Newsletter Datenschutz
Ausgabe 12 | 2016

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

Missverständnisse können schlimme Folgen haben, auch und gerade im Datenschutz. So tragen scheinbar harmlose Gaming-Apps wie Pokémon Go auf dem Smartphone enorme Datenrisiken in sich und sind nicht einfach eine kleine Spielerei. Auch der so wichtige Virenschutz kann zur Gefahr für den Datenschutz werden, wie diese Ausgabe zeigt.

Was auf der einen Seite schützt oder Spaß macht, kann auf der anderen Seite dem Datenschutz schaden. Es ist deshalb wichtig, sich immer gut zu informieren. Dabei hilft Ihnen Ihre Datenschutz-Zeitung. So erfahren Sie diesmal, was man unter dem sogenannten Privacy Shield versteht und was es mit dem Stand der Technik in der Datensicherheit auf sich hat. So vermeiden Sie unnötige und riskante Missverständnisse im Umgang mit Daten.

Wir wünschen Ihnen viel Spaß beim Lesen!

Ihre Datenschutzbeauftragten der agentia wirtschaftsdienst

Datenschutz auch bei Pokémon Go!

Die mobile App Pokémon Go hat für viele Menschen einen regelrechten Suchtfaktor. Und das keineswegs nur für Jugendliche - auch viele Erwachsene sind dem Spiel geradezu verfallen. Dabei darf der Datenschutz freilich ebenso wenig aus dem Blick geraten wie der Schutz von Unternehmensgeheimnissen. Noch im Dezember kommt übrigens ein von den Fans sehnsüchtig erwartetes Mega-Update. Allzu schnell kann es besonderen Leichtsinn auslösen.

Pokéstops, Arenen und Monster

In seiner Freizeit kann natürlich jeder tun, was er will - beispielsweise so viele Spiele-Monster erfolgreich jagen, dass er den nächsten Level von Pokémon erreicht. Aber was ist, wenn gerade auf dem Grundstück des eigenen Arbeitgebers wunderschöne Pokéstops zu finden sind? Wenn man also gerade dort die besten Monster einfangen kann?

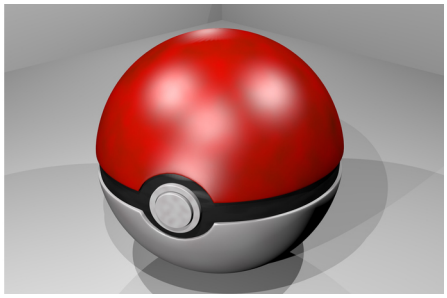
Die Spielkundigen verstehen sofort, was mit diesen Dingen gemeint ist. Sie ziehen sich in eine Arena zurück, um ein paar Monster zu besiegen. Ihre Kollegen wiederum wundern sich, wie ganz normale Menschen der Faszination von Dingen erliegen, die für die anderen um sie herum gar nicht sichtbar sind.

Arbeitszeit ist keine Spielzeit!

Klar ist, dass Spielen während der Arbeitszeit schon deshalb Fragen aufwirft, weil dann gerade nicht gearbeitet wird. Das ist zwar kein Thema des Datenschutzes, sondern des Arbeitsrechts. Freilich: Mehr Schaden als eine Zigarettenpause, die zu Unrecht nicht als Arbeitspause registriert wird, richtet das kurze Einfangen eines virtuellen Monsters während der Arbeitszeit auch nicht an, oder?

Bilder von Monstern und anderen Dingen

Das kommt darauf an. Vielfach ist es üblich, eben eingefangene Monster zu fotografieren und das Foto an Freunde zu schicken. Blöd nur,



Pokéball zum Fangen von Monstern - aber bitte nicht in der Arbeitszeit! (Bild: mario900/iStock/Thinkstock)

wenn da noch andere Dinge auf dem Bild sind, etwa Konstruktionen, die nicht fotografiert werden dürfen. Wer weiß, wo ein solches Foto landet, und wer weiß, ob jeden Empfänger des Fotos wirklich nur die Monster interessieren.

Harmlose und andere Apps

Vielfach untersagen Unternehmen aus gutem Grund, Apps für private Zwecke auf dienstlichen Smartphones oder Tablets zu installieren. Ein solches Verbot gilt dann auch für die Pokémon-App. Das Argument, sie sei harmlos und könne keinen Schaden anrichten, kann daran nichts ändern. Erstens kommt es auf diesen Gesichtspunkt nicht an. Zweitens stellt sich die Frage, ob er zutrifft. Schon ein kurzer Blick in die Nutzungsbedingungen der App zeigt, dass sich der App-Anbieter das Recht einräumen lässt, unter bestimmten Bedingungen Daten an Dritte weiterzugeben. Was daraus im Einzelfall entstehen könnte, vermag niemand sicher abzuschätzen.

Selbstverständliche Spielregeln

Ein völliges No-Go ist es vor diesem Hintergrund, berufliche Mail-Adressen bei dem Spiel zu benutzen. Wer spielen will, sollte das bitte nur auf seinem privaten Gerät tun und dabei nur eine private Mail-Adresse verwenden. Und die rechte Zeit für das Spiel ist die Freizeit, nicht die Arbeitszeit. Wer diese Punkte beachtet, kann sein Spiel genießen und sich beim Monster-Kampf bestens erholen.

Was bedeutet eigentlich "Stand der Technik?"

Der Datenschutz verlangt technisch-organisatorische Schutzmaßnahmen nach dem Stand der Technik. Das klingt nicht sehr konkret - mit Absicht!

Datensicherheit: Am schönsten wäre eine genaue Anleitung ...

Fast jeder zweite Internetnutzer (47 Prozent) ist in Deutschland in den vergangenen zwölf Monaten Opfer von Internetkriminalität geworden, so eine repräsentative Umfrage des Digitalverbands Bitkom. Die Vorfälle reichen von gefährlichen Infektionen durch Schadsoftware bis hin zu Online-Betrug und Erpressung. Um die eigenen Daten zu schützen, aber auch um die Daten der Kunden, Partner und Mitarbeiter im Unternehmen zu schützen, sind also umfangreiche Maßnahmen für die Datensicherheit erforderlich.

Doch welche Maßnahmen sind genau notwendig? Wie schützt man sich am besten? Der Bitkom-Verband schreibt dazu: Gegen digitale Angriffe nutzen vier von fünf Internetnutzern (80 Prozent) ein Virenschutz-Programm und zwei von drei (67 Prozent) eine Firewall auf ihrem Computer.

Antiviren-Programme und Firewall sind der absolute Basisschutz für jeden Computer. Aber reicht das aus? Was fordern zum Beispiel die Datenschutzvorschriften? Gibt es hier eine konkrete Vorgabe zum Schutzumfang?

BDSG und DSGVO nennen kaum genaue Sicherheitsverfahren

Im Bundesdatenschutzgesetz (BDSG) findet man: Eine Maßnahme für die Zugangskontrolle, Zugriffskontrolle und Weitergabekontrolle ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Die ab Mai 2018 anzuwendende Datenschutz-Grundverordnung (DSGVO) nennt die Verschlüsselung sowie die Pseudonymisierung.

Grundsätzlich aber sagen beide Gesetze zu den Maßnahmen der Datensicherheit: Geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, sind zu treffen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos

Sowohl BDSG als auch DSGVO nennen die Verschlüsselung als wichtiges Instrument der Datensicherheit (Bild: bygermina/iStock/Thinkstock)

für die Rechte und Freiheiten natürlicher Personen.

Statt Schutzverfahren aufzulisten, verweisen die Texte jeweils in erster Linie auf den Stand der Technik. Warum eigentlich?

IT und Bedrohungen dynamischer als Gesetzgebung

Die gesetzlichen Regelungen fordern Schutzmaßnahmen nach dem Stand der Technik, weil die IT-Sicherheitslösungen jeweils zur aktuellen Bedrohungslage, zum Schutzbedarf der Daten und zur eingesetzten IT passen müssen. Veraltete IT-Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz.

So sind zum Beispiel Verschlüsselungsverfahren, die vor einigen Jahren noch als Standard galten, heute kein wirksamer Schutz mehr. Datendiebe können diese Verschlüsselungsverfahren inzwischen relativ leicht brechen und umgehen.

Damit die Datensicherheit aktuell und damit hoch genug ist, müssen die Maßnahmen also regelmäßig angepasst und verstärkt werden. Würden rechtliche Vorgaben genaue IT-Sicherheitsverfahren benennen, müsste der Gesetzgeber die Texte fortlaufend ändern. Das geht natürlich nicht. Deshalb verlangen die Regelungen, dass die Datensicherheitsmaßnahmen aktuell sind und damit die Sicherheit den Stand der Technik abbildet.

Privat und beruflich am Puls der IT-Sicherheit bleiben

Für Sie als Anwender bedeutet dies, dass Sie jeweils aktuelle Lösungen für Ihre Datensicherheit benötigen. Am Arbeitsplatz sollten Sie sich an die IT-Sicherheitsrichtlinien der Firma halten und nur die entsprechend freigegebenen IT-Lösungen sowie Sicherheitsanwendungen nutzen.

Privat sind Sie erst einmal auf sich gestellt. Hier ist es aber ebenso wichtig, dass Sie auf eine aktuelle Datensicherheit achten. Nicht nur, wenn Sie Privatgeräte beruflich verwenden, sondern generell.

Was konkret tun?

Ihr aktuelles Datensicherheitsprogramm umfasst dabei, dass Sie die Betriebssysteme und Anwendungen auf allen genutzten Endgeräten aktuell halten und die Datenschutz- und Sicherheitsoptionen regelmäßig auf den passenden Stand bringen. Sicherheitslösungen wie den Virenschutz müssen Sie ebenfalls mit Updates versorgen.

Zudem ist wichtig, dass Sie sich neue Versionen der Sicherheitsprogramme beschaffen, in der Regel einmal jährlich. Die täglichen Updates gelten nämlich in aller Regel der aktuellen Viren-Erkennung. Neue Sicherheitsfunktionen bekommen Sie meist erst mit einer neuen Version der Anwendung.

Ob sich der Umstieg auf andere Sicherheitslösungen lohnt oder nicht, sollten Sie abhängig machen von Testergebnissen renommierter Prüfinstitute und von Berichten in der Fachpresse. Sicher werden Sie auch in Schulungen und Unterweisungen zu IT-Sicherheit und Datenschutz jeweils aktuell informiert. Wichtig ist: Bleiben Sie am Ball. Die Datendiebe haben immer neue Ideen, wie sie angreifen können.

Impressum

agentia wirtschaftsdienst
dipl.-inform. udo wenzel
budapester straße 31
10787 berlin

tel.: 030 2196 4390
fax: 030 2196 4393

udo.wenzel@agentia.de
thorsten.ritter@agentia.de

Was ist der Privacy Shield?

Wer in einem Unternehmen arbeitet, das Daten in die USA übermittelt, muss ihn kennen. Aber auch jeder Normalbürger sollte zumindest einmal davon gehört haben. Die Rede ist vom Privacy Shield, auf Deutsch etwa "Schutzschild für das Persönlichkeitsrecht". Er kann seit dem 1. August 2016 genutzt werden. Viele Unternehmen hatten dringend darauf gewartet.

Eine Herausforderung: Datenübermittlungen in die USA

Will ein Unternehmen Daten von Kunden oder auch Daten von Mitarbeitern an ein US-Unternehmen übermitteln, geht das nicht "leicht und locker". Und zwar auch dann nicht, wenn es sich bei dem US-Unternehmen beispielsweise um die "US-Mutter" handelt.

Bekanntlich gehören die USA nicht zur EU. Deshalb erlauben die EU-Regelungen zum Datenschutz den Transfer von Daten in die USA nur dann, wenn dort ein angemessenes Datenschutzniveau herrscht. Was als angemessen anzusehen ist, bestimmt sich dabei natürlich nach den Vorstellungen der EU.

Datenschutz in den USA: durchaus, aber ...

Damit beginnen in der Praxis die Probleme. Zwar gibt es in den USA sehr wohl Datenschutzvorschriften. Deshalb sollte man gegenüber Kollegen aus den USA auch nie zu überheblich davon sprechen, die USA würden sowieso keinen Datenschutz kennen.

Nur zu schnell kann es einem sonst passieren, dass diese Kollegen etwa auf Regelungen hinweisen, die die Daten von Kindern ganz besonders schützen. Die Abkürzung hierfür heißt COPPA (Children's Online Privacy Protection Rule) und ist auch den meisten Durchschnitts-Amerikanern bekannt.

Die US-Regelungen setzen die Schwerpunkte aber ganz anders als die Vorschriften der EU. Manche Aspekte des Datenschutzes, die in Europa ganz hoch gehalten werden, gelten in den USA kaum etwas. Langer Rede kurzer Sinn: Ein Datenschutzniveau, das nach den Vorstellungen der EU generell als angemessen anzusehen wäre, existiert in den USA nicht.

Individuelle Einwilligungen: nur theoretisch denkbar

Wie soll ein Unternehmen damit umgehen? Nun, es könnte beispielsweise jeden einzelnen Betroffenen um seine Einwilligung bitten und seine Daten erst dann übermitteln.

Theoretisch wäre das denkbar. In der Praxis funktioniert das aber schon wegen des Aufwands nicht. Deshalb wählt der neue Privacy Shield einen anderen Ansatz.

Der besondere Ansatz von Privacy Shield:

- Ein US-Unternehmen, das personenbezogene Daten aus der EU erhalten soll, verpflichtet sich dazu, umfangreiche Spielregeln für den Datenschutz einzuhalten. Sie sind unter dem Begriff "Privacy Shield" zusammengefasst.

- Diese Verpflichtung erfolgt gegenüber den zuständigen US-Behörden. Das ist meist die Federal Trade Commission (FTC), eine Verbraucherschutzbehörde.

- Der Inhalt der Spielregeln ist zwischen dem US-Handelsministerium (Department of Commerce) und der Europäischen Kommission abgestimmt.

- Ist ein US-Unternehmen eine solche Verpflichtung eingegangen, gilt das Datenschutzniveau in diesem Unternehmen auch seitens der EU als angemessen.

- Die positive Folge für die europäischen Geschäftspartner solcher US-Unternehmen: Sie dürfen personenbezogene Daten an dieses Unternehmen unter denselben Voraussetzungen übermitteln, unter denen dies auch innerhalb der Europäischen Union zulässig wäre.

Keine Einwilligung der Betroffenen nötig

Die Betroffenen müssen nicht gefragt werden, ob sie damit einverstanden sind. Sie müssen aber in geeigneter Weise informiert werden. Dabei sind viele Einzelheiten zu beachten, um die sich die Spezialisten in den Unternehmen kümmern. In Deutschland sind dies die Datenschutzbeauftragten der Unternehmen.

Erinnern Sie sich noch an Safe Harbor?

Manchem wird dieses Vorgehen irgendwie bekannt vorkommen. Völlig zu Recht! Ziemlich ähnlich lief dies auch schon bei den Safe-Harbor-Regelungen ab. Sie hatten sich über zehn Jahre lang beim Transfer von Daten aus der EU in die USA bewährt - jedenfalls aus der Sicht der meisten Unternehmen.

Allerdings hatte der Europäische Gerichtshof diese Regelungen im Oktober 2015 aus verschiedenen Gründen gekippt. Das geschah gewissermaßen über Nacht, also ohne jede Übergangsfrist. Deshalb waren neue Regelungen, wie sie der Privacy Shield nun vorsieht, dringend erforderlich. Etwas vereinfacht lässt sich sagen: Der Inhalt des Privacy Shield ist neu und wesentlich ausgefeilter, als es die Regelungen von Safe Harbor waren. Der Verfahrensablauf ist aber ziemlich ähnlich.

Gegen die Spielregeln verstoßen? Lieber nicht!

Wie sieht es übrigens damit aus, dass sich die Unternehmen auch wirklich an die Spielregeln halten, zu denen sie sich verpflichtet haben? Die Chancen dafür stehen gut. Jeder weiß, wie kräftig US-Behörden bei Rechtsverstößen zupacken können. Und das gilt nicht nur, wenn es um Verstöße gegen Abgasregelungen geht. Auch Datenschutzverstöße von US-Unternehmen haben die amerikanischen Behörden schon schwer geahndet. Gehen Sie also davon aus: Privacy Shield ist ernst gemeint!

Der Privacy Shield ist die aktuelle Grundlage für Datenübermittlungen in die USA (Bild: Fredex8/iStock/Thinkstock)

Virenschutz oder Datenschutz?

Die Frage, ob Sie Virenschutz oder Datenschutz wollen, erscheint auf den ersten Blick absurd. Denn Sie brauchen beides. Tatsächlich aber können Virenschutz-Lösungen zum Problem für den Datenschutz werden.

Wenn der Schutz zur Gefahr wird

Kaum jemand verzichtet komplett auf einen Virenschutz für den PC oder das Notebook, eigentlich sollte es niemand tun. Bei Smartphones sieht es schon deutlich schlechter aus: Jeder fünfte Smartphone-Besitzer (20,7 %) nutzt sein Mobilgerät ohne jegliche Sicherheitsfunktionen zum Schutz des Geräts und der darauf befindlichen Daten, so eine Umfrage für das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Aus Sicht des Datenschutzes sollte auf jedem Endgerät ein Schutz vor Malware oder Schadsoftware vorhanden sein. Doch diese Forderung kann zu einem Datenrisiko führen, wenn man nicht darauf achtet, wie es der Anbieter der Antiviren-Software mit dem Datenschutz hält.

Tatsächlich gibt es eine ganze Reihe von Virenschutz-Lösungen, die zwar Malware erkennen und abwehren, die es aber selbst nicht so genau mit dem Datenschutz zu nehmen scheinen.

Überprüfung von Datenschutzerklärungen ergab Mängel

Das Testinstitut AV-Test aus Magdeburg hat die Datenschutzerklärungen von 26 Antiviren-Programmen untersucht und dabei viele Unzulänglichkeiten und Probleme entdeckt. So hatten zwei Anti-Malware-Lösungen überhaupt keine Datenschutzerklärung. In fast jeder untersuchten Datenschutzerklärung räumten sich die Hersteller zudem in erheblichem Umfang Zugriffsrechte auf Daten ein, die für den Einsatz einer Schutz-Software nicht nötig sein dürften, so AV-Test.

Einige Extrembeispiele untermauern diese Einschätzung: So haben einzelne Hersteller angegeben, dass sie Daten über das Geschlecht, die Berufsbezeichnung sowie Rasse und sexuelle Orientierung eines Nutzers verarbeiten wollen. Der Bezug zum Schutzzweck der Software ist offensichtlich nicht vorhanden. Die Vermutung liegt nahe, dass die Anbieter Nutzerinformationen zu Werbezwecken erheben bzw. an Dritte für Werbemaßnahmen weitergeben.

Eine informierte Einwilligung, wie sie der Datenschutz fordert, erfragen sie dafür vom Nutzer nicht.

Kein blindes Vertrauen in die IT-Sicherheit

Leider können Sie also nicht davon ausgehen, dass alle Lösungen, die Ihre Daten vor Angreifern schützen, selbst mit den Daten so umgehen, wie es der Datenschutz verlangt. Auch IT-Sicherheitsanwendungen müssen hinterfragt werden, wie sie es mit dem Datenschutz halten, genau wie jede andere Applikation, die Sie installieren oder nutzen möchten. Genau genommen sollten Sie bei IT-Sicherheitslösungen wie den Antiviren-Programmen noch genauer hinschauen, was in der Datenschutzerklärung steht. Denn Sicherheitsprogramme haben sehr mächtige Funktionen und oftmals weitgehende Zugriffsberechtigungen auf die Daten. Diese Berechtigungen brauchen sie in Teilen zwar, um wirklich schützen zu können. Doch sie machen auch einen falschen Umgang mit personenbezogenen Daten durch Sicherheitssoftware so gefährlich.

Nutzen Sie also auf jedem Endgerät einen Virenschutz, aber prüfen Sie bei jedem Tool auch die Datenschutzerklärung. Virenschutz und Datenschutz werden beide gebraucht, getrennt voneinander sollten sie nicht sein. Ohne Virenschutz ist Datenschutz heute nicht mehr möglich, ohne Datenschutz sollte es jedoch keine Virenschutz-Lösung geben.

Virenschutz = Datenschutz? Testen Sie Ihr Wissen!

Frage: Virenschutz ist elementar für den Datenschutz. Stimmt das?

a) Ja, das stimmt. Trotzdem ist der Datenschutz beim Virenschutz nicht automatisch garantiert.
b) Virenschutz braucht man nur, wenn man das Internet nutzt.
c) Virenschutz-Lösungen berücksichtigen automatisch den Datenschutz.

Lösung: Die Antwort a) ist richtig. Virenschutz braucht man auf jedem Endgerät, gleich ob es einen Internetzugang hat oder nicht. Denn auch ein USB-Speicherstift kann zum Beispiel Malware einschleppen. Trotzdem kann man nicht davon ausgehen, dass der Datenschutz beim Virenschutz automatisch stimmt. Prüfen Sie die Datenschutzerklärung des Anbieters genau, bevor Sie sich für eine Lösung entscheiden.

Frage: Antiviren-Software verarbeitet personenbezogene Daten nur zu Sicherheitszwecken. Stimmen Sie dem zu?

a) Ja, zu welchen Zwecken sollte ein Sicherheitsprogramm denn sonst Daten verarbeiten?
b) Man sollte in der Datenschutzerklärung prüfen, zu welchen Zwecken der Software-Anbieter personenbezogene Daten erhebt, nutzt und speichert. Man kann Erstaunliches finden ...

Lösung: Die Antwort b) ist richtig, wie eine Untersuchung von AV-Test ergeben hat. Ob die erhobenen Nutzerdaten wirklich dem Sicherheitszweck dienen oder nicht, können Sie sich klarmachen, indem Sie die Sicherheitsfunktionen betrachten und sich fragen, ob Sie diese denn möchten oder nicht. So kann ein Zugriff auf die Standortdaten sinnvoll sein, wenn Sie die Funktion nutzen wollen, ein verlorenes oder gestohlenes Gerät wiederzufinden. Daten über das Geschlecht und die sexuelle Orientierung des Nutzers haben aber zweifellos nichts mit den Sicherheitsfunktionen zu tun. Trotzdem wollen manche Antiviren-Lösungen solche Daten erheben und verarbeiten. Hier ist mehr als Vorsicht angesagt - es empfiehlt sich die Suche nach einer anderen Antiviren-Software!