DOPPELTER NUTZEN FÜR DATENSICHERHEIT

Bild: fd-123f

Für die Umsetzung der EU-DSGVO haben Unternehmen zum Schutz der personenbezogenen Daten geeignete Prozesse und Technologien etabliert. Diese können sie auch nutzen, um ihr geistiges Eigentum vor Verlust und Diebstahl zu schützen und so ihren weiteren wirtschaftlichen Erfolg sicherzustellen.

Autor: Michael Bauner
Redaktion: Axel Pomper

➤ Dass Unternehmen personenbezogene Daten vor dem Zugriff Nicht-Berechtigter schützen müssen, fordert die DSGVO. Bußgelder bei Verstößen und drohender Vertrauensverlust bei den Kunden erzeugen Handlungszwang, Datenschutzkonzepte zu erarbeiten und umzusetzen und in geeignete Maßnahmen sowie Technologien zu investieren. Neben personenbezogenen Daten verfügt jedes Unternehmen über Daten, deren Schutz es in seinem eigenen Interesse für den Fortbestand der Firma sicherstellen muss: sein geistiges Eigentum. Dieses ist noch stärker als personenbezogene Daten von Diebstahl und Verlust bedroht. Und die Anfälligkeit nimmt mit der Digitalisierung rapide zu, denn Datenbestände wachsen schnell, die Zahl der Kommunikationskanäle steigt stetig und immer mehr Mitarbeiter, Zulieferer und Kunden haben täglich mit sensiblen Informationen zu tun.

Riskantes Verhalten wird toleriert

Anders als bei der DSGVO ist es Unternehmen selbst überlassen, wie sie mit ihrem Know-how und den Betriebs- und Geschäftsgeheimnissen umgehen. Zwar hat sich der Schutz vor externen Angriffen, beispielsweise mittels Firewall, flächendeckend durchgesetzt, aber das Bewusstsein für den Wert interner Informationen und den Umfang der Risiken bei Diebstahl oder Verlust ist wenig ausgeprägt. Wenn Mitarbeiter beispielsweise private Smartphones, für Consumer entwickelte Cloud-Tools oder private E-Mail-Accounts für die Arbeit benutzen, drücken viele Unternehmen nach wie vor ein Auge zu, statt über die Risiken aufzuklären, Richtlinien vorzugeben, zu überwachen und sichere Alternativen anzubieten.

Weil es so einfach ist, nimmt beispielsweise ein ehemaliger Mitarbeiter die Kundenliste zum Wettbewerber mit. Wirbt er damit die Kunden ab, bedroht das die Existenz des Unternehmens ebenso wie ein drohendes Bußgeld infolge einer Datenschutzverletzung. Informationen wie Kundenkontakte, Angebotsunterlagen und Daten aus der Produktentwicklung sind bares Geld wert oder verschaffen anderen einen zeitlichen Vorsprung. Den Schaden, der der deutschen Industrie in den vergangenen beiden Jahren durch das Komplettpaket aus Sabotage, Datendiebstahl und Spionage entstanden ist, beziffert der IT-Branchenverband Bitkom mit 43,4 Milliarden Euro. Möglicherweise ist das aber nur die Spitze des Eisbergs.

Großunternehmen und KMU sind gleichermaßen bedroht

Das Ziel von Wirtschaftsspionage und Konkurrenzausspähung sind nicht nur Großunternehmen und Konzerne, sondern ebenso KMU quer durch alle Branchen. Ihre Stärke ist es, sich mit großer Innovationskraft ihren Platz neben den Großen zu erobern und zu behaupten. Manches kleinere Unternehmen hat es zum weltweiten Marktführer in seinem Segment gebracht: sogenannte Hidden Champions. Wer da denkt, seine Daten seien uninteressant oder wertlos für Dritte, irrt sich gewaltig, denn jede Firma hat Wettbewerber und möglicherweise unzufriedene Angestellte. Untersuchungen aus dem Forschungsprojekt Wiskos (Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa) zeigen, dass in den vergangenen fünf Jahren etwa die Hälfte der KMU einen Spionagevorfall oder einen konkreten Verdachtsfall erlitten hat.

Risiko Innentäter

Das Risikopotenzial der eigenen Mitarbeiter wird dabei häufig unterschätzt. Sie kopieren in guter Absicht Unterlagen auf USB-Sticks, um zuhause weiterzuarbeiten, oder übermitteln versehentlich Daten an den falschen Adressaten. Aus Verärgerung oder Frust nehmen sie bei einem Arbeitgeberwechsel Daten mit, laut einer Dell-Untersuchung eine Art Volkssport in Deutschland, dem mehr als die Hälfte der Arbeitnehmer nachgehen. Wiskos-Ergebnissen zufolge sind Mitarbeiter für gut ein Drittel (34 Prozent) aller Spionagevorfälle verantwortlich, wobei ihnen das Wissen über Kunden, Produkte und Investitionen hilft, wertvolle Informationen zu identifizieren. In 15 Prozent der Vorfälle liegt darüber hinaus eine Kombination von Außen- und Innentäterschaft vor, bei denen Mitarbeiter beispielsweise mittels Social Engineering dazu gebracht werden, wichtige Informationen herauszugeben.

Die DSGVO als Denkanstoß

Die Umsetzung der DSGVO lässt sich eins zu eins auf den Schutz des geistigen Eigentums übertragen: Die Maßgabe aus Artikel 5, personenbezogene Daten in einer Weise zu verarbeiten, die sie vor unbefugter Verarbeitung und vor unbeabsichtigtem Verlust durch geeignete Maßnahmen schützt, erzeugt bei der Anwendung auf Geschäfts- und Firmengeheimnisse sowie Informationen zu kritischen Infrastrukturen unmittelbare Sicherheit. Daran müssen die Unternehmen aus wirtschaftlichen Gründen ein vitales Interesse haben, um negative Auswirkungen von Datendiebstahl und -verlust auf ihre Marktstellung zu verhindern.

Der Schutz des geistigen Eigentums kann dabei auf wirtschaftliche Weise umgesetzt werden. Die Systeme und Prozesse, die ein Unternehmen für die Absicherung der personenbezogenen Daten im Rahmen der DSGVO eingerichtet hat, lassen sich ohne zusätzliche Investitionen für alle weiteren sensiblen Daten nutzen.

Unerwünschte Datentransfers verhindern

Zu den technischen Hilfsmitteln, mit denen sich unbefugter Zugriff und Datenverlust verhindern lassen, gehört das Berechtigungsmanagement. Da zugriffsberechtigte Mitarbeiter in der Regel auch Daten aus den zentralen Systemen exportieren, auf ihren Desktops speichern und von dort aus auf mobile Geräte übertragen, in Cloud-Speicher laden oder über Webmail-Dienste verschicken können, müssen diese Aktionen ebenfalls überwacht werden.

Data Loss Prevention ergänzt das statische Berechtigungsmanagement durch eine dynamische inhaltbasierte Kontrolle. Daten in Bewegung werden auf voreingestellte Inhaltskriterien untersucht und nicht erlaubte Transfers über E-Mail oder browserbasierte Anwendungen blockiert. Zudem verhindert eine DLP-Lösung beispielsweise, dass Mitarbeiter Geräte wie USB-Sticks an die Arbeitsplatzrechner anschließen können. Bei zugelassener Verwendung von USB-Sticks stellt die Lösung darüber hinaus die Verschlüsselung von Daten auf dem Stick sicher.

Die Richtlinien für Daten in Bewegung finden zudem für die Suche nach ruhenden Daten Verwendung, die sich in unstrukturierter oder semistrukturierter Form auf lokalen Festplatten der Arbeitsplatzrechner sowie in Cloud-Speichern wie Dropbox, OneDrive, iCloud und Google Drive befinden. Die Suchergebnisse werden als Report ausgegeben, sodass die Daten gelöscht oder verschlüsselt werden können. Die auf personenbezogene Daten zugeschnittenen Richtlinien der DLP-Lösung dienen dabei als Vorlage für den Schutz des geistigen Eigentums. Mit denselben Werkzeugen werden unter Nutzung individueller Wörterbücher sowie Dateityp- und Semantik-Erkennung unternehmensspezifische Richtlinien konfiguriert.

Doppelter Nutzen

Unternehmen sollten das Budget, die Prozesse und die Lösungen, die für den Schutz der personenbezogenen Daten aufgewendet werden, zusätzlich für den Schutz des geistigen Eigentums nutzen. Lösungen für Data Loss Prevention sind heute ausgereifte Systeme mit umfassender Funktionalität zum Schutz vor nicht erwünschtem Datenabfluss. Unternehmen können sie für sämtliche Inhalte einsetzen, die im Rahmen internationaler Standards und gesetzlicher Vorgaben zu schützen sind, und gleichermaßen für Daten, die geistiges Eigentum oder sonstige immaterielle Werte repräsentieren. So entsteht doppelter Nutzen bei gleichen Kosten.

Michael Bauner ist Geschäftsführer bei Endpoint Protector