MITARBEITERINFORMATION

Mitteilung über kürzlich aufgetretenen Cyber-Vorfall

Liebe Mitarbeiterinnen und Mitarbeiter,

als international tätiges Unternehmen, das u. a. im Bereich kritische Infrastruktur in Asien tätig ist, registrieren wir, wie leider auch eine Vielzahl anderer in unserem Sektor tätigen Unternehmen und Versorgungsdienstleister, regelmäßige Angriffsversuche auf unsere IT-Infrastruktursysteme, die jedoch von unserem IT Infrastructure & Cyber Security Department sowie den externen Dienstleistern, mit denen wir in diesem Bereich kooperieren, in der Regel erfolgreich abgewehrt werden.

Über einen kürzlich aufgetretenen Cyber-Vorfall wollen wir Sie gleichwohl im Einklang mit den maßgeblichen rechtlichen Vorschriften der Datenschutz-Grundverordnung (DSGVO) informieren, auch wenn weder der laufende Betrieb unserer IT-Systeme, Webseiten und Portale unterbrochen wurde noch dem Unternehmen oder unseren Kunden ein finanzieller Schaden entstanden ist, da wir derzeit einen unberechtigten Zugriff auf Teile personenbezogener Daten nicht ausschließen können.

Auch die in der aktuellen Presseberichtserstattung des Handelsblatts aufgebrachten Behauptungen eines Datenverlusts personenbezogener Daten u.a. von Mitarbeitern und Mitarbeiterinnen können von uns nach ersten Prüfungen weder nachvollzogen noch bestätigt werden. Wir nehmen grundsätzlich jeden, so auch diesen (Verdachts-)Vorfall sehr ernst. Die Sicherheit und der Schutz von Daten haben bei ThomasLloyd höchste Priorität. In unserem Haus gelten klare und verbindliche Richtlinien zur IT- und Datensicherheit. Hinweisen auf mögliche Datenlecks gehen wir unverzüglich nach. Den oben erwähnten Sachverhalt prüfen wir derzeit umfassend, dabei geht es zunächst um die Authentizität der Daten und sodann um die Frage, auf welche Weise Daten erlangt worden sein könnten. Nach aktuellem Kenntnisstand kann es sich allenfalls um einen lokal begrenzten Vorfall handeln.

Gerne möchten wir Ihnen einige Informationen über den Vorfall zur Verfügung stellen, damit Sie nachvollziehen können, was passiert ist, inwieweit Sie betroffen sein könnten, wie wir reagiert haben und welche zusätzlichen Schritte zum Schutz Ihrer Daten unternommen werden können, falls Sie dies wünschen.

Was ist passiert?

Kürzlich haben wir einen Vorfall festgestellt, der sich auf einen Teilbereich unserer internen IT-Systeme auswirkte. Als wir den Vorfall entdeckten, führten wir umgehend Reaktionsprotokolle aus, leiteten mit Unterstützung externer Cybersicherheits- und Forensik-Experten eine Untersuchung zur Analyse des Vorfalls ein und implementierten unsere Business-Continuity-Pläne, um Störungen für unseren Geschäftsbetrieb zu minimieren und den Fortbestand der Sicherheit unserer IT-Systeme bestmöglich zu gewährleisten. Ziel der Zusammenarbeit mit unseren Experten war, den Vorfall zunächst einzudämmen und vollständig zu beheben sowie Empfehlungen zur Stärkung unserer Sicherheitslage gegen potenzielle zukünftige Bedrohungen zu erhalten und diese zur Sicherung und Stärkung unserer IT-Systeme zu implementieren. Sobald der o.g. Cyberangriff erkannt wurde, haben wir den Zugriff auf weitere Systeme gestoppt. Es lag keine Unterbrechung des Regelbetriebs vor und Systeme wurden nicht verschlüsselt.

Welche Daten und Systeme sind betroffen?

Im betroffenen Online-Speicher werden u.a. auch personenbezogene Daten und Dateien abgelegt. Ein teilweiser Download dieser Daten und Dateien von den Servern sowie deren Veröffentlichung im Darknet kann zum jetzigen Zeitpunkt nicht vollständig ausgeschlossen werden. Wir haben keine Anhaltspunkte dafür, dass bei uns gespeicherte personenbezogene Daten missbraucht wurden oder werden. Personenbezogene Daten können grundsätzlich alle Daten sein, die im Rahmen von Vertragsschlüssen oder Vertragsdurchführung überlassen wurden. Explizit nicht betroffen sind Passwörter und damit der Zugang zu Kundenkonten. Grundsätzlich ist es nicht möglich, die mit ThomasLloyd Kundenkonten verbundenen Daten zu ändern, da dies die Autorisierung durch einen ThomasLloyd-Mitarbeiter erfordern würde. Über die Konten können ebenfalls keine direkten Zahlungen oder andere Transaktionen veranlasst werden.

Wie haben wir auf den Vorfall reagiert?

Um Ihre Daten bestmöglich zu schützen und das Risiko ähnlicher Vorfälle in der Zukunft zu begrenzen, haben wir, unmittelbar nachdem wir von dem Vorfall erfahren haben, eine vollständige Systemprüfung durchgeführt und umfangreiche Eindämmungsmaßnahmen eingeleitet, darunter die Isolierung unseres Netzwerks, die Verbesserung unserer Fähigkeiten zur Erkennung von Eindringlingen und die Stärkung unserer Reaktionsmechanismen. Wir haben

vorsorglich die maßgeblichen Behörden umfassend über den Vorfall informiert und diesen fristgerecht bei den zuständigen Aufsichtsbehörden für den Datenschutz angezeigt.

Was könnte mit Daten geschehen und mit welchen Folgen ist zu rechnen?

Es kann nicht vollständig ausgeschlossen werden, sofern doch personenbezogene Daten offengelegt wurden bzw. werden, dass diese im Internet zum Nachteil von Kunden oder Ihren Bevollmächtigten verwendet werden könnten oder Dritte sich als die betroffenen Personen ausgeben. Jeder Cyber-Vorfall birgt grundsätzlich unternehmensunabhängig vor allem die folgenden Risiken:

- Die Angreifer könnten personenbezogene Daten auf Darknet-Plattformen veröffentlichen und sie Dritten zugänglich machen,
- Die Angreifer oder Dritte, die Ihre Daten erlangt haben, könnten Ihnen E-Mails mit Schadsoftware im Anhang schicken. Wenn Sie die Anhänge einer solchen E-Mail öffnen, könnte Ihr Endgerät mit Schadsoftware verseucht werden,
- Die Angreifer oder Dritte könnten mit Ihnen Kontakt aufnehmen, um Sie mit den entwendeten bzw. veröffentlichten Daten zu erpressen,
- Sofern die Angreifer Kopien Ihrer Ausweise erlangt haben, kann es sein, dass mit diesen als Vorlage rechtswidrig gefälschte Ausweiskopien erstellt werden,
- Auch könnten Bankdaten verwendet werden, um zum Beispiel nicht autorisierte Geldtransfers auszulösen, wenn sie mit weiteren Daten kombiniert werden.
- Mit den Informationen zu Name, Kontodaten und E-Mail-Adresse könnten die Hacker Identitätsdiebstahl begehen. Es könnten auf Ihre Kosten und Gefahr zu Lasten der dort gespeicherten Zahlungsquellen anderweitig Waren bestellt werden. Dies gilt insbesondere, wenn Sie dasselbe Passwort für verschiedene Shopsysteme verwenden.

Was können Sie grundsätzlich tun?

Im Allgemeinen und als bewährte Praxis empfehlen wir Ihnen, hinsichtlich Phishing-Versuchen, einschließlich dem Risiko von Identitätsdiebstahl und Betrug insbesondere bei Nachrichten und bei E-Mails, die Ihnen ungewöhnlich vorkommen, stets wachsam zu sein und niemals ohne Bedacht auf Links zu klicken. Es gibt verschiedene Vorsichtsmaßnahmen, die Sie ergreifen können, um Ihre Daten zu schützen, u. a.:

- schützen Sie Ihre personenbezogenen Daten und melden Sie ungewöhnliche Aktivitäten,
- verwenden Sie komplexe Passwörter und ändern Sie diese regelmäßig,
- vermeiden Sie das Öffnen von verdächtig aussehenden E-Mail-Anhängen und
- überprüfen Sie regelmäßig Ihre Kontoauszüge und Kreditauskünfte auf betrügerische oder irreguläre Aktivitäten.
- Weitere Informationen und Handlungsempfehlungen zur Datensicherheit finden Sie auf der Webseite des Bundesamtes für Sicherheit und Informationstechnik.

Wir möchten Sie daran erinnern, dass ein derartiger Vorfall und die damit verbundenen Informationen grundsätzlich vertraulich sind. Gleichwohl haben wir an Dritte außerhalb des Unternehmens – einschließlich unserer Kunden, Geschäftspartner und anderen Interessengruppen – gleichlautende Informationen in einer Mitteilung aufgearbeitet, welche im Falle von Anfragen weitergegeben werden kann.

Wir bedauern aufrichtig, dass es unter den gegebenen Umständen notwendig war, Sie zu kontaktieren und danken Ihnen für Ihr Verständnis sowie Ihre Unterstützung. Die Sicherheit Ihrer Daten hatte stets und hat weiterhin oberste Priorität für uns. Wir können Ihnen daher versichern, dass wir alles tun werden, um die dauerhafte Belastbarkeit unserer IT-Systeme zu gewährleisten und zu verhindern, dass sich ein solcher Vorfall wiederholt.

Sollten Sie Rückfragen zum Vorfall oder dieser Mitteilung haben, können Sie sich jederzeit gerne an Ihren direkten Vorgesetzten (MD/C-Level) oder ihren HR-Ansprechpartner werden. Darüber hinaus können Sie sich gerne auch per E-Mail (gdpr@thomas-lloyd.com) an unseren Datenschutzbeauftragten, Herrn Lars-Holger Krause, wenden.

Abschließend möchten wir uns für Ihre Unterstützung und Ihr Engagement ausdrücklich bedanken.

Freundliche Grüße,

Miriam Plater
Chief People Officer