Newsletter Datenschutz

Ausgabe März | 2018

Newsletter der Sanovis GmbH

Liebe Leserin, lieber Leser,

das Jahr 2018 ist für den Datenschutz wegweisend. Mit der Europäischen Datenschutz-Grundverordnung wird das Datenschutzrecht erstmalig europaweit einheitlich geregelt. Gleichzeitig bedeutet dies für Unternehmen, dass neue Anforderungen umgesetzt werden müssen. Das Verzeichnis der Verarbeitungstätigkeiten ist eine davon. In der aktuellen Ausgabe des Newsletters lesen Sie, was sich dahinter verbirgt und wie Sie Ihr Unternehmen bei der Umsetzung unterstützen können.

Außerdem erfahren Sie, wie mit Mitgliederlisten in Vereinen umzugehen ist, welche Sicherheitsrisiken durch Hardware entstehen können und mit welchen Bedrohungen im Rahmen der IT in diesem Jahr zu rechnen ist.

Wir wünschen Ihnen wieder viele wertvolle Einsichten in den Datenschutz!

Ihr Dr. Uwe Günther, Geschäftsführer, Sanovis GmbH; Geschäftsfeldleiter Datenschutz, Curacon GmbH

Datenrisiken 2018: Mit welchen IT-Bedrohungen müssen wir rechnen?

2018 ist ein spannendes Jahr für den Datenschutz. Nicht nur die Datenschutz-Grundverordnung erwartet uns, auch die IT bringt viele Neuheiten. Leider sind damit zugleich neue Risiken verbunden.

Mehr als Malware-Attacken

Vielleicht haben Sie schon in der einen oder anderen Computer-Zeitschrift von den Prognosen für die Datensicherheit 2018 gelesen. Kaum ein IT-Anbieter lässt die Chance ungenutzt, seine Einschätzung dazu zu veröffentlichen. Virenschutz-Hersteller berichten naturgemäß von neuen Computer-Schädlingen, die uns 2018 bedrohen. Anbieter im Bereich der E-Mail-Sicherheit weisen auf die steigende Gefahr durch Phishing-Angriffe hin, die es auf Passwörter der Opfer abgesehen haben. Hier soll jedoch nun nicht eine weitere Liste der neuen IT-Gefahren folgen, sondern es geht um den richtigen Umgang mit neuen Risiken.

Die Vielzahl der Prognosen für 2018 kann verwirrend sein. Einige der Vorhersagen stimmen überein, andere führen IT-Bedrohungen auf, von denen man als Nutzer vorher noch nie gehört hat. Wichtig ist, sich weder davon beirren zu lassen noch sich vor den Meldungen über neue Gefahren zu verschließen. Die IT-Risiken für personenbezogene Daten sind so mannigfaltig wie die IT selbst. Mit jeder neuen App können neue Schwachstellen verbunden sein, jede zusätzliche Vernetzung mit dem Internet kann eine weitere Hintertür für Hacker öffnen.

Wenn Angriffe auf Schwachstellen treffen

Gefährlich für den Schutz der Privatsphäre wird es immer dann, wenn ein Angriff eine Schwachstelle in der IT ausnutzen kann. Wir werden 2018 sowohl bei den Attacken als auch bei den Schwachstellen auf Neuheiten stoßen.

Wir müssen uns darauf einstellen, dass die Angreifer neue Wege suchen, um an vertrauliche Daten zu gelangen. Das kann etwa die Smartwatch sein, die man ins Büro mitbringt und dort über Bluetooth oder WLAN mit dem Tablet verknüpft, um den morgendlichen Lauf abzuspeichern. Dazu muss die Fitness-App ins Internet. Gibt es in der Smartwatch, dem Betriebssystem der Uhr oder den Watch-Apps Sicherheitslücken, können Angreifer diese ausnutzen.

In aller Regel bringen neue Geräte auch neue Schwachstellen mit (wobei die alten Geräte ebenfalls bekannte und unbekannte Sicherheitslücken haben). Jedes neue Gerät, jede neue Anwendung, jede neue Betriebssystem-Version macht somit eine neue Risikoanalyse und eine neue Risikoabwehr erforderlich.

Empfehlung: Prognosen als Weckruf sehen

Es wäre deshalb falsch, die Prognosen für 2018 als Liste zu verstehen, für die man nur die passenden IT-Sicherheitslösungen braucht. Stattdessen sind solche Vorhersagen eine Erinnerung daran, dass es laufend neue IT-Risiken gibt. Es gilt, die Augen offenzuhalten, welche neuen Gefahren drohen, nicht nur zu Beginn des Jahres. Das betrifft sowohl die Anschaffung privater IT-Geräte als auch die Planung neuer Verfahren und Prozesse im Unternehmen, bei denen personenbezogene Daten verarbeitet werden sollen.

Das Verzeichnis von Verarbeitungstätigkeiten

„Verzeichnis" – das hört sich nach Bürokratie und Arbeit an. Und was bitte bedeutet der seltsame Begriff „Verarbeitungstätigkeiten"? In jedem Fall sollten Sie wissen: Unternehmen droht Ärger, wenn sie kein solches Verzeichnis haben. Also helfen Sie mit, es zu erstellen, wenn man Sie darum bittet.

Neue Regeln ab 25. Mai 2018

Unternehmen müssen ab 25. Mai 2018 die Europäische Datenschutz-Grundverordnung (DSGVO) beachten. Sie ist ein EU-Gesetz. Das hat sich herumgesprochen. Weniger bekannt ist den meisten, dass die DSGVO neue Formalien mit sich bringt. Kernstück ist dabei das „Verzeichnis von Verarbeitungstätigkeiten".

Das Ziel: Überblick

Dieses Verzeichnis muss in jedem Unternehmen vorhanden sein. Es soll einen Überblick schaffen, mit welchen personenbezogenen Daten das Unternehmen umgeht und was es mit den Daten tut. Dabei wird es oft um Daten von Kunden gehen. Aber auch Daten von Arbeitnehmern sind erfasst. Ebenso Daten von Lieferanten, wenn dabei Namen von Personen auftauchen.

Pflicht zur Vorlage des Verzeichnisses

Die Datenschutzaufsicht kann jederzeit verlangen, dass ihr ein Unternehmen das Verzeichnis vorlegt. Ansonsten droht ein Bußgeld. Und wenn ein Betroffener Auskunft über seine Daten verlangt, hilft das Verzeichnis dabei, diese Daten zu finden. Es ist also sinnvoll, dieses Verzeichnis sorgfältig zu erstellen. Ab und zu muss es auch aktualisiert werden.

Formular mit oft banalen Antworten

Nehmen Sie es deshalb ernst, wenn Sie mithelfen sollen, für eine gute Qualität des Verzeichnisses zu sorgen! Normalerweise bedeutet das, dass Sie ein Formular ausfüllen müssen, sei es elektronisch oder auf Papier. Dort wird zum Beispiel gefragt,

- welche personenbezogenen Daten Sie am Arbeitsplatz verarbeiten,
- zu welchem Zweck Sie das tun und
- wie lange die Daten aufbewahrt werden.

Die Antworten darauf wirken manchmal recht banal. Beispielsweise ist jedem klar, dass eine Versandabteilung Kundendaten verwendet, um Bestellungen zu bearbeiten. Aber das muss eben festgehalten werden. Im Übrigen zeigt das Beispiel, dass das Formular oft schnell ausgefüllt ist. Der Aufwand hält sich also meistens in Grenzen.

Zögern Sie nicht lange!

Lassen Sie entsprechende Anfragen nicht lange liegen! Denn alle Meldungen aus dem Unternehmen zu einem Verzeichnis zusammen-zuführen – das braucht durchaus etwas Zeit. Und bis 25. Mai 2018 muss das Verzeichnis fix und fertig vorliegen. Sonst kann es für das Unternehmen Ärger geben.

„Verarbeitungen auf Papier"

Eines wundert viele: In das Verzeichnis müssen auch „Verarbeitungen" aufgenommen werden, bei denen keine EDV zum Einsatz kommt. Klar: Diese Fälle werden seltener. Aber da und dort gibt es immer noch Hängeregistraturen, die alphabetisch nach den Namen geordnet sind, um nur ein typisches Beispiel zu nennen. Auch das ist dann eine „Verarbeitung", die in das Verzeichnis muss. Dasselbe würde natürlich für Karteikarten gelten, die nach Namen geordnet sind.

Überflüssige Datenträger entsorgen!

Eine solche Kartei steht zwar noch herum, wird aber gar nicht mehr benutzt? Das hilft nichts, sie muss trotzdem in das Verzeichnis. Vielleicht ein guter Anlass, die Kartei endlich einmal zu entsorgen. Doch fragen Sie bitte vorher genau nach, ob sie wirklich entsorgt werden kann oder aus irgendwelchen Gründen doch noch aufgehoben werden muss. Das kann durchaus vorkommen, etwa weil die Steuergesetze das vorschreiben.

Kein Einsichtsrecht für Betroffene

Dürfen Betroffene eigentlich Einsicht in das Verzeichnis nehmen? Dürfte also beispielsweise ein Kunde Einsicht verlangen? Nein. So etwas gab es früher einmal. Jetzt ist das nicht mehr vorgesehen. Das Verzeichnis ist eine rein interne Angelegenheit.

Aufbewahrung des Verzeichnisses

Wo das Verzeichnis geführt wird, kann das Unternehmen selbst festlegen. Oft liegt es beim Datenschutzbeauftragten. Eine Aufbewahrung durch eine andere Stelle ist aber auch möglich. Für den Datenschutzbeauftragten ist das Verzeichnis wichtig, weil er einen Überblick haben muss, wo personenbezogene Daten liegen.

Zulässige Sprachen: Deutsch und Englisch

Normalerweise ist das Verzeichnis in deutscher Sprache zu führen. Die Aufsichtsbehörden für den Datenschutz akzeptieren es aber auch, wenn es auf Englisch verfasst wird. Hier hat das Unternehmen also die Wahl.

Manche Unternehmen legen dabei einen Katalog der englischen Begriffe fest, die verwendet werden dürfen. Das hat dann gute Gründe. Denn wenn eine Aufsichtsbehörde den Inhalt des Verzeich-nisses sprachlich nicht versteht, kann sie eine Übersetzung fordern. Sprachliche Originalität ist hier deshalb fehl am Platz.

CURACON
SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

Sanovis
Consulting with Care

Mitgliederlisten im Verein

Vereine spielen in der Gesellschaft eine wichtige Rolle – in Deutschland ganz besonders. In kleinen Vereinen kennen sich alle Mitglieder persönlich. In größeren Vereinen sieht das anders aus. Kann ein Vereinsmitglied dann fordern, dass es eine Liste aller anderen Mitglieder bekommt? Die Frage ist keineswegs banal, übrigens auch nicht für Unternehmen. Denn gerade kleine und mittelständische Unternehmen engagieren sich oft stark in regionalen Vereinen.

Spannungen im Verein

In einem Verein gibt es Spannungen. Fünf Mitglieder wünschen eine außerordentliche Mitgliederversammlung. Dort soll über die strittigen Punkte diskutiert werden. Der Vorstand des Vereins will von einer Mitgliederversammlung jedoch nichts wissen.

Mitgliederversammlung oder nicht?

Nun überlegt die „Fünferbande", wie sie erreichen kann, dass eine Mitgliederversammlung stattfindet. Sie greift zur Satzung des Vereins. Dort heißt es: Eine Mitgliederversammlung muss einberufen werden, wenn 10 % der Mitglieder das schriftlich fordern. Das ernüchtert die Fünf. Der Verein hat nämlich fast 4.000 Mitglieder. Optimistisch betrachtet kennen die Fünf vielleicht 300 Mitglieder persönlich. Und viele davon halten nichts von einer außerordentlichen Mitgliederversammlung.

Der Wunsch: eine Liste aller Mitglieder

Einer der Fünf hat eine Idee. Er verlangt vom Vorstand, dass er eine Liste aller Vereinsmitglieder bekommt, mit Name und Anschrift. Soweit die E-Mail-Adresse bekannt ist, möchte er auch die E-Mail-Adresse haben. Der Vorstand will aber auch davon nichts wissen. Schließlich gebe es den Datenschutz, und damit sei der Wunsch nicht zu vereinbaren.

Recht klare Regeln der Rechtsprechung

Wer Mitglied eines Vereins ist, weiß es: Über solche Fragen wird öfter einmal gestritten. Da wundert es nicht, dass es einige Gerichtsentscheidungen dazu gibt, bis hinauf zum Bundesgerichtshof. Daraus lassen sich recht klare Regeln für solche Fälle ableiten:

- Eine solche Liste enthält personenbezogene Daten. Sie müssen auch in Vereinen geschützt werden.
- „Einfach so" darf eine Mitgliederliste nicht herausgegeben werden.
- Der Wunsch, eine Mitgliederversammlung herbeizuführen, stellt ein berechtigtes Interesse dar. Schließlich gehört es zum Vereinsleben, dass man diskutiert und Beschlüsse dazu fasst, was im Verein geschehen soll.
- Ein Mitglied, das eine Mitgliederversammlung anstrebt, hat deshalb Anspruch auf eine Mitgliederliste.
- Diese Liste muss die Angaben enthalten, die notwendig sind, um die anderen Mitglieder zu kontaktieren.
- Dazu gehört auch die E-Mail-Adresse, aber selbstverständlich nur dann, wenn sie dem Verein vorliegt. Ein Verein muss also keine E-Mail-Adressen extra „einsammeln".

Strikte Zweckbindung der Daten

Selbstverständlich darf die Liste nur für den Zweck verwendet werden, Unterstützung für eine Mitgliederversammlung zu finden. Eine Verwendung für andere Zwecke wäre ein schwerer Datenschutzverstoß.

Einschaltung eines Treuhänders oder nicht?

Nicht ganz einig sind sich die Gerichte darüber, ob die Mitgliederliste dem Mitglied, das sie wünscht, persönlich auszuhändigen ist.

Manchmal verlangen die Gerichte, dass ein Treuhänder eingeschaltet wird. Das kann beispielsweise ein Rechtsanwalt oder Notar sein. Wichtig ist, dass der Treuhänder von Berufs wegen zur Verschwiegenheit verpflichtet ist.

Der Treuhänder erhält vom Verein die Mitgliederliste. Diese Liste verwendet er dazu, die anderen Mitglieder anzuschreiben. Das geschieht im Auftrag des Mitglieds, das eine Mitgliederversammlung anstrebt. Danach gibt der Treuhänder die Liste an den Verein zurück oder vernichtet sie. Diese Verfahrensweise ist besonders datenschutzkonform.

Die leidige Kostenfrage

Alle Kosten, die entstehen, muss natürlich das Mitglied tragen, das eine Mitgliederliste verlangt. Insgesamt kann dies bei größeren Vereinen ganz schön ins Geld gehen. Das gilt vor allem dann, wenn ein Treuhänder eingeschaltet werden muss. Denn selbstverständlich arbeitet auch ein Treuhänder nicht kostenlos.

Der Zweck eines Vereins

Manche wundern sich darüber, dass es offensichtlich relativ einfach ist, andere Vereinsmitglieder kontaktieren zu dürfen. Berücksichtigt man aber, wozu Vereine eigentlich da sind, ist das überhaupt nicht erstaunlich. Schließlich bildet ein Verein einen Zusammenschluss von Personen, die einen gemeinsamen Zweck verfolgen. Wer sich einem Verein anschließt, muss es deshalb akzeptieren, dass ihn andere Vereinsmitglieder um Kontakt bitten. Das gilt selbstverständlich nur im Rahmen des Vereinszwecks.

Impressum

Redaktion:
Dr. Uwe Günther
Sanovis GmbH

Anschrift:
Richard-Strauss-Str. 69
81679 München
Telefon: +49 89 99 27 579 22
E-Mail: Uwe.Guenther@Sanovis.com

Das Leck im Prozessor: Hardware als Schwachstelle

Sicherheitslücken in einem Betriebssystem betreffen die Nutzer eines anderen Betriebssystems in aller Regel nicht. Hat jedoch grundlegende Hardware eine Sicherheitslücke, sieht dies anders aus. Anfang Januar passierte genau das.

Hardware-Leaks

Geht es um Schwachstellen und IT-Sicherheitslücken, kommen (mobile) Betriebssysteme, Anwendungen und mobile Apps zur Sprache, oftmals auch Webbrowser und Browser-Erweiterungen. Doch die Löcher, durch die die Daten ungewollt abfließen und über die Angreifer Zugriff erhalten können, müssen nicht in der Software stecken. Auch die Hardware, zum Beispiel die Computer-Chips, können Fehler aufweisen, die Attacken auf die Daten zulassen.

Anfang Januar dieses Jahres wurde bekannt, dass die Prozessoren verschiedener Hersteller schwer zu behebende IT-Sicherheitslücken haben. Die Schwachstellen ermöglichen unter anderem das Auslesen von sensiblen Daten wie Passwörtern, Schlüsseln und beliebigen Speicherinhalten, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) betonte. Betroffen waren demnach nahezu alle Geräte, die über einen komplexen Prozessorchip bestimmter Hersteller verfügen, darunter Computer, Smartphones und Tablets mit allen gängigen Betriebssystemen. Aber auch Cloud-Dienste waren von den Sicherheitslücken betroffen. Denn viele davon laufen ebenfalls auf Server-Hardware, die entsprechende Chips nutzen.

Gegenmaßnahmen sind Updates und kein Hardware-Tausch

Was aber können Nutzer tun, wenn es Sicherheitslücken in der Hardware gibt? Müssen die Hardware-Besitzer dann die Chips austauschen – und geht das überhaupt? Natürlich wäre es ideal, die fehlerhafte Hardware austauschen zu können, doch das klappt praktisch nicht. Noch besser wäre es, die Hardware anders zu konzipieren.

Hierzu erklärte BSI-Präsident Arne Schönbohm: „Das BSI hat in der Vergangenheit bereits mehrfach auf die Problematik von IT-Sicherheitsproblemen in Hardware-Produkten hingewiesen, etwa in unseren jährlichen Lageberichten. Der vorliegende Fall ist ein erneuter Beleg dafür, wie wichtig es ist, Aspekte der IT-Sicherheit schon bei der Produktentwicklung angemessen zu berücksichtigen. 'Security by Design' und 'Security by Default' sind Grundsätze, die für den Erfolg der Digitalisierung unerlässlich sind."

Tatsächlich ist es so, dass die akute Abhilfe bei solchen Hardware-Sicherheitslecks den Maßnahmen sehr ähnlich ist, die auch bei Software-Schwachstellen nötig sind. Es müssen Updates stattfinden, allerdings nicht nur von einigen bestimmten Anwendungen, sondern sehr umfassende Updates. Das liegt daran, dass die Art und Weise, wie die Betriebssysteme und die Anwendungen mit der Hardware kommunizieren und arbeiten, verändert werden muss, auf breiter Front.

Patch-Management ist extrem wichtig

Das regelmäßige und zeitnahe Installieren von Updates als Fehlerbehebung, auch Patches genannt, ist somit nicht nur wichtig, weil Software fehlerbehaftet ist und Datendiebe deren Schwachstellen ausnutzen könnten. Auch in der Hardware lauern Sicherheitslücken, für die Updates nötig sind. Das gilt nicht nur für Prozessoren, sondern für jede Art von Hardware, also zum Beispiel Router, Drucker und Komponenten für Computer-Schnittstellen.

Denken Sie deshalb privat wie beruflich an das sogenannte Patch-Management. Suchen Sie also regelmäßig Patches und installieren Sie sie zeitnah. Die IT, ob Software oder Hardware, kann Fehler und Schwachstellen aufweisen. Machen Sie deshalb als Nutzer nicht den Fehler, Patches zu spät oder sogar überhaupt nicht zu installieren!

Kennen Sie die Risiken von Hardware-Fehlern? Machen Sie den Test.

Frage: ***Weder Software noch Hardware kann als fehlerfrei angenommen werden. Für Software gibt es Updates als Fehlerbehebung, bei Hardware hilft nur der Austausch. Stimmt das?***

a. **Nein, auch für Hardware-Fehler gibt es in der Regel Updates.**
b. **Ja, Hardware-Fehlern kann man durch Updates nicht begegnen. Das geht nur bei Software.**

Lösung: Die Antwort a. ist richtig. Die Updates ändern zwar die Hardware nicht, aber das Zusammenspiel von Hardware und Software, um so die Auswirkungen der Hardware-Fehler zu kompensieren.

Frage: ***Hardware-Risiken wie unsichere PC-Schnittstellen lassen sich nur durch direkten Zugriff auf die Hardware ausnutzen. Stimmt das?***

a. **Ja, zum Beispiel durch Anstecken eines verseuchten USB-Sticks an eine fehlerhaft konfigurierte USB-Schnittstelle.**
b. **Nein, es ist sogar aus der Ferne, also über das Internet, möglich, Hardware-Schnittstellen zu missbrauchen.**

Lösung: Die Antwort b. ist richtig. Angreifer können es schaffen, über das Internet Hardware-Schnittstellen zu manipulieren, wenn diese entsprechende Schwachstellen aufweisen. So kann es zum Beispiel bei einer Attacke gelingen, auf die unzureichend geschützte Verbindung zum Drucker zuzugreifen, um Daten zu stehlen oder um dem Drucker ungewollte Befehle zu erteilen. Dies ist bereits in der Vergangenheit geschehen, als Angreifer zahlreiche Drucker aus der Ferne aktiviert hatten, um Propaganda zu drucken.