The experts in screen privacy.

Voorbereiding op de algemene verordening gegevensbescherming Veelgestelde vragen

Enza Iannopollo, Forrester Research

Enza is een analist van het team 'beveiliging en risico's' en een Certified Information Privacy Professional (CIPP/E). Bij Forrester neemt zij gegevensbescherming, privacy en het internet voor haar rekening, met speciale nadruk op voorschriften en de technologieën die daaraan ten grondslag liggen.

De algemene verordening gegevensbescherming vormt één van de belangrijkste wijzigingen in de voorschriften inzake gegevensbescherming in 20 jaar. Deze stelt hoe organisaties de persoonlijke gegevens van hun klanten, medewerkers, en bedrijfspartners moeten hanteren, op een voortdurende basis. 3M had onlangs een bijeenkomst met Enza Iannopollo van Forrester Research om de beveiligingsmaatregelen, beleidslijnen en programma's voor de naleving van privacy te bespreken die door veel organisaties worden ingevoerd om te voldoen aan voorschriften zoals de algemene verordening gegevensbescherming. Enza gaf inzicht in de werkomgeving en benadrukte het belang van fysieke beveiligingsmaatregelen voor de privacy van gegevens.

Wat staat er op het spel?

Organisaties kunnen boetes ontvangen tot 4% van de jaarlijkse omzet of

€20 miljoen

Dit is wat ze zei:

V. Is het personeel erop voorbereid om te voldoen aan de algemene verordening gegevensbescherming?

A. Volgens onze gegevens is slechts één op de drie bedrijven wereldwijd voorbereid op de naleving van de algemene verordening gegevensbescherming (GDPR; General Data Protection Regulation). Aangezien deze verordening op 25 mei 2018 ingaat, is het helder dat veel organisaties snel moeten werken om hun voorbereidingen af te ronden.

Wij hebben gemerkt dat bedrijven vooral moeite hebben met de vereiste om training en bewustzijnsprogramma's over privacy in te voeren en te documenteren. Regelgevers van de EU hebben aangegeven dat deze programma's essentieel zijn voor de naleving van de algemene verordening gegevensbescherming. Wij hebben ook gezien dat organisaties die aan deze vereiste voldoen hun privacy-cultuur in het bedrijf hebben verbeterd en best practices hebben ingevoerd die soms de vereisten van de voorschriften te boven gaan.

V. Zijn bedrijven in bepaalde regio's beter voorbereid dan in andere?

A. 34 procent van de Amerikaanse bedrijven zegt dat het voorbereid is, vergeleken met 26 procent van de bedrijven in Europa.[1] Bedrijven die niet voldoen aan de algemene verordening gegevensbescherming nemen een groot risico, of zij dit nu weten of niet. Bedrijven die denken dat ze voorbereid zijn, maar die het niet zijn, nemen een nog groter risico.

Het is interessant om te zien dat meer bedrijven in de V.S. denken dat ze voorbereid zijn dan in Europa. Dit heeft te maken met het feit dat de algemene verordening gegevensbescherming in het buitenland speelt. De Verordening geldt voor alle bedrijven, ongeacht hun locatie, die persoonlijke gegevens verwerken of bewaren van inwoners van de

Europese Unie. Dit betekent dat niet alleen Europese bedrijven, maar ook veel bedrijven met hun hoofdkantoor in de V.S., vereist zijn om te voldoen aan deze strenge privacy-regels.

Wij denken dat veel van de bedrijven de regels niet goed hebben doorgenomen of denken dat de naleving van de algemene verordening gegevensbescherming niet zo nauw zal worden genomen.

V. Welke fysieke beveiligings- en privacy-maatregelen worden voorgeschreven door de algemene verordening gegevensbescherming?

A. De algemene verordening gegevensbescherming is op principes gebaseerd. Dit betekent dat de regelgevers geen definitieve acties voorschrijven. In plaats daarvan moeten de organisaties nadenken over de vereisten van de algemene verordening gegevensbescherming als een soort 'ideale toestand' voor de verwerking van gegevens. Het betekent tevens dat organisaties specifieke risico's moeten identificeren en beoordelen die zij moeten beperken om te voldoen aan de algemene verordening gegevensbescherming.

De bedrijven moeten de risico's in verband met de verwerking van gegevens identificeren, met name als gevolg van accidenteel of onrechtmatig verlies van en de onbevoegde vrijgave of toegang tot de persoonlijke gegevens die worden verzonden, opgeslagen en verwerkt. Het doet er niet toe of zo'n onbevoegde vrijgave van gegevens het gevolg is van een geraffineerde aanval op de website van een bedrijf door een hacker of van een foto die door een vreemde wordt genomen van zeer gevoelige gegevens op de laptop van een medewerker. Beide zijn even ernstige risico's en vereisen passende strategieën om ze te beperken.

V. Vormt visueel hacken een risico?

A. Absoluut. Denk eraan: Bij veel organisaties zijn de gebruikersnaam en wachtwoord de sleutel tot het koninkrijk. Met een korte blik op een onbeschermd scherm kan een onbevoegde deze sleutel krijgen en dus toegang. En met de groeiende complexiteit van social engineering groeien ook de risico's.

Een jaar geleden werd een journalist in een vliegtuig aangevallen door een hacker.[2] De hacker was in staat om de details te geven van een artikel die de journalist aan het schrijven was, van persoonlijke e-mails die hij had verstuurd, en van komende vergaderingen op zijn werk. Hij zij dat hij die via de wifi in het vliegtuig had bemachtigd. Of misschien had de hacker ze simpelweg gezien op het scherm van de laptop van de journalist. De journalist was woedend, maar hij begreep het: terwijl hij aan een gevoelig artikel zat te werken, in dit geval het ontleden van de diepgaande en verreikende gevolgen op de privacy van het feit dat Apple niet was ingegaan op het verzoek van de FBI om de telefoon van een terrorist te decoderen, vergat hij om de privacy en het intellectuele eigendom van zijn eigen apparaat te beschermen. Net als die journalist maken veel organisaties de fout dat ze het risico van cyber en visueel hacking onderschatten.

V. Wat zijn de voordelen van het invoeren van laagtechnologische fysieke veiligheidsmaatregelen?

A. Met de constante verhalen in het nieuws over grootschalige inbreuk op de gegevensbescherming is het gemakkelijk om te vergeten dat de digitale bedrijven van nu ook nog aan fysieke beveiliging moeten denken. Het invoeren van fysieke veiligheidsmaatregelen, zoals videocamera's voor bewaking, sloten op laptopkoffers en

privacy-filters voor monitors, laptops, tablets en smartphones, heeft meerdere voordelen. Privacy-filters verschaffen bijvoorbeeld een gedegen beperking van het risico van aanvallen op de privacy en gegevens. Als gevoelige gegevens van een klant of medewerker aan de verkeerde persoon worden blootgesteld, kan dit leiden tot een zeer nadelige en veel gepubliceerde inbreuk.

Zij kunnen tevens de naleving van andere voorschriften dan die van de algemene verordening gegevensbescherming ondersteunen. Een medisch assistent werd bijvoorbeeld een paar jaar geleden uit een ziekenhuis op de universiteit van Iowa ontslagen voor overtreding van de regels inzake de privacy

van gegevens van patiënten. Zij werd beschuldigd van het visueel hacken van een medewerker die de medische gegevens van een patiënt bekeek, wat een overtreding van de HIPAA is.[3]

Fysieke veiligheidsmaatregelen, zoals privacy-filters, kunnen de medewerkers er tevens aan herinneren dat de beste praktijken inzake de privacy een prioriteit zijn voor de organisatie. En zoals altijd gaat het bij visuele privacy niet alleen om het voldoen aan de vereisten. Het gaat erom dat de meest waardevolle activa van het bedrijf worden beschermd.

V. Hoe kunnen bedrijven van privacy gebruik maken om klanten een betere ervaring te geven?

A. Bedrijven die robuuste programma's inzake de algemene verordening gegevensbescherming en de privacy in positie hebben, merken een aantal voordelen die de naleving nog te boven gaan. Een betere ervaring aan de klant geven, is één daarvan. De manier waarop uw organisatie de gegevens van uw klanten beschermt, kan een directe invloed hebben op het vertrouwen dat de klant in u heeft.

Wij weten dat klanten bijvoorbeeld inderdaad naar een concurrent overstappen als gevolg van een inbreuk op de gegevens.[4] Bovendien toont ons onderzoek naar de houding van consumenten t.o.v. de privacy aan dat 30 procent van de mensen geen transacties online willen doen als zij iets in de privacyverklaring van het bedrijf hebben gelezen dat ze niet leuk vinden.[5]

Als u erop gericht bent om de gegevens van uw klanten en medewerkers te beschermen en u van deze toewijding blijk geeft in de communicatie met de klanten, kan dit u onderscheiden van de concurrentie.

23% van de Fortune 100
hebben privacy aangenomen als onderdeel van hun sociale verantwoordelijkheden van het bedrijf (CSR).

V. Zijn er bedrijven die uitblinken door hun toewijding aan privacy en beveiliging?

A. Privacy was vroeger een niche-onderwerp voor juridische afdelingen maar nu vormt het voor veel organisaties een kernwaarde. Nu is de bescherming tegen aanvallen op en de misbruik van gegevens bij veel CIO's, CMO's en andere executives een van de hoogste prioriteiten. Ons onderzoek toont aan dat 23 procent van de Fortune 100 de privacy hebben aangenomen als onderdeel van de sociale verantwoordelijkheden van het bedrijf (CSR).[6] Meer dan 70 procent nam beveiliging op in hun CSR-rapporten.

Wij hebben tevens gemerkt dat bedrijven die toegewijd zijn aan privacy en beveiliging er voordeel bij hebben om open en transparant te zijn over de manier waarop zij met persoonlijke gegevens omgaan. Dit kan een uitermate waardevolle manier zijn om zowel klanten als medewerkers en bedrijfspartners gerust te stellen. Maar het is niet eenvoudig om dit te doen. Vaak moeten organisaties de manier waarop zij werken wijzigen om deze doelstellingen tot leven te brengen en een bedrijfscultuur te scheppen met privacy en beveiliging als kernwaarden.

V. Spelen er nog andere voorschriften dan de algemene verordening gegevensbescherming?

A. Daar bestaat geen twijfel over: De algemene verordening gegevensbescherming geeft een trend aan. Wij hebben onlangs een nieuw stuk onderzoek afgerond dat de privacy-voorschriften en -praktijken van 54 landen analyseert.[7] Het is duidelijk dat regio's zoals Azië/Pacific naar de algemene verordening gegevensbescherming kijken als mogelijke evolutie voor hun eigen privacy-regels. Elementen van de algemene verordening gegevensbescherming, zoals de verblijfplaats van de gegevens, worden ook opgenomen in de privacy-regels in Latijns-Amerika en Rusland. Ten slotte werkt het Europese Parlement nu aan een bijgewerkte versie van de huidige richtlijn inzake ePrivacy. Er wordt nog aan de details gewerkt, maar het plan is om de eprivacy-eisen in lijn te brengen met de algemene verordening gegevensbescherming.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, 'Apple vs FBI shown in different light as journalist hacked mid-flight,' Jan. 25, 2016
[3]Veriphyr 'Medical Assistant Fired for 'Shoulder Surfing' and Breaching Patient Data Privacy,' 2011
[4]Ponemon Institute, 'The Impact of Data Breaches on Reputation and Share Value,' May 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (Part 2), 2016
[6]Rapport van Forrester 'The Future of Data Security and Privacy: Growth And Competitive Differentiation,' 2017

FORRESTER®