MEINUNGEN

ZEIGEN SIE MIR SENSIBLE DATEN AUF

Victor Poitevin
Editorial & Digital Manager, Stormshield

Personenbezogene Daten, sensible Daten, kritische Daten, lebenswichtige Daten... Das zur Beschreibung von Daten verwendete Vokabular ist vielfältig. Das führt auch dazu, dass einige Unternehmen und Organisationen glauben, dass sie für ihren Schutz nicht zuständig sind. Aber ist das wirklich der Fall? Sind die von der Datenschutz-Grundverordnung hervorgehobenen personenbezogene Daten nicht der sprichwörtliche Baum, hinter dem sich der Wald verbirgt? Alle Unternehmen generieren Daten, ohne sich deren Wert immer bewusst zu sein, und sind sich nicht im Klaren, dass sie zu schützen sind.

Seit ihrem Inkrafttreten im Mai 2018 in Europa hat die Datenschutz-Grundverordnung (DSGVO) zur Verbreitung neuer Begriffe beigetragen: personenbezogene Daten und sensible Daten. Ein kurzer Blick auf Suchmaschinen zeigt, wie sehr sensible Daten derzeit in aller Munde sind. Aber wovon genau sprechen wir? Bei näherer Betrachtung ist der Umfang sensibler Daten eher begrenzt und ihre stringente Definition ist bei weitem nicht die Ursache aller Datenprobleme eines Unternehmens. Und dennoch...

WAS SIND SENSIBLE DATEN?

Die von der Europäischen Kommission in der Datenschutz-Grundverordnung veröffentlichte Liste sensibler Daten ist eindeutig. Dabei handelt es sich um personenbezogene Daten einer Person, d. h. Informationen über die rassische bzw.ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten, das Sexualleben oder die sexuelle Orientierung.

Die Verarbeitung dieser Daten, einschließlich ihrer Erhebung und Verwendung ist gesetzlich streng geregelt. Aber sind sie die einzigen, die besonderen Schutz benötigen? *Spoiler-Alarm*: nein.

SENSIBLE, KRITISCHE, LEBENSWICHTIGE DATEN...

Die Datenvielfalt in einem Unternehmen ist weitaus größer als nur sensible Daten. In ihrem Leitfaden für die IT-Hygiene (auf Französisch: „guide d'hygiène informatique") bezieht sich die französische Informationssicherheitsbehörde ANSSI auf „*Daten, die für die Organisation und die betroffenen Server als lebenswichtig angesehen werden*". Ein neuer Begriff für die Diskussion von Daten. Was ist dann der Unterschied zwischen sensiblen Daten und lebenswichtigen Daten? Bei letzteren handelt es sich um Daten, die als wesentlich für das reibungslose Funktionieren eines Unternehmens angesehen werden: Produktionsdaten, Finanzdaten, F&E-Daten (z. B. das Geheimrezept für ein Getränk oder der Algorithmus einer Suchmaschine). Ohne sie existiert das Unternehmen nicht mehr oder verliert seinen Wettbewerbsvorteil. Dabei handelt es sich um Daten, die im Falle ihrer Weitergabe, ihres Diebstahls oder Verlusts kritische Auswirkungen auf das Unternehmen oder die Organisation haben würden, die sie verliert, zum Beispiel Daten aus einer laufenden Verhandlung, einem Fundraising oder einer bevorstehenden Übernahme. Aber nicht nur das. Wenn ein einziges Auftragsbuch neutralisiert wird, kann die gesamte Tätigkeit eines Kleinstunternehmens bzw. Klein- oder mittelständischer Unternehmen ins Stocken geraten. **Das Spektrum zu schützender Daten ist also viel breiter als nur sensible Daten**. All diese Daten sind das Ziel von Cyberkriminellen. „*In der Tat sind immer mehr kleine Organisationen Angriffen ausgesetzt, die ihre Daten unzugänglich machen*", betont die ANSSI in ihrem Leitfaden. Als solche müssen sie einer besonderen Wachsamkeit unterliegen und mit regelmäßigen Datensicherungen (Backups) auf nicht angeschlossenen Geräten gesichert werden, deren Wiederherstellung ebenfalls regelmäßig zu überprüfen ist.

„Oft denken wir zuerst an strategische Daten: Personal- oder Finanzdaten, F&E- oder Produktionsdaten... Aber alle von Unternehmen generierten Daten haben einen Wert. Wenn man sich die Zeit nimmt, sie zu erstellen, tragen sie zum Geschäft bei. Sie müssen daher ebenfalls geschützt werden."

Julien Paffumi, Senior Product Manager bei Stormshield

Personenbezogene Daten, sensible Daten, lebenswichtige Daten oder sogar kritische Daten – die zu schützenden Daten sind von Organisation zu Organisation unterschiedlich: Know-how über chemische Prozesse, Forschung und Entwicklung, Standort von Rohstoffen, internes Audit (Schutz von Zahlen, Investitionen usw.), Austausch zwischen Mitgliedern der Geschäftsleitung, Übernahmen/Beteiligungen, Personaldaten, Buchhaltungsdaten, Austausch zwischen einem Journalisten und seinen Quellen, Produktionslinie, Plan eines Industrieteils usw. „*Bei Stormshield erfolgt der Austausch von Lebensläufen zum Beispiel über verschlüsselte E-Mails, und gemeinsam genutzte Personaldaten werden in sicheren Verzeichnissen gespeichert*“, so **Jocelyn Krystlik**, Business Unit Data Security Manager bei Stormshield. „*Kritisch sind Daten, die das Kerngeschäft eines Unternehmens betreffen, oder das, was es ausmacht: Patente, kommerzielle Aktivitäten, Finanzdaten, strategische Daten... Also alles, was einen von Kunden anerkannten Wert hat. Wir müssen daher in Bezug auf Informationen und deren strategische Bedeutung für das Unternehmen denken*“, fasst **Laurence Houdeville**, Datenspezialist und Mitherausgeber des Weißbuchs „*Le cloud de confiance, un enjeu d'autonomie stratégique pour la France*“ (*Die datensichere Cloud, eine strategische Autonomiefrage für Frankreich*), zusammen. Es geht also um „verfeinerte“ Daten, dies ist aber nicht das Einzige.

„*Alle oder fast alle Daten eines Unternehmens sind wichtig und nützlich*“, so **Julien Paffumi**, Senior Product Manager bei Stormshield. *Oft denken wir zuerst an strategische Daten, von Personal- und Finanzdaten bis hin zu F&E- oder Produktionsdaten... Aber alle vom Unternehmen generierten Daten haben einen Wert. Wenn man sich die Zeit nimmt, sie zu erstellen, tragen sie zum Geschäft bei. Sie müssen daher ebenfalls geschützt werden. Dies gilt auch für unstrukturierte Daten.*“ Laut Gartners „*Magic Quadrant for Distributed File Systems and Object Storage*“, liegt die jährliche Wachstumsrate unstrukturierter Daten zwischen 30 und 60 %, und laut einer Thales-Studie verschlüsseln nur 17 % der Unternehmen mindestens die Hälfte ihrer Daten in der Cloud. Diese beiden Zahlen zeigen, dass Datenschutz ein wichtiges Thema ist. Aber wie soll das gehen?

IDENTIFIZIERUNG UND KLASSIFIZIERUNG VON DATEN ZUM OPTIMALEREN SCHUTZ

Laut Laurence Houdeville „*schützt man nur das gut, was man gut kennt*“. **Die erste Herausforderung des Datenschutzes besteht also darin, dass man die eigenen Datenbestände kennt**. Konkret bedeutet dies, dass durch automatisierte bzw. unautomatisierte Datenverarbeitung verarbeitete Daten (z. B. Kundendateien, Verträge) und die Datenträger, auf denen sie sich befinden, identifiziert werden müssen – in Bezug auf Hardware (z. B. Server, Laptops, Festplatten), Software (z. B. Betriebssystem, Unternehmenssoftware), aber auch Kommunikationskanäle (z. B. Glasfaser, WLAN, Internet).

„Man schützt nur das gut, was man gut kennt.“

Laurence Houdeville, Datenspezialist

„Wir führen eine Bestandsaufnahme mit einer Karte durch, die Referenzdaten zeigt, und stellen uns die Frage, welche Daten am wertvollsten sind und wann sie verwendet werden. Interessant sind also nicht die Nutzdaten, sondern die verfeinerten, mit Querverweisen versehenen Daten", so Laurence Houdeville. *Dann arbeiten wir am kritischen Pfad: Wie werden diese Daten mit anderen in Beziehung gesetzt, nach welchem Kriterium haben diese Daten einen Wert, usw.* Nach der Prüfung wird ermöglicht uns die Klassifizierung der Daten die Bestimmung der Kritizitätsgrades der Daten und damit ihrer Vertraulichkeit und Verteilung. Es gibt jedoch keine einheitliche Nomenklatur. *„Jede Organisation hat ihr eigenes Klassifizierungsniveau: C1, C2, C3 (vertrauliche 1. Stufe usw.); D1, D2, D3; intern oder extern... und sogar nach Farbe (gelb/rot...)*, erklärt Jocelyn Krystlik. *Es gibt keine Normung, jeder macht ein bisschen von dem, was er will, auch wenn der Inhalt mehr oder weniger derselbe bleibt.„* Dies ist, wie so oft, eine Frage der „Cyber-Reife".

REIFEGRAD VON ORGANISATIONEN IN BEZUG AUF DATEN

Für die Klassifizierung von Daten gibt es verschiedene Lösungen: eine von allen verwendete Vorlage mit auszufüllenden Feldern, ein Wasserzeichen in der Datei oder eine automatische Klassifizierung nach Wörtern oder Schlüsselinformationen (Sozialversicherungsnummer, Bankkundennachweis usw). *„Kleinere Unternehmen bieten oft eine E-Mail-Vorlage an, bei der Nutzer durch Ankreuzen des jeweiligen Kästchens die Klassifizierung selbst vornehmen*", so Jocelyn Krystlik. *Großunternehmen verfügen oft über Tools, die automatisch Schlüsselwörter erkennen, die Daten gegebenenfalls verschlüsseln oder sie sogar daran hindern, das Unternehmen zu verlassen, wenn sie nicht zur Weitergabe zugelassen sind.*"

Das Einstufungsverfahren kann von einer Organisation zur anderen variieren. Wo es ein solches gibt, legt der Datenschutzbeauftragte (DSB) in der Regel den Einstufungsrahmen fest, und dann ist es Sache des Datenproduzenten, zu entscheiden, ob dessen Daten vertraulich sind oder nicht. Dies wirft **die Frage der digitalen Hygiene** auf. Um Daten zu klassifizieren, zu schützen bzw. ihre Weitergabe einzuschränken, muss sich ihr Eigentümer oder Erzeuger über ihren Wert im Klaren sein. *„Es geht darum, vorsichtig damit zu sein, was man an wen sendet. Das ist „digitale Hygiene", aber sie setzt auch einen gewissen Reifegrad des Unternehmens in Bezug auf Daten und die Schulung des Personals in diesem Bereich und seinen Herausforderungen voraus*", erläutert Julien Paffumi. Dies wirft auch die Frage auf, wie diese Expertise unterhalten werden kann. *„Angesichts der Tatsache, dass das Cyber-Thema noch immer nicht im Alltag angekommen ist, müssen wir feststellen, dass Datenschutzbeauftragte von Unternehmen das Personal jedes Jahr in Bezug auf Datenschutzregeln schulen müssen.*" Das ist eine zeitaufwändige, aber unverzichtbare Praxis.

Die Frage des Reifegrads stellt sich auch bei der Absicherung. *„Datensicherung ist ein Thema, das von mehreren Personen angegangen werden muss*“, warnt Julien Paffumi. *Die Verantwortung wird zwischen der IT-Abteilung und dem Unternehmen aufgeteilt. Das Unternehmen muss feststellen, ob es über Daten verfügt, die für das Unternehmen wertvoll sind, und wie problematisch deren Zerstörung, Verlust oder Diebstahl sein kann. Es engagiert sich daher stark für seinen Schutz. Die IT-Abteilung muss sich dieser Daten bewusst sein, um die richtigen Tools und die richtige Infrastruktur zu deren Schutz bereitzustellen und sicherzustellen, dass sie sich bei Bedarf wiederherstellen lassen. Ziel ist das Vermeiden einer „Schattensicherung“ bzw. „Schattendatenspeicherung“, „bei der Unternehmensteams eine Lösung auf ihrer Seite betreiben und ihre Daten ohne Wissen der IT-Abteilung bzw. des Sicherheitsteams auf einem Server oder einer Cloud-Speicherlösung speichern.“* Das sieht auf dem Papier einfach aus, ist aber in der Realität dramatisch komplex, besonders wenn Schatten-IT ins Bild rückt...

Zusammenfassend lässt sich sagen, dass die Datensicherheit auf einem globalen Ansatz beruht, der den Schutz des Umfelds, der Arbeitsplätze und der Daten miteinander verbindet. *„Keinerlei Daten sind wirklich irrelevant. Es besteht daher ein echter Bedarf an verschiedenen Schutzschichten: Firewalls für Netzwerke, Endpunktlösungen für Workstations, Verschlüsselungs- oder Data Loss Prevention (DLP)-Lösungen für die Daten selbst*“, so Julien Paffumi. *Und man muss strenge Datenschutzrichtlinien umsetzen.*“ „Schließlich ist es am besten, einen Disaster Recovery Plan (DRP) bzw. einen Business Continuity Plan (BCP) zu haben. Diese können sie ausdrucken und an einem sicheren Ort aufbewahren oder sie in digitaler Form auf einem gesonderten und isolierten Server aufbewahren, damit sie nicht verschlüsselt werden!