

Zwischen der Universität Kassel, vertreten durch die Präsidentin, und dem Personalrat wird folgende

Regelungsabrede zur Nutzung von Sophos Central Intercept X Advanced XDR

geschlossen:

Präambel

Der Software-Hersteller Sophos Ltd. hat die On-Premise Varianten seines bisherigen Virenscanners sowie der „Sophos Enterprise Console“ zum 20. Juli 2023 abgekündigt. An deren Stelle sollen auch an der Universität Kassel die entsprechenden Nachfolgeprodukte treten. Sophos Central Intercept X Advanced XDR ist eine sog. „Endpoint-Protection-Software“. „Sophos Central“ bezeichnet dabei das einheitliche Benutzer-Interface von Sophos, und „XDR“ steht für „eXtended Detection and Response“ (Erweiterte Erkennung und Reaktion).

§ 1 Zweck der Vereinbarung

Ziel dieser Regelungsabrede ist es, den Funktionsumfang zum Start des Einsatzes von Sophos Central Intercept X Advanced XDR festzulegen, um damit die Persönlichkeitsrechte der Mitarbeitenden zu schützen. Auf dieser Basis erfolgt die weitere Rechtevergabe.

§ 2 Geltungsbereich

- (1) Sophos Central Intercept X Advanced XDR kommt auf allen zentral administrierten Uni-Kassel-Clients (Uni Kassel Client as a Service – UKCaaS) zum Einsatz; die Verteilung der Software erfolgt dabei mit Hilfe der Workspace-Management-Lösung Matrix 42.
- (2) Sofern Sophos Central Intercept X Advanced XDR auf dezentral administrierten Rechnern zum Einsatz kommt, gelten die Vereinbarungen entsprechend.
- (3) Zur Verbesserung der Lesbarkeit wird im Folgenden nur auf Sophos Central Intercept X Advanced XDR Bezug genommen. Sofern Antiviren-Software bzw. Endpoint-Protection-Lösungen mit vergleichbaren Funktionalitäten zum Einsatz kommen, gelten die Vereinbarungen jedoch entsprechend.
- (4) Auf jedem dezentral administrierten Rechner erfolgt die Nutzung von Sophos Central Intercept X Advanced XDR derzeit freiwillig (siehe Entscheidungshilfe). So können die Bediensteten im Rahmen ihrer Dienst- und Sorgfaltspflichten alternativ auch durch die Verwendung anderer gängiger Produkte (z.B. Microsoft Defender) für einen hinlänglichen Schutz vor Schad-Software sorgen.
- (5) Die Einwilligung zur Nutzung von Sophos auf dezentral administrierten Rechnern kann jederzeit widerrufen werden.

§ 3 Rollendefinition

- (1) Auf zentraler Ebene wird ein institutionelles Rollen-/Rechtemanagement geführt.
- (2) Die „Sophos Central Enterprise“ (Unternehmens-)Instanz ist im IT-Servicezentrum den Enterprise (Unternehmens-)Administratoren zugeordnet. Der Informationssicherheitsbeauftragte hat einen Read-Only-(Lese-)Zugriff.
- (3) Den zentralen und dezentralen IT-Administratoren ist für den jeweiligen Bereich / die jeweilige Einrichtung eine „Sophos Central Sub-Estates“-Instanz zugeordnet.
- (4) Weiteren Berechtigten kann je nach bereichsspezifischer Organisation ein Teil der unter Absatz 3 genannten Berechtigungen zugeordnet sein.
- (5) Vorgesetzte sowie stellvertretende Vorgesetzte dürfen (für die ihnen zugeordneten Beschäftigten) keine Administrationsrechte oder Rechte der unter Absatz 3 und 4 genannten Personengruppen für Sophos XDR erhalten.
- (6) Die Beschäftigten können die für sie verantwortlichen IT-Verantwortlichen auf einer internen Website des IT-Servicezentrums (<https://www.uni-kassel.de/its/dienstleistungen/it-arbeitsplatz-management/software/campuslizenzen/anmeldung/sophos-xdr-cybersecurity-campus/sophos-central-administratorinnen>) einsehen.

§ 4 Funktionsumfang

- (1) Die Nutzung der einzelnen Funktionen von Sophos XDR erfolgt in der Startphase auf Basis der als Anlage 1 beigefügten Übersicht. Eine fortlaufende Installationsdokumentation wird geführt.
- (2) Die nicht genutzten Funktionalitäten werden, soweit dies technisch möglich ist, zentral gesperrt oder vom IT-Servicezentrum mit dem Standardwert (Default) „Nein“ belegt. Ein Einschalten der auf diese Weise deaktivierten Funktionalitäten ist untersagt.
- (3) Vor dem Einsatz weiterer Funktionalitäten sind der Personalrat, die Schwerbehindertenvertretung sowie die Frauen- und Gleichstellungsbeauftragte rechtzeitig zu informieren und entsprechend zu beteiligen.

§ 5 Vereinbarungen

- (1) Sophos Central Intercept X Advanced XDR darf nicht zur Verhaltens-, Leistungs- und Anwesenheitskontrolle verwendet werden.
- (2) Die Beschäftigten (Nutzenden) werden in geeigneter Weise über den Anlass der Einführung von Sophos Central Intercept X Advanced XDR und die Funktionalitäten informiert. Darüber hinaus steht ihnen die Information zur Verfügung, wer auf von Sophos Central Intercept X Advanced XDR erhobene und ihnen zuordenbare Daten zugreifen kann.

- (3) Die zentralen und dezentralen IT-Administratorinnen und -Administratoren werden durch die Dienststelle in geeigneter Weise auf einschlägige Erfordernisse des Datenschutzes und der Verschwiegenheit sowie den reglementierten Funktionsumfang hingewiesen.

§ 6 Datenschutz und Verschwiegenheit

- (1) Die datenschutzrechtlichen Regelungen der Universität Kassel sind zu beachten.
- (2) Im Rahmen der Administration von Sophos Central Intercept X Advanced XDR bekanntwerdende personenbezogene Daten oder Nutzungsinformationen dürfen nicht zur Überwachung von Bediensteten verwertet, verwendet oder weitergegeben werden.
- (3) In diesem Zusammenhang wird auch auf die im Rahmen der Einstellung eingegangene einschlägige „Verpflichtung zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO) und dem Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG)“ verwiesen.
- (4) Bei Sophos betreffendem Auskunftsbedarf können sich Nutzer:innen an ihren Sophos-Admin oder ggf. an die behördliche Datenschutzbeauftragte wenden.
- (5) Von Sophos Central Intercept X Advanced XDR automatisch erhobene sicherheitsrelevante auf der Festplatte des Endgeräts gespeicherte Daten werden nach spätestens 90 Tagen automatisch gelöscht. Einige dieser Daten (s. Details unter <https://community.sophos.com/intercept-x-endpoint/edr-data-lake-eap/m/files/9496>) werden in einen sog. „Data Lake“ in der Cloud übertragen und dort nach spätestens 30 Tagen automatisch gelöscht. Aus der automatisierten Analyse dieser Daten ergibt sich ein Überblick über den Zustand aller Geräte (insb. auch, wenn diese wegen eines Angriffs offline geschaltet wurden), darüber hinaus dienen diese Daten dafür, Angriffe frühzeitig zu erkennen und deren KI-gestützte Abwehr durch aktuelle Trainingsdaten laufend zu verbessern.
- (6) Nutzer:innen werden durch ein Pop-Up am Rechner informiert, wenn eine Bedrohung erkannt oder entfernt wurde. Die Information kann in der Sophos-Anwendung abgefragt werden. Bei Fragen zu Sicherheits-Pop-Ups können sich Nutzer:innen an die Sophos-Administration wenden.

§ 7 Schlussbestimmungen

- (1) Diese Regelungsabrede tritt am 19.07.2023 in Kraft.
- (2) Änderungen und Ergänzungen dieser Regelungsabrede bedürfen zu ihrer Wirksamkeit der Schriftform.
- (3) Nach Abschluss der Einführungsphase von Sophos Central Intercept X Advanced XDR findet eine Evaluation statt und die Regelungsabrede wird zeitnah durch eine Dienstvereinbarung abgelöst. Die Erfahrungen im Umgang mit Sicherheitsrisiken und akuten Bedrohungslagen sollen bei der Erstellung der Dienstvereinbarung einbezogen werden. Über gemeldete Sicherheitsvorfälle wird im Rahmen der Evaluation berichtet.

(4) Die Frauen- und Gleichstellungsbeauftragte und die Schwerbehindertenvertretung wurden beteiligt.

Kassel, den 18.07.2023

Die Präsidentin

Der Personalrat

In Vertretung

Gez. im Original

Gez. im Original

Dr. Oliver Fromm
Kanzler

Dr. Dr. Peter Jahn
stellv. Personalratsvorsitzender

Vorläufiger Nutzungsvorschlag für Sophos Central - Intercept X Advanced with XDR an der Universität Kassel

11.07.2023

Als "Sophos Central" wird das einheitliche Benutzer-Interface von Sophos bezeichnet. Darüber haben wir Zugang zu unserem erworbenen Sophos-Produkt "Intercept X Advanced with XDR". Dabei handelt es sich um eine neue Generation der herkömmlichen "AntiViren-Software", für die oft auch die Bezeichnung "EndPointProtection" verwendet wird.

XDR steht dabei für "eXtended Detection and Response" - dieser Namenszusatz gibt etwas Aufschluss über die Funktionen der neuen Generation: **Erweiterte Erkennung und Reaktion**.

Nähere Informationen zu den Grundfunktionen des XDR: <https://doc.sophos.com/central/customer/help/de-de/ManageYourProducts/XDR/index.html>

Features	Gegenwärtig an der UKS zur Verfügung stehender Funktionsumfang	Davon zur Nutzung an der UKS aktuell vom ITS vorgeschlagen	Vom ITS technisch zentral gesperrt	Zentral untersagt und vom ITS als Default gesetzt
ANGRIFFSFLÄCHE				
Web Security	✓	✓		
Download Reputation	✓	✓		
Web Control/Kategoriebasierte URL-Filterung	✓			✗
Peripheriekontrolle	✓			✗
Application Control	✓			✗
VOR AUSFÜHRUNG AUF DEM GERÄT				
Deep-Learning-Malware-Erkennung	✓	✓		
Anti-Malware-Dateiscans	✓	✓		
Live Protection	✓	✓		
Verhaltensanalysen vor Ausführung (HIPS)	✓	✓		
Blockierung potenziell unerwünschter Anwendungen (PUAs)	✓	✓		
Intrusion Prevention System	✓	✓		
STOPPEN VON BEDROHUNGEN BEI AUSFÜHRUNG				
Data Loss Prevention	✓			✗
Laufzeit-Verhaltensanalyse (HIPS)	✓	✓		

Antimalware Scan Interface (AMSI)	✓	✓		
Malicious Traffic Detection (MTD)	✓	✓		
Exploit Prevention	✓	✓		
Active Adversary Mitigations	✓	✓		
Ransomware File Protection (CryptoGuard)	✓	✓		
Disk and Boot Record Protection (WipeGuard)	✓	✓		
Man-in-the-Browser Protection (Safe Browsing)	✓			✗
Enhanced Application Lockdown	✓			✗
ERKENNUNG				
Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)	✓		✗	
SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen) Erkennung und Priorisierung verdächtiger Ereignisse	✓		✗	
Erkennung verdächtiger Ereignisse und Priorisierung	✓	✓		
Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff	✓			✗
Produktübergreifende Datenquellen – z. B. Firewall, E-Mail (Sophos XDR)	✓	✓		
Produktübergreifende Abfragen (Sophos XDR)	✓	✓		
Sophos Data Lake Cloud-Speicher	✓ 30 Tage	✓ 30 Tage		
Geplante Abfragen	✓			✗
ANALYSE				
Bedrohungsfälle (Ursachenanalyse)	✓	✓		
Deep Learning-Malware-Analyse	✓	✓		
Erweiterte Bedrohungsdaten von Sophos X-Ops auf Abruf	✓		✗	
Export forensischer Daten	✓	✓		
BEREINIGUNG				

Automatisierte Malware-Entfernung	✓	✓		
Synchronized Security Heartbeat	✓	✓		
Sophos Clean	✓	✓		
Live Response (Remote-Analyse und -Reaktion)	✓		✗	
On-Demand-Endpoint-Isolation	✓	✓		
Mit einem Klick „Entfernen und blockieren“	✓	✓		
THREAT HUNTING und REAKTION DURCH EXPERTEN				
24/7 indizienbasiertes Threat Hunting	✗			
Security Health Checks	✗			
Datenspeicherung	✗			
Aktivitätsreports	✗			
Angriffserkennung	✗			
Beseitigung von Bedrohungen und ihren Folgen	✗			
Umfassende Reaktion auf Vorfälle: Bedrohungen werden vollständig eliminiert	✗			
Erfordert vollständigen Sophos XDR Agent (Schutz, Erkennung und Reaktion)				
Ursachenanalyse: um ein erneutes Auftreten in Zukunft zu verhindern	✗			
Dedizierter Ansprechpartner	✗			
ZERO TRUST NETWORK ACCESS				
Integrierter ZTNA-Agent	✗			
ZTNA-Zugriffsrichtlinien und -Kontrollen	✗			

Quellen

<https://www.sophos.com/de-de/products/endpoint-antivirus/tech-specs>

<https://doc.sophos.com/central/customer/help/de-de/ManageYourProducts/XDR/index.html>