Hackerangriffe sind schon jetzt schon für Unternehmen ein Horrorszenario. Durch die DSGVO kommt auf sie ein hoher Verwaltungsaufwand zu und das Problem, die DSGVO-Konformität wieder herzustellen. (Bild: Pixabay / CC0)

Hackerangriffe und Ransomware

Was die DSGVO bei Cyberangriffen fordert

28.03.18 | Autor / Redakteur: Stèphane Estevez / Peter Schmitz

Nur noch wenige Wochen bleiben Unternehmen, bis die Übergangsfrist für die neue Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 endet. Eine Deadline, die Firmen vor Herausforderungen stellt. Zum Beispiel im Hinblick auf die Auswirkungen für den Datenschutz, wenn trotz aller Sicherheitsvorkehrungen Hacker in das Datensystem eindringen.

Die Datenschutz-Grundverordnung verschafft EU-Bürgern mehr Kontrolle über ihre personenbezogenen Daten, sorgt für Transparenz bei der Verwendung der Daten und verlangt Sicherheit und Kontrollen zum Schutz der Daten. Dabei setzt sie auf eine breite Definition von Personendaten: Alle Daten, die einen Rückschluss auf eine reale Person zulassen, fallen in den Regulationsbereich der DSGVO – egal, ob das IP-Adressen oder die Lieblingsfarbe ist. Bei einem Verstoß gegen die DSGVO drohen Unternehmen hohe Geldstrafen. Seit der Verabschiedung der DSGVO beschäftigt Unternehmen die Frage, wie sie den Datenschutzanforderungen gerecht werden können. Doch was passiert, wenn Ransomware alle Schutzwälle nieder reißt?

Doch zahlreiche Vorfälle der vergangenen Jahre zeigen, dass eine vollständige Datensicherheit nahezu nicht gewährleitet werden kann. Die DSGVO hat es sich daher zum Ziel gemacht, das Vertrauen in die Digitalwirtschaft zu stärken – sie verbietet nichts, reguliert aber alles. Die neue Datenschutzverordnung gibt Unternehmen eine Vorgabe, was sie hinsichtlich Datenschutz und –Sicherheit tun müssen. Doch was passiert, wenn trotz aller Vorkehrungen Hacker in das Datensystem dringen? Dann steht das Thema Datenschutz plötzlich in neuem Licht. Was müssen Unternehmen tun, um trotzdem DSGVO-konform zu sein?

Klarheit bei der Datenschutz-Grundverordnung
9 DSGVO-Mythen enttarnt!

09.01.18 - Die Vorbereitungen auf die DSGVO / GDPR kommen bei vielen Unternehmen nicht schnell genug voran. Umso wichtiger ist deshalb die Aufklärung, was wirklich hinter der Datenschutz-Grundverordnung steckt. Aktuell kursieren viele Mythen und falsche Informationen zur DSGVO im Netz. Wir klären auf. lesen

MEHR ZUM THEMA

< PresseBox - unn | UNITED NEWS NETWORK GmbH

< totemo ag

share me

share me

tweet me

share me

PDF

Weiterempfehlen

Drucken

Was tun bei Hackerangriffen nach DSGVO?

Vor allem Viren- und Ransomware-Angriffe können als schwerwiegender Verstoß gegen die DSGVO angesehen werden. Nicht selten sind die eigenen Mitarbeiter im Unternehmen das Einfallstor für Hacker. Ausgeklügelten Social-Engineering-Angriffen kann vorgebeugt werden, indem Unternehmen ihre Mitarbeiter entsprechend schulen – und genau das verlangt auch die DSGVO in Artikel 39 Absatz 1a:

Artikel 39 DSGVO „Aufgaben des Datenschutzbeauftragten"
(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:
a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten. […]

Die DSGVO bietet eine weit gefasste Definition von Datenschutzverletzungen und Ransomware-Angriffen, die in Artikel 4 Absatz 12 festgelegt ist:

Artikel 4 DSGVO „Begriffsbestimmungen"
(12)„Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. […]

Welche Schritte Unternehmen bei einer Verletzung nach dieser Definition gehen müssen, ist in Kapitel 33 und 34 der DSGVO geregelt:

Artikel 33 DSGVO „Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde"
(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. […]

Laut Absatz 3 in Artikel 33 muss die Meldung mindestens folgende Informationen enthalten: Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, Namen und Kontaktdaten des Datenschutzbeauftragten, Beschreibung der wahrscheinlichen Folgen der Verletzung, Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Folgen. Ist es einem Verantwortlichen nicht möglich, diese Information gleichzeitig zur Verfügung zu stellen, können diese laut Absatz 4 Artikel 33 auch schrittweise zur Verfügung gestellt werden.

Datenschutz-Grundverordnung, Artikel 32
DSGVO sorgt mit „Stand der Technik" für Verwirrung

07.02.18 - Die Datenschutz-Grundverordnung sorgt bei vielen Unternehmen ohnehin schon für reichlich Stress, aber eine spezielle Anforderung der DSGVO sorgt für besondere Verwirrung: Artikel 32 verpflichtet Unternehmen, ihre Daten dem „Stand der Technik" entsprechend zu schützen. Das Problem dabei: IT-Entscheider und Hersteller sind sich in der Interpretation dieser Vorgabe alles andere als einig. lesen

Auf Basis dieser beiden Artikel kann ein Unternehmen diesen Anforderungen nur entgehen, wenn sie nachweisen kann, dass die Daten durch eine Form der Verschlüsselung für die Angreifer nicht lesbar sind.

In besonderen Fällen müssen Unternehmen sogar die betroffenen Personen informieren – dieser Aspekt ist in Kapitel 34 der DSGVO geregelt:

Artikel 34 DSGVO „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person“
(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung. […]

In Absatz 3 Kapitel 34 wird außerdem aufgeführt, wann dies nicht erforderlich ist.

Datenschutz-Grundverordnung im Mittelstand
Was KMU jetzt für die DSGVO unbedingt noch tun müssen

19.01.18 - Viele Unternehmen haben Schwierigkeiten mit der Umsetzung der DSGVO, das gilt für kleine und mittlere Unternehmen (KMU) ganz besonders. Weil aber bei KMU meist besondere Herausforderungen in Form von knappem Budget und wenig Personal zusammen kommen, sind jetzt Prioritäten gefragt, was in den nächsten Monaten zuerst angegangen werden muss. lesen

Welche Maßnahmen können zur Vorbeugung getroffen werden?

Welche Aspekte seitens der Unternehmen zur Schutzgewährleistung zu berücksichtigen sind, ist in Kapitel 32 der DSGVO festgelegt. Doch konkrete Maßnahmen zur Orientierung finden Unternehmen in der Datenschutzverordnung nicht. Einige halten Datensicherungen für die beste Verteidigung - doch immer mehr Ransomware-Hacker greifen auf Backups zu, bevor sie mit der Verschlüsselung von Produktionsservern oder Workstations beginnen. Die Replizierung von Disk Deduplizierungsappliances kann helfen, sich vor Ransomware-Angriffen zu schützen, indem sie eine Art Luftpolster erzeugt. Außerdem kann die Verwendung nicht standardmäßiger NAS-Protokolle dazu beitragen, dass Backup-Ziele bei Hackerangriffen versteckt bleiben. Doch der einzige Weg, um vollständig geschützt zu sein, ist die Verwendung von Offline-Medien wie Tape. Ein pragmatischer Ansatz kann darin bestehen, eine Kopie der Daten auf Tape mit einer ein- oder zweimonatigen Aufbewahrungsfrist vorzuhalten. Tape ermöglicht es, eine Lösegeld-freie Zone zu erstellen, die nichts verbirgt, sondern physisch von Ihrem Netzwerk getrennt ist. Selbst ein kompromittiertes Backup-Administratorkonto kann nicht auf Ransomware zugreifen und diese dann verwenden, um Backups auf Band zu verschlüsseln.

Hackerangriffe sind auch jetzt schon für Unternehmen ein Horrorszenario. Mit Inkrafttreten der DSGVO kommt auf Unternehmen vor allem ein hoher Verwaltungsaufwand zu. Viel problematischer können jedoch die notwendigen Maßnahmen werden, um im Nachgang die DSGVO-Konformität wieder herzustellen. Unternehmen sollten daher ihr Datensystem hinsichtlich Angriffsflächen genau unter die Lupe nehmen und dabei alle möglichen Hintertüren wie Backup-Vorrichtungen prüfen.

Über den Autor: Stéphane Estevez blickt auf mehr als 16 Jahre Erfahrung im Product Marketing in der High-Tech-Industrie zurück. Bei Quantum ist er als Backup and Disaster Recovery Product Marketing Manager in der Region EMEA für Archivierungslösungen zuständig.

Fragen zur Datenschutz-Grundverordnung
Was man bei der DSGVO erst später richtig angehen kann

26.01.18 - Viele Unternehmen schaffen es nicht, die Anforderungen der DSGVO fristgerecht umzusetzen. Das liegt an Unklarheiten in der Verordnung, aber oft auch an mangelnder Vorbereitung. Es hilft nichts, die Datenschutz-Grundverordnung muss dennoch zum Stichtag 25. Mai 2018 vollständig umgesetzt sein. Bei einigen Punkten gilt es trotzdem, auf weitere Informationen zu warten. lesen

Datenschutz-Grundverordnung im Mittelstand