3M | The experts in screen privacy.

GDPR-beredskap VANLIGA FRÅGOR

Enza Iannopollo, Forrester Research

Enza är analytiker i säkerhets- och riskteamet och certifierad expert på sekretess (CIPP/E). På Forrester arbetar hon med dataskydd, sekretess, analyser och Sakernas internet, med särskilt fokus på vilken inverkan reglerna och tekniken som stödjer detta har.

GDPR är en av de viktigaste förändringarna gällande regler för dataskydd på 20 år. Den nya förordningen fastställer hur organisationer måste behandla sina kunders, medarbetares och affärspartners personuppgifter. Representanter från 3M satte sig nyligen ned med Enza Iannopollo från Forrester Research för att diskutera vilka skyddsåtgärder, policyer och program för sekretessefterlevnad som många organisationer upprättar i syfte att följa förordningar som GDPR. Enza informerade om beredskap på arbetsplatsen och betonade behovet av fysiska säkerhetsåtgärder som ska förhindra hot mot dataskyddet.

Vilka är riskerna?

Organisationer kan dömas till böter på upp till 4 % av sin årliga totala omsättning eller

20 milj. euro

Hon berättade följande:

Fråga: Är personalen redo att följa GDPR?

Svar: Våra undersökningar visar att endast ett av tre företag i världen är redo att uppfylla kraven i EU:s allmänna dataskyddsförordning (GDPR). Eftersom GDPR träder ikraft den 25 maj 2018 är det tydligt att många organisationer måste agera snabbt för att slutföra sina förberedelser.

Vi ser i synnerhet organisationer som kämpar för att uppfylla kravet på att införa och dokumentera en sekretessutbildning och medvetenhetsprogram för anställda. EU:s tillsynsmyndigheter har meddelat att de här programmen är nödvändiga för efterlevnad av GDPR. Samtidigt vet vi att organisationer som uppfyller det här kravet har förbättrat sina rutiner för sekretess och fastställt en bästa praxis som ibland går längre än lagstadgade krav.

Fråga: Är företag i vissa regioner bättre förberedda än andra?

Svar: 34 procent av de amerikanska företagen uppger att de är redo, jämfört med 26 procent av företagen i Europa.[1] Företag som inte är uppfyller kraven i GDPR – vare sig de inser det eller inte – tar en stor affärsrisk. Företag som felaktigt tror att de är redo tar en ännu större risk.

Det är intressant att fler företag i USA tror att de är redo jämfört med de europeiska företagen. Detta måste bero på den exterritoriala effekten av GDPR. Förordningen gäller alla företag (oavsett var de är baserade) som hanterar eller innehar personuppgifter tillhörande EU-medborgare. Detta innebär att inte bara europeiska företag utan också många företag baserade i USA måste följa dessa strikta sekretessregler.

Vi misstänker att en ytlig genomläsning av reglerna, kombinerat med vilseledande och ogrundade förväntningar på en svag tillämpning av GDPR, kan påverka företagens uppfattning om sin egen beredskap.

Fråga: Vilken typ av fysisk säkerhet och sekretesskydd krävs enligt GDPR?

Svar: GDPR är en principbaserad förordning. Detta innebär att tillsynsmyndigheterna inte tillhandahåller en uppsättning bestämda åtgärder som organisationer ska följa. Istället ska kraven i GDPR ses som ett slags ”önskvärt tillvägagångssätt” vid hantering av personuppgifter. Det innebär också att organisationer ska identifiera och bedöma särskilda risker som de måste åtgärda för att uppfylla kraven i GDPR.

När organisationer identifierar risker måste de i synnerhet ta hänsyn till de risker som rör databehandling: oavsiktlig/olaglig förlust eller obehörigt röjande av personuppgifter och åtkomst till personuppgifter som överförs, lagras eller på annat sätt behandlas. Det spelar ingen roll om obehörigt röjande av personuppgifter beror på att en hackare utför en avancerad cyberattack mot ett företags webbplats eller på att en utomstående tar ett foto på mycket känsliga personuppgifter som visas på en medarbetares bärbara dator. Dessa två exempel är lika allvarliga risker och kräver lämpliga åtgärder som reducerar skadorna.

Fråga: Är visuell hackning en risk?

Svar: Ja, definitivt. Tänk på följande: För många organisationer kommer nyckeln till kungariket i form av ett användarnamn och ett lösenord. Det krävs bara en snabb titt på en oskyddad skärm för att en obehörig person ska få denna nyckel och därmed åtkomst. Och risken ökar i takt med att social manipulation blir alltmer avancerad.

För ett år sedan hackades en journalist som satt och jobbade under en flygresa.[2] Hackaren fick tillgång till information om en artikel som journalisten arbetade med, personliga e-postmeddelanden han hade skickat samt framtida möten. Hackaren uppgav att han fick åtkomst till all denna information genom att hacka flygplanets Wi-Fi. Eller så kanske hackaren helt enkelt fick tag på informationen genom att snegla på skärmen på journalistens bärbara dator. Journalisten var upprörd, men han förstod vad som hade hänt och vad detta innebar: medan han arbetade på en känslig artikel om de omfattande sekretessmässiga konsekvenserna av Apples vägran att låta FBI dekryptera en terrorists telefon glömde han att skydda sekretessen och den immateriell egendomen på sin egen dator. I likhet med journalisten begår många organisationer samma misstag när de underskattar riskerna med cyberattacker och visuell hackning.

Fråga: Vilka är fördelarna med att införa lågteknologiska fysiska säkerhetsåtgärder?

Svar: På grund av återkommande rapporter om stora dataförluster är det lätt att glömma bort att digitala organisationer fortfarande ställs inför fysiska säkerhetsutmaningar. Det finns många fördelar med att använda fysiska säkerhetsmetoder, t.ex. övervakningskameror, lås för fodral till bärbara datorer och sekretessfilter för skärmar, bärbara datorer, surfplattor och smarta telefoner. Sekretessfilter ger till exempel ger ett bra skydd mot kränkning av privatlivet och personuppgiftsincidenter. Allt

som krävs för att drabbas av en mycket skadlig och högst offentlig personuppgiftsincident är att några känsliga uppgifter om kunder eller medarbetare ses av fel person.

Fysiska säkerhetsmetoder kan även bidra till att kraven i andra förordningar än GDPR uppfylls. En läkarsekreterare blev t.ex. uppsagd från ett sjukhus vid University of Iowa för några år sedan för att brutit mot sekretessreglerna för patientuppgifter. Hon anklagades för att visuellt ha hackat en kollega när han läste en patients journal, vilket är en överträdelse av lagen Health Insurance Portability and Accountability Act (HIPAA).[3]

Fysiska skydd som sekretessfilter kan fungera som en visuell påminnelse för anställda om att bästa praxis för säkerhet och sekretess är viktiga prioriteringar för organisationen. Och som alltid med visuell sekretess handlar det inte bara om att uppfylla efterlevnadskraven. Den handlar om att skydda organisationens mest värdefulla tillgångar.

Fråga: Hur kan företag dra nytta av sekretessen för att åstadkomma en god kundupplevelse?

Svar: Företag som inför tillförlitliga GDPR- och sekretessprogram får ett antal affärsfördelar utöver efterlevnad. Tillhandahållande av en högkvalitativ kundupplevelse är en av dem. Det sätt på vilket din organisation skyddar kundernas data kan direkt bidra till att skapa, eller förstöra, den underliggande känslan av tillit som dina kunder har till din organisation.

Vi vet till exempel att kunderna byter till en konkurrent till följd av en sekretessöverträdelse.[4] Vår undersökning av konsumenters inställning till sekretess visar dessutom att 30 procent av alla konsumenter väljer att inte slutföra en transaktion på internet om de läser något som de inte gillar i företagets sekretesspolicy.[5]

23 % av företagen på Fortune 100-listan

har inkluderat sekretess som en del av företagets sociala ansvar (CSR).

Om du lägger stor vikt vid att skydda dina kunders personuppgifter och dina medarbetare vidkänns och uppvisar detta engagemang när de interagerar med kunderna kan det bidra till att du står ut från konkurrenterna.

Fråga: Finns det några företag som sticker ut vad gäller deras åtagande för sekretess och säkerhet?

Svar: Sekretess har gått från att vara ett ämne enbart för juridiska avdelningar till att vara ett kärnvärde för många organisationer. I dag tillhör IT-chefer och marknadschefer de personer på ledande befattningar som anser att en av deras viktigaste prioriteringar är att skydda datatillgångar från angrepp och otillbörlig användning. Vår forskning har visat att 23 procent av företagen på Fortune 100-listan har sekretess som en del av sitt sociala ansvar (CSR).[6] Ungefär 70 procent av företagen inkluderade säkerhet i sina CSR-rapporter.

Vi upptäckte också att företag som lägger stor vikt vid sekretess och säkerhet drar fördel av att vara öppna med hur de hanterar personuppgifter. Detta kan vara ett ytterst värdefullt sätt att få kunder, anställda och affärspartners att känna sig trygga. Att agera enligt detta åtagande är dock inte enkelt. Organisationer måste i många fall ändra sitt arbetssätt för leva upp till dessa åtaganden och skapa en företagskultur där sekretess och säkerhet är kärnvärden.

Fråga: Är fler förordningar som GDPR på gång?

Svar: Ja, det råder det ingen tvekan om: GDPR är en del av en trend. Vi har nyligen slutfört en ny studie som analyserar metoder och regler för sekretess i 54 länder.[7] Det är tydligt att regioner som till exempel Asien-Stillahavsområdet ser på GDPR som en potentiell utveckling av lokala sekretessregler. Delar av GDPR, såsom datalokalisering, håller också på att införas i regler om datasekretess i Latinamerika och Ryssland. Europaparlamentet är nu dessutom på väg att uppdatera kraven i direktivet om integritet och elektronisk kommunikation. Detaljerna återstår att utformas, men planen är att anpassa kraven i direktivet om integritet och elektronisk kommunikation till GDPR.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, ”Apple vs FBI shown in different light as journalist hacked mid-flight”, 25 januari 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,” maj 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (Part 2), 2016
[6]Forrester Report ”The Future of Data Security and Privacy: Growth And Competitive Differentiation”, 2017
[7]Forrester ”Interactive Data Privacy Heat Map”, 2017

FORRESTER®