3M | The experts in screen privacy.

GDPR-beredskab Ofte stillede spørgsmål

Enza Iannopollo, Forrester Research

Enza er analytiker på Security & Risk-teamet og Certified Information Privacy Professional (CIPP/E). Hos Forrester er hun ansvarlig for databeskyttelse, beskyttelse af privatlivets fred, analytik og IoT med fokus på indvirkningen af forordninger og de teknologier, der underbygger dem.

GDPR er en af de vigtigste ændringer i databeskyttelseslovgivningen i 20 år. Den fastlægger, hvordan organisationer løbende skal håndtere deres kunders, medarbejderes og forretningspartneres personoplysninger. 3M mødtes for nylig med Enza Iannopollo fra Forrester Research for at drøfte de sikkerhedsforanstaltninger, politikker og databeskyttelsesprogrammer, som mange organisationer indfører for at overholde forordninger som GDPR. Enza gav indsigt i beredskab på arbejdspladsen og understregede behovet for fysiske sikkerhedsforanstaltninger med henblik på at beskytte mod trusler mod privatlivets fred.

Hvad er der på spil?

Virksomheder kan idømmes bøder på op til 4 % af deres globale årlige omsætning eller

20 mio. EUR

Hun havde i den forbindelse følgende at sige:

Sp.: Er arbejdsstyrkerne klar til at overholde GDPR?

Sv.: Vores tal viser, at kun én ud af tre virksomheder over hele verden er klar til at overholde den nye databeskyttelsesforordning (GDPR). Da GDPR træder i kraft d. 25. maj 2018, står det klart, at mange organisationer skal arbejde hurtigt for at fuldføre deres forberedelser.

Vi ser især virksomheder, der kæmper for at opfylde kravet om at implementere og dokumentere uddannelse og oplysningsprogrammer inden for databeskyttelse til deres medarbejdere. EU-tilsynsmyndigheder har givet udtryk for, at disse programmer er væsentlige forudsætninger for GDPR-overholdelse. I mellemtiden har vi fundet ud af, at organisationer, der opfylder dette krav, har forbedret deres virksomheds databeskyttelseskultur og etableret bedste praksis, der undertiden går længere end lovkravene.

Sp.: Er virksomheder i bestemte regioner bedre forberedt end andre?

Sv.: 34 % af amerikanske virksomheder siger, at de er forberedte, i forhold til 26 % af virksomhederne i Europa.[1] Virksomheder, der ikke er klar til GDPR – uanset om de er klar over det eller ej – påtager sig en stor forretningsmæssig risiko. Virksomheder, som tror, at de er forberedte, men ikke er det, løber en endnu større risiko.

Det er interessant at bemærke, at flere virksomheder i USA mener, at de er forberedte, i forhold til Europa. Dette hænger sammen med Databeskyttelsesforordningens eksterritoriale effekt. Forordningen gælder for alle virksomheder – uanset deres placering – der behandler eller opbevarer personoplysninger om EU-borgere. Det betyder, at ikke kun europæiske virksomheder, men også mange virksomheder med hovedsæde i USA, skal overholde disse strenge regler om beskyttelse af privatlivets fred.

Vi har mistanke om, at en overfladisk læsning af reglerne kombineret med vildledende og ubegrundede forventninger om ringe GDPR-håndhævelse kan udfordre virksomhedernes opfattelse af deres beredskab.

Sp.: Hvilke fysiske sikkerhedsforanstaltninger vedrørende beskyttelse af privatlivets fred kræves i henhold til GDPR?

Sv.: GDPR er en principbaseret forordning. Det betyder, at tilsynsmyndighederne ikke forsyner organisationerne med et sæt definitive foranstaltninger, der skal følges. I stedet skal organisationer opfatte GDPR-krav som en slags "tilstræbt tilstand" for deres databehandlingspraksis. Det betyder også, at organisationer skal identificere og vurdere de specifikke risici, de har brug for at begrænse med henblik på at overholde GDPR-kravene.

Når virksomhederne identificerer risici, skal de overveje dem, der omhandler databehandling, især på grund af hændeligt eller ulovligt tab, uautoriseret videregivelse af eller adgang til personoplysninger, der transmitteres, opbevares eller behandles på anden måde. Det er ligegyldigt, om en uautoriseret datavideregivelse finder sted, fordi en hacker sætter et sofistikeret cyberangreb ind på en virksomheds websted, eller fordi en fremmed tager et billede af meget følsomme data, der vises på en medarbejders computerskærm. Begge er lige alvorlige risici og kræver passende afbødningsstrategier.

Sp.: Udgør visuel hacking en risiko?

Svar: Absolut. Du skal blot huske på følgende: For mange organisationer udgør et brugernavn og en adgangskode en hovednøgle, der giver adgang til hele systemet. For en uautoriseret person skal der ikke mere end et hurtigt kig på en ubeskyttet skærm til for at få fat i disse nøgler og skaffe sig adgang. Og risikoen vokser i takt med den tiltagende raffinering af social engineering-angreb.

For et år siden blev en journalist hacket, mens han arbejdede ombord på et fly.[2] Hackeren kunne beskrive detaljer om en artikel, journalisten var i færd med at skrive, personlige e-mails, han havde sendt, og kommende arbejdsmøder. Samtlige af disse oplysninger fik hackeren efter eget udsagn ved at hacke flyets Wi-Fi. Eller måske fik hackeren simpelthen bare oplysningerne ved at kigge på journalistens computerskærm. Journalisten var oprørt, men han forstod budskabet. Mens han arbejdede på en følsom artikel – i dette tilfælde om de omfattende og vidtgående konsekvenser for privatlivets fred, der udsprang af Apples afslag på FBI's anmodning om at dekryptere en terrorists telefon – glemte han at beskytte oplysningerne og den intellektuelle ejendom på sin egen enhed. Ligesom denne journalist begår mange organisationer den samme fejl ved at undervurdere risikoen for cyberangreb og visuel hacking.

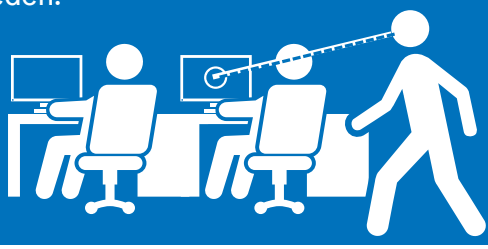
Sp.: Hvad er fordelene ved at implementere lavteknologiske fysiske sikkerhedsforanstaltninger?

Sv.: Med uafbrudte nyhedshistorier om massive brud på datasikkerheden er det nemt at glemme, at nutidens digitale virksomheder stadig er nødt til at kæmpe med fysiske sikkerhedsudfordringer. Der er flere fordele ved at implementere fysiske sikkerhedsforanstaltninger, såsom videokameraer til overvågning, låse til bærbare computere og beskyttelsessfiltre til skærme, bærbare computere, tablets og smartphones. Beskyttelsesfiltre tilbyder fx en solid strategi til at begrænse overtrædelser af privatlivets fred og brud på datasikkerheden. Der skal ikke mere til, end at nogle følsomme kunde- eller medarbejderoplysninger bliver set af en forkert person, før man kan stå over for et potentielt yderst skadeligt – og meget omtalt – brud på datasikkerheden.

Der skal ikke mere til, end at følsomme kunde- eller medarbejderoplysninger bliver

set af en forkert person,

før man kan stå over for et potentielt yderst skadeligt – og meget omtalt – brud på datasikkerheden.



De kan også understøtte overholdelse af andre forordninger end Databeskyttelsesforordningen. For eksempel blev en assisterende læge for nogle år siden fyret fra et hospital ved University of Iowa, fordi vedkommende overtrådte regler for beskyttelse af patienternes personoplysninger. Hun blev beskyldt for at hacke en kollega visuelt, mens denne gennemgik en patientjournal, hvilket er en overtrædelse af den amerikanske sygesikringslov.[3]

Fysiske sikkerhedsforanstaltninger, som fx beskyttelsesfiltre, kan tjene som en visuel påmindelse til medarbejderne om, at bedste praksis for sikkerhed og beskyttelse af privatlivets fred har høj prioritet i organisationen. Og som det altid er tilfældet med visuel beskyttelse af privatlivets fred, handler det ikke kun om at opfylde kravene til overholdelse. Det handler om at beskytte virksomhedens mest værdifulde aktiver.

Sp.: Hvordan kan virksomheder udnytte beskyttelse af privatlivets fred til at give en overlegen kundeoplevelse?

Sv.: Virksomheder, der gennemfører robuste GDPR-programmer og programmer til beskyttelse af privatlivets fred, oplever en række forretningsmæssige fordele, der rækker ud over kravoverholdelse. At kunne levere en overlegen kundeoplevelse er én af disse fordele. Den måde, din organisation beskytter dine kunders data på, kan have en direkte indvirkning på opbygningen – eller undermineringen – af den underliggende følelse af tillid, som dine kunder har til dig.

Vi ved fx, at kunderne går over til konkurrenter som følge af et brud på privatlivets fred.[4] Desuden fremhæver vores undersøgelse af forbrugernes holdninger til privatlivets fred, at 30 % nægter at gennemføre en onlinetransaktion, hvis de læser noget, som de ikke bryder sig om, i virksomhedens fortrolighedserklæring.[5]

Hvis du er forpligtet til at beskytte dine kunders data, og dine medarbejdere påskønner og giver udtryk for dette engagement i deres kundeinteraktioner, kan det få din virksomhed til at skille sig ud fra konkurrenterne.

Sp.: Er der nogen virksomheder, der skiller sig ud i kraft af deres engagement i sikkerhed og beskyttelse af privatlivets fred?

23 % af Fortune 100-virksomheder

har indført beskyttelse af privatlivets fred som en del af deres virksomheds sociale ansvar (CSR).

Sv.: Beskyttelse af privatlivets fred har udviklet sig fra at være et nicheemne for juridiske afdelinger til at være en kerneværdi for mange organisationer. I dag er it-direktører og marketingdirektører blandt de ledere, der mener, at beskyttelsen af dataaktiver fra angreb og misbrug er blandt deres højeste prioriteter. Vores undersøgelser viser, at 23 % af Fortune 100-virksomheder har indført beskyttelse af privatlivets fred som en del af deres virksomheds sociale ansvar (CSR).[6] Omtrent 70 % inddrog sikkerhed i deres CSR-rapporter.

Vi har også bemærket, at firmaer, som har forpligtet sig til beskyttelse af privatlivets fred og sikkerhed, drager fordel af dette ved at være åbne og klare om, hvordan de håndterer personoplysninger. Dette kan være en yderst værdifuld måde at sikre kunder, medarbejdere og forretningspartnere på. Men det er ikke så ligetil at arbejde i overensstemmelse med denne forpligtelse. Ofte skal organisationer ændre deres måde at føre disse forpligtelser ud i livet på og etablere en virksomhedskultur, der anerkender beskyttelse af privatlivets fred og sikkerhed som kerneværdier.

Sp.: Er der flere forordninger som GDPR undervejs?

Sv.: Det er der ingen tvivl om: GDPR er et udtryk for en tendens. Vi har for nylig gennemført en undersøgelse, der analyserer regler og praksis for beskyttelse af privatlivets fred i 54 lande.[7] Det er tydeligt, at regioner som Asien og Stillehavsområdet betragter GDPR som den mulige udvikling af deres lokale regler for beskyttelse af privatlivets fred. Elementer af Databeskyttelsesforordningen, såsom dataopbevaring, er også indlejret i databeskyttelsesreglerne i Latinamerika og Rusland. Endelig arbejder Europa-Parlamentet nu på at opdatere kravene i det nuværende e-databeskyttelsesdirektiv. Detaljerne skal stadig slås fast, men planen er at tilpasse disse krav til Databeskyttelsesforordningen.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, "Apple vs FBI shown in different light as journalist hacked mid-flight", 25. januar 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-rapport "The Future of Data Security and Privacy: Growth And Competitive Differentiation", 2017
[7]Forrester "Interactive Data Privacy Heat Map", 2017

FORRESTER®