers from the network, removing and re-installing hard drives from computers and providing 'administrator access rights'-support**. When such actions are taken, the undertaking **must not interfere** in any way with these measures and it is the undertaking's responsibility to **inform the employees** affected accordingly*“ (Hervorhebungen hinzugefügt, Rn. 11).

Contact Person

Dr. Alexander Birnstiel, LL.M. (College of Europe)
Mitglied der Practice Group Kartellrecht
Mitglied der Practice Group Compliance & Interne Ermittlungen
Rechtsanwalt

T +49 89 28628241