De essentiële gids naar naleving van GDPR

U gebracht door

Inhoud

Inleiding

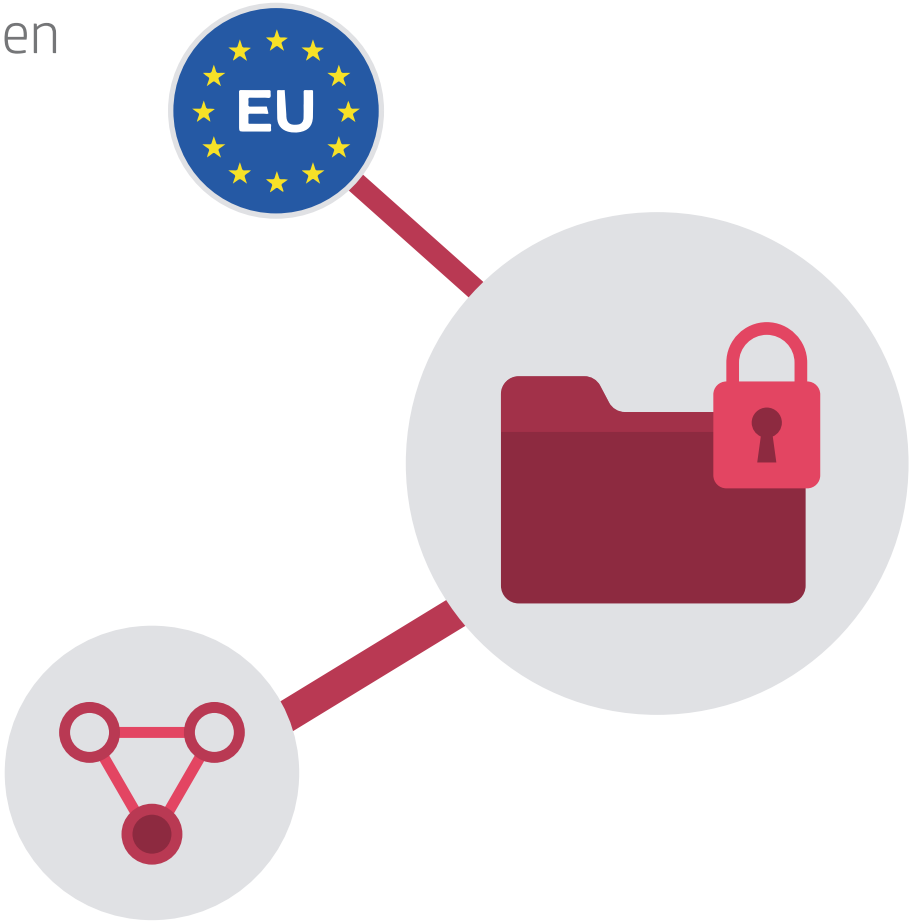
Het is tijd om privacy-door-ontwerp aan te nemen

Per 25 mei 2018 is de EU Algemene verordening gegevensbescherming (AVG) van kracht. Deze vervangt binnen de EU alle gegevensbeschermingsregelgeving en iedereen die binnen een en dezelfde markt zakendoet moet voor naleving zorgen. Dat geldt ook voor niet-EU-bedrijven die zakendoen met EU-klanten.

Krachtens GDPR moet iedere inbreuk op persoonlijke gegevens binnen 72 uur na gewaarwording worden gemeld. Verzuim of achteloosheid kan resulteren in boetes tot € 20 miljoen of 4% van de wereldomzet, het hoogste bedrag van die twee.

Gelukkigerwijs dienen de maatregelen ter bescherming van de bedrijfsgegevens als geheel tevens ter beveiliging van klantengegevens. Dezelfde meervoudig gelaagde eindpuntbeveiligingsaanpak die we bij HP al aanbevelen draagt bij aan de naleving van GDPR.

In deze e-gids onderzoeken we de belangrijkste componenten van GDPR die IT-professionals moeten kennen en kijken we hoe een apparaatgeleid eindpuntbeveiligingsprogramma kan bijdragen aan naleving.



EU GDPR toegelicht

De belangrijkste punten voor IT

Er is in essentie sprake van twee aspecten bij GDPR: beschermen van de rechten van EU-gegevenspersonen en beschermen van de privacy van EU-gegevenspersonen. Beide hebben technologische implicaties.

Voor de gezaghebbende details, lees de volledige tekst. Maar voor IT-besluitvormers moet u de volgende punten weten:

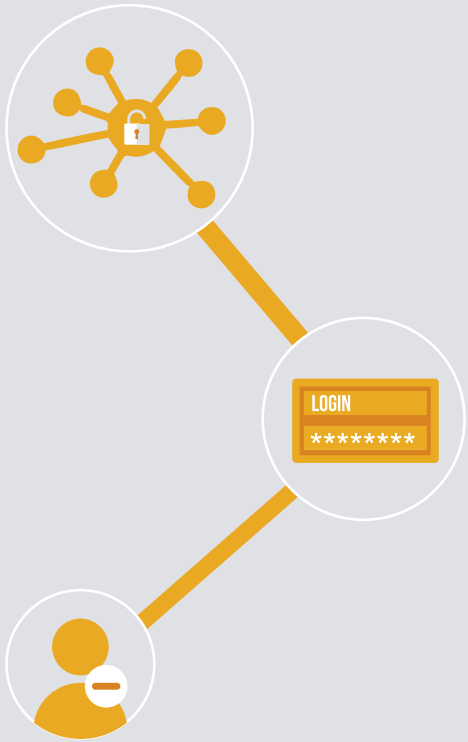
1. **Inbreuken moeten binnen 72 uur worden gemeld**
   Als een gegevensinbreuk plaatsvindt moet deze binnen 72 uur na gewaarwording worden gemeld. De boetes voor verzuim zijn stevig (zie pag. 5 'Wat zijn de boetes voor niet-naleving?')

2. **Het recht om te worden vergeten**
   Iedere EU-gegevenspersoon heeft het recht om te worden vergeten. Op verzoek moet u al zijn/haar gegevens inclusief kopieën wissen

3. **Het recht op dataportabiliteit**
   EU-ingezetenen hebben het recht hun eigen gegevens te controleren. Op verzoek moet u hun gegevens verstrekken in een voor hen toegankelijk formaat en ze hebben het recht deze over te dragen aan een derde partij

4. **Internationale overdrachten**
   Overbrengen van persoonlijke gegevens naar een andere gegevensjurisdictie (bijv. buiten de EU) behoeft uitdrukkelijke toestemming en mag alleen plaatsvinden naar regelgevers die worden beschouwd als 'adequaat', of wanneer aanvullende veiligheidsmaatregelen zijn getroffen[1]

5. **Privacy-door-ontwerp**
   Organisaties moeten een privacy-door-ontwerpaanpak aannemen die standaard gegevensbeveiliging integreert in producten, processen en diensten[2,3]



Op wie is de GDPR van toepassing?

De GDPR is van toepassing op ieder bedrijf dat de persoonlijke gegevens van EU-ingezetenen verzamelt en/of verwerkt. Hieronder vallen ook organisaties die gevestigd zijn buiten de EU maar werkzaam zijn in de EU.

[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

EU GDPR toegelicht

Wat geldt als ‘persoonlijke gegevens’?

Krachtens de GDPR omvat ‘persoonlijke gegevens’ ‘alle gegevens die kunnen worden gebruikt om een persoon te identificeren’.

Dit omvat genetische, psychische, culturele, economische of sociale informatie, naast de informatie die van oudsher wordt beschouwd als identificerende informatie.

Hierdoor worden organisaties onderhevig aan de GDPR die voorheen buiten de wetgeving van gegevensbescherming vielen.

Wat zijn de boetes voor niet-naleving?

De maximale boete is € 20 miljoen of 4% van de wereldomzet, het hoogste bedrag van die twee. Dit geldt voor de ernstigste overtredingen krachtens de wetgeving, zoals verzuimen om een beveiligingsinbreuk binnen 72 uur na gewaarwording te melden.

Minder ernstige overtredingen kosten maximaal € 10 miljoen of 2% van de wereldomzet. Onnodig te vermelden dat de kosten van niet-naleving aanzienlijk zijn.

GDPR procedure checklist

Binnen uw databeheerraamwerk heeft u expliciete procedures nodig voor:

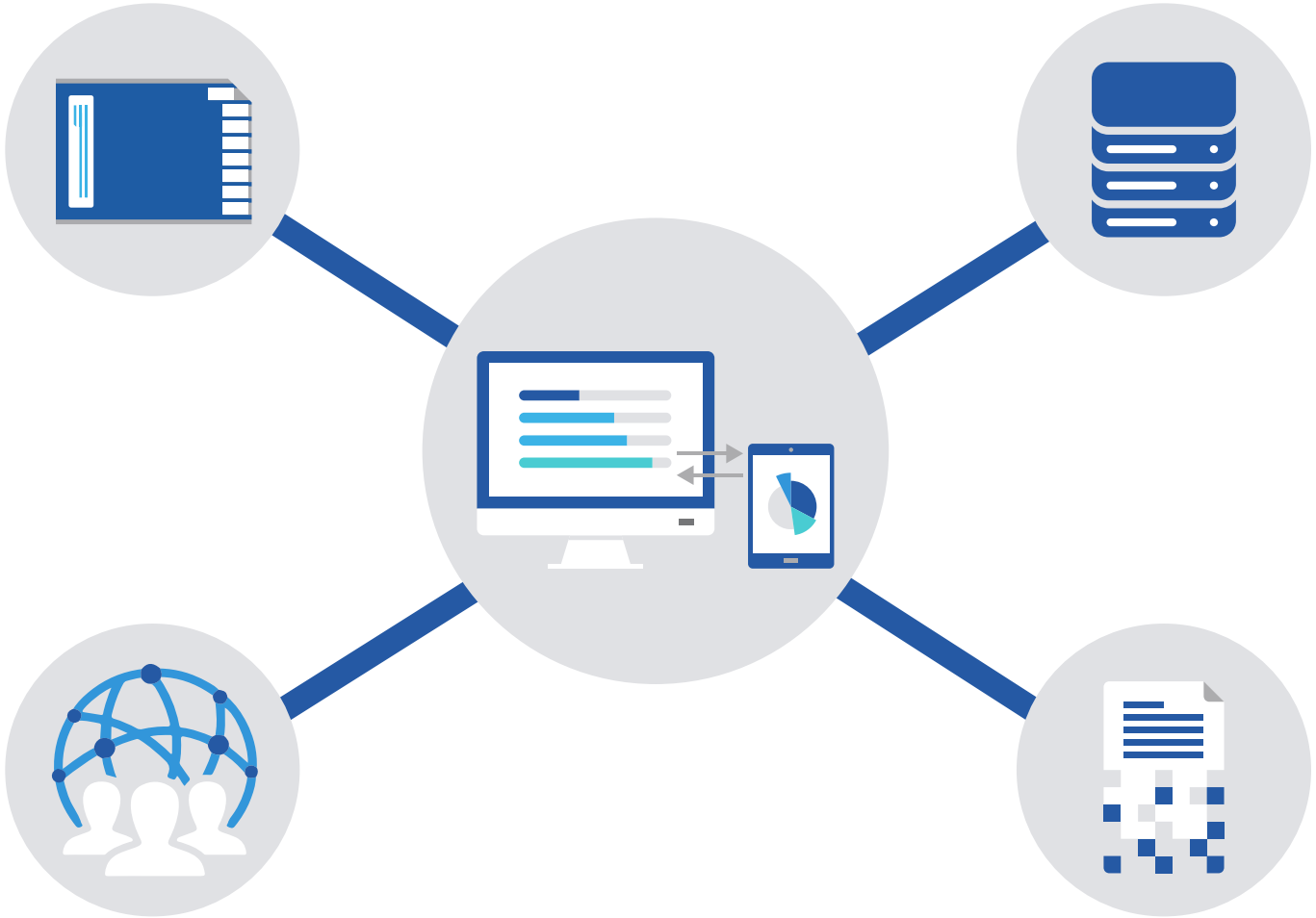
- Informeren van gegevenspersonen hoe hun gegevens worden verzameld, opgeslagen en verwerkt
- Verkrijgen van toestemming van gegevenspersonen hiervoor
- Verstrekken van gegevens van gegevenspersonen in een voor hen toegankelijk formaat
- Wissen van alle persoonlijke gegevens van een gegevenspersoon, inclusief kopieën
- Overdragen van gegevens naar een andere gegevenscontroller of -verwerker
- Overdragen van gegevens buiten de EU - ook binnen de organisatie

Technische uitdagingen voor naleving

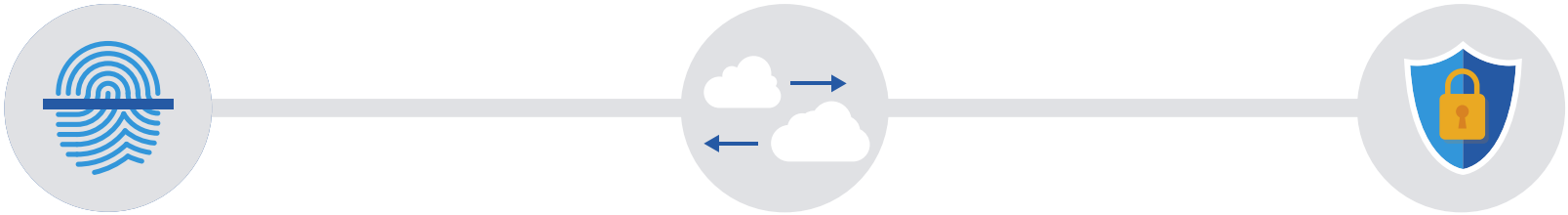
De grootste uitdagingen van GDPR zijn technisch.

Mogelijk maken van beveiligde dataportabiliteit, beschermen van gegevens van personen en hun recht om vergeten te worden vereisen een uitgebreide kaart van gegevenslocatie en -toegang tot aan apparatuurniveau.

Terwijl de dreiging van cybercriminaliteit jaar na jaar toeneemt, is het handhaven van absolute beveiliging een groeiende uitdaging.



Technische uitdagingen voor naleving



Apparaten bijhouden

Naleving van dataportabiliteit en het recht om vergeten te worden vereisen een gedetailleerde administratie van alle persoonlijke gegevens die in het bezit zijn van de organisatie.

U moet op de hoogte zijn van:

- Ieder apparaat dat persoonlijke gegevens bevat
- Ieder apparaat dat toegang heeft tot persoonlijke gegevens

Dat is de enige manier om te waarborgen dat u door het bedrijf gehouden persoonlijke gegevens kunt terughalen en/of wissen.

Clouds bijhouden

De gemiddelde Europese onderneming gebruikt 608 apps, een cijfer dat naar schatting 90% ondergewaardeerd wordt. Werknemers gebruiken vaak commerciële cloud-apps zonder dat de IT-afdeling daarvan op de hoogte is.[4]

Voor GDPR naleving moet gebruik van de cloud worden beperkt tot diensten die:

- Plaatsvinden binnen de EU en daarom vanzelf in naleving zijn met GDPR
- Onder de jurisdictie vallen van een gegevensbeschermingsregelgever die door de EU als 'adequaat' wordt beschouwd

Zo niet dan kan er sprake zijn van inbreuk op het internationale overdrachtsvoorschrift. En u moet weten welke clouddiensten werknemers gebruiken voor het geval personen zich beroepen op het recht om vergeten te worden.

Gegevens beschermd houden

De dreiging van cybercriminaliteit is groeiende. Niet in de laatste plaats omdat ook de groei van onbeveiligde netwerken en privé-apparaten toeneemt.

Inbreuken zijn vrijwel onvermijdelijk. De EU weet dit. Maar om een hoge boete te vermijden moet u:

- Een Systems Incident Event Monitoring (SIEM) tool implementeren om een inbreuk binnen 72 uur te melden
- Meervoudig gelaagde eindpunt beveiliging implementeren om due diligence te tonen in het voorkomen van een inbreuk

Gebruikers moet ook bewustwording worden bijgebracht van hun verantwoordelijkheden wat betreft het niet gebruiken van niet-gesanctioneerde apparaten en netwerken.

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

De dreiging van cybercriminaliteit

Cybercriminaliteit is een reële, aanwezige en groeiende dreiging

82%

van organisaties heeft een dreiging/inbreuk ervaren binnen 12 maanden[5]

80%

van IT-professionals denkt dat de dreiging van cybercriminaliteit de komende drie jaar zal toenemen[6]

78%

van bedrijven meldt een toename van malware-aanvallen in de afgelopen vijf jaar[7]

60%

van IT-leiders heeft het gevoel dat cybercriminaliteit verdedigingsmechanismen te snel af is[8]

81%

van bedrijven geeft achteloosheid van insiders de hoogste score voor bedreiging van cyberbeveiliging[9]

81%

van IT-leiders stelt dat mobiele apparaten op hun netwerk het doelwit zijn geweest van malware[9]

72%

zegt dat werknemersgebruik van commerciële cloud-software een risico vormt[9]

69%

zegt dat BYOD een beveiligingsrisico is

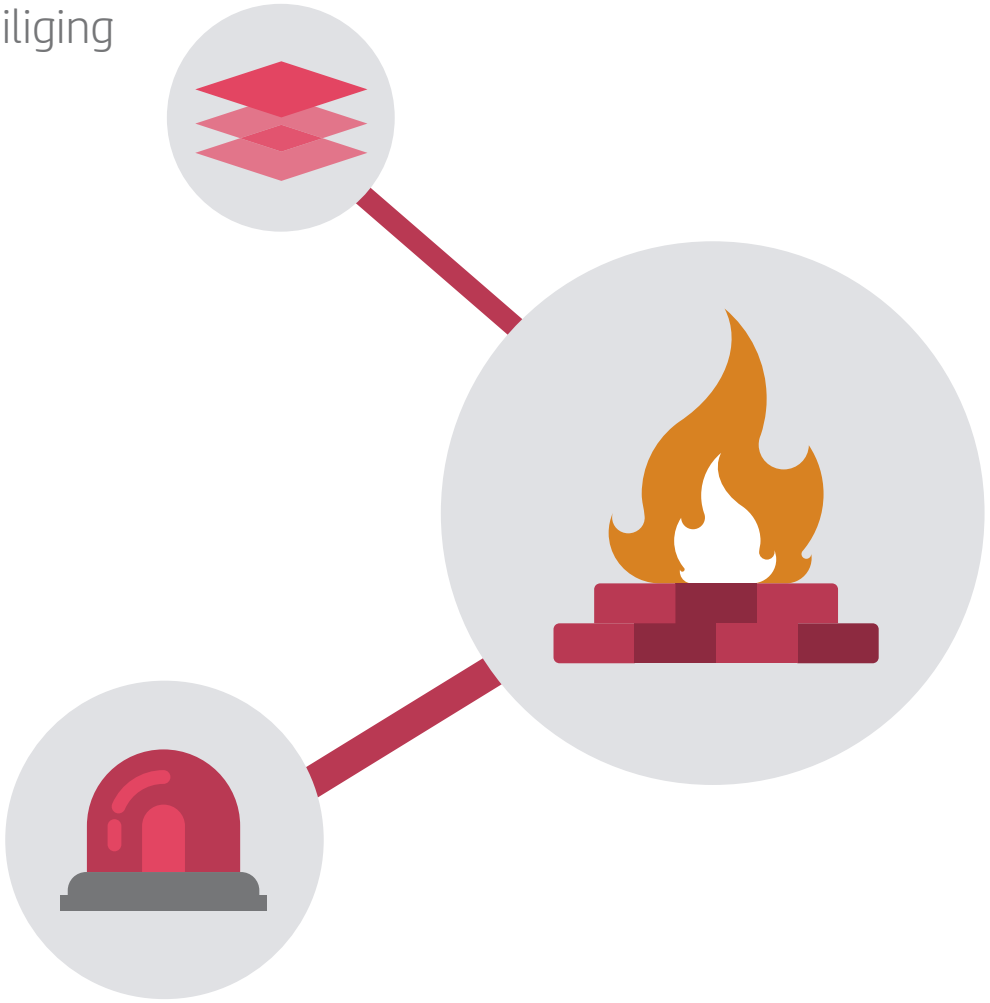
[5]HPI Printer Security Research 2016 (Spiceworks) [6]HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8]IBM CISO Assessment 2014 [9]Ponemon 2016 State of the Endpoint Report

Implementeren van eindpuntbeveiliging

HP's meervoudig gelaagde aanpak voor eindpuntbeveiliging

De voorkomings- en beschermings-aanpak voor cyberbeveiliging, firewall en antivirus, is niet voldoende. Dat is het nooit geweest. In een studie door Damballa had antivirussoftware zes maanden nodig om alle kwaadaardige bestanden te identificeren en elimineren.[10]

HP's standpunt is dat cyberbeveiliging meervoudig gelaagd moet zijn, werkzaam is op netwerk-, apparaat- en gebruikersniveau, met meerdere verdedigingsmechanismen op ieder niveau. Opsporen en reageren moet voorrang krijgen boven beschermen en verdedigen. En de eindpunten zijn het beginpunt: zowel apparaat als gebruiker.



Critical Security Controls (CSC)

Het Center for Internet Security (CIS) heeft 20 internationaal erkende Critical Security Controls (CSC) gedefinieerd, die zijn ontwikkeld, verfijnd en gevalideerd door leidende IT-beveiligingsdeskundigen wereldwijd. Deze worden gezien als belangrijke cyberhygiënische acties voor iedere organisatie. We verwijzen naar de belangrijkste CSC's voor GDPR-naleving, omdat het nuttige richtlijnen zijn, maar de volledige tekst is online beschikbaar. Download de tekst gratis in de CIS bibliotheek.

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

Netwerkbeveiliging

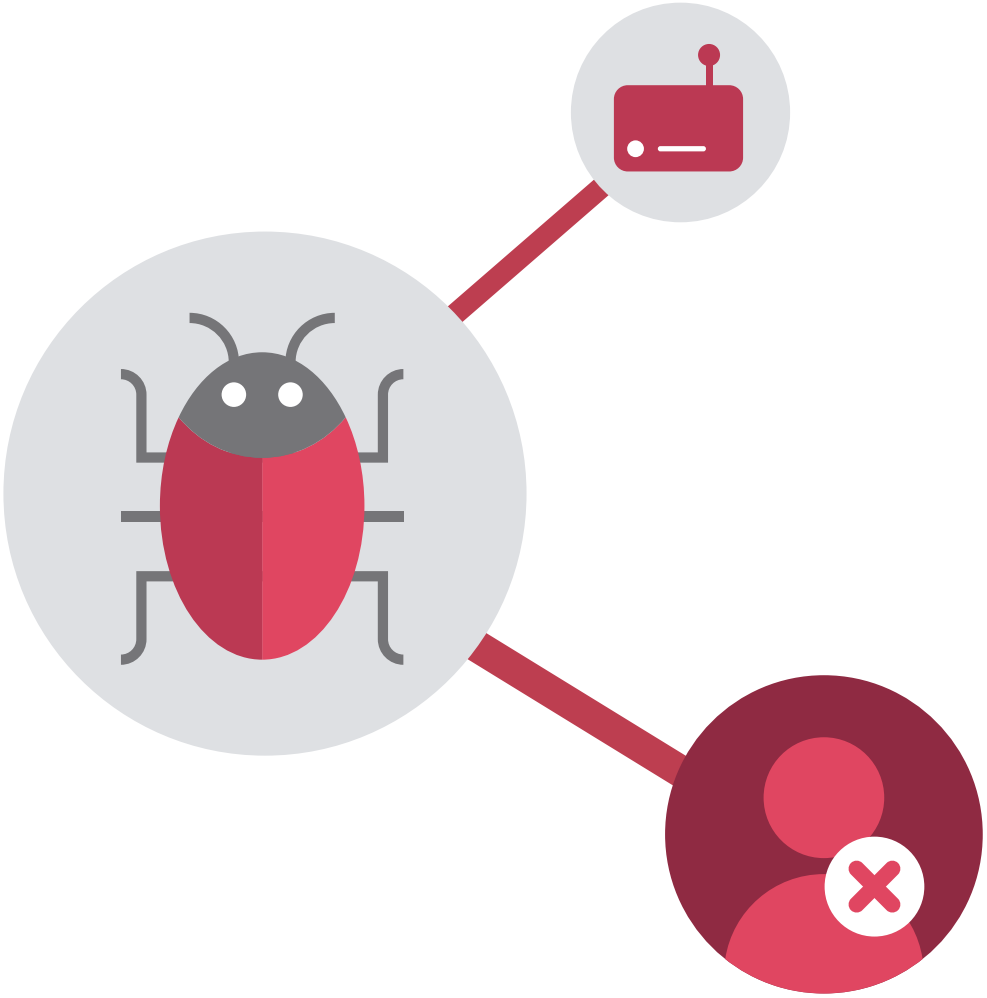
Grotere hacks maken vaak gebruik van een enkele ingang om toegang te krijgen tot het hele netwerk. Beveiliging op netwerkniveau moet er daarom op gebaseerd zijn om dat te voorkomen.

- **Controle van administratieve privileges (CSC 5)**
  De bevoegdheid tot het veranderen van netwerkinstellingen en wachtwoorden tot zo weinig mogelijk mensen beperken
- **Toegangscontrole op basis van 'need to know' (CSC 14)**
  Spits toegang tot gevoelige informatie toe op gebruiker, apparaat en locatie. Weeg het beveiligings risico af tegen de gevoeligheid van de gegevens
- **Beperking en controle van netwerkpoorten, protocollen en diensten (CSC 9)**
  Schakel onnodige toegangspunten uit (virtueel en fysiek) inclusief FTP, Telnet en printdiensten
- **Onderhoud, monitoring en analyse van audit logs (CSC 6)**
  Regelmatig audit logs beoordelen om systeemgedrag te analyseren en verdachte activiteiten op te sporen
- **Voortdurend(e) kwetsbaarheids-beoordeling en herstel (CSC 4)**
  Voortdurend de omgeving beoordelen op kwetsbaarheden en actie ondernemen tot herstel van resultaten en de kans op inbreuken terugbrengen tot een minimum

Het doel is een netwerk te creëren dat onderverdeeld is naar gelang de gevoeligheid van gegevens. Toegangsverzoeken worden geëvalueerd op beveiligingsrisico's. Niet-herkende apparaten, gebruikers en verzoeken van onbeveiligde netwerken worden geblokkeerd van de gevoeligste gegevens. Google's BeyondCorp-beleid is een goed model.[11]

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

Netwerkbeveiliging



Ieder apparaat is een potentiële kwetsbaarheid, ongeacht of het van het bedrijf of privé is. U moet iedere telefoon, tablet, laptop en bureaucomputer kennen die toegang heeft tot bedrijfsgegevens.

- **Inventarisatie van geautoriseerde en niet-geautoriseerde apparaten (CSC 1)** Voer een audit uit voor elk apparaat dat toegang heeft tot gegevens
- **Inventarisatie van geautoriseerde en niet-geautoriseerde software (CSC 2)** Voer een audit uit voor elke op het netwerk gebruikte applicatie, voor al dan niet rechtstreekse toegang tot gegevens
- **Malware verdedigings-mechanismen (CSC 8)** Zorg dat ieder apparaat bijgewerkte antivirus en antimalware heeft. Zorg voor regelmatige scans en updates

Apparatuurbeveiliging

Verder moeten IT-afdelingen deze aanvullende controles overwegen:

- **Meerzijdige authenticatie**
  Zorg ervoor dat ieder werkapparaat beveiligd is. Gebruik idealiter biometrische authenticatie naast wachtwoorden (zie pag. 14 'Privacy-door-ontwerp-apparaten')

- **Toegang op afstand**
  Zorg voor toegang tot apparaten op afstand om persoonlijke gegevens terug te halen of te wissen, processen in quarantaine te zetten of te beëindigen, en het apparaat af te sluiten en te vergrendelen in het geval van verlies of diefstal (zie pag. 14 'Opsporen en reageren')

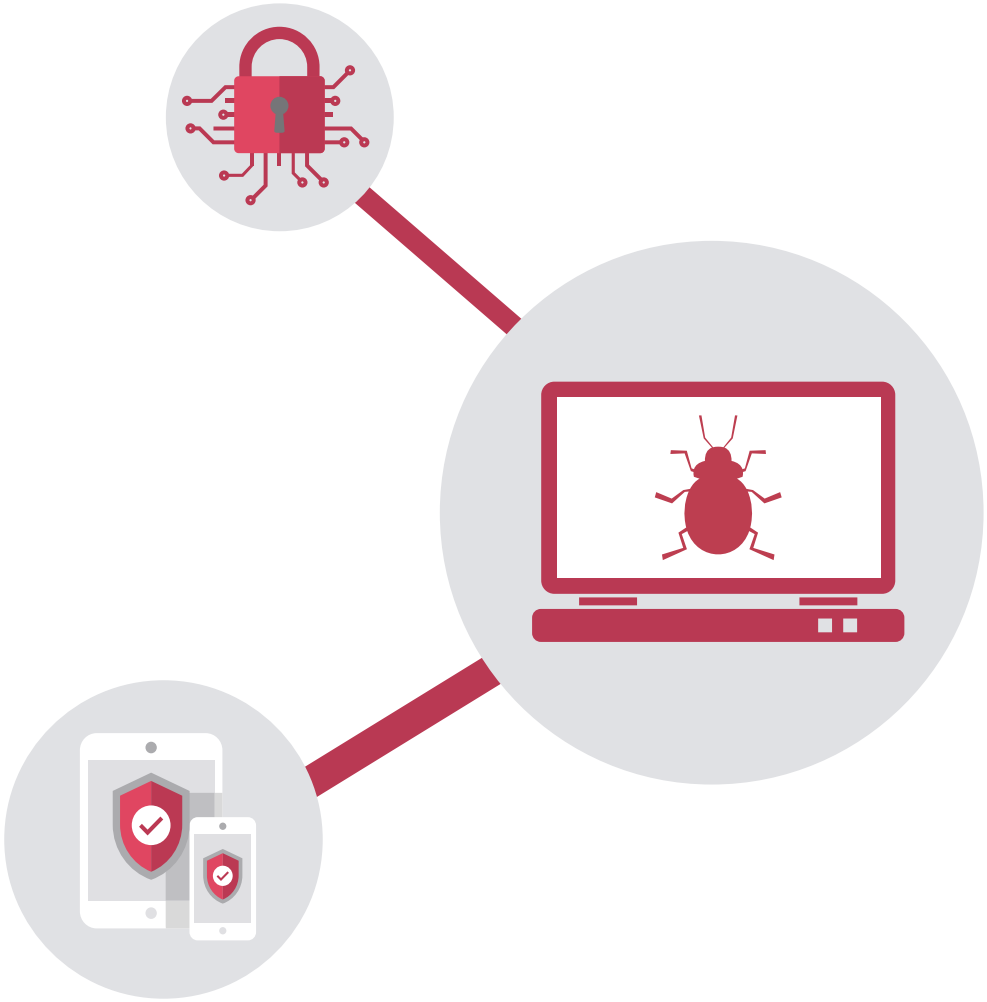
- **Informeer iedere werknemer over beveiligingsprotocollen en -procedures**
  Zorg dat iedere werknemer zich bewust is van zijn/haar verantwoordelijkheden betreffende cyberbeveiliging en deze kent, waaronder het melden van verdachte activiteiten

- **Zorg voor actieve cyberbeveiligingstraining**
  Houd workshops, seminars, phishing-oefeningen: zorg dat iedereen weet hoe men basisfouten vermijdt en hoe men in naleving blijft van GDPR

- **Minimaliseer het gebruik van privé-apparaten en -apps**
  Ontmoedig het gebruik van privé-apparaten en -apps voor bedrijfsdoeleinden. Een uitgebreid en flexibel CYOD-beleid kan daarbij helpen

Implementeren van een dergelijk beveiligingsraamwerk moet u helpen bij het handhaven van controle over bedrijfsapparaten voor het beschermen van gegevens en het faciliteren van de oplegging van dataportabiliteit en het recht om vergeten te worden.

Lees onze white paper voor meer informatie over HP's aanpak voor meervoudig gelaagde beveiliging
Beveiliging begint bij het eindpunt.



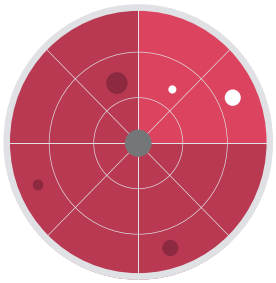
Waarom iedere werknemer cyberbewust moet zijn

58% van cyberdreigingen komt van werknemers, ex-werknemers en vertrouwde partners.[12] Ieder apparaat beveiligen betekent ook iedere gebruiker ervan beveiligen.

- De U.S. Democratic National Committee (DNC) werd in 2016 gehackt toen John Podesta op een phishing-link klikte die per ongeluk als legitiem was bestempeld door een naaste medewerker[13]
- In 2014 werd internet overspoeld met naaktfoto's van sterren nadat de 36-jarige Ryan Collins toegang kreeg tot o.a. Jennifer Lawrence's iCloud met eenvoudige phishing-e-mails die deden lijken alsof ze afkomstig waren van Apple[14]
- In 2012 werden 68 miljoen Dropbox-wachtwoorden gelekt dankzij een werknemer die hetzelfde wachtwoord gebruikte voor interne systemen als voor zijn LinkedIn[15]
- President Donald Trump gebruikt nog steeds een standaard Samsung Galaxy telefoon. Deskundigen vragen zich niet af óf hij gehackt is, maar eerder hoeveel buitenlandse inlichtingendiensten dat al hebben gedaan[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

Opsporen en reageren

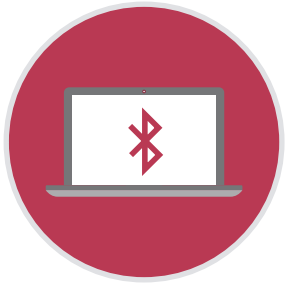


Opsporen en reageren is een cyberbeveiligingsraamwerk dat erkent dat totale preventie zo goed als onmogelijk is.

Wat belangrijk is, is u bewust te worden van de inbreuk (opsporen) en onmiddellijk actie te ondernemen (reageren).

Er zijn softwareproducten beschikbaar die van ieder apparaat een real-time sensor maken en de beheerder in staat stellen te reageren door bijvoorbeeld apparaten af te sluiten, bestanden in quarantaine te zetten en gegevens te wissen.

Privacy-door-ontwerp-apparaten



HP's apparaten belichamen privacy-door-ontwerp.

Beveiligingskenmerken omvatten 's werelds eerste zelfhelende BIOS, automatische Bluetooth-vergrendeling, die het apparaat vergrendelt als men wegloopt, en geïntegreerde privacyschermen.

Deze kenmerken alleen kunnen niet voor GDPR-naleving zorgen, maar dragen er zeker toe bij.

Voorbereiden voor GDPR

Praktische stappen die nu gezet moeten worden

De GDPR is per 25 mei 2018 van kracht. Er is nog tijd voor voorbereiding, maar zoals u inmiddels ongetwijfeld heeft begrepen, is er heel veel te doen.

De eerste stap is het **uitvoeren van een audit van uw huidige gegevenssituatie**. Beoordeel waar uw gegevens zijn opgeslagen, waar kopieën naar toe gaan en wie er toegang toe heeft. Als u cloudoplossingen gebruikt, zoek uit waar de servers ervan gevestigd zijn en of ze in naleving van GDPR zullen zijn. Hetzelfde geldt voor SaaS of andere partnerorganisaties waarmee u werkt en gegevens deelt. Dit zal u een duidelijke indruk geven van hoeveel er moet veranderen om in naleving te zijn

Ontwerp uw gegevensbeleid. Voeg gedetailleerde procedures en protocollen toe over waar gegevens zijn opgeslagen, wie toegang heeft en kopieën maakt buiten het bedrijf, of over landsgrenzen bij een multinational. Voeg procedures toe voor het terughalen en wissen van persoonlijke gegevens. Communiceer dit naar iedereen in het bedrijf. Regel trainingssessies. Onderstreep het belang ervan.

Ontwerp uw beveiligingsbeleid. Creëer een nieuw cyberbeveiligingsraamwerk dat werkt vanuit een opsporen-en-reageren-eindpuntbasis. Herzie zo nodig uw apparatuurbeleid. Investeer zo nodig in nieuwe technologie. Slechts 36% van IT-leiders heeft het gevoel genoeg budget te hebben voor eindpuntbeveiliging.[17] De GDPR-boetes zijn tenslotte misschien de stok achter de deur om de C-suite geïnteresseerd te krijgen.

[17] Ponemon 2016 State of the Endpoint Report

Voorbereiden voor GDPR

GDPR-checklist

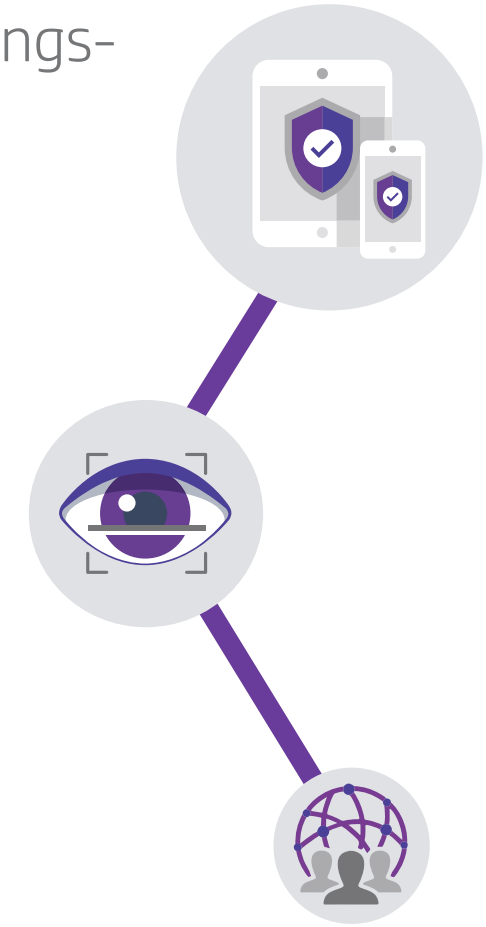
5 belangrijke stappen richting GDPR-NALEVING

1. Benoem iemand die verantwoordelijk is voor gegevens, een Data Protection Officer (DPO) indien gewenst
2. Voer een volledige gegevensaudit uit, inclusief geschiktheid van cloud- en SaaS-leveranciers met betrekking tot GDPR
3. Creëer een nieuw databeheer-raamwerk, inclusief procedures voor dataportabiliteit en het recht om vergeten te worden
4. Creëer een nieuw cyberbeveiligings-raamwerk en implementeer meervoudig gelaagde eindpunt-beveiliging
5. Communiceer beleidslijnen en protocollen met iedereen in het bedrijf

Apparatuurbeveiligings-checklist

6 belangrijke stappen richting beveiliging eindpunten

1. Voer een audit uit voor alle geautoriseerde en niet-geautoriseerde apparaten met toegang tot persoonlijke gegevens
2. Investeer zo nodig in nieuwe - beter beveiligde - apparaten
3. Implementeer het recht voor toegang op afstand tot bedrijfs gegevens op apparaten en het recht om ze te wissen op afstand
4. Implementeer een beleid voor het regelmatig scannen en updaten van beveiligingssoftware
5. Implementeer real-time opsporings- en responssoftware
6. Train werknemers in cyberbeveiliging



Kalender eindpuntbeveiliging

Een basistijdlijn voor implementatie van eindpuntbeveiliging door GDPR

2017

Mei

Projectmanager aanstellen die verantwoordelijk is voor het implementeren van eindpuntbeveiliging

Juni

Audit uitvoeren van huidig(e) beveiligingsbeleid, praktijken en apparaten

Juli

Apparatuureisen en -beleid overwegen voor eindpuntbeveiliging (CYOD/BYOD enz.)

Augustus

Software-oplossingen overwegen voor opsporings- en responsbeveiliging

September

Ontwerpen van meervoudig gelaagd toegangssysteem voor bedrijfsgegevens

Oktober

Openbare/privécloud ontwerpen om gepaste gegevenstoegang van buitenaf mogelijk te maken

November

Ontwerpen gebruikerstrainingsprogramma inclusief regelmatige phishing-oefeningen

December

Communiceren van nieuw beveiligingsbeleid aan de rest van het bedrijf

2018

Januari

Implementeren van nieuwe gegevensarchitectuur op openbare/privécloud

Februari

Implementeren van nieuw apparatuurbeleid

Maart

Implementeren van software-oplossing voor opsporing en respons

April

Gebruikersbeveiligingstraining uitvoeren waaronder beleid in relatie tot GDPR

Mei

GDPR wordt van kracht

Samenvatting

GDPR is niet ver weg

Als u geluk heeft brengt uw organisatie al veel van de voorschriften in de praktijk. Het gaat grotendeels om een inkapseling van dat wat staat voor beste praktijken.

En als u werkzaam bent geweest in meerdere EU-landen heeft u wellicht al te maken gehad met enkele van de straffere maatregelen daaruit.

De beveiligingsmaatregelen die we aanbevelen uit te voeren ter naleving van GDPR zijn maatregelen die bijdragen aan het voorkomen van welke inbreuk dan ook die een organisatie ongelooflijk veel geld kan kosten. Bij de meest recente telling schatte de regering van het Verenigd Koninkrijk dat Britse bedrijven in één jaar £ 21 miljard verloren en dat cijfer groeit naar verwachting.[18]

Verder dragen veel van de vereiste maatregelen voor werkelijk solide beveiliging ook bij tot naleving van andere aspecten van de GDPR. Beperken van gegevenstoegankelijkheid tot bepaalde gebruikers, apparaten en netwerken minimaliseert niet alleen de gegevensrisico's, het bijhouden van persoonlijke gegevens wordt ook gemakkelijker, en daarmee het naleven van dataportabiliteit en het recht om vergeten te worden; om nog niet te spreken van internationale overdrachten.

Deze e-gids is nog maar het begin. Beveiliging is altijd een prioriteit geweest bij HP. Privacy-door-ontwerp is al jarenlang ons beleid. Nu het vereist in plaats van gewenst is, zijn we in een goede positie om u te helpen dezelfde aanpak aan te nemen.

Ga naar **onze pagina Privacy-door-ontwerp om meer aan de weet te komen over hoe HP en onze producten u kunnen helpen bij het naleven van GDPR**

[18]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf