01.24

59. Jahrgang
Februar 2024
Seiten 1 – 52

www.ZIRdigital.de

ZIR

Zeitschrift Interne Revision

Fachzeitschrift für Wissenschaft und Praxis

Herausgeber:
DIIR Deutsches Institut für Interne Revision e.V.

Standards · Regeln · Berufsstand

Management · Best Practice · Arbeitshilfen

ESV ERICH SCHMIDT VERLAG
100 Jahre

20380

DR. STEPHEN FEDTKE

Umgang mit IT-Diagnosedaten

Risiken aus unzureichenden Schutzmaßnahmen im IT-Betrieb

Der nicht datenschutzgerechte Umgang mit IT-Diagnosedaten im internen IT-Betrieb oder beim externen IT-Dienstleister bedeutet ein gravierendes Datenschutz- und IT-Sicherheitsrisiko. Der Diebstahl eines Microsoft Master Key aus einem Crash-Dump für einen Angriff im Mai 2023 stellt dies unter Beweis. Mögliche negative Zusatzeffekte sind Obliegenheitsverletzungen oder Gefährdungserhöhungen im Kontext von Cyber- und D&O-Versicherung.

Dr. Stephen Fedtke,
CTO bei Enterprise-IT-Security.com, Zug, Schweiz.

1. Problemstellung

Wie entstehen IT-Diagnosedaten? Fehlerbedingte Abstürze von Computern oder Applikationen werden in sogenannten Dumps dokumentiert. Sie enthalten die Speicherinhalte im Moment des Systemversagens. Logs, also Protokolldaten, hingegen werden fortlaufend erzeugt. Traces schneiden den Netzwerkverkehr mit. Auf diese Weise werden auf lokalen, internen Servern des IT-Betriebs oder beim IT-Dienstleister permanent Mengen an IT-Diagnosedaten erzeugt.

Welches Risikopotenzial enthalten IT-Diagnosedaten? Man könnte vermuten, dass IT-Diagnosedateien nur technische Daten umfassen. Dies ist ein Trugschluss. Tatsächlich enthalten sie personenbezogene und sicherheitskritische Daten in großem Umfang. Dies sind Daten, die im Moment des Computerabsturzes zufällig im Speicher waren. Im Fall von Unternehmen sind es vordringlich Kundendaten und Firmengeheimnisse, im Gesundheitsumfeld geht es um Patientendaten, und im Fall von Behörden und staatlicher IT reicht das Spektrum von Bürger- und Sozialdaten bis hin zu polizeilichen, geheimdienstlichen und militärischen Daten.

Was sind die genauen Prozesse? Üblicherweise schickt der IT-Betrieb im Kontext eines Problemtickets die IT-Diagnosedaten per Upload zum Support der Softwareanbieter. Darin sind auch alle sensiblen Daten enthalten. Für diesen Weg nach USA, Indien, China oder Europa werden die Daten verschlüsselt. Vor Ort entschlüsseln, speichern und verarbeiten die Supportmitarbeiter und Entwickler die Dateien aber wieder und haben so auch Zugang zu den sicherheitskritischen und datenschutzrelevanten Daten. Dies ist ein Risiko, da es keine Kontrolle darüber gibt, was in der Folge mit den sensiblen Daten passiert und wer darauf zugreift.

IT-Betriebe, die outsourcen oder die Cloud nutzen, können sich der Verantwortung für den Export sensibler Daten via Dumps, Logs und Traces nicht entziehen. Die Entscheidung über den Versand liegt dann zwar bei den operativen Teams der externen IT-Service-Provider. Die Zuständigkeit für Datenschutz- und Compliance-Auflagen ist jedoch beim Daten-Owner verortet.

Das Risiko um IT-Diagnosedaten kann sich übrigens auch im eigenen Hause realisieren. Denn die Daten entstehen auch im Fall firmeneigener Softwareentwicklungen, und die eigenen Entwickler werten diese aus, um Probleme zu analysieren und zu fixen. Das heißt, es erfolgt kein Upload zu Herstellern, sondern Inhouse-Entwickler greifen direkt auf die Dumps, Logs und Traces der produktiven Systeme zu. Auf diese Weise erhalten eigene Entwickler ebenso Zugriff auf sensible Daten aus der produktiven IT, die sie zum Beispiel im Rahmen von Softwaretests nicht erhalten, weil diese auf anonymisierten Testdaten basieren.

2. Lösungsansatz

Eine rechtlich und sicherheitstechnisch wirksame Lösung bietet die Anonymisierung sämtlicher IT-Diagnosedaten vor dem Upload. Die Anonymisierung sollte lokal und automatisiert erfolgen. Sie befreit die Dokumente von datenschutz- und sicherheitssensiblen Inhalten, bei vollem Erhalt der technischen Aussagekraft. Erst danach werden die Dateien zum Support des Softwareherstellers hochgeladen – risiko- und rechtskonform. Mittels erstellter Begleitdokumente wird der Gesamtprozess transparent, nachweisbar und rechtskonform.

3. Bedeutung für die Interne Revision

Was bedeutet dies für die Interne Revision und IT-Audits?

1.) Zunächst stellt der Upload nicht-anonymisierter IT-Diagnosedaten einen DSGVO-Verstoß dar. Dieses Datenschutzproblem wird auch nicht durch eine verschlüsselte Übertragung gelöst. Denn beides, Speicherung und Verarbeitung der sensiblen Daten durch die Softwarehersteller, erfolgt ohne Zweck und Notwendigkeit. Die eingelagerten sensiblen Daten werden für die eigentliche Zielsetzung des Uploads definitiv nicht benötigt. Diese besteht ausschließlich in der Lösung eines jeweiligen softwaretechnischen Problems. Es verletzt den Datenschutz, wenn zu schützende sensible Daten zweckfremd an Dritte weitergeleitet werden.

Ein unsachgemäßer Umgang mit IT-Diagnosedaten ist ein Unternehmensrisiko und folglich revisionsrelevant.

2.) IT-Diagnosedaten bedeuten eine Gefahr für die IT-Sicherheit. Dies beweist der Cyber-Angriff chinesischer Hacker des Storm-0558 auf das US-Außenministerium im Mai 2023. Die Täter hatten einen Azure Cloud Signing Key, also einen Microsoft Master-Key, aus einem Crash-Dump bei Microsoft gestohlen und sich damit Zugang unter anderem zu 60.000 E-Mails aus zehn Accounts verschafft. Solche Schlüssel, wie auch Passwörter, Zertifikate oder IP-Adressen, befinden sich in Dumps, Logs und Traces. Diese sicherheitskritischen Informationen werden durch den Upload und Transfer zum Support für Dritte zugänglich gemacht. Cyberkriminelle können sie extrahieren und für Angriffe nutzen. Dumps und Logs gehören zu den Sicherheitsrisiken gemäß CWE von MITRE.[1] Laut CWE-528 sind bereits „herumliegende Dump-Dateien" ein Risiko, wenn Unbefugte darauf zugreifen können. Die CWE-200 „Exposure of Sensitive Information to an Unauthorized Actor" war bereits 2021 in der „CWE Top 25 Most Dangerous Software Weaknesses" als schwerwiegende Sicherheitslücke klassifiziert. Dies macht IT-Diagnosedaten für sogenannte Kritische Infrastrukturen (KRITIS) und für Verfechter der Zero-Trust-Idee zu einem ernst zu nehmenden Risiko.

3.) Geschäftsleiter könnten nervös werden, wenn Cyber-Insurance- und D&O-Versicherungspolicen den Upload nicht-anonymisierter IT-Diagnosedaten als Vorsatz beziehungsweise Obliegenheitsverletzung oder Gefährdungserhöhung einstufen würden, verbunden mit einer Infragestellung des Versicherungsschutzes.

Verglichen mit den vielfältigen Risiken ist die automatisierte Anonymisierung der IT-Diagnosedaten wenig aufwendig. Die Schieflage könnte also sofort beseitigt werden.

Neben drohenden Bußgeldern gemäß DSGVO steht seit dem EuGH-Urteil vom 4. Mai 2023 der Haftungs- und Schadensersatzanspruch im Vordergrund der Risikoanalyse. Juristische Akteure könnten unter anderem die Beweislastumkehr oder das Auskunftsrecht bei Hauptversammlungen mit obigem Thema strategisch verbinden.

Insgesamt wird deutlich, dass ein unsachgemäßer, nicht rechtskonformer Umgang mit IT-Diagnosedaten definitiv zum Unternehmensrisiko wird und folglich revisionsrelevant ist.

4. Prüfungskatalog

Welche Themen umfasst der Prüfkatalog einer Revisionsprüfung im Bereich IT-Diagnosedaten?

Die Prüfung des IT-Betriebs in Bezug auf einen gesetzeskonformen Umgang mit IT-Diagnosedaten sollte die folgenden als Frage formulierten Aspekte und Prüfdetails enthalten:

- Gibt es im IT-Betrieb eine dokumentierte Verfahrensvorgabe für den Umgang mit IT-Diagnosedaten?
- Sind alle Beteiligten verpflichtet, IT-Diagnosedaten vor dem Upload zu anonymisieren?
- Ist ebenso die Handhabung im Fall besonders hoher Dringlichkeit geregelt, zum Beispiel durch eine Fokussierung auf die besonders sensiblen Datentypen, damit der für den Anonymisierungsprozess notwendige Zeitbedarf reduziert wird?
- Werden sämtliche Uploads von IT-Diagnosedaten im Rahmen des Problemmanagements ausreichend dokumentiert (Zeit, Quellsystem der Daten, Ticket-ID, Bearbeiter etc.)?

1 Die MITRE Corporation ist eine Organisation zum Betrieb von Forschungsinstituten im Auftrag der Vereinigten Staaten, die durch Abspaltung vom Massachusetts Institute of Technology (MIT) entstanden ist. CWE™ (Common Weakness Enumeration) ist eine Liste von Software- und Hardwareschwachstellen. Sie dient als gemeinsame Sprache, als Messlatte für Sicherheitstools und als Grundlage für die Identifikation von Schwachstellen sowie für Maßnahmen zur Abschwächung und Prävention.

- Wer hat Zugriff auf IT-Diagnosedokumente, insbesondere wenn diese aus dem Produktionsumfeld stammen?
- Ist der Begriff IT-Diagnosedokument ausreichend präzise definiert, sodass alle relevanten Dokumentenarten eingeschlossen sind, insbesondere Dumps, Logs und Traces?
- Erfolgt der Upload, das heißt der Transfer, verschlüsselt?
- Sind sämtliche automatischen Transfers von IT-Diagnosedaten zu den Herstellern deaktiviert? Und werden sie unterbunden?
- Ist das Spektrum sensibler und damit zu anonymisierender Daten mit dem Datenschutz-, Risiko- und Sicherheitsmanagement abgeklärt und schriftlich festgelegt worden?
- Was passiert mit den Original-IT-Diagnosedateien? Wo werden diese gespeichert? Wann werden diese gelöscht? Wer darf auf die Dateien zugreifen?
- Auf welchen Systemen erfolgt die Anonymisierung? Auf ausgewählten Systemen oder auf den individuellen Laptops der Beteiligten?
- Wird die Anonymisierung in Begleitdokumenten dokumentiert und nachweisbar festgehalten?
- Welche weiteren Arten von Folgeverarbeitungen von IT-Diagnosedaten werden praktiziert? Dies gilt insbesondere bezüglich der Weiterverarbeitung von Log- und Protokolldaten, zum Beispiel durch SIEM-Lösungen.
- Werden IT-Diagnosedokumenten-Container ebenfalls einer Anonymisierung unterzogen? Manche Betriebssysteme erstellen zum Beispiel Pax- oder Zip-Files mit mehreren Hundert oder Tausend Einzeldokumenten. Erfolgt die Anonymisierung auch dann vollständig?
- Wie ist der Umgang mit binär-codierten IT-Diagnosedateien geregelt, das heißt mit Dateien, deren binäre Inhalte aufgrund fehlenden Wissens über die genauen Formate nicht inspiziert und damit anonymisiert werden können? Werden diese vom Upload ausgeschlossen? Oder werden sie einfach „as-is" weitergereicht? Letzteres impliziert ein Restrisiko, dass diese Binärdaten nicht nachvollziehbare Geheimnisse umfassen könnten, zum Beispiel IP-Adressen.
- Wie ist der Umgang mit ausführbaren Dateien als Bestandteil von IT-Diagnosedaten geregelt? In den IT-Diagnosedokumenten einiger Betriebssysteme sind auch ausführbare Dateien eingeschlossen. Im Vergleich zu binär kodierten Dateien unbekannten Formats ist hier die As-is-Weitergabe durchaus zu rechtfertigen.
- Wie ist der Zugang zu IT-Diagnosedokumenten für die firmeneigene Softwareentwicklung geregelt? Erhalten First- und Second-Level Support beziehungsweise Entwickler auch im Fall der Produktion Zugriff auf die Originaldateien oder nur auf anonymisierte Dokumente?
- Ist auf den Servern eine Detektion zum Entstehen von IT-Diagnosedokumenten etabliert?
- Sind die Zugriffsrechte für IT-Diagnosedokumente auf den einzelnen Betriebssystemen restriktiv geregelt? Insbesondere darf aufgrund fehlenden Customizings kein Public Access bestehen (siehe das bereits erwähnte CWE-528).
- Wurde die Cyber-Insurance-Police bezüglich möglicher Obliegenheiten in Bezug auf den Umgang mit IT-Diagnosedaten geprüft? Ist ausgeschlossen, dass der firmeneigene Umgang als Obliegenheitsverletzung oder Gefährdungserhöhung mit eventueller Folge der Deckungseinschränkung angesehen werden kann?

> **IT-Diagnosedaten bedeuten eine Gefahr für die IT-Sicherheit, weil sicherheitskritische Informationen von Cyberkriminellen für Angriffe genutzt werden können.**

Darüber hinaus kann eine Prüfung der datenschutzrechtlichen Vereinbarungen mit einem Dienstleistungsunternehmen sinnvoll sein. Ergänzende Fragestellungen im Fall des Outsourcings oder der Cloud-Nutzung:

- Ist mit Dienstleistern der Umgang mit IT-Diagnosedaten klar geregelt? Ein defensiver Ansatz kann sogar vorsehen, dass der Kunde die Anonymisierung selbst vornimmt und der Dienstleister die Dokumente dann für den Upload zurückerhält. Letztlich wäre nur so die Verantwortung „lupenrein" geregelt.
- Ist der Zugriff auf IT-Diagnosedaten auf den ausgelagerten Systemen klar definiert?
- Sind die Abläufe mit dem Dienstleister vertraglich und schriftlich klar festgelegt?

Stichprobenbasierte Prüfungen könnten sich wie folgt gestalten:

- Lassen Sie sich die Ticketsysteme für die Zusammenarbeit mit zum Beispiel drei Softwareherstellern zeigen. Schließen Sie auch

einen kleineren Softwarehersteller ein, wählen Sie nicht nur Big Players aus.

- Wählen Sie darin jeweils zum Beispiel zwei oder drei beispielhafte Vorgänge aus, die einen Upload von IT-Diagnosedokumenten beinhalten – vorzugsweise Dumps.
- Lassen Sie sich zu diesen Vorgängen die Begleitdokumente zu den Anonymisierungen und die eventuell vorhandenen Löschungsbestätigungen zeigen. Prüfen Sie anhand der Dokumente die Anonymisierung des beschlossenen Katalogs von sensiblen Datentypen.
- Lassen Sie sich den Vorgang der Anonymisierung einmal vorführen, und prüfen Sie hierbei die voreingestellten und praktizierten Datentypen, nach denen gesucht wird.
- Fragen Sie nach tatsächlichen dringenden Situationen, in denen gegebenenfalls nur eine reduzierte Menge an Datentypen anonymisiert wurden.

Der Prüfungskatalog macht deutlich, wie sensibel und praxisrelevant das Thema ist.

Literaturverzeichnis

Awareness-Video „Datenschutz- und Sicherheitsrisiken in IT-Diagnosedaten“, https://www.enterprise-it-security.com/info-video-de/ZIR (Stand: 13.09.2023).

Knop, D. (2023): Gestohlener Microsoft-Schlüssel stammt aus einem Crash-Dump, heise news, 07.09.2023, https://www.heise.de/news/Gestohlener-Microsoft-Schluessel-stammte-aus-einem-Crash-Dump-9297240.html (Stand: 05.01.2024).

Speichert, H. (2023): DSGVO-Haftungs- und Sicherheitsrisiken durch Protokoll- und Diagnosedaten im IT-Betrieb, Datenschutz und Datensicherheit (DuD), 47, 04/2023, S. 229-232, https://www.enterprise-it-security.com/DuD-Artikel-Speichert-042023/ZIR2 (Stand: 13.09.2023).

Steevens, P. (2023): 60.000 geklaute Regierungsmails: Erste Zahlen nach Microsofts Cloud-Key-Debakel, heise news, 29.09.2023, https://www.heise.de/news/60-000-geklaute-Regierungsmails-Erste-Zahlen-nach-Microsofts-Cloud-Key-Debakel-9321044.html?wt_mc=nl.red.security.secu-rity-nl.2023-10-02.link.link (Stand: 05.01.2024).