Pulse Secure®

Pulse Secure-Lösungen und GDPR

Anwendung von Secure Access-Lösungen, um Due Diligence und zusätzliche Kontrollen zum Schutz personenbezogener Daten und zur Milderung der GDPR-Risiken nachzuweisen.

Die Datenschutzgrundverordnung (GDPR) (Verordnung (EU) 2016/679) ist eine Verordnung, mit der das Europäische Parlament, der Rat der Europäischen Union und die Europäische Kommission den Datenschutz für alle Bürger der Europäischen Union (EU) stärken und harmonisieren möchten. Das primäre Ziel der GDPR besteht darin, Staatsangehörigen von Ländern der EU die Kontrolle über ihre personenbezogenen Daten zurück zu geben und die internationale Geschäftstätigkeit durch Harmonisierung der Regelungen innerhalb der EU zu vereinfachen.

Die GDPR ist Teil eines breiteren Trends zu mehr gesetzlicher Kontrolle in Bezug auf Daten in einer Zeit, in der Organisationen vermehrt Ressourcen aus Cloud-basierten Anwendungen nutzen, die häufig nicht direkt von der Organisation kontrolliert werden. Die Umstellung auf Hybrid-IT wird in vielen Fällen zum Zugang zu Anwendungsinformationen ermutigen, die ebenfalls GDPR-relevante personenbezogene Daten über ein breiteres Spektrum an Geräten, einschließlich Laptops, Desktops, Tablets und Smartphones, enthalten können. Dieses Papier zeigt auf, an welchen Stellen die GDPR Informationssicherheitsquellen beeinflusst, welche zusätzlichen Sicherheitsmaßnahmen die IT berücksichtigen sollte und welche Lösungen Pulse Secure Organisationen zur Konformität mit der GDPR anbietet.

Herausforderungen

- Gewährleistung, dass ausschließlich autorisierte, authentifizierte Benutzer Zugang zu personenbezogenen Daten haben
- Förderung der geschützten Konnektivität zwischen Benutzern, Geräten und Apps mit Zugang zu personenbezogenen Daten
- Konsequente Durchsetzung aktiver Endpunkt-Sicherheitsmechanismen
- Segregation und Schutz personenbezogener Daten auf smarten Mobilgeräten
- Prüffähigkeiten, die aktive Zugangskontrollen zur Förderung des Datenschutzes zeigen

GDPR-Artikel zur Sicherheit der Verarbeitung

Die GDPR umfasst 11 Kapitel mit 99 Gesetzesartikeln. Sie finden die abschließende Version der Verordnung, veröffentlicht am 06. April 2016, unter http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. Die Kapitel enthalten wichtige Grundsätze, die Rechte der Datensubjekte und die Verantwortlichkeiten des Verantwortlichen und Verarbeiters personenbezogener Daten. Kapitel 4, Artikel 32 „Sicherheit der Verarbeitung" umfasst mehrere Absätze, die viele technische und organisatorische Notwendigkeiten enthalten, die IT Abteilungen, insbesondere diejenigen, die für einen sicheren Benutzer-, Anwendungs- und Datenzugriff verantwortlich sind, verstehen und umsetzen müssen, um sowohl die besten Praktiken, als auch die Gesetzeskonformität zu gewährleisten.

Artikel 32 GDPR besagt, dass der Verantwortliche und Verarbeiter personenbezogener Daten gemäß der Definition der GDPR geeignete technische und organisatorische Maßnahmen ergreifen sollen, um ein dem Risiko angemessenes Schutzniveau zu erreichen. Hierzu sollten unter anderem zählen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Darüber hinaus besagt der Artikel, dass ein angemessenes Schutzniveaus zum Schutz gegen unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, zu erreichen ist.

1. Bei der Verarbeitung personenbezogener Daten der EU muss die Organisation die verfügbaren technischen Kontrollen, die Kosten der Implementierung und die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung der Daten sowie das Risiko einer sich verändernden Wahrscheinlichkeit und Schwere des Datenverlusts, die die Rechte und Freiheiten natürlicher Personen betreffen, berücksichtigen. Der Verantwortliche und der Verarbeiter werden angemessene technische und organisatorische Maßnahmen ergreifen, um ein Schutzniveau zu gewährleisten, das dem Risikoniveau entspricht, einschließlich der folgenden Datenschutzeigenschaften, wie jeweils anwendbar:
   - die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
   - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
   - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
   - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
2. Eine Beurteilung sollte - unbeabsichtigt oder unrechtmäßig - die Vernichtung, den Verlust, die Veränderung oder die unbefugte Offenlegung von oder den Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, berücksichtigen.
3. Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40* oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten in diesem Artikel nachzuweisen.
4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 32 Auswirkungen auf InfoSec-Organisationen

Artikel 32* bestimmt, dass Organisationen Schutzmaßnahmen ergreifen müssen, die organisationsbasierte und überprüfbare Sicherheitskontrollen für alle Benutzer und Systeme einführen, die Zugang zu personenbezogenen Daten gemäß der GDPR haben. Basierend auf „geeigneten technischen und organisatorischen Maßnahmen" kann angenommen werden, dass jede Organisation, um ein „dem Risiko angemessenes Schutzniveau zu erreichen", wenigstens verfügen sollte über:

- eine starke Benutzerauthentifizierung, um sicherzustellen, dass nur Personen, die unter der Aufsicht des Datenverantwortlichen agieren, Zugang zu personenbezogenen Daten haben;
- eine geschützte Verbindung zwischen Benutzern, Geräten, Anwendungen und Datenspeichern, die personenbezogene Daten enthalten;
- die Sicherheit aktiver Endpunkt-Sicherheitsmechanismen für diejenigen Benutzer und ihre Geräte, die auf personenbezogene Daten zugreifen und diese speichern;
- sichere Smart-Mobilgeräte mit verschlüsselten Arbeitsumgebungen, die Anwendungen und heruntergeladene personenbezogene Daten trennen, einschließlich der Möglichkeit der Datenlöschung aus der Ferne, sollte das Mobilgerät beeinträchtigt, verloren oder gestohlen werden.
- die Fähigkeit, einheitliche Regelungen für alle Geräte und IT-Quellen mobiler Arbeitskräfte, die personenbezogene Daten verarbeiten oder speichern, anzuwenden, ungeachtet dessen, ob sich die Daten auf Mobilgeräten, zu Hause oder in Cloud-basierten Systemen befinden.
- einen aktiven, eingehaltenen und einheitlich verwendeten Prüfpfad, der geeignete technische Kontrollen, Überwachung und Resonanz in Bezug auf den Zugang und den Datenschutz nachweist.

Benachrichtigung bei Datenschutzverletzung

Der andere große Problembereich für IT-Organisationen ist Artikel 34* der GDPR, der sich mit der „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen" beschäftigt. Zusammengefasst bekräftigt dieser Artikel den Umfang und die Pflichten der Benachrichtigung von Datensubjekten durch den Verantwortlichen im Falle einer Datenschutzverletzung. Der Datenverantwortliche muss die Verletzung des Datenschutzes nicht offenlegen, wenn er geeignete technische und organisatorische Schutzmaßnahmen ergriffen hat, es sei denn, der Verantwortliche ist aufgrund des Urteils einer Aufsichtsbehörde zur Offenlegung verpflichtet. Dieser Artikel besagt insbesondere:

1. Wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

2. Die Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.*

3. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:
   - es wurden geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden;
   - der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht;
   - die Benachrichtigung der betroffenen Person durch den Verantwortlichen mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

4. Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Artikel 34 Auswirkungen auf InfoSec-Organisationen

Eine Auslegung von Artikel 34* lässt darauf schließen, dass, wenn eine Organisation eine Datenverletzung erlitten hat, beispielsweise eine Verletzung der Kundentransaktionsdatenbank, aus der unverschlüsselte personenbezogene Daten der EU herausgefiltert wurden, die besagte Organisation alle betroffenen Personen „in klarer und einfacher Sprache“ über die Verletzung informieren muss. Dasselbe gilt, wenn der Schutzmechanismus, der der Sicherung einer Sitzung zwischen einem Gerät und einer Cloud-basierten Anwendung dient, beeinträchtigt wurde, wenn das Endgerät eines Firmenanwenders mit Zugang zu Verarbeitungssystemen, die GDPR-relevante Daten verarbeiten, beeinträchtigt wurde und demzufolge Daten herausgefiltert wurden, wenn ein Mobilgerät, auf dem heruntergeladene und unverschlüsselte Kopien von personenbezogenen Daten verloren oder gestohlen wurde.

Artikel 34 bezieht sich auf die Möglichkeit, eine Benachrichtigung der von einer Verletzung betroffenen Person zu vermeiden, wenn die von der Verletzung betroffenen Daten „Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich waren, beispielsweise durch Verschlüsselung“. Aus diesem Grund kann als bewährtes Verfahren für alle Geräte, die GDPR-relevante personenbezogene Daten verarbeiten und möglicherweise speichern, die Aufrechterhaltung einer geschützten und verschlüsselten Arbeitsumgebung in jedem Mobilgerät betrachtet werden, die bei Verlust oder Diebstahl des Geräts aus der Ferne gelöscht werden kann. Wenn keine sichere Zugangskontrollen, wie die Zugangsauthentifizierung, die Verschlüsselung von Sitzungen und die Sicherstellung des Schutzes von personenbezogenen Daten am Endpunkt, vorhanden sind, um eventuelle künftige Verletzungen des Schutzes personenbezogener Daten zu verhindern, kann die Aufsichtsbehörde den Verantwortlichen verpflichten, eine Verletzung offen zu legen, auch wenn mehr nominelle Verteidigungen und Unkenntlichmachungen von Daten vorhanden sind.

Welche Relevanz hat die GDPR für andere Konformitätsrahmen?

Obwohl dieser Leitfaden die Gesetzeskonformität unter der DSGVO fördern soll, spiegeln sich die umfassenden Anforderungen der GDPR in Datenschutzvorgaben anderer geschäftlicher oder gesetzlicher Konformitätsvorgaben wider, einschließlich, aber nicht beschränkt auf:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPPA)
- Federal Information Security Management Act of 2002 (FISMA)
- Gramm Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)

Neben diesen Konformitätsrahmen gibt es eine steigende Zahl von länder- und branchenspezifischen regulatorischen Rahmenbedingungen, die - im Einklang mit der GDPR - die Sicherung sensibler, finanzieller und personenbezogener Daten vorschreiben. Diese enthalten vielfach Regelungen in Bezug auf den Erhalt, die Übertragung, die Speicherung, die Verarbeitung und die Vernichtung von Daten und darüber hinaus Sicherheitskontrollen für Benutzer und Geräte mit Zugang zu solchen Daten. Die meisten schreiben eine Form der Zugangskontrolle, des Datenschutzes (einschließlich Verschlüsselung) und der Prüffähigkeit vor, zusammen mit der Verantwortung, Behörden und Endnutzer über die Art der Verletzungen des Datenschutzes und/oder des Datenverlusts zu informieren

Wie die Lösungen von Pulse Secure die GDPR unterstützen

Pulse Secure bietet ein einfaches, umfassendes und integriertes Paket aus Secure Access-Lösungen an, um Due Diligence und zeitgenössische Kontrollen zum Schutz personenbezogener Daten nachzuweisen. Das Lösungspaket umfasst die Zugangsauthentifizierung, die geschützte Kommunikation, die Anwendung von Endpunktverteidigungen, die Containerisierung von Daten auf Mobilgeräten sowie die Netzwehrzugangstransparenz und IOT-Sicherheit.

Unternehmen und Dienstleistungsanbieter aus allen Branchen vertrauen darauf, dassPulseSecureihremobilenArbeitskräftebefähigt,sicheraufAnwendungenund Informationen im Rechenzentrum und der Cloud zuzugreifen und gleichzeitig die Unternehmenskonformität zu gewährleisten. Das Secure Access-Portfolio besteht aus integrierten virtuellen privaten Netzwerken (VPN), Netzwerkzugangskontrolle (NAC), virtuelle Application Delivery Controller (vADC) und Sicherheitstechnologien für Mobilgeräte.

Pulse Connect Secure

Pulse Connect Secure bietet die verlässlichste funktionsreiche SSL VPN, die eine nahtlose geschützte Verbindung zwischen geschäftlichen und persönlichen Mobilgeräten mit den Rechenzentren und Cloud-Ressourcen und Anwendungen des Unternehmens bietet.

- Client-loser Zugang, starke Authentifizierung, Host-Überprüfung für die Einhaltung der Endpunktsicherheit, granulare Richtlinien, Zugriff auf virtuelle Desktops, Integration von Mobilgerätemanagement (MDM) und umfassende Prüffunktionen
- Authentifizierter und konformer Zugang zu Anwendungen am Standort und in der Cloud, der SSO und SAML in solchen Anwendungen ermöglicht, wie Office 365 und Salesforce.com
- Verifizierung der Sicherheitsverteidigungen am Endpunkt, Patches, Registry-Einstellungen, Konfigurationen und spezifizierte Anwendungen werden installiert, aktualisiert und aktiviert
- Erweiterte Funktionen, um die permanenten, anwendungsaktivierten und mobilen VPN-Fähigkeiten mit Multifaktor- und zertifikatbasierter Authentifizierung zu instrumentieren
- Umfassende Transparenz und Logging, um die Prüfung und Reaktion auf Sicherheitsanomalien und Konformitätsverletzungen zu ermöglichen

Pulse Workspace

Pulse Workspace ist eine umfangreiche Anwendungs- und Gerätemanagementlösung für Mobilgeräte, die persönliche und geschäftliche Anwendungen und Daten trennt und gleichzeitig die native Benutzererfahrung aufrecht erhält und einen geringen Verwaltungsaufwand verursacht. Organisationen können geschäftliche und verbotene Anwendungen einsetzen, die Konnektivität sicherstellen und gewährleisten, dass geschäftliche Daten während der Übertragung oder Aufbewahrung auf Android- und Apple-Mobilgeräten geschützt sind

- Eine einfache, aber wirkungsvolle Containerisierung und der Schutz gegen Datenverlust für geschäftliche Anwendungen und Daten, die die Privatsphäre des Geräteeigentümers nicht verletzen.
- Bestimmen Sie, welche Benutzer und Anwendungen VPN-Zugang zum Netzwerk und den Cloud-Ressourcen und Daten über ihr Mobilgerät erhalten
- Arbeitsflussautomatisierung zur Vorkonfiguration von Anwendungen, Konten, Einstellungen, Zertifikaten und Konformitätsprüfungen anhand der Funktion und Datenschutzanforderungen
- Granulare Richtlinienkonformität und Durchsetzung, wie die Ablehnung gerooteter oder gehackter Geräte, Passwortsicherheit, von Mobilgeräteanwendungen ausgelöste VPN usw.
- Erhalt der Kontrolle von Daten während der Übertragung oder Aufbewahrung mit Sofortmaßnahmen zur Zugangsverweigerung und zur Löschung geschäftlicher Daten und Anwendungen im Container aus der Ferne
- Umfassende Transparenz und Logging, um die Prüfung und Reaktion auf Sicherheits- und Datenschutzprobleme zu ermöglichen

Pulse Cloud Secure

Pulse Cloud Secure wurde entwickelt, um mobilen Arbeitskräften jederzeit geschützten Zugang zu Hybrid-IT-Umgebungen durch Single Sign-On (SSO) von Mobilgeräten auf Cloud-Ressourcen und SaaS-Anwendungen mit starker Authentifizierung und Gerätekonformität zu ermöglichen.

- Erweiterte Endpunkt-MFA-Integration in Kombination mit SAML 2.0 basiertem SSO für Cloud-Zugang sowie Kerberos Constrained Delegation und NT LAN Manager für den Zugang zu Altrechenzentrumsanwendungen
- Breite Interoperabilität mit dem Identitäts- und Zugangsmanagement (IAM) von Drittanbietern, mit der Absicht, als SAML Identity Provider (IdP) und als SAML Service Provider (SP) für einen flexiblen Einsatz und eine nahtlose Benutzererfahrung zu dienen
- Verifizierung von Laptops, iOS- und Android-Geräteschutzmechanismen, um sicherzustellen, dass autorisierte Benutzer mit sicheren Geräten Zugang zur Cloud und zum Rechenzentrum haben
- Skalierbare, zentralisierte Kontrolle durch Pulse One, um ein einheitliches Richtlinienmanagement, Transparenz und die Prüfung der Autorisierung des Zugangs zum Rechenzentrum und zur Cloud sowie Konformität zu ermöglichen

Pulse Policy Secure

Pulse Policy Secure ist eine Network Access Control-Lösung der nächsten Generation, die Transparenz, einer richtlinienbasierte Kontrolle und die Befähigung von Benutzern, Endpunkten und IOT-Geräten, die Zugang zu einem Firmennetzwerk haben oder damit arbeiten, bietet. Diese Lösung bietet Zugangsintelligenz, Konformität, Prüfung und die Reaktion auf Bedrohungen von Geräten, die auf Netzwerkressourcen zugreifen, die personenbezogene Daten verarbeiten und speichern.

- Vereinfachte Administration und vereinfachter Einsatz von Leveraging Configuration Wizards und Pulse VPN-Richtlinien
- Agentbasierte und agentlose Endpunkttransparenz, optimiertes Gastmanagement und automatisiertes Windows-, MAC-, Smartphone-, Tablet- und BYOD-Onboarding
- Dynamische Endpunkt- und IOT-Geräteerkennung, Klassifizierung, Inventarisierung, Überwachung und kontextabhängige Zugangsbefähigung mit granularen Konformitätsrichtlinien
- Starke Mitigationsfähigkeiten mit Unterstützung von 802.1X Port-Level und L2-L4-Befähigung, automatisierte und benutzerorientierte Endpunktwiederherstellung, Netzwerkquarantäne und -blockierung und IOT-Sicherheit
- Interoperabilität mit gängigen Netzwerk- und Wireless-Switches, BGFW-, SIEM- und EMM-Tools

Schließen Sie Ihre GDPR-Kontrolllücken

Die Lösungen von Pulse Secure bieten einen einfachen, umfassenden und ganzheitlichen Ansatz zur Erweiterung der Secure Access- Möglichkeiten Ihrer Organisation. Der Ansatz ermöglicht einen einheitliche, richtlinienbasierte Zugangstransparenz, eine sichere Verbindung, Datenschutz und Prüfungen von Benutzern und ihren Mobilgeräten sowie Rechenzentren und Cloud-Anwendungen und Ressourcen, die personenbezogene Daten verarbeiten und speichern. Mit der Implementierung von Pulse Secure können Unternehmen die Einhaltung der GDPR und die technischen Sicherheitsmaßnahmen zur Milderung von Verletzungen des Schutzes personenbezogener Daten nachweisen. Weitere Informationen finden Sie unterhttps://www.pulsesecure.net/solutions/.

* Abschnitte in diesem Leitfaden enthalten eine kurze Zusammenfassung von GDPR-Artikeln. Die vollständigen und direkten Spezifikationen zur GDPR finden Sie unter: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf, https://gdpr-info.eu/art-32-gdpr/, https://gdpr-info.eu/art-33-gdpr/ und https://gdpr-info.eu/art-34-gdpr/.

Über Pulse Secure

Die Pulse Secure, LLC bietet die einfachsten und umfangreichsten Secure Access-Lösungen an, die Transparenz und eine nahtlose, geschützte Verbindung zwischen Benutzern, Geräten, Dingen und Dienstleistungen ermöglichen. Das Unternehmen liefert Pakete, die Cloud-, mobile Geräte-, Anwendungs- und Netzwerkzugang auf einzigartige Weise integrieren, um Hybrid-IT zu ermöglichen. Mehr als 20.000 Unternehmen und Dienstleistungsanbieter aus allen Branchen vertrauen darauf, dass Pulse Secure ihre mobilen Arbeitskräfte befähigt, sicher auf Anwendungen und Informationen im Rechenzentrum und der Cloud zuzugreifen und gleichzeitig die Unternehmenskonformität zu gewährleisten. Weitere Informationen unter www.pulsesecure.net.