การปกป้องข้อมูลและระบบความปลอดภัยทางคอมพิวเตอร์ในกระบวนการต่อเนื่องจาก GDPR

#KingstonIsWithYou

การปกป้องข้อมูลและระบบความปลอดภัยทางคอมพิวเตอร์ในกระบวนการต่อเนื่องจาก GDPR

เกรินนำ

บริษัทและหน่วยงานเป็นจำนวนมากต้องทำงานอย่างหนักเพื่อเตรียมพร้อมสำหรับมาตรการ GDPR สถานการณ์ของคุณก็อาจอยู่ในกลุ่มนีเช่นกัน ภัยคุกคามทางคอมพิวเตอร์ที่มีการพัฒนาอยู่ตลอดเวลาทำให้คุณไม่สามารถหยุดยั้งหรือเตรียมการได้ทัน การควบคุมมาตรฐานภายใต้ GDPR ไม่ใช่กระบวนการที่ระบุได้อย่างชัดเจนอีกต่อไป แต่จะต้องอาศัยวิจารณญาณในการปกป้องข้อมูลและความปลอดภัยของระบบคอมพิวเตอร์อย่างต่อเนื่อง ซึ่งหมายถึงเราจะหยุดนิ่งในช่วงเวลาใดเวลาหนึ่งไม่ได้เลย

ในอีบุ๊กฉบับย่อนี เราได้รวบรวมรวบรวมแหล่งข้อความรู้จากผู้ให้ข้อเสนอแนะที่มีประสบการณ์สูงของสหราชอาณาจักรด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เพื่อกล่าวถึงแนวทางในการปกป้องข้อมูลที่เปลี่ยนแปลงไปนับจากเริ่มใช้ GDPR นอกจากนี้เรายังกล่าวถึงบริษัทต่าง ๆ ที่ให้ความรู้กับพนักงานเกี่ยวกับความจำเป็นด้านการควบคุมมาตรฐานและการทำงานของฝ่าย IT หรือเทคโนโลยีเพื่อปรับปรุงโครงสร้างพื้นฐานด้าน IT และให้ความรู้แก่ผู้ใช้ปลายทางเกี่ยวกับปัญหาด้านความปลอดภัยใหม่ ๆ ที่กำลังเกิดขึ้น

การปกป้องข้อมูลและระบบความปลอดภัยทางคอมพิวเตอร์ในกระบวนการต่อเนื่องจาก GDPR

ผู้สนับสนุน

อีบุ๊กฉบับย่อนี้รวบรวมเนื้อหาจากผู้เชี่ยวชาญห้ารายด้านการปกป้องและการรักษาความปลอดภัยของข้อมูล

Rob Allen
@Rob_A_kingston

Rob คือผู้อำนวยการฝ่ายการตลาดและบริการด้านเทคนิคของ Kingston Technology และร่วมงานกับบริษัทมากตั้งแต่ปี 1996 Rob รับหน้าที่ดูแลด้านงานประชาสัมพันธ์โซเชียลมีเดีย การตลาดผ่านช่องทางจัดจำหน่ายต่าง ๆ และสื่อการตลาดดิจิตอลและการสร้างสรรค์ผลงานสำหรับแบรนด์และผลิตภัณฑ์ทั้งหมดภายใต้ Kingston

Tara Taubman-Bassirian
@clarinette02

Tara มีประสบการณ์ในหลาย ๆ ด้าน ทั้งในฐานะนักกฎหมาย ที่ปรึกษา นักไกล่เกลี่ย ผู้วิจัย ผู้ให้คำปรึกษา ผู้บรรยายและนักเขียน ความเชี่ยวชาญในหลาย ๆ ด้านเกี่ยวกับความเป็นส่วนตัว ทรัพย์สินทางปัญญาและการปกป้องข้อมูล ทำให้เธอเป็นที่รู้จักในหลายพื้นที่ทั่วโลก โดยเฉพาะในสหราชอาณาจักร ฝรั่งเศสและสหรัฐฯ

Rafael Bloom
@rafibloom73

Rafael เป็นกรรมการของ Salvatore ltd. หน้าที่ของเขาคือการช่วยบริษัทในการจัดการปัญหาเชิงกลยุทธ์ การพาณิชย์และกระบวนการต่าง ๆ รวมทั้งโอกาสที่เกี่ยวข้องที่เกิดขึ้นจากการเปลี่ยนแปลงด้านเทคโนโลยีและระเบียบข้อบังคับ

Miriam Brown
@Kingston_MBrown

ผู้จัดการฝ่ายการตลาดเชิงกลยุทธ์ B2Bของ Kingston Technology ซึ่งเคยร่วมงานกับบริษัทมากตั้งแต่ปี 1997 ในบทบาทของเธอ Miriam มีหน้าที่ดูแลด้านแผนการตลาด เนื้อหาและแคมเปญต่าง ๆ สำหรับผลิตภัณฑ์ B2B ทั้งหมดของ Kingston

Sally Eaves
@sallyeaves

ศ. Sally Eaves ได้รับการยอมรับว่าเป็น 'ผู้ผลักดันด้านเทคโนโลยีในการควบคุมด้านจรรยาบรรณ' เธอมีประสบการณ์ที่ยาวนานในฐานะประธานเจ้าหน้าที่บริหารและประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี รวมทั้งในฐานะศาสตราจารย์ด้านเทคโนโลยีใหม่และที่ปรึกษาเชิงกลยุทธ์ในระดับสากล Sally ยังเป็นผู้บรรยายเนื้อหาในระดับนานาชาติ นักเขียน นักวิจัยและอินฟลูเอนเซอร์ที่มีรางวัลรับรองมากมายและเป็นผู้นำวงการความคิดต้นแบบที่สำคัญคนหนึ่ง

การปกป้องข้อมูลและระบบความปลอดภัยทางคอมพิวเตอร์ในกระบวนการต่อเนื่องจาก GDPR

สารบัญ

หัวข้อที 1 – การปกป้องข้อมูลมีการเปลียนแปลงไปอย่างไรนับตั้งแต่มีการประกาศใช้ GDPR

การควบคุมมาตรฐานเป็นกระบวนการทีมีรายละเอียดมากมาย ในช่วงสองปีทีผ่านมา ทีมงานฝ่ายกฎหมายได้มีการคัดสรรเจ้าหน้าทีกำกับดูแลด้านการปกป้องข้อมูลเพิมขึนอย่างมาก[1] และมีการใช้บริการทีปรึกษาด้านความเป็นส่วนตัวของข้อมูลจากภายนอกเพิมขึนอย่างมาก การประเมินผลกระทบด้านการปกป้องข้อมูล (DPIA) ปัจจุบันเป็นเรืองทีหลายหน่วยงานคุ้นเคยกันเป็นอย่างดี

แต่ยังมีอีกหลายอย่างทีเรายังต้องเรียนรู้

หนึงในปัญหาทีสำคัญทีสุดเกียวกับ GDPR คือคุณไม่สามารถปล่อยปละละเลยได้เลย ในหน่วยงานส่วนใหญ่ ทีมงานทุกคนก็อาจทำผิดพลาดได้ทังสิน ปัญหาจะยิงรุนแรงในภาคส่วนทีมีการใช้แรงงานหลายส่วนและแต่ละส่วนมีการทำงานทีเป็นอิสระ เช่น ในกลุ่มสุขภาพ การศึกษาและกฎหมาย ในแง่มุมทางกฎหมาย ทนายมักมีการแลกเปลียนข้อมูลทีอ่อนไหวผ่านทางเอกสารแนบอีเมล บุคลากรด้านการแพทย์จะมีการแลกเปลียนข้อมูลผู้ป่วยหรือผลการตรวจสแกน MRI จากอีเมลแอดเดรทีปลอดภัย ในหน่วยงานทีอยู่ภายใต้แรงกดดันสูง การเพิมความกดดันอีกเพียงเล็กน้อยในการทำงานก็อาจทำให้หลายคนย่อหย่อนในการควบคุมมาตรฐานไปได้ ผลผลิตคือเป้าหมายสำคัญสูงสุดสำหรับทุกคน

และนีคือสิงทีต้องเปลียนแปลง

นอกจากนียังมีประเด็นในส่วนของภาคการกุศลอีก หลายครังองค์กรการกุศลคิดว่าตนเองได้รับการยกเว้นจาก GDPR แม้ว่าพวกเขาจะเข้าใจว่า GDPR มีผลกับภาคเอกชน ภาครัฐและหน่วยงานจากภายนอก แต่ก็อาจลังเลทีจะต้องลงทุนด้านมาตรการการปกป้องข้อมูล ซึงฟังดูทุ่มเทแต่ถือว่าอ่อนด้อยเกินไป ค่าปรับทีอาจถูกเรียกเก็บจากการละเมิดหลักเกณฑ์ GDPR มีผลกดดันโดยตรงต่อการลงทุนด้าน IT

Tara Taubman-Bassirian
@clarinette02

GDPR มาตรการปกป้องข้อมูลและทีปรึกษาด้าน IP

"หน่วยงานอิสรต่าง ๆ (third sector) หลายแห่งกล่าวว่า: 'GDPR ไม่มีผลกับเรา เราเป็นแค่องค์กรการกุศลเท่านัน" แม้ว่าจะมีการกำหนดมาตรการควบคุมมาตรฐานของเว็บไซต์อย่างจริงจัง สิงทีผมพยายามบอกกับทุก ๆ คนคือประเด็นไม่ได้อยู่ทีข้อมูลทีเราต้องการจัดเก็บ แต่อยู่ทีบุคคลภายนอกทีเราเปิดช่องให้เข้ามาสืบค้นข้อมูลผู้เยียมชมของเรา"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [**สืบค้นเมือ** 26.11.19]

นับตังแต่ปี 2016 ความต้องการของกลุ่มผู้บริหารด้านการปกป้องข้อมูล (DPO) ได้เพิมขึนมากกว่า 700%

การปกป้องข้อมูลมีการเปลี่ยนแปลงไปอย่างไรนับตั้งแต่มีการประกาศใช้ GDPR

มาตรการลดการเก็บรักษาข้อมูลที่ไม่จำเป็นได้กลายเป็นเทรนด์ที่กำลังได้รับความสนใจ

เราอยู่ในยุคที่มีการรวบรวมข้อมูลไว้เป็นจำนวนมหาศาล "The Big Four" (Google, Apple, Facebook และ Amazon) คือสี่ยักษ์ใหญ่ที่ครอบครองข้อมูลของลูกค้าเป็นจำนวนมาก หน่วยต่าง ๆ มีการใช้แนวทางเดียวกับ The Big Four ในการรวบรวมข้อมูลไว้เป็นจำนวนมาก แต่ยิ่งมีข้อมูลเก็บไว้มากเท่าไร คุณก็ยิ่งได้รับความเสี่ยงมากขึ้นตามไปด้วย หนึ่งในเทรนด์ที่เป็นประโยชน์มากที่สุดนับตั้งแต่มีการปรับใช้ GDPR คือการต่อต้าน

Tara Taubman-Bassirian
@clarinette02

GDPR มาตรการปกป้องข้อมูลและทีปรึกษาด้าน IP

"การลดจำนวนข้อมูลที่จัดเก็บอาจเป็นหนึ่งในวิธีที่ดีที่สุดภายใต้แนวทาง GDPR การจัดทำฐานข้อมูลใด ๆ ย่อมมาพร้อมกับความเสี่ยงทั้งสิ้น"

Rob Allen
@Rob_A_kingston

ผู้อำนวยการฝ่ายการตลาดและบริการด้านเทคนิค
Kingston Technology

"เรามีกฎในการลบข้อมูลที่เข้มงวด แน่นอนว่าข้อมูลที่สำคัญทางธุรกิจจะต้องมีการจัดเก็บอย่างถูกต้อง แล้วข้อมูลอื่น ๆ ล่ะ หลังจากผ่านไปหนึ่งปี เราจะเก็บข้อมูลเหล่านี้ต่อไปเพื่ออะไร"

การจัดเก็บหรือรวบรวมข้อมูลไว้มากเกินความจำเป็น บริษัทที่ชาญฉลาดจะใช้ระบบลดการจัดเก็บข้อมูลเป็นสำคัญ กล่าวคือหากคุณไม่ต้องใช้ก็ไม่จำเป็นต้องจัดเก็บไว้

ข้อดีที่มากกว่าแค่การจำกัดความเสี่ยง ยกตัวอย่างเช่นในมุมมองด้านการตลาด หากฐานข้อมูลด้านการตลาดของคุณไม่ได้รับการจัดการดีพอ คุณอาจมีข้อมูลที่ล้าสมัยถูกเก็บอยู่เป็นจำนวนมาก เมื่อฐานข้อมูลของคุณครอบคลุมคนเป็นจำนวนมากขึ้น และคุณต้องมีการทำแคมเปญการตลาดทางอีเมลเป็นประจำ ค่าใช้จ่ายของคุณก็จะเพิ่มขึ้น ซึ่งจะส่งผลต่อผลสัมฤทธิ์ของแคมเปญในเวลาเดียวกัน

การลดการเก็บข้อมูลที่ไม่จำเป็นครอบคลุมทั้งเอกสารจัดพิมพ์ด้วย ระมัดระวังเอกสารที่จัดพิมพ์ให้ดี (เช่น การสแกนหนังสือเดินทางของลูกค้า) รวมทั้งสิ่งที่คุณจดไว้ (เช่น รหัสผ่านบัญชีผู้ใช้) เมื่อต้องเก็ฐรักษาสำเนาข้อมูลจัดพิมพ์ใด ให้จัดเก็บไว้อย่างปลอดภัย กองเอกสารเป็นจำนวนมากบนโต๊ะของคุณอาจทำให้ดูน่าเชื่อถือ แต่ไม่ใช่เรื่องปลอดภัย

Rafael Bloom
@rafibloom73

ผู้อำนวยการฝ่าย
Salvatore Ltd.

"เราได้พบเจอแนวคิดมากมายเกี่ยวกับการใช้งานเทคโนโลยีและสิ่งที่ธุรกิจต่าง ๆ นำไปใช้ ความพร้อมด้านระบบดิจิตอลของธุรกิจที่มีความเป็นผู้นำอย่างแท้จริงคือสิ่งที่จำเป็นอย่างยิ่ง"

ผลกระทบจากปัจจัยแวดล้อม: จากระดับบริหารจนถึงผู้บริโภค

การปกป้องข้อมูลคือแนวคิดด้านการกำกับดูแลที่มีมานานนับทศวรรษแล้ว แต่ก็ยังพบว่ามีการเรียกเก็บค่าปรับเป็นจำนวนมากกับผู้ประกอบการต่าง ๆ ไม่เว้นแม้แต่ Google[1], British Airways และโรงแรมในเครือ Marriott[2] อีกทั้งข่าวที่ถูกเผยแพร่ยิ่งทำให้ผู้บริหารระดับสูงต้องให้ความสำคัญกับ GDPR อย่างจริงจัง ซึ่งนำไปสู่แผนงานเพื่อลดผลกระทบที่อาจเกิดขึ้น

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [**สืบค้นเมื่อ** 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [**สืบค้นเมื่อ** 26.11.19]

การปกป้องข้อมูลมีการเปลี่ยนแปลงไปอย่างไรนับตั้งแต่มีการประกาศใช้ GDPR

ต่อ...

อีกปัจจัยผลักดันเบื้องหลังการใช้มาตรการปกป้องข้อมูลที่เข้มงวดคือการประสานความร่วมมือทางธุรกิจ ธุรกิจขนาดใหญ่ปัจจุบันต้องมีการตรวจสอบประวัติและความซื่อตรงในการทำงาน รวมทั้งมาตรการรักษาความปลอดภัยของข้อมูลของซัพพลายเออร์ของตนเพื่อหลีกเลี่ยงปัญหาการละเมิดข้อมูลระหว่างความร่วมมือทางธุรกิจ

แต่ก็ยังมีอีกด้านของเหรียญในการสร้างความเข้าใจในเชิงพาณิชย์เกี่ยวกับ GDPR กล่าวคือ ผู้บริโภคเองก็เริ่มตระหนักในสิทธิ์ของตนเองมากขึ้น พวกเขารู้ดีว่าหากบริษัทไม่สามารถควบคุมข้อมูลของตนเองได้ กล่าวคือไม่จำเป็นต้องมีการละเมิดข้อมูลแต่อย่างใด พวกเขาก็มีสิทธิ์เรียกร้องค่าชดเชย ธุรกิจต่าง ๆ จึงต้องระมัดระวังมากขึ้น

Sally Eaves
@sallyeaves

CEO และผู้อำนวยการของ
Sally Eaves Consultancy

"การปกป้องข้อมูลเป็นข้อกำหนดทางธุรกิจที่สำคัญในการสร้างความเชื่อถือจากบุคคลทั่วไป"

หัวข้อที 2 – หน่วยงานต่าง ๆ มีการให้ความรู้แก่พนักงานอย่างไรบ้าง

การฝึกอบรมพนักงาน: คำสองคำที่สามารถสร้างความฉงนให้กับทีมงานของคุณ

สาเหตุเพิ่มเติมเพื่อให้แน่ใจว่าเนื้อหาการฝึกอบรมของคุณมีความน่าสนใจ แรงงานที่มีความรู้มีโอกาสน้อยลงที่จะกระทำผิดในมาตรการปกป้องข้อมูล และหากมีการละเมิดข้อมูลเกิดขึ้น Information Commissioner's Office (ICO) ก็จะมีความเชื่อถือคุณมากกว่า หากคุณสามารถพิสูจน์ได้ว่าคุณได้พยายามอย่างเต็มที่ในการฝึกอบรมพนักงานด้านการรักษาความปลอดภัยของข้อมูล

Rafael Bloom
@rafibloom73

ผู้อำนวยการ
Salvatore

"ฉันคิดว่าข้อมูลก็เหมือนส่วนประกอบหนึ่งในเครือข่ายการจัดหา ซึ่งจะต้องมีการกำกับดูแลด้านการเก็บรักษาและดูแลตลอดวงจรอายุของข้อมูลอย่างเหมาะสม แนะนำให้สละเวลาสักครึ่งชั่วโมงเพื่อพูดคุยกับทีมงานในห้องเพื่อบอกให้พวกเขาทราบว่าต้องทำอะไรภายในห้อง และอย่าเปิดเผยข้อมูลใด ๆ รวมทั้งดังรหัสผ่านที่มีความปลอดภัย วิธีการนี้ช่วยลดความเสี่ยงให้กับองค์กร แต่สิ่งเล็ก ๆ น้อย ๆ เหล่านี้ส่งผลกระทบกดดันต่อบุคลากรเพิ่มเติมอย่างใดหรือไม่ เปล่าเลย"

อย่างไรก็ตาม เมื่อเดือนเมษายน 2019 Margot James รัฐมนตรีดิจิตอลได้กล่าวว่าหน่วยงานในสหราชอาณาจักรสามในสิบแห่งมีการฝึกอบรมพนักงานในการจัดการกับภัยคุกคามทางคอมพิวเตอร์[1] ถึงเวลาที่จะให้ความรู้ในด้านนี้อย่างจริงจังกันแล้ว

นี่เป็นเรื่องของการแยกประเภทข้อมูลที่ไม่ได้เป็นแค่งานแบบเดิม ๆ ซ้ำ กัน

การฝึกอบรมจะเป็นเรื่องของการปรับเปลี่ยนพฤติกรรมและวัฒนธรรมในการทำงาน ไม่ใช่การทำตามขั้นตอนที่กำหนดไว้แบบตายตัว คุณสามารถศึกษาผ่านบทเรียนออนไลน์ได้ง่าย ๆ ซึ่งจะมีการจัดทำชุดคำถามเบื้องต้นเกี่ยวกับการปกป้องข้อมูล ซึ่งทุกคนสามารถเลือกตอบได้อย่างไม่ยากจนเกินไป แต่วิธีนี้จะช่วยปกป้องหน่วยงานของคุณได้จริง ๆ หรือไม่

พฤติกรรมในการปกป้องข้อมูลที่ดีจะต้องอาศัยพื้นฐานที่สำคัญสองข้อ อย่างแรกคือการฝึกอบรมจะต้องมีประเด็นที่ตรงเป้า น่าสนใจและมุ่งหมายเพื่อเป็นการท้าทายสถานะปัจจุบันในหน่วยงานของคุณ ประการที่สองคือการตระหนักว่า GDPR คือแนวทางที่เชื่อมโยงกับวัฒนธรรมในการทำงานที่มีผลกับการทำงานในแต่ละวันของพนักงานทุกคน นี่เป็นเรื่องของการทำในสิ่งที่ถูกต้องเกี่ยวกับข้อมูล ด้วยวิธีที่ถูกต้องภายในหน่วยงาน ดูตัวอย่างได้จากงานด้านทรัพยากรบุคคล ลองพิจารณาจากข้อมูลรายละเอียดผู้สมัครงานที่ค้างอยู่ในเซิร์ฟเวอร์อีเมล การปกป้องข้อมูลคือความรับผิดชอบของทุกคน

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [**สืบค้นเมื่อ** 26.11.19]

หน่วยงานต่าง ๆ มีการให้ความรู้แก่พนักงานอย่างไรบ้าง

มีบุคคลหนึ่งทีอยู่เบื้องหลังข้อมูลเหล่านี้

ในหัวข้อแรกเราได้กล่าวไปแล้วว่าผู้บริโภคมีการตระหนักเกียวกับสิทธิ์ในข้อมูลของตนมากขึนเรือย ๆ วิธีทีดีในการฝึกอบรมด้านการปกป้องข้อมูลคือการช่วยให้พนักงานของคุณสามารถเชือมโยงกับบุคคลทีอยู่เบืองหลังข้อมูลต่าง ๆ ได้ พูดคุยกับพนักงานของคุณให้พิจารณาเกียวกับหน่วยงานต่าง ๆ ทีตนเองให้ข้อมูล และสร้างความเข้าใจกับพนักงานว่าการปกป้องข้อมูลคือ เรืองความเป็นส่วนตัวของบุคคล

จัดทำแผนสำรองไว้

Sally Eaves
@sallyeaves

"การให้ความรู้แก่พนักงานอย่างต่อเนืองด้านการรักษาความปลอดภัยของข้อมูลถือเป็นมาตรการภาคบังคับของธุรกิจ ไม่ควรจัดการฝึกอบรมแบบครังเดียวแล้วจบ แต่ควรดำเนินการอย่างจริงจัง และมีการเข้าถึงและแลกเปลียนข้อมูลระหว่างกันเพือให้กลายเป็นส่วนหนึงของการทำงานในภาคปฏิบัติไปด้วย พนักงานทุกคนจะต้องมีส่วนในการพูดคุยเกียวกับสิงทีเราต้องการเพือปรับลด จัดการและปกป้อง"

Miriam Brown
@Kingston_MBrown

"สิงทีน่าสนใจระหว่างการฝึกอบรมบุคลากรคือการถามว่า: 'จะทำอย่างไรหากนีคือข้อมูลของคุณเอง' หากผู้จัดการธนาคารของฉันกำลังทำงานจากทีบ้านโดยใช้โน้ตบุ๊กของตัวเอง และมีข้อมูลทีอ่อนไหวในโน้ตบุ๊ก ฉันก็คาดหวังว่าไดร์ฟของเขาจะมีการเข้ารหัสไว้"

Rob Allen
@Rob_A_kingston

"ปฏิบัติต่อข้อมูลเสมือนเป็นของคุณเอง"

หัวข้อที่ 3 –
ส่วนงานด้าน IT สามารถดูแลอุปกรณ์ต่าง ๆ ให้ปลอดภัยมากขึ้นได้หรือไม่

การทำงานจากทางไกลถือเป็นอีกมาตรฐานใหม่

พนักงานของคุณสามารถเลือกทำงานจากอุปกรณ์ต่าง ๆ รวมทั้งอุปกรณ์ส่วนตัวซึ่งอาจถูกวางลืมไว้บนรถไฟหรือทำหายบนแท็กซี่ สิ่งที่ท้าทายคือการหาวิธีในการช่วยให้พนักงานทำงานได้อย่างมีประสิทธิภาพโดยไม่ทำให้ตนเองได้รับความเสี่ยงด้านความปลอดภัยหรือการถูกล้วงข้อมูล เพียงแค่คนคนเดียวเลินเล่อในการปกป้องข้อมูล ความเสียหายก็อาจเกิดขึ้นได้กับทุกคนในทันที

Sally Eaves
@sallyeaves

CEO และผู้อำนวยการของ
Sally Eaves Consultancy

"ข้อมูลจะต้องได้รับการปกป้องระหว่างการนำส่ง พักเก็บและใช้งาน สิ่งสำคัญจึงเป็นการกำหนดมาตรการด้านความปลอดภัยที่รอบด้านและแผนการลบข้อมูลภายใต้บริบทการดำเนินงานนี้ การนำเสนอประเด็นความเสี่ยงที่มักถูกมองข้ามก็เป็นสิ่งที่สำคัญ เช่น การใช้ USB ที่ไม่มีการเข้ารหัส การใช้อีเมลเพื่อส่งเอกสารแนบแบบไม่เข้ารหัส และการใช้เว็บเบราเซอร์เพื่อเปิดเผยข้อมูลผู้ใช้ที่อ่อนไหว อุปกรณ์มากมายที่ถูกใช้เพื่อเชื่อมต่อและรูปแบบการทำงานที่หลากหลายมากขึ้น ทำให้เราจำเป็นต้องแน่ใจว่าข้อมูลในโทรศัพท์มือถือมีความปลอดภัยไม่แพ้ข้อมูลที่ถูกจัดเก็บไว้ในเซิร์ฟเวอร์ของบริษัท"

การตรวจรับรองสองชั้น

สำหรับหน่วยงานทั่ว ๆ ไป วิธีที่ดีและง่ายที่สุดที่คุณสามารถทำได้คือการปกป้ององค์ประกอบทางเครือข่ายของคุณ เช่น การเลือกใช้ระบบกำกับดูแลรหัสผ่านและระบบตรวจรับรองสองชั้น ตัวอย่างที่ดีของระบบตรวจรับรองสองชั้นคือกรณีที่ผู้ใช้ได้รับแจ้งให้กรอกรหัสผ่านในโน้ตบุ๊กร่วมกับรหัสผ่านที่แจ้งทางโทรศัพท์มือถือหลังจากกรอกรหัสผ่านชุดแรกเสร็จสิ้น

VPN และ SSD/USB แบบเข้ารหัส

VPN เริ่มเป็นที่นิยมมากขึ้นเรื่อย ๆ ในกลุ่ม SME นี่ถือเป็นองค์ประกอบที่สำคัญอย่างยิ่งสำหรับพนักงานที่ต้องสืบค้นข้อมูลทางธุรกิจผ่านเครือข่าย Wi-Fi สาธารณะ แต่ธุรกิจต่าง ๆ ก็ยังต้องระมัดระวังไม่พึงพา VPN มากจนเกินไป นี่เป็นเพียงส่วนหนึ่งของการป้องกันเท่านั้น หลายครั้งที่ธุรกิจต่าง ๆ เลือกใช้ VPN เฉพาะกับแรงงานทางไกลที่ใช้โน้ตบุ๊กโดยไม่มีการเข้ารหัสฮาร์ดแวร์ใด ๆ เกือบทุกคนมีข้อมูลที่จัดเก็บไว้ในโน้ตบุ๊กของตนเอง จะเกิดอะไรขึ้นหากข้อมูลเหล่านี้ถูกแฮ็ค ขโมย หรือสูญหาย USB และ SSD เข้ารหัสมีราคาแพงกว่าไดร์ฟมาตรฐานเพียงเล็กน้อยเท่านั้น การเลือกใช้ USB เข้ารหัสและติดตั้ง SSD แบบเข้ารหัสเชิงฮาร์ดแวร์ให้กับโน้ตบุ๊กของคุณจะช่วยลดปัญหาในการทำงานจากระยะไกลได้อย่างมาก และหากอุปกรณ์สูญหายหรือถูกขโมย คุณก็สามารถมั่นใจได้ว่าจะไม่มีคนอื่นที่สามารถสืบค้นไฟล์เข้ารหัสของคุณ คุณยังสามารถทำลายข้อมูล USB ที่สูญหายได้จากระยะไกล

"ฉันเคยได้พบกับผู้เชี่ยวชาญด้านระบบความปลอดภัยทางคอมพิวเตอร์ที่พยายามแนะนำให้ CEO ของบริษัทเลือกใช้ระบบตรวจรับรองสองชั้น แต่ได้รับการปฏิเสธว่า: 'เราไม่ใช้หรอก มันยุ่งยาก วุ่นวายละไม่ใช่สิ่งที่เราต้องการ" ไม่นานหลังจากนั้นพวกเขาก็เป็นข่าวในคดีฉ้อโกงมูลค่า 40,000 ปอนด์"

Rafael Bloom
@rafibloom73

ผู้อำนวยการฝ่าย
Salvatore Ltd.

"ท้ายที่สุดแล้ว วิธีที่ดีที่สุดในการส่งเสริมความเข้าใจด้านการรักษาความปลอดภัยคือการพูดคุยอย่างเปิดเผยกับพนักงานเพื่อพิจารณากลยุทธ์ต่าง ๆ ที่ทั้งปลอดภัยและจะสะดวกต่อการทำงานมากที่สุด"

Rob Allen
@Rob_A_kingston

ผู้อำนวยการฝ่ายการตลาดและบริการด้านเทคนิค
Kingston Technology

ส่วนงานด้าน IT สามารถดูแลอุปกรณ์ต่าง ๆ ให้ปลอดภัยมากขึ้นได้หรือไม่

เซิร์ฟเวอร์ส่วนตัวและ MSP

หน่วยงานขนาดใหญ่จำนวนมากเริ่มมีการปรับตัวในการจัดเตรียมเซิร์ฟเวอร์ของตนเองไว้ภายในหน่วยงาน ซึ่งหมายถึงพวกเขาจะสามารถควบคุมทรัพยากรเซิร์ฟเวอร์ได้อย่างเต็มที่ โดยไม่มีข้อมูลที่ถูกสืบค้นได้ผ่านระบบคลาวด์สาธารณะ นอกจากนี้ยังมีไฮบริดเซิร์ฟเวอร์สำหรับจัดเก็บข้อมูลที่ไม่อ่อนไหวไว้ในคลาวด์ ส่วนข้อมูลส่วนบุคคลก็จะเก็บไว้ในไซต์งาน สำหรับ SME และหน่วยงานอิสระ (ภาคการกุศล) การจัดระบบเซิร์ฟเวอร์ของตนเองอาจมีค่าใช้จ่ายสูง และนี่เป็นที่ทำให้ต้องอาศัยผู้ให้บริการภายใต้ระบบจัดการและเซิร์ฟเวอร์ส่วนตัวเสมือนจริง ระบบเหล่านี้เน้นด้านความปลอดภัยและค่าใช้จ่ายในการดำเนินงานที่ไม่สูงมากนัก

การทำหมายเหตุกำกับข้อมูลที่กำลังจะหมดอายุอัตโนมัติ

หนึ่งในหลักการสำคัญของ GDPR คือการลบข้อมูลเก่า ข้อมูลส่วนบุคคลบางประเภทจะต้องไม่ถูกเก็บไว้นานเกินกว่าเจ็ดปี จะทำอย่างไรหากคุณได้รับแจ้งผ่านระบบอัตโนมัติว่าข้อมูล'กำลังจะหมดอายุแล้ว ฐานข้อมูลที่มีการจัดทำอย่างเหมาะสม จะทำให้สะดวกสำหรับฝ่าย IT ในการแจ้งอีเมลอัตโนมัติไปยัง DPO เมื่อข้อมูลของคุณใกล้ถึงกำหนดเวลาในการเลิกใช้แล้ว

ร่วมงานกับผู้ให้บริการที่เหมาะสม

เมื่อพูดถึงระบบความปลอดภัยด้าน IT เรามีผู้ผลิตและผู้ให้บริการเป็นจำนวนมากที่จะต้องพิจารณา ศึกษาข้อมูลให้ดี สิ่งสำคัญคือระบบที่จัดโดยผู้ให้บริการที่น่าเชื่อถือและมีความเชี่ยวชาญเฉพาะด้านเพื่ออำนวยความสะดวกให้แก่หน่วยงานต่าง ๆ ในอุตสาหกรรมและส่วนการทำงานของคุณ ผู้ให้บริการที่คุณเลือกจะต้องมีความเข้าใจเกี่ยวกับข้อจำกัดต่าง ๆ ในการรักษาความปลอดภัยของข้อมูล ไม่จำกัดเฉพาะในด้านเทคโนโลยีเท่านั้น

หัวข้อที 4 – ผู้ให้บริการด้านเทคนิคจะปรับปรุงกระบวนการและการดำเนินการได้อย่างไร

TLC สำหรับ DPO

นับตั้งแต่ปี 2016 ความต้องการของกลุ่มผู้บริหารด้านการปกป้องข้อมูล (DPO) ได้เพิ่มมากขึ้นกว่า 700%[1] ปัจจุบันมี DPO ที่ถูกเลือกใช้งานกว่า 500,000 อัตราในยุโรป ซึ่งเป็นหกเท่าของข้อมูลที่คาดการณ์ไว้ในปี 2017[2] บทบาทที่สำคัญของ DPO มักถูกมองข้ามและไม่ได้รับความสำคัญ

DPO จะต้องสามารถตรวจสอบโครงสร้างระบบความปลอดภัยทั้งหมดในบริษัทของคุณ และขอบเขตด้านการรักษาความเป็นส่วนตัวของข้อมูลที่เกี่ยวข้อง นี่เป็นงานเต็มเวลา แต่ในบางองค์กร 'DPO' อาจถูกใช้เป็นแค่ป้ายชื่อบุคลากรที่มีข้อมูลด้านเทคโนโลยีมากกว่าคนอื่น ๆ ในองค์กรเท่านั้นเอง บุคคลเหล่านี้มีหน้าที่ดูแลด้านความเป็นส่วนตัวสำหรับข้อมูลของบริษัท และมีหน้าที่ในการปฏิบัติงานทั่วไปอื่น ๆ ด้วยในเวลาเดียวกัน

ในความเป็นจริงคือมีบริการและเครื่องมือเฉพาะด้านมากมายที่จัดไว้เพื่อสนับสนุน DPO รูปแบบใหม่นี้ แม้ว่าคุณจะมี DPO แบบเต็มเวลา แต่การดูแลความปลอดภัยของข้อมูลก็มีปัจจัยที่แปรผันและมีข้อจำกัดต่าง ๆ มากมายที่อาจต้องมีการประสานเพื่อขอความเห็นเพิ่มเติม การร่วมงานกับที่ปรึกษาจากภายนอกด้านการรักษาความปลอดภัยของข้อมูลเป็นกระบวนการที่ละเอียดอ่อน แต่สิ่งแรกคือคุณจะต้องกำหนดโครงสร้างที่ชัดเจนภายในหน่วยงานก่อนเป็นอันดับแรก

ความชัดเจน แผนสำรอง และการปฏิบัติงานร่วมกัน

โครงสร้างพื้นฐานด้าน IT ของคุณมีความน่าเชื่อถือพอ ๆ กันกับจุดอ่อนที่คุณมี ด้วยเหตุนี้ เมื่อมีการเพิ่มองค์ประกอบใหม่ ๆ ด้าน IT ใด ๆ เข้ามา เจ้าหน้าที่ด้านเทคนิคของคุณก็จะต้องมีความชัดเจนว่าอาจเกิดปัญหาด้านความปลอดภัยขึ้นได้บ้าง และให้คำแนะนำที่ชัดเจนในการใช้งานผลิตภัณฑ์ใหม่ของคุณอย่างปลอดภัย

Tara Taubman-Bassirian
@clarinette02

GDPR มาตรการปกป้องข้อมูลและที่ปรึกษาด้าน IP

"ผมพยายามอธิบายกับทุกคนที่ติดตั้งกล้อง CCTV ว่านี่อาจจะไม่ใช่ระบบความปลอดภัยเสมอไป เพราะหลายครั้งเราติดตั้งกล้องโดยไม่ได้ตั้งรหัสผ่านไว้ คุณแค่ล็อกอินไปยังเว็บไซต์ก็สามารถเรียกชมฟีดภาพได้ทันที นี่เหมือนกับเป็นการให้ข้อมูลกับโจรว่า "เข้ามาสิ ไม่มีคนอยู่ ด้วยซ้ำ!"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [**สืบค้นเมื่อ** 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [**สืบค้นเมื่อ** 26.11.19]

ผู้ให้บริการด้านเทคนิคจะปรับปรุงกระบวนการและการดำเนินการได้อย่างไร

นอกจากนียังมีประเด็นเกียวกับสถานการณ์ทีไม่คาดคิดอีก จะเกิดอะไรขึนหากผลิตภัณฑ์หมดอายุการใช้งานหรือต้องมีการอัพเดต ผู้ให้บริการด้านเทคนิคควรมีคำแนะนำสำหรับกรณีฉุกเฉินหากเกิดปัญหากับข้อมูลโดยไม่คาดคิด หรือหากเกิดปัญหาด้านความปลอดภัยกับระบบ IT โดยรวม ดูจากตัวอย่างของเครืองสแกน MRI ระบบอาจติดตัง SSD เข้ารหัสขนาดสีเทราไบต์ไว้เพือจัดเก็บภาพของผู้ป่วย แต่จะเกิดอะไรขึนหากพืนทีจัดเก็บข้อมูลไม่เหลืออีกต่อไป

ผู้ให้บริการด้านเทคนิคและหน่วยงานต่าง ๆ จะต้องมีการประสานงานกันอย่างใกล้ชิดในด้านระบบดิจิตอลและระบบข้อมูล ทังภายในหน่วยงานเองและในการประสานงานกับซัพพลายเออร์และพันธมิตรต่าง ๆ โดยเฉพาะอย่างยิงสำหรับหน่วยงานทีต้องมีการประสานงานกันระหว่างแผนกและระหว่างพืนทีต่าง ๆ อย่าง NHS

Miriam Brown
@Kingston_MBrown

ผู้จัดการฝ่ายการตลาดเชิงกลยุทธ์แบบ B2B จาก
Kingston Technology

"เราจำหน่ายผลิตภัณฑ์เป็นจำนวนมากให้แก่ NHS แต่ทุกความไว้วางใจทีเราได้รับล้วนมีข้อแตกต่าง เมือเราสอบถามเกียวกับนโยบายและขันตอนในการรักษาความปลอดภัยของข้อมูลของพวกเขา"

ระบบสแกนแนวนอน

เทคโนโลยีมีการเปลียนแปลงอย่างรวดเร็ว และหลายครังก้าวไปได้เร็วกว่ามาตรการด้านความปลอดภัยทีมี เทคโนโลยีใหม่ ๆ ทีเกิดขึนมากมาย เช่น การจ่ายเงินผ่านระบบตรวจจำใบหน้าในประเทศจีน ก็เป็นอีกตัวอย่างทีหน่วยงานตาง ๆ พยายามแข่งขันด้านเทคโนโลยีโดยมองด้านความปลอดภัยและการปกป้องข้อมูลเป็นประเด็นรอง เครือข่าย 5G ทีขยายตัวอย่างรวดเร็วในช่วงเวลาเพียงหนึงถึงสองปี มาพร้อมกับ Edge Computing รวมทังระบบ Distributed Data Silo ทีเริมมีการใช้งานจริง ผู้ให้บริการด้านเทคนิคจึงต้องสามารถช่วยให้องค์กรต่าง ๆ สามารถใช้ประโยชน์จากเทคโนโลยีใหม่ ๆ ได้อย่างปลอดภัยโดยไม่กระทบต่อความสมบูรณ์ของข้อมูลและการรักษาความปลอดภัยด้าน IT

Sally Eaves
@sallyeaves

CEO และผู้อำนวยการของ
Sally Eaves Consultancy

"ฉันเชือว่าเราจะเริมเห็นการเปลียนแปลงเกียวกับ GDPR จากเดิมทีเน้นด้านการลดปัญหาจากการดำเนินการเป็นการให้ความสำคัญกับการปรับปรุงสิทธิภาพ เช่น กระบวนการด้าน IT ระบบสำรองและกู้ข้อมูลทีดีขึน และระบบความปลอดภัยทีดีกว่าเดิม และใช้สิงเหล่านีเพือสร้างความแตกต่างจากผู้ประกอบการรายอืน ๆ"

สรุป

GDPR นำการเปลี่ยนแปลงมาสู่ธุรกิจต่าง ๆ เพื่อยกระดับความเป็นส่วนตัวของข้อมูลและความปลอดภัยของระบบเครือข่ายทั้งในมุมมองของผู้บริหารและผู้บริโภคในเวลาเดียวกัน อย่างไรก็ตาม การปฏิบัติตามจะต้องอาศัยที่ปรึกษาเพื่อให้คำแนะนำด้านการรักษาความปลอดภัยของข้อมูลแบบวันต่อวันกับบุคลากรในทุกฝ่าย เทคโนโลยีและภัยคุกคามทางคอมพิวเตอร์ที่เปลี่ยนแปลงอยู่ตลอดเวลาทำให้โครงสร้างรองรับด้านการรักษาความปลอดภัยและการฝึกอบรมที่ดี พร้อมทั้งการให้คำปรึกษาด้านเทคโนโลยีและความเป็นส่วนตัวของข้อมูลกลายเป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับธุรกิจ การแจ้งเตือนพนักงานเกี่ยวกับบุคคลที่อยู่เบื้องหลังข้อมูลต่าง ๆ อาจต้องมีการเน้นย้ำไปพร้อม ๆ กับการสร้างวัฒนธรรมในการปกป้องข้อมูลสำหรับกลุ่มผู้ปฏิบัติงานของคุณ การเปลี่ยนแปลงด้านวัฒนธรรมถือเป็นแนวทางที่จะมีประสิทธิภาพกว่าการฝึกอบรมแบบบอกเล่ามาก

เกียวกับ Kingston

ประสบการณ์กว่า 32 ปีทำให้ Kingston มีองค์ความรู้ในการพิจารณาและแก้ไขปัญหาในการทำงานจากระยะไกล ทำให้เกิดความสะดวกและแรงงาของคุณ ในการทำงานได้อย่างปลอดภัยจากทุกทีโดยไม่กระทบต่อหน่วยงานของคุณ

#KingstonIsWithYou