Datenschutz vs. IT-Security:

Darauf sollten Unternehmen achten

IT-Security-Lösungen dienen sowohl der Datensicherheit als auch dem Datenschutz. Aber sie sammeln und analysieren in manchen Fällen selbst Daten, die laut Datenschutzgrundverordnung (DSGVO) als personenbezogen gelten. Was müssen Unternehmen hierbei beachten?

Von Richard Werner, Trend Micro

IT-Security und Datenschutz: Beides ist heute unverzichtbar. Unternehmen sind in der Pflicht, wirksame Schutzmaßnahmen gegen Cyberangriffe zu treffen. Tun sie dies nicht und werden dadurch Menschen geschädigt, drohen unter anderem zivilrechtliche Folgen. Geschäftsführer, Vorstände und Aufsichtsräte können zudem persönlich in Haftung genommen werden. Gleichzeitig müssen Unternehmen die europäische Datenschutzgrundverordnung (DSGVO) einhalten. Dafür sind angemessene technische und organisatorische Maßnahmen nach Stand der Technik vorgeschrieben. IT-Security-Software trägt also entscheidend dazu bei, den Datenschutz zu gewährleisten. Gleichzeitig steht sie aber auch selbst im Spannungsfeld mit der DSGVO. Denn häufig sammeln Security-Lösungen Daten, die im rechtlichen Sinne als personenbezogen gelten.

Datenerhebung bei einem Angriff via E-Mail

Über 90 Prozent aller Cyberangriffe starten mit einer E-Mail. Selbstverständlich überwachen Unternehmen diesen Übertragungsweg deswegen auch am genauesten. Häufig ist nicht die initiale E-Mail als Schadcode identifizierbar, vielmehr dient sie lediglich als Vehikel, um einen Eintrittspunkt in das Unternehmen zu schaffen. Empfänger werden zum Beispiel dazu aufgefordert, einen Link anzuklicken, eine Software herunterzuladen oder einen Anhang zu öffnen. Erst diese nachgelagerte Aktion löst dann einen Alarm aus. Solche Angriffe verlaufen millionenfach nach dem gleichen Muster. Daher sind Informationen zum Versandweg und zur Infektionstechnik sehr wertvoll, um Cyberattacken zu bekämpfen. Moderne Security-Werkzeuge loggen auch mit, dass der Nutzer den Link anklickt oder den Anhang öffnet.

Für Betreiber kritischer Infrastrukturen sind Systeme zur Angriffserkennung laut IT-Sicherheitsgesetz vorgeschrieben. Aber auch für alle anderen Unternehmen sind sie wichtig, um komplexe, mehrstufige Cyberattacken frühzeitig aufzudecken. Denn häufig erstrecken sich diese über mehrere Wochen oder gar Monate. Währenddessen spionieren Cyberkriminelle Netzwerke aus, versuchen privilegierte Rechte zu erlangen und Security-Systeme auszutricksen. Nur indem man einzelne Indikatoren für Kompromittierungen sammelt und im Zusammenhang betrachtet, wird der Angriff offensichtlich. Dann lässt er sich stoppen, bevor es zur Verschlüsselung oder anderweitigem Schaden kommt.

Darf Security-Software personenbezogene Daten sammeln?

Laut DSGVO ist die Verarbeitung von personenbezogenen Daten nur dann erlaubt, wenn sie auf rechtmäßige Weise erfolgt und zweckgebunden ist. Um den Grundsatz der Rechtmäßigkeit zu erfüllen, müssen Unternehmen in den meisten Fällen die freiwillige, ausdrückliche Einwilligung einer betroffenen Person einholen. Aber gilt das auch für die Security? Haben Mitarbeiter oder unbeteiligte Dritte ein Mitspracherecht, wenn es um ihre personenbezogenen Daten im Hinblick auf die IT-Sicherheit geht?

Tatsächlich ist laut DSGVO keine Einwilligung vorgeschrieben, wenn die Datenverarbeitung „zur Wahrung der berechtigten Interessen des Unternehmens oder eines Dritten erforderlich ist“, sofern diese Interessen mehr wiegen als die Interessen der betroffenen Person. Das ist beim IT-Schutz der Daten der Fall und gilt auch für die Verarbeitung von personenbezogenen Daten durch An-

bieter von Sicherheitstechnologie und -diensten. So steht es in den Erwägungsgründen der Datenschutz-Grundverordnung. Allerdings muss die Datenverarbeitung unbedingt nötig und verhältnismäßig sein, um die Netz- und Informationssicherheit zu gewährleisten. Unternehmen sind in der Pflicht, dies sorgfältig zu prüfen und ihre Interessensabwägung zu dokumentieren.

Datenschutzrechtliche Pflichten

Security-Lösungen, die personenbezogene Daten temporär speichern und verarbeiten, sind also datenschutzrechtlich zulässig. Unternehmen können sie einsetzen, ohne die Einwilligung der betroffenen Personen für die Datenverarbeitung einzuholen. Allerdings schreibt die DSGVO umfassende Informationspflichten vor. Unternehmen müssen die betroffene Person zum Beispiel über ihre Kontaktdaten, den Zweck, die Rechtsgrundlage, den Empfänger der personenbezogenen Daten, eine etwaige Übermittlung an ein Drittland außerhalb der EU sowie gegebenenfalls über ihren Datenschutzbeauftragten unterrichten. Diese Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erteilt werden.

Außerdem müssen die eingesetzten Security-Lösungen datenschutzgerecht gestaltet sein und datenschutzfreundliche Voreinstellungen haben. Dazu zählt zum Beispiel, dass man nur Daten erhebt, die unbedingt erforderlich sind, und diese nur zeitlich begrenzt speichert. Der Schutz der Daten ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten. Empfehlenswert sind zum Beispiel Verschlüsselung, Pseudonymisierung und Anonymisierung von personenbezogenen Daten. Zudem gilt es, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sicherzustellen.

Wie sieht es bei der Auftragsdatenverarbeitung aus?

Unternehmen sind auch dann für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich, wenn eine sogenannte Auftragsdatenverarbeitung vorliegt. Ob das der Fall ist, gilt es im Einzelfall zu prüfen. Bei den meisten Security-Lösungen erfolgt die Datenverarbeitung auf den Servern des Security-Anbieters. Eine Auftragsverarbeitung ist dadurch gekennzeichnet, dass der Auftragnehmer den Weisungen des Auftraggebers unterliegt. Das ist bei komplexen Security-Anwendungen oft nicht möglich, weil den Kunden hierfür das fachliche Know-how fehlt. Bei der Ausgestaltung der Vereinbarung mit dem Security-Anbieter sollten Unternehmen daher klären, ob eine Auftragsverarbeitung nach Artikel 28 DSGVO oder eine gemeinsame Verantwortlichkeit von Security-Anbieter und Kunde gemäß Artikel 26 DSGVO vorliegt. In letzterem Fall ist genau festzulegen, wer welche Verpflichtungen übernimmt.

Als Anbieter im Bereich Cybersicherheit, der in über 65 Ländern tätig ist, verfolgt Trend Micro einen umfassenden und ganzheitlichen Datenschutzansatz. Wir haben ein Programm zur DSGVO-Compliance eingeführt, um die Verantwortlichkeiten als Datenverarbeiter gemäß der DSGVO zu erfüllen. Außerdem stellt Trend Micro in seinem Trust Center detaillierte Informationen zu allen Produkten und Lösungen bereit, die genau aufzeigen, welche personenbezogenen Daten verarbeitet werden, auf welche Weise und für welche Zwecke.

Leitfaden klärt rechtliche Fragen

Die Erfahrung zeigt, dass auch Mitarbeiter innerhalb der IT-Sicherheits-Abteilung in puncto Datenschutz oft verunsichert sind. Das führt mitunter dazu, dass sie Funktionen von Security-Lösungen deaktivieren, um einen vermeintlichen Verstoß gegen die DSGVO zu vermeiden. Doch gerade moderne Lösungen zur Angriffserkennung wie Extended Detection & Response (XDR) speichern und verarbeiten temporär personenbezogene Daten. Sie korrelieren und analysieren Anzeichen für Cyberattacken über alle Angriffsvektoren hinweg und fügen diese zu einem ganzheitlichen Bild zusammen. Unternehmen brauchen solche Lösungen, denn mit dem zunehmenden Einsatz von Cloud-Services, IoT und New-Work-Konzepten werden IT-Umgebungen immer größer, komplexer und unübersichtlicher.

Datenschutz in der IT-Security ist ein wichtiges Thema. Rückfragen dazu sind berechtigt und kommen häufig vor. Daher hat Trend Micro einen externen Fachanwalt beauftragt, die entsprechenden Security-Lösungen auf ihre DSGVO-Tauglichkeit zu prüfen. Er klärt wichtige Fragen des IT-Rechts und Datenschutzes in der mittlerweile siebten Auflage unseres juristischen Leitfadens, den man hier downloaden kann: https://bit.ly/3EcJE1q

Artikel und Leitfaden dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.