STORMSHIELD

MEINUNGEN

AUSTAUSCH VERTRAULICHER DATEN MIT DER AUSSENWELT: JA, MIT ANGEMESSENER SICHERHEIT

Jocelyn Krystlik
Business Unit Data Security Manager, Stormshield

Wenn es um Daten geht, kann jeder Austausch mit der Außenwelt Anlass zu Bedenken um deren Vertraulichkeit und Integrität werden, denn sobald diese Daten von einem Datenraum in einen anderen gelangen, können sie abgefangen, modifiziert oder unbrauchbar gemacht werden. Zum bestmöglichen Schutz gegen verschiedene Risiken müssen die für IT-Sicherheit zuständigen Teams eine Reihe bewährter Verfahren anwenden. Erläuterungen, um wieder Vertrauen zu fassen und gelassen zu handeln.

Alle Unternehmen und Institutionen sind gleichermaßen von den drei Hauptrisiken für Daten betroffen: Vertraulichkeit, Integrität und Verfügbarkeit. Aber wie kann man dann sein Unternehmen schützen und dem Personal trotzdem einen ungestörten Austausch ermöglichen?

DATEN ALS RISIKOMATERIAL FÜR CYBER-ANGRIFFE

Das Konzept des Datenschutzes ist daher eng **mit den Risiken in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit** verknüpft. In diesem Punkt laufen die Definitionen zusammen: Vertraulichkeit stellt sicher, dass eine Information nur für entsprechende befugte Personen zugänglich ist; Integrität gewährleistet, dass eine Information während ihres Lebenszyklus unverändert bleibt; und Verfügbarkeit sorgt dafür, dass eine Information innerhalb eines bestimmten Zeitraums zugänglich ist. Zusammen mit dem Begriff der Rückverfolgbarkeit sind diese Aspekte die grundlegenden Kriterien für Informationssicherheit.

Die allgemeine Antwort zum Schutz dieser Daten in Bezug auf Integrität und Vertraulichkeit heißt Verschlüsselung. Doch auch wenn eine solche Maßnahme notwendig ist, wird sie nicht unbedingt immer ordnungsgemäß umgesetzt. Ob wichtige Daten, vertrauliche oder kritische Daten, es ist leicht, sich in den mit diesem Thema verbundenen Begriffen zu verlieren. Viele Unternehmen glaubendaher, dass sie nicht betroffen sind und deswegen ihre Dateien und den Datenaustausch nicht schützen müssen. Dennoch sind **dieser notwendige Datenschutz alle Unternehmen etwas an**. Kundendateien, Buchhaltungsunterlagen oder andere wichtige Akten sind allesamt Elemente, die den täglichen Betrieb eines Unternehmens ermöglichen. Ein Jahr Buchhaltung für ein klein- bzw. mittelständisches Unternehmen zu verlieren, kann zum Beispiel katastrophal sein. Um sich zurechtzufinden, muss jeder definieren, welche Informationen für das jeweilige Unternehmen oder die Institution strategisch wichtig sind, wobei zu berücksichtigen ist, dass alle erzeugten Daten wertvoll sind.

„Ob wichtige Daten, vertrauliche oder kritische Daten, es ist leicht, sich in den mit diesem Thema verbundenen Begriffen zu verlieren. Viele Unternehmen glauben daher, dass sie nicht betroffen sind und deswegen ihre Dateien und den Datenaustausch nicht schützen müssen. Dennoch sind dieser notwendige Datenschutz alle Unternehmen etwas an.“

Parallel dazu muss man besser verstehen, wann **solche Daten zugänglich und damit für Angriffe anfällig** sind. Denn zum Erhalten von Datenzugang kann der Weg eines Cyberkriminellen über ein Terminal oder ein Netzwerk des Unternehmens führen – alles Elemente, die ebenfalls in die Logik des Cyberschutzes einzubeziehen sind. Im speziellen Fall eines Trojanerangriffs kann eine Gruppe von Cyberkriminellen z. B. Zugriff auf alles haben, was auf den Bildschirmen des infizierten Systems angezeigt wird, sowie auf Tastatureingaben. „*Solche Angriffe können sehr gezielt sein und von Staaten ausgehen*“, präzisiert **Sébastien Viou**, Direktor für Cybersicherheit und Berater für Cyber-Evangelismus bei Stormshield, zu diesem Thema. „*Trojaner, mit denen Passwörter und Zugangsdaten, insbesondere Bankdaten von Privatpersonen abgefangen werden, lassen sich auch durch einfaches Herunterladen eines Spiels, einer Erweiterung oder eines Passwortmanagers in großem Umfang einschleusen. Oft denken wir dabei nur an den*

Computer, aber auch das Smartphone ist ein großes Einfallstor für diese Art Malware..." Dies unterstreicht die Notwendigkeit des Schutzes von Arbeitsplätzen, nährt aber auch die Überlegung, berufliche Endgeräte auf berufliche Zwecke zu beschränken.

WIE KANN MAN SEINE DATEN BESSER SCHÜTZEN?

Ein Datensatz ist wertlos, wenn er in der hintersten Schublade oder in einem Verzeichnis Ihres Computers liegt. Häufig sind **Daten nur dann wertvoll, wenn sie gut zugänglich** sind. Bei diesem Austausch sind sie daher am anfälligsten, denn sie verlassen die (theoretisch) geschützte Enklave ihrer Speicherung.

Der Austausch kann dann verschiedene Formen annehmen: Informationen werden per E-Mail verschickt, in der Cloud abgelegt oder auf einem USB-Stick gespeichert. Dies sind unterschiedliche Methoden und vor allem Technologien, die jedoch auf **den gleichen „Sicherheitsreflex" zurückgreifen müssen: die Verschlüsselung überall von Daten.** Eine solche Verschlüsselung sorgt mithilfe eines robusten Authentifizierungsmechanismus dafür, dass die Informationen nur vom Absender und vom Empfänger gelesen werden können. Sie bleiben damit außerhalb der Reichweite von Eindringlingen, Neugierigen und sogar veröffentlichenden Personen, die daher keinen Zugang zu den Daten im Klartextformat haben. Aber **damit diese Verschlüsselung überall wirksam ist, ist sie jedoch unter der alleinigen Kontrolle des Unternehmens, das seine Daten schützen möchte, durchzuführen.** Die Schutzschlüssel, mit denen ausgetauschte Dateien verschlüsselt werden, müssen daher im alleinigen Besitz des Unternehmens bleiben, das seine Daten schützen will. Nur so kann der Schutz der Daten völlig unabhängig von ihrer Speicherung sein.

„Damit diese Verschlüsselung überall wirksam ist, ist sie jedoch unter der alleinigen Kontrolle des Unternehmens, das seine Daten schützen möchte, durchzuführen. Die Schutzschlüssel, mit denen ausgetauschte Dateien verschlüsselt werden, müssen daher im alleinigen Besitz des Unternehmens bleiben, das seine Daten schützen will."

Mit der mobilen Nutzung oder dem massiven Einsatz von Tools für die Zusammenarbeit werden einige Datenfreigaben jedoch nicht durchgängig vom Unternehmen kontrolliert. Bei der Nutzung bestimmter SaaS-Bürosoftwaresuiten kann die Bereitstellung einer unabhängigen Datenverschlüsselungslösung die tatsächliche Vertraulichkeit der dort übertragenen Daten gewährleisten. Angesichts der einfachen Nutzung dieser Online-Office-Suiten besteht die Herausforderung für die Lösungsanbieter darin, sie für Endbenutzer nahtlos zu integrieren und so für **unter Beibehaltung eine einfachen und effektiven Benutzererfahrung für entsprechende Sicherheit zu sorgen.** Nach Dateien und E-Mails müssen Daten nun direkt in Webbrowsern überall verschlüsselt werden.

DIE BEDEUTUNG VON DATENSICHERUNG UND ZUGRIFFSRECHTEN

Wenn die Datenverschlüsselung den zwingenden Anforderungen an Integrität und Vertraulichkeit gerecht wird, wie sieht es dann mit der Verfügbarkeit aus? Denn **Daten, die für alle zugänglich sind, selbst wenn sie verschlüsselt sind, können immer noch ... gelöscht werden.** So muss in einem ersten Schritt für eine wirksame Sicherung gesorgt werden. Sébastien Viou fasst zusammen: *„Die Datensicherung sollte regelmäßig getestet werden und verschlüsselt sowie offline oder unveränderbar sein.“* Sie ist von IT- und Geschäftsteams mit gemeinsamer Verantwortung anzugehen, um alle notwendigen Parameter einschließlich der Verwaltung des Wiederherstellens von Verschlüsselungsgeheimnissen zu berücksichtigen. Es ist auch besser, einen Notfallplan (Disaster Recovery Plan, DRP) oder einen Geschäftskontinuitätsplan (Business Continuity Plan, BCP) zu erstellen, der in einem sicheren digitalen oder nicht-digitalen Raum gespeichert wird.

Parallel dazu muss auch die Verwaltung der Zugriffsrechte auf die Daten antizipiert werden. Dies soll sicherstellen, dass sowohl intern als auch extern nur befugte Personen auf sensible Daten zugreifen können. Dies ist jedoch ein komplexes Thema, denn die Verwaltung von Zugriffsrechten und Zugängen (*Identity and Access Management* – IAM) betrifft alle Verantwortlichen in jeder Abteilung oder jedem Geschäftsbereich eines Unternehmens. Sie müssen in der Lage sein, zu bestimmen, wer in seinem Team Zugriff auf was hat und wer was tun darf. Eine einfache Darstellung, aber im Verhältnis zur wachsenden Anzahl von Tools und dem Phänomen der Fluktuation in Unternehmen kann die flüssige Verwaltung von Zugriffsprivilegien schnell zu einer echten *„ewigen Baustelle“* werden. Aber es ist ein notwendiges Projekt, das zur Sicherheit des Unternehmens beiträgt.