

Riesiges Datenleck bei Buchbinder

Heise spricht von einem der größten Datenlecks in der Geschichte der Bundesrepublik: Zehn Terabyte sensibler Kundendaten der Autovermietung Buchbinder waren wochenlang für jedermann im Netz zugänglich.

Kommentar von Matthias Canisius, Director CEE, SentinelOne

„Unsere digitalen Daten sind unser wertvollstes und gleichzeitig das am stärksten bedrohte Gut. Egal ob personenbezogene Kunden- und Mitarbeiterdaten, geistiges Eigentum, Entwicklungsinformationen oder Umsatzzahlen – eine unerwünschte Offenlegung sensibler Daten kann sehr schnell sehr teuer werden. Das dürfte auch Buchbinder zu spüren bekommen. Denn aus juristischer Sicht ist ein derart offener Server ein katastrophaler Verstoß gegen die Vorgaben der DSGVO. Sollte die Aufsichtsbehörde tatsächlich Nachlässigkeiten auf Seiten des Unternehmens feststellen, dürfte ein empfindlich hohes Bußgeld fällig sein.“

Ich gebe zu: Wirksamer und nachhaltiger Datenschutz ist im Zeitalter von Digitalisierung und Big Data längst kein Kinderspiel mehr. Gerade die sichere Verwaltung von sensiblen personenbezogenen Informationen ist allein ob der schiereren Menge der Daten eine enorme Herausforderung. Hinzu kommen hochentwickelte Cyber-Angriffsmethoden und aggressive Malware, die immer schwerer aufzuspüren und abzuwehren ist.

Beim Buchbinder-Datenleak war dies jedoch nicht das Problem. Ursache des Lecks war vielmehr ein schlichter Konfigurationsfehler bei einem Backup-Server, der es jedem Internetnutzer ermöglicht hat, die auf dem Server abgelegten Dateien herunterzuladen – und zwar ohne die Eingabe eines Passwortes. Das ist ärgerlich, denn das Aufspüren solcher Schwachstellen im System ist an sich keine große Herausforderung. Schon heute gibt es verschiedene Open-Source-Tools, die sämtliche IPv4-Adressen auf offene Dienste hin untersuchen. Hinzu kommt, dass das Unternehmen wohl schon vor ein paar Wochen über die offenen Ports informiert wurde, darauf aber – warum auch immer – nicht reagiert hat.

Der Vorfall macht eines deutlich: Auch knapp zwei Jahre nach Einführung der DSGVO sind Unternehmen bei der Umsetzung eines konsequenten Datenschutzes nach wie vor ziemlich überfordert und zum Teil nicht in der Lage, grundlegende Sicherheitsmaßnahmen zu ergreifen. Ich hoffe, dass der Buchbinder-Fall ein Weckruf ist und die Verantwortlichen in Unternehmen zum Handeln auffordert. Wenn nicht die negativen Schlagzeilen allein Bauchschmerzen verursachen, dann vielleicht die extremen Bußgelder der DSGVO, die folgen könnten.“



Über SentinelOne

SentinelOne ist ein Pionier für autonomen Endpunktschutz und vereint die Prävention, Identifikation, Abwehr und Reaktion auf Angriffe jeglicher Art in einem einzigen Agenten. Dank dem Einsatz von künstlicher Intelligenz können Bedrohungen sowohl on-premises als auch in Cloud-Umgebungen automatisch und in Echtzeit eliminiert werden. Dabei ist die SentinelOne-Plattform ausgesprochen bedienerfreundlich und bietet eine herausragende Sichtbarkeit über alle kritischen Netzwerkvorgänge. Distributor in Deutschland, Österreich und der Schweiz ist [Exclusive Networks](#).

Folgen Sie SentinelOne:

Website: [sentinelone.com](https://www.sentinelone.com)

Blog: <https://www.sentinelone.com/blog/>

Twitter: twitter.com/SentinelOneDE

LinkedIn: [Linkedin.com/company/SentinelOne](https://www.linkedin.com/company/SentinelOne)

YouTube: [SentinelOne on YouTube](#)