EU DATENSCHUTZ-GRUNDVERORDNUNG:

Daten schützen und Transparenz steigern mit Trend Micro

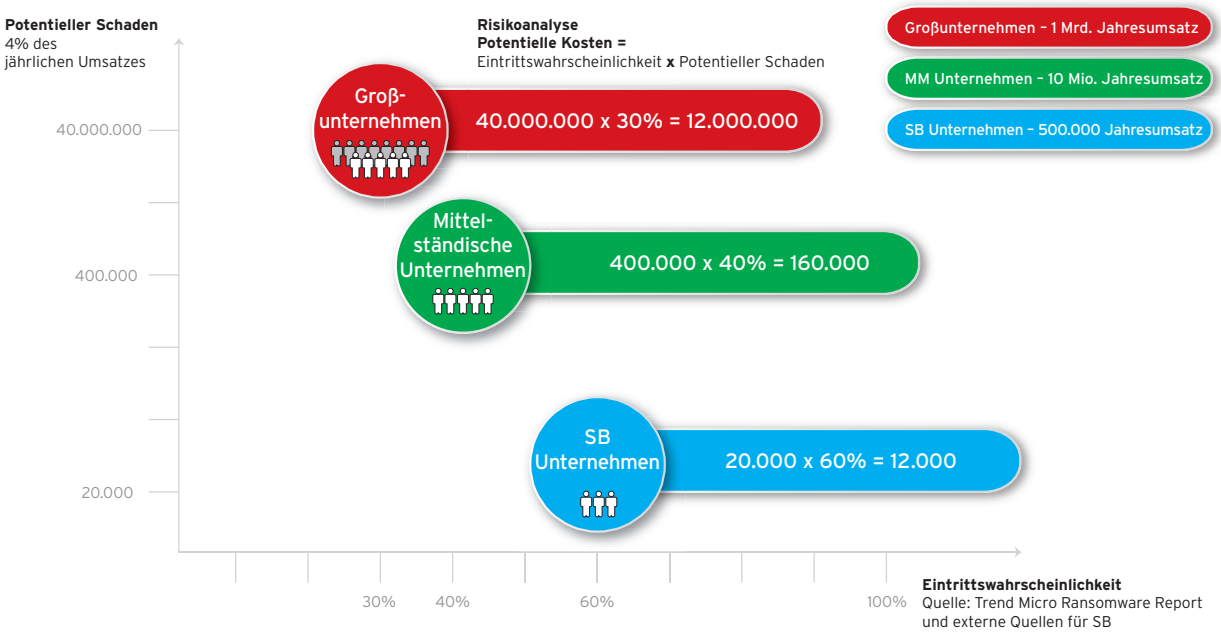
Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung der Europäischen Union (General Data Protection Regulation, GDPR). Auf über 200 Seiten werden signifikant erweiterte Rechte für EU-Bürger eingeführt sowie umfangreiche organisatorische und technische Anforderungen an Unternehmen gestellt, die personenbezogene Daten erheben (Data Controller) oder im Auftrag verarbeiten (Data Processor). Zu den wesentlichen Neuerungen gehört dabei die Reichweite der Verordnung:

Von der GDPR betroffen sind weltweit Unternehmen jeder Größe, die personenbezogene Daten von EU-Bürgern sammeln, verarbeiten und speichern – auch wenn damit keine kommerzielle Transaktion verbunden ist.

Zur Überwachung der Umsetzung werden nationale Datenschutzbehörden mit weitgehenden Rechten ausgestattet, darunter Anordnung der Informationsherausgabe, Durchführung von investigativen Audits, Verbot der Datenübertragung in Nicht-EU-Länder, Zugriff auf Daten und Einrichtungen vor Ort und Genehmigung von Standard-Vertragsbedingungen. Konkretes Risiko für Unternehmen: Fehlende Compliance kann mit Geldbußen bis zu vier Prozent des globalen Jahresumsatzes oder bis zu 20 Millionen Euro geahndet werden.

Wichtigste Änderungen für Bürger

Im Rahmen der GDPR sind EU-Bürger (Data Subjects) die Besitzer ihrer personenbezogenen Daten, die an Unternehmen nur ausgeliehen werden. Auf Nachfrage müssen Data Controller über die Verarbeitung personenbezogenen Daten informieren und eine Kopie bereitstellen. Bürger erhalten zudem das Recht auf Zugriff, Portierung, Richtigstellung, Löschung und Begrenzung ihrer personenbezogenen Daten. Es liegt in der Verantwortung von Unternehmen, über diese Rechte nicht nur zu informieren, sondern auch deren Wahrnehmung zu ermöglichen. Allen Bürgern steht es offen, bei Verletzung ihrer Rechte Beschwerden bei den Aufsichtsbehörden einzureichen oder auf dem Rechtsweg Schadensersatz vom Data Controller oder Data Processor zu fordern.



Quelle: Trend Micro Ransomware Report und externe Quellen für SB

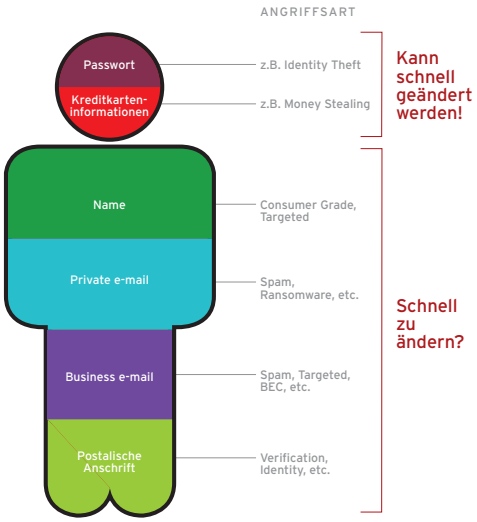
Organisatorische Konsequenzen für Unternehmen

Im Vergleich zu bestehenden Datenschutzregelungen werden durch die GDPR weitergehende Anforderungen formuliert: Personenbezogene Daten dürfen nur für spezifische, explizit angegebene und rechtmäßige Zwecke erhoben werden. Die Sammlung und Speicherung ist auf das für Verarbeitungszwecke notwendige Maß zu begrenzen. Jede weitere Verarbeitung, die mit diesen Prinzipien kollidiert, bedeutet einen Verstoß gegen die GDPR. Die Zustimmung zur Verarbeitung personenbezogener Daten muss darüber hinaus absolut eindeutig sein, Inaktivität kann nicht als Einverständnis gewertet werden. Um die Compliance sicherzustellen, müssen Unternehmen ihre gesamten Praktiken und Prozesse der Datensammlung auf den Prüfstand stellen. Auf organisatorischer Ebene gehört dazu:

- Anpassung aller internen Abläufe der Datensammlung und Verarbeitung
- Anpassung von Datenschutzerklärungen und Codes of Conduct
- Verhaltensregeln und Schulungen für Mitarbeiter
- Trennung der persönlichen Daten von EU-Bürgern von anderen Nationalitäten
- Bestellung eines Datenschutzbeauftragten, wenn der Unternehmensfokus auf Datenverarbeitung liegt (z.B. Marktforschung). Ansonsten gelten nationale Regelungen.

Die Umsetzung der Prinzipien liegt nicht im Ermessen der Unternehmen, denn mit der GDPR wird auch eine neue Rechenschaftspflicht eingeführt: Unternehmen müssen die Compliance durch Audits, Zertifizierungen, Dokumentation aller Entscheidungen und Aktivitäten hinsichtlich Datenverarbeitung sowie Privacy Impact Assessments nachweisen.

Über welche Daten sprechen wir?



Herausforderung: Technische Sicherheit und Meldepflicht

Neben den organisatorischen bilden die technischen Anforderungen das Herzstück der GDPR: Bei der Sammlung, Speicherung und Verarbeitung muss durch technische Maßnahmen sichergestellt sein, dass personenbezogene Daten vor folgenden Risiken geschützt sind:

- Zugriff oder Manipulation durch unberechtigte Dritte
- Nicht autorisierte oder nicht rechtmäßige Verarbeitung
- Diebstahl
- Versehentlicher Verlust
- Beschädigung oder Zerstörung
- Unbefugte Offenlegung

Auch hier greift wieder die Rechenschaftspflicht: Unternehmen müssen belegen, dass sie geeignete technische Maßnahmen ergriffen haben, wozu neben IT-Sicherheitslösungen auch Verfahren wie Pseudonymisierung gehören. Im Falle einer versehentlichen oder vorsätzlichen Verletzung der Datensicherheit besteht unter der GDPR zudem eine Meldepflicht, sobald das Unternehmen von dem Vorfall Kenntnis erlangt hat. Zu informieren sind:

- Aufsichtsbehörden
- Betroffene Individuen, auf Anordnung der Aufsichtsbehörden

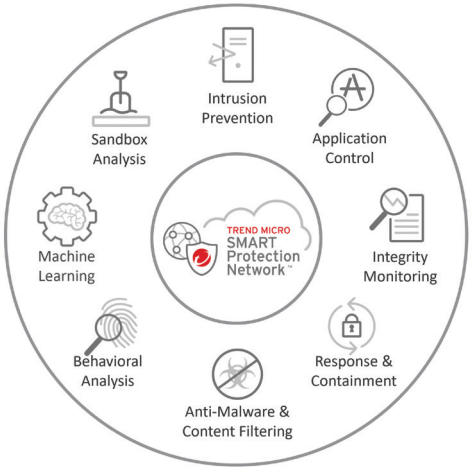
Die Meldung muss ohne „unangemessene Verzögerungen" erfolgen, ein bloßer Verdacht ist allerdings bislang nicht meldepflichtig. Data Controller und Data Processor stehen also vor der zusätzlichen Aufgabe, ihre internen Einrichtungen zur Erkennung von Sicherheitsvorfällen anzupassen, darunter technische Systeme und Reaktionspläne.

Trend Micro: Partner für GDPR-konforme Sicherheit

Die Umsetzung der Anforderungen der GDPR bedeutet für die allermeisten Unternehmen einen erheblichen organisatorischen Aufwand sowie Investitionen in technische Sicherheitsmaßnahmen. Umso wichtiger ist es, jetzt aktiv zu werden: Aufgrund der Komplexität des Themas empfiehlt sich auf organisatorischer Ebene die Zusammenarbeit mit speziellen Dienstleistern und Rechtsbeiständen, auf technischer Ebene ist Trend Micro ein Partner für den Schutz personenbezogener Daten vor Diebstahl, Manipulation oder unerwünschter Übertragung. Mit dem Trend Micro Portfolio führender Lösungen können technische Anforderungen der GDPR in physischen, virtuellen, cloudbasierten und hybriden Umgebungen abgedeckt werden, sowohl hinsichtlich Datensicherheit als auch frühzeitiger Erkennung von meldepflichtigen Vorfällen. Unternehmen müssen sich dabei bewusst sein, dass es keine absolute Sicherheit und auch keine technischen Allheilmittel gibt – durch die Zusammenarbeit mit Trend Micro können aber für jedes Szenario individuell optimale Lösungen gefunden werden, die State-of-Art-Sicherheits-technologien mit maximaler Transparenz und wirtschaftlicher Verhältnismäßigkeit verbinden.

Schutz vor bekannten und unbekannten Bedrohungen

Für bekannte Bedrohungen stehen erprobte Abwehrmechanismen bereit – aber wie können Unternehmen personenbezogene Daten vor unbekannten Bedrohungen schützen, die immer komplexer werden und sich immer besser tarnen? Mit XGen™ Security stellt Trend Micro einen Sicherheitsansatz bereit, der die besten Technologien aus jeder Generation mit aktuellsten Informationen aus dem weltweiten Smart Protection Network kombiniert. XGen Security unterstützt Trend Micro Lösungen auf allen Ebenen der Infrastruktur, jeweils optimiert für hybride Cloud-, Netzwerk- und Anwenderumgebungen. Dies ermöglicht die Abwehr noch unbekannter Bedrohungen, darunter beispielsweise Ransomware, Business E-Mail Compromise (BEC) und Business Process Compromise (BPC).

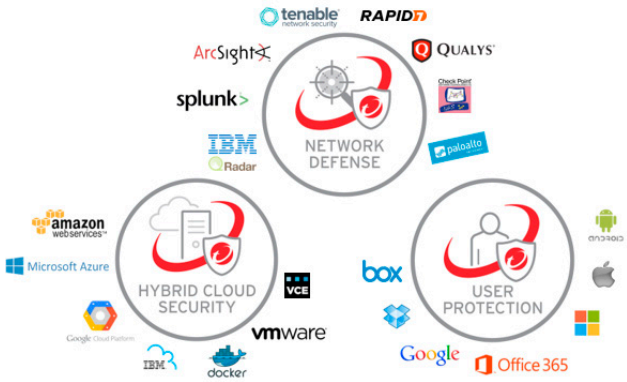


SMART

Bietet Schutz vor bekannten und unbekannten Bedrohungen

OPTIMIERT

Nahtlose Integration der Sicherheitslösungen in VMware, Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud und Office 365



VERNETZT

Austausch von Bedrohungsinformationen beschleunigt Reaktionszeiten

Die standort- und geräteunabhängige Erkennung in einem vernetzten System und die umgehende Anwendung der richtigen Abwehrtechnologie zum richtigen Zeitpunkt sorgen für maximale Transparenz und Performance.

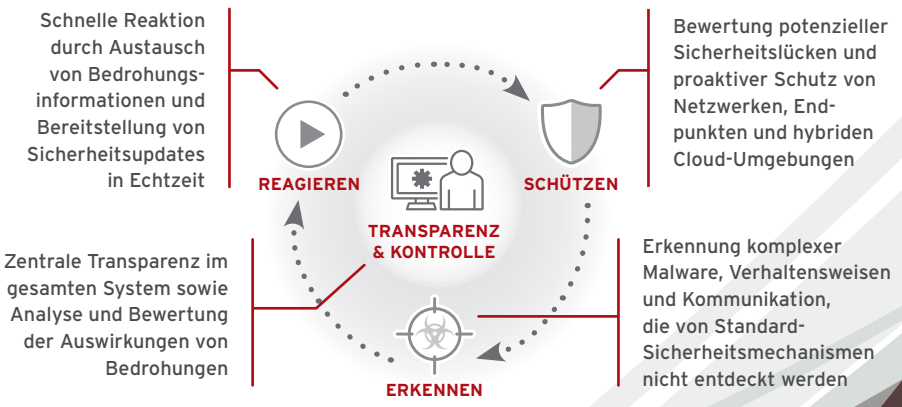
Schnellere Erkennung von Sicherheitsvorfällen

Isolierte Einzelprodukte haben einen zu engen Fokus, deshalb verknüpft Trend Micro seine XGen-powered Lösungen auf Endpunkten, Gateways und Servern sowie IPS Systeme zu einer Connected Threat Defense. Dadurch multipliziert sich die Sicherheit, denn alle relevanten Informationen stehen jetzt auf allen Ebenen sofort zur Verfügung und Reaktionen können in jeder Bedrohungsphase optimal koordiniert werden:

- **Prävention:** Proaktiver Schutz von Schwachstellen in Netzwerken, Endpunkten und Hybrid Clouds
- **Erkennung:** Identifikation komplexer Malware, Verhaltensweisen und Kommunikation
- **Analyse:** Untersuchung und Bewertung der Auswirkungen von Bedrohungen
- **Reaktion:** Bedrohungsinformationen und Sicherheits-Updates unternehmensweit in Echtzeit

Mit Deep Discovery bietet Trend Micro darüber hinaus eine Plattform zum Schutz vor komplexen Bedrohungen, die getarnte und gezielte Angriffe erkennt, analysiert und flexibel abwehrt. Mit speziellen Erkennungs-Engines, benutzerdefiniertem Sandboxing und den globalen Bedrohungsinformationen aus dem Smart Protection Network deckt die Lösung Angriffe auf, die von Standardsicherheitslösungen nicht erkannt werden. Deep Discovery erkennt und identifiziert auf einzigartige Weise versteckte Bedrohungen in Echtzeit und liefert im Anschluss eine ausführliche Analyse sowie aufschlussreiche Informationen zu Sicherheitsvorfällen.

Connected Threat Defense: besserer, schnellerer Schutz



Schutz von Anwenderaktivitäten

Anwender greifen heute mit unterschiedlichsten Geräten zuhause, unterwegs oder im Büro auf Unternehmensressourcen zu – das macht Endpunkt-Sicherheit zu einer komplexen Herausforderung. Trend Micro Smart Protection Suites bieten einen zentral verwalteten, mehrschichtigen Schutz für sensible Daten auf allen Endpunkten. Smart Protection Suites schützen alle Anwenderaktivitäten und verringern so das Risiko des Verlusts vertraulicher Daten. Unternehmen profitieren von erweitertem Schutz mit Sicherheit für Endpunkte, E-Mail- und Kollaborationslösungen, Internetaktivitäten und mobile Geräte. Durch das flexible Installationsmodell können lokale, Cloud-basierte oder hybride Installationen jederzeit optimal unterstützt und auch nachträglich unkompliziert angepasst werden.

Maximaler Schutz durch XGen Security: Zuverlässige maschinelle Lernverfahren werden mit weiteren Technologien zur Bedrohungsabwehr kombiniert. Für eine präzisere Erkennung werden Dateien sowohl vor der Ausführung als auch zur Laufzeit des Prozesses analysiert. Methoden zur Gegenprüfung reduzieren Fehlalarme.

Ineinandergreifende Sicherheitslösungen: Automatischer Austausch lokaler Bedrohungsdaten zwischen Endpunkt- und Gateway-Sicherheitsebenen schützt vor ubekannten Angriffen

Integrierter Schutz vor Datenverlust (iDLP): Sorgt für Datensicherheit, während Endpunkt- und E-Mail-Verschlüsselung sicherstellt, dass Daten nur von autorisierten Personen eingesehen werden können. Applikations- und Portkontrolle hindert Anwender daran, Informationen an falsche Stellen zu senden.

Transparenz der Anwendersicherheit: Alle Sicherheitsebenen werden über eine zentrale Management-Konsole verwaltet. Dies ermöglicht umfangreiche Analysen von Daten und Bedrohungen für die gesamte IT-Umgebung

Abwehr von Ransomware

Moderne Ransomware kann nicht nur den befallenen Rechner verschlüsseln, sondern auch angeschlossene Netzwerklaufwerke. Die Verschlüsselung der Daten kann dabei einen unrechtmäßigen Zugriff durch Dritte im Sinne der GDPR darstellen, der unter Umständen meldepflichtig ist. Selbst nach Zahlung verbleiben zudem Rückstände der Ransomware, die kostspielig entfernt werden müssen. Trend Micro Smart Protection Suites bieten verschiedene Funktionen, mit denen Sie das Risiko von Ransomware-Angriffen per E-Mail oder Web auf Ihren Endpoints minimieren, darunter:

- **Verhaltensüberwachung:** Erkennung von verdächtigem Verhalten, wie zum Beispiel die schnelle Verschlüsselung multipler Dateien. Der Verschlüsselungs-prozess kann automatisch gestoppt werden. Der betroffene Endpoint wird isoliert, bevor sich die Ransomware verbreitet und weiteren Schaden anrichten kann.
- **Applikationskontrolle:** White Lists erlauben nur das Ausführen von bekannten und seriösen Applikationen. Der Start von Ransomware wird dadurch verhindert.
- **Vulnerability Shielding:** Schützt vor Ransomware, die Software-Sicherheitslücken auf dem Endpunkt ausnutzen soll.

Ransomware greift darüber hinaus in zunehmendem Maße gezielt Server an. Angreifer nutzten hier bekannte Software-Schwachstellen zur Verbreitung aus. Trend Micro Deep Security schützt Ihre physischen, virtuellen und Cloud-basierten Server vor Ransomware durch:

- **Identifikation verdächtiger Aktivitäten:** Wenn Ransomware versucht, sich in einem Rechenzentrum auszubreiten (z.B. von einem Anwender zu einem Datei-Server), erkennt und blockiert Deep Security das verdächtige Verhalten. Gleichzeitig werden Verantwortliche alarmiert.
- **Schwachstellen-Abschirmung:** Bekannte Software-Schwachstellen werden abgeschirmt und Exploits somit verhindert. Dieses virtuelle Patching gewährleistet Schutz bis ein Patch eingespielt wird.
- **Erkennung lateraler Ausbreitung:** Falls Ransomware in ein Rechenzentrum gelangt, kann die Ausbreitung durch Erkennungs- und Blockade-Techniken wirkungsvoll eingedämmt werden.

Sprechen Sie uns an – wir hören zu

Trend Micro gehört zu den Pionieren der IT-Sicherheit und entwickelt seine Technologien und Lösungen seit 28 Jahren kontinuierlich weiter, damit Unternehmen der aktuellen Bedrohungslage immer einen Schritt voraus sind. Deshalb belegt Trend Micro die Spitzenposition im Gartner Magic Quadrant – seit 14 Jahren in Folge. Nutzen Sie dieses Know-how für Projekte zur GDPR-konformen Datensicherheit in Ihrem Unternehmen. Wir diskutieren gerne individuelle Herausforderungen und optimale Lösungswege.

TREND MICRO Deutschland GmbH
Zeppelinstraße 1 • 85399 Hallbergmoos
Tel: +49 (0)811 88990 – 700
Fax: +49 (0)811 88990 – 799
www.trendmicro.de