Datenmanagement, Cloudcomputing und Sicherheit IV

# Zum Umgang mit der Datenschutz-Grundverordnung

Dem Wettlauf gegen die Zeit bei der Umsetzung der Datenschutz-Grundverordnung (DSGVO) müssen sich Organisationen jeder Branche und Grösse stellen. Ein UTM-Ansatz (Unified Threat Management) kann dazu beitragen, den Weg zu gesetzeskonformen Abläufen zu ebnen.

› Thomas Fleischmann

Die Datenschutz-Grundverordnung ist eines der Top-Themen 2018. Schliesslich wird es am 25. Mai ernst. Während viele Unternehmen mit den einschlägigen Projekten in den kommenden Wochen bereits in den Endspurt gehen, sind andere gerade noch dabei, sich mit der Bedeutung und den direkten Auswirkungen der neuen Gesetzgebung auseinanderzusetzen. Doch für sie wird die Zeit jetzt besonders knapp.

Das strukturierte Zusammenspiel der Sicherheitsdienste im Rahmen einer UTM-Lösung sorgt dafür, dass sich eventuelle Lücken bei der Netzwerksicherheit zügig und verlässlich schliessen lassen. Passgenaue Visualisierungsmöglichkeiten garantieren zudem eine schnelle Reaktionsfähigkeit und erleichtern ein spezifisches Reporting.

## Der Geltungsbereich

In den Geltungsbereich der Datenschutz-Grundverordnung (DSGVO) fallen ausnahmslos alle Organisationen, welche personenbezogene Informationen von EU-Bürgern erfassen, speichern und/oder verarbeiten. Der Sitz des Unternehmens spielt dabei keine Rolle. Die Definition «personenbezogener Daten» ist gleichwohl gross gefasst. Darunter werden alle Informationen verstanden, die zur direkten oder indirekten Identifizierung von Personen herangezogen werden können – von Namen, Fotos, E-Mail-Adressen und Bankdaten über steuerliche Identifikationsnummern oder Posts in sozialen Medien bis hin zu medizinischen Informationen und sogar IP-Adressen von Computern, mit denen bestimmte Benutzerkonten oder Geräte verknüpft sind. Im Zuge dessen gibt es unterschiedliche Fallstricke zu beachten.

**kurz & bündig**

- In den Geltungsbereich der Datenschutz-Grundverordnung fallen ausnahmslos alle Organisationen, die personenbezogene Informationen von EU-Bürgern erfassen, speichern und/oder verarbeiten.
- Es gilt, auf Basis effektiver Netzwerksicherheitstechnologie Massnahmen zu ergreifen, um Daten während der Übertragung und Speicherung zu schützen und eine situationsbedingte Risikosensibilisierung sicherzustellen.
- Zudem zählen die verschiedenen Möglichkeiten zur vorbeugenden sowie korrektiven Abwehr und die jederzeitige Überprüfung der gültigen Sicherheitsrichtlinien.

So besteht beispielsweise mit der DSGVO für Unternehmen die Pflicht, Datensicherheitsverletzungen innerhalb von 72 Stunden den Aufsichtsbehörden zu melden und betroffene Personen unverzüglich darüber zu informieren. Ausgenommen sind hierbei Sicherheitsverletzungen bei verschlüsselten Daten. Darüber hinaus erfordert die neue Gesetzgebung, dass von jedem Individuum bei der Erfassung seiner persönlichen Daten eine ausdrückliche Einwilligung vorliegen muss. Die generischen Zustimmungserklärungen verlieren ihre Gültigkeit.

Stattdessen müssen Unternehmen spezifische Informationen zur erfassten Datenart sowie zum Speicher- und Verarbeitungszeitraum in klarer und verständlicher Sprache bereitstellen. Der EU-Bürger muss zudem jederzeit in der Lage sein, eine gegebene Einverständniserklärung einfach zurückziehen zu können. Ebenfalls sollte auf Unternehmensseite geprüft werden, ob die Benennung eines Datenschutzbe-

auftragten als zentraler Ansprechpartner gegenüber den Aufsichtsbehörden sowie für alle in diesem Zusammenhang eingehenden Beschwerden und Anfragen verpflichtend wird. Die Anforderungen sind hoch – genau wie die Sanktionen, die bei Nichterfüllung im Raum stehen. Geldstrafen in Höhe von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Umsatzes sind durchaus kein Pappenstiel.

## Netzwerksicherheit im Blick

Es gilt, auf Basis effektiver Netzwerksicherheitstechnologie Massnahmen zu ergreifen, um Daten während der Übertragung und Speicherung zu schützen, eine situationsbedingte Risikosensibilisierung sicherzustellen, Möglichkeiten zur vorbeugenden sowie korrektiven Abwehr zu gewährleisten und im Idealfall die Effektivität gültiger Sicherheitsrichtlinien jederzeit überprüfen zu können. Zudem kommt dem Thema Backup entscheidende Bedeutung zu. Gleichzeitig zählen optimierte Prozesse und Reporting-Strukturen, um Einverständniserklärungen und Meldungen in Bezug auf Compliance nachzuverfolgen.

Zur Minimierung des damit einhergehenden Aufwands sollte im Vorfeld in Erwägung gezogen werden, die Anzahl der Felder, die personenbezogene Daten enthalten, zu reduzieren und Daten bei der Übertragung und Speicherung zu verschlüsseln. Da ebenso der Faktor Mensch nicht zu unterschätzen ist, kann es von Vorteil sein, die Zahl der Mitarbeitenden, die auf die jeweiligen Daten Zugriff haben, zu reduzieren und die verbleibenden entsprechend zu sensibilisieren.

Vor diesem Hintergrund lassen die Ergebnisse einer weltweiten Umfrage von Watchguard vermuten, dass unterdessen zahlreiche Unternehmen unter Zeitdruck hinsichtlich der Umsetzung der DSGVO stehen. Im August 2017 waren 37 Prozent der insgesamt über 1600 befragten Organisationen auf der ganzen Welt noch nicht einmal sicher, ob ihr Unternehmen überhaupt von der Datenschutzgrundverordnung betroffen ist. Darüber hinaus gaben zum Zeitpunkt der Datenerhebung nur zehn Prozent der befragten Unternehmen an, die DSGVO-Vorgaben bereits umfassend erfüllen zu können. Von den Teilnehmern, die sich mit den Implikationen der Datenschutz-Grundverordnung bereits befasst hatten, bestätigten jedoch 51 Prozent, dass die Umsetzung mit signifikanten Änderungen der IT-Landschaft einhergeht. Hierbei wurden die Aspekte Firewall, VPN, Verschlüsselung, Webfilter, WLAN sowie Intrusion Prevention als in diesem Zusammenhang besonders relevant eingestuft.

Es liegt also nahe, sich mit einem Ansatz der Netzwerksicherheit zu befassen, der all diese Kernelemente effektiv kombiniert: Unified Threat Management. Auf Basis leistungsstarker Hardware können unterschiedliche Sicherheitsdienste –

von der Firewall über URL-Filter, Gateway Antivirus, Application Control, Data Loss Prevention bis hin zu weiteren, modernen Werkzeugen zur Gefahrenerkennung und -abwehr – gezielt unter einen Hut gebracht werden. Der Vorteil hierbei: Alle Schutzmechanismen lassen sich im Handumdrehen über zentrale Management-Funktionalität aktivieren und an individuelle Bedürfnisse anpassen – auch hinsichtlich der DSGVO-Vorgaben. Sind die Daten und Prozesse, die unter den Schutzmantel der DSGVO fallen, einmal ausgelotet, können passgenaue Einstellungen die Sicherheit entlang der gesetzlichen Vorgaben gewährleisten und potenzielle Risiken minimieren.

## Risiken reduzieren

Natürlich ist selbst die ausgefeilteste Technologie nicht in der Lage, den Unternehmen die projektspezifische Vorbereitung abzunehmen. Neben der Analyse, welche personenbezogenen Daten von EU-Staatsbürgern überhaupt in den eigenen Reihen erfasst werden, spielt auch die Gestaltung der damit einhergehenden Einwilligungsverfahren und -prozesse sowie der grundsätzlichen Kommunikationsabläufe eine wichtige Rolle. Zudem muss die Angemessenheit von Datenverarbeitungsrichtlinien und Dokumentationsmassnahmen auf Herz und Nieren geprüft werden.

Ist die Vorbereitungshürde erst einmal genommen, kann über den UTM-Ansatz allerdings schnell sichergestellt werden, dass Daten bei der Speicherung sowie Übertragung bestmöglich geschützt sind, indem beispielsweise VPN-Verbindungen per Drag&Drop verschlüsselt oder IP-Adressen maskiert werden. Das Risiko gegenüber äusseren Gefahren lässt sich über spezifische Mechanismen zur Bedrohungsbewertung, -erkennung und -abwehr, die darüber hinaus mit allen weiteren Security-Diensten Hand in Hand arbeiten, deutlich reduzieren. Dieses gezielte Zusammenspiel einzelner Security-Funktionalitäten ermöglicht nicht zuletzt zu jedem Zeitpunkt eine genaue, situationsabhängige Risikobewertung. Auf dieser Basis können identifizierte Schwachstellen im Ernstfall umgehend geschlossen werden. Gleichzeitig umfassen die Möglichkeiten im Rahmen von UTM auch Werkzeuge, mit denen Administratoren den Wirkgrad aktuell geltender Sicherheitsregeln jederzeit anwendungsübergreifend nachvollziehen und gegebenenfalls korrigierend eingreifen können.

Durch das zentrale Management und eine konsolidierte Erfassung sowie Visualisierung aller sicherheitsrelevanten Ereignisse ist gleichzeitig umfassende Transparenz zur Sicherheitslage des Unternehmens gegeben – Bedrohungen können deutlich schneller aufgedeckt werden: ein Argument, das im Hinblick auf die Forderung der DSGVO zur 72-stündigen Meldefrist bei Datenschutzverletzungen besonders ins Gewicht fällt. Letztendlich ist diese Fähigkeit bares Geld wert, die Strafen bei Missachtung sind hoch. Best Practice ist jedoch, es erst gar nicht so weit kommen zu lassen. Darum gibt es UTM-Funktionspakete, mit welchen zu jedem Zeitpunkt Richtlinien zur automatischen Abwehr von Vorkommnissen mit hoher Gefahrenstufe aufgesetzt werden können.

Einmal erkannte Bedrohungen werden via Cloud erfasst und haben keinerlei Chance mehr, weiter vorzudringen. Der Data-Loss-Prevention-Service (DLP) identifiziert parallel dazu alle Dateien, die persönliche Daten enthalten, und blockiert eine netzwerkfremde Übertragung. Hierbei lassen sich jederzeit individuelle Regeln erstellen, um beispielsweise erfasste Sozialversicherungsnummern, Kontodaten oder Krankenakten nachhaltig abzusichern. Last but not least sind sichere VPN-Verbindungen zwischen Unternehmenszentrale und verteilten Niederlassungen problemlos möglich, ganz im Sinne durchgängiger Datenverfügbarkeit bei gleichzeitig bestem Schutz.

Es lässt sich also festhalten, dass die Verankerung eines UTM-Szenarios die Umsetzung von DSGVO-Konformität entscheidend beschleunigen kann. Hier ist es wichtig, die Anbieterlandschaft genauer unter die Lupe zu nehmen und sich für den Lösungsansatz zu entscheiden, der hinsichtlich der UTM-Funktionalität den besten Schutz bietet. Zudem sollten auch Aspekte wie die Einfachheit der Bedienung und Performanceparameter in die Entscheidung einfliessen. Denn es geht ja nicht allein darum, den Stichtag 25. Mai zu halten. Die eingesetzte Sicherheitstechnologie sollte sich auch darüber hinaus als hilfreich erweisen und entsprechende Prozesse für KMU nachhaltig erleichtern. «

### Porträt

**Thomas Fleischmann**
Senior Sales Engineer in der Region Central Europe,
Watchguard Technologies

### Kontakt

thomas.fleischmann@watchguard.com
www.watchguard.com