Die neue EU-Datenschutzverordnung kommt – so viel scheint sicher

Fünf Gründe weshalb Verschlüsselung eine wichtige Rolle spielt

Es ist als sicher zu betrachten, dass die neue EU-Datenschutzverordnung kommt. In den ersten Gremien und Abstimmungen auf EU-Ebene erfährt diese Gesetzesinitiative breite Zustimmung aus allen europäischen Ländern. Mit der neuen EU-Datenschutzverordnung sollen die Datenschutzrechte von EU-Bürgern gestärkt, das Vertrauen in Online-Aktivitäten wiederhergestellt und Kundendaten durch die Einführung neuer Datenschutzprozesse und Kontrollen in Unternehmen besser geschützt werden. Der derzeitige Gesetzesentwurf umfasst knapp 100 Artikel und wird sicherlich noch durch den einen oder anderen ergänzt werden. Die Gesetze werden für alle Unternehmen auf europäischem Boden gelten, auch für diejenigen, deren Muttergesellschaft außerhalb der europäischen Union beheimatet ist.

Hohe Strafen für Gesetzesverletzungen

Die neuen Gesetze definieren momentan noch nicht, welche Technologien zur Einhaltung zu verwenden sind, legen jedoch ganz klar fest, in welchem Umfang die Sicherheit in der Datenverarbeitung vorausgesetzt wird. So müssen beispielsweise die für die Verarbeitung Verantwortlichen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische geeignete Maßnahmen für ein Schutzniveau treffen, das den Risiken angemessen ist. Eine solche Sicherheitspolitik umfasst, unter Berücksichtigung des Stands der Technik und der Implementierungskosten, folgendes:

1. die Fähigkeit zu gewährleisten, dass die Vollständigkeit der personenbezogenen Daten bestätigt wird
2. die Fähigkeit, die Vertraulichkeit, Vollständigkeit, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen
3. die Fähigkeit, die Verfügbarkeit und den Zugang zu Daten rasch im Falle eines physischen oder technischen Vorfalls (...) wiederherzustellen (...)

Des Weiteren muss ein Unternehmen bei einer Verletzung des Schutzes personenbezogener Daten nach Artikel 32 der Gesetzesvorlage unverzüglich die Aufsichtsbehörde benachrichtigen.

Erfüllt ein Unternehmen diese Vorschriften nicht, muß gemäß Artikel 79 mindestens eine der folgenden Sanktionen verhängt werden:

1. eine schriftliche Verwarnung im Fall eines ersten und nicht vorsätzlichen Verstoßes,
2. regelmäßige Überprüfungen betreffend den Datenschutz,
3. eine Geldbuße bis zu 100.000.000 EUR oder, im Fall eines Unternehmens, bis zu 5 Prozent seines weltweiten Jahresumsatzes, je nachdem, welcher der Beträge höher ist.

Zusammengefasst: Wenn ein Unternehmen keine entsprechenden Maßnahmen zum Schutze sensibler Daten umgesetzt hat, muss es mit empfindlich Strafen rechnen. Hinzu kommt ein zusätzlicher Schaden hinsichtlich Reputation, Firmengeschäftswert oder Vertrauen bei Kunden.

Verschlüsselungsverfahren bringen Sicherheit

Kaum ein Unternehmen wird sich hohe Strafen oder gar Imageverluste leisten wollen. Die Sicherheit der Daten muss also gewährleistet sein. Doch welche Strategie und welche Technologie kann dies möglichst einfach und ohne hohe Budget- und Ressourcenbelastung garantieren? Ein probates Mittel zum Schutze der Daten und im Sinne der Einhaltung von Datenschutzverordnungen ist die Verschlüsselung. Fünf Gründe warum:

1. Moderne Verschlüsselung ist quasi unmöglich zu knacken. Ein Cyberkrimineller, der sich etwa Zugang zu verschlüsselten Daten verschafft hat, kann damit rein gar nichts anfangen, da er sie nicht auslesen kann. Bis auf den ärgerlichen Diebstahl (unlesbarer!) Daten, wurde dem betroffenen Unternehmen also kein weiterer Schaden zugefügt und es sind keine weiteren Konsequenzen zu befürchten.
2. Datenverschlüsselung funktioniert auch in der Cloud. Immer mehr Unternehmen verlagern ihre Daten in die Cloud und sind somit auf die Sicherheitsvorkehrungen externer Provider angewiesen. Mit einer Verschlüsselung sind die Daten für unbefugte nicht lesbar und somit wertlos.
3. Mobile Geräte sind gerade für sensible Daten ein hohes Risiko. Auch hier greifen Verschlüsselungstechnologien. Diese Daten können von unautorisierten Geräten nicht angezeigt werden. Somit hat ein Unternehmen Kontrolle darüber, auf welchen Geräten die Daten in welchem Sicherheitszustand gespeichert sind.
4. Geeignete Verschlüsselungstechnologien bieten ein zentrales Management, das sowohl Computer, Netzlaufwerke, Wechselmedien und in der Cloud gespeicherte Daten für Windows und Mac verwaltet. Damit kann ein Unternehmen sicherstellen, dass mit relativ geringem Aufwand ein sehr hohes Maß an Schutz realisiert werden kann und Strafen nach der EU-Datenschutzverordnung nicht zu befürchten sind.
5. Gute Verschlüsselungstechnologien bieten nützliche Zusatzfunktionen. Audit- und Reportfunktionen beispielsweise unterstützen die Compliance-Anstrengungen, damit die IT-Abteilung jederzeit nachweisen kann, dass eine Datei, ein Rechner oder ein externer oder mobiler Datenspeicher zum Zeitpunkt des Verlusts, Diebstahls oder Verstoßes gegen den Datenschutz verschlüsselt war.

Sophos SafeGuard kann diese Anforderungen an die Verschlüsselung erfüllen. Alle Geräte werden unabhängig von der Plattform geschützt, ohne dass die Benutzer bei ihrer Arbeit gestört werden oder ihre Arbeitsweise anpassen müssen. SafeGuard folgt den Daten und schützt sie dort, wo sie gerade sind. Egal ob in der Cloud, auf Wechselmedien, in Netzwerkdateien oder auf mobilen Geräten.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de