LEITFADEN

McAfee
Together is power.

Mini-Leitfaden zur Datenschutz-Grundverordnung

Einführung

Die Datenschutz-Grundverordnung (DSGVO) bringt die längst überfällige Modernisierung und Vereinheitlichung der Gesetze zu Datenschutz und Privatsphäre in der gesamten Europäischen Union. Sie ersetzt eine Richtlinie aus Zeiten, bevor Telefone smart wurden und Clouds die Geschäftswelt veränderten.

Es wurde viel über die durchaus erheblichen Geldbußen geschrieben, die bei Nichteinhaltung der DSGVO verhängt werden können. Statt sich jedoch auf die Geldbußen zu konzentrieren, sollten Sicherheitsexperten die DSGVO eher als hervorragende Chance sehen – als Chance, bei der Unternehmensführung die empfohlenen Vorgehensweisen zur Gewährleistung von Privatsphäre und Datenschutz in den Mittelpunkt zu rücken, die wir seit Jahren verfechten.

Dieser Leitfaden soll Sie bei der Vorbereitung auf die DSGVO unterstützen. Er zeigt die wichtigsten Fakten sowie Zahlen auf und geht auf die Fragen ein, mit denen Unternehmen feststellen können, wie gut sie vorbereitet sind. Außerdem werden die umfangreichen Tools vorgestellt, mit denen Unternehmen die Prozesse einrichten können, die zur Einhaltung der DSGVO erforderlich sind. Abschließend enthält dieser Leitfaden eine kurze Referenzliste mit den wichtigsten Fakten, die Informationssicherheitsexperten für die Vorbereitung benötigen.

1. Die wichtigsten Fakten zur DSGVO
2. Wie gut ist Ihr Unternehmen auf die DSGVO vorbereitet? 10 Fragen, die Sie stellen sollten
3. Die Prozesse und Funktionen, die zur Einhaltung der DSGVO erforderlich sind
4. Messung der Sicherheitsergebnisse

1. Die wichtigsten Fakten zur DSGVO

- Die Datenschutz-Grundverordnung (DSGVO) wurde am 14. April 2016 vom EU-Parlament verabschiedet und tritt am 25. Mai 2018 in Kraft.
- Die DSGVO ersetzt die bestehende Datenschutz-richtlinie 95/46/EG. Ihr Ziel ist die Vereinheitlichung der Datenschutzgesetze innerhalb der EU sowie die Stärkung der Rechte der EU-Bürger.
- Die Verordnung (keine Richtlinie) gilt sofort für das gesamte EU-Gebiet. Die Mitgliedsländer müssen keine individuellen Gesetze verabschieden.
- Die Geldbußen für die Nichteinhaltung der DSGVO-Bestimmungen sind erheblich – bis zu 20 Millionen EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes (je nachdem, welcher der Beträge höher ist).
- Einer der Grundsätze der DSGVO verlangt „standardmäßigen Datenschutz“. Das bedeutet, dass Datenschutz und Privatsphäre in allen Unternehmen Priorität haben und nicht erst nachträglich hinzugefügt werden sollen.

25. Mai 2018 –
die DSGVO tritt in Kraft

Ersetzt die bestehende Daten-schutzrichtlinie 95/46/EG

Eine Verordnung, keine Richtlinie

Geldbußen bis zu 20 Mio. EUR
oder bis zu 4 % des gesamten
weltweiten Jahresumsatzes

Datenschutz standardmäßig
integriert, nicht nachträglich
hinzugefügt

2. Wie gut ist Ihr Unternehmen auf die DSGVO vorbereitet?

Die DSGVO ist eine umfangreiche Rechtsvorschrift. Doch wo sollen Unternehmen ansetzen? Wir haben ein Team aus Experten für Datenschutz, Compliance sowie Technologie zusammengestellt und gebeten, die wichtigsten Fragen zu formulieren, die sich Unternehmen in Bezug auf die Einhaltung der DSGVO stellen sollten.

Für viele Unternehmen lauten diese Fragen: „Wo sollen wir ansetzen?“ und „Was sollte Priorität erhalten?“

Die Unternehmensführung sowie die Sicherheitsverantwortlichen sollten ihr bestehendes Datensicherheitsprogramm einer genauen Prüfung unterziehen und sich dann die 10 nachfolgenden Fragen stellen. Account Manager und Pre-Sales-Techniker sollten diese Erkundungsfragen in Kundengespräche zum Thema DSGVO einbauen.

1. Ist in unserem Unternehmen eine Kultur der Datensicherheit und des Sicherheitsbewusstseins etabliert?

Alle Personen im Unternehmen – von Führungskräften bis hin zu Anwendern, Administratoren und Entwicklern – müssen geschult, zertifiziert und darauf vorbereitet werden, eine Unternehmenskultur zu unterstützen, in der Datensicherheit und Privatsphäre standardmäßig eine große Rolle spielen. In vielen Fällen muss zur Vorbereitung auf die neue Verordnung zunächst ein Datenschutzbeauftragter ernannt werden, der für die Einhaltung der Vorschriften und die Kommunikation mit den Aufsichtsbehörden verantwortlich ist.

Diese neue Position und die Unterstützung durch die Unternehmensführung sind für eine positive Änderung der Unternehmenskultur erforderlich.

2. Wissen wir, welche Datenschutz-relevanten Daten wir erfassen und wo diese gespeichert sind?

Ein zentraler Grundsatz der DSGVO verlangt die Datenminimierung, d. h. dass nur die Daten erfasst werden, die zur Bereitstellung einer Ware oder eines Dienstes erforderlich sind. Wenn das Unternehmen versteht, welche Daten erfasst werden, kann es sich auf die Compliance konzentrieren, statt einen pauschalen und kostenintensiven Ansatz zu verfolgen.

Außerdem können Sie den Schutz der Daten nur dann gewährleisten, wenn Sie die wichtigen Repositorys, Anwendungen und geschäftlichen Abläufe kennen. Viele Programme zum Schutz vor Datenverlusten versagen aus genau diesem Grund. Heute sind Daten überall verteilt, zunehmend auch auf Mobilgeräten und in Cloud-Systemen, wo sie noch stärker durch Angriffe oder Missbrauch gefährdet sind.

Daher wäre es wichtig, die Implementierung eines Programms zur kontinuierlichen Datenerkennung, -bestandserfassung und -klassifizierung in Betracht zu ziehen. Zu diesem Programm sollte auch ein funktionsübergreifendes Team aus Geschäftsdaten-Eigentümern, Sicherheitsprozess-Verantwortlichen und Datensicherheitsexperten gehören.

Für viele Unternehmen lauten diese Fragen: „Wo sollen wir ansetzen?“ und „Was sollte Priorität erhalten?“.

3. Verwenden wir Verschlüsselung zum Schutz der Daten?

Verschlüsselung ist eine wichtige Maßnahme zur Minimierung der Folgen von versehentlichen sowie absichtlichen Datenlecks und sollte überall dort angewendet werden, wo Daten gespeichert oder übertragen (insbesondere bei mobilen Geräten wie Notebooks) bzw. in Cloud-Dienste hochgeladen werden. Der McAfee®-Forschungsbericht „Wachsendes Vertrauen in die Cloud“[1] zeigte, dass 74 % aller Unternehmen sensible Daten in der Cloud speichern. Außerdem zeigen die Untersuchungen von McAfee zu Datenexfiltrationstechniken, dass mehr als ein Drittel der Kompromittierungen in der Cloud erfolgen.

4. Ist bereits ein Datensicherheitsprojekt implementiert oder ist die Einführung eines solchen Projekts für dieses Jahr geplant?

Die Implementierung eines Datensicherheits-programms einschließlich Host- und Netzwerk-basierter Kontrollpunkte für die Richtlinienerzwingung ist dringend erforderlich, um Zwischenfälle mit versehentlichen Datenverlusten sowie absichtlichen Datendiebstahl verhindern zu können. Da die Verordnung im Mai 2018 in Kraft treten wird und die Implementierung effektiver Datensicherheitskontrollen kompliziert ist, sollten Unternehmen so bald wie möglich die erforderlichen Ressourcen dazu abstellen.

5. Verfügen wir über ein eigenes Anwendungssicherheitsprogramm?

Viele Unternehmen entwickeln eine erhebliche Anzahl eigener Geschäftsanwendungen. Diese haben meist Internetzugriff und verwenden private Kundendaten. Laut dem „Verizon 2016 Data Breach Investigations Report“ (Verizon-Untersuchungsbericht zu Datenkompromittierungen)[2] stellen Angriffe auf Web-Anwendungen die größte Angriffskategorie dar.

Da viele Unternehmen kontinuierliche DevOps implementieren, ist die Umsetzung eines Ansatzes nach dem Prinzip „Sicherheit von Anfang an“ umso wichtiger. Zu den wichtigsten Sicherheitskontrollen gehören sichere Programmierung sowie entsprechende Schulungen für Entwickler, die Erfassung von Anwendungsprotokollen, regelmäßige Penetrationstests sowie Netzwerkeindringungsschutz-Systeme für die Peripherie.

6. Wissen wir, wo sich alle unsere Datenbanken befinden und welche Daten darin gespeichert werden?

Datenbanken enthalten häufig die wertvollsten Informationen eines Unternehmens und insbesondere solche Daten, die sich auf die Kunden beziehen. Dennoch setzen zu viele Unternehmen ausschließlich auf grundlegende Sicherheitskontrollen, installieren Patches aufgrund der Ausfallzeiten für die Anwendungen nur unregelmäßig und vertrauen die Aktivitätsüberwachung komplett den

Datenbanken enthalten häufig die wertvollsten Informationen eines Unternehmens und insbesondere solche Daten, die sich auf die Kunden beziehen.

Administratoren an. Zudem werden in für Test und Entwicklung bereitgestellten Datenbanken häufig Produktionsdaten verwendet, sodass ein weiteres Risiko für den Verlust sensibler Daten entsteht.

Zur Vorbereitung auf die DSGVO sollten Sie wichtige Aktivitäten wie die Erkennung lokaler sowie gehosteter Datenbanken, die Überprüfung von Datenbank-Sicherheitsprozeduren, die Bereitstellung zusätzlicher Exploit-Schutzfunktionen sowie die Definition von Datenbank-Kompromittierungs-Anwendungsszenarien für Ihre Sicherheitsumgebung gewährleisten. Bei extern gehosteten Datenbanken wird empfohlen, die Verträge mit dem Hosting-Unternehmen sowie deren Sicherheitsmaßnahmen zu überprüfen.

7. Wie gehen wir mit Software-as-a-Service-Cloud-Anwendungen um, in denen private Daten verarbeitet oder gespeichert werden?

Die von fast allen Unternehmen verwendeten Cloud-Anwendungen reichen von Geschäfts-Apps (z. B. Salesforce) bis zu Cloud-Speicherdiensten (z. B. Box). Während der Cloud-Anbieter für die Sicherheit der Infrastruktur verantwortlich ist, trägt das Unternehmen weiterhin die Verantwortung für den Schutz der Daten und die Überwachung der Benutzeraktivitäten.

Zwei wichtige und möglicherweise relevante DSGVO-bezogene Sicherheitskontrollen sind Cloud Access Security Broker (CASBs) sowie Benutzerverhaltensanalysen, mit denen der Zugriff kontrolliert sowie die Identifizierung und Reaktion auf ungewöhnliche Kontoaktivität ermöglicht werden.

8. Wie kontrollieren wir Berechtigungen und die Aktivitäten von Benutzern mit umfangreichen Zugriffsrechten, insbesondere im Zusammenhang mit Cloud-Diensten?

Laut dem „Verizon 2016 Data Breach Investigations Report“ (Verizon-Untersuchungsbericht zu Datenkompromittierungen)[3] wird als häufigste Insider-Bedrohung der Missbrauch von Zugriffsrechten genannt. Insider-Aktionen gehören zu den Gefahren, die besonders schwer zu erkennen sind: Solche Zwischenfälle werden meist erst nach Monaten erkannt. Gleichzeitig stellen Cloud-Dienste eine wachsende Angriffsfläche dar. Daher ist die Einschränkung, Kontrolle und Überwachung der Aktivitäten privilegierter Benutzer ein wichtiger Faktor für die Einhaltung der DSGVO-Vorgaben sowie für die Verbesserung des Datenschutzes im Allgemeinen.

9. Wie weit ist unser Plan zum Schutz vor hochentwickelter Malware implementiert?

Laut dem „Verizon 2016 Data Breach Investigations Report“ (Verizon-Untersuchungsbericht zu Datenkompromittierungen)[4] hängen 60 % aller Malware-Zwischenfälle mit Malware zusammen, die Daten stiehlt oder exportiert. Spearphishing ist die häufigste Malware-Übertragungsart, die permanent Zugriff auf das System gewährt. Sobald sich der Angreifer im Netzwerk befindet, kann er mit diesem Ansatz gestohlene Anmeldeinformationen für den Zugriff auf sensible Systeme sowie verschlüsselte Kanäle nutzen und so Daten exfiltrieren.

Erwägen Sie neben hochentwickeltem Malware-Schutz auf Endgeräten auch den Einsatz von Schutzlösungen, die den häufigsten Exfiltrationskanal HTTPS überprüfen können.

10. Sind in den Sicherheitsprozessen Anwendungsszenarien zur Erkennung von Datenkompromittierungen definiert?

Laut DSGVO müssen Unternehmen Datenkompromittierungen innerhalb von 72 Stunden melden. Das bedeutet unter anderem, dass Sicherheitsverletzungen innerhalb dieses Zeitraums erkannt werden müssen. Die aktuelle „The 2017 SANS Incident Response Survey" (SANS-Umfrage von 2017 zur Reaktion auf Zwischenfälle)[5] ergab, dass 84 % aller Unternehmen mindestens ein dediziertes Mitglied im Zwischenfallreaktionsteam haben, doch nur 53 % stuften ihre Fähigkeiten zur Zwischenfallreaktion als „ausgereift" oder „teilweise ausgereift" ein. Gleichzeitig fällt es selbst Unternehmen mit ausgereiften Sicherheitskontrollzentren schwer, Datenkompromittierungen zu erkennen, zu untersuchen und darauf zu reagieren – ganz besonders innerhalb eines kurzen Zeitraums. Ein wichtiger Aspekt für die Vorbereitung auf die DSGVO ist daher die Konsolidierung der Sicherheitsdaten in einem SIEM-System und die Durchführung von Verhaltensanalysen von Benutzern und Entitäten (User and Entity Behavior Analytics, UEBA) zur Identifizierung von ungewöhnlichem Verhalten.

3. Die Prozesse und Funktionen, die zur Einhaltung der DSGVO erforderlich sind

Für die Vorbereitung auf die DSGVO müssen Sie die Unternehmenskultur so verändern, dass sie Aspekte wie Privatsphäre, Schutz personenbezogener Daten sowie Cyber-Sicherheit im Allgemeinen berücksichtigt. Eine detaillierte Erläuterung des Hintergrunds finden Sie im Blog Securing Tomorrow.
Die im Unternehmen erforderlichen Faktoren können nach vier Gesichtspunkten betrachtet werden: Governance, Personen, Prozesse und Technologie. Wir gehen dabei näher auf die Cyber-Sicherheit ein.

	Schutz	Erkennung	Behebung
Governance	■ Gewährleistung, dass die Unternehmensführung die Problematik kennt und Cyber-Sicherheit und Datenschutz unterstützt ■ Benennung eines Datenschutzverantwortlichen mit der entsprechenden Befugnis, Compliance-Standards im erforderlichen Umfang zu erzwingen ■ Entwicklung eines Programms für kontinuierliche Compliance-Überwachung und -Bewertung, mit dem die Compliance proaktiv überprüft wird ■ Etablierung eines Informationssicherheitsprogramms basierend auf branchenüblichen Frameworks (z. B. NIST, ISO 27001, SABSA) und Kontrollen (z. B. SANS) ■ Förderung einer positiven und kollaborativen Unternehmenskultur in Bezug auf die Datensicherheit von Mitarbeitern und Geschäftspartnern ■ Einrichtung eines Sicherheitskontrollzentrums, das rund um die Uhr mit Mitarbeitern besetzt ist ■ Verankerung von Klauseln zu Zwischenfallreaktion und Datenschutz in Verträgen mit Cloud-Dienstanbietern und externen Lieferanten		
Personen	■ Schulung und Zertifizierung der Anwendungsentwickler zu sicherer Programmierung ■ Schulung und Zertifizierung der Endbenutzer zu Datenschutz ■ Schulung und Zertifizierung von Domänen- und Technologie-Administratoren zu sicherer Konfiguration, Verantwortlichkeiten und empfohlenen Vorgehensweisen ■ Schulung und Zertifizierung von Domänen- und Technologie-Administratoren zu sicherer Konfiguration	■ Schulung aller Benutzer und Administratoren zu den Prozeduren und Verantwortlichkeiten in Bezug auf die Meldung von Sicherheitsverletzungen ■ Schulung und Zertifizierung der Zwischenfallverantwortlichen zur Meldung von Sicherheitsverletzungen und zur Handhabung der Vorgaben	■ Entwicklung von Coaching-Mechanismen zur positiven Verstärkung der Datenschutzrichtlinien ■ Etablierung einer Verbindung zwischen den Mitarbeitern und den Sicherheitssystemen bei der Behebung und Handhabung von Richtlinienverstößen im Bereich Datenschutz ■ Aufbau eines Krisenaktionsteams, das die Reaktionsmaßnahmen bei Sicherheitsverstößen koordiniert
Prozesse	■ Implementierung eines Prozesses für kontinuierliche Anwendungssicherheitstests ■ Durchführung regelmäßiger Scans zur Suche nach Datenbanken und anderen sensiblen Daten-Repositorys ■ Verankerung von Klauseln zum Datenschutz in Verträgen mit Cloud-Anbietern und externen Lieferanten ■ Kontinuierliche Überprüfung der Berechtigungen und Zugriffsrechte für sensible Daten-Repositorys und Anwendungen ■ Entwicklung einer Datenklassifizierung, die kontinuierlich angewendet wird	■ Kontinuierliche Überwachung des Verschlüsselungsstatus gespeicherter Daten auf Endgeräten, in Rechenzentren sowie auf Cloud-Servern ■ Erarbeitung eines Playbooks zur Erkennung von und Reaktion auf Kompromittierungen, um versehentliche oder absichtliche Datenlecks zu identifizieren ■ Kontinuierliche Überwachung auf Datenkompromittierungsszenarien ■ Entwicklung der Berichterstellungsprozesse zur Meldung von Sicherheitsverletzungen an Behörden innerhalb des vorgegebenen Zeitraums ■ Verankerung von Klauseln zur Zwischenfallerkennung in Verträgen mit Cloud-Anbietern und externen Lieferanten	■ Übungen des Krisenaktionsteams mindestens einmal pro Jahr ■ Erarbeitung von Reaktionsmaßnahmen, mit denen Kompromittierungen innerhalb von vier Stunden isoliert und vollständig erfasst werden können ■ Entwicklung eines Systems zur kontinuierlichen Überwachung der Schwachstellenbehebungen für DevOps ■ Erarbeitung eines Playbooks für Reaktionsmaßnahmen und Übungen, die IT, SecOps, Personalabteilung, Public Relations, Unternehmensführung sowie Vertreter der Geschäftsbereiche umfassen

	Schutz	Erkennung	Behebung
Technologie	■ Hochentwickelte Malware-Schutzlösungen für Endbenutzergeräte und Server, die Signaturen, Intelligenz und Verhaltensanalysefunktionen verwenden ■ Verschlüsselung der Daten, die auf Endbenutzergeräten, Servern und Datenbanken gespeichert sind ■ Eindringungsschutzsysteme für Workload- und Anwendungssicherheit ■ Schutz vor Datenkompromittierungen in Netzwerken zum Schutz übertragener Daten ■ Schutz vor Datenkompromittierungen für Endgeräte zum Schutz verwendeter und übertragener Daten auf Endbenutzergeräten ■ Datenbank-Aktivitätsüberwachung zum Schutz der Unternehmensanwendungen vor Exploits ■ Cloud-Web-Sicherheits-Gateways für Mobilgerätedaten und Bedrohungsschutz ■ Cloud Security Broker zur Bereitstellung von Überblick und Kontrolle über die Daten in SaaS-Anwendungen	■ Zentrale Übersicht und Richtlinienverwaltung für Tools zum Schutz vor Datenkompromittierungen und Verschlüsselung ■ System für Sicherheitsinformations- und Ereignis-Management für Echtzeit-Zwischenfallerkennung und Forensik ■ Protokollerfassungssystem mit der Kapazität, Daten zu wichtigen Sensoren und Datenquellen über einen Zeitraum von mindestens sechs Monaten bis zu einem Jahr zu speichern ■ Sicheres Nachweis-Repository für Untersuchungen von Zwischenfällen mit Datenkompromittierungen ■ Tools für Erkennungs- und Reaktionsmöglichkeiten für Endgeräte mit Datenverkehr- und Benutzeraktivitätsverlauf für Zwischenfalluntersuchungen ■ Benutzerverhaltensanalysen zur Identifizierung verdächtiger Aktivitäten bei Unternehmens- und Cloud-Anwendungen	■ Automatisierte Richtlinien-basierte Verschlüsselung für übertragene Daten im E-Mail-, Web- und Cloud-Datenverkehr ■ Tools für Abwehrmaßnahmen, die Hosts, Netzwerke, Anwendungen, Daten sowie Benutzer isolieren und so Kompromittierungen eindämmen können

4. Messung der Sicherheitsergebnisse

In der Tabelle unten erhalten Sie einen umfassenden Überblick über die Funktionen, die Unternehmen für die Gewährleistung der Einhaltung der DSGVO-Vorgaben benötigen:

	Schutz	Erkennung	Behebung
Beseitigung von Bedrohungen	■ Verhinderung der Installation bekannter und unbekannter Malware auf Endbenutzergeräten, Datenbanken und Servern ■ Verhinderung von Anwendungs-Exploits, die nicht autorisierte Zugriffe und Datenkompromittierungen ermöglichen können ■ Einschränkung und Kontrolle der Endbenutzer- und Administrator-Rechte	■ Identifizierung, Untersuchung und Validierung von Malware-Infektionen unabhängig davon, wo sie erfolgen ■ Identifizierung, Untersuchung und Validierung von Exploit-Versuchen bei Anwendungen, die private Daten hosten ■ Identifizierung, Untersuchung und Validierung von Exploit-Versuchen bei Datenbanken, die private Daten hosten	■ Automatischer Austausch von Malware-Erkenntnissen über Sensoren und Kontrollpunkte ■ Isolierung infizierter Hosts oder Systeme mithilfe vorab geplanter Reaktionen und automatisierter Aktionen ■ Blockierung böswilliger Dateien auf Endgeräten, Netzwerken und Web-Kanälen mithilfe automatisierter Aktionen ■ Blockierung von Befehls- und Steuerungsaktivitäten im Netzwerk, im Web oder in anderen Kanälen mithilfe automatisierter Aktionen ■ Entfernung von Kompromittierungsindikatoren von infizierten Hosts oder Neuinstallation zur Verhinderung von Neuinfektionen
Schutz von Daten	■ Verwendung automatisierter Erkennungs- und Klassifizierungs-Tools zur Identifizierung und Kennzeichnung privater Daten ■ Schutz verwendeter, gespeicherter oder übertragener privater Daten vor versehentlichen oder Richtlinien-basierten Datenkompromittierungen ■ Schutz verwendeter, gespeicherter oder übertragener privater Daten vor absichtlichen Datenkompromittierungen ■ Verhinderung der Exfiltration privater Daten an bekannten oder unbekannten Orten ■ Verhinderung von unberechtigtem Zugriff auf private Daten ■ Verwendung automatisierter Verschlüsselung zur Identifizierung und zum Schutz übertragener Daten	■ Identifizierung, Untersuchung und Validierung Richtlinien-basierter Datenkompromittierungen ■ Identifizierung, Untersuchung und Validierung böswilliger Datenkompromittierungen ■ Identifizierung, Untersuchung und Validierung von Exploit-Versuchen bei Datenbanken, die private Daten hosten ■ Identifizierung, Untersuchung und Validierung nicht autorisierter Zugriffsversuche bei Anwendungen, Datenbanken oder Servern, die private Daten hosten	■ Automatischer Austausch von Datenerkenntnissen über Sensoren und Kontrollpunkte ■ Isolierung infizierter Hosts oder Systeme mithilfe vorab geplanter Reaktionen und automatisierter Aktionen ■ Isolierung von Benutzerrechten und Zugriffen auf private Daten mithilfe vorab geplanter Reaktionen und automatisierter Aktionen ■ Verwendung automatisierter Verschlüsselung zur Identifizierung und Korrektur von Datenkompromittierungen
Schutz von Cloud-Umgebungen	■ Verwendung automatisierter Erkennungs- und Klassifizierungs-Tools zur Identifizierung von Cloud-Anwendungen und Kennzeichnung privater Daten ■ Verhinderung der Installation bekannter und unbekannter Malware auf Infrastructure-as-a-Service-Cloud-Servern ■ Verhinderung der Ausnutzung von Anwendungen auf Cloud-Infrastrukturen oder -Plattformen ■ Schutz verwendeter, gespeicherter oder übertragener privater Daten vor versehentlichen oder böswilligen Datenkompromittierungen auf Cloud-Anwendungen	■ Identifizierung, Untersuchung und Validierung nicht autorisierter Zugriffe auf Cloud-basierte Dienste ■ Identifizierung, Untersuchung und Validierung von Kompromittierungen mit Sicherheitskontrollen für private Daten bei Software-as-a-Service-Anwendungen ■ Identifizierung, Untersuchung und Validierung von Kompromittierungen mit Sicherheitskontrollen für private Daten bei gehosteten Anwendungen	■ Automatischer Austausch von Daten- und Malware-Erkenntnissen über Sensoren und Kontrollpunkte ■ Isolierung infizierter Hosts oder Systeme mithilfe vorab geplanter Reaktionen und automatisierter Aktionen ■ Isolierung von Benutzerrechten und Zugriffen auf private Daten mithilfe vorab geplanter Reaktionen und automatisierter Aktionen ■ Verwendung automatisierter Verschlüsselung zur Identifizierung und Korrektur von Datenkompromittierungen in Cloud-Anwendungen

	Schutz	Erkennung	Behebung
Optimierung der Sicherheits-abläufe	■ Kontinuierliche Scans zur Identifizierung und Klassifizierung privater Daten und Daten-Repositorys ■ Kontinuierliche Reduzierung der Angriffsfläche für Schwachstellen- und Anwendungs-Exploits durch Patch- und Schwachstellen-Scans ■ Kontinuierliche Überwachung des Schutzkontrollstatus für alle verwalteten Endbenutzergeräte, Datenbanken und Server	■ Kontinuierliche Überwachung auf Kompromittierungsindikatoren, insbesondere auf Befehls- und Steuerungsaktivitäten ■ Kontinuierliche Überwachung auf Kompromittierungen mit Sicherheitskontrollen für private Daten ■ Kontinuierliche Überwachung auf nicht autorisierten Zugriff oder Berechtigungsmissbrauch bei Systemen mit privaten Daten	■ Verwendung von Automatisierung und integrierten Technologien, damit Neuinfektionen verhindert und die Kompromittierung privater Daten verhindert werden ■ Verwendung von Automatisierung und integrierten Technologien, damit potenzielle Infektionen, Insider-Aktivitäten oder Datenkompromittierungsindikatoren schnell überprüft werden können

Zusammenfassung

Die Vorbereitung auf die Datenschutz-Grundverordnung wird in diesem Jahr viele Unternehmen und Sicherheitsexperten beschäftigen. Führungskräfte und Sicherheitsverantwortliche in Unternehmen müssen Investitionen priorisieren und neue Programme bzw. Lösungen implementieren, mit denen die Einhaltung der neuen Vorgaben gewährleistet werden kann.

McAfee bietet eine breite und umfassende Palette an Funktionen, mit denen Sie gespeicherte sowie übertragene Daten schützen und einen Überblick über die Cloud erhalten – hervorragende Voraussetzungen für die Einhaltung der Datenschutz-Grundverordnung.

Weitere Informationen finden Sie unter mcafee.com/GDPR.

1. Wachsendes Vertrauen in die Cloud
2. Verizon 2016 Data Breach Investigations Report (Verizon-Untersuchungsbericht zu Datenkompromittierungen)
3. ebd.
4. ebd.
5. The 2017 SANS Incident Response Survey (SANS-Umfrage von 2017 zur Reaktion auf Zwischenfälle)

Informationen zu McAfee

McAfee ist eines der weltweit führenden unabhängigen Cyber-Sicherheitsunternehmen. Inspiriert durch die Stärke, die aus Zusammenarbeit resultiert, entwickelt McAfee Lösungen für Unternehmen und Privatanwender, mit denen die Welt etwas sicherer wird. Mit unseren Lösungen, die mit den Produkten anderer Unternehmen zusammenarbeiten, können Unternehmen Cyber-Umgebungen koordinieren, die wirklich integriert sind und in denen der Schutz vor sowie die Erkennung und Behebung von Bedrohungen nicht nur gleichzeitig, sondern auch gemeinsam erfolgen. McAfee bietet Schutz für alle Geräte von Privatanwendern und sichert dadurch das digitale Leben zu Hause und unterwegs. Durch die Zusammenarbeit mit anderen Sicherheitsakteuren fördert McAfee zudem den gemeinsamen Kampf gegen Cyber-Kriminelle. Davon profitieren alle.

www.mcafee.com/de

McAfee™
Together is power.

Ohmstr. 1
85716 Unterschleißheim, Deutschland
+49 (0)89 3707 0
www.mcafee.com/de