Umfassender Leitfaden zur DSGVO-Konformität

Präsentiert von

Inhalt

Einführung

Es ist an der Zeit für integrierten Datenschutz

Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung der EU in Kraft. Sie ersetzt alle nationalen Datenschutzbestimmungen innerhalb der EU. Jeder, der mit Kunden im Binnenmarkt Geschäfte betreibt, muss sich daran halten. Dies betrifft auch Unternehmen, die nicht in der EU angesiedelt sind, aber mit EU-Kunden Geschäfte machen.

Gemäß DSGVO muss jeder Diebstahl persönlicher Daten binnen 72 Stunden nach Bekanntwerden gemeldet werden. Nichtbeachtung oder grobe Fahrlässigkeit können Geldstrafen in Höhe von bis zu 20 Millionen Euro oder vier Prozent des Gesamtumsatzes nach sich ziehen, je nachdem, welche Zahl höher ausfällt.

Glücklicherweise schützen die Maßnahmen, die zum Schutz der Unternehmensdaten erforderlich sind, auch die Kundendaten. Die mehrstufige Herangehensweise an die Endpunktsicherheit, die wir bei HP bereits jetzt empfehlen, sorgt auch für Konformität mit der DSGVO.

Dieser E-Guide untersucht die wichtigsten Punkte der DSGVO, die IT-Spezialisten kennen müssen, und beschreibt, wie ein geräteorientiertes Programm zur Endpunktsicherheit zur Konformität beitragen kann.

Die EU-DSGVO erklärt

Die wichtigsten Punkte für die IT

Die DSGVO umfasst im Wesentlichen zwei Punkte: den Schutz der Rechte und Privatsphäre von Betroffenen in der EU. Beides hat technologische Auswirkungen.

Die maßgeblichen Details finden Sie auf der Webseite EUR-Lex. Für Entscheidungsträger in der IT sind folgende Punkte wesentlich:

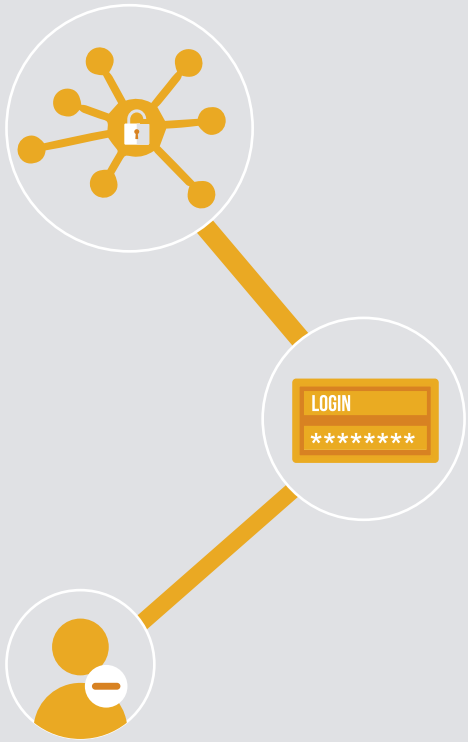
1. **Verstöße müssen binnen 72 Stunden gemeldet werden**
   Sollte eine Datenschutzverletzung auftreten, muss diese innerhalb von 72 Stunden gemeldet werden. Zuwiderhandlung zieht empfindliche Strafen nach sich (siehe Seite 5: „Welche Strafen drohen bei Nichtbeachtung?“)

2. **Das Recht auf Vergessenwerden**
   Jeder Betroffene in der EU hat das Recht, vergessen zu werden. Auf Anforderung müssen alle Daten einschließlich aller Kopien gelöscht werden.

3. **Das Recht auf Datenübertragbarkeit**
   Einwohner der EU haben das Recht darauf, Ihre eigenen Daten zu kontrollieren. Auf Anfrage müssen ihre Daten in einem zugänglichen Format bereitgestellt werden können, welches der Nutzer an eine Drittpartei weiterleiten darf.

4. **Internationale Übertragungen**
   Die Übertragung persönlicher Daten (z. B. außerhalb der EU) darf nur mit ausdrücklicher Genehmigung und nur an „zuständige“ Behörden oder an Stellen erfolgen, die zusätzliche Sicherheitsmaßnahmen implementiert haben[1]

5. **Integrierter Datenschutz**
   Unternehmen müssen einen Ansatz zum Datenschutz von Grund auf umsetzen, der standardmäßig Datensicherheit in Produkten, Abläufen und Diensten umfasst[2,3]



Für wen gilt die DSGVO?

Die DSGVO gilt für alle Unternehmen, die Daten von EU-Bürgern erfassen und/oder verarbeiten. Dies betrifft auch Unternehmen außerhalb der EU, die in der EU tätig sind.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Allen & Overy – The EU General Data Protection Regulation 2016
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

Die EU-DSGVO erklärt

Was fällt unter „persönliche Daten“?

Laut DSGVO umfassen persönliche Daten „alle Daten, die zur Identifizierung eines Individuums verwendet werden können“.

Dies umfasst genetische, psychische, kulturelle, wirtschaftliche oder soziale Informationen sowie traditionell als identifizierende Daten betrachtete Informationen.

Somit fallen auch Unternehmen unter die Bestimmungen der DSGVO, die bislang nicht von geltenden Datenschutzbestimmungen betroffen waren.

Welche Strafen drohen bei Nichtbeachtung?

Die Höchststrafe beträgt bis zu 20 Millionen Euro oder vier Prozent des Gesamtumsatzes, je nachdem, welche Zahl höher ausfällt. Dies gilt für die schwersten Zuwiderhandlungen, wie z. B. der Nichtbeachtung der Meldepflicht binnen 72 Stunden nach Bekanntwerden eines Datendiebstahls.

Weniger schwere Vergehen werden mit einer Höchststrafe von bis zu 10 Millionen Euro oder zwei Prozent des Gesamtumsatzes bestraft. Es versteht sich von selbst, dass die Kosten bei Nichtbeachtung erheblich sind.

DSGVO-Maßnahmen-Prüfliste

Ihre Data-Governance-Richtlinie muss über folgende explizite Vorgehensweisen verfügen:

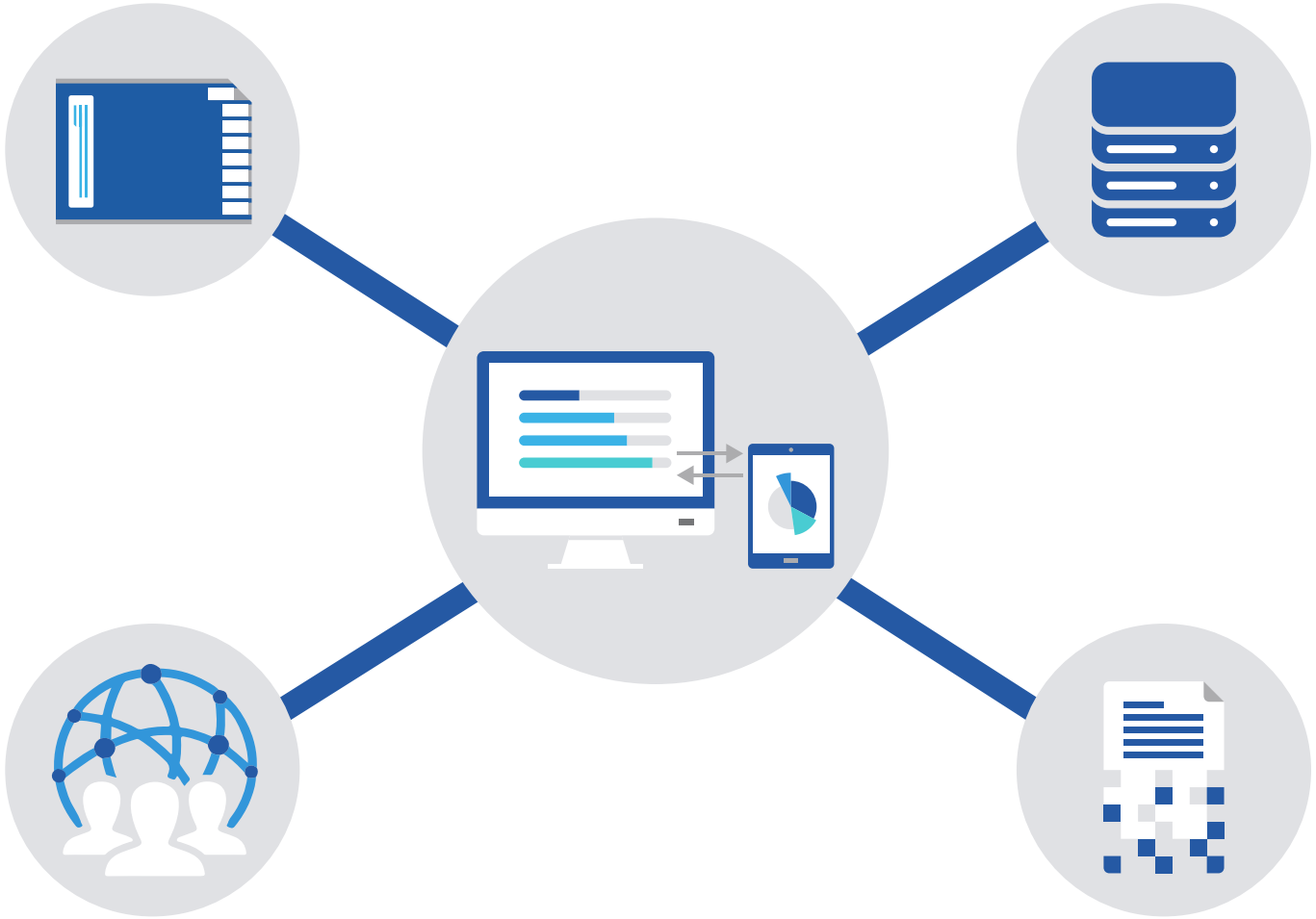
- Aufklärung der Betroffenen über die Erfassung, Speicherung und Verarbeitung ihrer Daten
- Einholung der ausdrücklichen Einverständniserklärung des Betroffenen zur Verwendung der Daten
- Bereitstellung der Informationen in einem für den Betroffenen zugänglichen Format
- Löschung aller persönlicher Daten des Betroffenen, einschließlich aller Kopien
- Übertragung der Daten an einen anderen Datenverantwortlichen oder -verarbeiter
- Übertragung der Daten außerhalb der EU – auch innerhalb des Unternehmens

Technische Herausforderungen der Konformität

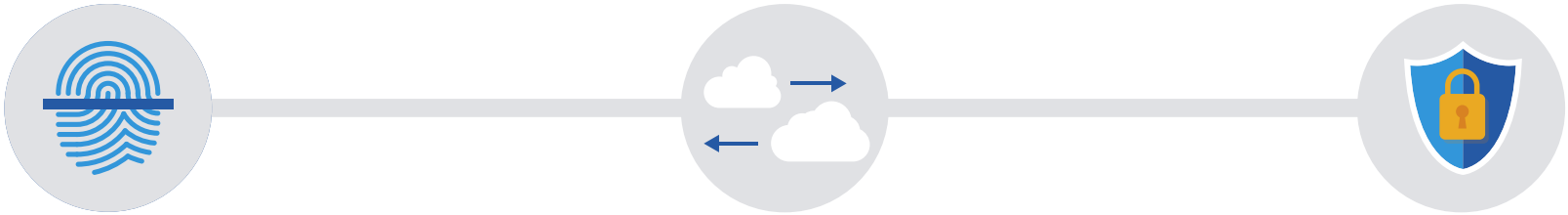
Die größten Herausforderungen der DSGVO sind technischer Natur.

Die Umsetzung einer sicheren Datenübertragbarkeit, der Schutz der Personendaten des Individuums sowie dessen Recht auf Vergessenwerden erfordern eine umfassende Datenkartierung und Zugriff bis hinunter auf Geräteebene.

Da die Bedrohung durch Cyberkriminalität Jahr für Jahr zunimmt, ist die Gewährleistung absoluter Sicherheit eine wachsende Herausforderung.



Technische Herausforderungen der Konformität



Überwachung von Geräten

Die Konformität in Bezug auf Datenübertragbarkeit und dem Recht auf Vergessenwerden erfordern eine detaillierte Aufzeichnung aller Personendaten, die das Unternehmen speichert.

Sie müssen Folgendes im Blick behalten:

- Jedes Gerät, auf dem persönliche Daten gespeichert sind
- Jedes Gerät, das Zugriff auf persönliche Daten hat

Nur so kann garantiert werden, dass vom Unternehmen gespeicherte persönliche Daten aufgefunden und/oder gelöscht werden können.

Überwachen von Clouds

Ein durchschnittliches europäisches Unternehmen verwendet 608 Apps. Man geht aber davon aus, dass diese Zahl nur zehn Prozent der Gesamtnutzung darstellt. Angestellte nutzen häufig kommerzielle Cloud-Apps, ohne dass die IT-Abteilung Bescheid weiß.[4]

Für DSGVO-Konformität muss der Gebrauch von Cloud-Diensten auf Dienste mit folgenden Eigenschaften beschränkt sein:

- Dienste, die innerhalb der EU operieren und daher selbst die DSGVO beachten müssen
- Dienste, die unter das Datenschutzgesetz eines von der EU als „ausreichend" beurteilten Gesetzgebers fallen

Alles andere könnte die internationale Übertragungsrichtlinie verletzen. Zudem müssen Sie wissen, welche Cloud-Dienste Ihre Angestellten verwenden, falls das Recht auf Vergessenwerden in Anspruch genommen wird.

Verteidigung von Daten

Die Bedrohung durch Cyberkriminalität nimmt zu. Nicht zuletzt aufgrund unsicherer Netzwerke und der zunehmenden Verwendung persönlicher Geräte.

Angriffe sind nahezu unvermeidbar. Die EU weiß das. Um allerdings kostspielige Strafen zu vermeiden, müssen Sie:

- Ein Systems Incident Event Monitoring (SIEM)-Tool implementieren, um Datendiebstähle binnen 72 Stunden melden zu können
- Mehrstufige Endpunktsicherheit implementieren, um die Sorgfaltspflicht in der Vorbeugung von Datendiebstählen zu gewährleisten

Der Benutzer muss auf seine Verantwortung zur Nichtverwendung unbestätigter Geräte hingewiesen werden.

[4]https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

Bedrohung durch Cyberkriminalität

Cyberkriminalität ist eine reelle, präsente und wachsende Bedrohung

82%

der Unternehmen hatten in den vergangenen 12 Monaten mit einer Sicherheitsbedrohung/-lücke zu tun[5]

80%

der Experten meinen, dass Computerkriminalität in den nächsten drei Jahren zunehmen wird[6]

78%

der Unternehmen berichten eine Zunahme von Malware-Angriffen in den letzten fünf Jahren[7]

60%

der IT-Verantwortlichen sind der Meinung, dass ihre Verteidigungsmechanismen der Internetkriminalität nicht ausreichend gerecht werden[8]

81%

der Unternehmen betrachten Nachlässigkeiten der Beschäftigten als größte Bedrohung für Computersicherheit[9]

81%

der IT-Verantwortlichen sagen, dass mobile Geräte in ihrem Netzwerk bereits das Ziel von Malware waren[9]

72%

der IT-Verantwortlichen sagen, dass der Gebrauch kommerzieller Software im Unternehmen ein Sicherheitsrisiko darstellt[9]

69%

der IT-Verantwortlichen sagen, BYOD sei ein Sicherheitsrisiko

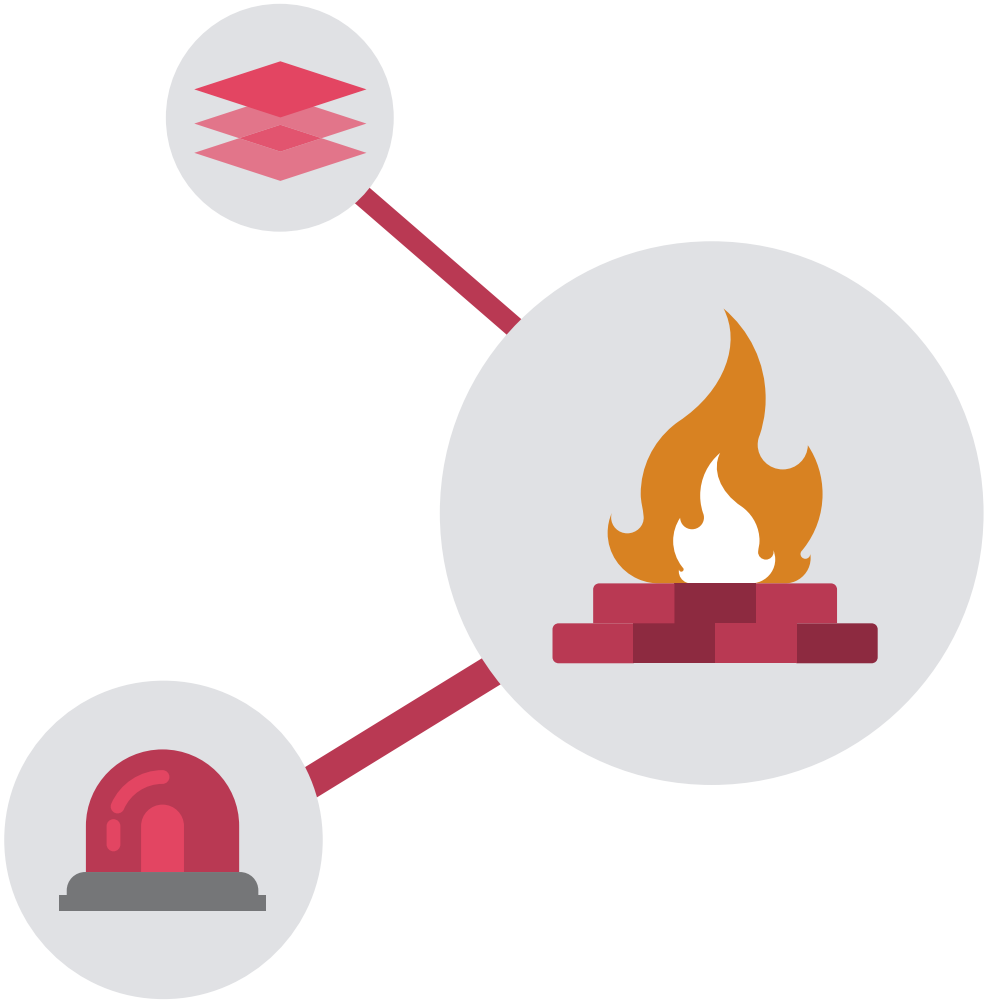
[5]HPI Printer Security Research 2016 (Spiceworks) [6]HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8]IBM CISO Assessment 2014 [9]Ponemon 2016 State of the Endpoint Report

Endpunktsicherheit implementieren

HPs mehrstufiger Ansatz zur Endpunktsicherheit

Der obstruktive und protektive Ansatz in der Cybersicherheit – Firewall und Antivirus – ist nicht genug. Und ist es nie gewesen. Eine Studie von Damballa hat gezeigt, dass eine Antivirensoftware sechs Monate brauchte, um 100 Prozent aller bösartigen Dateien zu erkennen, die ihr serviert wurden.[10]

HP ist der Ansicht, dass Sicherheit mehrstufig sein muss und auf Netzwerk-, Geräte- und Benutzerebene mit jeweiligen Verteidigungsoptionen operieren sollte. Erkennung und Reaktion müssen wichtiger sein als Schutz und Verteidigung. Und an den Endpunkten wird begonnen: nämlich beim Gerät und Nutzer.



Kritische Sicherheitskontrollen (CSC)

Das Zentrum für Internet-Sicherheit (Center for Internet Security, CIS) hat 20 international wesentliche Sicherheitskontrollen (Critical Security Controls, CSC) definiert. Diese gelten als wichtige Maßnahmen für die Cyber-Hygiene in jedem Unternehmen.

Wir haben die wichtigsten CSC für die DSGVO-Konformität aufgegriffen. Den Volltext finden Sie auch online als kostenlosen Download in der CIS Library.

[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Netzwerksicherheit

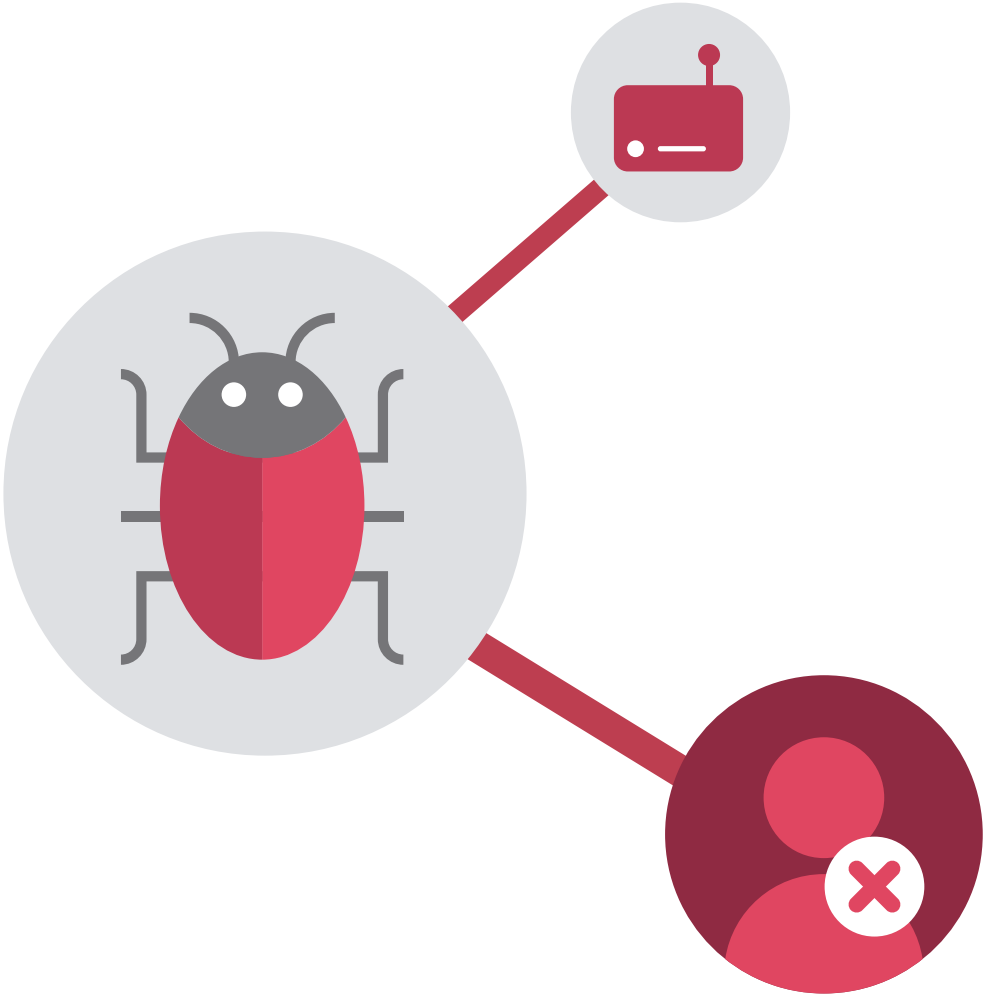
Schwerwiegende Angriffe nutzen in der Regel einen einzigen Eintrittspunkt, um Zugang zum gesamten Netzwerk zu erhalten. Sicherheit auf Netzwerkebene sollte daher darauf aufbauen, dies zu verhindern.

- **Administrative Privilegien kontrollieren (CSC 5)**
  Beschränken Sie die Fähigkeit, Netzwerkseinstellungen und Passwörter zu verändern auf so wenige Personen, wie nötig
- **Kontrollieren Sie den Datenzugriff nach dem Need-to-know-Prinzip (CSC 14)**
  Strukturieren Sie die Zugangskontrollen je nach Benutzer, Gerät und Standort. Wägen Sie Risiken und die Sensibilität der Daten gegeneinander ab
- **Beschränkung und Kontrolle von Netzwerkports, Protokollen und Diensten (CSC 9)**
  Schließen Sie jegliche unnötigen Zugriffspunkte – virtuell und physisch – einschließlich FTP, Telnet und Druckdienste.
- **Instandhaltung, Überwachung und Analyse von Auditprotokollen (CSC 6)**
  Prüfen Sie regelmäßig Auditprotokolle, um das Systemverhalten zu analysieren und auf ungewöhnliches Verhalten reagieren zu können
- **Kontinuierliche Anfälligkeitsbewertung und Wiederherstellung (CSC 4)**
  Untersuchen Sie die Umgebung kontinuierlich auf Anfälligkeiten und treffen Sie Maßnahmen, um die Sicherheit wiederherzustellen. Das minimiert die Wahrscheinlichkeit eines Angriffs.

Das Ziel ist ein je nach Sensibilität der Daten strukturiertes Netzwerk. Zugriffsversuche werden auf Sicherheitsrisiken überprüft. Nicht erkannte Geräte, Benutzer und Anfragen aus unsicheren Quellen werden vom Zugriff auf sensible Informationen ausgeschlossen. Die BeyondCorp-Policy von Google ist ein gutes Modell.[11]

[11] https://research.google.com/pubs/pub43231.html

Netzwerksicherheit



Jedes Gerät, ob geschäftlich oder privat, stellt ein potentielles Sicherheitsrisiko dar. Alle Telefone, Tablets, Notebooks und Desktops, welche Zugriff auf Unternehmensdaten haben, müssen bekannt sein..

- **Inventur autorisierter und nicht autorisierter Geräte (CSC 1)**
  Überprüfen Sie jedes Gerät, das Zugriff auf Daten hat
- **Inventur autorisierter und nicht autorisierter Software (CSC 2)**
  Überprüfen Sie jede im Netzwerk verwendete Anwendung – ob sie direkten Zugriff auf Daten hat oder nicht
- **Abwehr von Malware (CSC 8)**
  Stellen Sie sicher, dass jedes verwendete Gerät über aktuellen Antiviren- und Malwareschutz verfügt. Sorgen Sie für regelmäßige Scans und Updates

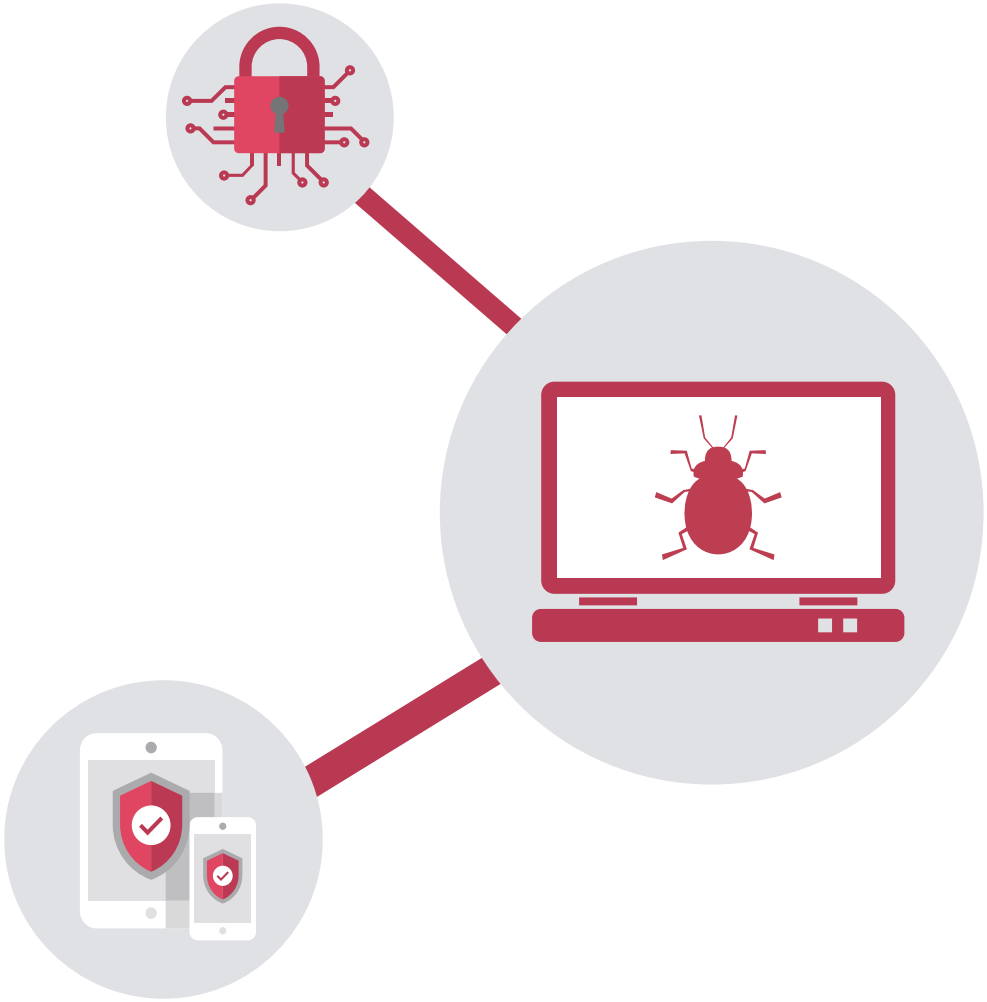
Gerätesicherheit

Außerdem sollte die IT-Abteilung zusätzlich folgende Schritte prüfen:

- **Mehrstufige Authentifizierung**
  Sorgen Sie dafür, dass jedes Arbeitsgerät sicher ist. Nutzen Sie im Idealfall biometrische Authentifizierung in Verbindung mit Passwörtern (siehe Seite 14: „Von Grund auf sichere Geräte“)
- **Remote-Zugriff**
  Sorgen Sie für Remote-Zugriff zum Abruf und Löschen persönlicher Daten, zur Quarantäne und Beendigung von Prozessen sowie zum Blockieren und Abschalten von Geräten im Falle von Verlust oder Diebstahl (siehe Seite 14: „Erkennen und reagieren“)
- **Informieren Sie jeden Angestellten über Sicherheitsprotokolle und -prozeduren**
  Stellen Sie sicher, dass jeder Angestellte sich seiner Verantwortung hinsichtlich Computersicherheit bewusst ist, einschließlich der Meldung verdächtiger Aktivitäten
- **Führen Sie aktiv Schulungen zur Computersicherheit durch**
  Halten Sie Workshops und Seminare ab, besprechen Sie Phishing-Angriffe – stellen Sie sicher, dass jeder weiß, wie man grundlegende Fehler vermeidet und die DSGVO-Konformität wahrt
- **Beschränken Sie den Gebrauch persönlicher Apps und Geräte auf ein Minimum**
  Unterbinden Sie die Verwendung persönlicher Apps und Geräte zu Arbeitszwecken. Eine umfängliche und flexible CYOD-Richtlinie sollte hilfreich sein

Die Implementierung einer solchen Sicherheitsrichtlinie erhält die Kontrolle über unternehmenseigene Geräte und hilft beim Schutz der Daten. Sie vereinfacht auch die Umsetzung der Datenübertragbarkeit und des Rechts auf Vergessenwerden.

Erfahren Sie mehr über HPs Ansatz zur mehrstufigen Sicherheit im Whitepaper Sicherheit beginnt am Endpunkt.



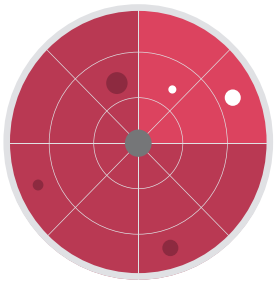
Warum jeder Mitarbeiter wachsam sein muss

58 Prozent der Cyberangriffe erfolgen durch Mitarbeiter, Ex-Mitarbeiter und vertrauenswürdige Partner. Die Sicherung jedes Geräts bedeutet auch die Sicherung jedes Benutzers.

- Das Democratic National Committee (DNC) der Vereinigten Staaten von Amerika wurde im Jahr 2016 gehackt indem John Podesta eine E-Mail öffnete, die ein Mitarbeiter fälschlicherweise als vertrauenswürdig einstufte[13]
- Nacktfotos von Prominenten verbreiteten sich im Jahr 2014 im Internet, nachdem sich der 36-jährige Ryan Collins, mithilfe von angeblich durch Apple versandte Phishing-Mails, Zugriff auf die iClouds von Jennifer Lawrence und anderen verschaffte[14]
- 68 Millionen Dropbox-Passwörter sind im Jahr 2012 offengelegt worden, weil ein Mitarbeiter das gleiche Passwort für seine internen Systeme und sein LinkedIn-Konto verwendet hatte[15]
- Präsident Donald Trump nutzt nach wie vor ein gewöhnliches Samsung Galaxy-Telefon. Experten fragen sich nicht, ob es gehackt wurde, sondern wie viele ausländische Geheimdienste es schon getan haben[16]

[12]http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13]https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14]http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16]https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Erkennen und reagieren

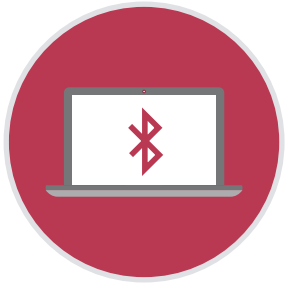


Erkennen und reagieren ist ein Framework zur Computersicherheit, welches die Tatsache anerkennt, dass ein hundertprozentiger Schutz nahezu unmöglich ist.

Wichtig ist vielmehr, einen Datendiebstahl sofort zu bemerken (erkennen) und unverzüglich zu handeln (reagieren).

Es stehen Software-Produkte zur Verfügung, die jedes Gerät zu einem Echtzeitsensor machen. Dies erlaubt es Administratoren, z. B. durch Herunterfahren von Geräten, Quarantäne von Dateien und Löschen von Daten zu reagieren.

Von Grund auf sichere Geräte



Geräte von HP verfügen über integrierte Sicherheit.

Die Sicherheitsmerkmale umfassen das erste selbstheilende BIOS der Welt, eine automatische Bluetooth-Sperre – die das Gerät sperrt, wenn Sie sich entfernen – und integrierte elektronische Blickschutztechnologie (HP Sure View).

Diese Funktionen an sich garantieren keine DSGVO-Konformität, aber sie helfen dabei, diese zu erreichen.

Lernen Sie alle HP Security Features kennen: hp.de/pc-security.

Vorbereitung auf die DSGVO

Schritte, die Sie jetzt schon unternehmen können

Die DSGVO tritt am 25. Mai 2018 in Kraft. Noch bleibt Zeit zur Vorbereitung. Aber wie Sie jetzt zweifelsohne wissen, ist noch viel zu tun.

Der erste Schritt besteht darin, **ihre aktuelle Datenlage zu prüfen**. Prüfen Sie, wo Ihre Daten gespeichert werden, wo sie kopiert werden und wer darauf Zugriff hat. Falls Sie Cloud-Lösungen verwenden, finden Sie heraus, wo die Server stehen, und ob sie DSGVO-konform sind. Dasselbe gilt für SaaS-Lösungen oder andere Partnerunternehmen, mit denen Sie arbeiten und Daten austauschen. Dadurch gewinnen Sie einen fundierten Überblick darüber, was für die Konformität anzupassen ist.

Entwerfen Sie eine Datenrichtlinie. Setzen Sie detaillierte Verfahren um und führen Sie Protokolle darüber, wo Daten gespeichert werden, wer Zugriff hat und außerhalb des Unternehmens oder innerhalb eines multinationalen Konzerns Kopien anfertigt. Schließen Sie eine Richtlinie zum Abruf und zur Löschung von Daten ein. Geben Sie diese im gesamten Unternehmen bekannt. Führen Sie Testläufe durch. Betonen Sie den Stellenwert.

Gestalten Sie Ihre Sicherheitsrichtlinien. Entwerfen Sie einen Sicherheitsrahmen, der auf Erkennen und Reagieren auf Endpunktbasis beruht. Überarbeiten Sie bei Bedarf Ihre Sicherheitsrichtlinien. Investieren Sie bei Bedarf in neue Technologie. Nur 36 % der IT-Verantwortlichen sind der Meinung, dass ihr Budget zur Endpunktsicherheit ausreicht. Die in der DSGVO vorgesehenen Sanktionen sollten auch das Interesse der Vorstandsebene auf sich ziehen.

[17]Ponemon 2016 State of the Endpoint Report

Vorbereitung auf DSGVO

Die DSVGO-Checkliste

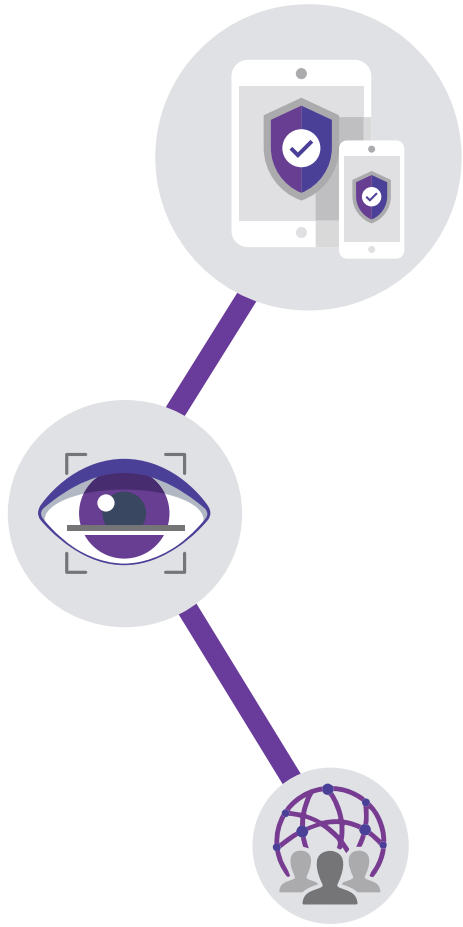
Fünf wichtige Schritte zur DSGVO-Konformität

1. Ernennen Sie bei Bedarf einen Datenschutzbeauftragten (Data Protection Officer, DPO).
2. Führen Sie eine vollumfängliche Datenprüfung durch, einschließlich der Eignung ihrer Cloud- und SaaS-Anbieter in Bezug auf die DSGVO.
3. Erstellen Sie ein Data Governance Framework, einschließlich Vorgehensweisen für Datenübertragbarkeit und das Recht auf Vergessenwerden.
4. Erstellen Sie ein Computersicherheits-Framework und implementieren Sie mehrstufige Endpunktsicherheit.
5. Kommunizieren Sie die Richtlinien und Protokolle gegenüber allen Mitarbeitern des Unternehmens.

Checkliste zur Gerätesicherheit

Sechs wichtige Schritte zur Endpunktsicherheit

1. Prüfen Sie alle autorisierten und nicht-autorisierten Geräte, die Zugang zu personenbezogenen Daten haben
2. Investieren Sie wenn nötig in neue, sicherere Geräte
3. Implementieren Sie einen Fernzugriff und Löschrechte auf unternehmenseigenen Geräten
4. Implementieren Sie Richtlinien, die regelmäßige Untersuchungen und Sicherheitssoftware-Updates vorschreiben
5. Implementieren Sie Erkennungs- und Reaktionssoftware, die in Echtzeit arbeitet
6. Schulen Sie Ihre Mitarbeiter zum Thema Cybersicherheit



Endpunktsicherheitskalender

Ein Umsetzungsplan für die Endpunktsicherheit gemäß DSGVO

2017

Mai

Ernennen Sie einen für die Implementierung der Endpunktsicherheit verantwortlichen Projektmanager.

Juni

Führen Sie eine Bewertung der aktuellen Sicherheitsrichtlinien, Praktiken und Geräte durch

Juli

Ziehen Sie eine Richtlinie zum Austausch von Geräten in Betracht (CYOD/BYOD etc.)

August

Suchen Sie nach Softwarelösungen für die Sicherheit durch „Erkennen und Reagieren“

September

Entwerfen Sie ein mehrstufiges, gestaffeltes Zugriffssystem für Unternehmensdaten

Oktober

Entwerfen Sie eine öffentliche/private Cloud, um außerhalb des Unternehmens ausreichende Sicherheit zu gewährleisten

November

Entwerfen Sie ein Schulungsprogramm einschließlich regelmäßiger Übungen zum Thema Phishing.

Dezember

Implementieren Sie eine neue Datenarchitektur auf Basis einer öffentlichen/privaten Cloud

2018

Januar

Implementieren Sie eine neue Datenarchitektur auf Basis einer öffentlichen/privaten Cloud

Februar

Implementieren Sie die neue Geräterichtlinie

März

Implementieren Sie die Softwarelösung zum „Erkennen und Reagieren“

April

Implementieren Sie die Softwarelösung zum „Erkennen und Reagieren“

Mai

DSGVO tritt in Kraft

Zusammenfassung

Die DSGVO kommt immer näher

Möglicherweise werden in Ihrem Unternehmen schon viele der in den Bestimmungen vorgesehenen Punkte umgesetzt – zum großen Teil handelt es sich schlicht um eine Bündelung bewährter Vorgehensweisen.

Wenn sich Ihr Geschäftszweig auf mehrere Mitgliedsstaaten der Europäischen Union erstreckt, sind Ihnen einige der wichtigeren Vorgaben möglicherweise bereits bekannt.

Die von uns empfohlenen Sicherheitsmaßnahmen zur DSGVO-Konformität umfassen alle Verstöße, die einem Unternehmen Kosten verursachen können. Der Schaden beläuft sich für die deutsche Industrie nach Berechnungen des Bitkom auf rund 22,4 Milliarden Euro pro Jahr. Eine Ziffer, die erwartungsgemäß weiter ansteigen wird.[18]

Viele der erforderlichen Maßnahmen dienen auch der Konformität mit anderen Punkten der DSGVO. Die Beschränkung des Datenzugriffs auf bestimmte Benutzer, Geräte und Netzwerke minimiert nicht nur Datenrisiken, sondern vereinfacht auch die Protokollierung personenbezogener Daten – und damit die Einhaltung der Datenübertragbarkeit und des Rechts auf Vergessenwerden; ganz zu schweigen von internationalen Transfers.

Dieser E-Guide ist nur der Anfang. Sicherheit hat bei HP seit jeher Priorität. Integrierte Sicherheit ist seit Jahren unser Anspruch. Weil Sicherheit nun erforderlich und nicht nur erwünscht ist, stehen wir bereit, Sie bei diesem Ansatz zu unterstützen.

Um mehr darüber zu erfahren, wie HP und unsere Produkte Sie bei der DSGVO-Konformität unterstützen können, besuchen **Sie unsere Seite „Integrierter Datenschutz“**.

[18]https://www.bitkom.org/Presse/Presseinformation/Industrie-im-Visier-von-Cyberkriminellen-und-Nachrichtendiensten.html