Compliance zur EU-Datenschutz-Grundverordnung – mit Vectra

Innerhalb der Europäischen Union sind die personenbezogenen Daten aller natürlicher Personen grundrechtlich geschützt. Um diesen Schutz zu gewährleisten und zugleich den freien Fluss von Daten zwischen Mitgliedsstaaten der EU zu ermöglichen, wurde die EU-Datenschutz-Grundverordnung (EU-DSGVO) entworfen.

Die Globalisierung und die rasante technische Entwicklung – vom Cloud Computing über standortbezogene Dienste bis hin zu sozialen Netzwerken – haben zu einem signifikanten Anstieg des Umfangs geführt, in dem personenbezogene Daten durch Unternehmen und öffentliche Institutionen gesammelt und weitergegeben werden.

Es sind vor allem diese Trends, die hinter der Entwicklung der EU-DSGVO stehen. Sie wird am 25. Mai 2018 in Kraft treten und die EU-Richtlinie zum Datenschutz von 1995 ersetzen.

Die EU-DSGVO modernisiert die Datenschutzregeln innerhalb der EU und schafft ein einheitliches, harmonisiertes EU-Recht, das an die Stelle des aktuell gültigen Flickwerks aus nationalen Vorschriften in den 28 Mitgliedsstaaten.

Dem Bereich für Justiz und Verbraucherschutz der Europäischen Kommission zufolge existieren Schätzungen, nach denen die EU-DSGVO einen wirtschaftlichen Nutzen in Höhe von 2,3 Milliarden Euro pro Jahr erbringen wird. Der Grund dafür ist die reduzierte Komplexität des Datenschutzrechts. Unternehmen haben es in Zukunft einfacher, ihre Tätigkeit innerhalb der EU auszudehnen.

Die EU-DSGVO wird lokal umgesetzt. Jeder EU-Mitgliedsstaat setzt dazu eine Aufsichtsbehörde ein. Die Auswirkungen der Verordnung werden über die Grenzen der EU hinaus spürbar sein, da sie für alle Organisationen gilt, die Daten von EU-Bürgern speichern oder verarbeiten, um Waren oder Dienstleistungen anzubieten oder das Verhalten von Personen zu beobachten, die sich in der EU befinden – unabhängig davon, wo die jeweilige Organisation niedergelassen ist.

Überblick über die EU-DSGVO

Folgende Aspekte stehen im Zentrum der EU-DSGVO:

- Die personenbezogenen Daten von in der EU ansässigen Personen sind geschützt – gleichgültig, wohin sie übermittelt oder wo sie verarbeitet oder gespeichert werden, auch außerhalb der EU. „Personenbezogene Daten“ umfassen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

  Eine identifizierbare natürliche Person ist dadurch gekennzeichnet, dass sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

- Organisationen müssen die explizite, auf hinreichender und verständlich vermittelter Information beruhende Einwilligung der Betroffenen einholen, wenn sie personenbezogene Daten sammeln und verarbeiten wollen.
- Individuen bekommen ein Recht darauf, dass ihre Daten in einer Form gespeichert werden, in der sie von einem Provider zu einem anderen transferiert werden können. Sie haben außerdem das Recht, personenbezogene Daten löschen zu lassen, und sie können der Nutzung ihrer Daten für „Profiling“-Zwecke widersprechen.

- Individuen haben das Recht zu erfahren, wenn ihre Daten kompromittiert wurden. In Fällen, in denen mit dem Vorfall ein hohes Risiko verbunden ist (etwa dann, wenn ein Identitätsdiebstahl befürchtet wird), müssen Unternehmen und Organisationen betroffene Einzelpersonen innerhalb von 72 Stunden über die Verletzung des Schutzes ihrer personenbezogenen Daten informieren.

  Als „Verletzung des Schutzes personenbezogener Daten" wird eine Verletzung der Sicherheit verstanden, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

- Dem „One-Stop-Shop"-Prinzip zufolge hat ein Unternehmen mit Niederlassungen in mehreren EU-Mitgliedsstaaten nur mit der Aufsichtsbehörde in demjenigen Land zu tun, in dem sich seine Firmenzentrale oder seine eigentliche Betriebsstätte befindet.

- Jede Organisation, gleich ob sie in der EU niedergelassen ist oder nicht, unterliegt dem EU-Datenschutzrecht, wenn sie in der EU Waren oder Dienstleistungen anbieten oder das Verhalten von Personen beobachten will, die in der EU ansässig sind.

- Auftragsverarbeiter und Verantwortliche für Daten dürfen Daten nur dann in Länder außerhalb der EU übermitteln, wenn sie angemessene Schutzmaßnahmen ergreifen und wenn sichergestellt ist, dass die Betroffenen ihre Rechte durchsetzen und Rechtsmittel einlegen können.

  Als „Auftragsverarbeiter" gilt eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

  Der „Verantwortliche" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

- Den Aufsichtsbehörden im Sinne der EU-DSGVO stehen eine Reihe von Sanktionsmöglichkeiten zur Verfügung, darunter schriftliche Verwarnungen, Audits, und Geldbußen in einem Rahmen von bis zu 20 Millionen Euro oder von bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Die folgenden Abschnitte befassen sich mit Schutzmaßnahmen gemäß der EU-DSGVO und dem Impact der Verordnung. Sie stellen außerdem im Detail dar, wie die Vectra-Networks-Cybersecurity-Plattform dazu beiträgt, Compliance zur Datenschutzverordnung zu erzielen und personenbezogene Daten effektiv zu schützen – indem sie netzwerkweit kontinuierliche, automatisierte Überwachungs- und Erkennungsmaßnahmen gegen Bedrohungen ermöglicht.

Vectra automatisiert die Jagd auf Cyberkriminelle, die sich in Netzwerken versteckt halten. Die Lösung beschleunigt Incident-Response-Maßnahmen, mit denen sich aktive Bedrohungen stoppen lassen. Sie verkürzt einen Arbeitsaufwand von Wochen und Monaten auf eine Zeitspanne von wenigen Minuten, sodass Security-Teams schnell agieren können, um Datendiebstahl oder andere Schäden zu verhindern.

Zentrale Datenschutzanforderungen der EU-DSGVO

Die EU-DSGVO ist ein robuster Satz an Regulierungen zu Rechten und Verantwortlichkeiten. Dazu gehört eine umfassende Anforderung, nach der Organisationen Maßnahmen ergreifen müssen, die den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

Von den Organisationen wird somit erwartet, dass sie Sicherheitsbelange schon beim Design ihrer Prozesse und Abläufe berücksichtigen und dass sie überdies Techniken und Dienste einsetzen, die mit eingebauten Funktionen zum Schutz von Daten ausgestattet sind und datenschutz-freundliche Voreinstellungen aufweisen. Dies betrifft zum Beispiel soziale Netzwerke und Apps für mobile Geräte.

Die EU-DSGVO wartet mit spezifischen Vorschlägen auf, welche Security-Maßnahmen als Risiko-adäquat angesehen werden können. Dazu gehören:

- Verschlüsselung und/oder Anonymisierung personenbezogener Daten oder der Einsatz von numerischen oder anderen Kenndaten als Pseudonym für den Realnamen einer Person.
- Sicherstellung der permanenten Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandskraft gegen Angriffe auf Datenverarbeitungssysteme und -dienste.
- Entwicklung eines Verfahrens, die Verfügbarkeit von Daten und den Zugriff darauf innerhalb eines angemessenen Zeitraums nach einem physischen oder technischen Vorfall wiederherzustellen.
- Regelmäßige Tests, Assessments und Evaluationen der Effektivität technischer und organisatorischer Maßnahmen, die die Sicherheit der Datenverarbeitung gewährleisten sollen.

Darüber hinaus verlangt die EU-DSGVO die Benennung eines Datenschutzbeauftragten. Die Person, die diese Rolle übernimmt, ist innerhalb der Organisation verantwortlich für die Implementierung des Datenschutzes, die Compliance und das Reporting. Der Datenschutzbeauftragte kann auch andere Aufgaben und Pflichten erfüllen. So ist es beispielsweise möglich, dass der IT-Sicherheitsbeauftragte eines Unternehmens (Chief Information Security Officer, CISO) zugleich als Datenschutzbeauftragter fungiert.

Vectra hilft Organisationen, der EU-DSGVO gerecht zu werden

Compliance zur EU-DSGVO lässt sich nur mittels geeigneter Technik und passender Prozesse erreichen. Die Cybersecurity-Plattform von Vectra stärkt die Handlungsfähigkeit von Cybersecurity-Teams und verschafft ihnen die unerlässlichen technischen Mittel, die Anforderungen der EU-DSGVO zu erfüllen.

Vectra unterstützt Maßnahmen für Datenschutz, indem die Lösung Funktionen für permanentes Traffic-Monitoring im Netzwerk, Bedrohungserkennung in Echtzeit, Triage und Incident Reporting bereitstellt. Mithilfe von künstlicher Intelligenz und der Analyse des Angreiferverhaltens spürt das System aktive Cyber-Bedrohungen automatisch im gesamten Unternehmensnetz auf und erfasst dabei sowohl entfernte Standorte, Büronetzwerke, Rechenzentren als auch Cloud-Umgebungen.

Vectra automatisiert eine ganze Reihe arbeitsintensiver Aufgaben, die normalerweise im Verantwortungsbereich von Tier-1-Cybersecurity-Analysten und Incident-Response-Teams liegen. Dadurch reduziert Vectra den Zeitaufwand, den Untersuchungen von Bedrohungen gewöhnlich nach sich ziehen, dramatisch – um bis zu 90 Prozent. Die Security-Teams bekommen so die Chance, sich auf Data-Loss-Prevention und die Schadensbegrenzung zu konzentrieren.

Zu den zentralen Funktionen der Cybersecurity-Plattform von Vectra zählen:

- Kontinuierliches Monitoring und ununterbrochene Analyse des gesamten Netzwerk-Traffics, inklusive des auf das Internet gerichteten Datenverkehrs und des internen Netzwerk-Traffics zwischen physischen und virtuellen Hosts mit IP-Adresse. Eingeschlossen sind beispielsweise Laptops, Server, Drucker, BYOD-Geräte und IoT-Devices – unabhängig vom Gerätetyp, dem Betriebssystem und der Applikation.
- Echtzeit-Einblicke in den Netzwerk-Traffic auf der Basis extrahierter Paket-Metadaten anstelle einer Deep-Packet-Inspection ermöglichen Schutzmaßnahmen, ohne personen-bezogene oder sensible Nutzdaten auszuspionieren.
- Die Analyse von Metadaten mitgeschnittener Pakete auf der Basis verhaltensbasierter Erkennungsalgorithmen macht Aktionen versteckt agierender und unbekannter Angreifer sichtbar, gleich ob der Traffic verschlüsselt ist oder nicht.
- Vectra identifiziert Angriffsverhalten deterministisch und macht so den Einsatz von Remote-Access-Trojanern, verschlüsselten Tunneln, Botnet-Methoden und Ransomware erkennbar. Ebenfalls aufgedeckt werden Insider-Attacken und ausgefeilte, gezielte Angriffsversuche.

Vectra verfolgt Bedrohungen beharrlich in ihrem zeitlichen Verlauf und während aller Phasen einer Attacke – beginnend mit Command and Control (C&C) über Internal Reconnaissance und Lateral Movement bis hin zu Data Exfiltration, wobei letzteres ein für die EU-DSGVO besonders wichtiger Punkt ist.

- Vectra korreliert Bedrohungen automatisch mit konkret angegriffenen Host-Devices und Details der Bedrohungs-erkennung. Diese Details umfassen den Host-Kontext, mitgeschnittene Pakete, die Ernsthaftigkeit der Bedrohungen und Scoring-Werte, mit deren Hilfe entschieden wird, mit welcher Wahrscheinlichkeit ein Angriff echt ist.
- Vectra unterstützt adaptive Cybersecurity auf der Basis eines iterativen Verbesserungsprozesses. Dieser macht sich die Arbeit der Vectra Threat Labs zunutze, einer Gruppe von hoch ausgebildeten Security-Researchern, und setzt verhaltensorientierte Erkennungsalgorithmen ein, deren Lernmechanismen ununterbrochen Informationen aus der lokalen Umgebung und Daten zu globalen Trends verarbeiten.

Wie Vectra die Kern-Anforderungen der EU-DSGVO unterstützt

Die folgende Tabelle listet verschiedene Ansatzpunkte für Organisationen auf, spezifische Aspekte der EU-DSGVO-Anforderungen mit Hilfe von Vectra zu erfüllen.

Artikel in der EU-DSGVO	Vectra-Funktionalität
Art. 25 DSGVO: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. 2. Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.	Vectra assistiert bei der Durchsetzung von Standards für den Umgang mit Daten, indem es die Cybersecurity-Spezialisten über Datentransfers informiert, die von der etablierten Praxis abweichen und Regeln verletzen. Dies wird erreicht, indem das System zunächst das normale Netzwerkverhalten ermittelt und definiert und weitere Aktivitäten dann auf anomale Datenübermittlungen zwischen Hosts hin überwacht – hierzu gehören beispielsweise Transfers ungewöhnlicher Datenmengen oder auffällig häufige Übertragungen. Wenn Vectra anomale Transfers erkennt, stellt das System sofort Informationen über den Host zur Verfügung, der die Daten überträgt, und zeigt, wohin sie geschickt werden. Außerdem ermittelt Vectra die Menge der transferierten Daten und die Technik, mit der die Übermittlung ausgeführt wird. Darüber hinaus unterstützt Vectra die Datenschutz-Anforderungen in den Bereichen Verschlüsselung und Pseudonymisierung (Datenschutz per Design), weil das System die Packet Header im Netzwerk analysiert und nicht die Nutzdaten. Vectra macht jegliche Form der Entschlüsselung unnötig, vermeidet Data Routing und setzt auf Überwachungs- und Verarbeitungsprozesse, die ohne übermäßige Zugriffe auf die eigentlichen Informationen auskommen.
Art. 32 DSGVO: Sicherheit der Verarbeitung 1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: a. Die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b. Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; c. Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; d. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.	Indem Vectra das Netzwerk permanent auf Indikatoren für eine Kompromittierung hin überwacht, hilft das System Organisationen dabei, die Wirksamkeit ihrer technischen Abwehrlösungen im Rahmen ihrer EU-DSGVO-Maßnahmen zu validieren. Vectra zeigt den Security-Teams genau, welche Bedrohungen ihre Verteidigungslinien überwinden. Dazu alarmiert es die Spezialisten, wenn es typische Verhaltensweisen erkennt, die Vorbote einer Bedrohung sind – darunter C&C, Internal Reconnaissance, Lateral Movement und Data Consolidation. Vectra stellt verschiedene Frühwarn-Optionen zur Verfügung, um Ransomware, andere Malware-Varianten und gezielt ausgeführte schädliche Aktivitäten aufzudecken. All diese Phänomene können einem Datendiebstahl, Manipulationen oder destruktiven Angriffen gegen beliebige Geräte im Netz vorangehen – darunter Devices, auf denen kein Virenschutz läuft. Darüber hinaus behält Vectra die interne Kerberos-Infrastruktur und Systemverwaltungswerkzeuge im Blick – zunächst, um die normalen Aktivitäten zu registrieren. Danach erkennt das System, wenn an sich vertrauenswürdige Anmeldedaten durch einen böswilligen Insider oder externe Angreifer missbraucht werden. Die dabei beobachteten Verhaltensweisen umfassen beispielsweise den Missbrauch von administrativen Credentials und von Systemverwaltungsprotokollen wie IPMI. Security-Teams können Angriffe auf dieser Basis schnell identifizieren und bekämpfen. Außerdem unterstützt Vectra Organisationen dabei, nachzuweisen, dass sie angemessene technische Maßnahmen implementiert haben. Die automatisierte Erkennung, Triage und Bedrohungs-Priorisierung von Vectra etwa versorgt Security-Teams mit sicherheitsrelevanten Meldungen in Echtzeit. Diese Benachrichtigungen liefern kurzgefasste und prägnante Erläuterungen zu jeder erkannten Attacke. Darin enthalten sind Informationen über zugrundeliegende Events und den historischen Kontext, die zur Aufdeckung geführt haben, und Hinweise auf mögliche Auslöser, Ursachen, Business-Auswirkungen sowie die nötigen Schritte, um den Vorfall zu verifizieren.

Artikel in der EU-DSGVO	Vectra-Funktionalität
Art. 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. 2. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. 3. Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen: A. Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze; B. Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen; C. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten D. Eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. 4. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen. 5. Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.	Vectra macht sich eine Kombination von Techniken künstlicher Intelligenz zunutze. Damit automatisiert das System die Identifizierung und die Dokumentation von Angriffen und findet heraus, welche Attacken gegebenenfalls den Reporting-Pflichten der EU-DSGVO unterliegen. Security-Teams erhalten kurz zusammen-gefasste, präzise Erklärungen zu jedem erkannten Vorfall – inklusive Informationen über mögliche Auslöser, Ursachen, Business-Auswirkungen und Schritte zur Verifizierung. Vectra unterstützt Security-Teams auf folgende Weise: • Vectra stellt Informationen über erkannte Bedrohungen in einem einfach gehaltenen Dashboard zur Verfügung, das jene kompromittierten Hosts priorisiert, von denen das höchste Risiko ausgeht. Host-bezogenes Scoring macht den jeweils aktuellen Grad einer Bedrohung einschätzbar und die Wahrscheinlichkeit, mit der es sich um einen echten Angriff handelt. Außerdem weist Vectra gezielt auf wichtige Assets hin, die Anzeichen einer Attacke zeigen. • Mit Vectra fällt Security-Teams der gemeinsame Zugriff auf Informationen leicht. Das System gibt Daten entweder auf Anfrage oder nach einem vorgegebenen Zeitplan weiter, wozu seine flexible, benutzerspezifisch konfigurierbare Reporting-Engine zum Einsatz kommt. • Vectra setzt seinen Threat Certainty Index dazu ein, in Echtzeit Bedrohungsmeldungen auszulösen. Security Teams erfahren auf diese Weise sofort, welche angegriffenen Hosts mit der höchsten Eintrittswahrscheinlichkeit das größte Risiko nach sich ziehen. • Vectra ermöglicht zeitgerechtes Reporting und rechtzeitige Benachrichtigungen bei Verletzungen der Sicherheit personenbezogener Daten, indem das System Fälle von Data Exfiltration erkennt und Nachweise für versuchte Kompromittierungen liefert. Vectra unterstützt zusätzlich folgende Security-Response- und Abhilfemaßnahmen: • Echtzeit-Alarmierungen per E-Mail, Syslog oder mittels anderer Werkzeuge, die über eine REST API eingebunden sind. • Vectra bietet einen vorkorrelierten Einstiegspunkt für Sicherheitsnachforschungen mithilfe von Security-Information-und-Event-Management-Systemen (SIEM) und Forensik-Werkzeugen. • Vectra steuert Response-Maßnahmen über dynamische Regeln oder setzt Response-Aktionen in Zusammenarbeit mit existierenden Security-Orchestration- und Enforcement-Lösungen in Gang.
Art. 35 DSGVO: Datenschutz-Folgenabschätzung 1. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden. […] 7. Die Folgenabschätzung enthält zumindest Folgendes: a. Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen; b. Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck; c. Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und d. Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.	Vectra überwacht ununterbrochen die Kommunikation zwischen Applikationen, Werkzeugen und Systemen. Werden neue technische Lösungen oder Plattformen mit dem Netzwerk verbunden, startet Vectra sofort mit dem Monitoring und sucht nach Anzeichen einer Attacke. Vectra bringt kontinuierlich unprofessionellen Umgang mit Daten ans Tageslicht und zeigt Fehlkonfigurationen auf, die Daten exponieren könnten oder das Risiko einer Verletzung ihrer Sicherheit heraufbeschwören. Vectra erleichtert eine holistische Datenschutz-Folgenabschätzung. Dazu liefert das System Beweismaterial für vermutetes oder bereits als echt erkanntes Bedrohungsverhalten im Netz, das auf Datenmanipulationen oder Datenverluste schließen lässt. Auch Vorboten eines Angriffs werden anhand der Verhaltensanalyse sichtbar.

Artikel in der EU-DSGVO

Art. 35 DSGVO: Datenschutz-Folgenabschätzung

8. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

[…]

11. Where Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Schutz personenbezogener Daten mit Vectra

Die einheitliche Anwendung der EU-DSGVO in den EU-Mitgliedsstaaten dürfte es Organisationen erleichtern, Regelwerke für den Schutz von Daten und Prozeduren zur Benachrichtigung des Betroffenen im Falle einer Verletzung des Schutzes personenbezogener Daten aufzusetzen, die als „compliant“ gelten dürfen. Der Schlüssel dazu liegt darin, die geeigneten Werkzeuge und Techniken einzusetzen.

Unglücklicherweise ist die Erkennung und Bekämpfung von Cyber-Angriffen eine recht langwierige Angelegenheit. Dem M-Trends-Report von 2016 zufolge dauert es durchschnittlich 146 Tage, bevor eine Verletzung der Informationssicherheit aufgedeckt wird. Und 53 Prozent dieser Angriffe fallen erst dann auf, wenn die betroffene Organisation von außen darüber informiert wird, ergänzt der Bericht.

Die Cybersecurity-Plattform von Vectra reduziert den Zeitaufwand für Benachrichtigungs- und Response-Prozesse von Wochen oder Tagen auf Minuten. Mittels künstlicher Intelligenz identifiziert die Plattform für automatisierte Bedrohungserkennung Bedrohungen proaktiv und in Echtzeit.

Indem Vectra eine ganze Reihe arbeitsintensiver Aufgaben automatisiert, die typischerweise zum Verantwortungsbereich von Tier-1-Cybersecurity-Analysten und Incident-Response-Teams gehören, verringert die Lösung den Zeitbedarf für die Untersuchung von Bedrohungen dramatisch – um bis zu 90 Prozent. Security-Teams können sich deshalb auf Data Loss Prevention und Maßnahmen zur Schadensbegrenzung konzentrieren.

Vectra gewährt IT-Security-Teams auf effiziente und ökonomische Weise aufschlussreiche Echtzeit-Einblicke in den gesamten Netzwerk-Traffic, macht versteckt agierende und unbekannte Angreifer aus und liefert Kontext-Informationen zu Security-Events direkt an den Arbeitsplatz der Sicherheitsspezialisten.

Weil Vectra die Cybersecurity-Teams dazu befähigt, schon frühe Stadien eines Angriffs zu identifizieren und gegen die Attacke vorzugehen, noch bevor eine echte Verletzung der Informationssicherheit geschieht, reduziert Vectra das Risiko von Vorfällen, die nach den Vorgaben der EU-DSGVO bekanntgemacht werden müssen.

Darüber hinaus sind die Erkennungsmechanismen und Eingriffsmöglichkeiten für Assessments nützlich und bilden einen wichtigen Teil einer angemessenen technischen Cybersecurity-Architektur, die den Compliance-Anforderungen der EU-DSGVO gerecht wird.

VECTRA®

E-Mail info_DACH@vectranetworks.com **Tel.** +41 43 810 47 52 / +49 89 660 634 57 www.vectranetworks.de