Datenverlust bei MOVEit Transfer: So sollten Unternehmen jetzt handeln

Hacker haben offenbar eine Sicherheitslücke der Software „MOVEit Transfer“ genutzt, um Daten abzugreifen und Zahlungen zu fordern. Zahlreiche Unternehmen könnten betroffen sein. Der Hersteller der Software hat inzwischen Updates bereitgestellt. Doch mit einer Aktualisierung der Software ist es nicht getan. Das Datenschutzrecht verlangt weitergehende Maßnahmen von Unternehmen, insbesondere eine lückenlose Aufklärung.

MOVEit Transfer ist ein Programm, mit dem man große Dateien austauschen kann, zum Beispiel wenn diese zu groß sind, um sie in eine E-Mail zu hängen. Tausende Unternehmen nutzten diese Software, um mit ihr Unternehmensdaten auszutauschen.

Der Hersteller hatte bekannt gegeben, dass eine kritische Schwachstelle (CVE-2023-36934) in seinem Softwareprodukt gefunden wurde. Medienberichten zufolge wurde die Sicherheitslücke von einer Gruppe von Hackern ausgenutzt. Diese sind möglicherweise an enorme Mengen von sensiblen Unternehmensdaten gelangt. Die Gruppe soll jetzt mit der Veröffentlichung der Daten drohen, wenn kein Lösegeld gezahlt wird.

In den letzten Tagen und Wochen stieg die Zahl der Unternehmen, die öffentlich äußern, dass sie betroffen seien. Darunter sind Unternehmen aus allen Branchen und aller Größenordnungen – vom Start-up bis zum DAX-Unternehmen. Handeln sollten jedoch nicht nur Unternehmen, die ein Datenleck festgestellt haben, sondern alle Anwender:innen der Software MOVEit Transfer.

Das ist bei Datenverlusten in rechtlicher und technologischer Hinsicht zu tun

Aus rechtlicher Sicht

Bei einem Datenverlust ist es nicht damit getan, die Sicherheitslücke zu schließen. Vielmehr sollte sofort untersucht werden, welche Daten betroffen sind und welche Konsequenzen drohen. Wenn zum Beispiel vertrauliche Daten von Kunden in falsche Hände gekommen sind, bedeutet dies regelmäßig einen Verstoß gegen vertragliche Verpflichtungen und Vertraulichkeitsvereinbarungen. Neben der umgehenden Information der betroffenen Kunden ist es erforderlich, zu prüfen, ob das Datenleck auch Schadensersatzansprüche von Kunden oder Lieferanten auslösen könnte. Nur so kann vermieden werden, dass der Schaden intensiviert wird oder unerkannt bleibt.

Soweit personenbezogene Daten betroffen sind, greifen die Melde- und Benachrichtigungspflichten der Datenschutzgrundverordnung (DSGVO): Spätestens 72 Stunden nach Kenntnisnahme durch das Unternehmen müssen die zuständige Datenschutzaufsichtsbehörde und womöglich auch die betroffenen Kunden oder Mitarbeiter:innen umfangreich informiert werden. Auch hier ist es entscheidend, dass die Ursache und das Ausmaß der Datenpanne ermittelt werden. Nur so kann beurteilt werden, welche Risiken für die betroffenen Personen bestehen und welche Melde- und Benachrichtigungspflichten konkret bestehen. Für KRITIS-Unternehmen kommt unter Umständen eine Meldung beim Bundesamt für Sicherheit in der Informationstechnik (BSI) hinzu. Bei Nichteinhalten dieser Pflichten drohen erhebliche Bußgelder und weitere aufsichtsrechtliche Maßnahmen.

Auch wenn es in Anbetracht einer schnellen Lösung verlockend sein kann, dem Lösegeldverlangen nachzugeben, sollte diese Entscheidung keinesfalls voreilig getroffen werden. Da die Zahlung auf derartige Lösegeldforderungen als Terrorismusfinanzierung oder Unterstützung einer kriminellen Vereinigung strafbar sein kann, sollte in jedem Fall rechtlicher Beistand zu Rate gezogen werden.

Aus technologischer Sicht

Selbst wenn Organisationen inzwischen die Sicherheitslücke durch die Updates des Herstellers geschlossen haben, bleibt die Notwendigkeit der lückenlosen, forensischen Aufklärung des Vorfalls.

Nach Einschätzung von Expert:innen konnten Kriminelle die Sicherheitslücke schon lange ausnutzen. Womöglich ist die Hackergruppe also schon seit einiger Zeit in den IT-Systemen der betroffenen Unternehmen unterwegs und hatten Zugriff auf deren Daten. Das BSI empfiehlt daher schon seit Wochen, aktiv nach Anzeichen für eine Kompromittierung Ausschau zu halten.

eDiscovery schafft Transparenz

Zudem ist es wichtig zu verstehen, welche Daten genau abgeflossen sind, um die richtigen Maßnahmen (siehe oben) ergreifen zu können. Eine eDiscovery und damit eine Sichtung der abgeflossenen Daten schafft Transparenz. Beispielsweise können damit die abgeflossenen Daten in Kategorien (zum Beispiel „Personenbezogene Daten“, „Daten Dritter“ oder „Betriebsgeheimnisse“) eingeteilt und erforderliche Maßnahmen eingeleitet werden.

So sollten MOVEit Transfer-Nutzer:innen jetzt handeln

Alle Unternehmen, die MOVEit Transfer genutzt haben, sollten zeitnah eine forensische Untersuchung durchführen und prüfen, ob möglicherweise Daten abgegriffen wurden, und wenn ja, mittels einer eDiscovery überprüfen, welche Daten betroffen sind. Hierbei sollten Datenschutzexpert:innen eng mit Forensiker:innen und Cyber-Security-Expert:innen zusammenarbeiten. Präventiv sollten Unternehmen ein Security-Audit durchführen, um Sicherheitslücken aufzudecken und passende Gegenmaßnahmen abzuleiten, die helfen, derartige Fälle künftig zu verhindern.

Wenn ein Datenleck festgestellt wird (zum Beispiel durch interne Ermittlungen oder Hinweise Dritter), sollte untersucht werden, ob es sich bei den betroffenen Daten um personenbezogene oder sogar um besonders sensible personenbezogene Daten handelt. In dem Fall muss das betroffene Unternehmen unverzüglich Kontakt mit der Aufsichtsbehörde und den betroffenen Dateninhaber:innen aufnehmen. Damit werden einerseits Rechtspflichten erfüllt und durch eine professionelle Handhabung möglicherweise auch Massenklagen wegen der Datenschutzverstöße verhindert.

Die gute Nachricht: Um in Zukunft solche Fälle zu vermeiden, können Unternehmen Maßnahmen treffen. Ein gutes Datenschutz-Management und Information Security Management erschweren es Hackern erheblich, an Daten zu

gelangen.

Gemeinsam mit Expert:innen für Cyber Incident Response & Investigation der KPMG AG Wirtschaftsprüfungsgesellschaft können wir von der KPMG Law Rechtsanwaltsgesellschaft mbH als Datenschutzexpert:innen die notwendigen Maßnahmen für Sie übernehmen. Sprechen Sie uns an.

Dieser Beitrag ist in Kooperation mit Michael Sauermann und Jan Stoelting, beide Partner der KPMG AG Wirtschaftsprüfungsgesellschaft, entstanden.

Ansprechpartner:

Francois Heynike, LL.M. (Stellenbosch)
Tel: +49-69-951195770
fheynike@kpmg-law.com

Dr. Jyn Schultze-Melling, LL.M.
Tel: +49 30 530199 410
jschultzemelling@kpmg-law.com