Dienstvereinbarung zum Betrieb von Endpoint-Detection and Response Lösungen (DV EDR)

zwischen

der Universität Leipzig
(ohne Medizinische Fakultät)

und

dem Personalrat Hochschulbereich
der Universität Leipzig

§ 1 Gegenstand der Dienstvereinbarung und Begriffsbestimmung

(1) Die Universität Leipzig betreibt „Endpoint-Detection and Response"-Lösungen. Der Einsatz von EDR-Lösungen stellt eine unverzichtbare technische Sicherheitsmaßnahme zum Schutz vor Schadsoftware und damit explizit auch für den Schutz von persönlichen Daten der Bediensteten der Universität Leipzig (ohne Medizinische Fakultät) dar. Der Einsatz einer solcher Schutzmaßnahmen ist für die Universität Leipzig gemäß einschlägiger Sicherheitsanforderungen aus dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik obligatorisch.[1]

(2) Prinzipiell sollen die Schutzlösungen durch automatische Systemüberwachung schädliche Dateien und auffälliges Systemverhalten erkennen und die Ausführung von Schadcode verhindern. Der Zweck der EDR-Lösungen ist die Verhinderung, die Bearbeitung und die Auswertung von IT-Sicherheitsvorfällen.

(3) Ein IT-Sicherheitsvorfall ist ein negatives Ereignis, dass die Informationssicherheit (also Vertraulichkeit, Verfügbarkeit und/oder Integrität) von Daten, Informationen, Geschäftsprozessen, IT-Services, IT-Systemen, IT-Anwendungen und der Universitäts-infrastruktur beeinträchtigt.

§ 2 Zweck der Dienstvereinbarung

(1) Die Dienstvereinbarung dient dem Schutz der Beschäftigten vor unzulässigem Gebrauch ihrer persönlichen Daten sowie dem Schutz der zuständigen Administratoren, welche mit der Bearbeitung betraut sind.

(2) Zweck der Dienstvereinbarung ist es, eine Leistungskontrolle und Leistungsmessung auf Basis der Erhebung, Verarbeitung und Auswertung der in den EDR-Lösungen anfallenden Protokolldaten auszuschließen. Gleiches gilt für eine unzulässige Verhaltenskontrolle.

(3) Es dürfen ausschließlich zu folgenden Zwecken Daten protokolliert werden:
a. Bearbeitung, Untersuchung und Dokumentation von IT-Sicherheitsvorfällen,
b. Nachweis über die Einhaltung der datenschutzrechtlichen Bestimmungen,
c. technische Fehlersuche in den Systemen,
d. Sicherstellung und Aufrechterhaltung der Betriebsbereitschaft des Systems,
e. Abwehr von Gefahren.

§ 3 Geltungsbereich

(1) Diese Dienstvereinbarung gilt für alle Nutzer:innen, die IT-Systeme mit EDR-Lösungen nutzen, die in Verbindung mit der IT-Infrastruktur der Universität Leipzig verwendet werden. Sie gilt grundsätzlich für alle Beschäftigte der Universität Leipzig, die vom Personalrat Hochschulbereich gemäß § 4 SächsPersVG vertreten werden.

(2) Alle weiteren Personen, die nicht unter Absatz 1 fallen und die Zugang zu auf den IT-Systemen gespeicherte Daten haben oder denen Zugriff auf die IT-Systeme der Universität Leipzig gewährt wird, sind auf die Einhaltung der Regelungen dieser Dienstvereinbarung zu verpflichten.

§ 4 Leistungs-/Verhaltenskontrolle

(1) Eine Verwendung von Protokolldaten aus den EDR-Systemen über die im § 1 und § 2 Abs. 3 genannten Zwecke hinaus ist unzulässig.

(2) Eine über die im § 1 und § 2, Abs. 3 genannten Zwecke hinausgehende Überwachung und Kontrolle der Arbeitsleistung sowie des Verhaltens von Beschäftigten durch die Erhebung, Verarbeitung und Auswertung der in den EDR-Lösungen anfallenden Protokolldaten ist ausdrücklich untersagt.

[1] Baustein OPS.1.1.4 „Schutz vor Schadprogrammen" aus dem IT-Grundschutz-Kompendium

§ 5 Zugriff

Der Zugriff auf, sowie die Auswertung von anfallenden Protokolldaten wird unter Beachtung der o. g. Zweckbestimmungen auf einen sehr eingeschränkten und autorisierten Kreis zuständiger Bediensteter begrenzt (siehe Anlage 1). Der zugriffsberechtigte Personenkreis ist zu dokumentieren und auf die Einhaltung dieser Dienstvereinbarung zu verpflichten. Die Weitergabe von Protokolldaten und Informationen an Dritte ist nur zu den in § 1 und § 2 genannten Zwecken zulässig. Eine Weitergabe zu anderweitigen Verwendungen, z. B. zur Leistungs- und Verhaltenskontrolle von Bediensteten ist ausdrücklich untersagt.

§ 6 Datenspeicherung-, -auswertung und -löschung

(1) Es dürfen nur Daten gespeichert werden, welche den in § 1 und § 2 Abs. 3 genannten Zwecken dienen. Darüber hinausgehende nicht erforderliche Daten, die in diesem Zusammenhang abgerufen werden dürfen nur – sofern unbedingt notwendig – pseudoanonymisiert erfasst werden.

(2) Die Datenspeicherung, -auswertung und -löschung erfolgt gemäß den Bestimmungen in § 12 und § 13 SächsISichG.

(3) Durch geeignete technische und organisatorische Maßnahmen ist durch die Dienststellenleitung sicherzustellen, dass Unbefugte keine Möglichkeit haben, die gespeicherten Daten und Protokolldaten zu lesen, zu verändern, zu kopieren oder zu löschen.

(4) Eine Zurückverfolgung pseudoanonymisierter Daten ist nur zur Erfüllung der im Rahmen von § 1 und § 2 Abs. 3 genannten Zwecke gestattet.

(5) Werden Erkenntnisse über Leistung und Verhalten von Beschäftigten unter Missachtung oder Verletzung dieser Vereinbarung gewonnen, so sind sie zur Begründung, Rechtfertigung oder als Beweismittel für personelle Maßnahmen unzulässig. Gleichermaßen sind arbeitsrechtliche Maßnahmen, die auf einer nach dieser Vereinbarung rechtswidrigen Datenerfassung und/oder –nutzung basieren, untersagt. Personelle Maßnahmen, die dennoch unter Verletzung dieser Vereinbarung angeordnet bzw. durchgeführt werden, sind unwirksam und rückgängig zu machen. Das gilt auch bei arbeitsgerichtlichen Streitigkeiten.

(6) Die Auswertung der Daten sowie die Bearbeitung der Sicherheitsvorfälle erfolgt nach den Vorgaben des IT-Grundschutz (BSI), insbesondere dem Baustein DER 2.1 Behandlung von Sicherheitsvorfälle des aktuell gültigem IT-Grundschutz-Kompendiums.[2]

§ 7 Schulung

Die zuständigen Bediensteten nach § 5 dieser Dienstvereinbarung sind in geeigneter Weise in die Handhabung einzuweisen.

§ 8 Datenschutz

(1) Bei der Verarbeitung und Speicherung sämtlicher Daten, insbesondere personenbezogener Daten, sind die Datenschutzvorschriften gemäß EU-DSGVO, BDSG und des SächsDSDG zu beachten.

(2) Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten erfolgt ausschließlich für die in § 1 und § 2 Abs. 3 dieser Dienstvereinbarung benannten Zwecke. Der Zugriff auf Protokolldaten ist einzig den jeweiligen zugriffberechtigten Personen nach § 5 und § 9 dieser Dienstvereinbarung gestattet. Diese sind dem Datengeheimnis verpflichtet. Die Verantwortung aus dieser Verpflichtung ist ihnen angemessen zu erläutern und im Rahmen der Unterschriftsleistung gemäß § 5 dieser DV zu bestätigen.

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2023.pdf?__blob=publicationFile&v=3#download=1

§ 9 Information/Mitbestimmung des Personalrats Hochschulbereich und Beauftragter

(1) Der Personalrat Hochschulbereich, die/der Datenschutzbeauftrage sowie die/der Sicherheitsbeauftragte haben das Recht, die Einhaltung der Dienstvereinbarung unter Beachtung der gesetzlichen Regelungen, der Personalrat Hochschulbereich insbesondere unter Beachtung des § 73 Abs. 1 Nr. 2 SächsPersVG, zu überprüfen.

(2) Den in Abs. 1 genannten Interessensvertretern sind auf Verlangen notwendige Informationen zu geben, um die Einhaltung der Dienstvereinbarung zu überprüfen.

(3) Der Hochschulpersonalrat kann sich in Abstimmung mit den Verantwortlichen in den betroffenen Struktureinheiten (§ 5) über die praktische Arbeit mit der EDR-Lösung informieren.

(4) Liegt ein Verdacht auf Verletzung des § 6, Abs. 5 vor, hat die Dienststelle dem Personalrat Hochschulbereich auf dessen Anforderung alle den Sachverhalt betreffende Informationen und Unterlagen umfassend und schriftlich zur Verfügung zu stellen. Der ist zu unterrichten.

(5) Der Personalrat Hochschulbereich ist frühzeitig über die Einführung einer neuen Version inkl. neuer Funktionen zu informieren.

§ 10 Salvatorische Klausel

Sollten eine oder mehrere Bestimmungen dieser Dienstvereinbarung ganz oder teilweise unwirksam sein oder werden, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. An die Stelle der rechtsunwirksamen Bestimmungen tritt eine inhaltlich möglichst gleiche Regelung, die dem Zweck der gewollten Regelung am nächsten kommt.

§ 11 Inkrafttreten, Geltungsdauer und Kündigung

04. Aug. 2023

Diese Dienstvereinbarung tritt mit dem … 2023 in Kraft und gilt unbefristet. Sie kann von beiden Seiten mit einer Kündigungsfrist von sechs Wochen zum Quartalsende gekündigt werden. Im Falle der Kündigung wirkt die Dienstvereinbarung 6 Monate nach. In diesem Zeitraum haben die Parteien Verhandlungen über eine neue Dienstvereinbarung aufzunehmen.

Einvernehmliche Änderungen und Erweiterungen bedürfen der Schriftform und sind jederzeit ohne Kündigung möglich.

Leipzig, den 1. August 2023

Für die Universität Leipzig:

Prof. Dr. Eva Inés Obergfell
Rektorin der Universität Leipzig

Leipzig, den 04. Aug. 2023

Für den Personalrat Hochschulbereich:

Thomas Biermann
Vorsitzender des Personalrates Hochschulbereich

Anlage 1

Security-Administratoren/-Administratorinnen der Endpoint-Detection and Response Lösung des Universitätsrechenzentrums Leipzig

Mitarbeiterinnen und Mitarbeiter Servicedesk des Universitätsrechenzentrums Leipzig