… und plötzlich sind die Daten weg

Haftung bei Cybersichersicherheitsvorfällen in der Forschung

| ROLF SCHWARTMANN | STEVE RITTER | **Hochschulen werden immer häufiger Ziel von immer kniffligeren Cyberangriffen. Durch die Abwehr über die IT und Schulungen von Beschäftigten können viele von ihnen abgewehrt werden. Was aber, wenn doch einmal Daten entwendet oder verschlüsselt werden? Wer haftet für den Verlust?**

Nicht erst seit der Corona-Krise ist IT eine unverzichtbare Voraussetzung für Forschung und Lehre geworden. Einige Forschungsbereiche wären ohne IT kaum denkbar, da die benötigten enormen Datenmengen den Forschenden erst durch Algorithmen erschlossen werden können. In anderen Bereichen sind es die großen Zahlen und komplizierten Berechnungen, die erst dank leistungsfähiger IT eine praktische wissenschaftliche Untersuchung von Theorien erlauben.

Angriffsziel Forschungsdaten

Allem gemeinsam ist, dass die zugrundeliegenden Daten als Forschungsgrundlage und -ergebnisse in den Computern vorliegen, mit denen sie verarbeitet werden. Sind diese Rechner an ein Netzwerk angeschlossen, sind die Daten auch für Angreifer zugänglich. Gerade in technologienahen Forschungsbereichen muss immer damit gerechnet werden, dass Dritte an die Forschungsergebnisse gelangen wollen, um dadurch ihren Rückstand aufzuholen oder einen Vorsprung zu gewinnen.

Bereits 2014 wurde der Fall des Deutschen Zentrums für Luft und Raumfahrt publik, bei dem ausländische Angreifer versuchten, Daten zu Raumfahrt- und Rüstungstechnologien durch einen Cyberangriff zu erlangen, indem sie Netzwerke mit Schadsoftware infiltrierten.

Wenn Dritte Schadensanspruch geltend machen

Wenn durch einen Cybersicherheitsvorfall die Daten einer Forschungsgruppe gestohlen oder vernichtet werden, kann das auch Haftungsansprüche in den verschiedensten Konstellationen auslösen. Das gilt natürlich nur, wenn der Cyberangriff erfolgreich war, weil die notwendigen Schutzmaßnahmen pflichtwidrig unterlassen wurden. Was bedeutet das für die Forschenden?

Im Rahmen von Forschungskooperationen befinden sich unter den Daten oft solche, die von Dritten – z.B. Unternehmen – bereitgestellt oder für diese erarbeitet wurden. Werden diese Daten bei einem Cyberangriff entwendet, können diese Dritten den Ersatz des ihnen dadurch entstandenen Schadens verlangen. Diesen Anspruch werden sie in der Regel gegenüber der Hochschule geltend machen, da sie bei einer Kooperation meist die Vertragspartnerin ist. Wenn der Dritte keinen Vertrag mit der Hochschule, sondern direkt mit den Mitgliedern der Forschungsgruppe hat – und sei es auch nur im Rahmen einer Vertraulichkeitsvereinbarung – kann der Dritte auch von den Forschenden selbst Schadensersatz verlangen. Oftmals sehen Vertraulichkeitsvereinbarungen entsprechende Klauseln über Vertragsstrafen oder pauschalierten Schadensersatz vor. Falls nicht, wird sich der Dritte jedenfalls bei Vorliegen eines Verschuldens der Forschenden auf die üblichen zivilrechtlichen Schadensersatzregelungen stützen können.

> »Wenn ein Dritter mit den Mitgliedern einer Forschungsgruppe einen Vertrag hat, kann er auch von ihnen Schadensersatz verlangen.«

Der Auftraggeber eines Forschungsprojekts kann Schadensersatz geltend machen, wenn die für ihn und mit seinem Geld erarbeiteten Daten etwa durch Ransomware unbrauchbar gemacht werden und er dadurch einen geldwerten Schaden erleidet. Auch hier hängt es in der Regel von der Vertragslage ab, worauf sich der Schadensersatzanspruch stützt und gegen wen er sich richtet. In der Regel wird der Auftraggeber von seinem Vertragspartner Ersatz verlangen, dies können die Hochschule oder auch direkt die Forschenden sein. Ist es die Hochschule

AUTOREN

Foto: TH-Köln/Schmülgen

Rolf Schwartmann ist Professor an der Kölner Forschungsstelle für Medienrecht, TH Köln, sowie Sachverständiger des DHV für IT- und Datenrecht.

Foto: privat

Steve Ritter ist Referatsleiter für IT-Sicherheit und Recht im Bundesamt für Sicherheit in der Informationstechnik (BSI).

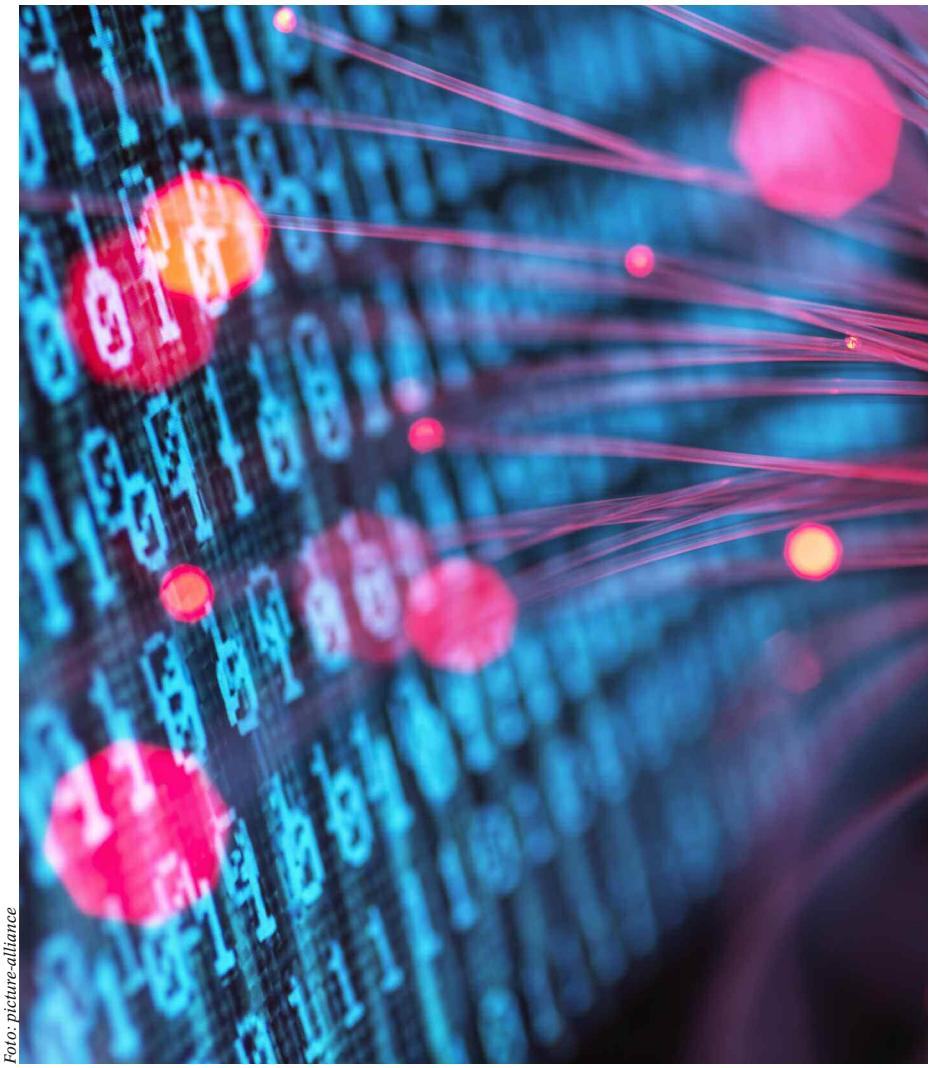

Foto: picture-alliance

und wurden die notwendigen Sicherheitsmaßnahmen durch die Forschenden als Mitarbeiter der Hochschule unterlassen, so kann die Hochschule ihrerseits im Wege des Regress Schadensersatzansprüche gegenüber ihren Angestellten geltend machen. Denn das Unterlassen der notwendigen Absicherungsmaßnahmen stellt in der Regel eine Verletzung der Pflichten aus dem Arbeits- bzw. Dienstverhältnis dar.

Daten sind nicht gleich Daten

Wenn zwar die Vertragsbeziehung direkt zu den Forschenden besteht, die unterlassene Absicherung aber vom IT-Personal der Hochschule zu vertreten ist (z.B. weil die Daten in deren Rechenzentrum lagen) kann es zu einem Regress der Forscher gegen die Hochschule kommen, sofern diese die Absicherung pflichtwidrig unterlassen hat. Da der Absicherungsbedarf davon abhängt, was für Daten verarbeitet werden (für geheime industrielle/staatliche Forschungsergebnisse betreiben Angreifer viel Aufwand), müssen die Forscher sich jedoch zuvor versichern, dass der Hochschule das notwendige Absicherungsniveau auch bekannt ist. Gehen die Daten trotz normaler Absicherung verloren, weil die Daten für Angreifer sehr wertvoll waren, können die Forscher keinen Regress fordern, wenn der Hochschule der hohe Schutzbedarf nicht bekannt war.

Wenn es sich bei den gestohlenen oder verschlüsselten Daten um personenbezogene Daten handelt (z.B. Gesundheitsdaten in der medizinischen Forschung oder biometrische Daten bei der Forschung zu digitalen Identitäten), können die Betroffenen Schadensersatz nach Art. 82 Abs. 1 DSGVO von den Verantwortlichen fordern. Erfasst sind sowohl immaterielle Schäden – denkbar etwa bei intimen Informationen – als auch Vermögensschäden. Letztere können bei wirtschaftlich relevanten Daten entstehen. Die Verantwortung trifft sowohl den (gemeinsam) Verantwortlichen als auch den Auftragsverarbeiter und zwar entsprechend des jeweiligen Verursachungsbeitrages. Bußgelder nach Art. 83 DSGVO gegen Amtsträger und Beschäftigte öffentlicher Stellen, die für die Hochschule handeln können weder nach DSGVO noch nach BDSG verhangen werden. Es kommen die sonstigen Befugnisse nach Artt. 58, 84 DSGVO und gegebenenfalls Amtshaftungsansprüche gegen die Handelnden in Betracht. Für private Forschung, etwa im Rahmen von privater Nebentätigkeit, sind Forscherinnen und Forscher auch datenschutzrechtlich selbst verantwortlich und können Bußgeldadressaten sein.

Abwendung der Haftung

Um die Haftung abzuwenden, sollten die Forschenden den Schutzbedarf der Daten ermitteln und dann die entsprechenden Schutzmaßnahmen – z.B. nach BSI-IT-Grundschutz – vornehmen. Werden die IT-Systeme nicht durch sie selbst betrieben, sondern durch die Hochschule, sollten sie sich entsprechende Schutzmaßnahmen schriftlich zusichern lassen. Bei personenbezogenen Daten kann dafür auch eine Vereinbarung zur Auftragsdatenverarbeitung nebst Vereinbarung der notwendigen technischen und organisatorischen Maßnahmen gehören. Es kann auch über eine Cybersicherheitsversicherung nachgedacht werden. Üblicherweise wird diese jedoch auch entsprechende IT-Sicherheitsmaßnahmen einfordern, bevor das Restrisiko durch sie übernommen wird. Teilweise bieten die Versicherungen dafür aber auch Unterstützung bei der Bewältigung von IT-Sicherheitsvorfällen an. Gegen den Verlust der Daten durch Ransomware oder schlichte Löschung hilft es oft schon, adäquat gegen Zugriff gesicherte regelmäßige Backups der Daten auf nicht vernetzten Speichern anzulegen.

ONLINE

→ ***Hochschulen arbeiten an besserem IT-Schutz***
Wie können sich Hochschulen am besten vor Hacking schützen? Welche Cyberangriffe hält das BSI für besonders gefährlich? F&L-Hintergrund: https://t1p.de/no5a

Weitere Beiträge zur IT-Sicherheit an Hochschulen im F&L-Schwerpunkt:
forschung-und-lehre.de/it-sicherheit/