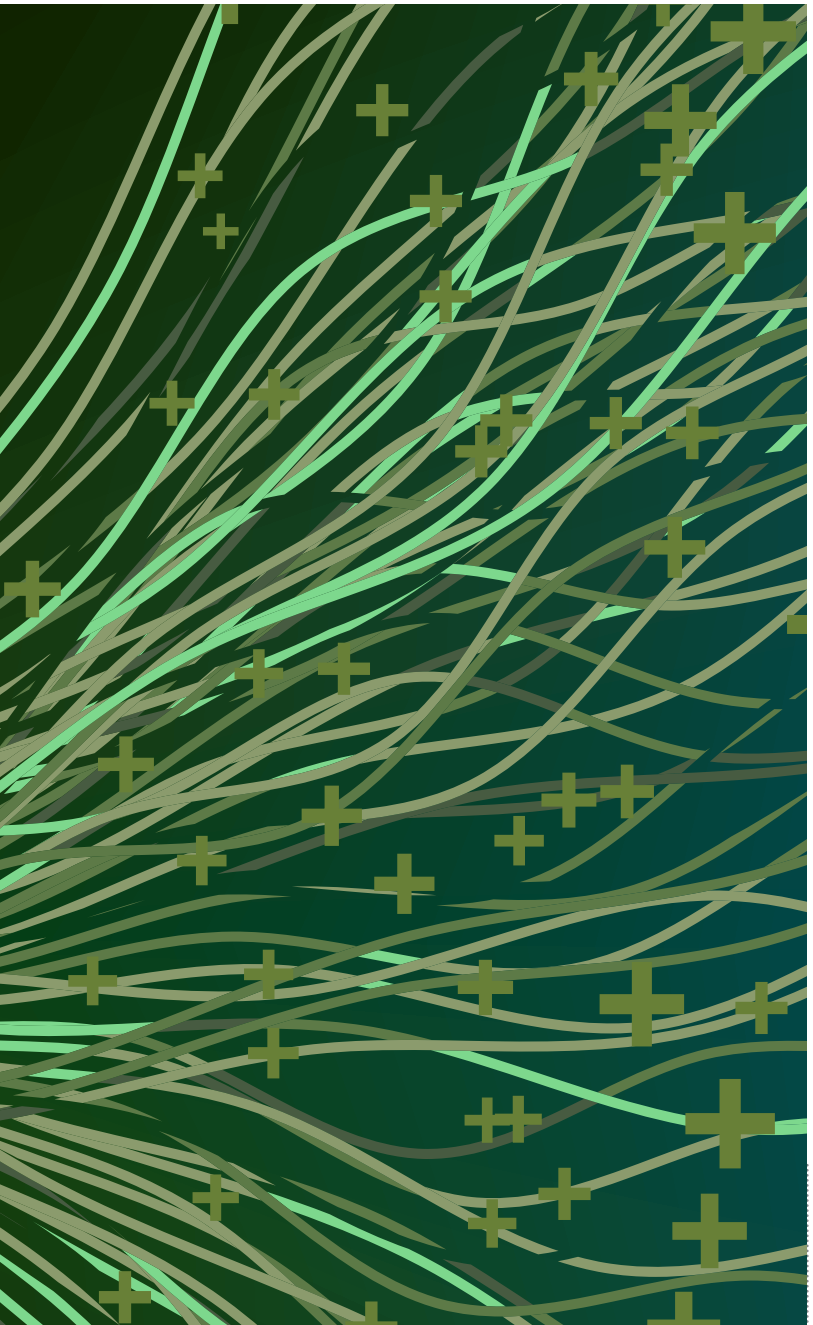
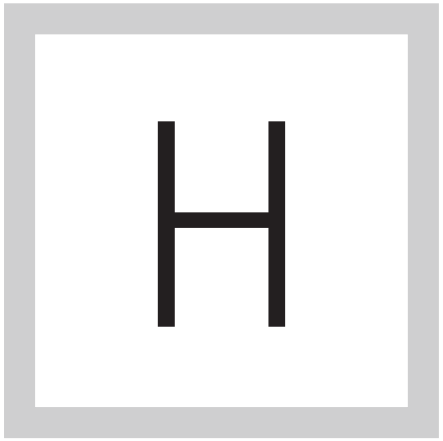


Special Report

WIE SIE FÜR VERBESSERTE DATENSICHERHEIT UND MEHR DATENSCHUTZKONTROLLE SORGEN

TechTarget | SearchSecurity.de



EUTZUTAGE SOLLTE SICH jedes Unternehmen mit der Thematik der Datensicherheit beschäftigen, da es bei Zwischenfällen in der Verantwortung steht. Die Einführung entsprechender Richtlinien führt oft zu einem trügerischen Gefühl der Sicherheit. Besonders mit dem zunehmenden BYOD-Trend und mobilen Daten sind Unternehmensdaten um einiges mehr verwundbar als vor einigen Jahren. Dieser E-Guide erklärt, wie Sie für optimierte Datensicherheit und mehr Datenschutzkontrolle sorgen.

DATENCONTAINER: REICHT DAS FÜR DIE DATENSICHERHEIT?

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn es durch rechtliche Vorschriften erlaubt wird oder der Betroffene eingewilligt hat. Um Unbefugte davon abzuhalten, die personenbezogenen Daten einzusehen, zu verändern, zu löschen oder anderweitig zu missbrauchen, sind zahlreiche Maßnahmen der Datensicherheit vorgeschrieben.

Werden zu schützende Daten mit anderen Daten gemeinsam vorgehalten, erscheinen die Schutzmaßnahmen besonders schwierig. Das zeigt sich zum Beispiel bei der betrieblichen Nutzung privater Endgeräte (BYOD, Bring Your Own Device). Hier werden betriebliche Daten und Anwendungen mit privaten Apps und Informationen gemeinsam gespeichert und genutzt. Auf die besonderen Datenrisiken weist zum Beispiel der Berliner Beauftragte für Datenschutz und Informationsfreiheit hin.

Viele Sicherheitslösungen bieten inzwischen die Kapselung von Daten und Anwendungen an, ein sogenanntes Containering. Es stellt sich die Frage, ob diese Abkapselung für den Schutz personenbezogener Daten ausreicht oder nicht?

DATENTRENNUNG IST EIN WICHTIGER SCHRITT

Werden bestimmte Daten von anderen abgekapselt, also verschiedene Datenbereiche in einem Speicher zum Beispiel des Smartphones oder Tablets geschaffen, hat dies klare Vorteile: Der Datenschutz verlangt, dass personenbezogene Daten nur für den Zweck ihrer Erhebung verarbeitet werden, sofern keine Einwilligung zur Zweckänderung vorliegt (Prinzip der Zweckbindung).

Private Daten und betriebliche Daten wurden aber ohne Zweifel für verschiedene Zwecke erhoben, so dass sie nicht ohne weiteres gemeinsam verarbeitet werden dürfen. Für Cloud-Dienste haben die Aufsichtsbehörden unterstrichen, dass die Daten verschiedener Mandanten strikt getrennt werden müssen (Mandantenfähigkeit). Eine Trennung in Datenbereiche, die eine zweckfremde Verarbeitung verhindert, ist also ganz im Sinne des Datenschutzes.

DOCH NICHT JEDE TRENNUNG IST WIRKLICH DICHT

Die grundsätzliche Idee hinter einem Datencontainer als Datentrennung ist, dass die betreffenden Daten über eine spezielle Anwendung (Container-App) mit Verschlüsselung geschützt werden. Ohne den Schlüssel können weder Nutzer noch andere Anwendungen auf die Daten zugreifen. So erhalten dann zum Beispiel

betriebliche Anwendungen die Berechtigung, betriebliche Daten zu verarbeiten und private Apps können private Informationen nutzen.

Doch die Verwendung von Container-Lösungen hat Vor- und Nachteile, worauf auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem Überblickspapier „IT-Consumerisation und BYOD“ hingewiesen hat. So sind Datencontainer ein einfacher Weg zur Datentrennung, bieten aber nicht den vollständigen Schutz, den sich so manches Unternehmen davon verspricht.

Einerseits hängt die Sicherheit der Datenkapsel von der Stärke der Verschlüsselung und von der Komplexität des gewählten Passwortes ab. Andererseits macht es wenig Sinn, die Daten in dem Container zu schützen, wenn die Übertragung der Informationen in und aus dem Container heraus nicht ausreichend geschützt ist. Verbindungen zum Netzwerk des Unternehmens müssen kryptografisch abgesichert werden. Container-Lösungen, die dies nicht unterstützen, bieten keinen hinreichenden Schutz und sollten daher nicht eingesetzt werden, so das BSI. Eine strikte Trennung der Datenbereiche erreicht man eher mit einer Virtualisierungs- als mit einer Container-Lösung.

AKZEPTANZ BEIM NUTZER HINTERFRAGEN

Wie Datenschützer unterstreichen, gibt es bei Container-Lösungen auch Probleme mit der Akzeptanz bei den Nutzern: Ist die Container-App nicht geöffnet, werden zum Beispiel keine beruflichen E-Mails empfangen. Anwender begreifen dieses Anwendungsverhalten als Fehler und sind nicht bereit zu akzeptieren, dass es sich um ein Leistungsmerkmal handelt, so der Hessische Datenschutzbeauftragte. Bei mangelnder Akzeptanz suchen Anwender jedoch bekanntlich nach Ausweichstrategien und versuchen, die Sicherheitslösung zu umgehen.

DATENCONTAINER SICHERN NICHT DIE VERFÜGBARKEIT

Einen weiteren Punkt dürfen Sie nicht vergessen: Die Kapselung von Datenbereichen über Container-Apps hat das Ziel, die missbräuchliche Nutzung der Daten zu verhindern, sie soll also gegen unerlaubte Zugriffe schützen. Für die Datensicherheit allerdings werden noch weitere Forderungen gestellt. So muss unter anderem auch die Verfügbarkeit der personenbezogenen Daten gewährleistet werden. Einen Schutz gegen versehentliches Löschen von Daten bieten Datencontainer allerdings nicht. Nach Eingabe des Container-Passwortes kann der Nutzer ohne weiteres Daten löschen oder auch Daten verändern (Integritätsverlust).

Die Maßnahmen der Verfügbarkeitskontrolle gegen den Datenverlust können durch Container-Lösungen sogar erschwert werden: Damit die Daten in dem Container bei dem regelmäßigen Backup berücksichtigt werden können, ist entweder die komplette Containerdatei zu sichern oder aber die Backup-Lösung benötigt Zugriff auf den Containerinhalt. Das ist insbesondere erforderlich, um eine Sicherung der Dateiänderungen vornehmen zu können. Eine Integration des Containers in das Backup ist aber nicht ohne weiteres gegeben.

CONTAINER-LÖSUNGEN IN DAS DATENSCHUTZKONZEPT INTEGRIEREN

Alleine durch die Einführung von Container-Lösungen ist die Datensicherheit also nicht gewährleistet. Vielmehr müssen Unternehmen die genauen Funktionen und Einschränkungen der Datencontainer kennen und bei ihrem Datenschutzkonzept berücksichtigen. Das gilt zum Beispiel bei den Vorgaben für Passwörter, bei der Freigabe von Anwendungen, bei der Vereinbarung für BYOD und bei der Datensicherung.

MEHR DATENSCHUTZKONTROLLE DURCH APP-ANBIETER UND APP-STORES ERFORDERLICH

Wenn es in Veröffentlichungen um Datenschutz und mobile Apps geht, steht meist der Nutzer im Fokus, so zum Beispiel in dem Faltblatt „Smartphones und Apps - Spione in der Hosentasche“, das unter anderem von dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz herausgegeben wurde.

Der teils große Aufklärungsbedarf bei Smartphone- und Tablet-Nutzern macht dies notwendig. Um den Datenschutz bei Apps aber umfassend verbessern zu können, gilt es, auch andere Zielgruppen anzusprechen.

So kann ein Nutzer lediglich auf eine App verzichten oder eine bereits installierte App wieder löschen, wenn Datenschutzlücken sichtbar werden. Ein nachhaltiger Datenschutz für Apps muss bei den App-Entwicklern, App-Anbietern und App-Stores ansetzen, ganz im Sinne des Prinzips Privacy by Design, das die Einhaltung des Datenschutzes schon in der Konzeption und Entwicklung von Lösungen verlangt.

AUFSICHTSBEHÖRDEN STELLEN VERANTWORTUNG KLAR

Generell sind die Entwickler und Anbieter der Apps gefordert, die gesetzlichen Anforderungen an eine datenschutzgerechte App zu erfüllen. Die Aufsichtsbehörden für den Datenschutz in Deutschland haben bereits mehrfach auf die zentralen Punkte hierbei hingewiesen, wie zum Beispiel in der Entschließung „Datenschutzgerechte Smartphone-Nutzung ermöglichen!“.

So gehören dazu die Transparenz für den Nutzer bezüglich der Preisgabe seiner personenbezogenen Daten, Steuerungsmöglichkeiten der Nutzer für die Preisgabe ihrer personenbezogenen Daten, Einflussmöglichkeiten auf das Löschen von Spuren bei der (mobilen) Internet-Nutzung sowie anonyme und pseudonyme Nutzungsmöglichkeiten für mobile Apps und Dienste. Neben den App-Anbietern und -Programmierern sehen die Aufsichtsbehörden aber auch die App-Store-Betreiber in der Pflicht und Mitverantwortung.

APP-STORES TRAGEN MITVERANTWORTUNG FÜR DEN APP-DATENSCHUTZ

Wie zum Beispiel der Landesbeauftragte für Datenschutz Baden-Württemberg betont hat, sind App-Store-Betreiber für die Bereitstellung von Datenschutzerklärungen mitverantwortlich. Wer Produkte vertreibt, müsse sich auch mitverantwortlich

zeigen, wenn es um Aufklärung und Transparenz beim Datenschutz geht, so der Landesdatenschutzbeauftragte.

App-Store-Betreiber müssten ihre passive Rolle im Datenschutz aufgeben und aktiv daran mitwirken, dass alle Apps, die personenbezogene Daten verarbeiten, auch eine Datenschutzerklärung haben, wie sie in Deutschland von dem Telemediengesetz (TMG) gefordert wird.

Die Mitverantwortung der App-Store-Betreiber bedeutet, dass der Datenschutz generell und speziell das Vorhandensein einer App-spezifischen, verständlichen, gut lesbaren und leicht zu findenden Datenschutzerklärung zu den Kriterien gehören, die für die Freigabe einer App für den App-Store erfüllt sein müssen. Bislang werden auch solche Apps in den App-Stores veröffentlicht, die keine solche Datenschutzerklärung besitzen, wie zum Beispiel Prüfungen einer Aufsichtsbehörde ergeben haben.

DATENSCHUTZERKLÄRUNG ALLEINE REICHT ABER NICHT

So wichtig die Datenschutzerklärung bei Apps auch für die Transparenz der Datenverarbeitung ist, sollten weitere Kriterien für den Datenschutz hinzukommen, die die App-Entwickler und App-Anbieter berücksichtigen. Die Aufsichtsbehörden

haben dazu eine eigene Orientierungshilfe veröffentlicht, die sich an Entwickler und Anbieter mobiler Apps richtet und datenschutzrechtliche und technische Anforderungen aufzeigt.

So gelten auch für mobile Apps die Datenschutzgrundsätze der Direkterhebung, der Datenvermeidung und der Datensparsamkeit, der anonymen und pseudonymen Nutzung, der Zweckbindung und der Erforderlichkeit der Verarbeitung, Speicherung und Nutzung personenbezogener Daten.

Heimliches Sammeln von Daten, die nicht für den offensichtlichen Zweck der App erforderlich sind, ist ebenso nicht erlaubt wie die Auswertung der erhobenen Daten zu anderen Zwecken. Leider gibt es zahlreiche Beispiele für Apps, die genau ein solches Verhalten aufweisen, wie das Sammeln von Standortdaten, obwohl diese für die vom Nutzer gewünschte Funktion der App nicht notwendig sind.

DATENSICHERHEIT MUSS GRUNDEIGENSCHAFT VON APPS SEIN

Neben den Anforderungen aus dem Datenschutz gibt es auch eine Reihe von Vorgaben zur Datensicherheit, die bei einer kleinen App ebenso wenig fehlen dürfen wie bei einer großen Serveranwendung.

Der sichere Umgang mit Anmeldedaten sollte bei Apps ebenso selbstverständlich

sein wie die geschützte Speicherung vertraulicher Nutzerdaten.

Auch hier gibt es leider genug Beispiele für Apps, die genau hier Schwachstellen aufweisen und die bereits Fälle von Datendiebstahl ermöglicht haben.

Apps haben eine so große Verbreitung gefunden, dass sie nicht nur zu einem wichtigen Geschäftsfeld für Softwarehäuser und Werbeagenturen geworden sind. Sie können auch zu einem erheblichen Datenrisiko beitragen, das weit über das Missbrauchspotenzial auf mobilen Endgeräten hinausgeht.

Ohne guten Datenschutz und zuverlässige Datensicherheit können Apps zur Hintertür in Firmennetzwerk und Clouds werden. Jede Anstrengung für mehr App-Datenschutz lohnt sich also gleich mehrfach.

Außerdem können Sie in unserem Social Network, dem IT Knowledge Exchange, praxisnahe Erfahrungsberichte mit Fachkollegen und Experten in Echtzeit austauschen.

WAS MACHT TECHTARGET SO EINZIGARTIG?

Bei TechTarget steht die Unternehmens-IT im Mittelpunkt. Unsere Autoren und das Redaktions-Team sowie auch unser großes Netzwerk an Industrieexperten bietet Ihnen Zugriff auf die neuesten Entwicklungen und relevantesten Themen der Branche.

TechTarget liefert klare und überzeugende Inhalte und umsetzbare Informationen für die Profis und Entscheidungsträger der IT-Branche. Wir nutzen die Schnelligkeit und Unmittelbarkeit des Internets, um Ihnen in realen und virtuellen Kommunikationsräumen hervorragende Networking-Möglichkeiten mit Fachkollegen zu ermöglichen.