EU-DSGVO: IT-Risiken dauerhaft eindämmen

28.09.2018 | **Fachartikel, Management**

Das Inkrafttreten der neuen EU-Datenschutzgrundverordnung trieb den Verantwortlichen in vielen kleinen und mittleren Unternehmen – selbst in großen Konzernen die Schweißperlen auf die Stirn. Nun ist der 25. Mai 2018 schon wieder Geschichte und viele gehen zur Tagesordnung über. Dass das ein fataler Fehler sein kann, wird die Zukunft zeigen. Denn die Risiken sind in vielen Organisationen längst nicht eingedämmt, wie sich insbesondere im IT-Bereich zeigt. So ist beispielsweise nach wie vor in vielen Häusern nicht abschließend klar, wo genau in der IT – sowohl in den internen als auch in externen Systemen – überhaupt personenbezogene Daten verarbeitet werden. Die entsprechenden Stellen müssen zweifelsfrei identifiziert und folgerichtig dauerhaft geschützt sein.

Autor: Stefan Schaffner, Geschäftsführer, ASS it-Systemhaus GmbH

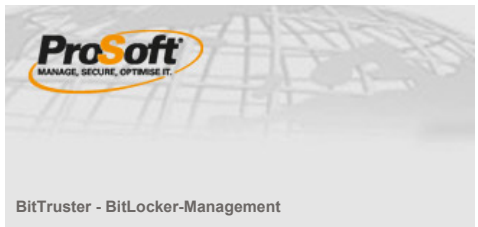
Teure Nachlässigkeiten

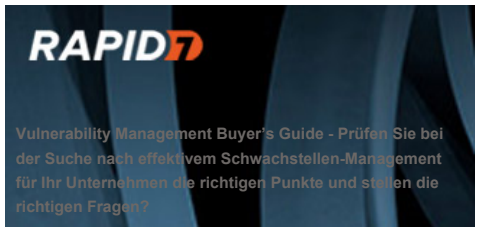
Das große Ereignis, das Inkrafttreten der EU-DSGVO am 25. Mai 2018, erzeugte branchenübergreifend einen Sturm der Aufregung. Inzwischen hat sich der Hype etwas gelegt – vorerst jedenfalls. Viele Unternehmen mussten sich des Themas notgedrungen annehmen und sind die aus ihrer Sicht (oder aus Sicht ihrer Berater) wichtigsten Punkte angegangen oder haben zumindest mit deren Bearbeitung begonnen. Fakt ist: Bei nahezu allen Anforderungen aus der EU-Datenschutzgrundverordnung spielt die IT eine zentrale Rolle, wie beispielsweise bei dem Datenverarbeitungsverzeichnis, vor allem jedoch bei den „Technischen und Organisatorischen Maßnahmen (TOM)“ nach DSGVO. Gerade diese TOMs erfordern eine tiefe Kenntnis der eigenen IT-Strukturen – und überfordern damit die fachlichen Kompetenzen vieler Datenschutzbeauftragter in kleinen und mittelständischen Unternehmen. **Fragen wie: „Welche Daten werden von welchen IT-Prozessen intern und auch extern bearbeitet und wo werden sie gespeichert? Welche Personen und welche Systeme haben Zugriff? Und schließlich: Welche Schutzmaßnahmen wurden ergriffen?“** müssen aber eindeutig beantwortet werden, damit nicht (im schlimmsten Fall) teure Rechtsfolgen drohen. Trotzdem sich viele der damit verbundenen Haftungsrisiken bewusst sind, wird gerade die Integration und Pflege geeigneter IT-Schutzmaßnahmen zum Beispiel – wenn überhaupt – oft noch viel zu nachlässig umgesetzt.

Erstens: Bestandsaufnahme und Identifikation

Um die eigenen Systeme im Sinne der DSGVO effektiv schützen zu können, müssen die Datenschutzverantwortlichen zunächst Kenntnis von ihrer Existenz, ihrem Ort und ihrem Einsatzzweck haben. Zudem sollten sie zwingend wissen, wer wann wie wo und warum Zugriff auf die Systeme hat. Insbesondere in Zeiten der Cloud stellt diese Bestandsanalyse nicht nur die Datenschutzbeauftragten, sondern sogar viele IT-Verantwortliche vor neue Herausforderungen.

UNTERNEHMEN IM FOKUS





Denn: Die Frage nach dem „WO“ zum Beispiel, ist hier teilweise nur sehr schwer zu beantworten. Grundsätzlich zählen zu den Systemen neben den PCs als Endpunkte auch Softwarelösungen mit ihren Datenbanken, SaaS-Lösungen und die gesamte Peripherie. So muss beispielsweise auch der Multifunktionsdrucker in die Liste aufgenommen werden: Immerhin verarbeitet und speichert das Gerät ebenfalls Daten. Sind alle datenverarbeitenden Systeme und Komponenten erfasst und identifiziert, müssen diese Informationen zentral dokumentiert und natürlich fortwährend gepflegt und aktualisiert werden.

Zweitens: Schutz der Systeme sicherstellen

Ist die Bestandsanalyse abgeschlossen, gilt es nachhaltige Konzepte zu entwickeln, wie die identifizierten datenverarbeitenden IT-Systeme und Komponenten dauerhaft geschützt bleiben. Abhängig vom Umfang der Infrastruktur kann es dabei sinnvoll oder notwendig sein, ein Monitoringsystem für alle Endgeräte und die Peripherie zu installieren. Auf diese Weise sind nachfolgende Anforderungen wie etwa das Patchen und das Auditieren der Sicherheitsmaßnahmen einfacher umsetzbar. Zunächst einmal gilt es, Prozesse für das On- und Offboarding von Systemen aller Art zu etablieren: vom einfachen PC als Endpoint bis zur Aufnahme einer komplexen Softwarelösung als SaaS. Auf diese Weise bleibt die Dokumentation der eigenen IT-Infrastruktur aktuell. Zudem müssen die Endpoints an sich mit den notwendigen Sicherheitsfeatures ausgestattet sein: Anti-Virus und Anti-Spyware gehören hier ebenso dazu, wie ein aktives automatisches und zentrales Patchmanagement aller kritischen Softwarekomponenten. Darüber hinaus sollte die Sicherheitsstufe jedes Endgeräts dokumentiert sein – abhängig von der Kritikalität der verarbeiteten personenbezogenen Daten. So ist zum Beispiel der PC in der Auftragsverarbeitung oder der Kundendatenverarbeitung einer höheren Stufe zuzuordnen, als der PC in der Marketingabteilung, der allgemeine Unternehmensinformationen aufbereitet. Für das erstgenannte Gerät gelten im Rahmen der TOMs-Liste strengere Regeln. Besondere Aufmerksamkeit gebührt den Schnittstellen der Systeme intern und vor allem auch nach außen. Oftmals finden sich hier lang gediente Systeme, die getreu dem Motto „Never touch a running system“ tatsächlich nie wieder unter dem Gesichtspunkt moderner Sicherheitsstandards betrachtet wurden. Modernisierung in diesem sensiblen Bereich ist darum ein stetiges Muss – denn: Nur moderne API-basierte Systeme bieten ausreichenden Schutz vor Datenabfluss oder -manipulation. Grundsätzlich helfen regelmäßig wiederkehrende Audits aller Systeme ab einer selbst zu definierenden Sicherheitsstufe und die Dokumentation der Ergebnisse. Im Falle von Sicherheitsvorfällen kann diese Maßnahme – und der Nachweis darüber, dass sie regelmäßig stattgefunden hat sowie dokumentiert wurde – vor größeren Strafen schützen.

Drittens: Dokumentation, Dokumentation, Dokumentation!

Wollen kleine und mittlere Unternehmen die strengen Vorschriften der EU-DSGVO einhalten, werden sie schnell feststellen: Ein wesentlicher Bestandteil der Rechtskonformität ist die Dokumentation – von der Erstellung des Datenverarbeitungsverzeichnisses bis hin zur schriftlichen Protokollierung IT-schutzrelevanter Maßnahmen. Essentiell ist hier die Erstellung einer umfangreichen und detaillierten Dokumentation der gesamten IT-Infrastruktur, die mit personenbezogenen Daten in Verbindung steht. Diese bildet die Grundlage für Teile des Verarbeitungsverzeichnisses, der TOMs-Liste und auch der Notwendigkeit zum Abschluss von Auftragsverarbeitungsverträgen. Diese Dokumentation sollte unter anderem enthalten:

• Auflistung aller Systeme (Endgeräte, Server, Softwarelösungen und SaaS)

• Einteilung in die Sicherheitsstufen

• Art der (personenbezogenen) Daten, die auf den Systemen verarbeitet werden

• Datenfluss (von System, nach System / von extern, nach extern)

• Art der Verarbeitung (Neuanlage, Einsicht, Änderung, Löschung)

• Personen, die mit diesen Systemen arbeiten

• Prozesse, in die diese Systeme einzogen sind (siehe Verarbeitungsverzeichnis).

Wichtig bleibt hier, dass die Überprüfung der Bestände – also quasi eine IT-Inventur mit dem Schwerpunkt DSGVO – regelmäßig wiederholt und die Einhaltung des Turnus ebenfalls dokumentiert werden sollte.

Fazit

Das Inkrafttreten der EU-Datenschutzgrundverordnung hat nahezu jedes Unternehmen in Deutschland aus dem Dornröschenschlaf gerissen. Bevor die meisten von ihnen wieder sorglos

wegschlummern, sollten sie ihre Hausaufgaben erledigen und darauf achten, dass ihre IT-Landschaft rechtskonform aufgestellt ist. Parallel dazu müssen sie überprüfen, ob ihre Dokumentation vollständig vorliegt und sie regelmäßige Reviews der Sachlage im Kalender stehen haben. Wenn es um die Ableitung und Umsetzung konkreter Maßnahmen geht, ist es eventuell ratsam, einen externen Dienstleister hinzuziehen, der die notwendige Expertise und Erfahrung mitbringt.

Artikel drucken

Diesen Artikel empfehlen

Verwandte Nachrichtenn

- 11.09.2018 **Studie: Sicherheitsverantwortliche haben nur wenig Mitspracherecht bei IoT-Entscheidungen**
- 11.09.2018 **Trend Micro und Moxa schützen gemeinsam das Industrial Internet of Things**
- 11.09.2018 **Entwickler-Studie: Ein besserer Einsatz von Software-Entwicklern könnte die globale Wirtschaftsleistung um 2,6 Billionen Euro steigern**
- 06.09.2018 **Cyberstudie: Service Provider sind das Ziel von DDoS-Attacken**
- 05.09.2018 **Neu! 5 Minuten Terrine**

© Copyright
All-About-Security.de 2006-2015.
Alle Rechte vorbehalten.

SERVICE
Impressum
Datenschutz
Kontakt
RSS-Feed
Logo Download
Mediadaten anfordern

SOZIALE NETZWERKE
Twitter
XING