IT-Sicherheit und die EU-Datenschutznovelle: Worauf deutsche Unternehmen sich einstellen müssen

von Sebastian Nerz

Im Rahmen der Erstellung des IT-Sicherheitsgesetzes, wurde in Deutschland viel über Meldepflichten für Angriffe auf IT-Systeme diskutiert. Der aktuelle Entwurf zum IT-Sicherheitsgesetz sieht jetzt tatsächlich auch Meldepflichten bei IT-Sicherheitsvorfällen vor – allerdings nur für bestimmte Branchen und Unternehmen. So gibt es diese Meldepflichten für Betreiber „kritischer Infrastrukturen", also für manche Unternehmen aus den Bereichen Energie, IKT, Finanzen, Gesundheit, Wasser, Ernährung und Transport/Verkehr.

Für einen Teil dieser Unternehmen werden diese Meldepflichten nichts Neues sein. Weniger bekannt ist vielen Unternehmen aber, dass die Meldepflichten bezüglich Datenschutz aller Wahrscheinlichkeit nach verschärft werden. Seit mehreren Jahren ist die EU-Datenschutznovelle bereits in Arbeit. Die aktuellen Entwürfe des EU-Parlamentes und der EU-Kommission stellen beide Anforderungen an Datensicherheit und formulieren entsprechende Meldepflichten. Die Novelle sieht dabei Schutzziele vor, die sich weitgehend mit den Zielen der Informationssicherheit decken – geschützte Daten dürfen nicht unberechtigt verändert, zerstört, verarbeitet oder eingesehen bzw. verbreitet werden. Diese Bedingungen dürften für Unternehmen – unabhängig von rechtlichen Aspekten – keine Neuerungen darstellen und soweit selbstverständlich sein. Neu für Unternehmen werden hier allerdings die Meldepflichten.

Schon jetzt gelten für Unternehmen Meldepflichten nach §42a des Bundesdatenschutzgesetzes. Wenn unberechtigte Dritte Zugriff auf besonders schützenswerte Daten hatten – wenn also beispielsweise auf Kontodaten, Informationen über Krankheiten oder Gewerkschaftszugehörigkeiten zugegriffen wurde – , so muss dies unverzüglich der zuständigen Aufsichtsbehörde gemeldet werden. Unter bestimmten Umständen müssen auch die Betroffenen selbst darüber informiert werden. Dies kann jedoch solange warten, bis beispielsweise eine Strafverfolgung nicht mehr gefährdet wird und die Daten gesichert wurden.

Mit der geplanten EU-Datenschutznovelle kommen auf Unternehmen neue gesetzliche Anforderungen im Bereich IT-Sicherheit zu.
Quelle: Zsschreiner/Shutterstock.com

Mit der erwarteten EU-Datenschutznovelle werden diese Pflichten nochmals erweitert. Je nachdem, ob man von der Fassung der europäischen Kommission oder derjenige des Parlaments ausgeht, bestehen die Meldepflichten weiterhin „unverzüglich" (EU-Parlament) oder „ohne unangemessene Verzögerung" und „nach Möglichkeit binnen 24 Stunden" (Kommission). Im Unterschied zu den bisherigen Definitionen sind hier aber nicht mehr nur unberechtigte Veröffentlichungen von Daten erfasst; auch beispielsweise bereits eine unberechtigte Veränderung könnte darunter gefasst werden.

Darüber hinaus werden die Meldepflichten detaillierter gefasst und selbige Pflichten an Betroffene schärfer formuliert. Während bisher nur besonders schützenswerte Daten erfasst waren, sind es nun alle Daten, die von der Datenschutznovelle erfasst werden. Insbesondere müssen auch keine „schwerwiegenden Beeinträchtigungen für die Rechte" der Betroffenen existieren, eine Verletzung der Privatsphäre oder eine Verletzung des „Schutzes der personenbezogenen Daten" ist nun ausreichend für eine Meldepflicht.

Sollte sich das Europäische Parlament durchsetzen, werden sich für Unternehmen noch sehr viel mehr direkte Folgen aus der geplanten Novelle ergeben. So müssen beispielsweise regelmäßige Überprüfungen der Schutzmaßnahmen nachgewiesen werden. Außerdem werden die Meldepflichten umfangreicher und müssen für die Betroffenen verständlicher formuliert werden. Risikoanalysen werden eingeführt und es wird ein öffentliches Verzeichnis von Angriffsarten geführt. Nicht zuletzt sehen alle Vorschläge vor, dass wahlweise die Kommission oder der europäische Datenschutzausschuss die Regelungen konkretisieren und damit auch neue Anforderungen definieren können. Es bleibt abzuwarten, welche weiteren Bedingungen sich dadurch ergeben – Auditierungs- und Dokumentationspflichten für Sicherheitsmaßnahmen und bei Vorfällen sind zu erwarten.

Für Unternehmen hat die Datenschutznovelle nun mehrere Folgen. Erstens müssen die Anforderungen an Informationssicherheit stärker als bisher berücksichtigt werden. Zweitens werden kryptographische Schutzmaßnahmen wichtiger: Der Nachweis einer entsprechend wirksamen Verschlüsselung von Daten kann im Falle eines Angriffs auf die IT-Systeme

einige negative Folgen und rechtliche Anforderungen ersparen bzw. vereinfachen. Drittens müssen Unternehmen stärker als bisher Sorge dafür tragen, dass Angriffe auf IT-Systeme sauber analysiert und dokumentiert werden.

Die bisher in vielen Unternehmen praktizierte Vorgehensweise, einen Angriff durch ein reines Neuaufsetzen der betroffenen Maschinen zu beenden, wird sich mit den neuen Regelungen nicht mehr halten lassen: Unternehmen müssen damit rechnen, dass sie Angriffswege nachvollziehen und schließen müssen, dass sie genauer dokumentieren müssen, welche Daten betroffen sind und dass sie auch bisher nicht betroffene Arten von Angriffen betrachten müssen.

Die SySS GmbH möchte an dieser Stelle dringend empfehlen, die Logging- und Monitoring-Richtlinien im Unternehmen zu überprüfen und gegebenenfalls Administratoren und IT-Verantwortliche in den wichtigsten Grundlagen der Incident-Behandlung zu schulen. Die neuen Meldepflichten werden es Unternehmen nicht einfacher machen, IT-Sicherheit fach- und rechtskonform zu betreiben.

Unsere Abteilung für Digitale Forensik und Incident Response sowie unsere speziell auf diesen Bereich abgestimmten Schulungsmodule bieten hier entsprechende Unterstützung.