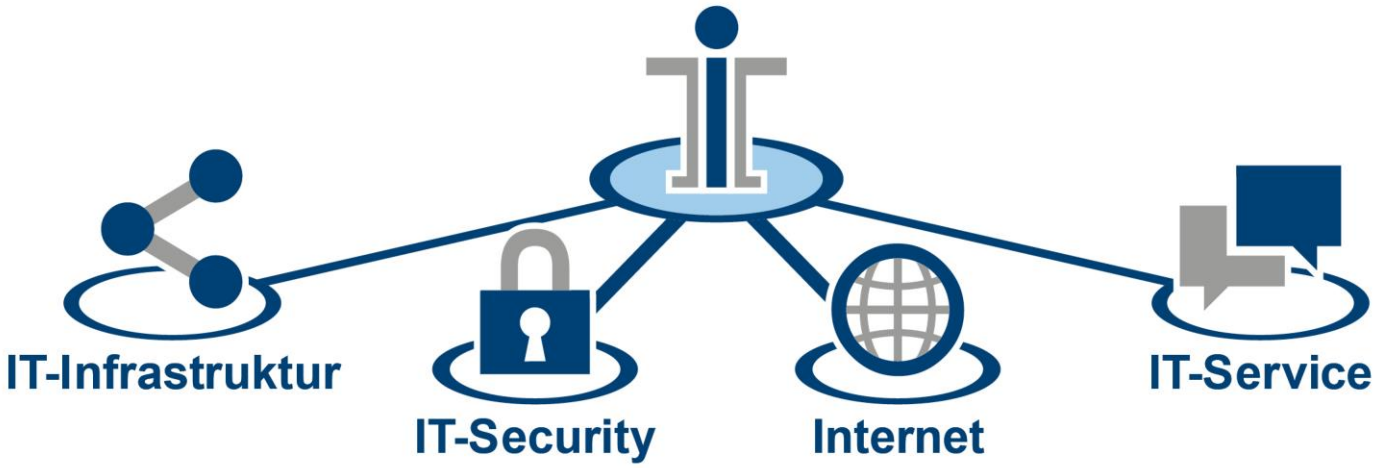
IT-ON.NET

Gut für Sie.
Gut für Ihre IT.

Datenschutzmaßnahmen mit WatchGuard

Datenschutz-Grundverordnung der EU

Erstellt von:
Kamil Jasinski
IT-On.NET GmbH • Wiesenstraße 21 • 40549 Düsseldorf



Zertifizierung der IT-On.NET GmbH & IT-On.NET Süd GmbH

TÜVRheinland ZERTIFIZIERT
Management System
ISO 9001:2008
www.tuv.com
ID 9105053408

Inhaltsverzeichnis

1. Der Wettlauf gegen die Zeit hat begonnen! 3
2. Wer ist davon betroffen 3
3. Was umfasst die Definition personenbezogener Daten 4
4. Achten Sie auf Stolpersteine 4
5. Die Erfolgsstrategie 5
6. Schneller am Ziel! 6
7. Die Total Security Suite von WatchGuard 10
8. DSGVO-Planungscheckliste 10

1. Der Wettlauf gegen die Zeit hat begonnen!

Im April 2016 wurde die EU-Verordnung 2016/679, auch bekannt als Datenschutz-Grundverordnung (DSGVO), verabschiedet. Unternehmen wie das Ihre setzen nun zum Endspurt an, um die Compliance vor dem Inkrafttreten dieser Verordnung ab 25. Mai 2018 sicherzustellen, da andernfalls hohe Geldstrafen und Gerichtsverfahren drohen. Diese Compliance-Maßnahmen erfordern einen größeren Aufwand und sind schwieriger umzusetzen, weil die Verordnung den Zuständigkeitsbereich der bisherigen Datenschutzrichtlinie aus dem Jahr 1995 (der Richtlinie 95/46/EC) maßgeblich erweitert.

Die gute Nachricht lautet – **Sie sind nicht allein!** Die meisten Unternehmen befinden sich beim Compliance-Prozess im „Hauptfeld“, um eine Analogie aus dem Radrennsport zu verwenden. Wir können die Ziellinie durch eine Zusammenarbeit aber einfacher und schneller erreichen.

2. Wer ist davon betroffen

Organisationen, die personenbezogene Informationen erfassen, speichern und/oder verarbeiten, müssen die Datenschutz-Grundverordnung erfüllen, wenn:

- Sie EU-Bürgern innerhalb der EU Waren und Dienstleistungen anbieten ODER
- das Verhalten von EU-Bürgern innerhalb der EU beobachten

Hierzu zählen Organisationen, die weder ihren Hauptsitz, noch Vertretungen in der Europäischen Union unterhalten, oder die EU-Mitarbeiter beschäftigen, aber keine Kunden in der Europäischen Union haben. Solange Sie personenbezogene Daten von Bürgern in der Europäischen Union in irgendeiner Form handhaben, gilt diese Verordnung auch für Sie.

Alle Organisationen, die dieses Kriterium erfüllen, müssen die Compliance sicherstellen. Falls Sie im größeren Umfang personenbezogene Daten verarbeiten gelten erweiterte Auflagen.

In der Verordnung werden Organisationen, die zur Einhaltung der DSGVO verpflichtet sind, entweder als „Datenverantwortliche“ oder „Datenverarbeitungsverantwortliche“ bezeichnet. Datenverantwortliche bestimmen Zweck, Umstände und Mittel zur Verarbeitung personenbezogener Daten, während Datenverarbeitungsverantwortliche die personenbezogenen Daten im Auftrag der Datenverantwortlichen verarbeiten.

„Eine Gesundheitseinrichtung kann Laborarbeiten beispielsweise extern vergeben. Sie müsste dafür bestimmte personenbezogene Informationen, die für Labordienste erfasst wurden, mit dem externen Anbieter teilen, um die Ergebnisse dem richtigen Patienten zuordnen zu können. Gemäß der DSGVO ist die Gesundheitseinrichtung in diesem Szenario der Datenverantwortliche, und das Labor ist der Datenverarbeitungsverantwortliche. Im Rahmen der Verordnung werden teils unterschiedliche Anforderungen an beide Rollen gestellt, Sie sollten sich also darüber informieren, welche dieser Rollen auf Ihre Organisation zutreffen.“

3. Was umfasst die Definition personenbezogener Daten

Die Verordnung interpretiert den Begriff der personenbezogenen Daten weitläufig. Alle Informationen, die zur direkten oder indirekten Identifizierung von Personen verwendet werden können, fallen unter diese Definition. Sie kann praktisch alles umfassen – Namen, Fotos, E-Mail-Adressen, Bankverbindungen, steuerliche Identifikationsnummern, Posts in sozialen Netzwerken, medizinische Informationen und sogar IP-Adressen von Computern, mit denen bestimmte Benutzerkonten oder Geräte verknüpft sind.

„Wenn Sie zum Beispiel ein Radrennen organisieren und die Startnummern in einem Computersystem erfassen oder zuweisen, sind diese Nummern mit einer bestimmten Person verknüpft. Diese Informationen gelten als personenbezogene Daten. Darüber hinaus können die Startnummern häufig problemlos auf Personendaten bezogen werden, z. B. Name, Adresse, Foto, Voruntersuchung vor dem Rennen und weitere Informationen."

4. Achten Sie auf Stolpersteine

Die DSGVO ergänzt die bisherige Datenschutzrichtlinie um verschiedene Punkte, die sich unter Umständen als Fallstricke erweisen können. Einige der wichtigsten neuen Auflagen sind nachstehend beschrieben. Eine vollständige Liste und zugehörige Einzelheiten entnehmen Sie bitte der Verordnung.

• MELDEPFLICHT BEI DATENSICHERHEITSVERLETZUNGEN:
Daten- und Datenverarbeitungsverantwortliche sind nun dazu verpflichtet, Aufsichtsbehörden Datensicherheitsverletzungen innerhalb von 72 Stunden zu melden und die betroffenen Personen unverzüglich hierüber zu informieren.

• AUSDRÜCKLICHE EINVERSTÄNDNISERKLÄRUNG:
Die DSGVO erfordert, dass die betroffene Person zum Erfassungszeitpunkt ihre ausdrückliche Einwilligung zur Erfassung ihrer personenbezogenen Daten geben muss. Das bedeutet, dass Organisationen generische Zustimmungserklärungen nicht länger in seitenlangem Juristenjargon verbergen können. Stattdessen müssen Organisationen spezifische Informationen zur erfassten Datenart sowie zum Speicher- und Verarbeitungszeitraum in klarer und verständlicher Sprache bereitstellen. Vor diesem Hintergrund gibt sich die Verordnung nur mit einer ausdrücklichen Einverständniserklärung zufrieden. Die Einverständniserklärung ist freiwillig und muss ferner ebenso einfach widerrufen werden können, wie sie erteilt wurde. Die Einverständniserklärung zur Datenerhebung und –Verarbeitung darf zudem nicht mehr über diverse Passsagen der AGB versteckt werden, sondern muss der betreffenden Person den Zweck der jeweiligen Erklärung explizit erwähnen.

• DATENÜBERTRAGUNG IN LÄNDER AUSSERHALB DER EU:
Personenbezogene Daten dürfen nicht in Länder außerhalb der EU übermittelt werden, sofern keine entsprechende Genehmigung der Aufsichtsbehörden vorliegt (Sichere Drittstaaten in Sinne des BDSG) oder die betroffene Person über den Datentransfer und die damit verbundenen Risiken informiert wurde und die Übertragung bewilligt.

• ERNENNUNG EINES DATENSCHUTZBEAUFTRAGTER (DSB):
Öffentliche und nichtöffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nichtöffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme Ihrer Tätigkeit verpflichtet (§4f (1) BDSG). Der Datenschutzbeauftragte vertritt Sie vor den Aufsichtsbehörden, die die Einhaltung der Verordnung überwachen und sicherstellen. Er oder sie ist auch der Ansprechpartner für alle Anfragen oder Beschwerden vonseiten betroffener Personen. Außerdem unterstützen Datenschutzbeauftragte gemäß der Datenschutz-Folgeabschätzung (DPIA) die Compliance-Aktivitäten in Ihrem Unternehmen. Sie sind für die Kommunikation der Sicherheitsrichtlinien, Compliance-Einschätzungen, Anfragen betroffener Personen und für die Meldepflicht im Falle von Datensicherheitsverletzungen zuständig. Gemäß der Verordnung erstattet der Datenschutzbeauftragte an eine Führungskraft Bericht und wird für einen Zeitraum von zwei Jahren ernannt, der verlängert werden kann.

• GELDBUSSEN BEI NICHTEINHALTUNG:
Unternehmen und Organisationen drohen bei Nichterfüllung der Datenschutz- Grundverordnung Geldbußen in Höhe von bis zu 20 Millionen Euro oder 4 % des weltweiten Konzern-Umsatzerlöses. Die Geldbußen sind gestaffelt und können bereits beim ersten Verstoß verhängt werden. Sie können überdies eine Geldstrafe in Höhe von 2 % oder 10 Millionen des weltweiten Konzern-Umsatzes enthalten, wenn beispielsweise keine ordnungsgemäßen Aufzeichnungen geführt werden (Artikel 28). Hinzu kommt, dass weitere Kosten für Organisationen anfallen können, etwa Anwaltskosten oder Kosten für gerichtliche Verfügungen, falls EU-Bürger das Gefühl haben, dass ihre Rechte verletzt wurden, auf Schadensersatz klagen und den Prozess gewinnen.

5. Die Erfolgsstrategie

Die Umsetzung der Verordnung erfordert maßgebliche Anstrengungen von praktisch allen Unternehmen. Sie müssen voraussichtlich folgende Elemente zu Ihrer Sicherheitsinfrastruktur hinzufügen:

- Datenschutzmaßnahmen auf der Grundlage der neuesten und effektivsten Netzwerksicherheitstechnologie, die:
  - Daten während der Speicherung und Übertragung schützt
  - eine situationsbedingte Risikosensibilisierung sicherstellt
  - eine echtzeitnahe Umsetzung vorbeugender, korrektiver Abwehrmaßnahmen ermöglicht und vor Schwachstellen oder Vorfällen schützt, die die Datensicherheit gefährden können
  - Werkzeuge zur Beurteilung der Wirksamkeit von Sicherheitsrichtlinien bereitstellt
- Eine Möglichkeit zur Wiederherstellung von Daten, um die Datenverfügbarkeit sicherzustellen, falls sie aufgrund eines Sicherheitsvorfalls temporär unterbrochen wird
- Neue oder optimierte Prozesse und Reporting-Strukturen, um Einverständniserklärungen sowie Meldungen in Bezug auf Compliance und Datensicherheitsverletzungen nachzuverfolgen.

Sie sollten darüber hinaus in Erwägung ziehen, die Auswirkungen/Risiken bei der Umsetzung der DSGVO zu beschränken, um den mit Überwachungs-, Dokumentations- und Compliance-Maßnahmen verknüpften Aufwand zu senken.

Sie können zum Beispiel:

- Die Anzahl der erfassten/verarbeiteten Felder, die personenbezogene Daten enthalten, reduzieren
- Den Zeitaufwand für die Aufbewahrung/Verarbeitung von personenbezogenen Daten reduzieren
- Daten bei der Speicherung und Übertragung verschlüsseln
- IP-Adressen maskieren und weitere, benutzerrelevante Informationen anonymisieren
- Die Zahl der autorisierten Mitarbeiter, die Zugriff auf personenbezogene Daten haben, beschränken
- Den Bedrohungsschutz und die Gefahrenabwehr für personenbezogene Daten erhöhen oder diverse organisatorische Maßnahmen einleiten.

Am Ende dieses Dokuments finden Sie eine DSGVO-Planungscheckliste, die Ihnen den Einstieg in die Compliance-Planung erleichtert. Anhand der Checkliste und der zugehörigen Fragen können Sie aktuelle Sicherheitsrichtlinien und -vorkehrungen evaluieren und im Anschluss verordnungsrelevante Lücken und Anpassungsbedarf identifizieren.

6. Schneller am Ziel!

Jetzt haben Sie also bereits eine gute Vorstellung davon, wo Sie in Bezug auf die DSGVO-Compliance Ihres Unternehmens ansetzen müssen. Sie werden sicherlich versuchen, Lücken zu füllen und Unzulänglichkeiten auszuräumen, die der Erfüllung der DSGVO im Wege stehen, um diese gewaltige Aufgabe termingerecht abzuschließen. WatchGuard kann Sie bei der Erfüllung der Compliance-Vorschriften mit hochwirksamer Datensicherheitstechnologie und Datenschutzmaßnahmen unterstützen.

Und wir machen es Ihnen leicht. WatchGuard stellt Ihnen das Datensicherheitsupgrade bereit, das Sie zur Einhaltung der DSGVO-Datenschutzmaßnahmen benötigen – in einem benutzerfreundlichen Paket inklusive Total Security Suite. Die WatchGuard Firebox® Security Appliance mit Total Security Suite bietet umfängliche Sicherheit auf Enterprise-Niveau. Sie deckt 16 der Top 20 SANS-Sicherheitskontrollen (V6) ab. Mit diesem Rundumpaket können Sie bei der DSGVO-Compliance auf Nummer sichergehen.

Eine Firebox Security Appliance von WatchGuard mit Total Security Suite deckt 16 der Top 20 SANS-Sicherheitskontrollen ab

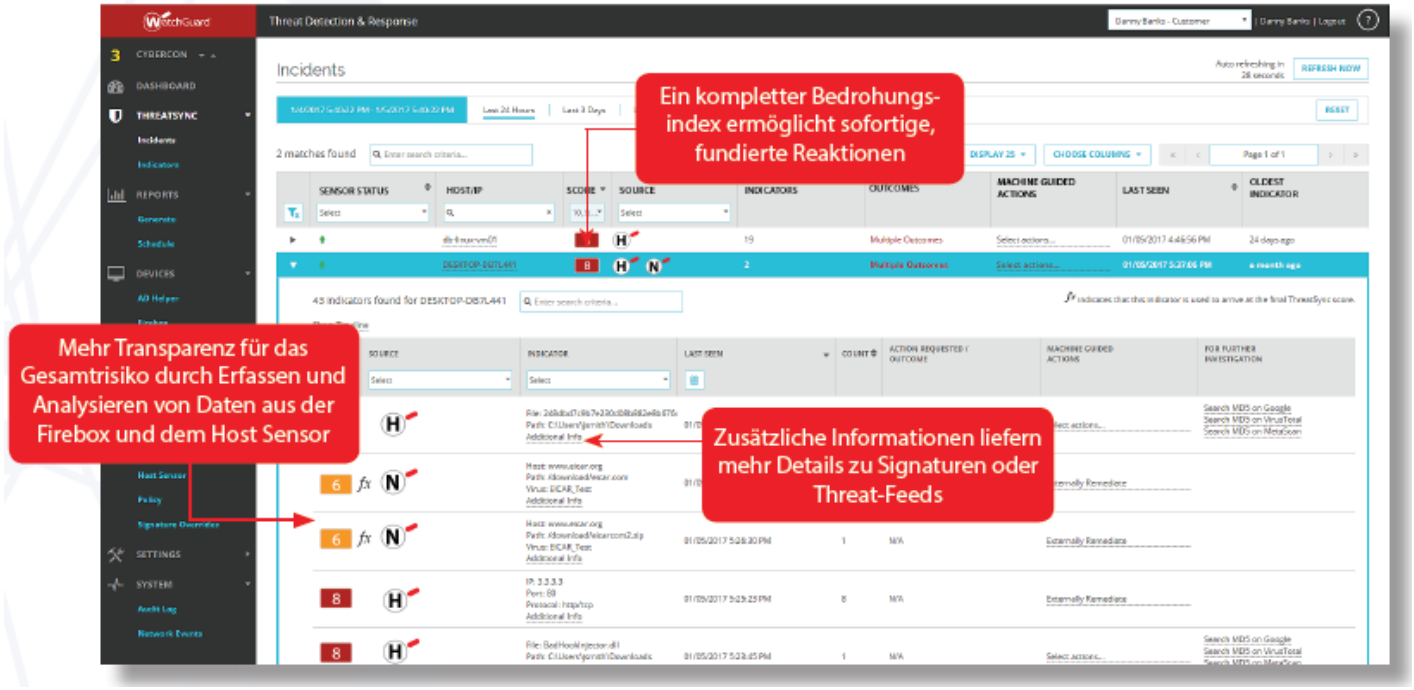
Die Top 20 SANS-Sicherheitskontrollen (V6)

CS1	Inventarisierung autorisierter und nicht autorisierter Geräte	*Ja*	CS11	Sichere Konfigurationen für Netzwerkgeräte wie Firewalls, Router und Switches	*Ja*
CS2	Inventarisierung autorisierter und nicht autorisierter Software	*Ja*	CS12	Absicherung des Netzwerkperimeters	*Ja*
CS3	Sichere Hardware- und Softwarekonfigurationen auf Mobilgeräten, Laptops, Workstations und Servern	*Ja*	CS13	Datenschutz	*Ja*
CS4	Kontinuierliche Bewertung und Behebung von Schwachstellen	*Ja*	CS14	Kontrollierter Zugriff basierend auf dem Need-to-Know-Prinzip	*Ja*
CS5	Kontrollierte Nutzung von Administratorrechten	*Ja*	CS15	Kontrolle drahtlosen Zugangs	*Ja*
CS6	Verwaltung, Monitoring und Analyse von Prüfprotokollen	*Ja*	CS16	Kontenüberwachung und -kontrolle	*Ja*
CS7	Schutz für E-Mail und Webbrowser	*Ja*	CS17	Bewertung der Sicherheitskompetenzen und angemessene Schulungen zum Schließen von Lücken	–
CS8	Schutz vor Malware	*Ja*	CS18	Sicherheit der Anwendungssoftware	*Ja*
CS9	Einschränkung und Kontrolle von Netzwerkports, -protokollen und -diensten	*Ja*	CS19	Ereignisabhängige Reaktion und Eingriff	–
CS10	Möglichkeit zur Wiederherstellung von Daten	*Nein*	CS20	Penetrationstest und Red-Team-Übungen	–

Die Total Security Suite ist eine einzigartige Lösung, die speziell auf DSGVO-Anforderungen abgestimmt ist. Sie umfasst:

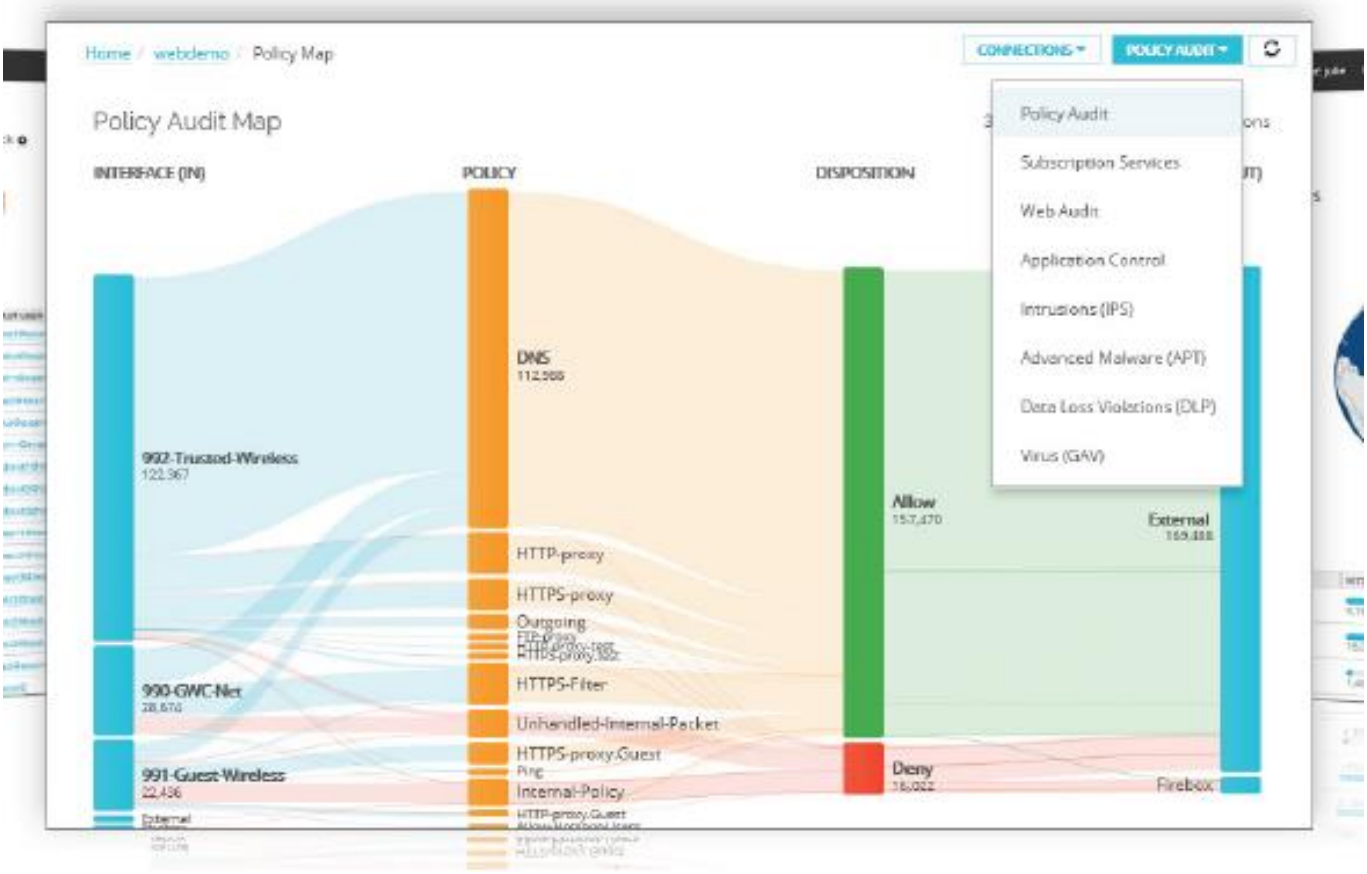
• Threat Detection and Response (TDR):
Die DSGVO fordert eine „situationsbedingte Sensibilisierung“, die Sie mit unserer besonderen ThreatSync-Funktion sicherstellen können. ThreatSync setzt Endpunkt- und Netzwerksicherheitsdaten zueinander in Beziehung und informiert Sie anhand eines übersichtlichen Dashboards über eskalierende Sicherheitsvorfälle.

Sie können ferner Richtlinien für die automatische Abwehr von Sicherheitsvorfällen mit hoher Gefahrenstufe erstellen, die über die benötigten „echtzeitnahen, vorbeugenden, korrektiven und Abwehrmaßnahmen“ hinausgehen. Noch besser: Wurde eine Bedrohung abgewehrt, werden die Daten mit Informationen zur Bedrohungslage kombiniert, sodass die Bedrohung nachfolgend erkannt wird und nicht erneut in Ihr Netzwerk gelangt. Und da Threat Detection and Response ein cloudbasierter Dienst ist, können Sie Ihre Daten in der EU speichern lassen, um den Auflagen des zugehörigen DSGVO-Datenübertragungsartikels Rechnung zu tragen.



• WatchGuard Dimension™:

Dimension bietet eine zeitnahe und effektive Lösung für DSGVO-Auflagen, die einen einfachen Zugriff auf aussagekräftige Protokolldaten vorsehen. Mit diesen Big Data-Visualisierungs- und Reporting-Werkzeugen lassen sich wichtige Bedrohungen für die Netzwerksicherheit sowie Probleme und Trends zeitnah identifizieren, Bedrohungen schneller abwehren und Berichte über sämtliche Sicherheitsaktivitäten im Netzwerk erstellen. Auf diese Weise können Sie schneller entsprechende Sicherheitsrichtlinien für das gesamte Netzwerk festlegen. Dimension umfasst darüber hinaus eine leistungsstarke Funktion zur Anonymisierung des Benutzers, die sämtliche personenbezogenen Daten in Berichten, Dashboards und Zusammenfassungen durch Platzhaltertexte ersetzen kann. Die Verschlüsselung von Benutzernamen, IP-Adressen, Host- und Mobilgerätenamen erfolgt durch eindeutige, zufällig generierte alphanumerische Sequenzen, um sicherzustellen, dass die Daten während der Übertragung maskiert werden.



• Data Loss Prevention (DLP):
Bei der DSGVO dreht sich alles um den Datenschutz. Unser DLP-Dienst identifiziert Dateien, die personenbezogene Daten enthalten, blockiert eine netzwerkfremde Übertragung und beugt somit unbeabsichtigten Datensicherheitsverletzungen vor. DLP sucht auf der Grundlage der von Ihnen festgelegten Regeln nach persönlichen Angaben wie Sozialversicherungsnummern, Bankkontodaten und Krankenakten.

• Verschlüsselung und VPN:
Der Erfolg einer Compliance-Strategie wird maßgeblich durch das Verschlüsseln personenbezogener Daten bei der Speicherung und Datenübertragung bestimmt, da sich die Meldepflichtauflagen im Falle einer Datensicherheitsverletzung dadurch erheblich reduzieren. Mit Firebox UTM-Lösungen von WatchGuard können Sie problemlos Drag-&-Drop-VPN-Verbindungen zwischen der Unternehmenszentrale und Ihren Firmenstandorten erstellen. Drag-&-Drop-VPNs zeichnen sich nicht nur durch ein schnelles und benutzerfreundliches Setup aus, sie sind zudem langlebig und für ihre Stabilität bekannt – das ist von zentraler Bedeutung, wenn Ihr Unternehmen auf eine durchgängige Datenverfügbarkeit angewiesen ist.

Berücksichtigt man sämtliche leistungsstarken Sicherheits- und VPN-Funktionen, die Transparenz und Benutzeranonymisierung von WatchGuard Dimension, die automatisierte Gefahrenabwehr und die situationsbedingte Sensibilisierung durch Threat Detection and Response, ist die WatchGuard Firebox mit Total Security Suite der eindeutige Gewinner, mit dem Sie die DSGVO-Compliance-Ziele fristgerecht erreichen!

• DNS Watch:
WatchGuard DNS Watch nutzt die Erkennung auf DNS-Ebene, um eine zusätzliche Sicherheitsebene zu schaffen, um Malware-Infektionen zu erkennen und zu stoppen. Bösartige DNS-Anfragen werden automatisch erkannt und blockiert und leiten die Benutzer an einen sicheren Ort statt an den Angreifer weiter. Die Personal Touch-Komponente dieses Dienstes liefert detaillierte Berichte über die erkannte und blockierte Infektion.

Das Beste daran ist, dass der Benutzer, der die Anfrage stellt, auf eine sichere Seite weitergeleitet wird, die ergänzende Informationen zu Ihrer bereits absolvierten Phishing-Ausbildung enthält. Ihre Mitarbeiter an ihre Schulung zu erinnern, wenn sie gerade auf einen Link oder eine Anlage geklickt haben, ist der effektivste Weg, dies in Zukunft zu verhindern. Verbunden mit dieser Schulung ist eine Nachricht von Ihnen, die den Benutzer möglicherweise dazu auffordert, Sie anzurufen oder die E-Mail weiterzuleiten, auf die er gerade geklickt hat. Im Moment sind die Benutzer viel empfänglicher für Ratschläge, sodass sich die Möglichkeit bietet, neue Sicherheitsfunktionen wie die Multi-Faktor-Authentifizierung oder die Aktivierung eines Passwortmanagers zu aktivieren.

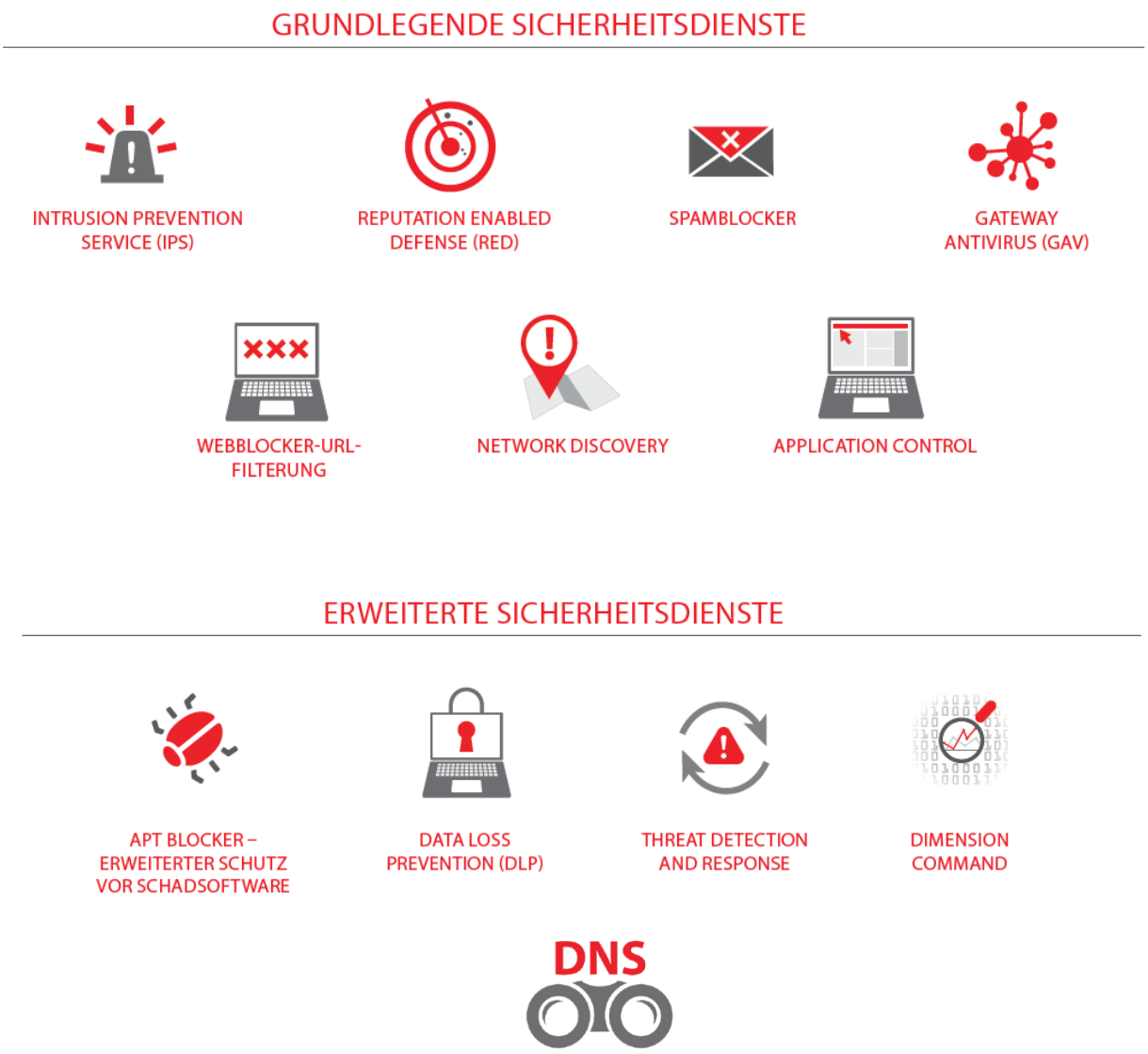
IT-On.NET GmbH
Wiesenstraße 21, 40549 Düsseldorf

Tel.: +49 211 / 95 69 1 – 0
Email: info-dus@it-on.net

IT-On.NET SÜD GmbH
Römerstr. 39, 78183 Hüfingen Behla

Tel.: +49 771 / 89784 - 300
Email: info-sued@it-on.net

7. Die Total Security Suite von WatchGuard



8. DSGVO-Planungscheckliste

Unsere DSGVO-Planungscheckliste unterstützt Sie bei der Evaluierung und Umsetzung von DSGVO-Compliance-Maßnahmen. Die Planungscheckliste erhebt keinen Anspruch auf Vollständigkeit und sollte in Verbindung mit anderen Ressourcen zur Ausarbeitung eines umfassenden Compliance-Plans genutzt werden.

• Ermittlung der Felder mit personenbezogenen Daten von EU-Staatsbürgern, die von Ihrem Unternehmen erfasst werden

- Welche personenbezogenen Daten werden erfasst und/oder verarbeitet?
- Wo werden die Daten gespeichert oder übertragen? Wie lange?
- Welche Aufbewahrungsrichtlinien oder -prozesse werden auf diese Daten angewendet? Könnten sie gestrafft werden?
- Haben Sie oder eine Fremdfirma die Kontrolle über die Daten?
- Verbleiben diese Daten jederzeit innerhalb der EU?

• Einwilligungsverfahren und -prozesse bei der Erfassung personenbezogener Daten

- Werden alle betroffenen Personen unmissverständlich um ihre ausdrückliche Einverständniserklärung zur Erfassung und Verarbeitung ihrer Daten gebeten?
- Wird die Einverständniserklärung zum Erfassungszeitpunkt erteilt?
- Sind in die Kontaktdaten des Datenverantwortlichen, Verarbeitungsverantwortlichen und Datenschutzbeauftragten (DSB) (falls zutreffend) in den Mitteilungen ausdrücklich angegeben?
- Werden der Zweck der Datenverarbeitung, die Verarbeitungssicherheit und die rechtlichen Grundlagen beschrieben?
- Wird der Aufbewahrungszeitraum für die Daten genannt?
- Werden die Empfänger oder Empfängerkategorien für die Daten angegeben?
- Werden die betroffenen Personen über ihre Rechte bezüglich des Zugriffs, der Berichtigung und Löschung der Daten, der Verwendung tragbarer Datenträger sowie über ihr Recht zum Einreichen von Beschwerden bei einer Aufsichtsbehörde informiert?
- Ist eine Absichtserklärung zur Übermittlung der Daten außerhalb der EU enthalten?
- Wird darauf hingewiesen, ob die Datenerfassung obligatorisch oder freiwillig ist, und werden die Folgen im Falle einer Verweigerung der benötigten Angaben dargelegt?
- Kann die Einverständniserklärung ebenso einfach widerrufen werden, wie sie erteilt wurde?

• Kommunikation mit betroffenen Personen

- Wie können betroffene Personen auf ihre Daten zugreifen, diese berichtigen, das Löschen der Daten beantragen und sie für die Datenübertragung extrahieren?
- Wie können betroffene Personen ihre Einwilligung widerrufen?
- Wie nimmt Ihr Unternehmen mit den betroffenen Personen Kontakt auf, um eine Datensicherheitsverletzung zu melden?

• Angemessenheit von Datenverarbeitungsrichtlinien und aktuellen Dokumentationsmaßnahmen

- Arbeiten Sie mit Datensätzen, die eine Einverständniserklärung erfordern?
- Verarbeiten Sie Datensätze, oder verfügen Sie über Datenverarbeitungsprotokolle, die personenbezogene Angaben beinhalten?
- Sind diese Datensätze geschützt? Können sie von autorisiertem Personal abgerufen, durchsucht oder in Berichten zusammengefasst werden?
- Sind die Richtlinien, die die Datenverarbeitung hinsichtlich der Compliance-Anforderungen der Verordnung beschreiben, auf dem neuesten Stand?
- Bei Datenverantwortlichen außerhalb der EU: Wurde ein Vertreter innerhalb der EU ernannt und ist dies dokumentiert?
- Falls Datenverarbeitungsdienste vertraglich vereinbart wurden, enthält der rechtsgültige Vertrag die erforderlichen Klauseln, um einen angemessenen Schutz und die Handhabung personenbezogener Daten im Einklang mit der DSGVO sicherzustellen?
- Besteht eine ausreichende Zugriffskontrolle für Server und Gebäude, um einen unbefugten Zugriff auf personenbezogene Daten zu verhindern?

• Ermitteln Sie, ob Ihre Sicherheit und Technologie die DSGVO-Anforderungen erfüllen

- Werden angemessene technische und organisatorische Maßnahmen umgesetzt, um die Daten vor versehentlicher oder unrechtmäßiger Vernichtung, Verlust, Modifizierung sowie vor unerlaubter oder widerrechtlicher Speicherung, Verarbeitung, Zugriff und Offenlegung zu schützen?
- Decken die Sicherheitsrichtlinien Folgendes ab:
  - Den Schutz der Daten während der Speicherung und Übertragung
  - Die Wiederherstellung des Datenzugriffs, falls die Daten aufgrund eines Sicherheitsvorfalls temporär nicht verfügbar sind
  - Ist eine situationsbedingte Risikosensibilisierung sichergestellt und eine echtzeitnahe Umsetzung vorbeugender, korrektiver und Abwehrmaßnahmen gegeben, die vor Schwachstellen oder Vorfällen schützt, die die Datensicherheit gefährden können?
  - Beschreiben Sie den Prozess zur regelmäßigen Einschätzung der Wirksamkeit der Sicherheitsrichtlinien
- Gibt es einen Prozess, mit dem Datensicherheitsverletzungen innerhalb von 72 Stunden gemeldet werden können?
- Wurde eine Datenschutz-Folgeabschätzung (DSFA) durchgeführt, um zu beurteilen, ob Verarbeitungsvorgänge etwaige spezifische Risiken beinhalten? Wurde die Folgeabschätzung innerhalb der letzten zwei Jahre bzw. direkt im Anschluss an Änderungsmaßnahmen durchgeführt, die sich auf spezielle Risiken bei Verarbeitungsvorgängen bezogen?
- Wurde ein Datenschutzbeauftragter (DSB) ernannt?

Die Antworten auf die Fragen in dieser Checkliste helfen Ihnen, Unzulänglichkeiten zu identifizieren, so dass diese fristgerecht behoben werden können.

Bei weiteren Fragen wenden Sie sich bitte an unserem Vertriebsteam:

Ihre Ansprechpartner bei der IT-On.NET:

Aziz El Malahi
Kamil Jasinski
Jürgen Thurau
Kerim Kirecci
Timo Becirovic
Jonathan Braun
Viktor Kloster

Oder senden Sie eine E-Mail an:

vertrieb-nord@it-on.net

Weitere Informationen finden Sie unter:

www.it-on.net und www.watchguard.de