

ICO Information Commissioner's Office

Pse kodimi është i rëndësishëm për sigurinë e të dhënave

Ruajtja e çdo informacioni personal paraqet dhe risk. Duke e regjistruar atë, ju rrezikoni ta humbisni, dhe kjo mund të irrirojë individë të caktuar. Por shpesh, në qoftë se ju nuk keni të ruajtur të dhënat personale, ju nuk mund të ofroni shërbimin e duhur. Dhe kjo gjithashtu mund të bezdis shume individë.

Kjo është arsyeja pse, nëse ju jeni duke mbledhur informacion personal, ju duhet të siguroheni që po kujdeseni për të në mënyrën e duhur.

Që të mbronni këtë informacion në mënyrë efektive duhet të ndërmerren disa masa për të reduktuar rrezikun e përhapjes së tij. Duke pasur parasysh dhe faktin se një sasi e madhe e të dhënave tani mund të mbahet në pajisje të vogla si smartphone ose tablet PC, ekziston rreziku real që informacioni personal mund të komprometohet nëse një pajisje e tillë humbet ose vidhet.

Në këto rrethana, përdorimi i një kodimi të përshtatshëm mund të jetë një masë e thjeshtë dhe efektive për të mbrojtur të dhënat personale, dhe marrjen e një mase të tillë ne jua këshillojmë të gjithë organizatave, në rast se humbja e të dhënave do të shkaktonte dëme individëve të prekur. Megjithatë, provat tregojnë se kontrolluesit e të dhënave nuk e kanë adresuar ende këtë problem.

Ky artikull ka për qëllim informimin tuaj për mënyrën se si kodimi funksionon dhe opsionet për implementimin e tij në dispozicion të organizatës tuaj, për t'ju ndihmuar të mbani të dhënat personale të sigurta.

Keqkuptimi i madh

Le të sqarojmë diçka që në fillim. Një keqkuptim i zakonshëm është që nëse përdoruesit aksesojnë një pajisje, apo shërbim, me një emër dhe fjalëkalim kjo siguron një nivel të barasvlershëm mbrojtjeje me kodim. Ky nuk është rasti. Një fjalëkalim ose PIN për të kontrolluar aksesin në një pajisje nuk është kodim dhe është e pamjaftueshme për tu mbrojtur kundër aksesit të paautorizuar ose të paligjshëm. Në praktikë një fjalëkalim mund të anashkalohet lehtësisht dhe në këtë mënyrë të arrihet akses i plotë në të dhënat.

Si funksionon kodimi?

Programet për kodim përdorin një seri komplekse algoritmesh matematikore për të mbrojtur dhe koduar informacionin. Kjo fsheh të dhënat bazë dhe parandalon akses të rastësishëm, ose përhapje të paautorizuar të informacionit. Kjo do të thotë se edhe nëse një pajisje që përmban të dhëna personale humbet apo vidhet, informacioni do të mbetet i sigurt për aq kohë sa nuk disponohet edhe çelësi përkatës i kodimit për të thyer algoritmin. Produkte të përshtatshme për kodim janë gjerësisht të disponueshme, por është e rëndësishme që organizatat (kontrolluesit) të kuptojnë llojin e mbrojtjes që një produkt i veçantë për kodimin ofron dhe rrethanat nën të cilat të dhënat personale do të mbrohen nga aksesit i paautorizuar ose i paligjshëm.

Çfarë programi kodimi duhet të përdor?

Ka një shumëllojshmëri mundësish në dispozicion. Përcaktimi opsionit që do të jetë më i përshtatshëm për organizatën tuaj varet nga ndryshmëria e informacionit që ju jeni duke përdorur dhe mënyra se si ky informacion ruhet dhe përpunohet.

Për këtë arsye është e vështirë që të përcaktohet një listë e plotë e këtyre programeve pasi kërkesat e gjithsecilit janë të ndryshme. Megjithatë ju mund të shikoni për standartet e njohura ndërkombëtare si ato të përshkruara në [seksionin e kodimit](#) në faqen tonë të internetit.

Kodimi i plotë i diskut

Ky është një proces i cili kodon të tërë diskut, duke përfshirë të gjitha të dhënat personale dhe informacionin që ai përmban. Përdoret zakonisht për kodimin e laptop-eve, desktop PC dhe pajisjeve të lëvizshme, të tilla si celular dhe tableta. Disku duhet të ç'kodohet me një çelës, i cili shpesh është i mbrojtur nga një fjalëkalim i vendosur nga përdoruesi, para se sistemi operativ të ngarkohet.

Megjithatë, ka rrethana kur të dhënat ende mund të jetë në rrezik. Për shembull, nëse dikush lë një tabletë të hapur dhe të pambikëqyrrur në një restorant, atëherë kushdo që merr këtë pajisje do të ketë fillimisht një mundësi për nxjerrjen e të dhënave të pambrojtura. Është gjithashtu e rëndësishme që të kuptohet se nëse një skedar transferohet jashtë diskut, për shembull në qoftë se ju e dërgoni informacionin me një email ose e ruani atë në një pajisje tjetër, atëherë skedari nuk do të jetë më i koduar.

Kodimi i plotë i diskut ofrohet nga një gamë e gjerë programesh dhe sistemet operative të fundit kanë një opsion kodimi të inkorporuar, por është vetë përdoruesi që do të duhet ta aktivizojë fillimisht këtë opsion.

Kodimi i skedarëve të veçantë

Ky është një proces që kërkon kodimin e një skedari të veçantë ose krijimin e një mbajtësi të kodur skedarësh, në të cilin mund të vendosen skedarë të tjerë. Kur ky mbajtës-skedarësh mbyllet, bëhet dhe i koduar. Kjo do të thotë se në rastin kur ky mbajtës-skedarësh transferohet në një pajisje tjetër, psh nëse dërgohet me email apo ruhet në një disk USB, të dhënat personale (skedarët e veçantë brenda mbajtësit) mbeten të koduar. Megjithatë skedarët e veçantë nuk janë më të koduar nëse ruhen jashtë këtij mbajtësi.

Disa sisteme operative moderne janë në gjendje për të krijuar mbajtës-skedarësh të koduar, por dhe një numër i madh programesh të tjera gjithashtu mund të ofrojnë të njëjtin nivel kodimi. Megjithatë është e rëndësishme të kuptohet që kjo teknikë kodimi nuk është e njëjtë me mbrojtjen me fjalëkalimin të një skedari apo dosjeje, proces i cili nuk realizon kodimin e të dhënave.

Shumica e programeve për dërgim email, gjithashtu mbështesin dërgimin e mesazheve email me përmbajtje mesazhi apo skedarë të bashkangjitur në një format të koduar. Megjithatë për një rast të tillë duhen realizuar disa konfigurime fillestare tek programi-email i dërguesit dhe marrësit.

Kodimi i të dhënave gjatë transferimit të tyre

Është gjithashtu e rëndësishme të kuptohet dallimi mes teknikave të kodimit të përdorura për ruajtjen e të dhënave dhe teknikave të kodimit të përdorura në transferimin e të dhënave.

Ju mund të transferoni të dhëna duke përdorur një protokoll të koduar transferimi të dhënash, të tillë si *Secure Sockets Layer (SSL)* ose *Transfer Layer Security (TLS)*. Kjo është teknologjia që qëndron pas simbolit të drynit të kyçur që shfaqet kur hapim disa faqe në Internet. Ajo na ofron sigurinë që komunikimi ndërmjet klientit dhe serverit nuk mund të kontrollohet. Për më tepër ajo është një mjet për të vërtetuar se ku të dhënat janë duke u transferuar.

Përdorimi i një protokollit të koduar nuk ofron asnjë garanci që e dhëna do të mbetet e koduara, ose do përpunohet në mënyrë të sigurt, pasi ajo të mbërrijë në destinacionin. Kjo do të duhet të vlerësohet më tej.

Rëndësia e mbajtjes sekretit të çelësit

Nëse ju instaloni një sistem modern sigurie për shtëpinë tuaj, nuk do kishte kuptim të fshihnit çelësin e derës kryesore dikur pranë hyrjes. E njëjta gjë vlen edhe për ruajtjen e një çelësi kodimi apo fjalëkalimi për laptop në të njëjtën çantë me laptop-in, ose, të dërgonit të dhëna të koduara me një e-mail dhe të përfshinit në brendësi të email-it edhe çelësin për ç' kodimin.

Nëse ju veproni si më sipër atëherë garancitë e ofruara nga akti i kodimit bëhen të paqena, sepse të gjithë informacionin e kërkuar për të ç' koduar të dhënat e gjejmë po aty. Prandaj mbajtja e fshehtë e çelësit të përdorur për kodimin e të dhënave është e një rëndësie të madhe.

Për të siguruar nivelin maksimal të mbrojtjes së ofruar nga procesi kodimit, çelësi apo fjalëkalimi duhet të transmetohet duke përdorur mjete alternative komunikimi. Për shembull të dhënat e koduara mund të dërgohen me email dhe pasi marrësi i parashikuar të ketë konfirmuar marrjen me sukses të tyre, çelësi ti komunikohet përmes telefonit. Në këtë mënyrë, edhe në qoftë se ju aksidentalisht dërgoni të dhënat tek marrësi i gabuar, informacioni do të mbetet i sigurt, pasi ky marrës nuk e disponon çelësin.

Dhe në fund ...

Ndërsa kodimi tingëllon si një mjet i komplikuar për të mbrojtur të dhënat personale sensitive, aspekt i rëndësishëm është të identifikojmë formën më të përshtatshme të kodimit dhe të ndjekim një strategji të arsyeshme për të mbajtur çelësin, dhe rrjedhimisht të dhënat, të sigurt. Përdorimi i një kodimi efektiv është zakonisht më i përshtatshëm se sa adoptimi i mjeteve alternative për të ofruar një nivel të ngjashëm sigurie për të dhënat.

Koha dhe kostoja për kodim është sot e arsyeshme, po të kihet parasysh gjobat e vendosura (£700,000 në total) në tre raste të fundit të shqyrtuara ku kodimi nuk përdorej. Pra çmimi i paguar në këtë rast tejkalon thjesht mërzitjen e individëve që u cënohen të dhënat...

Simon Rice
28 Gusht 2013