OTS0016, 10. Mai 2016, 09:00

Mitarbeiter im sozialen Netz als Compliance-Risiko für Unternehmen

Mitarbeiter und Kunden sind heute ständig „online". Am 21. Compliance Netzwerktreffen diskutierte eine Expertenrunde über die Compliance-Risiken, die daraus für Unternehmen entstehen.

Wien (OTS) - „Think! It's not illegal yet." – Ein Plakat mit diesem Ratschlag hat der Rechtsanwalt Rainer Knyrim seinen Mitarbeitern an die Wand geklebt. Nachdenken, bevor man etwas über digitale Wege in die Welt hinausposaunt, sollte eigentlich selbstverständlich sein. Aber man müsse trotzdem öfter daran erinnern, denn über Soziale Medien werde „sehr viel Blödsinn" gepostet. Das sagte der Datenschutzexperte am Podium des 21. Compliance Netzwerktreffens. Rund 180 Gäste folgten der Einladung von LexisNexis und dem Bundesamt für Korruptionsprävention und -bekämpfung (BAK) am 27. April ins Wiener C3 Convention Center, um sich zu den Risiken im Umgang mit Internet und Social Media am Arbeitsplatz auszutauschen.

Moderiert von Dr. Martin Eckel, Partner der Kanzlei Taylor Wessing, diskutierten neben Dr. Rainer Knyrim noch Charlotte Eberl, Director Corporate Compliance Agrana, Mag. Leopold Löschl, Leiter des C4 Cybercrime Competence Center beim Bund und Mag. Maximilian Schrems miteinander. Letzterer ist Begründer der Initiative „Europe versus Facebook". Mit seinem juristischen Kampf für die Durchsetzung von europäischem Datenschutzrecht auch gegen US-Konzerne hat er unter anderem das „Safe Harbor-Abkommen" zwischen EU und USA zu Fall gebracht.

Cyberattacken: Das Dunkelfeld wächst

Cybercrime-Bekämpfer Leopold Löschl sprach eine Warnung aus: Die Zahl der Cyberattacken nimmt zu. Der neueste Trend ist Ransomeware, also Programme, die Unternehmensdaten verschlüsseln. Erst nach Zahlung eines „Lösegelds" an die Angreifer werden die IT-Systeme wieder freigegeben. Daher sollten Mitarbeiter nur mit Geräten der Firma arbeiten, vor allem auch im Home Office.

Kontrolle: Privates und Job trennen

Auch Rainer Knyrim sieht die Vermischung von Privat- und Firmensystemen als wichtigste Risikoquelle: Die Behörden haben im Verdachtsfall das Recht, jede Art von Kommunikation zu durchsuchen, sei es nun WhatsApp oder Facebook. Nicht so das Unternehmen, dem das Auslesen privater Mitteilungen seiner Mitarbeiter verboten ist. Charlotte Eberl sprach sich gegen die generelle Freigabe privater Internetnutzung am Arbeitsplatz aus. Duldet dies der Arbeitgeber über längere Zeit, gibt es bei Missbrauch kaum mehr eine Handhabe, so die Compliance-Verantwortliche der Agrana.

Facebook: Wahrheit und Mythos

Maximilian Schrems gab Einblicke in das Innenleben von Facebook. Der Aktivist hatte sich vom US-Internetkonzern alle über ihn gespeicherten Userdaten zusenden lassen. Dieses umfangreiche Dokument enthielt auch jene Kommentare, die zwar von Schrems selbst gelöscht, von Facebook jedoch nur als „gelöscht" gekennzeichnet wurden. Das Problematische an Facebook ist nach Ansicht des Juristen die Datensammelwut, ohne dass irgendjemand wüsste, was mit den Daten geschieht und wer sie in die Hände bekommt.

Nähere Infos und Fotos zur Veranstaltung unter www.compliance-praxis.at.

Rückfragen & Kontakt:

LexisNexis
Mag. (FH) Sonja Thomschitz
Leitung Marketing & PR
01/ 534 52-1918
presse@lexisnexis.at
www.lexisnexis.at

LexisNexis

ADRESSE

RÜCKFRAGEN & KONTAKT

LexisNexis
Mag. (FH) Sonja Thomschitz
Leitung Marketing & PR
01/ 534 52-1918
presse@lexisnexis.at
www.lexisnexis.at

MEHR ZU DIESER AUSSENDUNG

Stichworte:
Unternehmen, Justiz, Recht, Kriminalität, Veranstaltung

Channel:
Wirtschaft

Geobezug:
Wien