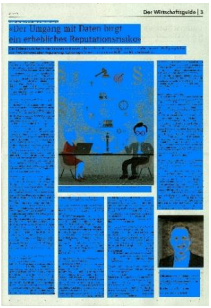
x-mediasolutions

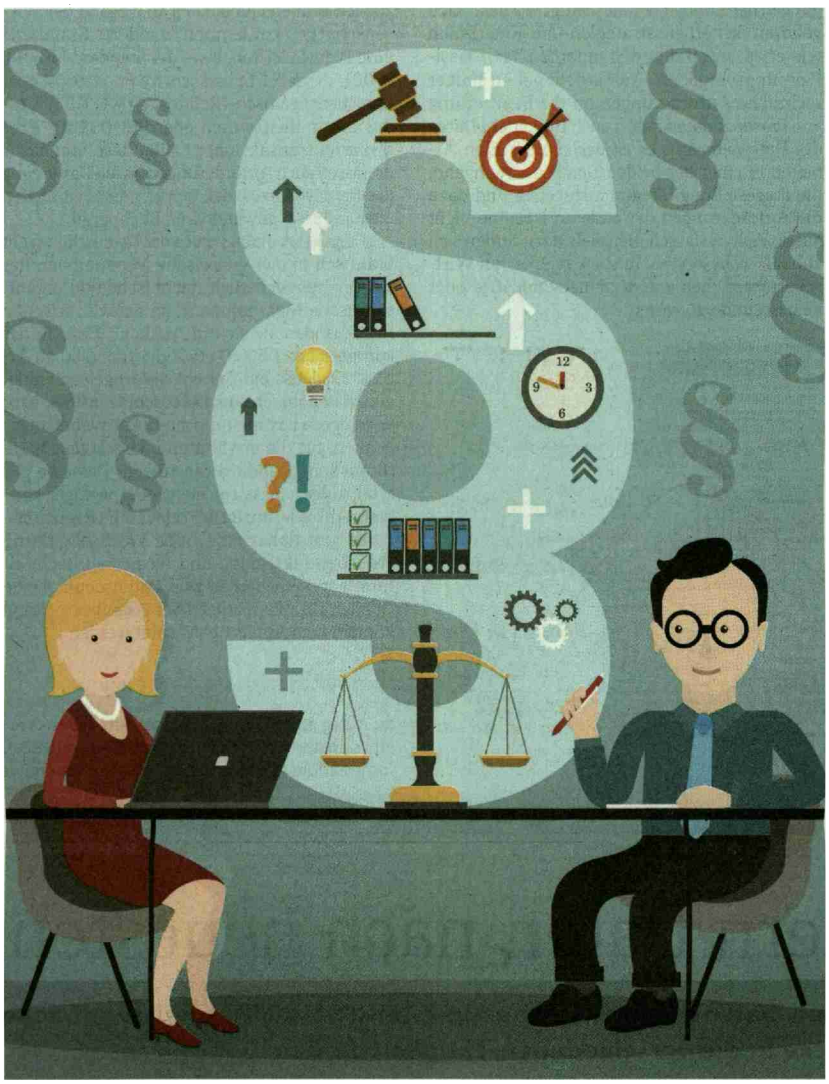


Datum: 15.07.2018

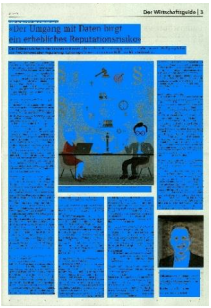
UNTERNEHMENSBEITRAG – INTERVIEW

«Der Umgang mit Daten birgt ein erhebliches Reputationsrisiko»

Der Datenschutz hat in der Schweiz in diesem Jahr rasch an Bedeutung gewonnen. Cyberexperte Wolfgang Schurr von PwC Schweiz über Regulierung, Cyberangriffe und die zentrale Rolle der Mitarbeitenden.



Schweizer Unternehmen sollten sich mit Datensicherheit und der Gesetzeskonformität ihrer Geschäftsprozesse auseinandersetzen.



Datum: 15.07.2018

Herr Schurr, Sie sind zuständig für den Bereich Cybersecurity & Privacy bei PwC Schweiz. Wie macht sich die Schweiz im Kontext der Digitalisierung?

Wir stellen fest, dass immer mehr Schweizer Unternehmen die Chancen der Digitalisierung wahrnehmen, um ihre Wertschöpfungskette zu optimieren: Sie automatisieren repetitive Geschäftsprozesse durch Softwareroboter, nutzen leistungsfähige Technologien, um Marketingaktivitäten über multiple Kanäle zu steuern oder erweitern und optimieren ihr Service- und Produktportfolio, beispielsweise durch intelligente Datenanalysewerkzeuge.

Das ist eine vielversprechende Einschätzung. Gibt es auch Schattenseiten?

Für den Wirtschaftsstandort Schweiz und die Positionierung der Unternehmen im internationalen Wettbewerb ist eine solche Entwicklung enorm wichtig. Diesen Chancen stehen aber natürlich auch Herausforderungen gegenüber, die insbesondere für kleine und mittelständische Unternehmen in der Schweiz oftmals überfordernd sind. Beispielhaft sind hier der Schutz gegenüber immer komplexeren Cyberangriffen, der personelle Mangel an IT-Sicherheitsspezialisten oder die Umsetzung anspruchsvoller Anforderungen an den Datenschutz, aktuell unter anderem durch das revidierte Bundesgesetz über den Datenschutz (E-DSG) oder die neue EU-Datenschutz-Grundverordnung (DSGVO). Gerade im Umgang mit ihren Daten haben Schweizer Unternehmen Aufholbedarf. Oft wissen sie gar nicht, was mit ihren Daten genau passiert oder dass sie diese indirekt an Drittparteien weitergeben. Informationen auf jeder Unternehmenswebsite können theoretisch abgeschöpft und weiterverarbeitet werden – zum Beispiel durch User Tracking für Online-Marketing –, wenn sie nicht ausreichend geschützt sind. Auch der Diebstahl von sensiblen und privaten Unternehmens- oder Kundendaten bleibt vielfach lange unbemerkt.

Wie sehen Cyberattacken heutzutage aus?

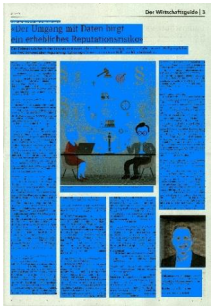
Cyberangriffe gelangen entweder über den technischen oder den menschlichen Weg an ihr Ziel, das heisst mittels eines Hacks auf ein IT-System oder via dem sogenannten «Social Engineering». Darunter ist die gezielte Manipulation von Personen zu verstehen, die bestimmte Handlungen oder Verhaltensweisen in ihnen hervorrufen soll. Das können die Weitergabe vertraulicher Informationen oder die Freigabe von Zahlungen sein. Ein beliebtes und erfolgreiches Mittel ist das «Phishing Mail», das oft eingesetzt wird, um über einen E-Mail-Account ein Schadprogramm, etwa zu Spionagezwecken, in ein IT-System einzuschleusen. Eine weitere Cyberbedrohung stellt vermehrt auch «Ransomware» dar, die Daten in den Zielsystemen blockiert oder gar löscht. Die betroffenen Parteien werden anschliessend von den Urhebern der Schadsoftware auf ein Lösegeld erpresst, wollen sie ihre Systeme wieder freigeschalten haben. Neben den regulatorischen, finanziellen sowie betrieblichen Risiken führen solche Angriffe für Unternehmen vor allem zu einem hohen Vertrauens- und Reputationsverlust. Denn von einem Datenklau können aufgrund der immer stärkeren digitalen Vernetzung auch Kunden, Mitarbeiter oder Lieferanten betroffen sein. Diese Risiken dürfen keinesfalls unterschätzt werden.

Können Unternehmen solche Angriffe auf ihre Netzwerke verhindern?

Wichtig sind hier vor allem präventive Massnahmen. Nebst technischen Hilfsmitteln, um solche Attacken frühzeitig zu erkennen, liegt einer der Schlüssel für einen effektiven Schutz in der Ausbildung und Schulung der Mitarbeiter. Diese können mittels einfacher Verhaltensweisen bereits einen gewissen Teil der Angriffe identifizieren und grössere Schäden verhindern, indem sie ungewöhnliche E-Mails oder andere Abnormitäten in den IT-Systemen frühzeitig melden. Zudem sollten grundlegende Gewohnheiten etabliert werden, wie zum Beispiel das regelmässige Ändern der Passwörter. Dies insbesondere vor dem Hintergrund, dass sich unautorisierte Benutzer womöglich bereits im Netzwerk befinden.

Die DSGVO ist seit dem 25. Mai 2018 verbindlich – Kunden werden von Unternehmen mit Updates ihrer Datenschutzangaben überflutet. Was steckt dahinter?

Die DSGVO verlangt eine transparente Verarbeitung personenbezogener Daten. Personenbezogene Daten sind all jene, die die Identifikation



Datum: 15.07.2018

einer natürlichen Person ermöglichen. Die Verarbeitung schliesst praktisch jeden Vorgang im Zusammenhang mit personenbezogenen Dateien – beispielsweise Speicherung, Anpassung, Verbreitung, Löschung – ein. Einfacher ausgedrückt: Natürliche Personen mit Wohnsitz oder Aufenthalt in der EU müssen mit der neuen Grundverordnung vollumfänglich und klar verständlich darüber informiert werden, was mit ihren Daten geschieht. Die aktuelle Informationswelle ist also ein gutes Zeichen, die Unternehmen kommen ihrer Pflicht nach.

Warum findet die EU-Verordnung auch in der Schweiz so grosse Beachtung?

Die DSGVO richtet sich primär an Unternehmen mit Sitz in der EU. Allerdings hat die Verordnung extraterritoriale Gültigkeit, wenn Unternehmen ihre Produkte und Dienstleistungen in der EU sesshaften oder sich befindenden, natürlichen Personen anbieten oder deren Nutzungsverhalten analysieren. Da viele schweizerische Firmen ebenfalls Kunden im europäischen Ausland haben, betrifft sie die EU-Gesetzgebung gleichermassen. Zudem – und diese Tatsache wird in vielen Informationsbeiträgen missachtet – fallen auch Angestellte unter die Definition einer natürlichen Person. Unternehmen, die Grenzgänger aus der EU beschäftigen, müssen die DSGVO also ebenfalls berücksichtigen. Aber auch im Hinblick auf die Revision des Datenschutzrechts in der Schweiz und die sogenannte ePrivacy-Verordnung der EU, die beide 2019 zu erwarten sind, müssen sich Schweizer Unternehmen mit der Gesetzeskonformität ihrer Geschäftsprozesse auseinandersetzen. Vor allem KMU sollten sich verstärkt aktiv informieren, um nicht plötzlich mit unerwünschten Bussen rechnen zu müssen.

Ein bewusster Datenschutz ist für viele Schweizer KMU Neuland. Was gilt es zu beachten?

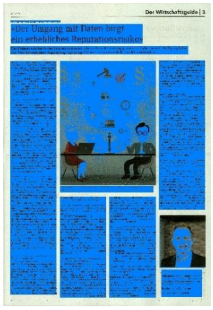
Allgemein sollte in einem ersten Schritt ein gründliches Inventar der Datenbestände und Verarbeitungsprozesse erstellt werden: Welche Daten werden in welchen Systemen und Applikationen bearbeitet? Anschliessend folgt die Prüfung der Rechtmässigkeit der Datenverarbeitung. Dabei sollte das Unternehmen die gesamte IT-Systemlandschaft betrachten. Beide Schritte sind elementar, um weiterreichende Anforderungen, beispielsweise die Informations- und Auskunftspflichten zu personenbezogenen Daten im Rahmen der DSGVO, erfüllen zu können.

Vermögen kleinere Firmen den damit verbundenen Mehraufwand sowie die damit entstehenden Kosten überhaupt zu stemmen?

Das hängt stark davon ab, wie komplex die Datenverarbeitungsprozesse eines Unternehmens sind und wie gründlich die IT-Systeme überprüft werden sollen. Es ist wichtig, die neuen Anforderungen des Datenschutzes auch als Chance zu sehen: Zum einen, um bei der oben beschriebenen Inventarisierung der Datenbestände die aktuelle Systemlandschaft auf ihre Sicherheit zu prüfen, und zum anderen, um über eine effizientere IT-Infrastruktur nachzudenken. Wir sehen in der Praxis, dass viele Unternehmen die Einführung des DSGVO als Startpunkt nehmen, um ihre Cyberstrategie zu überdenken. Ich bin sogar der Meinung, dass die Cyberstrategie die gesamte Unternehmensstrategie unterstützen und ermöglichen sollte. Entschliesst sich ein Unternehmen beispielsweise Teile ihrer Prozesse kostengünstiger auszulagern, so müssen die in diesem Rahmen verwendeten Daten entsprechend geschützt werden.

Sprechen Sie von der Cloud?

Die Cloud ist aktuell sicher eines der bekanntesten Beispiele. Die Bereitstellung der IT-Infrastruktur durch Drittanbieter über das Internet ist aber wie andere Outsourcing-Optionen mit Vor- und Nachteilen verbunden. Es bedarf einer situativen, strategischen Entscheidung, ob ein Unternehmen diesem Weg folgen möchte. Vorteilhaft – insbesondere im KMU-Bereich – kann der Kostenfaktor sein. Denn durch die Nutzung der Cloud, die meistens in flexiblen Preismodellen angeboten wird, entfallen die Kosten lokaler Soft- und Hardware sowie deren Wartung durch IT-Personal. Besonders dem Problem des IT-Fachkräftemangels, wie es häufig in KMU der Fall ist, kann dadurch vorgebeugt werden. In meiner Erfahrung stehen KMU jedoch der Auslagerung ihrer sensiblen Daten insbesondere an Cloud-Anbieter ausserhalb der Schweiz kritisch



Datum: 15.07.2018

gegenüber. Zum einen aus datenschutzrechtlichen Sorgen, zum anderen aufgrund des Abhängigkeitsverhältnisses zum Anbieter. Hier können aber oft Hybrid-Lösungen den Ansprüchen der Unternehmen gerecht werden.

Angenommen ein Unternehmen verzichtet auf die Auslagerung der IT-Infrastruktur an Drittanbieter – wie kann es seine Daten ausreichend selbst schützen?

Es ist wichtig, dass Unternehmen die Kontrollhoheit ihrer Daten sicherstellen. Diese Grundlage wird ebenso von den regulatorischen Anforderungen erwartet. Es muss zudem sichergestellt werden, dass nur autorisierte Personen Zugriff auf diese Daten haben. Darunter fällt auch der physische Zugang, etwa zu Serverräumen. Darüber hinaus sollte ein Notfallwiederherstellungsplan existieren, um den Betrieb anhand von Backups auch in Notfällen zu garantieren. Das von der Melde- und Analysestelle Informationssicherung (MELANI) des Bundes veröffentlichte «Merkblatt Informationssicherheit für KMUs» bietet eine erste hilfreiche Anlaufstelle und Checkliste, um die Sicherheit der eigenen IT-Infrastruktur zu prüfen.

IM INTERVIEW

Wolfgang Schurr ist zuständiger Partner für Cybersecurity & Privacy bei PwC Schweiz und berät seit über 18 Jahren Unternehmen im Bereich Informationssicherheit.

E: wolfgang.schurr@ch.pwc.com

www.pwc.ch/cybersicherheit