Newsletter Datenschutz

konzept 17

Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,

Datenschutz und IT-Sicherheit sind in aller Munde. Trotzdem oder gerade deshalb ist der Aufklärungsbedarf so hoch wie nie zuvor. Nicht immer spiegeln zum Beispiel die Schlagzeilen in den Tagesmedien die wirkliche Gefahrenlage wider. Bestimmte Themen werden oft genannt, andere dagegen gehen unter. Deshalb finden Sie in Ihrer neuen Ausgabe auch etwas zu der oftmals übersehenen Gefahr durch DDoS (Überlastungsangriffe), denn Ransomware ist gefährlich, aber nicht alles.

Ebenso scheint der Einsatz sogenannter Dashcams (Unfallkameras) in Fahrzeugen geläufig, trotzdem sind die Regeln dazu nicht bekannt genug. Sie finden dazu ebenso einen Beitrag in dieser Ausgabe wie zu klassischen Datenpannen, die es schon lange gibt, die aber immer noch sehr häufig passieren, wie Verwechslungen beim Postversand.

Nicht zuletzt hilft die neue Ausgabe dabei, bestimmte Grundprinzipien der Datensicherheit und des Datenschutzes zu verstehen, wie das Prinzip der minimalen Berechtigungen (Need to know). Erfahren Sie, was sich dahinter verbirgt und warum es so wichtig ist.

Ihr Frank Berns, Datenschutzbeauftragter

Impressum
Redaktion: Frank Berns,
Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de

DDoS, die vergessene Gefahr

Attacken mit Ransomware und Online-Erpressungen füllen die Schlagzeilen, doch über DDoS (Distributed Denial-of-Service) wird zu wenig berichtet. Dabei nehmen diese Überlastungsangriffe deutlich zu und sorgen für Systemausfälle. Doch wie können Sie sich schützen?

Wenn Online-Dienste scheinbar streiken

Viele Cyberangriffe werden erst sehr spät entdeckt, denn die Internetkriminellen verwischen ihre Spuren und wollen nicht entdeckt werden, um möglichst viel Zeit zu haben, sich in den befallenen IT-Systemen umzusehen und Daten auszuspähen. Cyberattacken mit Ransomware hingegen fallen schnell auf, denn die betroffenen Daten werden kriminell verschlüsselt und sind nicht mehr im Zugriff. Zudem melden sich die Angreifer mit Lösegeldforderungen. Es gibt aber auch Angriffe aus dem Internet, die deutliche Auswirkungen haben, aber trotzdem nicht richtig wahrgenommen werden. Dazu gehören die sogenannten Überlastungsangriffe, auch DDoS-Attacken genannt.

Dabei werden zum Beispiel Internetserver so stark mit Aufrufen der dort betriebenen Online-Auftritte belastet, dass die Server ausfallen und ihren Dienst einstellen. Es scheint, als ob die Webauftritte ihren Dienst verweigern.

IT-Sicherheitsbehörden melden vermehrte DDoS-Angriffe

Nicht jeder ausgefallene Online-Dienst wurde Opfer einer solchen DDoS-Attacke, doch es gibt weitaus mehr solcher Vorfälle, als man aus den relativ wenigen Medienberichten darüber schließen könnte. So erklärt das BSI (Bundesamt für Sicherheit in der Informationstechnik) im aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland: „Bei DDoS-Angriffen haben Qualität und Häufigkeit deutlich zugenommen."

Die Folgen eines DDoS-Angriffs sind zum einen finanzielle Schäden für Dienstleister oder Onlineshops, wenn diese nicht erreichbar sind, so das BSI. Zum anderen können Imageschäden und gegebenenfalls Unsicherheit in der Bevölkerung folgen. Doch auch der Datenschutz leidet unter der steigenden DDoS-Gefahr, die oftmals nicht wahrgenommen wird.

So können die Überlastungsangriffe dazu führen, dass personenbezogene Daten wie zum Beispiel Kundendaten oder Beschäftigtendaten nicht mehr verfügbar sind. Dadurch stellen DDoS-Attacken eine Datenschutzverletzung dar.

Daten müssen besser geschützt werden, auch vor DDoS

Als IT-Nutzerin oder IT-Nutzer hat man weder die Aufgabe noch die Möglichkeit, die von dem Unternehmen betriebenen oder genutzten Webserver zu schützen. Doch man ist trotzdem ein wichtiger Teil der Prävention und Abwehr von Überlastungsangriffen.

In Zeiten von mobiler Arbeit und Homeoffices werden vielfach IT-Dienste aus der Cloud genutzt, die nicht im eigenen Unternehmen betrieben und überwacht werden. Wenn man also Nutzerin oder Nutzer eines speziellen, von der eigenen IT freigegebenen Cloud-Dienstes ist und dieser nicht erreichbar ist, sollte man auch an die Möglichkeit denken, dass der Cloud-Dienst Opfer einer DDoS-Attacke geworden sein könnte. Das passiert in der Praxis leider häufig.
Eine Meldung des möglichen Vorfalls an die eigene IT-Abteilung kann zwar den gewünschten Cloud-Dienst nicht sofort wieder lauffähig machen. Doch die eigene IT kann den Vorfall zusammen mit dem Cloud-Anbieter prüfen. Insbesondere können und sollten solche Cloud-Ausfälle als Zeichen gesehen werden, dass man über eine Ausweichstrategie, also einen alternativen Cloud-Dienst nachdenken sollte, der als Ersatz dienen kann, während der andere Cloud-Service nicht erreichbar ist. Wie wichtig solch ein Ausweichdienst ist, hängt von der notwendigen Verfügbarkeit der Dienste und Daten ab. Wird der Cloud-Dienst regelmäßig und dringend benötigt, sollte eine Alternative für den Notfall nicht fehlen. Diesen Bedarf kennt die Nutzerin und der Nutzer, nicht aber automatisch die IT. Diese ist für den Hinweis auf einen hohen Bedarf deshalb dankbar.

Nicht selbst ungewollt zum Teil einer DDoS-Attacke werden

Ein weiterer Punkt gehört auf die To-do-Liste jeder Nutzerin und jedes Nutzers: Viele DDoS-Attacken missbrauchen unzureichend geschützte Endgeräte, um diese für die Angriffe fernzusteuern und auf die Ziele und damit die Online-Server zu richten. Die zahllosen Anfragen, mit denen die angegriffenen Server überhäuft werden, stammen meist von gekaperten Endgeräten, deren Nutzer und Besitzer nicht ahnen, dass ihre Geräte gerade Teil eines Angriffs geworden sind.

Deshalb sollten alle Endgeräte, ob Smartphone, Tablet, Notebook oder PC, aber auch jedes andere vernetzte Gerät, das mit dem Internet verbunden werden kann, besser geschützt werden. Dazu gehören regelmäßige, umgehend installierte Updates, aktuelle Anti-Malware-Programme und aktive Firewalls auf den Geräten. Gerade bei mobilen Endgeräten gibt es hier noch Nachholbedarf, entsprechend häufig werden diese für DDoS-Angriffe missbraucht.

DDoS ist leider eine oftmals vergessene Gefahr, aufseiten der Internetkriminellen aber ein sehr beliebtes Werkzeug. Das muss sich ändern.

Dashcams in Fahrzeugen

Nach einem Unfall kann es Gold wert sein, wenn eine Videoaufzeichnung den Ablauf des Geschehens dokumentiert. Wer die Datenschutzregeln für solche „Dashcam-Aufnahmen“ missachtet, muss allerdings mit ernsthaftem Ärger rechnen. Und zwar auch ganz ohne Unfall!

Dashcams dienen der Dokumentation

Der Begriff „Dashcam“ bezeichnet kleine Videokameras, die in einem Auto angebracht sind. Sie filmen das Verkehrsgeschehen aus der Perspektive des Fahrers und zeichnen es auf. Wenn alles gut geht, belegen die Aufnahmen nach einem Unfall bis ins Detail, was genau abgelaufen ist. So kann man möglicherweise belegen, dass ein anderer Verkehrsteilnehmer den Unfall verschuldet hat.

Aufnahmen von Dashcams unterliegen der DSGVO

Dashcams erfassen so gut wie immer auch Menschen. Dabei kann es sich um andere Autofahrer handeln, aber auch um Fußgänger auf der Fahrbahn oder um Passanten auf dem Gehsteig. Damit enthalten die Aufnahmen personenbezogene Daten. Sie unterliegen deshalb der DSGVO.

Das gilt für alle Formen von Dashcams

Außer der fast schon klassischen Dashcam, die am Armaturenbrett (englisch: Dashboard) angebracht und nach vorn ausgerichtet ist, gibt es auch Heckkameras. Sie dokumentieren das Geschehen hinter einem Fahrzeug. Motorradfahrer benutzen gern Helmkameras, weil eine Kamera am Lenker des Motorrads unpraktisch wäre.

Für alle diese Formen von Dashcams gelten dieselben rechtlichen Regeln.

Die „Haushaltsausnahme“ greift in aller Regel nicht

Wenn Privatpersonen personenbezogene Daten anderer Personen „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ verarbeiten, findet die DSGVO keine Anwendung. Diese Regelung ist in Art. 2 Abs. 2 Buchstabe c DSGVO enthalten. Sie wird meist als „Haushaltsausnahme“ bezeichnet. Für Aufnahmen mit Dashcams gilt diese Ausnahme nicht. Wenn jemand gezielt ein Verkehrsgeschehen filmt, an dem auch andere Personen beteiligt sind, betrifft das gerade nicht ausschließlich ihn persönlich.

Etwas anderes gilt nur für „Panoramafahrten“

Relevant wird die „Haushaltsausnahme“ nur dann, wenn persönliche Interessen bei den Aufnahmen völlig im Vordergrund stehen. Dies wäre etwa der Fall, wenn ein Motorradfahrer mit seiner Helmkamera die Fahrt auf einer landschaftlich reizvollen Strecke filmt. Dabei mag kurz auch einmal ein anderer Verkehrsteilnehmer ins Bild kommen. Der Fokus liegt aber auf der Strecke als solcher. Deshalb ist die DSGVO dann tatsächlich nicht anwendbar.

Die „3-Minuten-Regel“ ist der Maßstab

Die DSGVO lässt die Verarbeitung von personenbezogenen Daten zu, wenn das der Wahrung von berechtigten Interessen dient (Art. 6 Abs. 1 Buchstabe f DSGVO).

Wer ein Unfallgeschehen mit der Kamera dokumentieren will, hat ein solches berechtigtes Interesse.
Wenn es erst einmal „geknallt“ hat, ist es allerdings für das Einschalten der Kamera zu spät. Zudem ist gerade das wichtig, was unmittelbar vor dem eigentlichen Unfall abgelaufen ist. Daher darf eine Dashcam das Verkehrsgeschehen zwar fortlaufend aufzeichnen. Es muss aber sichergestellt sein, dass die Speicherkarte der Kamera immer nur eine Aufzeichnung von maximal 3 Minuten enthält. Nur dafür besteht ein berechtigtes Interesse.

Sensoren dürfen längere Aufzeichnungen auslösen

Viele Dashcams enthalten Sensoren, die auf außergewöhnliche Situationen wie Vollbremsung oder Schleuderbewegungen reagieren. In solchen Fällen geben sie ein entsprechendes Signal an die Speicherkarte. Es bewirkt, dass ab diesem Moment alle schon vorhandenen und noch erfolgenden Aufzeichnungen erhalten bleiben.

Sensoren dürfen längere Aufzeichnungen auslösen

Viele Dashcams enthalten Sensoren, die auf außergewöhnliche Situationen wie Vollbremsung oder Schleuderbewegungen reagieren. In solchen Fällen geben sie ein entsprechendes Signal an die Speicherkarte.
Es bewirkt, dass ab diesem Moment alle schon vorhandenen und noch erfolgenden Aufzeichnungen erhalten bleiben. Sie blockieren also die Löschroutine, die sonst für die Einhaltung der „3-Minuten-Regel“ sorgt. Das ist in Ordnung, weil besondere Vorfälle ein berechtigtes Interesse an einer länger dauernden Aufzeichnung begründen.

Innenkameras sind ein Sonderproblem

Manche Kameras zeichnen das Geschehen im Innenraum eines Fahrzeugs auf. Wer allein in einem Fahrzeug sitzt, kann das gern tun. Interessen anderer Personen werden dann nicht berührt. Wenn eine Familie gemeinsam in einem Fahrzeug unterwegs ist, gilt für solche Aufnahmen die „Haushaltsausnahme“. Anders sieht es dagegen aus, wenn andere Personen mit im Fahrzeug sitzen, etwa Kollegen oder Anhalter. In solchen Fällen wäre die Einwilligung dieser Personen nötig. Solche Einwilligungen einzuholen, ist in der Praxis kaum realistisch.

Geldbußen sind möglich

Wer sich als Fahrer eines Fahrzeugs nicht an die Regeln hält, muss durchaus mit Sanktionen rechnen. In einer ganzen Reihe von Fällen haben Aufsichtsbehörden für den Datenschutz Geldbußen von mehreren 100 € verhängt, wenn jemand eine Dashcam in unzulässiger Weise betrieben hat.

Wichtig: Klassische Datenpannen vermeiden!

Selbst wenn bei einer Datenpanne vordergründig „nichts Ernstes passiert“ zu sein scheint, gewähren die Gerichte neuerdings oft Schmerzensgeld. Voraussetzung ist, dass betroffene Personen zumindest für eine gewisse Zeit die Kontrolle über ihre Daten verloren haben. Diese Rechtsprechung betrifft gerade klassische Datenpannen, die viele kaum noch ernst nehmen.

Es geht schnell um erhebliche Beträge

Die Rechtsprechung des Europäischen Gerichtshofs (EuGH) zum DSGVO-Schadensersatz führt dazu, dass betroffene Personen nach Datenpannen häufig ein Schmerzensgeld durchsetzen können. Laut EuGH gewährt die DSGVO Schmerzensgeld selbst bei geringen Beeinträchtigungen. Auch ein kurzzeitiger Verlust der Kontrolle über die eigenen Daten gilt als Schaden, der ausgeglichen werden muss. Dieser Ausgleich erfolgt über ein Schmerzensgeld. Selbst wenn es im Einzelfall nur um 100 € geht – sollte eine größere Zahl von Personen betroffen sein, addiert sich dies rasch zu erheblichen Summen.

Ausgangspunkt sind oft banale Pannen

Alle Menschen in einem Unternehmen machen irgendwann einmal Fehler. Manchmal geht es dabei um die falsche Bedienung eines komplizierten EDV-Programms. Solche Pannen sind aber seltener, als viele glauben. Denn wer weiß, dass seine Tätigkeit fehlerträchtig ist, passt besonders gut auf. Bei scheinbar einfachen Tätigkeiten ist die Aufmerksamkeit dagegen oft viel geringer. Denn man fühlt sich sicher. Dies ist dann der Nährboden, auf dem banale Fehler mit erheblichen Folgen gedeihen.

Briefpost hat nach wie vor Bedeutung

Das papierlose Büro streben alle an. Oft kollidiert dieses Ziel aber mit Kundenwünschen und manchmal auch mit rechtlichen Notwendigkeiten.

Das Problem dabei: Gerade viele Jüngere versenden privat überhaupt keine Briefe mehr, Postkarten und dergleichen schon gar nicht. Es fehlt dann schlicht an der Übung, wie mit so etwas umzugehen ist. Wer es nicht glauben mag, frage einmal einen Praktikanten, an welche Stelle eines Briefumschlags die Anschrift gehört und an welche Stelle der Absender.

Ein Fehlversand von Unterlagen ist rasch passiert

In vielen Unternehmen, in Behörden ohnehin, existieren noch klassische Poststellen für Papierpost. Es ist ihr Job, eingehende Papierpost zu öffnen und für den korrekten Versand ausgehender Papierpost zu sorgen. Bei ihnen sind die nötigen Umschläge verschiedener Größe vorrätig und bei ihnen erfolgt auch die Beschriftung der Umschläge. Wehe, wenn dann langjähriges Personal in Rente geht und Neulinge nach dem Motto „das kann jeder“ kaum eingearbeitet werden! Schnell sind dann Unterlagen in einen Umschlag eingetütet, der an den falschen Adressaten gerichtet ist. Betreffen die Unterlagen Gesundheitsdaten, steht ein „Schmerzensgeld wegen Kontrollverlust“ von ohne Weiteres 1000 € im Raum. So die einschlägige Rechtsprechung.

Telefaxe gibt es nach wie vor

Der Einsatz von Telefaxgeräten ist oft Gegenstand von Spott über die angebliche Rückständigkeit von Behörden oder auch Unternehmen. Übersehen wird dabei, dass Telefaxe in wichtigen Branchen wie dem Gesundheitswesen, aber auch teils in der Logistik nach wie vor ein gängiges Arbeitsmittel sind. Dass es oft auch anders ginge, hilft dabei zunächst einmal nichts.

Klare Anweisungen sind notwendig

Viele sind sich zu schade dafür, neben das Telefaxgerät eine genaue Benutzungsanleitung zu hängen. Dabei wäre genau das notwendig, und zwar am besten mit durchnummerierten Vorgehensschritten und illustriert mit passender Bebilderung. Denn zu schnell ist aus dem Adressatenregister eine falsche Nummer ausgewählt. Und ein einmal versandtes Telefax lässt sich nicht mehr zurückholen. Peinlich, wenn dann – wie in Anwaltskanzleien schon geschehen – ein Text mit prozesstaktischen Überlegungen nicht an den eigenen Mandanten geht, sondern an den Prozessgegner. Diese Freude sollte man ihm nicht bereiten.

BCC und CC sind zwei verschiedene Dinge

Nach wie vor findet sich in gefühlt jedem zweiten Tätigkeitsbericht einer Aufsichtsbehörde die Schilderung eines Falls, bei dem jemand beim Mailversand die beiden Funktionen cc und bcc miteinander verwechselt hat. Erfolgt der Versand eines beliebten Newsletters versehentlich mittels cc statt wie eigentlich gewollt per bcc, können plötzlich Hunderte von Adressaten die Mailadressen aller anderen Adressaten im Klartext sehen. Selbst wenn nur einige Dutzend betroffene Personen Schadensersatz fordern und jeweils nur 50 € Schadensersatz durchsetzen können – es wäre mit etwas Aufmerksamkeit leicht zu vermeiden gewesen.

Eine Frage der Berechtigung

„Warum habe ich keinen Zugriff auf diese Datei?" Diese Frage stellen sich Nutzerinnen und Nutzer nicht selten. Wäre es nicht besser, wenn man auf möglichst viele Dateien „ungestört" Zugriff hätte? Das wäre doch gut für die Produktivität, denkt man. In Wirklichkeit aber müssen es so wenige Berechtigungen wie möglich sein. Lesen Sie hier, warum.

„Zugriff verweigert"

Auf den ersten Blick ist es ärgerlich. Man will dem Marketing bei der Messevorbereitung helfen und möchte dazu die Versandliste für die Einladungen öffnen. Plötzlich erscheint die Meldung auf dem PC, dass der Zugriff auf die Excel-Liste mit den entsprechenden Adressen verweigert wird. Was soll das? Dann kann man doch nicht aushelfen!

Tatsächlich mag dies die Produktivität im Moment etwas hemmen, denn ein Ausdruck der Versandaufkleber ist jetzt nicht möglich. Doch es gibt gute Gründe, warum Dateien vor Zugriffen geschützt werden, ein wichtiger Grund ist der Datenschutz.

Daten vor unbefugten Zugriffen schützen

Die Datenschutz-Grundverordnung (DSGVO) verlangt unter anderem einen Schutz vor „unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten".

Dafür ist ein Berechtigungssystem entscheidend, das die Zugriffe auf die Daten regelt und überwacht.
Zentral ist dabei die richtige und aktuelle Definition der Berechtigungen für alle Nutzerinnen und Nutzer. Es stellt sich die Frage, wer was wann mit welchen Daten tun können muss. Im Sinne des Datenschutzes und der Datensicherheit ist es, wenn die Rechte an Daten nur dann vergeben werden, wenn sie wirklich für die Erfüllung der Aufgaben erforderlich sind. Man spricht von dem Prinzip der minimalen Berechtigungen oder „Need to know".

Die minimalen Rechte sind auch dann ein Schutzfaktor, wenn Angreifer versuchen, die Berechtigungen auszunutzen, dann bekommen auch die Internetkriminellen nur einen minimalen Zugang zu den Daten.

Auch für interne Suchen und Auswertungen gelten die Grenzen

Dabei sind die Berechtigungen nicht nur dann wichtig, wenn man aktiv über den Datei-Explorer in Windows auf eine Datei wie die beispielhaft genannte Versandliste zugreifen will, es aber aktuell nicht darf, weil die Berechtigung (noch) nicht erteilt wurde.

Wenn man nun feststellt, dass man an eine Datei nicht gelangen kann, ob direkt oder indirekt über eine Suche, dann sollte man sich zuerst fragen, wofür man diese Datei wirklich braucht.
Besteht Bedarf für die Erfüllung aktueller Aufgaben, dann ist dies etwas, was man mit der oder dem Vorgesetzten besprechen sollte. Dann bekommt man temporär die erforderlichen Rechte, zum Beispiel zum Ausdrucken, aber nicht zum Schreiben in der Versandliste, wenn dies nicht erforderlich ist.
Dann kann man produktiv und sicher arbeiten.

Das Gleiche gilt, wenn man mit einem modernen PC arbeitet, der zum Beispiel einen lokalen KI-Dienst (Künstliche Intelligenz) bietet, um Auswertungen zu machen.
Über die KI dürfen auch nur solche Daten zugänglich werden, auf die der Nutzer oder die Nutzerin der KI selbst zugreifen darf. Das ist sehr wichtig für den datenschutzgerechten Einsatz einer KI oder einer internen Suchmaschine.

Wissen Sie, welche Rolle Berechtigungen in der IT spielen?

Frage: Wer eine Datei öffnen darf, kann sie auch verändern. Stimmt das?

1. Nein, es gibt unterschiedliche Rechte an Dateien, Öffnen und Schreiben/Verändern werden dabei unterschieden.
2. Ja, ist eine Datei erst einmal offen, kann man auch mit ihr arbeiten, sie also auch verändern.

Lösung Frage 1: Die Antwort 1. ist richtig. Beim Zugriff oder beim Arbeiten mit Dateien und Ordnern in Windows werden Berechtigungen wie Öffnen, Ändern, Speichern oder Löschen unterschieden. So können Dateien zur Ansicht freigegeben sein, aber im Status Schreibgeschützt vorliegen. Das ist auch sinnvoll, denn nicht jeder, der etwas lesen darf, sollte es auch verändern können, um gewollte oder ungewollte Manipulationen zu verhindern.

Frage: Das Prinzip „Need to know" bei Berechtigungen dient dem Datenschutz und der IT-Sicherheit. Stimmt das?

1. Ja, mit minimalen Berechtigungen lassen sich die Folgen von IT-Angriffen verringern.
2. Nein, dieses Prinzip behindert nur die Produktivität und ist umständlich.

Lösung Frage 2: Die Antwort 1. ist auch hier richtig. Wenn jeder nur die Rechte an Dateien bekommt, die tatsächlich für die Aufgabe benötigt werden, kann ein Angreifer, der die Identität übernimmt, auch weniger Berechtigungen missbrauchen. Wenn also eine Versandliste im Normalfall nicht von einer Nutzerin oder einem Nutzer benötigt wird, ist es richtig, sie nicht für den generellen Zugriff durch diese Person freizugeben.