Dienstvereinbarung über den Einsatz eines Endpoint Detection and Response Systems (EDR)

Zwischen der

Ruprecht-Karls-Universität Heidelberg

– nachfolgend „Dienststelle“ –

und dem

Personalrat

der Ruprecht-Karls-Universität Heidelberg

– nachfolgend „Personalrat“ –

Präambel

Die fortschreitende Digitalisierung von Forschung, Lehre und Verwaltung an Universitäten führt zu einer stetig wachsenden Abhängigkeit von informationstechnischen Systemen. Hochschulen sind aufgrund ihrer offenen Netzstrukturen, internationaler Kooperationen, sensibler Forschungsdaten sowie personenbezogener Daten von Studierenden und Beschäftigten in besonderem Maße Ziel von Cyberangriffen.

In den vergangenen Jahren haben sicherheitsrelevante Vorfälle an deutschen Hochschulen gezeigt, dass Angriffe auf IT-Infrastrukturen zu erheblichen Einschränkungen des Lehr-, Forschungs- und Verwaltungsbetriebs führen können.

Zum Schutz der IT-Infrastruktur, der wissenschaftlichen Daten, der personenbezogenen Daten sowie zur Sicherstellung der Funktionsfähigkeit der Universität ist der Einsatz moderner IT-Sicherheitsmaßnahmen erforderlich. Endpoint Detection and Response Systeme (EDR) ermöglichen es, sicherheitsrelevante Ereignisse auf Clients und Servern frühzeitig zu erkennen, automatisiert zu analysieren und geeignete Gegenmaßnahmen einzuleiten.

Ziel dieser Dienstvereinbarung ist es, den Einsatz eines EDR-Systems transparent zu regeln, die Rechte der Beschäftigten zu wahren, eine Leistungs- und Verhaltenskontrolle auszuschließen und die Anforderungen des Datenschutzes sowie des Landespersonalvertretungsrechts Baden-Württemberg zu erfüllen.

§1 Geltungsbereich

(1) Diese Dienstvereinbarung gilt für alle Beschäftigten der Universität im Sinne des Landespersonalvertretungsgesetzes Baden-Württemberg (LPVG BW), einschließlich wissenschaftlicher und nichtwissenschaftlicher Beschäftigter, Auszubildender sowie studentischer Hilfskräfte.
(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 Heidelberg gewährt wird, sind auf die Einhaltung der Regelungen dieser Dienstvereinbarung zu verpflichten.
(3) Sie gilt für alle informationstechnischen Endgeräte (Clients) und Server, die durch die Universität betrieben oder administriert werden.

§2 Zweck des Einsatzes

(1) Das EDR-System dient ausschließlich der IT-Sicherheit, insbesondere:

- der Erkennung und Abwehr von Schadsoftware,
- der Identifikation und Analyse von Angriffsmustern,
- der Reaktion auf Sicherheitsvorfälle,
- der Wiederherstellung der Integrität betroffener Systeme.

(2) Eine Leistungs- oder Verhaltenskontrolle von Beschäftigten ist ausdrücklich ausgeschlossen.
(3) Die Nutzung der erhobenen Daten zu disziplinarischen Zwecken ist unzulässig, soweit nicht ein konkreter, dokumentierter Verdacht auf eine auf eine schwerwiegende grobfahrlässige Gefährdung der IT-Sicherheit vorliegt.

§3 Beschreibung des Systems

(1) Das EDR-System wird auf dienstlichen Clients sowie auf Servern installiert. Welche Gerätetypen und in welchen Bereichen der Universität dies ausgerollt wird, wird im Anhang 2 geregelt.
(2) Es erfasst sicherheitsrelevante Systemereignisse, u.a. insbesondere:

- Programm-/Prozessstarts und -beendigungen,
- auffällige Dateioperationen,
- Netzwerkverbindungen bzw. Metainformationen dazu,
- Hinweise auf bekannte Schadsoftware oder verdächtige Verhaltensmuster.

(3) Eine inhaltliche Auswertung von Dateien, Dokumenten, E-Mails, Bildschirminhalten oder Kommunikationsinhalten erfolgt nicht.
(4) Die eingesetzte Software wird im Anhang aufgeführt.
(5) Die Dienstleister werden im Anhang aufgeführt.

§4 Datenverarbeitung und Datenschutz

(1) Die Verarbeitung personenbezogener Daten erfolgt unter Beachtung der Datenschutz-Grundverordnung (DSGVO) sowie des Landesdatenschutzgesetzes Baden-Württemberg.
(2) Es werden nur solche Daten erhoben, die zur Erreichung des in § 2 genannten Zwecks erforderlich sind (Grundsatz der Datenminimierung).
(3) Sicherheitsereignisse werden grundsätzlich systembezogen ausgewertet. Eine personenbezogene Zuordnung erfolgt nur, wenn dies zur Aufklärung eines konkreten IT-Sicherheitsvorfalls zwingend erforderlich ist.
(4) Der Zugriff auf EDR-Daten ist auf einen eng begrenzten, namentlich benannten Personenkreis in der IT-Sicherheitsorganisation beschränkt. Zugriffe werden protokolliert. Der Personenkreis wird im Anhang 2 geregelt.

§5 Beteiligung des Personalrats

(1) Der Personalrat wird vor Einführung oder wesentlichen Änderungen des EDR-Systems oder eines Dienstleisters umfassend informiert und beteiligt.
(2) Ihm werden folgende Unterlagen zur Verfügung gestellt:

- technische Dokumentation,
- Datenschutz- und Sicherheitskonzepte,
- Lösch- und Berechtigungskonzepte.

(3) Der Personalrat kann die Protokolle der Zugriffe einsehen.

§6 Transparenz und Information der Beschäftigten

(1) Die Beschäftigten werden vor Inbetriebnahme und bei wesentlichen Änderungen des Systems in Absprache mit dem Personalrat in geeigneter Weise informiert.

(2) Die Information umfasst insbesondere:

- Zweck und Funktionsweise des Systems,
- Art der erhobenen Daten,
- Speicherdauer,
- Ansprechpartner für Datenschutz- und IT-Sicherheitsfragen.

§7 Ausschluss der Leistungs- und Verhaltenskontrolle

(1) Das EDR-System darf nicht zur Überwachung von Arbeitsleistung oder Arbeitsverhalten eingesetzt werden.
(2) Eine Auswertung personenbezogener Daten zu Leistungs- oder Kontrollzwecken ist unzulässig.
(3) Technische Funktionen, die eine individuelle Leistungsüberwachung ermöglichen, sind – soweit möglich – zu deaktivieren.
(4) Eine Zweckänderung ist nur mit Zustimmung des Personalrats zulässig.

§8 Schlussbestimmungen

(1) Sollten eine oder mehrere Bestimmungen dieser Dienstvereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Regelungen unberührt. Die Vertragsparteien verpflichten sich, die unwirksame Regelung durch eine solche zu ersetzen, die dem angestrebten Zweck sachlich möglichst nahekommt.
(2) Die Dienstvereinbarung kann mit einer Frist von sechs Monaten zum Ende eines Kalenderjahres schriftlich gekündigt werden. Im Falle einer Kündigung gilt sie bis zum Abschluss einer neuen Regelung, längstens jedoch zwölf Monate nach Kündigungsmitteilung, weiterhin fort.
(3) Die Dienststelle und der Personalrat vereinbaren, diese Dienstvereinbarung spätestens zwei Jahre nach Inkrafttreten zu überprüfen und ggf. anzupassen.

Unterzeichnung

Ort, Datum: Heidelberg 31.7.20

Für die Universität Heidelberg:

F. Melchior

Rektorin Prof. Dr. Frauke Melchior

Für den Personalrat:

C. Belle-Fejsa

Vorsitzende Charlotte Belle-Fejsa

Anhang 1 Eingesetzte Software und Dienstleister

Der aktuelle Dienstleister ist die Fa. Bechtle.

Die aktuell eingesetzte Software ist das EDR der Firma Cybereason.

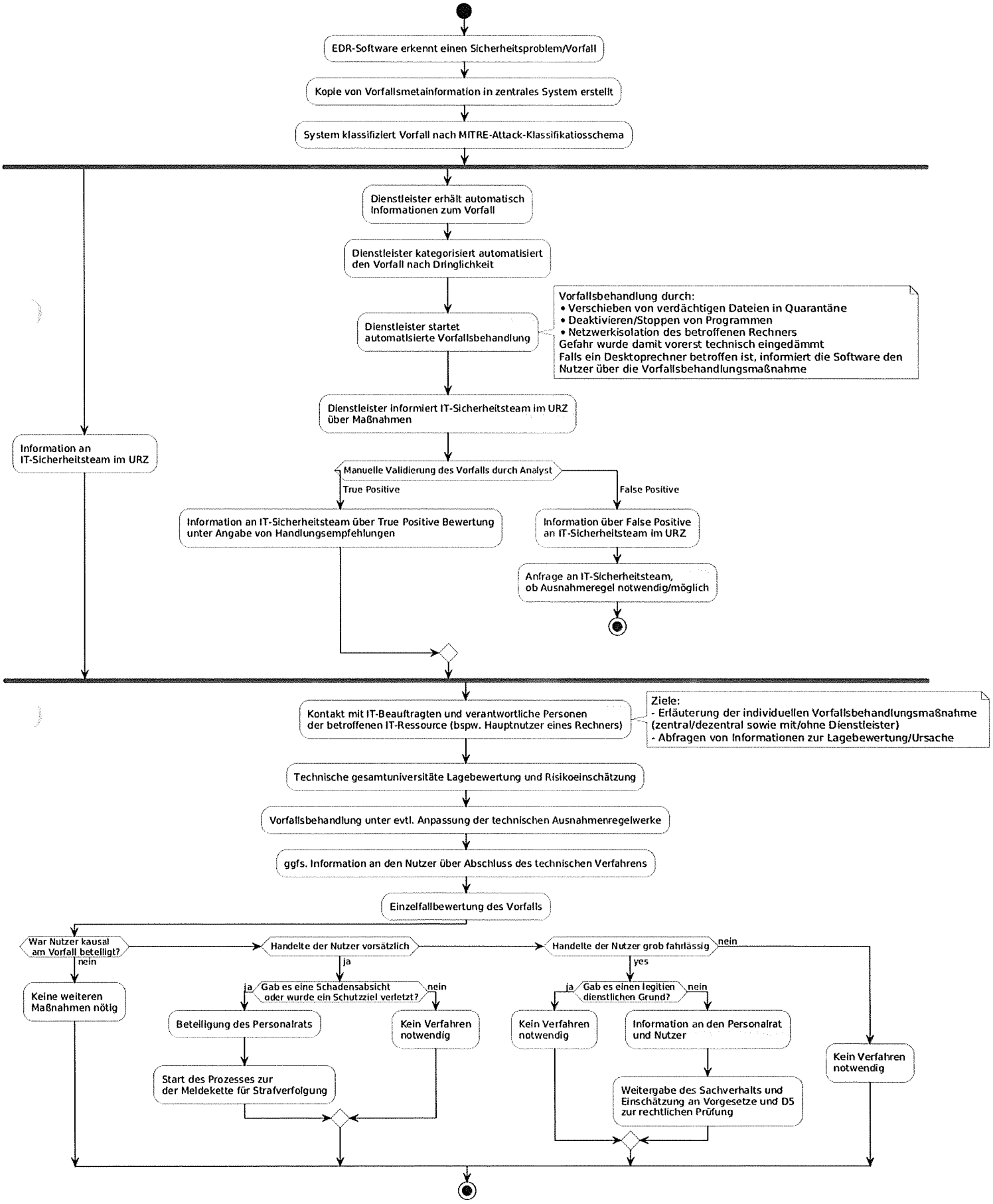
Anhang 2 (nicht öffentlich): Liste der Personen mit Systemzugriff

Die eine namentliche Liste der Personen liegt dem Personalrat vor. Systemzugriff haben drei Personen aus dem Universitätsrechenzentrum sowie mehrere Personen des aktuellen Dienstleisters.

Eine namentliche Liste der URZ-Beschäftigten des EDR-Zugriffssystems wird online tagesaktuell geführt und ist dem Personratrat auf Nachfrage in der jeweils aktuellen Version zur Verfügung zu stellen. Der externe Partner zählt als eine (juristische) Person und ist entsprechend zu vermerken.

Eine Liste der dienstlichen Clients sowie der Servern auf denen das EDR läuft ist tagesaktuell online zu führen und dem Personratrat auf Nachfrage in der jeweils aktuellen Form zur Verfügung zu stellen

Anhang 3: Prozessbeschreibung Vorfallsbehandlung



Anhang 4: Informationen zu Datenkategorien

Das EDR System sammelt Daten zur Bestimmung des Sicherheitszustands des Geräts. Folgende Datenarten werden auf den geschützten Geräten gesammelt:

- Metainformationen zu Dateien (bspw. Dateihash oder -modifikationsdatum)
- Metainformationen zum Netzwerkverkehr (bspw. IP-Adressen und Datenmengen)
- Informationen zum Progammverhalten (bspw. Speicher-/Dateizugriffe, Subroutinenaufrufe, Starten anderer Programme/Skripte)
- Geräteinformationen (u.a. Betriebssystemversion, eingeloggte Usernamen, User-OU im Active-Directory)

Folgende Daten werden nicht gesammelt bzw. sind nicht Bestandteil der Software:

- Dateiinhalte
- Bildschirmaufzeichnungen/Screenshots
- Remote-Desktop Zugriff
- Usertrackingdaten wie bspw. Mausklicks/-Bewegungen oder Tastatureingaben

Anhang 5: Wirkungsbereich

Im Folgenden sind alle Einrichtungen aufgelistet, die aktuell mit dem EDR System aus dieser Dienstvereinbarung versorgt werden:

- Universitätsrechenzentrum
- Universitätsverwaltung und Rektorat