Ghid cu informații de bază privind conformitatea cu RGPD

Pregătiți-vă pentru impactul acestor reglementări alături de HP

Oferit de

Cuprins

Introducere

A sosit momentul să adoptați încă din proiectare securitatea datelor

În data de 25 mai 2018, va intra în vigoare Regulamentul general al UE privind protecția datelor. Acesta va înlocui toate reglementările naționale privind protecția datelor din UE, iar orice entitate care își desfășoară activitatea pe piața unică va trebui să îl respecte. Sunt incluse aici și societățile din afara UE care au clienți în UE.

În conformitate cu RGPD, orice breșă de securitate în privința datelor cu caracter personal trebuie raportată în termen de 72 de ore de la momentul în care ați aflat despre ea. În caz contrar , având ca scop descurajarea neglijenței, se pot percepe amenzi de până la 20 de milioane de EUR sau 4% din cifra globală de afaceri, oricare dintre aceste sume este mai mare - sau pentru descurajarea neglijenței - se pot percepe amenzi de până la 20 de milioane EUR sau 4% din cifra globală de afaceri, oricare dintre aceste sume este mai mare.

Din fericire, măsurile necesare pentru protejarea datelor societății în ansamblul lor vor servi și la protejarea securității datelor clienților. Aceeași abordare a securității la punctul final structurată pe linii de apărare, recomandată deja de HP, va ajuta la asigurarea conformității cu RGPD.

În acest ghid, vom examina componentele esențiale ale RGPD pe care trebuie să le cunoască specialiștii IT și vom analiza modul în care un program de securitate la punctul final, instalat pe un dispozitiv, poate ajuta la asigurarea conformității.

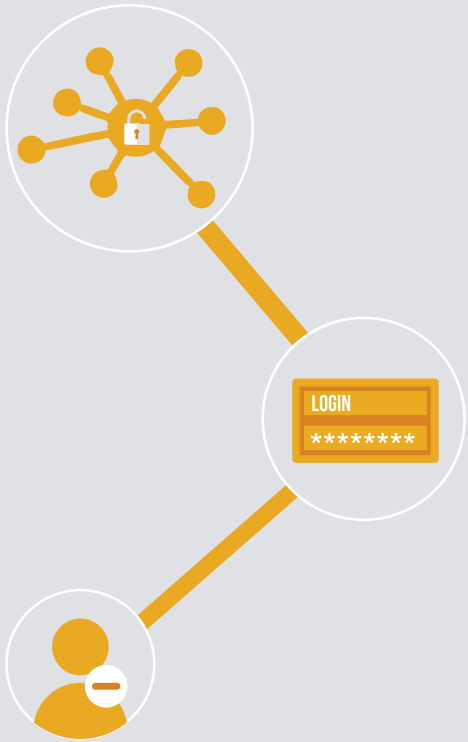
RGPD în UE explicat

Aspectele esențiale pentru IT

Există, în principal, două aspecte ale RGPD: protejarea drepturilor subiecților de date din UE și protejarea confidențialității subiecților de date din UE. Ambele au implicații tehnologice.

Pentru detalii oficiale, consultați textul complet. Însă pentru decidenții din sfera IT, acestea sunt aspectele pe care trebuie să le cunoașteți:

1. **breșele de securitate trebuie raportate în termen de 72 de ore**
   În cazul în care se produce un incident de securitate în privința datelor, acesta trebuie raportat în termen de 72 de ore de la momentul în care luați cunoștință cu privire la el. Penalitățile pentru nerespectarea acestei prevederi sunt foarte importante (consultați pagina 5, „Care sunt penalitățile pentru neconformitate?")
2. **dreptul de a fi uitat**
   Fiecare subiect de date din UE are dreptul de a fi uitat. La cerere, trebuie să ștergeți datele sale, inclusiv toate copiile acestora
3. **dreptul la portabilitatea datelor**
   Rezidenții UE au dreptul de a-și controla propriile date. La cerere, trebuie să le puneți la dispoziție datele într-un format accesibil, pe care să aibă permisiunea de a-l transfera către o entitate externă
4. **transferuri internaționale**
   Mutarea datelor cu caracter personal către o altă jurisdicție de date (anume în afara UE) se poate realiza numai cu consimțământul explicit și numai către autoritățile de reglementarea considerate „adecvate" sau după instituirea măsurilor de protecție suplimentare[1]
5. **securitatea datelor instalată din proiectare**
   Organizațiile trebuie să adopte o abordare tip confidențialitate din proiectare, care să integreze securitatea datelor în produse, procese și servicii, în mod predefinit[2,3]



Cui i se aplică RGPD?

RGPD se aplică oricărei societăți care colectează și/sau prelucrează datele cu caracter personal ale rezidenților UE. Aceasta include organizațiile din afara UE care își desfășoară activitatea în Uniune.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Allen & Overy – Regulamentul UE general privind protecția datelor din 2016
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

RGPD în UE explicat

Ce anume reprezintă „datele cu caracter personal”?

În conformitate cu RGPD, „datele cu caracter personal” includ „orice date care pot fi folosite pentru identificarea unei persoane”.

Aceasta include informații genetice, mentale, culturale, economice sau sociale, pe lângă cele considerate în mod tradițional a reprezenta informații de identificare.

Aceasta poate face ca organizațiilor care anterior nu intrau sub incidența legislației privind protecția datelor să li se aplice acum prevederile RGPD.

Care sunt penalitățile pentru neconformitate?

Amenda maximă este de 20 de milioane EUR sau 4% din cifra globală de afaceri, oricare dintre sume este mai mare. Aceasta se aplică celor mai grave abateri, în virtutea regulamentului, precum neraportarea unei breșe de securitate în termen de 72 de ore de la momentul la care ați luat cunoștință de ea.

Abaterile mai puțin grave implică o amendă maximă de 10 milioane EUR sau 2% din cifra globală de afaceri. Evident, costurile nerespectării acestor prevederi sunt semnificative.

Lista de verificare privind procedura RGPD

În cadrul dvs. de gestionare a datelor veți avea nevoie de proceduri explicite pentru:

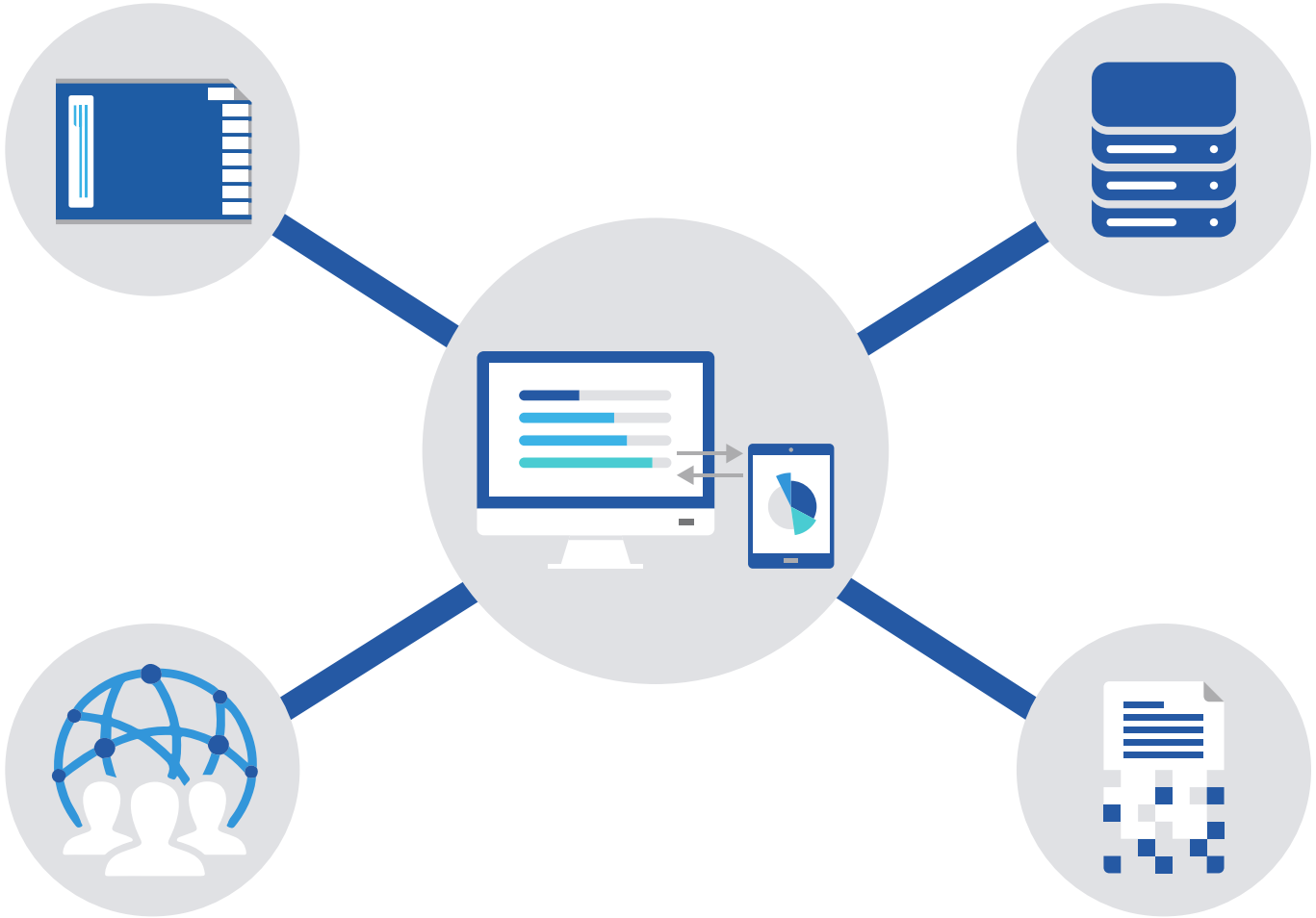
- a informa subiecții de date despre cum vor fi colectate, stocate și prelucrate datele lor
- a obține consimțământul explicit al subiecților de date în acest sens
- a oferi informațiile subiecților de date într-un format accesibil lor
- a șterge toate datele cu caracter personal ale unui subiect de date, inclusiv copiile acestora
- a transfera datele către un alt controlor de date sau entitate care prelucrează datele
- a transfera datele în afara UE - inclusiv în cadrul organizației

Provocări tehnice în privința conformității

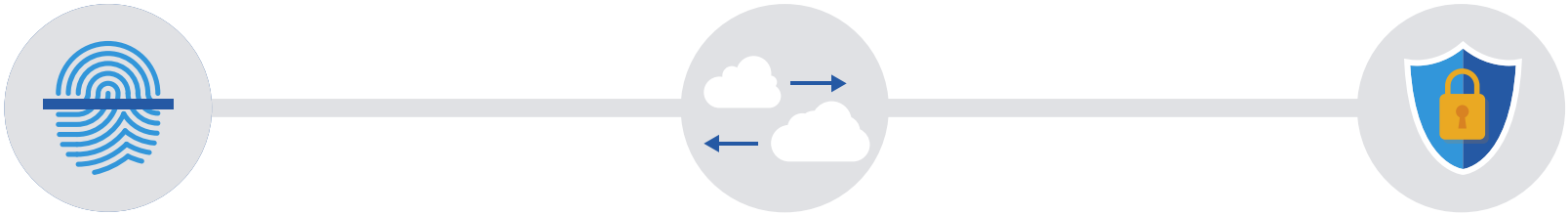
Cele mai mari provocări ale RGPD sunt de natură tehnică.

Activarea portabilității securizate a datelor, protejarea datelor persoanelor și a dreptului lor de a fi uitate, toate aceste necesită o cartografiere exhaustivă a locației datelor și a accesului la ele, până la nivel de dispozitiv.

Dat fiind că amenințarea criminalității cibernetice crește de la an la an, menținerea unei securități absolute reprezintă o provocare în creștere.



Provocări tehnice în privința conformității



Ținerea evidenței dispozitivelor

Conformitatea prevederilor referitoare la portabilitatea datelor și la dreptul de a fi uitat necesită o evidență detaliată a tuturor datelor cu caracter personal deținute de organizație.

Trebuie să știți:

- fiecare dispozitiv care stochează date cu caracter personal
- fiecare dispozitiv care are acces la date cu caracter personal

Aceasta este singura modalitate care vă oferă garanția că puteți recupera și/sau șterge datele personale deținute de către societate.

Urmărirea sistemelor cloud

Întreprinderea europeană medie folosește 608 aplicații, o cifră care este considerată subestimată în proporție de 90%. Angajații folosesc adesea aplicații cloud comerciale, fără a informa în acest sens departamentul IT.[4]

Pentru a asigura conformitatea cu prevederile RGPD, utilizarea sistemului cloud trebuie limitată la servicii care sunt:

- în cadrul UE și, prin urmare, ele însele conforme cu RGPD
- sub jurisdicția unei autorități de reglementare în privința protecției datelor considerată „adecvată” de UE

Orice altceva ar putea încălca norma privind transferul internațional. Și trebuie să știți ce servicii cloud folosesc angajații, dacă invocă dreptul de a fi uitate.

Datele trebuie protejate în permanență

Amenințarea criminalității cibernetice este în creștere. Și aceasta nu în ultimul rând din cauza utilizării în creștere a unor rețele și dispozitive personale nesecurizate.

Breșele de securitate sunt aproape inevitabile. UE cunoaște acest lucru. Însă, pentru a evita o amendă costisitoare, trebuie:

- să implementați un instrument de monitorizare a evenimentelor tip incident de sistem (MEIS) pentru raportarea unei breșe de securitate în termen de 72 de ore
- să implementați o securitate la punctul final structurată pe linii de apărare pentru a da dovadă de diligența cuvenită în prevenirea unei breșe

Utilizatorii trebuie, de asemenea, să fie informați cu privire la responsabilitățile lor de a nu folosi dispozitive și rețele neaprobate.

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

Amenințarea criminalității cibernetice

Criminalitatea cibernetică este o amenințare reală, prezentă și în creștere

82%

dintre organizații s-au confruntat cu o amenințare/breșă de securitate în decurs de 12 luni[5]

80%

dintre profesioniștii IT consideră că amenințarea criminalității cibernetice va crește în următorii trei ani[6]

78%

dintre firme raportează o creștere a atacurilor de tip malware în decursul ultimilor cinci ani[7]

60%

dintre managerii IT consideră criminalitatea cibernetică superioară metodelor de apărare[8]

81%

dintre firme consideră că neglijența personalului intern este cea mai mare amenințare la adresa securității cibernetice[9]

81%

dintre managerii IT afirmă că dispozitivele mobile din rețeaua lor au reprezentat o țintă pentru malware[9]

72%

afirmă că utilizarea software-ului cloud comercial de către angajați reprezintă un risc[9]

69%

afirmă că BYOD reprezintă un risc de securitate

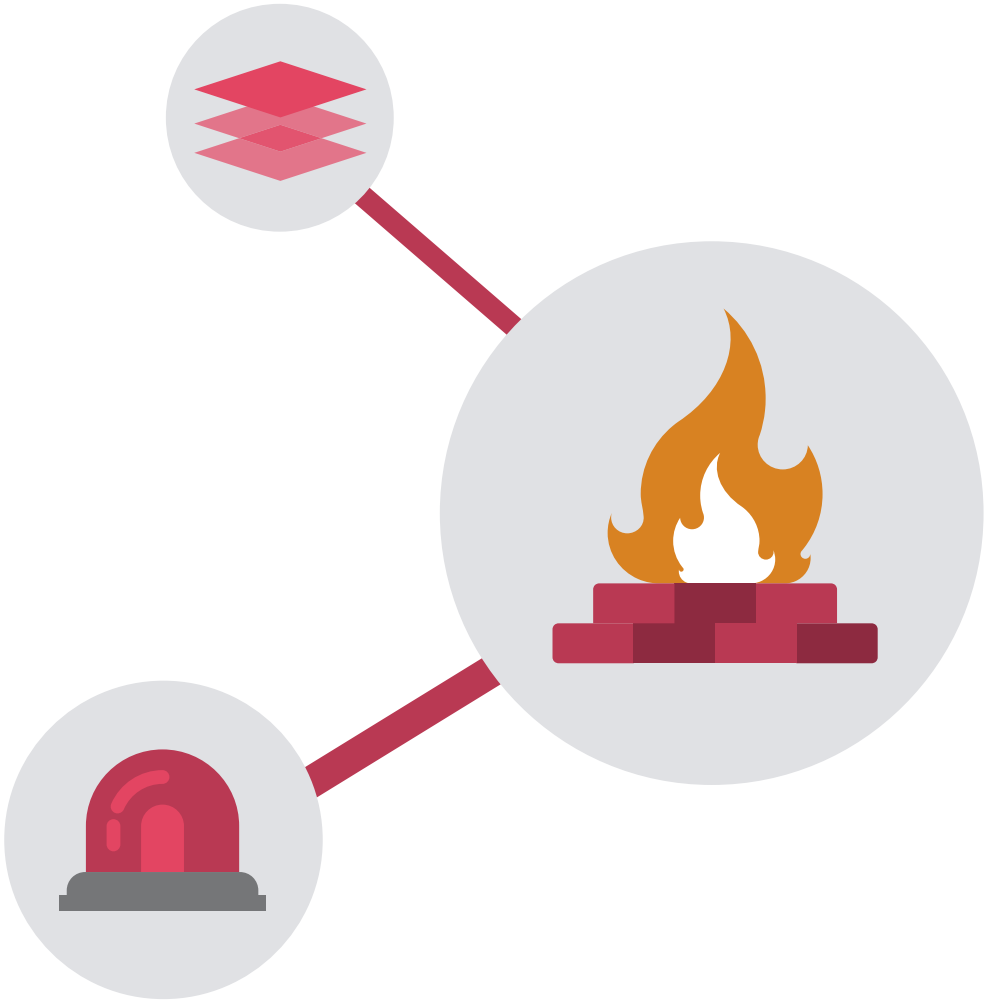
[5]Cercetarea privind securitatea imprimantelor HPI, Spiceworks 2016 [6]Raportul HP din 2015 privind securitatea imprimantelor [7] Raportul Ponemon din 2016 privind starea punctelor finale [8]Evaluarea IBM CISO din 2014 [9]Raportul Ponemon din 2016 privind starea punctelor finale

Implementarea securității la punctul final

Abordarea HP în privința securității la punctul final structurată pe linii de apărare

Abordarea prevenire și protecție în privința securității cibernetice - firewall și antivirus - nu este suficientă. Și nu a fost niciodată suficientă. Conform unui studiu derulat de Damballa, programului antivirus i-au trebuit șase luni pentru a identifica și elimina 100% dintre fișierele rău intenționate cu care a fost atacat.[10]

Opinia HP este că securitatea cibernetică trebuie să fie structurată pe linii de apărare, să opereze la nivel de rețea, dispozitiv și utilizator, cu mai multe mecanisme de apărare pentru fiecare nivel. Detectarea și răspunsul trebuie să prevaleze asupra protecției și a apărării. Iar punctele finale sunt punctul de începere: atât la nivel de dispozitiv, cât și la nivel de utilizator.



Controale esențiale de securitate (CES)

Center for Internet Security (Centrul pentru Securitatea pe Internet, CIS) a definit 20 de controale esențiale de securitate (CES) recunoscute la nivel internațional și dezvoltate, rafinate și validate de experți de marcă în securitatea IT de pe glob. Acestea sunt considerate acțiuni importante de „igienă cibernetică” pentru fiecare organizație.

Am indicat principalele CES-uri din perspectiva respectării prevederilor RGPD, deoarece ele reprezintă îndrumări utile, însă textul complet este disponibil online. Descărcați gratuit din biblioteca CIS.

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

Securitatea în rețea

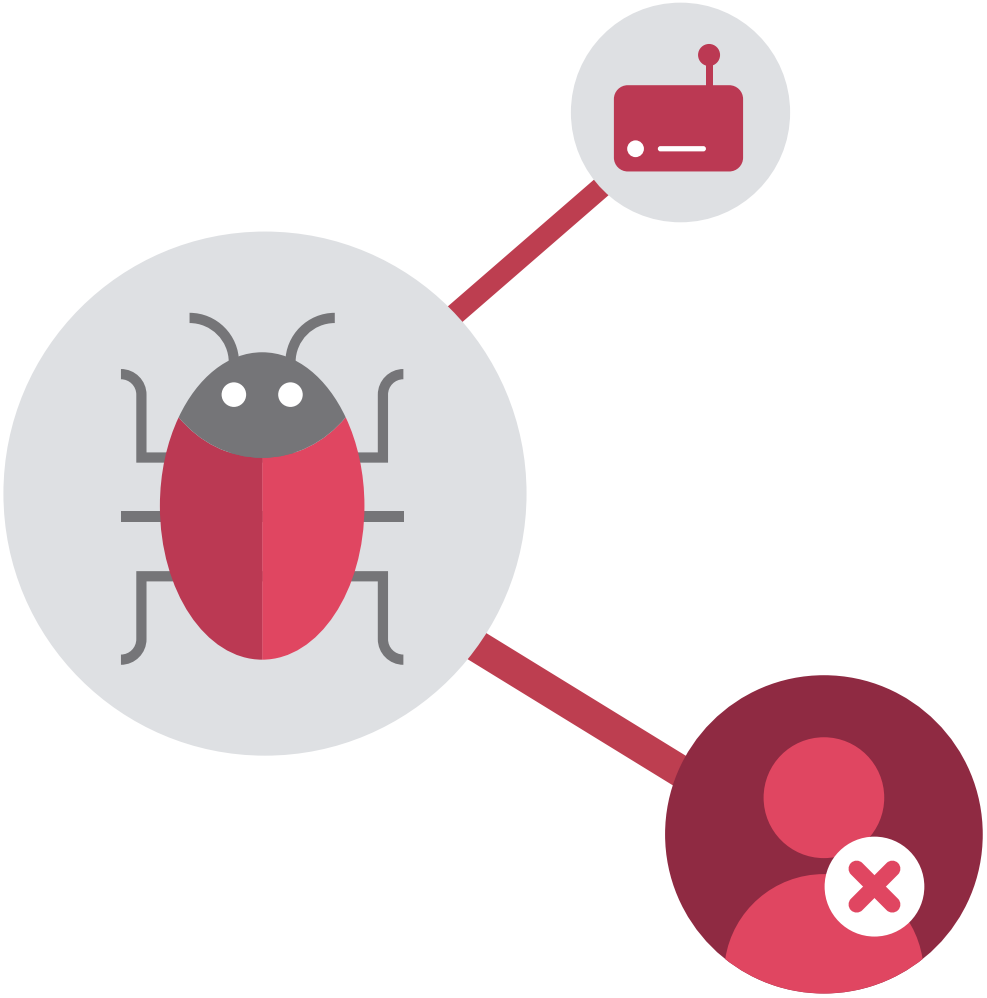
Intruziunile majore tind să exploateze un singur punct de intrare, pentru a obține acces la o rețea întreagă. Securitatea la nivel de rețea trebuie, așadar, să aibă la bază prevenirea acestei situații.

- **Controlul privilegiilor administrative (CES 5)**
  Restricționarea capacității de a schimba setările și parolele de rețea la cât mai puține persoane posibil
- **Controlul accesului pe baza principiului necesității de a cunoaște (CES 14)**
  Accesul în funcție de nivel la informații sensibile despre utilizator, dispozitiv și locație. Cântărirea riscului de securitate în funcție de gradul de confidențialitate a datelor
- **Limitarea și controlul porturilor, a protocoalelor și a serviciilor de rețea (CES 9)**
  Închiderea oricăror puncte de acces care nu sunt necesare - virtuale și fizice - inclusiv FTP, Telnet și servicii de imprimare
- **Întreținerea, monitorizarea și analiza jurnalelor de audit (CES 6)**
  Analiza regulată a jurnalelor de audit din perspectiva comportamentului sistemelor și în vederea detectării oricăror activități suspecte
- **Evaluarea continuă a vulnerabilității și remedierea acesteia (CSC 4)**
  Evaluarea continuă a mediului din punct de vedere al vulnerabilității și întreprinderea de acțiuni de remediere în funcție de rezultate, minimizând oportunitatea producerii de breșe de securitate

Obiectivul constă în realizarea unei rețele împărțite în funcție de gradul de confidențialitate a informațiilor. Cererile de acces sunt evaluate din punct de vedere al riscurilor de securitate. Dispozitivele, utilizatorii și solicitările care nu sunt recunoscute și care provin din rețele nesecurizate sunt blocate, pentru cele mai sensibile informații. Politica BeyondCorp instituită de Google reprezintă un model bun.[11]

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

Securitatea în rețea



Fiecare dispozitiv reprezintă o potențială vulnerabilitate, indiferent dacă este profesională sau personală. Trebuie să cunoașteți fiecare telefon, tabletă, laptop și desktop care are acces la datele firmei.

- **Inventarul dispozitivelor autorizate și neautorizate (CES 1)**
  Auditarea fiecărui dispozitiv care are acces la date
- **Inventarul software-ului autorizat și neautorizat (CES 2)**
  Auditarea fiecărei aplicații folosite în rețea pentru a accesa sau nu date în mod direct
- **Instrumente de apărare împotriva programelor malware (CES 8)**
  Asigurați-vă că fiecare dispozitiv are protecție actualizată antivirus și malware. Realizați scanări și actualizări regulate

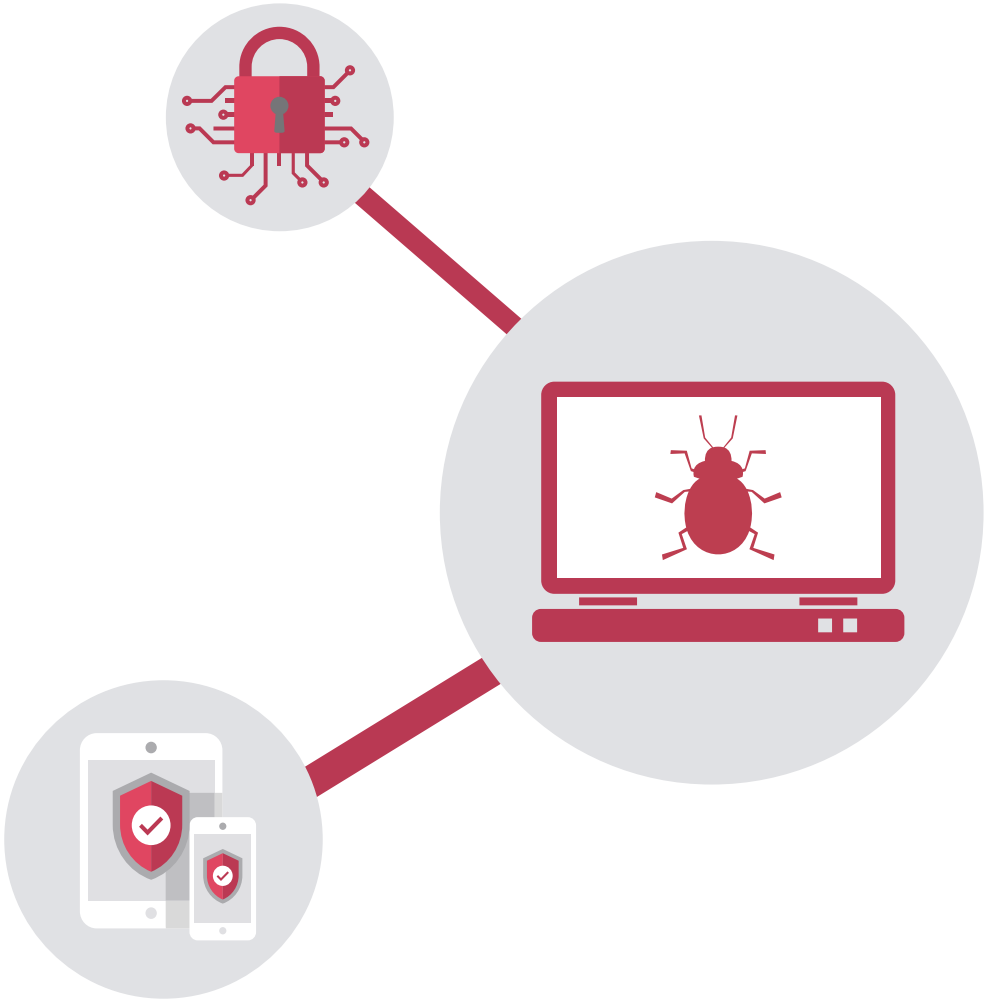
Securitatea dispozitivului

De asemenea, departamentele IT trebuie să ia în considerare și aceste verificări suplimentare:

- **autentificarea multifactorială**
  Asigurați-vă că fiecare dispozitiv profesional este securizat. În mod ideal, folosiți autentificarea biometrică împreună cu parolele (a se vedea pagina 14, „Dispozitive cu mecanisme de securitate a datelor din proiectare”)
- **acces la distanță**
  Asigurați accesul la distanță la dispozitive, pentru recuperarea sau ștergerea datelor cu caracter personal, pentru introducerea în carantină și stoparea proceselor și pentru oprirea și blocarea dispozitivului în cazul în care este pierdut sau furat (a se vedea pagina 14, „Detectare și răspuns”)
- **informați fiecare angajat cu privire la protocoalele și procedurile de securitate**
  Asigurați-vă că fiecare angajat își cunoaște responsabilitățile în domeniul securității cibernetice, inclusiv semnalarea activităților suspecte
- **derulați sesiuni de instruire pe tema securității cibernetice**
  Organizați ateliere, seminarii, precum și exerciții practice privind activitățile de phishing și asigurați-vă că toți angajații știu cum să evite greșelile de bază și cum să mențină conformitatea cu RGPD
- **minimizați utilizarea de dispozitive/aplicații personale**
  Descurajați utilizarea dispozitivelor și a aplicațiilor personale în scop profesional. O politică CYOD exhaustivă și flexibilă ar trebui să fie utilă.

  Implementarea unui cadru de securitate precum acesta ar trebui să vă ajute să păstrați controlul asupra dispozitivelor companiei, să protejați datele și să facilitați aplicarea portabilității datelor și a dreptului de a fi uitat.

  Pentru mai multe informații despre abordarea HP în privința securității structurată pe linii de apărare, citiți raportul nostru, Securitatea începe la punctul final.



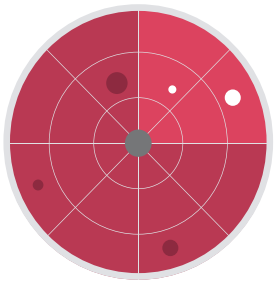
De ce fiecare angajat trebuie să cunoască aspectele cibernetice

58% dintre amenințările cibernetice provin de la angajați, foști angajați și parteneri de încredere.[12] Securizarea fiecărui dispozitiv înseamnă și securizarea utilizatorului său.

- Comisia Națională Democratică din S.U.A. (DNC) a făcut obiectul unei intruziuni în 2016, când John Podesta a făcut clic pe un link de phishing care fusese considerat în mod greșit a fi fost legitim de unul dintre consilierii săi[13]
- Fotografii nud cu celebrități au inundat internetul în 2014, după ce Ryan Collins, în vârstă de 36 de ani, a obținut acces la sistemele iCloud ale lui Jennifer Lawrence și ale altor persoane, trimițând e-mailuri phishing foarte simple, care păreau a fi adresate de Apple[14]
- În 2012 au fost sustrase 68 de milioane de parole Dropbox, din cauza unui angajat care folosea aceeași parolă pentru sistemele interne și pentru contul său de LinkedIn[15]
- Președintele Donald Trump continuă să folosească un telefon standard Samsung Galaxy. Experții nu se mai întreabă dacă a fost accesat neautorizat, ci mai degrabă câte servicii de informații străine au făcut acest lucru[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

Detectare și răspuns

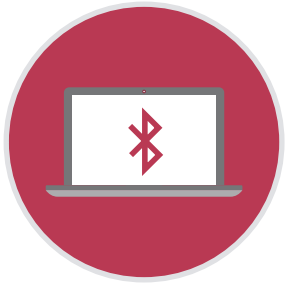


Detectarea și răspunsul reprezintă un cadru de securitate cibernetică ce recunoaște faptul că prevenția totală este aproape imposibilă.

Ceea ce contează este identificarea breșei (detectare) și întreprinderea unei acțiuni imediate (răspuns).

Sunt disponibile produse software care transformă fiecare dispozitiv într-un senzor în timp real și care îi permit administratorului să răspundă prin, de ex., închiderea dispozitivelor, introducerea în carantină a fișierelor și ștergerea datelor.

Dispozitive cu mecanisme de securitate a datelor instalate din proiectare



Dispozitivele HP materializează principiul confidențialității din proiectare.

Funcționalitățile de securitate includ primul BIOS din lume cu reparare automată, blocare Bluetooth automată - care blochează dispozitivul atunci când vă îndepărtați de el - și ecrane cu confidențialitate integrată.

Aceste funcționalități nu vor asigura independent confidențialitatea cu RGPD, însă cu siguranță vor fi foarte utile în acest sens.

Pregătirea pentru RGPD

Măsuri practice de întreprins acum

RGPD intră în vigoare pe 25 mai 2018. Mai este încă timp să vă pregătiți însă, după cum probabil că știți deja, există foarte multe lucruri de făcut.

Primul pas este să **auditați situația existentă a datelor dvs.** Evaluați unde anume sunt stocate datele dvs., unde sunt copiate și cine are acces la ele. Dacă folosiți soluții în cloud, aflați unde sunt serverele respective și dacă vor respecta prevederile RGPD. Același lucru se aplică pentru orice SaaS sau alte organizații partenere cu care lucrați și cu care partajați date. Aceasta vă va oferi o imagine clară cu privire la amploarea schimbării pentru a o putea respecta.

Concepeți-vă politica privind datele. Includeți proceduri și protocoale detaliate cu privire la locul în care sunt stocate datele, cine anume din afara companiei sau de peste hotare, dacă este vorba despre o multinațională, are acces la ele și cine poate face copii ale acestora. Includeți proceduri pentru recuperarea și ștergerea datelor cu caracter personal. Comunicați acest lucru tuturor persoanelor din companie. Derulați sesiuni de instruire. Subliniați importanța lor.

Concepeți-vă politica de securitate. Creați un nou cadru de securitate cibernetică, care să funcționeze pe baza detectării și răspunsului de la punctul final. Dacă este necesar, revizuiți-vă politica privind dispozitivele. Dacă este necesar, investiți în noi tehnologii. Numai 36% dintre managerii IT consideră că dispun de un buget suficient pentru securitatea la punctul final.[17] Penalitățile RGPD pot în cele din urmă să reprezinte factorul motivant care să suscite interesul cadrelor de conducere.

[17] Raportul Ponemon din 2016 privind situația la punctul final

Pregătirea pentru RGPD

Listă de verificare RGPD

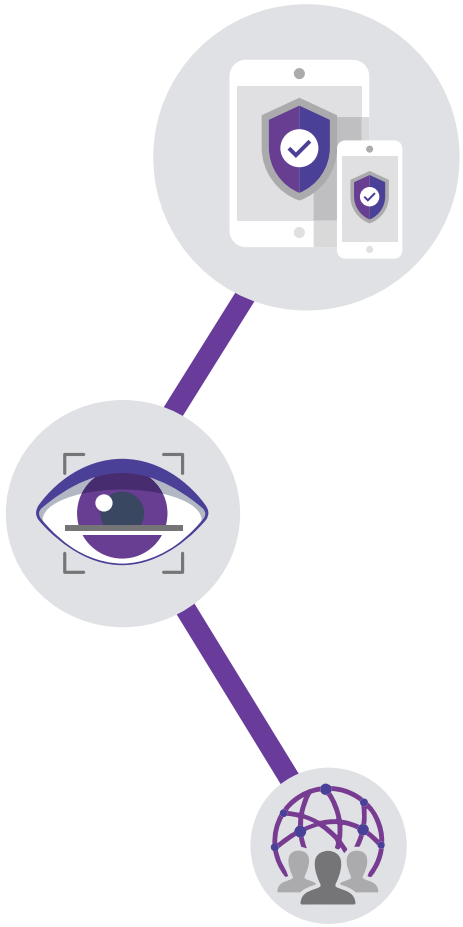
5 pași esențiali către conformitatea cu RGPD

1. Numiți o persoană responsabilă de date, un ofițer pentru protecția datelor (DPO), dacă este necesar
2. Derulați un audit complet asupra datelor, care să includă adecvarea furnizorilor cloud și SaaS cu privire la RGPD
3. Creați un nou cadru de administrare a datelor, care să includă proceduri pentru portabilitatea datelor și dreptul de a fi uitat
4. Creați un nou cadru de securitate cibernetică, implementând o securitate la punctul final structurată pe linii de apărare
5. Comunicați politicile și protocoalele către toate persoanele din companie

Listă de verificare privind securitatea dispozitivelor

6 măsuri esențiale pentru securizarea punctelor finale

1. Auditați toate dispozitivele autorizate și neautorizate cu acces la date cu caracter personal
2. Investiți în dispozitive noi - mai securizate - dacă acest lucru este necesar
3. Implementați drepturi de acces și ștergere la distanță pentru datele companiei aflate pe dispozitive
4. Implementați o politică privitoare la scanările regulate și actualizările software de securitate
5. Implementați un software de detectare și răspuns în timp real
6. Instruiți angajații în domeniul securității cibernetice



Calendar de securitate la punctul final

O planificare temporală de bază pentru implementarea securității la punctul final în conformitate cu RGPD

2017

Mai

Numirea unui manager de proiect care să implementeze instrumente de securitate la punctul final

Iunie

Derularea unui audit asupra politicilor, practicilor și dispozitivelor de securitate existente

Iulie

Analizarea cerințelor și a politicii privind dispozitivul, pentru securitatea la punctul final (CYOD/BYOD etc.)

August

Analizarea soluțiilor software pentru detectarea și răspunsul la problemele de securitate

Septembrie

Conceperea unui sistem de acces în mai multe straturi, structurat pe niveluri, pentru accesul la datele companiei

Octombrie

Crearea unui cloud public/privat pentru a permite accesul adecvat la date din afara sediului

Noiembrie

Conceperea unui program de instruire pentru utilizator, care să includă cu regularitate exerciții practice despre phishing

Decembrie

Comunicarea noilor politici de securitate către restul angajaților din companie

2018

Ianuarie

Implementarea unei noi arhitecturi de date în cadrul sistemului cloud public/privat

Februarie

Implementarea noii politici privind dispozitivele

Martie

Implementarea soluției software de detectare și răspuns

Aprilie

Derularea instruirii utilizatorilor pe probleme de securitate, inclusiv în privința politicilor privitoare la RGPD

Mai

RGPD intră în vigoare

Rezumat

RGPD este aproape

Dacă aveți noroc, organizația dvs. a pus deja în practică multe prevederi din acest regulament, care este, în mare parte, o reducere la esențial a bunelor practici.

Și, dacă ați lucrat în mai multe state UE, probabil că ați întâlnit deja unele dintre măsurile cele mai stricte pe care le conține.

Măsurile de securitate pe care vă recomandăm să le instituiți pentru a respecta prevederile RGPD sunt măsuri care ajută la prevenirea oricăror breșe, breșe ce pot fi foarte costisitoare pentru o organizație. Conform ultimei estimări, guvernul britanic a constatat că firmele britanice au pierdut 21 de miliarde GBP într-un singur an, cifră care se anticipează că va crește.[18]

De asemenea, multe dintre măsurile necesare pentru a avea o securitate cu adevărat robustă vor ajuta de asemenea la respectarea altor aspecte ale RGPD. Restricționarea accesului la date, care va fi permis numai anumitor utilizatori, dispozitive și rețele nu numai că va minimiza riscul cu privire la date, ci va fi mai ușor să urmăriți datele cu caracter personal - și, prin urmare, să respectați prevederile privind portabilitatea datelor și dreptul de a fi uitat; ca să nu mai menționăm transferurile internaționale.

Acest ghid electronic reprezintă doar începutul. Securitatea a fost întotdeauna o prioritate pentru HP. Securitatea datelor instalată din proiectare a fost politica noastră timp de ani la rând. Acum că este obligatorie, mai degrabă decât dezirabilă, ne aflăm într-o postură bună pentru a vă ajuta să adoptați aceeași abordare.

Pentru a afla mai multe despre modul în care HP și produsele noastre vă pot ajuta să respectați RGPD, vizitați **pagina noastră Securitatea datelor instalată din proiectare.**

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