Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Informatikdienste

Logging Policy "Unified Audit Log von Microsoft 365"

Datum: 22. Februar 2021
Version: 1.0
Autoren: D. Salvati, A. Harder, F. Consani, H. Vögeli & U. Spätig
Ansprechperson: A. Harder
Klassifizierung: nur für internen Gebrauch

Abstract

Diese Policy beschreibt den Rahmen sowie die dazugehörigen flankierenden technischen und organisatorischen Massnahmen, welche die Voraussetzungen für den Betrieb des Unified Audit Log von Microsoft 365 bilden.

Freigaben

Version	Bemerkung	Datum	Freigegeben durch
1.0	Inkraftsetzung ab 1. März 2021	22. Feb 21	Durch ID GL

Involvierte Stellen

Name	Department / Responsibility
Domenico Salvati	GS – Chief Information Security Officer ETH Zürich
Anja Harder	ID – Chief IT Security Officer Informatikdienste
Fabio Consani	ID – IT Procurement & Portfolio
Heiko Vögeli	ID – Mitarbeiter bei IT-Security Center (IT-SeC)
Thomas Richter	ID – Fachbereichsleiter IT-Security Center (IT-SeC)
Stephen Sheridan	ID – Gruppenleiter IT-SeC – Vulnerability Management
Dieter Gut	ID – Qualitätsmanagement
Urs Spätig	ID – Projektmanagement

Inhaltsverzeichnis

1. Ausgangslage

Die Schulleitung hat am 15. Juni 2020 beschlossen, Microsoft 365/Teams für alle ETH Angehörigen freizugeben.

Microsoft 365 führt die Log-Daten aller benutzten Microsoft 365 Cloud-Dienste inkl. Azure Active Directory (AAD) im zentralen Unified Audit Log (UAL) zusammen. Diese Protokollierung von Log-Daten wird von Microsoft in der Cloud gespeichert und der ETH Zürich *temporär* zugänglich gemacht.

Die zur Verfügung gestellte Protokollierung legt einerseits die Basis für das Erkennen von sicherheitsrelevanten Bedrohungen und Vorfällen. Andererseits sollen bei allfällig angeordneten Auswertungen (insbesondere forensische Untersuchungen bei Missbrauch) nachträglich alle diesbezüglich relevanten Transaktionen rekonstruiert und – falls zutreffend – einer oder einem Benutzenden zugeordnet werden können.

Insbesondere das IT-Security Center (IT-SeC) soll einerseits zur Verbesserung der IT-Security mittels proaktiver Bedrohungssuche (Threat Hunting) und andererseits im Verdachtsfall eines Security Incident auf diese Log-Daten zugreifen dürfen, um z. B. die Dynamik eines sicherheitsrelevanten Ereignisses oder bei Verdacht auf Missbrauch nachzuvollziehen. Ohne Unified Audit Log ist das IT-Security Center nur sehr bedingt in der Lage, diese Aufgaben auszuführen und ihr Mandat zu erfüllen.

Das vorliegende Dokument beschreibt den Rahmen sowie die dazugehörigen flankierenden technischen und organisatorischen Schutzmassnahmen, welche die Voraussetzungen für den Betrieb des Unified Audit Log von MS 365 bilden.

1.1. Definitionen

Ein **sicherheitsrelevanter Vorfall** bezeichnet das Resultat einer unerwünschten Entwicklung oder Einwirkung auf ein oder mehrere IT-Systeme, welche zu einem Verlust der Verfügbarkeit, Integrität und/oder Vertraulichkeit von Diensten sowie Informationsbestände führt bzw. führen kann.

Protokollierung (Logging) bezeichnet die Erstellung von manuellen oder automatisierten Aufzeichnungen, welche bestimmte (Benutzer)-Aktivitäten und IT-Systemzustände zu einem gegebenen Zeitpunkt festhalten.

Monitoring ist eine spezifische Nutzungsart der Protokollierung. Sie bezeichnet die Überwachung obiger (Benutzer)-Aktivitäten und IT-Systemzustände mittels spezifischer Auswertungen, Messungen oder Beobachtungen. [Quelle: in Analogie zu https://de.wikipedia.org/wiki/Monitoring]

1.2. Ziel und Zweck

Mit der Protokollierung und Monitoring sollen *primär* sicherheitsrelevante Bedrohungen und Vorfälle festgehalten, erkannt und nachvollzogen werden können.

Des Weiteren sollen *sekundär* mittels Monitorings (potentiell) relevante betrieblicher Vorfälle/Entwicklungen auch Hard- und Softwareprobleme, Ressourcenengpässe zeitnah erkannt bzw. nachvollzogen werden können.

In dieser Policy wird festgehalten, welche Ereigniskategorien von sicherheitsrelevanten wie auch betrieblicher Vorfälle für die Protokollierung relevant sind und wie Protokolldaten zu speichern, zu schützen und «revisionssicher» aufzubewahren sind. Im Dokument **Kommunikation der ID an CISO und ISO-Organisation** (vgl. Anhang A-5) sind die relevanten Ereigniskategorien für sicherheitsrelevante Vorfälle erwähnt. Die Ereigniskategorien relevanter betrieblicher Vorfälle sind in Anhang A-5 aufgeführt.

Dieses Dokument spezifiziert – unter Berücksichtigung der «Weisung Informationssicherheit» sowie der «Benutzungsordnung Informations- und Kommunikationstechnologie (BOT)» – die Grundsätze und Handlungsanweisungen für den bestimmungsgemässen Betrieb des «Unified Audit Logs».

Das Unified Audit Log kommt zum Einsatz:

- bei der Abklärung von auffälligem oder störendem Verhalten von Maschinen
- bei der Behandlung von Reklamationen über das Verhalten einer Maschine oder deren Benutzenden (z. B. bei Missbrauch im Sinne der BOT)
- zur Information über Ergebnisse von Monitoring an die Betroffenen
- als mögliche Grundlage zur Anordnung von Notmassnahmen
- zur Mitteilung von getroffenen individuellen Notmassnahmen bei Cyber-Bedrohungen und -Attacken sowie IT-Sicherheitsproblemen

Im Fall von Missbrauch sollen verantwortliche Personen und/oder missbrauchte Maschinen zeitnah gefunden werden können und die Log-Daten auf Anfrage auch in Zusammenarbeit mit Ermittlungsbehörden verwendet werden können.

Personenbezogene Auswertungen, bei denen es um das **Verhalten von Mitarbeitenden oder Studierenden (Nutzerprofile)** geht, sind prinzipiell nicht zulässig, können aber in begründeten Ausnahmefällen erfolgen (siehe Kapitel 3.1 und Kapitel 3.8).

2. Geltungsbereich

2.1. Geltungsbereich

Diese Logging-Policy gilt für das

- *Off-Premises* «Unified Audit Log» aller Tenants der ETH Zürich bei Microsoft (in der Cloud), die von den Informatikdiensten zentral verwaltet werden und – sofern vorhanden – auch für die entsprechende
- *On-Premises Kopie* bei der ETH Zürich (IT-SeC Log-Container des IT-Security Centers).
- Ebenso gilt diese Logging-Policy für allfällige Leistungserbringer*innen, die die Unified Audit Log Infrastruktur im Auftrag der ETH Zürich betreiben.

Ausnahmen von dieser Logging-Policy sind schriftlich zu begründen, zu befristen und durch den CISO zu bestätigen.

3rd Party Log-Daten (z. B. von Cloud Services) müssen separat geregelt werden (z. B. Vertrag / SLA mit externem Dienstleister).

2.2. Rechtlicher und regulatorischer Hintergrund

Die heutigen Informationstechnologien erlauben es, sämtliche Aktionen eines Nutzenden zu erheben und zu speichern. Damit lässt sich z. B. nachvollziehen, wann und wie lange, welche Seiten besucht oder welche Dokumente angeklickt oder bearbeitet wurden.

Werden keine oder nur ungenügende Massnahmen zur Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit obiger Informationen getroffen, kann dies beispielsweise dazu führen, dass Angreifer*innen auf vertrauliche Informationen zugreifen oder dass, durch manipulierte Protokollierungsdaten, Sicherheitsvorfälle bewusst verschleiert werden können.

Ebenso können Angreifer*innen, wenn sie an eine grössere Menge von Protokollierungsdaten gelangen, diese Informationen nutzen, um die interne Struktur der ETH-Tenants aufzudecken und dadurch ihre Angriffe gezielter ausrichten.

Das Loggen von Daten betrifft somit einen sehr sensiblen Bereich, bei welchem rechtliche und regulatorische Vorgaben einzuhalten sind:

- Das **Bundesgesetz über den Datenschutz (DSG)** dient dazu, personenbezogene Informationen zu schützen. Die vom Unified Audit Log generierten Protokollierungsdaten wie beispielsweise Benutzernamen, IP-Adressen und durchgeführte Aktivitäten können konkreten Personen zugeordnet werden. Alle Log-Daten, die einen direkten oder indirekten Personenbezug haben, unterstehen diesem Bundesgesetz. Unter Umständen können im «Unified Audit Log» auch besonders schützenswerte Personendaten im Sinne des Datenschutzgesetzes anfallen. Es muss verhindert werden, dass sich solche Informationen kopieren, abhören und manipulieren lassen.
- Die **Verordnung des ETH-Rates über das Personal im Bereich der Eidgenössischen Technischen Hochschulen (PVO)** regelt die Arbeitsverhältnisse der Mitarbeiterinnen und Mitarbeiter des ETH-Bereichs.
- Die Weisung **Informationssicherheit an der ETH Zürich** vom 9. April 2018 legt die Informationssicherheitsziele, die Eckwerte für den Umgang mit Risiken fest und regelt die Verantwortlichkeiten für Steuerung und Kontrolle der Ziele und Risiken.
- Die **Benutzungsordnung Informations- und Kommunikationstechnologie (BOT)** gilt sowohl für jede Benutzung und Mitbenutzung aller ETH Zürich-eigenen IKT-Mittel, als auch für nicht ETH Zürich-eigene Systeme, die aber im Datennetzwerk der ETH Zürich betrieben werden, und zwar durch **ETH Zürich-Angehörige** oder **Dritte.**

- Die **ID Security Logging Policy** der Informatikdienste (ID) vom 18. November 2019 befasst sich mit dem IT-sicherheitsbezogenen Log-Management, welches Sicherheitsanalysten des IT-SeC ermöglicht, Informationen zum Zwecke der sicherheitstechnischen sowie der forensischen Analyse zu sammeln, auszuwerten und Risiken für die IT-Infrastruktur der ETH Zürich zu identifizieren oder zu beseitigen.

3. Log-relevante Tätigkeiten und Ereignisse für «Unified Audit Log» von MS 365

3.1. Verwendung für die Sammlung und Auswertung von Log-Daten

Die Sammlung von Logfiles darf ausschliesslich für die Entdeckung und/oder den Nachweis des Missbrauchs von Maschinen durch Unberechtigte durchgeführt werden. Andere Erkenntnisse über die Tätigkeit von Personen aus diesen Daten sind zu vermeiden. Wo sie dennoch entstehen, unterstehen sie der Geheimhaltung (vgl. z. B. das Berufs-, Geschäfts- und Amtsgeheimnis gemäss Art. 57 PVO oder Fernmeldegesetz Art. 7).

Nicht personenbezogene Auswertungen werden zur proaktiven *Abwehr von Bedrohungen* der Infrastruktur (z. B. Threat Hunting, Intrusion Detection), sowie zum Zweck der *Fehlersuche und zum Sicherstellen des ordnungsgemässen Betriebs* durchgeführt. Personenbezogene Auswertungen von Protokolldaten sind ausnahmsweise zulässig, sofern die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel ernsthaft gefährdet sind und dies zur Störungsbehebung unumgänglich ist (z. B. Analyse und Behebung von technischen Störungen gemäss Art. 18 Abs. 3 BOT). Diese (personenbezogenen) Auswertungen erfolgen im Auftrag des/der CISO.

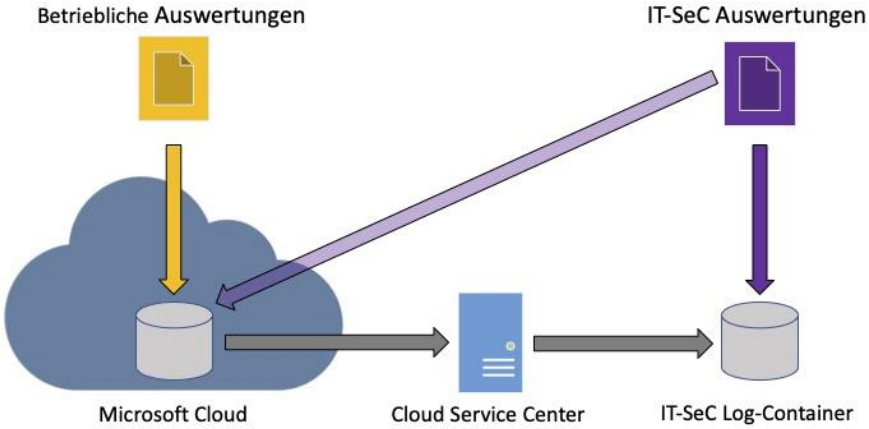
Bei *festgestelltem oder begründetem Verdacht auf Missbrauch* von Informatikmitteln sind nach vorgängiger schriftlicher Information der betroffenen Benutzenden personenbezogene Auswertungen von Protokolldaten (Metadaten) möglich. Dieser Entscheid wird vom/von der CISO in Zusammenarbeit mit dem/der direkten Vorgesetzten sowie dem/der Leiter*in HR bzw. Personalchef*in oder Studiendirektor*in bzw. Rektor*in getroffen[1]. Diese Auswertungen dürfen sich grundsätzlich *nicht auf den Inhalt* elektronisch übermittelter Informationen beziehen bzw. bedürfen der vorgängigen Autorisierung durch der/den CISO (z. B. bei Gewaltdarstellungen, Pornographie, Herstellung, Anleitung zur Herstellung oder absichtliche Verbreitung von schädlichen Programmen, Cyber-Attacken sowie weitere missbräuchliche Nutzung[2]).

Personenbezogene Auswertungen, bei denen es um das *Verhalten von Mitarbeitenden oder Studierenden* (Nutzerprofile) geht, sind nicht zulässig, es sei denn, diese werden von der Leitung der Personalabteilung, dem Rektorat (Stufe Abteilungsleitung) oder der Staatsanwaltschaft angeordnet. Das IT-Security Center oder das Cloud Service Center wird diesbezüglich ausschliesslich im Auftrag der/des CISO tätig. Die Logfiles dürfen nicht zur (automatisierten) Auswertung der Verhaltensweisen von Personen genutzt und nicht mit anderen gesammelten Daten in Verbindung gebracht werden.

[1] vgl. Ziff. 5b Anhang BOT
[2] vgl. Art. 19 BOT

3.2. Anforderungen für die Protokollierung und Auswertung von Log-Daten

Wie bereits erwähnt wird grundsätzlich zwischen einer sicherheitsrelevanten und betrieblichen Verwendung (Auswertung) der Log-Daten unterschieden.



Das Sammeln von Protokolldaten im Unified Audit Log, welches die Log-Daten der diversen Microsoft 365 Cloud-Diensten inkl. AAD zusammenführt, ermöglicht die Auswertung und Korrelation der Log-Einträge von verschiedenen Systemen (Nachvollziehbarkeit von verteilten Aktivitäten).

Deshalb gelten für die Auswertung folgende generelle Anforderungen:

Unified Audit Log in der Microsoft Cloud

Betriebliche Auswertungen erfolgen durch das Cloud Service Center (CSC) der Informatikdienste direkt in der Microsoft Cloud. Die in der Cloud befindlichen Log-Daten dürfen für betriebliche Zwecke maximal 90 Tage lang ausgewertet werden. Diese Daten dürfen nur zum Sicherstellen des ordnungsgemässen Betriebs ausgewertet werden, d.h. es sind nur die in Anhang A5 spezifizierten Auswertungen erlaubt.

Personenbezogene Auswertungen über das Verhalten von Mitarbeitenden oder Studierenden (Nutzerprofile) sind prinzipiell nicht erlaubt.

Der Informationseigner der Log-Daten im Unified Audit Log in der Microsoft Cloud ist das Cloud Service Center (CSC).

Unified Audit Log im IT-SeC Log-Container

Die sich in der Microsoft Cloud befindlichen Daten des Unified Audit Logs werden dem IT-Security Center mittels geeigneter Schnittstelle **als Realtime-Information** und **unverändert** im dafür designierten IT-SeC Log-Container («On-Premises») zugänglich gemacht.

Der Informationseigner der Log-Daten im Unified Audit Log (IT-SeC Log-Container) ist das IT-Security Center.

Weitere Anforderungen

Die Log-Daten in der Microsoft Cloud wie auch im IT-SeC Log-Container des IT-Security Centers sind «vertraulich». Sicherheitsrelevante Auswertungen (inkl. allfällige Auswertungen der Nutzerprofile) gelten als streng vertraulich sofern diese vom/von der Informationseigner*in (= Auftraggeber*in der Auswertung) nicht als «vertraulich» klassifiziert werden.

Um Missbrauch vorzubeugen, muss jeder *Zugriff* auf das Unified Audit Log (unabhängig davon ob dieser in der Microsoft Cloud oder «On-Premises» bei der ETH Zürich ist) *stark eingeschränkt* und *nachvollziehbar* sein. Beigezogene Dritte werden sorgfältig ausgewählt und auf die Wahrung der Vertraulichkeit verpflichtet (Geheimhaltungsvereinbarung).

3.3. Erforderliche Log-Inhalte

Jeder Protokolleintrag muss so viele Informationen enthalten, dass dieser verständlich und dessen Aussagekraft gewährleistet ist. Dies umfasst folgende Elemente:

- Datum- und Zeitstempel
- Ursprung der Log-Daten (Applikations- / Servicename)
- Aktivitäts- / Ereignis- / Fehler-Typ
- Benutzer-ID / IP-Adresse (Quelladresse)
- Ziel der Aktion (Daten, System, Ressource)
- Hinweis, ob die Aktion erfolgreich war oder nicht

Bei der Bestimmung der aufzuzeichnenden Informationen sind die im Anhang A-1 enthaltenen Vorgaben zu verwenden.

3.4. Synchronisation der Systemzeit

Die Zeitsynchronisierung ist insbesondere für die Ereigniskorrelation unterschiedlicher Log-Daten wichtig. Fehlt eine angemessene/korrekte Zeitsynchronisation über alle IT-Systeme,

- können die Protokollierungsdaten möglicherweise nicht miteinander korreliert werden bzw. kann die Korrelation zu fehlerhaften Aussagen führen
- kann die Auswertung erhobener Protokollierungsdaten erschwert werden
- kann die Protokollierung möglicherweise nicht zur Beweissicherung herangezogen werden.

Microsoft 365 und Azure verfügen über Algorithmen zur Korrektur der Uhrzeit und zur Konditionierung der lokalen Uhr zum Synchronisieren mit UTC (Coordinated Universal Time). Sämtliche Aktivitäten werden in UTC protokolliert.

3.5. Zuständigkeiten

Diese Logging-Policy wird durch die/den CITSO ID im Auftrag und in Rücksprache mit dem/die CISO periodisch aktualisiert (alle 2 Jahre). Die/der CITSO ID arbeitet hierbei mit dem Cloud Service Center (Service Owner MS 365) und mit dem IT-Security Center zusammen.

Das Cloud Service Center ist verantwortlich für die Überwachung der Verfügbarkeit, Integrität und Vertraulichkeit der Log-Daten in der Microsoft Cloud und macht mittels geeigneten Schnittstelle(n) diese Log-Daten dem IT-SeC Log-Container des IT-Security Centers zugänglich (ordnungsgemässer Betrieb des API).

Das IT-Security Center ist verantwortlich für die Übernahme dieser Log-Daten und für die Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit der erhaltenen Daten während des gesamten Lebenszyklus. Das IT-Security Center ist verantwortlich für sämtliche sicherheitsrelevanten Auswertungen.

Diese Logging-Policy wird für die Informatikdienste von der ID-Geschäftsleitung in Kraft gesetzt.

3.6. Schutz der Log-Daten

Folgende Schutzmassnahmen gelten im Sinne von Mindestanforderungen und sind sowohl für die Log-Daten in der Microsoft Cloud (Cloud Security Center) wie auch für den IT-SeC Log-Container des IT-Security Centers anzuwenden.

Sicherheitsmassnahmen und Prozeduren für den (physischen und logischen) Schutz der Integrität & Vertraulichkeit:

- Änderungen an der Protokollierung sind revisionssicher zu dokumentieren (vgl. Prüfrecht CISO gemäss Weisung Informationssicherheit).
- Zudem muss verhindert werden, dass
    - Protokolldaten gelöscht oder geändert werden (bzw. dass das Log abgeschaltet wird)
    - bei der «On-Premises» Lösung soll die Speicherkapazität für Protokolldaten nicht überschritten werden und dadurch die ältesten Einträge überschrieben werden. Die Speicherkapazität ist derart auszulegen, dass die Daten mindestens ein Jahr lang «On-Premises» gespeichert werden können
- Sofern nicht anders vermerkt, gelten die Log-Daten als «vertraulich» und weisen einen hohen Schutzbedarf bzgl. Integrität (Nachvollziehbarkeit) sowie einen normalen Schutzbedarf bzgl. Verfügbarkeit auf (vgl. Weisung Informationssicherheit Art. 23).
- Es muss sichergestellt werden, dass Log-Einträge vollständig und unverfälscht sind, dass die zeitliche Reihenfolge der Einträge korrekt ist und der Zugriffsschutz erfüllt ist.
- Log-Einträge mit Personendaten oder anderen schützenswerten Informationen müssen mit restriktiven Zugriffsberechtigungen geschützt abgelegt werden.

- Sicherheitsrelevante, personenbezogene Auswertungen gelten als streng vertraulich sofern diese vom/von der Informationseigner*in (= Auftraggeber*in der Auswertungen) nicht als «vertraulich» klassifiziert werden.

Sicherheitsmassnahmen und Prozeduren für den Schutz der Verfügbarkeit:

- Schutzmassnahmen, welche die Verfügbarkeit gewährleisten («normaler Schutzbedarf» bzgl. der Verfügbarkeit, vgl. Weisung Informationssicherheit Art. 23)
- Es ist die minimale Zeitspanne zu definieren, während welcher die Logs ohne Verlust von Informationen (z. B. durch Überschreiben) zu speichern sind.
- Bei der «On-Premises» Lösung muss das Unified Audit Log von MS 365 redundant ausgelegt werden und darf keinen Single Point of Failure beinhalten.

3.7. Autorisierter Zugriff auf das «Unified Audit Log von MS 365»

Da über das Unified Audit Log auch eine gezielte Auswertung von Nutzerprofilen (User Profiling) möglich wäre, ist für interne ETH-Mitarbeitende der Zugang mittels Multi-Faktor-Authentication (MFA) und Privileged Identity Management (PIM) abzusichern.

Unified Audit Log im IT-SeC Log-Container

Der Zugriff auf den IT-SeC Log-Container wird für Mitarbeitende des IT-Security Centers eingeschränkt. Gemäss Least-Privilege Ansatz ist für das IT-Security Center eine Custom Exchange Online Gruppe mit ‘View-Only Audit Logs’ Berechtigungen nötig.

Unified Audit Log in der Microsoft Cloud

Der Zugriff auf das Unified Audit Log in der Microsoft Cloud wird auf *ETH-Mitarbeitende* mit Administrationsrollen im Azure/M365 Umfeld beschränkt. Die/der CITSO ID entscheidet über den Mechanismus wie zusätzliche privilegierte Berechtigungen vergeben werden dürfen. Diese sind periodisch zu überprüfen (jährlich oder ad hoc). Die Entscheide sind in nachvollziehbarer Weise revisionssicher zu dokumentieren und können vom CISO geprüft werden. Es handelt sich insbesondere um folgende Rollen:

- Global Admins (technischer Zugriff auf API und globalem Scope)
- Global Readers (technischer Zugriff auf API und globalem Scope)
- Organization Management Role in Exchange Online (technischer Zugriff auf API)

Bezüglich des Zugriffes von ihren *Mitarbeitenden* zeigt *Microsoft* auf, mit welchen Mitteln die Zugriffe auf die ETH Tenants erfolgen und aufgezeichnet werden (insbesondere Customer Lockbox). Sie räumt der ETH Zürich das Recht ein, das Vorhandensein und die Wirksamkeit dieser Mittel zu prüfen, prüfen zu lassen oder Nachweise dazu einzufordern. Die/der CITSO ID entscheidet über die Regeln, wie und ob Zugriffe für Microsoft-Mitarbeitende freigegeben werden.

3.8. Meldung eines Verdachtsfalls und Auswertung von Log-Daten

Bei Verdacht auf operationelle Einschränkung/Verfügbarkeit von IT-Infrastruktur/Dienste (Sicherstellung des ordnungsgemässen Betriebs)

Die Sammlung von Log-Daten zur Sicherstellung des ordnungsgemässen Betriebs wird von der Geschäftsleitung der Informatikdienste freigegeben (durch Inkraftsetzung dieser Weisung).

Als Ausgangspunkt für die (automatische) Auswertung von Log-Daten gilt die Abklärung

- von auffälligem oder störendem Verhalten von Maschinen oder
- von gemeldeten (störendem) Verhalten einer Maschine oder von Benutzenden

Hierfür ist keine Bewilligung notwendig sofern keine personenbezogenen Auswertungen aufgrund von festgestelltem oder konkretem Verdacht auf Missbrauch vorgenommen werden (vgl. Art. 18 Abs. 3 BOT). Bei allfällig festgestellten Missbräuchen oder bei entsprechendem Verdacht teilen dies Systemverantwortliche umgehend der/dem CITSO ID sowie der/dem CISO mit (in Analogie zu Ziff. 3.3 Anhang BOT). Für weiterführende personenbasierte Abklärungen ist die Zustimmung der/des CISO erforderlich.

Bei Verdacht auf Missbrauch von IT-Infrastruktur/Dienste (sicherheitsrelevante Vorfälle)

Die Sammlung von Log-Daten mit Bezug zu sicherheitsrelevanten Vorfällen wird von der/dem CITSO ID im Auftrag der/des CISO freigegeben. Die Durchführung der Sammlung sowie das Monitoring und Auswertung sicherheitsrelevanter Vorfälle obliegt dem IT-Security Center und darf ausschliesslich für die Bedrohungssuche, die Aufklärung von Anomalien sowie die Entdeckung und/oder den Nachweis des Missbrauchs von Maschinen durch Personen oder Programme durchgeführt werden. Die inhaltliche Analyse der Log-Daten muss durch den CISO genehmigt werden (in Analogie zu Art. 18 Abs. 3 BOT).

Als Ausgangspunkt für die (automatische) Auswertung von Log-Daten gilt die Meldung eines Verdachtsfalls auf Zugangs- oder Datenmissbrauch seitens

- der Dateninhaber*in/Team
- Operations
- IT-Security Center (z. B., wenn sich ein Verdachtsfall anhand anderer Datenquellen erhärtet)
- oder seitens einer ETH-externen Quelle.

Der Verdacht ist umgehend der/dem CITSO ID und der/dem CISO zu melden (in Analogie zu Ziff. 3.3 Anhang BOT). Die/der CISO entscheidet aufgrund Ziff. 2.5 Anhang BOT über die Durchführung von Stichproben. Gemäss Ziff. 5 Abs. 1 Bst. a Anhang BOT entscheidet die/der CISO über die personenbezogene Auswertung sofort oder erst nach wiederholter Feststellung eines Missbrauchs.

Das IT-Security Center versucht bei vorliegenden Verdachtsmomenten anhand der 6 Ws des Incident Response Prozesses (Wer, Wann, Was, Wo, Wie, Warum), eine Timeline über die ausgeführten Aktionen zu erstellen, um eine Einschätzung zu erhalten, ob es sich um einen Missbrauch im Sinne der BOT handelt (vgl. Art. 19). Die Ergebnisse werden der/dem CISO weitergeleitet und entsprechend validiert.

Die/der CISO entscheidet bei nach einer nicht personenbezogenen Auswertung von Aufzeichnungen festgestellten *Missbräuchen* im Sinne von Art. 19 BOT oder beim Vorliegen eines konkreten Verdachts auf solche Missbräuche nach bestimmten Grundsätzen (vgl. Ziffer 5 Anhang BOT) über die weiteren Schritte, insbesondere

- über die personenbezogene Auswertung von aufgezeichneten Daten.
- Im Falle dringender akuter Bedrohungslagen oder Angriffen mit grossem Risiko für die Informationssicherheit der ETH Zürich ordnet die/der CISO gemäss Art. 5 Abs. 5f. der Weisung Informationssicherheit Sofortmassnahmen an (insb. Sperrung des Zugangs von IKT-Mitteln, Blockierung von Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken).
- Die erwähnten Sofortmassnahmen können in dringenden Fällen auch von der/dem CITSO ID angeordnet werden, wobei die/der CISO umgehend zu informieren ist und über die Aufrechterhaltung der getroffenen Massnahmen entscheidet (vgl. Ziffer 4 Anhang BOT).

Auswertung von Nutzerprofilen (Profiling)

Es ist verboten, andere Erkenntnisse aus diesen Daten über die Tätigkeit von Personen zu gewinnen, (insbesondere für das Profiling von Verhalten von Benutzenden). Wo sie dennoch entstehen und unterstehen der Geheimhaltung (vgl. z. B. das Berufs-, Geschäfts- und Amtsgeheimnis gemäss Art. 57 PVO oder Fernmeldegesetz Art. 7). Das IT-Security Center oder das Cloud Service Center wird diesbezüglich ausschliesslich im Auftrag der/des CISO tätig.

3.9. Aufbewahrung, Fristen und Datenlöschung

Die Aufbewahrung von Protokolldaten, insbesondere im IT-SeC Log-Container, stellt sicher, dass Ereignisse oder Aktivitäten über einen längeren Zeitraum analysiert werden können.

Die ETH regelt in der Benutzungsordnung Informations- und Kommunikationstechnologie der ETH Zürich (BOT) den Umgang mit IKT-Mitteln. Im Anhang der BOT ist auch das Aufzeichnen und die Nutzung von Logdaten geregelt (6. Abschnitt). Die im Anhang unter Punkt 1 erwähnten Vorgaben zur Aufzeichnung, Aufbewahrung und Vernichtung von Daten, insbesondere die Aufbewahrungsfrist für Daten gemäss Abs. 2 Bst. b von zwei Jahren, sind einzuhalten.

Die Aufbewahrungsfrist der protokollierten Aktivitäten in der Microsoft Cloud ist Lizenz-abhängig pro Benutzenden geregelt:

Lizenz	**Aufbewahrungsfrist**
A5	365 Tage
Non-A5 (z. B. A3 oder A1)	90 Tage

Im ETH-Kontext wird eine Grosszahl der Studierenden und Mitarbeitenden mit einer A5 Lizenz ausgerüstet. Nur Mitarbeitende bzw. Studierende mit einem Dienstverhältnis «im Auftrag», «externe Mitarbeitende» oder «externe Mitarbeitende mit Entschädigung» (Dienstverhältnis 87-89,

90-93 bzw. 95 und 96) oder sog. ETH-Gäste werden mit einer A1 Lizenz bestückt. Diese berechtigt zu einem Online Zugang, hat jedoch Anrecht für eine Installation der Office-Anwendungen auf dem Rechner.

Die oben erwähnten Fristen sind für die Aufbewahrung in der Microsoft Cloud gültig. Diese sind vorgegeben und können nicht geändert oder angepasst werden. Die Daten werden über die ganze Zeitspanne gleich aufbewahrt. Es gibt keine Archivierung. Nach der oben erwähnten Aufbewahrungsfrist werden die Daten gelöscht. Eine vorzeitige Löschung der Daten ist (auch im Einzelfall) nicht vorgesehen/möglich. Es ist auch nicht möglich, das Aufzeichnen von Aktivitäten von Benutzenden und Administrator*innen pro Cloud-Dienst (z. B. Microsoft Teams) individuell ein- oder auszuschalten.

Die «Unified Audit Log M365» Daten werden dem IT-Security Center mittels geeigneter Schnittstelle im dafür designierten IT-SeC Log-Container («On-Premises») zugänglich gemacht (vgl. Kapitel 3.2).

Alle Log-Daten, die einen direkten oder indirekten Personenbezug haben, unterstehen dem Datenschutzgesetz. Logs müssen unwiderruflich gelöscht werden, wenn ihre Aufbewahrungszeit verstrichen ist. Wenn für die Vernichtung angegeben, müssen alle ursprünglichen Sicherungen und Kopien von Logs ebenfalls unwiderruflich gelöscht werden.

4. Compliance mit der Logging-Policy «Unified Audit Log MS 365»

Aller involvierten Personen haben den hier beschriebenen Regeln Folge zu leisten.

Die Logdaten dürfen nur für die erlaubten Zwecke (vgl. Kapitel 3.1) ausgewertet werden. Diese sind:

4.1. Prüfungen der Compliance

Die Einhaltung der hier beschriebenen Regelungen kann unangekündigt durch den/die CISO oder im Auftrag vom CISO beim Cloud Service Center (Service Owner M365) und beim IT-Security Center überprüft werden. Dies umfasst i.d.R. stichprobenartige Kontrollen, ob Log-Daten zu bestimmten Diensten vorhanden sind und welche Auswertung in einem Zeitraum vorgenommen wurden.

4.2. «Exception Handling»

Ausnahmen, warum ein Dienst (oder für einzelne Nutzende) keine Logdaten erfasst und sendet, sind schriftlich bei dem/der CISO zu beantragen und zu begründen.

4.3. Non-Compliance bzw. Konsequenzen bei missbräuchlicher Nutzung

Die meisten Verstösse resultieren erfahrungsgemäss aus Unkenntnis der vorliegenden Logging-Policy oder technischer Unzulänglichkeit. In solchen Fällen ist es ausreichend, wenn die/der Verursacher*in über den Verstoss aufgeklärt wird und die Umsetzung zeitnah erfolgt.

Wird eine missbräuchliche Auswertung der Log-Daten festgestellt, so kann die/der CISO entsprechende Massnahmen und Sanktionen anordnen, wie etwa die vorsorgliche Sperrung des Zugangs zu den Log-Servern und die Blockierung/Sicherung der Daten zu Beweiszwecken (vgl. Art. 20 BOT).

Leichte Verstösse werden durch die/den CISO abgemahnt (Art. 20 Abs a BOT). Die/der CISO leitet Fälle von schwerem Missbrauch an die Rechtsabteilung / HR / Rektorat oder der Verwaltungsdirektion zur weiteren Behandlung und Entscheidung weiter (vgl. Art. 19, Art. 20 und Art. 20^{bis} BOT).

Die Kenntnis schwerer oder wiederholter missbräuchlicher Nutzung verpflichtet die direkten Vorgesetzten das IT-Security Center der Informatikdienste, sowie die System- bzw. Netzwerkzonenverantwortlichen zur Meldung an die/den CISO (Art. 19 Abs. 4 BOT / Stand 1. April 2019).

5. Inkraftsetzung

Diese Policy wurde per 1. März 2021 durch die Geschäftsleitung der Informatikdienste in Kraft gesetzt.

Anhang

A-1: Funktionsumfang / Log-Umfang geloggte Dienste

Alle Informationen, die zu sicherheitsrelevanten Ereignissen und Aktivitäten auf einem IT-System anfallen, sind entsprechend zu protokollieren. Das zentrale Auditing protokolliert folgende Aktivitäten:

- Aktivitäten von Benutzenden in SharePoint Online und OneDrive for Business
- Aktivitäten von Benutzenden in Exchange Online (Postfachüberwachungsprotokollierung)
- Aktivitäten von Administrator*innen in SharePoint Online
- Aktivitäten von Administrator*innen in Azure Active Directory (dem Verzeichnisdienst für Office 365)
- Aktivitäten von Administrator*innen in Exchange Online (Exchange-Administratorüberwachungsprotokollierung)
- eDiscovery-Aktivitäten im Security und Compliance Center
- Aktivitäten von Benutzer*innen und Administrator*innen in Power BI
- Aktivitäten von Benutzer*innen und Administrator*innen in Microsoft Teams
- Aktivitäten von Benutzer*innen und Administrator*innen in Dynamics 365
- Aktivitäten von Benutzer*innen und Administrator*innen in Yammer
- Aktivitäten von Benutzer*innen und Administrator*innen in Microsoft Power Automate
- Aktivitäten von Benutzer*innen und Administrator*innen in Microsoft Stream
- Aktivitäten von Benutzer*innen und Administrator*innen in Microsoft Workplace Analytics
- Aktivitäten von Benutzer*innen und Administrator*innen in Microsoft Power Apps
- Aktivitäten von Benutzer*innen und Administrator*innen in Microsoft Forms
- Aktivitäten von Benutzer*innen und Administrator*innen für Vertraulichkeitsbezeichnungen für Websites, die SharePoint Online oder Microsoft Teams verwenden

Diese Dienst-spezifischen Aktivitätsprotokollierungen werden auch fortlaufend erweitert und verfeinert [Quelle: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide].

Abgrenzung (nicht im Log-Umfang). Es gilt zu beachten, dass die ETH Zürich seine Exchange-Infrastruktur in eigenen Rechenzentren im sogenannten Hybrid-Modus betreibt. Die obenerwähnten Auditing-Aktivitäten für Exchange Online werden daher nicht benutzt. Ebenso sind weitere Dienste aktuell deaktiviert – es sind dies Dynamics 365, Yammer, Power Automate, Workplace Analytics und Power Apps. Für diese Cloud-Dienste werden demzufolge auch keine Logs erzeugt.

Je nach Datenquelle / Cloud Dienst / Ereignis dauert es zwischen 30 Minuten und 24 Stunden bis das protokollierte Ereignis im zentralen Auditing angezeigt wird.

A-2: Ereigniskategorien für Logauswertungen im Rahmen des Betriebs von IT-Systemen und Applikationen

Logauswertungen im Rahmen des Betriebs von IT-Systemen und Applikationen sind Auswertungen und Analysen von Log-Daten, die lediglich zur Sicherstellung eines stabilen Betriebes oder zur Analyse von Störungen gemacht werden. Ziel solcher Auswertungen ist es, frühzeitig mögliche Engpässe der technischen Ressourcen resp. Ausfälle eines IT Services zu erkennen, um Massnahmen für einen unterbruchfreien Betrieb einleiten zu können (proaktive Auswertungen), resp. die Ursachen von Störungen zu finden und zu beheben (reaktive Auswertungen).

Dazu gehören z. B:

Zugriffsberechtigung auf Ressourcen.
Prüfen ob Nutzende (User) über die notwendigen Berechtigungen für den entsprechenden Service oder die entsprechende Aktivität verfügen.

- **Zugriffsberechtigung auf Ressourcen**. Prüfen, ob Nutzende (User) über die notwendigen Berechtigungen für den entsprechenden Service oder die entsprechende Aktivität verfügen.
- **Verfügbarkeit der Ressourcen**
  - Überwachung technischer Indikatoren (Netzwerk, Memory, CPU, Speicher) zur Sicherstellung der Verfügbarkeit.
  - Rekonstruktion von Ursachen zur Behebung von Problemen der Verfügbarkeit und/oder Funktionalität.
- **Sicherstellung der vereinbarten Performance.** Überwachung vereinbarter Performanceindikatoren.
- **Sicherstellung einer korrekten Kostenweiterverrechnung.** Quantitative Auswertung der Nutzung von Ressourcen hinsichtlich Kosten- oder anderer «Dächer» (z. B. maximaler Speicher, etc.).

Explizit nicht zu Logauswertungen im Rahmen des Betriebs von IT-Systemen und Applikationen zählen Auswertungen, Analysen und Korrelation verschiedener Log-Daten zum Zweck der Analyse des Verhaltens der Nutzenden.

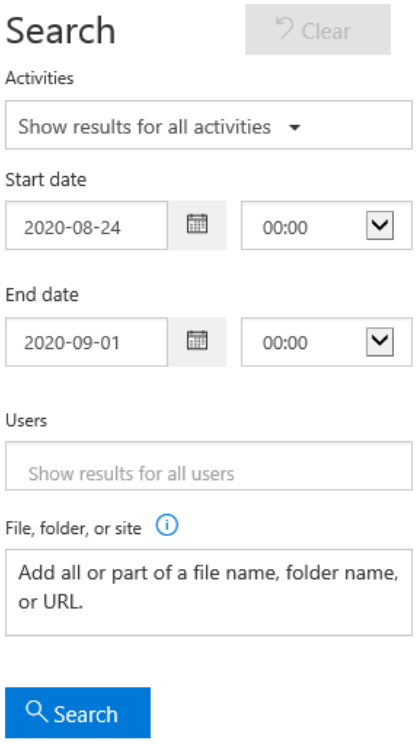
Dazu gehören z. B:

- **Support bei Datenverlust, -manipulation und -wiederherstellung**
  - Einsicht in Zugriffs- und Anmeldeprotokolle
  - Überwachung der Rechteverwaltung
  - Auditieren von nicht den Richtlinien entsprechenden Ereignissen bei der Manipulation von Daten (Bulk-Aktionen, ungewöhnliche Aktionen wie automatisierte Verschlüsselungen, usw.)

- **Sicherstellung der finanz-, lizenz- und exportrechtlichen Compliance**
  - Auditieren der Nutzung von Applikationen und/oder Software
  - Auswertung der Nutzungsmuster von Applikationen/Software
- **Berechtigungsverwaltung**
  - Sicherstellung der Einhaltung des Life Cycles von Identitäten
  - Auditieren/Monitoren/Beurteilen von Veränderungen in der Berechtigungsstruktur

A-3: Filter Funktionalität

Mittels Filterfunktionen kann das zentrale Auditing im Verdachtsfall gezielt nach Zeitraum, Benutzername, durchgeführten Aktionen und/oder Filenamen durchsucht und analysiert werden.



Alternativ kann das zentrale Auditing auch über eine API-Schnittstelle abgefragt bzw. exportiert werden.

A-4: Glossar

Term	Bedeutung
AAD	Azure Active Directory (AAD oder auch Azure AD) ist ein Dienst zur Verwaltung von Identitäten und Zugriffsrechten in der Microsoft Cloud. Azure AD ist mit On-Premises Active Directory der ETH verbunden. Über eine Synchronisation sind die beiden Verzeichnisse verbunden (dabei ist das On-Premises AD das führende System). AAD ist sowohl für Cloud-Dienste wie Microsoft 365 (Office 365) als auch für externe SaaS-Anwendungen und Ressourcen nutzbar.
API	Application Programming Interface (API) bezeichnet eine Programmierschnittstelle und dient dazu, Informationen zwischen einer Anwendung und einzelnen Programmteilen standardisiert auszutauschen.
CISO	Chief Information Security Officer der ETH
CITSO ID	Chief IT-Security Officer der Informatikdienste
IT-SeC	IT-Security Center (Informatikdienste)
Logging	Definieren, Empfangen, Auswerten, Speichern und Löschen von System- und Applikationsrelevanten Prozessen. (dt. Protokollieren) [Quelle: https://de.wikipedia.org/wiki/Logging, abgerufen am 3.02.2021]
Log-Daten Protokoll	"Bei der Datenverarbeitung werden Log-Daten aufgezeichnet, die entweder Ereignisse festhalten, die in einem Betriebssystem oder anderen Softwareausführungen auftreten, oder Nachrichten zwischen verschiedenen Benutzern einer Kommunikationssoftware." [Quelle: in Analogie zu https://de.wikipedia.org/wiki/Logdatei, abgerufen am 3.02.2021]
MFA	Die Multi-Faktor-Authentifizierung (MFA), auch Multifaktor-Authentisierung, ist eine Verallgemeinerung der Zwei-Faktor-Authentisierung, bei der die Zugangsberechtigung durch mehrere unabhängige Merkmale (Faktoren) überprüft wird. [Quelle: https://de.wikipedia.org/wiki/Multi-Faktor-Authentisierung, abgerufen am 3.02.2021]
PIM	Privileged Identity Management (PIM) basiert auf dem Konzept, wonach Benutzende nur die für ihre jeweiligen Aufgaben erforderliche Mindestzugriffsebene erhalten. Dies ist zeitlich beschränkt und kann mit einem Genehmigungsprozess verbunden sein. Mit der Durchsetzung des Least-Privilege-Prinzips, können Unternehmen ihre Angriffsfläche verringern und die Gefahr kostspieliger Datenschutzverletzungen durch böswillige Insider*innen oder externe Cyber-Angriffe senken.
UTC	UTC / Weltzeit Coordinated Universal Time - ist die heute gültige Weltzeit, die eine weltweit gleiche Zeitangabe herstellt. [Quelle: https://de.wikipedia.org/wiki/Koordinierte_Weltzeit, abgerufen am 3.02.2021]

A-5: Links

	Link	Datum
Benutzungsordnung für Informations- und Kommunikationstechnologie an der ETH Zürich (BOT)	https://rechtssammlung.sp.ethz.ch/Dokumente/203.21.pdf	01.04.2019
Weisung Informationssicherheit an der ETH Zürich	https://rechtssammlung.sp.ethz.ch/Dokumente/203.25.pdf	09.04.2018
Bundesgesetz über den Datenschutz (DSG)	https://www.admin.ch/opc/de/classified-compilation/19920153/index.html	01.03.2019
ID Security Logging Policy	https://sherlock.sp.ethz.ch/221b/policies/Shared Documents/ID Security Logging Policy.docx?d=w292bd66344644e72b7f80580a355e425	18.11.2019
Liste “Kommunikation der ID an CISO und ISO-Organisation”	https://sherlock.sp.ethz.ch/spaces/ITSECID/CITSO/_layouts/15/WopiFrame2.aspx?sourcedoc={8BD07B8B-307E-4C3B-9206-B0A442CE2009}&file=IT-Sicherheit_Kommunikation%20ID%20an%20CISO%20und%20ISOs.docx&action=default	26.11.2019