Cybercrime durch Microsoft Crash-Dump – IT-Diagnose-Daten jetzt im Fokus von Cyberversicherung und Underwritern

Dr. Stephen Fedtke,
CTO,
Enterprise-IT-Security.Com

In den Laboren von Microsoft haben chinesische Hacker im Mai 2023 einen Master-Key aus einem Crash-Dump gestohlen (vgl. [Knop 2023]). Mit diesem Azure Cloud Signing Key konnten sie 60.000 Mails aus zehn Accounts sowie alle Mail-Adress-Listen der amerikanischen Regierung erbeuten (vgl. [Steevens 2023]).

IT-Diagnose-Daten wie Dumps, Logs und Traces sind wahre Fundgruben für sicherheitskritische Informationen. Hacker können sich hier frei bedienen und Schlüssel, User-IDs, Passwörter oder IP-Adressen extrahieren. Dieses Risiko betrifft alle Unternehmen und Behörden gleichermaßen, nicht nur Microsoft. Demzufolge sollte diese IT-Sicherheits-Schwachstelle des IT-Betriebs fester Bestandteil der Risikoabfrage und der Obliegenheiten der Cyberversicherungen sein. Denn Prävention in Form von Anonymisierung der sensiblen Daten wäre ein sinnvoller Vertragsbestandteil.

Der Fall Microsoft hat den Handlungsbedarf offengelegt. Viele Unternehmen, Behörden und Institutionen ignorieren oder unterschätzen IT-Diagnose-Daten als Angriffsfläche für Datensicherheit und auch Datenschutz. Sie praktizieren, trotz Verfügbarkeit automatisierter Anonymisierungstechnologien, nahezu täglich den Upload nicht-geschützter IT-Diagnose-Daten in die ganze Welt. Dieses Sicherheits- und Datenschutzrisiko kann vom Versicherungsgeber im Rahmen der Risikodialoge und -fragebögen im Renewal-/Abschlussprozedere von Cyberversicherungspolicen thematisiert werden.

Alle Beteiligten sollten ein Interesse daran haben, dieses Sicherheits- und Datenschutz-Risiko durch Anonymisierung in Zukunft zu vermeiden.

Funktion und Sicherheitsrisiko von IT-Diagnose-Daten im IT-Betrieb

Worum handelt es sich bei den typischen IT-Diagnose-Daten, wie Dumps, Logs und Traces? Dumps sind Speicherauszüge, die bei allen Computer- und Applikationsabstürzen entstehen. System-Logs oder Protokolldaten werden fortlaufend erzeugt. Traces, also Mitschnitte von Netzwerk-Protokollen und -Paketen, dienen der Analyse des Netzwerkdatenstroms.

Worin besteht das konkrete Risiko? IT-Diagnose-Dateien enthalten große Mengen versteckt eingelagerter sensibler Personendaten, Geschäftsgeheimnisse und sicherheitsrelevanter Informationen. Der IT-Betrieb, wie z.B. die Administratoren, schicken diese IT-Diagnose-Daten zur Analyse und Fehlerbehebung an den Support ihrer Software-Anbieter und Dienstleister oder an eigene Entwicklungsabteilungen. Somit gelangen sie in die weltweit verteilten Labore, Support- und Entwicklungszentren. Teilweise passiert dies sogar vollautomatisch.

Die eingelagerten sensiblen Daten sind für die Problemanalyse jedoch nicht notwendig und damit vollkommen zweckfremd. Sie stellen daher in zwei Richtungen ein ernstzunehmendes Risiko dar. Gemäß dem aktuellen Datenschutzgesetz, der DSGVO, dürfen Daten mit Personenbezug grundsätzlich nicht zweckfremd an Dritte übertragen und von diesen auch nicht verarbeitet werden. Bereits der Transfer stellt eine Verletzung des Datenschutzes und der Datensicherheit dar.

Das zweite Risiko resultiert aus den in ihnen enthaltenen IT-sicherheitsrelevanten Details. Sie bieten die Blaupause für einen erfolgreichen Angriff, wie im Fall Microsoft. Dumps sind potentielle „Handelsware" im Darknet und bieten exzellente Informationen für jegliche Form von Cybercrime. Die Ausführung einer Ransomware-Attacke ist nur eines von vielen denkbaren Szenarien.

IT-Diagnose-Daten als Zielscheibe von Cybercrime

Den IT-Spezialisten ist das Risiko um IT-Diagnose-Daten bekannt. Der Security-Standard MITRE zum Beispiel beschreibt und klassifiziert Dumps u.a. via „CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere" offiziell als Risiko (vgl. [CWE 2023]). Dies betrifft auf Systemen lokal „herumliegende" IT-Diagnose-Daten. Jeder, der Zugang zu Dumps, Logs und Traces erlangt, kann diese IT-Diagnose-Dateien gezielt auswerten, um einen perfekten Angriff zu planen. So auch Hacker, wie im Fall Microsoft. Mit der Weitergabe von IT-Diagnose-Daten an Dritte, wie beim Upload zu Herstellern, potenziert sich dieses CWE-528-Grundrisiko.

Der Diebstahl des Microsoft Master Key aus einem Crash Dump durch die chinesische Storm-0558-Gruppe hat die Risikolage für IT-Diagnose-Daten für alle deutlich gemacht. Die Medienresonanz auf den Microsoft-Hack war groß. Von IT-Medien wie Heise News (vgl. [Knop 2023], [Steevens 2023]) bis zu Wirtschaftszeitungen wie Handelsblatt (vgl. [Jahn 2023]) wurde über diese schwerwiegende Cyber-Attacke berichtet. Sie ist in einem hochprofessionellen Labor eines führenden Herstellers passiert, in dem Softwareprobleme analysiert und gefixt werden. Diese Debugging-Zentren sind Angriffsziele für Cyberkriminelle. Wenn IT-Diagnose-Daten von tausenden von IT-Betrieben weltweit in diese Labors geschickt werden, bieten sie eine interessante Quelle für attraktive, weil sensible Daten. Somit sind die Hersteller selbst Teil

des Sicherheitsrisikos. Demzufolge ist die ZeroTrust-Leitidee nicht nur für kritische Infrastrukturen, sondern generell für alle Unternehmen sinnvoll.

Unbereinigte IT-Diagnose-Daten dürfen weder direkt noch indirekt in Drittländer übermittelt werden, die im Sinne des Datenschutzes kein gleichwertiges Schutzniveau wie Deutschland, die EU oder die Schweiz besitzen (vgl. [Speichert 2023]). Dazu zählen auch USA, Indien oder China. Die führenden Software-Anbieter, insbesondere deren Support-, Entwicklungszentren und Labore, befinden sich allerdings genau in diesen Lokationen. Jedoch auch in Ländern mit gleichwertigem Schutzniveau, wie der EU, bieten die zweckfremd in Dumps, Logs und Traces versteckt enthaltenen Daten eine datenschutzrechtliche und sicherheitskritische Angriffsfläche und damit eine „Haftungsfläche" für Versicherungsgeber.

Outsourcing und Cloud-Nutzung eliminieren die Risiken nicht, verschärfen sie eher

Ein in die Cloud oder an Hosting-Provider ausgelagerter IT-Betrieb befreit nicht vom Risiko um IT-Diagnose-Daten. Auch dann nicht, wenn der Cloud-Anbieter identisch mit dem Software-Hersteller ist. Es wird eher komplizierter, weil der IT-Betrieb von Dritten betreut wird und damit fremde Administratoren, nämlich die der Provider, über den Upload der sensiblen Daten entscheiden. Der Fall eines konfigurierten automatischen Uploads von IT-Diagnose-Daten ist als „worst case" zu betrachten und darf im professionellen Umfeld überhaupt nicht stattfinden.

Risikoabwägung und Risikoprüfung für Cyberversicherungen

Sollten Cyberversicherer das Risiko der IT-Diagnose-Daten offen kommunizieren? Auf jeden Fall, und zwar im eigenen Interesse, denn das Risikovolumen ist beträchtlich. Jeder IT-Betrieb erzeugt regelmäßig IT-Diagnose-Daten. Das Resultat beträgt im Durchschnitt circa 100 solcher kritischen Transfers pro Jahr und Firma bzw. Institution. Für die rund 50.000 Rechenzentren in Deutschland (siehe Bitkom-Studie 2022, vgl. [Bitkom 2022]) bedeutet dies ein Versand- und somit Risiko-Volumen von 5 Millionen IT-Diagnose-Dateien mit sensiblen Daten aus produktiven IT-Umgebungen an Hersteller in der ganzen Welt. Das ist eine signifikante Größenordnung.

Insider kennen die „Schätze", die man in IT-Diagnose-Daten heben kann. In welcher Form und von wem genau sie in den internationalen Software-Zentren oder durch Hacker genutzt werden, lässt sich kaum nachvollziehen. Der Mangel an Transparenz und die Verharmlosung dieser – meist ungeschützten – Sicherheitslücke potenziert das Risiko. Da der Upload von IT-Diagnose-Daten Best Practice der IT ist, kann der Nachweis einer (Mit-)Schuldfrage des Versicherungsnehmers auch nur schwer geführt werden.

Bis zur Veröffentlichung des Hacks bei Microsoft lief das Thema praktisch „unter dem Radar". Im Gegensatz zu anderen Disziplinen, wie etwa dem Patch-Management, war die Anonymisierung der sensiblen Informationen in Dumps, Logs und Traces bis dato noch keine technische Standard-Maßnahme. Der Microsoft Cybercrime-Vorfall hat ein Umdenken erzeugt und stellt nun auch die Cyberversicherungen vor neue Aufgaben.

Schutzmaßnahmen für IT-Diagnose-Daten

Man könnte annehmen, dass die Verschlüsselung der IT-Diagnose-Dateien bereits eine compliancegerechte Lösung bieten würde. Leider nein, denn die Diagnose-Daten werden im Support zur Fehleranalyse entschlüsselt und verarbeitet.

Demzufolge sollten sensible Daten in IT-Diagnose-Dateien vor dem Versand anonymisiert oder falsifiziert werden. Dann sind sie auch nach der Entschlüsselung nicht sichtbar. Passiert dies nicht – und dies ist in der Praxis noch der Normalfall –, begeht das Unternehmen einen Verstoß gegen das Datenschutzrecht und die Sicherheitsgesetze. Eine automatisierte Anonymisierung und Falsifizierung der sensiblen Daten ist Stand der Technik und bietet einen hohen Grundschutz gegen die sicherheitsgefährdende Verletzung der DSGVO und vieler Sicherheitsregularien wie u.a. BSI-Gesetz (BSIG), IT-Sicherheitsgesetz 2.0 (IT-SIG 2.0) und die in nationale Umsetzung befindliche NIS2-RL bzw. das IT-SIG 3.0. Als Bestandteil der Obliegenheiten der Cyberversicherung hätten diese Schutzmaßnahmen einen risikomindernden und sicherheitswirksamen Effekt.

Aus Sicht technologischer Verfügbarkeit ist die Anonymisierung bereits „Stand der Technik". IT-Diagnose-Daten können per lokaler Anonymisierung vor dem Transfer einfach und automatisiert bereinigt werden. Die IT-Diagnose-Daten würden sowohl von sicherheitskritischen als auch von datenschutzsensiblen Inhalten bereinigt. Dieses Elementarrisiko jeden IT-Betriebs ist zum Glück technisch abwendbar. Es ist also im Interesse der Versicherungen wie auch deren Kunden, die Angreifbarkeit durch definierte präventive Maßnahmen zu verhindern.

Neben der Cyber-Versicherung sind auch andere Versicherungen von den Risiken des unsachgemäßen Umgangs mit IT-Diagnose-Daten betroffen: IT-Haftpflicht, IT-bezogene Berufshaftpflicht und die D&O. Potenziell ist jedes Unternehmen mit einem IT-Betrieb juristisch angreifbar. Denn jeder IT-Betrieb erzeugt IT-Diagnose-Dokumente. Dies ist unverzichtbar. Sie werden zu den Herstellern hochgeladen. Dies ist ebenfalls unverzichtbar. Das Bewusstsein hierüber und die Reduzierung des Sicherheits-, Datenschutz- und somit auch Versicherungsrisikos würde durch die Aufnahme technischer Maßnahmen, wie der Anonymisierung, gefördert werden.■

Quellen:

[Bitkom 2022] Bitkom e.V. (Hrsg.): Rechenzentren in Deutschland – Aktuelle Marktentwicklungen, Stand 2022. Borderstep Institut, Berlin, 2022, S. 8; https://www.bitkom.org/sites/main/!les/2022-02/10.02.22-studie-rechenzentren.pdf.

[CWE 2023] Common Weakness Enumeration: CWE-528: Exposure of Core Dump File to anUnauthorized Control Sphere, 2023; https://cwe.mitre.org/data/de!nitions/528.html.

[Jahn 2023] Jahn, T., Kerkmann, C.: Softwarekonzern denkt nach Cyberangriff Sicherheit neu, Handelsblatt online 16.11.2023; https://www.handelsblatt.com/technik/it-internet/microsoft-softwarekonzern-denkt-nach-cyberangriff-sicherheit-neu/29497982.html.

[Knop 2023] Knop, D.: Gestohlener Microsoft-Schlüssel stammte aus einem Crash-Dump, heise news 07.09.2023; https://www.heise.de/news/Gestohlener-Microsoft-Schluessel-stammte-aus-einem-Crash Dump-9297240.html.

[Speichert 2023] Speichert, H.: DSGVO-Haftungs- und Sicherheits-risiken durch Protokoll- und Diagnosedaten im IT-Betrieb. Datenschutz und Datensicherheit (DuD) 47, 04/2023, S. 229-232; https://www.enterprise-itsecurity.com/DuD-Artikel-Speichert-042023/GOV.

[Steevens 2023] Steevens, P.: 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.security-nl.2023-10-02.link.link.