KASPERSKY lab

Die DSGVO – mehr als nur Kontrollkästchen

Cybersicherheitslösungen allein können zwar keine Compliance sicherstellen, bieten aber wirksamen Schutz vor Datenschutzverletzungen und Lecks von sensiblen Daten.

www.kaspersky.de

#truecybersecurity

Die DSGVO – mehr als nur Kontrollkästchen

„Ohne Sicherheit keine Privatsphäre" ist ein lang etablierter Grundsatz, was Datenschutz betrifft. Jetzt, da die Datenschutz-Grundverordnung der EU Realität wird, ist es Zeit, einen Blick darauf zu werfen, wie Cybersicherheitstechnologien den von der Verordnung angestrebten breiteren Schutz von Daten und Privatsphäre unterstützen können.

Personenbezogene Daten: ein Goldesel für Cyberkriminelle

Personenbezogene Daten sind praktisch allgegenwärtig.

Routinemäßig übermitteln die Menschen personenbezogene Daten an Unternehmen aller Art, oft ohne zu hinterfragen oder zu verstehen, warum oder wie sie verwendet werden oder sich zu informieren, an welche unbekannten Dritten die Daten weitergegeben werden.

Für das Jahr 2017 gaben 23 % der der DSGVO unterliegenden Unternehmen an, in den letzten 12 Monaten einen Cyberangriff erlebt zu haben.[1]

Wir alle haben schon bis ans Ende einer vagen Endbenutzer-Lizenzvereinbarung geblättert und auf „Zustimmen" geklickt, ohne wirklich zu wissen, was mit unseren Daten passiert. Indem sie die Leistungserbringung von dieser Zustimmung abhängig machen, zwingen viele Unternehmen den Benutzer effektiv, das Risiko einzugehen, dass seine Daten in falsche Hände geraten könnten. Dies ist leider oft der Fall.

Während die Mehrheit der Unternehmen ihr Bestes tun, um die von ihnen gesammelten Daten zu schützen, geschieht das Sammeln der Daten oft ohne wirklichen Sinn, außer dem, sich Informationen zu verschaffen, die „vielleicht ganz praktisch sein" könnten.

Mit dem besten Willen der Welt bedeutet ein Mangel an etablierten Prozessen in Kombination mit eingeschränktem Bewusstsein für die begleitenden Risiken und Verantwortlichkeiten häufig, dass Daten ohne jegliche Sicherheitsvorkehrungen gesammelt und gespeichert werden. Schlimmer noch, die Daten werden oft ohne Umsetzung von Datenschutzvereinbarungen – oder ohne Wissen oder ausdrückliche Zustimmung der betroffenen Person an Dritte weitergegeben (oder verkauft).

Leider sind die personenbezogenen Daten, die für Ihre Geschäftstätigkeit wichtig und nützlich sind, auch lukrativ für Cyberkriminelle: ob Treueprogramme oder Zahlungsdaten, Geburtsdaten oder Krankenakten. Alles, was Ihrem Unternehmen hilft, den Kundenkontakt zu personalisieren oder Mitarbeiter zu verwalten, ist besonders attraktiv für Cyberkriminelle. Letztlich werden Daten zu einer Art krimineller Währung, mit der auf den Schwarzmärkten des Darknets getauscht und gehandelt wird.

Seit dem 25. Mai 2018 sind solche Vorkommnisse nicht mehr nur das Problem der betroffenen Personen, sondern auch Ihr Problem.

1 Marsh: GDPR Preparedness: An Indicator of Cyber Risk Management (Oktober 2017)

Fünf Buchstaben, eine große Datenschutzinitiative

59 % der Unternehmen gehen davon aus, dass ihre IT-Sicherheit irgendwann kompromittiert wird, und erkennen die Notwendigkeit, sich auf solche Ereignisse vorzubereiten.[2]

Datenschutzverletzung? Strafe

Nach einer massiven Verletzung von Kundendaten im Jahr 2015 wurde dem britischen Telekommunikationsunternehmen TalkTalk vom Information Commissioner's Office, dem britischen Datenschutzbeauftragten, die Rekordstrafe von 400 000 GBP auferlegt.

Die Geldbuße war deshalb so hoch, weil festgestellt wurde, dass der Verstoß hätte verhindert werden können, hätte das Unternehmen grundlegende Schritte unternommen, um die Kundendaten zu schützen.

Angesichts der vorgesehenen Höchststrafe der DSGVO von 4 % des globalen Umsatzes hätten diese 400 000 GBP auch 60 Millionen GBP betragen können, wenn das Gesetz in vollem Ausmaß angewandt worden wäre. Zumindest Audits, Überwachungen und eine Überarbeitung der Prozesse wären notwendig – dies alles kostet Geld.[3]

Schlagzeilen mit Strafsätzen von 4 % des weltweiten Gesamtumsatzes und der Anforderung, Datenschutzverletzungen innerhalb von 72 Stunden zu melden, ziehen viel Aufmerksamkeit auf sich. Es muss aber auch gesagt werden, dass die DSGVO Ihre Chance ist, einmal zu analysieren, was Sie mit den von Ihnen erhobenen personenbezogenen Daten eigentlich tun und warum.

Zudem ist es auch ein perfekter Zeitpunkt, um das Konzept Ihres Unternehmens hinsichtlich Cybersicherheit neu zu betrachten, denn wenngleich Sicherheitstechnologien nicht die Compliance gewährleisten können, spielen sie doch eine wichtige unterstützende Rolle für Unternehmen, ihre Datenschutzziele zu erreichen.

Was es ist und was es nicht ist …

Trotz der großen Anzahl von Dokumenten, Anleitungen und anderen Veröffentlichungen, die auf die Ankündigung der DSGVO folgten, bleibt das grundlegende Verständnis vieler Aspekte der DSGVO vage. Einige Führungskräfte glauben weiterhin, die Rechtsvorschriften würden auf sie nicht zutreffen, weil sie „solche Daten gar nicht erheben". Andere glauben, es handle sich um einen einmaligen Vorgang, ein Kontrollkästchen anzuklicken und dann mit „Business as usual" weiterzumachen.

Leider liegen beide falsch:

- Sie haben Angestellte? Die Informationen, die Sie in der Regel über diese Personen sammeln und verarbeiten, sind personenbezogene Daten und fallen unter die DSGVO. Jedes Unternehmen, das personenbezogene Daten erhebt, verarbeitet und/oder speichert, auch Daten von Mitarbeitern, die sich auf eine Transaktion oder Aktivität in der EU beziehen, oder Daten von externen Mitarbeitern, ist verpflichtet, diese zu schützen.

- Die DSGVO hat weniger vorschreibenden als rahmengebenden Charakter. Sie liefert keine Liste von Aufgaben, die abgehakt werden können, um hinsichtlich Datenschutz alles richtig gemacht zu haben.

Obgleich die DSGVO Regeln beinhaltet, die einzuhalten sind, geht sie wenig detailliert auf die Besonderheiten ein, wie man diese erfüllt: Was die Methodik betrifft, muss jedes Unternehmen weitgehend eigene Entscheidungen treffen. Der springende Punkt ist, dass es sich beim Datenschutz um einen Prozess handelt und Unternehmen deshalb kontinuierlich an ihm arbeiten müssten.

Es gibt keinen einheitlichen Ansatz für die Messung der Compliance. Das Anklicken von Kontrollkästchen hilft Ihnen nur begrenzt. Die Umstände (und die damit verbundenen Risiken) ändern sich, und Listen sind selten vollständig, d. h. bei einem Ansatz mit Einheitsgröße können Schwachpunkte übersehen werden.

Letztlich ist es das, was Ihr Unternehmen zur Prävention von Verstößen tut, zusammen mit der Strategie für frühzeitige Erkennung und Verfolgung, was Sie wirklich in Richtung einer DSGVO-Konformität bringt.

Die Next Generation Kaspersky-Technologien und -Lösungen können Ihrem Unternehmen helfen, seine Ziele hinsichtlich Cybersicherheit als Teil der Gesamtstrategie in Sachen DSGVO-Konformität zu erreichen.

Sehen wir uns einmal näher an, was dies aus praktischer Perspektive bedeutet.

2 Kaspersky Lab: Bericht zu globalen IT-Risiken 2017

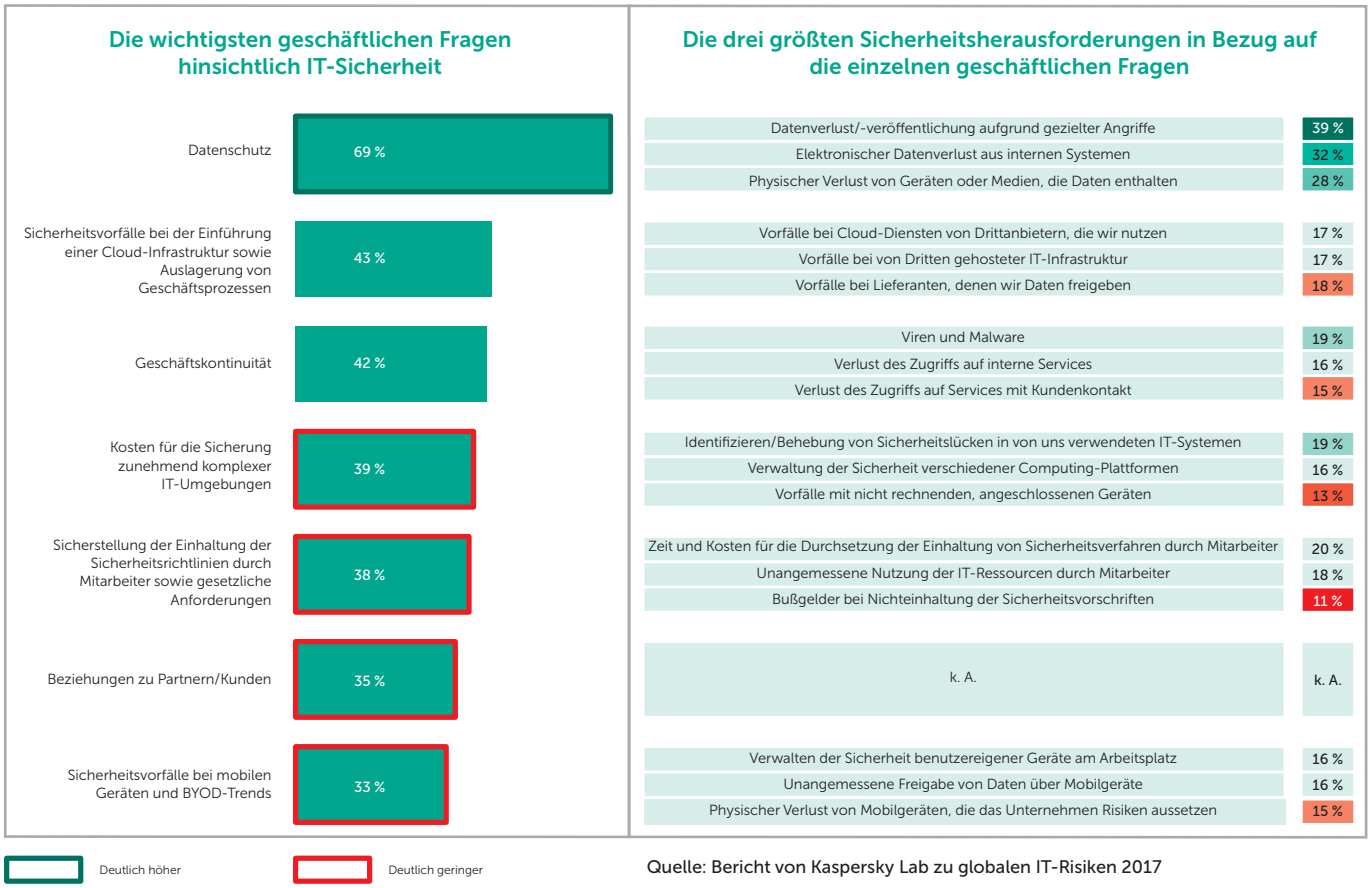
3 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

Vorbeugung ist die beste Medizin

Menschliches Handeln, ob versehentlich oder vorsätzlich, spielt bei Datenschutzverletzungen eine bedeutende Rolle. Die häufigste Ursache von Sicherheitsverstößen hinsichtlich PII-Daten (identifizierbare personenbezogene Daten) sind weiterhin Cyberangriffe, die nicht nur im Volumen anwachsen, sondern sich auch ständig verändern. Das ist der Grund, warum Cybersicherheit im Datenschutz und in der Strategie zur Vermeidung von Sicherheitsverstößen eine so grundlegende Rolle spielt.

69 % der IT-Fachleute meinen, Datenschutz sei ihre größte Sorge, während 38 % angeben, eine Herausforderung sei es, sicherzustellen, dass das Personal die Sicherheitsrichtlinien und -vorschriften einhält.

Die wichtigsten IT-Fragen



Quelle: Bericht von Kaspersky Lab zu globalen IT-Risiken 2017

Sicherheit der Verarbeitung – Artikel 32 der DSGVO

Artikel 32 der DSGVO fordert geeignete technische und organisatorische Maßnahmen, um ein angemessenes Sicherheitsniveau zu gewährleisten, das dem Risiko der Kontrolle oder Verarbeitung personenbezogener Daten entspricht. Dazu zählen:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Maßnahmen zur Unterstützung der dauerhaften Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Verarbeitungssysteme und Services
- Kapazität zur Wiederherstellung der Verfügbarkeit und Zugänglichkeit nach einem Ereignis
- Fähigkeit, wiederkehrende Prüfungen und Bewertungen der technischen und organisatorischen Kapazitäten zur Datensicherung und -verarbeitung durchzuführen

Die Cybersicherheit spielt eine Rolle sowohl für den Datenschutz als auch für die Sicherstellung der Ausfallsicherheit.

Bedenkt man, dass im Jahr 2017 24 % der Unternehmen einen Verlust, ein Leck oder eine Offenlegung von Daten als Folge eines Malwareangriffs gemeldet haben [4], sieht man leicht, warum eine effektive Cybersicherheitsstrategie eine wichtige unterstützende Rolle bei der DSGVO-Konformität und Gesamt-Risikominderung spielt.

Und einer der besten Orte, um mit der Härtung der Unternehmens-IT zu beginnen, ist der Endpoint. Wir erklären Ihnen, warum.

4 Bericht von Kaspersky Lab zu globalen IT-Risiken 2017

Beginnen wir am Ende – dem Endpoint

Wenn es um die Verbesserung der allgemeinen IT-Sicherheit und der Datenschutzstrategie geht, ist der Schutz des Endpoints der beste Anfang. Dieser Bereich der Unternehmensverteidigung kann noch heute verbessert werden, ohne Beeinträchtigung von Prozessen und unabhängig von anderen, neuen Prozessen.

- Endpoints bleiben die Nummer eins für die Mehrheit der heutigen Cyberangriffe, und E-Mails sind der Malware-Vektor Nummer eins für Unternehmen[5].
- Sie können zu einem „Fenster" für die vertraulichen Daten Ihrer Unternehmensprozesse werden, selbst wenn sich die Daten selbst auf einem entfernten Server befinden.
- Als wichtigster Baustein für Ihr IT-Netzwerk müssen Endpoints am selben Ort überwacht werden, um rechtzeitige Alarme bei verdächtigen Aktivitäten sicherzustellen. Selbst Aktivitäten, die nicht direkt an der Verarbeitung personenbezogener Daten beteiligt sind, können eine erhebliche Gefahr darstellen, wenn sie mit demselben Netzwerk verbunden sind, da Malware sich ausbreiten und die gesamte Datenverarbeitungsinfrastruktur beeinträchtigen kann.

49 % der Unternehmen haben 2017 einen Malwareangriff erlebt, ein Anstieg von 11 % gegenüber dem Vorjahr.[6]

In einer solchen Umgebung sind die Erkennungsraten entscheidend. Bei mehr als 300 000 neu erfassten Malware-Varianten täglich können sogar 0,9 Prozent Unterschied in der Fähigkeit zur Bedrohungserkennung Hunderttausende erkannte Malware-Teile im Laufe eines Jahres bedeuten. Und weil die fortschrittlichste Malware in der Regel in die letzten 1-2 % der Angriffe fällt, kann dieser zusätzliche Tropfen den Unterschied zwischen der Bewältigung eines Cyberangriffs und eine Betriebsunterbrechung ausmachen, gerade bei kleineren Unternehmen.

Die effektivsten Endpoint-Erkennungslösungen machen nicht an einer einzelnen Schicht der Prävention und Erkennung halt; sie benutzen mehrere Schichten von Next Generation-Technologien, die in der Lage sind, selbst raffinierteste unbekannte Bedrohungen zu erkennen und zu blockieren und den Schaden zu begrenzen.

65 % der Unternehmen, die 2017 von Ransomware betroffen waren, verloren den Zugriff auf einen Großteil ihrer Daten. Ein Drittel von ihnen sah die Daten nie wieder.[8]

Kaspersky Endpoint Security for Business verbindet weltweit vielfach getestete und ausgezeichnete Sicherheit[7] mit mehreren Ebenen von Next Generation-Sicherheitstechnologien zum Schutz von Unternehmens-Endpoints vor Bedrohungen jeder Art. Unsere Verhaltens-Engine bedient sich einer einzigartigen, dynamischen intelligenten Technologie und Cloud-basierter Bedrohungserkennung zur Minderung von bekannten, unbekannten und fortgeschrittenen Bedrohungen wie auch neu aufkommender Angriffe wie Ransomware, die eine direkte Bedrohung der Integrität und Verfügbarkeit personenbezogener Daten darstellen.

Blockieren, bevor sie geladen werden

52 % der Unternehmen geben an, dass die Unachtsamkeit der Endbenutzer die größte Schwäche in ihrer IT-Sicherheitsstrategie darstellt.[9]

Einen Angriff zu verhindern, bevor er Schaden anrichten kann, ist ein wichtiger Aspekt der Systemhärtung und -belastbarkeit. In dieser Hinsicht können das Erkennen und Schließen von Sicherheitslücken und Schwachstellen wichtiger Softwareprogramme Cyberkriminelle daran hindern, verbreitete Unternehmenssoftware unbefugt zu nutzen und so auf personenbezogene Daten zuzugreifen und sie zu stehlen.

Warum ist das wichtig? Denken Sie darüber nach: Phishing-Angriffe, Ransomware, schädliche Anhänge und Spyware sind nur einige Beispiele für Cyberangriffe mit Datendiebstahl, die darauf beruhen, dass der Endbenutzer ohne Nachdenken darauf klickt. Es braucht nur eine gut getarnte E-Mail mit einem überzeugenden Anhang, um eine ernste Datenschutzverletzung zu verursachen.

Die **hostbasierte Angriffsüberwachung** (HIPS) von Kaspersky Endpoint Security for Business bietet eine weitere Schicht an Stabilität. Sie erkennt und blockiert unerwünschte oder schädliche Programmaktivitäten in Echtzeit und ohne Auswirkungen auf die Leistung der legitimen Programme. Auf Grundlage der

5 Verizon Data Breach Investigation Report 2017
6 Bericht von Kaspersky Lab zu globalen IT-Risiken 2017
7 https://www.kaspersky.com/top3
8 Kaspersky Security Bulletin: Geschichte des Jahres 2017
9 Bericht von Kaspersky Lab zu globalen IT-Risiken 2017

neuesten Cloud-basierten Bedrohungsinformationen werden die Programme einer von vier Vertrauenskategorien zugeordnet, die die Art des Zugriffs auf sensible Systemelemente regeln. Im Hinblick auf die DSGVO kann dies zusätzliche Sicherheit bieten, indem der Zugriff auf ausgewählte Dateien/Verzeichnisse für Programme mit niedriger Vertrauensstufe eingeschränkt wird.

Das **Vulnerability und Patch Management** von Kaspersky Lab (in Kaspersky Endpoint Security for Business – Advanced enthalten) ergänzt Ihre Verteidigung um eine zusätzliche Sicherheitsschicht. Diese Lösung erkennt und patcht anfällige Programme, bevor deren Sicherheitslücken ausgenutzt werden können. Da sie eine Automatisierung ermöglicht, können IT-Teams von der operativen Belastung der rechtzeitigen Implementierung von Patches befreit werden; Planungsfunktionen ermöglichen es, weniger dringende Patches außerhalb der Betriebszeiten zu legen, was die Infrastruktur entlastet.

Um einen echten mehrstufigen Schutz zu erzielen, kann die Endpoint-basierte **Exploit Prevention**-Technologie sogar bisher unbekannte Zero-Day-Exploits verhindern, da sie auf der Verhaltens-Engine aufbaut und so ein äußerst breites Spektrum von Exploit-Typen abdeckt.

Nicht sammeln, wenn Sie nicht schützen können: Speicher

Endpoints befinden sich dort, wo personenbezogene Daten und Menschen aufeinandertreffen. Die Risiken, die dadurch entstehen, müssen verringert werden. Aber auch nach einer Eingrenzung der Anzahl der Mitarbeiter, die mit der Verarbeitung von PII-Daten betraut sind (entsprechend DSGVO-konformen Prozessen), bestehen immer noch Risiken im Zusammenhang mit der Frage, wo und wie die Daten gespeichert werden. Um die Sicherheit und Transparenz zu erhöhen, werden regulierte Speichervorrichtungen (wie Dateiserver oder ein angeschlossenes Speichermedium) zugewiesen, die strengen Zugriffsichtlinien und kontinuierlicher Überwachung unterliegen. Leider macht sie diese hochsensible Rolle zu lukrativen Zielen für Datendiebe, was die Notwendigkeit für hohe Sicherheit unterstreicht.

Kaspersky Security for File Server (verfügbar als Teil von Kaspersky Endpoint Security und Kaspersky Total Security for Business) und **Kaspersky Security for Storage** können umfassenden Schutz für die regulierte Datenspeicherung zur Verfügung stellen. Neben leistungsstarkem mehrstufigem Schutz sind diese Lösungen speziell für Server- und Speicheranforderungen ausgelegt, um die geringstmögliche Auswirkungen auf die Leistung oder Stabilität zu erreichen, unabhängig von der Auslastung. Sie umfassen auch einen einzigartigen Anti-Verschlüsselungsmechanismus[10], der die Auswirkungen von aus der Ferne gestarteter Ransomware blockiert. Solche Ransomware kann erhebliche, dauerhafte Schäden verursachen, wenn sie auf einem Computer gestartet wird, der Netzwerkzugriff auf PII-Daten verarbeitende Server oder Speicher hat.

Überwachung der Engpässe

E-Mail- und Proxy-Server sind die zwei Gateways, über die Cyberangriffe in das Unternehmens-IT-Netzwerk eindringen oder über die personenbezogene Daten das Netzwerk verlassen können. Auch versehentlich durch menschliche Fehler versendete Daten gelten als Verstoß gegen die Datensicherheit. Diese zwei Engpässe im Sicherheitsbereich des Unternehmens zu überwachen, ist entscheidend.

Kaspersky Security for Mail Server und Kaspersky Security for Internet-Gateways[11] können helfen, diese Risiken erheblich zu senken, indem sie bis zu 95 % der eingehenden Bedrohungen abwehren, bevor diese den Endpoint erreichen. So lassen sich der menschliche Faktor sowie auf Endpoints abzielende Angriffe verhindern. Darüber hinaus kann das Risiko, dass personenbezogene Daten in die Systeme eindringen oder diese verlassen, verringert werden, indem bestimmte Dateitypen am Eindringen oder Verlassen gehindert werden.

10 Kaspersky Security for Storage unterstützt Anti-Verschlüsselungsfunktionalität nur für angeschlossene NetApp-Speicher.

11 Auch als Teil von Kaspersky Total Security for Business verfügbar

- 18 % der Unternehmen haben Datenverlust aufgrund des physischen Verlusts von Geräten oder Wechselmedien erlebt.
- 16 % haben Datenveröffentlichungen durch den physischen Verlust von mobilen Geräten erfahren.
- 15 % der Unternehmen haben eine unerwünschte Veröffentlichung von Daten über mobile Geräte erlebt.[12]

Mobile Geräte sind bewegliche Ziele

Dank ihrer Eignung für die Speicherung, Übertragung und gemeinsame Nutzung von Daten spielen mobile Geräte schon lange eine wichtige Rolle bei der Verarbeitung personenbezogener Daten. Und genau wie bei anderen Technologien sollte besondere Aufmerksamkeit darauf gerichtet werden, diese zu sichern.

Kaspersky Security for Mobile ist ein integraler Bestandteil von Kaspersky Endpoint Security for Business, indem es wirksamen Schutz vor Bedrohungen mit Datensicherungsmaßnahmen wie Verschlüsselung und Trennung von Geschäftsdaten kombiniert – neben Tools für Remote-Management. All dies schafft eine solide Basis für die sichere Verwendung mobiler Geräte, auch solcher, die Teil der PII-Verarbeitungskette sind.

Vorteile für jede Cloud

43 % der Unternehmen geben Sicherheitsvorfälle im Zusammenhang mit der Cloud-Infrastruktur als eines der größten IT-Sicherheitsprobleme an.[13] Kaspersky Hybrid Cloud Security erleichtert die Sicherung datenverarbeitender, auch PII-Daten verarbeitender Arbeitslasten, unabhängig vom physischen/virtuellen Status oder Standort (lokal/Cloud). Es bietet die gleiche umfassende Sicherheit für virtualisierungsfähige Infrastruktur, Server und virtuelle Desktops. Die meisten Sicherheitsebenen in Programmen für physische Arbeitslasten sind auch in Formaten erhältlich, die speziell für virtuelle Systeme entwickelt wurden.

Schulung: Gefahr erkannt, Gefahr gebannt

Die DSGVO fordert die Förderung einer Sensibilisierung für Datenschutz und Datensicherheit unter den Mitarbeitern, die gegebenenfalls auch Schulungen beinhalten kann. Während prozessbezogene Aspekte der Datenverarbeitung wie z. B. Verhältnismäßigkeit, Zweck oder integrierter Datenschutz („Privacy by Design“) für die meisten Unternehmen die Grundpfeiler der DSGVO-Konformität bilden, spielt ein größeres Bewusstsein für Cybersicherheit, E-Mail- und andere Online-Bedrohungen für die Sicherheit der Daten eine wichtige Rolle.

Das Kaspersky Security Awareness Training unterstützt diese Förderung und Sensibilisierung für die Best Practices im Datenschutz am Arbeitsplatz mithilfe von spielerischen Szenarien, die die Sensibilisierung für bzw. Prävention von Cyberbedrohungen erleichtern. Dadurch, dass Datenschutzrisiken aufgrund menschlicher Fehler reduziert werden, können Unternehmen ihre Compliance über Kontrollkästchen hinaus erhöhen und die Sensibilisierung sowie sicherere Praktiken insgesamt fördern.[14]

Die Risiken verstehen

Artikel 35 der Verordnung enthält Maßnahmen, die ergriffen werden können, um Risiken zu mindern. Dazu gehören u. a. „Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt” wird.

Aus Perspektive der Cybersicherheit kann dazu die Bewertung von datenverarbeitender Software hinsichtlich Sicherheitslücken oder Risiken im Zusammenhang mit der Art ihrer Implementierung gehören. In Fällen, wo die Verarbeitung personenbezogener Daten einen unternehmenskritischen Bestandteil der Geschäftsprozesse darstellt, bietet die Betrachtung der IT-Gesamtinfrastruktur als „eine personenbezogene Daten verarbeitende Einrichtung“ einen hilfreichen Ansatz für eine erfolgreiche Risikobewertung. Die Expertenkenntnisse in der Cybersicherheit, die für diese Aufgabe erforderlich sind, stehen selten intern zur Verfügung, was bedeutet, dass viele Unternehmen mit spezialisierten externen Cybersicherheitsexperten zusammenarbeiten, um dieses Ziel zu erreichen.

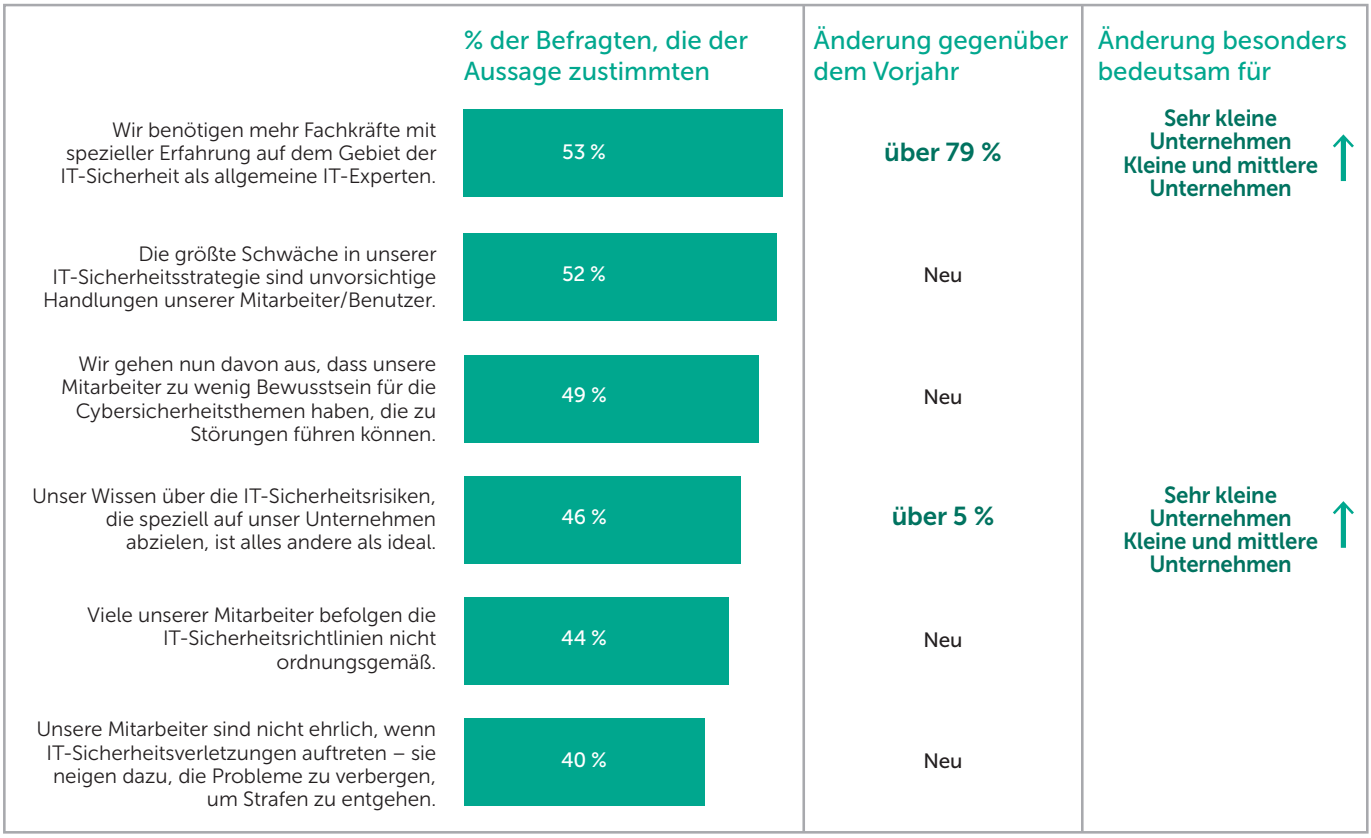
12 Bericht von Kaspersky Lab zu globalen IT-Risiken 2017

13 Bericht von Kaspersky Lab zu globalen IT-Risiken 2017

14 Das Angebot von Kaspersky Lab ergänzt prozessbezogene Schulungen, statt sie zu ersetzen.

Zu viel für den Augenblick?! Ein Grund mehr für Sicherheitsschulungen

Über die Hälfte der Unternehmen stimmt der Aussage zu, dass Handlungen von unvorsichtigem Personal ihre größte Schwäche in der IT-Sicherheit darstellen; die Aufklärung der Mitarbeiter über die vorhandenen Gefahren und wie man sich vor ihnen schützt, ist daher offensichtlich unbedingt erforderlich!



Dies gilt insbesondere für größere Unternehmen, die diesen Aussagen deutlich häufiger zustimmten.

Kaspersky Security Assessment Services können durch Application Security Assessment helfen, indem überprüft wird, ob die zur Datenverarbeitung eingesetzte Software für Missbrauch und Exploits anfällig ist. Kaspersky-Experten können auch **Penetrationstests** durchführen, um die Schwächen Ihres IT-Netzwerks zu ermitteln und die nötige Beratung zu deren Behebung zu bieten. Dies hilft sicherzustellen, dass Systeme und Prozesse für bessere Sicherheit optimiert sind, und trägt zu einer soliden Datenschutz-Folgenabschätzung bei.

Cybersicherheit kann die Einhaltung der DSGVO unterstützen

Im Kern verfolgt die DSGVO den Zweck, vor dem Hintergrund einer technologiebedingt gewandelten Art der Sammlung, gemeinsamen Nutzung und Speicherung personenbezogener Daten den Datenschutz zu sichern und zu ermöglichen.

Während die Verordnung selbst erst seit dem 25. Mai 2018 gilt, hat die lange Vorlaufzeit den Unternehmen Zeit gegeben, ihre Verfahren der Datenverarbeitung zu untersuchen und Änderungen entsprechend den verwendeten Technologien und gesammelten und verwalteten Arten von Daten umzusetzen.

Für die meisten Unternehmen bietet die DSGVO eine Gelegenheit, ihre Art der Datenverarbeitung und im weiteren Sinne die Cybersicherheit zu prüfen und zu verbessern. Das an sich ist eine gute Nachricht für Cybersicherheitsexperten, die lange darüber geklagt haben, wie sorglos sich Unternehmen hinsichtlich ihrer Schutzfunktionen und Prozesse zum Sichern ihrer Daten und Systeme verhalten. Die DSGVO bietet Unternehmen eine große Chance, ihre Haltung zur Cybersicherheit aus Perspektive der Datensicherheit zu überprüfen. Denn was für die Sicherheit der personenbezogenen Daten gut ist, kann schließlich auch für die Sicherheit vieler anderer geschäftlicher Aspekte Ihres Unternehmens sinnvoll sein. Das Kaspersky-Portfolio an Lösungen gewährleistet zwar als solches nicht die Einhaltung der DSGVO, kann aber durchaus die PII-Datenverarbeitungsrisiken Ihres Unternehmens sowie auch all die anderen bestehenden Cyberbedrohungen verringern.

Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de