Arbeitsrichtlinie Protokollierung und Überwachung

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Protokollierung und Überwachung
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	30.11.2020
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
20.0	30.11.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0.	Daniel Fürdauer
21.0	17.11.2021	In Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0: Kapitel 4.8: Ergänzung zu Aufbewahrungsfristen	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. EINLEITUNG

Unter Protokollierung wird die Dokumentation von Ereignissen und Benutzeraktivitäten verstanden. Die dokumentierten Aktionen und Ereignisse werden im Folgenden Protokolldaten oder kurz Protokolle genannt. Die Protokollierung wird zur Identifizierung von Unregelmäßigkeiten und zur Gewährleistung der Nachvollziehbarkeit erfolgter Aktionen und Ereignisse innerhalb des IT-Betriebs eingesetzt. Ferner dient die Protokollierung dazu, die Einhaltung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der verarbeiteten Daten und Informationen zu überwachen.

2. GELTUNGSBEREICH

Diese Richtlinie gilt 3 Monate nach dem jeweiligen Änderungsdatum (siehe „Dokumentenhistorie“), frühestens jedoch 2 Jahre nach erstmaliger Freigabe (siehe „Dokumenteneigenschaften“).

3. ABGRENZUNG

Die Vorgaben gelten für die Protokollierung aller IT-Systeme sowie der damit zusammenhängenden Anwendungen, Dienste und Komponenten, sofern diese einen sicherheitsrelevanten Mehrwert bieten. Eine Auflistung, welche Ereignisse sicherheitsrelevant sind, ist im Anhang enthalten. Aktive Netzwerkkomponenten sind gleichermaßen zu behandeln wie alle sonstigen IT-Systeme.
Nicht Bestandteil der Vorgaben ist die Überwachung der Systemzustände von eingesetzten Hardwarekomponenten, die Einhaltung von SLAs und die Protokollierung von fachlichen Prozessen und deren spezifischen Inhalte auf Ebene von IT-Systemen.

4. VORGABEN ZUR PROTOKOLLIERUNG

Im Folgenden sind die allgemeinen Vorgaben beschrieben, die bei beim Umgang mit Protokollen einzuhalten sind.

4.1. Zweckbindung

Protokolle dürfen ausschließlich für dokumentierte Zwecke erzeugt, gespeichert und ausgewertet werden (Zweckbindungsgrundsatz). Hierzu zählt u.a. die forensische Untersuchung von sicherheitsrelevanten Vorfällen, Warnungen, Fehlern und Alarmen. Sofern bei der Erhebung von Protokolldateien personenbezogene Daten (zum Beispiel Benutzerkonten oder IP-Adressen) erfasst werden, ist diese Erhebung im Vorfeld mit dem **Datenschutzbeauftragten** abzustimmen. Die Regelungen der Betriebsvereinbarungen sind zu beachten.

4.2. Einheitliche Systemzeit

Aufgrund des Einsatzes mehrerer IT-Systeme und der komponentenübergreifenden Auswertung der Protokolldateien ist es notwendig, dass alle Systeme über dieselbe Systemzeit verfügen.
Zu jedem Protokolleintrag sind daher das exakte Datum und die Uhrzeit zu dokumentieren. Datum und Uhrzeit sind in einem einheitlichen Format zu erfassen und zwischen den Systemen soweit möglich und angemessen synchron zu halten. Die Systemzeiten sind periodisch zu aktualisieren.

Systemzeiten sind soweit möglich und angemessen durch eine zentrale Referenzzeitquelle zu beziehen.
Es muss sichergestellt sein, dass die Funktionalität und Integrität des zentralen Referenzzeitquellenservers gewährleistet ist und regelmäßig überprüft wird.
Die Einrichtung einer einheitlichen Systemzeit obliegt der IT.

4.3. Zentrales Protokollierungssystem

Ziel der zentralen Protokollierung ist es, wesentliche sicherheitsrelevante Veränderungen an IT-Systemen nachvollziehen zu können.
So lassen sich die zu protokollierenden sicherheitsrelevanten Ereignisse zentral filtern und auswerten. Dies bietet u. a. den Vorteil, dass Sicherheitsprobleme und Angriffe auf verschiedene IT-Systeme in Zusammenhang gebracht und effektiver behandelt werden können.
Das zentrale Protokollierungssystem muss innerhalb des internen Netzes platziert und betrieben werden. Das System muss zugriffsgeschützt sein.
Es muss sichergestellt sein, dass die Erreichbarkeit des Protokollierungssystems durch die Produktivsysteme gewährleistet ist. Unter Umständen sind dazu entsprechende Regelsätze auf dem Sicherheitsgateway (Firewall) anzupassen. Anpassungen von Regelsätzen auf den Sicherheitsgateways sollten dabei nach Möglichkeit mit dem Whitelisting-Verfahren erfolgen.
Aufgrund der zentralen Erreichbarkeit und Zugänglichkeit des Protokollierungssystems durch die Produktivsysteme darf auf dem Protokollierungssystem kein sonstiger zentraler Dienst betrieben werden, der insbesondere für die Unterstützung kritischer Geschäftsprozesse oder für die Verarbeitung von Informationen mit erhöhtem Schutzbedarf genutzt wird.
Die Einrichtung eines zentralen Protokollierungssystems gemäß den Vorgaben dieser Richtlinie obliegt dem Verantwortlichen des Protokollierungssystems. Die Zulieferung, der zu protokollierenden Daten, hat durch den jeweiligen Produktverantwortlichen zu erfolgen.
Eine ausschließlich dezentrale Protokollierung und Überwachung kommt für nicht-sicherheitsrelevante Daten in Betracht.

4.4. Schutz von Protokolldateien

Alle Protokolldaten sind sicher aufzubewahren und vor unbefugtem Zugriff und Manipulation zu schützen.
Der Schutz der dezentralen Protokolldaten auf den Quellsystemen obliegt dem jeweils zuständigen Produktverantwortlichen. Der Verantwortliche des Protokollierungssystems hat den Schutz der Protokolldaten am zentralen Protokollierungssystem sicherzustellen.
Bei der Beeinträchtigung der Verfügbarkeit oder Störung der Integrität des zentralen Protokollierungssystems, beispielsweise durch den Ausfall von Hardwarekomponenten, besteht keine Möglichkeit, unautorisierte Zugriffe oder den fehlerhaften Betrieb von Hard- und Software in Korrelation zu bringen. Dementsprechend sind Prozesse (manuell) oder Funktionsweisen (automatisiert) zu implementieren, die sowohl den zuständigen Produktverantwortlichen als auch den Verantwortlichen des Protokollierungssystems sowie die Stabstelle Datenschutz und Informationssicherheit benachrichtigen.
Die implementierten Sicherheitsmaßnahmen sowie die zulässigen Zugriffe und deren Notwendigkeit sind nachvollziehbar zu dokumentieren.

Um eine Manipulation von Protokollen, insbesondere von Benutzern mit privilegierten Zugangsrechten zu verhindern, sind die Security- und Account-Protokolle außerhalb des Einflussbereiches der Systemadministratoren aufzubewahren. Hierzu sind Security- und Account-Protokolle auf einer gesicherten zentralen Protokollierungsinstanz zu hinterlegen.

4.5. Erhebung von Protokolldaten

Die Erhebung von Rohdaten zur Protokollierung hat primär auf dem jeweiligen Produktivsystem zu erfolgen.
Der Umfang der Informationen, die innerhalb dieser Protokolldaten erfasst wird, richtet sich nach dem Zweck der zu protokollierenden Ereignisse. Die Protokolldaten sind daher im erforderlichen Umfang bereitzustellen.
Der Umfang eines Protokolleintrags ist je nach Ereignis und IT-System durch den Verantwortlichen des Protokollierungssystems auf Basis von inhaltlichen Gruppierungen, in Abstimmung mit dem Systemadministrator des liefernden Systems und der Stabstelle Datenschutz und Informationssicherheit, festzulegen. Dabei sind die im Anhang definierten Anforderungen zu beachten. Ist die Umsetzung aus technischen Gründen nicht möglich, sind geeignete alternative Maßnahmen zu treffen und mit der Stabstelle Datenschutz und Informationssicherheit festzulegen.
Die Protokollierung muss so erfolgen, dass die zugehörigen Aufzeichnungen durch einen fachkundigen Dritten nachvollzogen werden können.
Die Systemadministratoren dürfen, die Protokollierung ihrer eigenen Aktivitäten nicht ändern, löschen oder deaktivieren.

4.6. Transfer von Protokolldaten

Die Übertragung der Protokolldaten sollte nach dem Push-Verfahren erfolgen. Dabei ist sicherzustellen, dass das zentrale Protokollierungssystem durch dieses Verfahren nicht in seiner Verfügbarkeit und Leistung gestört wird. Um auch zeitlich aktuelle Vorfälle korrelieren und bewerten zu können ist eine zeitnahe Speicherung auf dem zentralen Protokollierungssystem zu verfolgen.
Die Auswahl und Einrichtung von geeigneten Synchronisationsverfahren obliegen dem Produktverantwortlichen und dem Verantwortlichen des Protokollierungssystems. Die relevanten Protokolldaten sind vor einer ungewünschten Manipulation zu schützen. Es muss sichergestellt sein, dass eine regelmäßige Überwachung der Kapazitäten auf den Speichermedien des Quellsystems sowie dem zentralen Protokollierungssystems erfolgt, um Ressourcenengpässe zu vermeiden.
Die Einrichtung und der Betrieb des Speichermediums des zentralen Protokollierungssystems obliegt dem Verantwortlichen des Protokollierungssystems.

4.7. Auswertung und Überwachung von Protokolldaten

Dezentrale Protokolldaten dienen ausschließlich der technischen Protokollierung und werden anlassbezogen ausgewertet. Die Auswertung muss durch benannte, fachlich qualifizierte und vertrauenswürdige Mitarbeiter oder sachverständige Dritte geschehen. Die Auswertung der Protokolle auf dem zentralen Protokollierungssystem obliegt dem zuständigen Verantwortlichen des Protokollierungssystems.

Der Fokus bei der zentralen Auswertung liegt dabei auf sicherheitsrelevanten Ereignissen, Warnungen, Fehlern und Alarmen. Aufgrund des Umfangs der Protokolle ist eine automatisierte Auswertung anzustreiben. Die Definition von sicherheitsrelevanten Indikatoren muss je Systemgruppe[1] vom Verantwortlichen des Protokollierungssystems in Abstimmung mit der Stabstelle Datenschutz und Informationssicherheit erfolgen und regelmäßig überprüft werden. Sollte sich im Rahmen der Auswertung der Verdacht auf einen Sicherheitsvorfall abzeichnen, ist die Stabstelle Datenschutz und Informationssicherheit unverzüglich einzubinden.

4.8. Aufbewahrung von Protokolldaten

Protokolldaten sind bedarfsgerecht, maximal sechs Monate für die Nachbearbeitung und Analyse auf dem zentralen Protokollierungssystem vorzuhalten. Anschließend sind diese unwiderruflich zu löschen. Die Löschung sollte nach Möglichkeit automatisiert erfolgen. Anderenfalls sind manuelle Löschprozesse zu definieren und umzusetzen. Die Vernichtung der Protokolle muss so erfolgen, dass sämtliche Kopien und Vervielfältigungen (z.B. Ausdrucke und Backups) ebenfalls mit einem sicheren Verfahren vernichtet werden.
Sicherheitsrelevante Protokolldaten können über die hier definierte Frist hinaus vorgehalten werden, wenn die Aufbewahrung aufgrund anderer regulatorischer Anforderung erforderlich ist. Die Anforderungen für die weitere Behandlung der Protokolle und die Zuständigkeit für die weitere Verarbeitung ergeben sich in diesen Fällen aus denjenigen Richtlinien, welche die regulatorischen Anforderungen umsetzen.
Wird innerhalb der festgelegten Ausbewahrungsfristen ein berechtigtes Interesse für eine Verlängerung der Aufbewahrungsfristen festgestellt, ist dies zu begründen und zu dokumentieren. Eine Verlängerung von Aufbewahrungsfristen ist im Vorfeld mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen.
Die Les- und Auswertbarkeit der Protokolle muss über den gesamten Aufbewahrungszeitraum gewährleistet bleiben. Werden z.B. im Rahmen einer Langzeitarchivierung, Migrationen vorgenommen, ist die Unverfälschtheit der Inhalte sicherzustellen.

[1] Indicators of Compromise (IoC) z. B. für Datenbankserver, Fileserver, Firewall, Proxy, Webserver, Switch, AD etc.

ANHANG: MINDESTANFORDERUNGEN AN DIE ZU PROTOKOLLIERENDE EREIGNISSE

Zur Identifizierung von Unregelmäßigkeiten und zur Gewährleistung der Nachvollziehbarkeit erfolgter Aktionen und Ereignisse hat der IT-Betrieb für jedes System die Parameter der Logfiles entsprechend zu konfigurieren. Die folgende Tabelle gibt entsprechende Anforderungen wieder.
In der Spalte „IT-System“ werden die zu betrachtenden IT-Systeme dargestellt und mit den jeweiligen zu protokollierenden Ereignissen und deren Zweck verknüpft. Sofern das IT-System als „übergreifend“ definiert ist, gelten die Anforderungen für sämtliche IT-Systeme, soweit dies anwendbar ist. Die Anwendbarkeit ist gegeben, wenn das IT-System über die technische Funktionalität verfügt und die entsprechenden Dienste durch das IT-System bereitgestellt werden. Alle anderen Einträge sind spezifisch auf ein IT-System abgestimmt.

IT-System	Kategorie	Ereignis	Zweck
Übergreifend	Benutzeraktivitäten	An-/Abmeldung von Administratorenkonten	Nachvollziehbarkeit von administrativen Tätigkeiten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Modifikation von Applikationsparametern	Nachvollziehbarkeit von administrativen Tätigkeiten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Hinzufügen oder Löschen von Administratorenarbeitsstationen	Nachvollziehbarkeit von administrativen Tätigkeiten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Manuelles Starten und Stoppen von Systemen und Diensten	Nachvollziehbarkeit von administrativen Tätigkeiten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Manuelles Starten und Stoppen von Applikationen	Nachvollziehbarkeit von administrativen Tätigkeiten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Manuelles Starten und Stoppen von Agenten	Nachvollziehbarkeit von administrativen Tätigkeiten im Missbrauchs- und Fehlerfall

IT-System	Kategorie	Ereignis	Zweck
Übergreifend	Benutzeraktivitäten	Erfolgreiche An-/Abmeldung von Benutzerkonten	Nachvollziehbarkeit von Benutzeraktivitäten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Abgewiesener Anmeldeversuch	Nachvollziehbarkeit von Benutzeraktivitäten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Sperrung von Benutzerkonten	Nachvollziehbarkeit von Benutzeraktivitäten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	An-/Abmeldung von Dienstkonten	Nachvollziehbarkeit von Benutzeraktivitäten im Missbrauchs- und Fehlerfall
Übergreifend	Benutzeraktivitäten	Unberechtigte Zugangs- und Zugriffsversuche	Nachvollziehbarkeit von Benutzeraktivitäten im Missbrauchs- und Fehlerfall
Übergreifend	Datensicherung	Durchführung einer Datensicherung oder einer Datenwiederherstellung	Verifizierung des Funktionierens der Datensicherung und Erkennen von unautorisierten Datenwiederherstellungen
Übergreifend	Konfigurationsänderung	Änderungen der Systemkonfiguration	Nachvollziehbarkeit von administrativen Handlungen im Missbrauchs- und Fehlerfall
Übergreifend	Rechtevergabe	Erstellung von Rechteprofilen	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen

IT-System	Kategorie	Ereignis	Zweck
Übergreifend	Rechtevergabe	• Zugriffsversuche auf Mechanismen zum Management von Authentifikationsdaten, • Erfolgreiche Zugriffsversuche auf Authentifikationsdaten, • Unautorisierte Zugriffe auf Benutzer-Authentifikationsdaten, • Unberechtigte Versuche auf Funktionen zur Administration von Benutzer-Einträgen zuzugreifen, • Durchgeführte Tests auf Passwort-Güte, • Jede Benutzung von Authentisierungsmechanismen, • Installation von Authentisierungsmechanismen, • Jede Konfiguration der Abbildung von Authentisierungsmechanismen zu spezifischen Authentifikationsereignissen.	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen
Übergreifend	Rechtevergabe	Erstellung, Änderungen und Löschung an den Policies / Richtlinien (Gruppenrichtlinien)	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen
Übergreifend	Rechtevergabe	Änderungen der domänenweiten Betriebsmasterfunktion	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Übergreifend	Rechtevergabe	Änderungen von Berechtigungen	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen
Übergreifend	Rechtevergabe	Änderungen an der Dateiorganisation, insbesondere Änderungen von Berechtigungen auf Datei- oder Ordnerebene	Nachweis und Analyse der Tätigkeiten im Missbrauchs- und Fehlerfall
Datenbanken	Verbindung	Fehlgeschlagene beziehungsweise abgewiesene Verbindungsversuche	Erkennung und Vermeidung von Angriffen und Fehlkonfigurationen

IT-System	Kategorie	Ereignis	Zweck
Netzwerkdienste	Dienste und Protokolle	Verzeichnisdienst, DNS-Server, Dateireplikationsdienst, IIS-Protokolle, RRAS-Protokolle, RADIUS-Protokolle	Vermeidung und Erkennung von Missbräuchen und Fehlern
Protokollierungssysteme	Administrative Tätigkeiten	Änderungen der Protokollierungseinstellungen	Erkennen und Nachvollziehbarkeit von Manipulationsversuchen und Manipulationen an Protokollierungsdateien
Protokollierungssysteme	Administrative Tätigkeiten	Änderungen oder Löschung von Protokolldateien	Erkennen und Nachvollziehbarkeit von Manipulationsversuchen und Manipulationen an Protokollierungsdateien
Public-Key-Infrastruktur	Zertifikate	Stellen und Beantworten von Zertifikatsanfragen	Vermeidung und Erkennung von Missbräuchen und Fehlern
Public-Key-Infrastruktur	Zertifikate	Übertragung von Schlüsseln und Zertifikaten	Vermeidung und Erkennung von Missbräuchen und Fehlern
Public-Key-Infrastruktur	Zertifikate	Wechsel von Schlüsseln und Zertifikaten	Vermeidung und Erkennung von Missbräuchen und Fehlern
Public-Key-Infrastruktur	Zertifikate	Erzeugung von Schlüsseln und Zertifikaten	Vermeidung und Erkennung von Missbräuchen und Fehlern
Public-Key-Infrastruktur	Zertifikate	Sicherung und Wiederherstellung von Schlüsseln und Zertifikaten	Vermeidung und Erkennung von Missbräuchen und Fehlern
Public-Key-Infrastruktur	Zertifikate	Löschung von Schlüsseln und Zertifikaten	Vermeidung und Erkennung von Missbräuchen und Fehlern
Public-Key-Infrastruktur	Zertifikate	Export von Schlüsseln und Zertifikaten	Vermeidung und Erkennung von Missbräuchen und Fehlern
Verzeichnisdienst	Administrative Tätigkeiten	Active Directory-Zugriffe	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten

IT-System	Kategorie	Ereignis	Zweck
Verzeichnisdienst	Administrative Tätigkeiten	Objektzugriffe und Rechteverwendungen (Objekte, Sicherheitsgruppen, Benutzer- oder Computerkonten)	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten
Verzeichnisdienst	Administrative Tätigkeiten	Änderungen an Administratorarbeitsstationen	Nachvollziehbarkeit von Konfigurationsänderungen im Missbrauchs- und Fehlerfall
Verzeichnisdienst	Konfigurationsänderung	Änderungen am Active Directory Schema	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten
Verzeichnisdienst	Konfigurationsüberwachung	Kontenverwaltungsereignisse	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen
Verzeichnisdienst	Konfigurationsüberwachung	Änderungen der LDAP-Richtlinien inklusive Verwendung LDAP Server	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Verzeichnisdienst	Konfigurationsüberwachung	Änderungen an der Replikationstopologie zwischen Domänen Controllern	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Verzeichnisdienst	Konfigurationsüberwachung	Änderungen der gesamtstrukturweiten Betriebsmasterfunktionen	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Verzeichnisdienst	Rechtevergabe	Änderungen der Vertrauensstellungen	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen

IT-System	Kategorie	Ereignis	Zweck
Verzeichnisdienst	Rechtevergabe	Änderung des AdminSDHolder-Objekts	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Verzeichnisdienst	Rechtevergabe	Änderungen der Mitgliedschaft vordefinierter Dienste-Administratorengruppen	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Verzeichnisdienst	Rechtevergabe	Änderungen der Überwachungsrichtlinien für eine Domäne	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen.
Verzeichnisdienst	Rechtevergabe	Änderungen an der Einstufung von Domänen-Controllern	Sicherstellung der System- und Netzintegrität sowie Verfügbarkeit von Diensten Erkennen von Manipulationsversuchen
Verzeichnisdienst	Rechtevergabe	Einrichten, Ändern und Löschen von Gruppen im Active Directory	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen
Verzeichnisdienst	Rechtevergabe	Einrichten, Ändern und Löschen von Benutzern im Active Directory	Nachvollziehbarkeit der Vergabe und des Entzugs von Berechtigungen
VPN Gateway / Sicherheitsgateway	Paketfilter	Paketfilter: IP-Adresse, Dienst für jedes Paket, aber auch eingeschränkt auf bestimmte Pakete Zutreffende Regel des Paketfilters	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch
VPN Gateway / Sicherheitsgateway	Paketfilter	Ungewöhnliche Pakete	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch

IT-System	Kategorie	Ereignis	Zweck
VPN Gateway / Sicherheitsgateway	Gateway	SMTP: E-Mail-Adresse des Absenders und des Empfängers der E-Mail, Menge der übertragenen Daten, Hinweis auf angewandte Filterkriterien, Statusnachricht über Erfolg oder Misserfolg der Weiterleitung	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch
VPN Gateway / Sicherheitsgateway	Gateway	FTP: Ziel-Adresse (URL), abgelehnte PORT-Befehle, Name der übertragenen Datei, Menge der übertragenen Daten, Statusnachricht, Nutzung von gesperrten Request-Methoden, Benutzernamen im Falle einer Authentisierung	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch
VPN Gateway / Sicherheitsgateway	Gateway	DNS: Ablehnen und Zulassen von Anfragen, von anderen IT-Systemen initiierte „ausgehende“ Zonen-Transfers, vom Application Layer Gateway initiierte „eingehende“ Zonen-Transfers	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch
VPN Gateway / Sicherheitsgateway	Gateway	Telnet: Benutzername im Falle einer Authentisierung	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch

IT-System	Kategorie	Ereignis	Zweck
VPN Gateway / Sicherheitsgateway	Gateway	Application Level Gateway: IP-Adresse des Quell- und Zielrechners, Portnummern, Dienst, Datum und die zutreffende Regel, übertragene Datenmenge, Uhrzeit des Verbindungsauf- und Verbindungsabbaus HTTP: Zusätzliche Protokollierung der aufgerufenen Webseiten und Protokollierung der Nutzung von gesperrten Request-Methoden, Verbindungsmethode (z. B. GET, POST, CONNECT), Hinweis auf angewandte Filterkriterien, Statusnachricht HTTPS: Zusätzliche Protokollierung der abgerufenen Webseite	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch
VPN Gateway / Sicherheitsgateway	Gateway	Auf- und Abbau jeder VPN-Verbindung sowie abgewiesene Verbindungen	Erkennung und Vermeidung von Angriffen, Fehlkonfigurationen und Missbrauch
Webserver	Dienste und Protokolle	Webserver wie IIS, Apache: Methode, Stamm-URI, WIN32-Status, HTTP-Status, Benutzeragent, Server IP-Adresse und Server Anschluss	Vermeidung und Erkennung von Missbräuchen und Fehlern

Tabelle 1: Mindestanforderungen an die zu protokollierenden Ereignisse